aws

Manual do usuário

Amazon Fraud Detector

Versão latest

Amazon Fraud Detector: Manual do usuário

Table of Contents

O que é o Amazon Fraud Detector?

O Amazon Fraud Detector é um serviço de detecção de fraudes totalmente gerenciado que automatiza a detecção de atividades potencialmente fraudulentas on-line. Essas atividades incluem transações não autorizadas e a criação de contas falsas. O Amazon Fraud Detector funciona usando aprendizado de máquina para analisar seus dados. Ele faz isso de uma forma que se baseia na experiência experiente de mais de 20 anos em detecção de fraudes na Amazon.

Você pode usar o Amazon Fraud Detector para criar modelos personalizados de detecção de fraudes, adicionar lógica de decisão para interpretar as avaliações de fraude do modelo e atribuir resultados, como aprovação ou envio para análise, para cada avaliação de fraude possível. Com o Amazon Fraud Detector, você não precisa de experiência em aprendizado de máquina para detectar atividades fraudulentas.

Para começar, colete e prepare os dados de fraude que você coletou em sua organização. Em seguida, o Amazon Fraud Detector usa esses dados para treinar, testar e implantar um modelo personalizado de detecção de fraudes em seu nome. Como parte desse processo, o Amazon Fraud Detector usa modelos de aprendizado de máquina que aprenderam padrões de fraude AWS e a própria experiência em fraudes da Amazon para avaliar seus dados de fraude e gerar pontuações e dados de desempenho do modelo. Você configura a lógica de decisão para interpretar a pontuação do modelo e atribuir resultados sobre como lidar com cada avaliação de fraude.

Benefícios

O Amazon Fraud Detector oferece os seguintes benefícios. Esses benefícios possibilitam que você detecte fraudes rapidamente sem precisar investir o tempo e os recursos tradicionalmente necessários para criar e manter um sistema de gerenciamento de fraudes.

Criação automatizada de modelos de fraude

Os modelos de detecção de fraudes do Amazon Fraud Detector são modelos de aprendizado de máquina totalmente automatizados, personalizados para atender às suas necessidades comerciais específicas. Você pode usar os modelos do Amazon Fraud Detector para identificar possíveis fraudes em qualquer transação on-line, como criação de novas contas, pagamentos on-line e pagamento de hóspedes.

Como os modelos de fraude são criados por meio de um processo automatizado, você pode renunciar a muitas das etapas associadas à criação e ao treinamento de um modelo. Essas etapas

incluem validação e enriquecimento de dados, engenharia de recursos, seleção de algoritmos, ajuste de hiperparâmetros e implantação de modelos.

Para criar um modelo de detecção de fraudes usando o Amazon Fraud Detector, você só carrega o conjunto de dados históricos de fraudes da sua empresa e seleciona o tipo de modelo. Em seguida, o Amazon Fraud Detector encontra automaticamente o algoritmo de detecção de fraudes mais adequado para seu caso de uso e cria o modelo. Você não precisa conhecer programação nem ter experiência em aprendizado de máquina para criar modelos de detecção de fraudes.

Modelos de fraude que evoluem e aprendem

Os modelos de detecção de fraudes devem evoluir constantemente para acompanhar as mudanças no cenário de fraudes. O Amazon Fraud Detector faz isso automaticamente calculando informações, incluindo idade da conta, tempo desde a última atividade e contagem de atividades. O resultado é que seu modelo aprende a diferença entre clientes confiáveis que fazem transações com frequência e as tentativas contínuas típicas de fraudadores. Isso ajuda a manter o desempenho do seu modelo por mais tempo entre as sessões de reciclagem.

Visualização do desempenho do modelo de fraude

Depois que seu modelo é treinado usando os dados que você fornece, o Amazon Fraud Detector valida o desempenho do seu modelo. Ele também fornece ferramentas visuais para você avaliar o desempenho. Para cada modelo que você treina, você pode ver a pontuação de desempenho do modelo, o gráfico de distribuição da pontuação, a matriz de confusão, a tabela de limites e todas as entradas fornecidas classificadas por seu impacto no desempenho do modelo. Usando essas ferramentas de desempenho, você pode aprender o desempenho do seu modelo e quais entradas estão impulsionando o desempenho do seu modelo. Se necessário, você pode ajustar seu modelo para melhorar seu desempenho geral.

Previsão de fraudes

O Amazon Fraud Detector gera previsões de fraudes para as atividades comerciais da sua organização. A previsão de fraude é uma avaliação do risco de fraude de uma atividade comercial. O Amazon Fraud Detector gera previsões usando a lógica de previsão com os dados associados à atividade. Você forneceu esses dados ao criar seu modelo de detecção de fraudes. Você pode obter previsões de fraude para uma única atividade em tempo real ou obter previsões de fraude off-line para um conjunto de atividades.

Visualização da explicação da previsão de fraudes

O Amazon Fraud Detector gera explicações de previsão como parte do processo de previsão de fraudes. As explicações de previsão fornecem informações sobre como cada elemento de dados usado para treinar seu modelo afetou a pontuação de previsão de fraudes do seu modelo. As explicações de previsão são fornecidas usando ferramentas visuais, como tabelas e gráficos. Você pode usar essas ferramentas para identificar visualmente quanta influência cada elemento de dados tem nas pontuações de previsão. Em seguida, você pode usar essas informações para analisar os padrões de fraude em seu conjunto de dados e detectar preconceitos, se houver. Por último, você também pode usar as explicações de previsão para identificar os principais indicadores de risco durante um processo manual de investigação de fraudes. Isso ajuda a restringir as causas-raiz que levam a previsões falsas positivas.

Ações baseadas em regras

Depois que seu modelo de detecção de fraudes for treinado, você poderá adicionar regras para realizar ações nos dados avaliados, como aceitar os dados, enviar dados para análise ou coletar mais dados. Uma regra é uma condição que diz ao Amazon Fraud Detector como interpretar os dados durante a previsão de fraudes. Por exemplo, você pode criar uma regra que sinalize contas de clientes suspeitas para serem revisadas. Você pode definir essa regra para ser iniciada se a pontuação do modelo detectado for maior que o limite predeterminado e se o código de autorização de pagamento da conta (AUTH_CODE) não for válido.

Conceitos e termos fundamentais

A seguir está uma lista dos principais conceitos e termos usados no Amazon Fraud Detector:

Evento

Um evento é a atividade comercial da sua organização que é avaliada quanto ao risco de fraude. O Amazon Fraud Detector gera previsões de fraudes para eventos.

Rótulo

Um rótulo classifica um único evento como fraudulento ou legítimo. Os rótulos são usados para treinar modelos de aprendizado de máquina no Amazon Fraud Detector.

Entidade

Uma entidade representa quem está realizando o evento. Você fornece o ID da entidade como parte dos dados de fraude da sua empresa para indicar a entidade específica que realizou o evento.

Tipo de evento

Um tipo de evento define a estrutura de um evento enviado ao Amazon Fraud Detector. Isso inclui os dados enviados como parte do evento, a entidade que realiza o evento (como um cliente) e os rótulos que classificam o evento. Exemplos de tipos de eventos incluem transações de pagamento on-line, registros de contas e autenticação.

Tipo de entidade

Um tipo de entidade classifica a entidade. Classificações de exemplo incluem cliente, comerciante ou conta.

Conjunto de dados do evento

O conjunto de dados do evento são os dados históricos da sua empresa sobre uma atividade comercial específica ou um evento. Por exemplo, o evento da sua empresa pode ser o registro de uma conta on-line. Os dados de um único evento (registro) podem incluir o endereço IP, endereço de e-mail, endereço de cobrança e data e hora do evento associados. Você fornece um conjunto de dados de eventos ao Amazon Fraud Detector para criar e treinar modelos de detecção de fraudes.

Modelo

Um modelo é uma saída de algoritmos de aprendizado de máquina. Esses algoritmos são implementados em código e executados nos dados de eventos que você fornece.

Tipo do modelo

O tipo de modelo define os algoritmos, os enriquecimentos e as transformações de recursos que são usados durante o treinamento do modelo. Ele também define os requisitos de dados para treinar o modelo. Essas definições funcionam para otimizar seu modelo para um tipo específico de fraude. Você especifica o tipo de modelo a ser usado ao criar seu modelo.

Treinamento de modelos

O treinamento de modelos é o processo de usar um conjunto de dados de eventos fornecido para criar um modelo capaz de prever eventos fraudulentos. Todas as etapas do processo de treinamento do modelo são totalmente automatizadas. Essas etapas incluem validação de dados, transformação de dados, engenharia de recursos, seleção de algoritmos e otimização de modelos.

Pontuação do modelo

A pontuação do modelo é o resultado da avaliação dos dados históricos de fraudes da sua empresa. Durante o processo de treinamento do modelo, o Amazon Fraud Detector avalia o

conjunto de dados em busca de atividades fraudulentas e gera uma pontuação entre 0 e 1000. Para essa pontuação, 0 representa baixo risco de fraude, enquanto 1000 representa o maior risco de fraude. A pontuação em si está diretamente relacionada à taxa de falsos positivos (FPR).

Versão do modelo

Uma versão do modelo é um resultado do treinamento de um modelo.

Implantação de modelos

A implantação do modelo é um processo para ativar uma versão do modelo e disponibilizá-la para gerar previsões de fraudes.

Endpoint SageMaker modelo Amazon

Além de criar modelos usando o Amazon Fraud Detector, você pode, opcionalmente, usar endpoints SageMaker de modelos hospedados nas avaliações do Amazon Fraud Detector.

Para obter mais informações sobre como criar um modelo em SageMaker, consulte Treinar um modelo com Amazon SageMaker.

Detector

Um detector contém a lógica de detecção, como o modelo e as regras de um evento específico que você deseja avaliar quanto à fraude. Você cria um detector usando uma versão modelo.

Versão do detector

Um detector pode ter várias versões, com cada versão tendo um status de`Draft`,`Active`, ou`Inactive`. Somente uma versão do detector pode estar em `Active` status por vez.

Variável

Uma variável representa um elemento de dados associado a um evento que você deseja usar em uma previsão de fraude. As variáveis podem ser enviadas com um evento como parte de uma previsão de fraude ou derivadas, como a saída de um modelo do Amazon Fraud Detector ouAmazon SageMaker.

Regra

Uma regra é uma condição que diz ao Amazon Fraud Detector como interpretar valores variáveis durante uma previsão de fraude. Uma regra consiste em uma ou mais variáveis, uma expressão lógica e um ou mais resultados. As variáveis usadas na regra devem fazer parte do conjunto de dados de eventos que o detector avalia. Além disso, cada detector deve ter pelo menos uma regra associada a ele.

Outcome

Esse é o resultado, ou resultado, de uma previsão de fraude. Cada regra usada em uma previsão de fraude deve especificar um ou mais resultados.

Previsão de fraudes

A previsão de fraudes é uma avaliação da fraude em um único evento ou em um conjunto de eventos. O Amazon Fraud Detector gera previsões de fraude para um único evento on-line em tempo real, fornecendo de forma síncrona uma pontuação do modelo e um resultado com base nas regras. O Amazon Fraud Detector gera previsões de fraude para um conjunto de eventos off-line. Você pode usar as previsões para realizar uma análise off-line proof-of-concept ou para avaliar retrospectivamente o risco de fraude de hora em hora, dia ou semana.

Explicação da previsão de fraude

As explicações de previsão de fraude fornecem informações sobre como cada variável afetou a pontuação de previsão de fraude do seu modelo. Ele fornece informações sobre como cada variável influencia as pontuações de risco em termos de magnitude (variando de 0 a 5, com 5 sendo o mais alto) e direção (aumentando ou diminuindo a pontuação).

Como funciona o Amazon Fraud Detectore

O Amazon Fraud Detector cria um modelo de aprendizado de máquina personalizado para detectar possíveis atividades on-line fraudulentas em sua empresa. Para começar, conceda conceda seguinte ao caso de uso comercial. Dependendo do seu caso de uso comercial, o Amazon Fraud Detector recomenda um tipo de modelo que será usado para criar um modelo de detecção de fraudes para você. Além disso, ele também fornece informações sobre os elementos de dados que você precisa fornecer como parte dos dados históricos da sua empresa. O Amazon Fraud Detector usa o conjunto de dados históricos para criar e treinar automaticamente um modelo personalizado para você.

O processo automatizado de treinamento de modelos envolve a escolha de um algoritmo de aprendizado de máquina que detecta fraudes em seu caso de uso comercial específico, a validação dos dados fornecidos e a realização de manipulações de dados para melhorar o desempenho do modelo. Depois de treinar o modelo, o Amazon Fraud Detector gera pontuações do modelo e outras métricas de desempenho do modelo. Você pode usar a pontuação e as métricas de desempenho para avaliar o desempenho do modelo. Se necessário, você pode adicionar ou remover elementos de dados do conjunto de dados fornecido para treinamento e treinar novamente o modelo para melhorar a pontuação do modelo.

Depois que o modelo é criado, treinado e ativado, você precisa configurar a lógica de decisão, também conhecida como regras, que diz ao modelo como interpretar os dados gerados pela sua empresa e atribuir resultados sobre como lidar com a interpretação de cada atividade. Os resultados podem representar ações como aprovar ou revisar a atividade, ou podem representar os níveis de risco da atividade, como alto risco, médio risco e baixo risco.

Um detector é um contêiner que contém seu modelo e as regras associadas. Você precisará criar, testar e implantar o detector em seu ambiente de produção.

O detector implantado em seu ambiente de produção fornece a capacidade de detecção de fraudes para seus aplicativos de negócios. Para realizar a avaliação de fraudes, o modelo compara todos os dados recebidos de sua atividade comercial com os dados históricos da sua empresa e usa seus sofisticados algoritmos de aprendizado de máquina com as regras que você criou para analisar os resultados e atribuir resultados. Com o Amazon Fraud Detector, você pode avaliar dados de uma única atividade comercial em tempo real ou avaliar dados de várias atividades comerciais off-line.

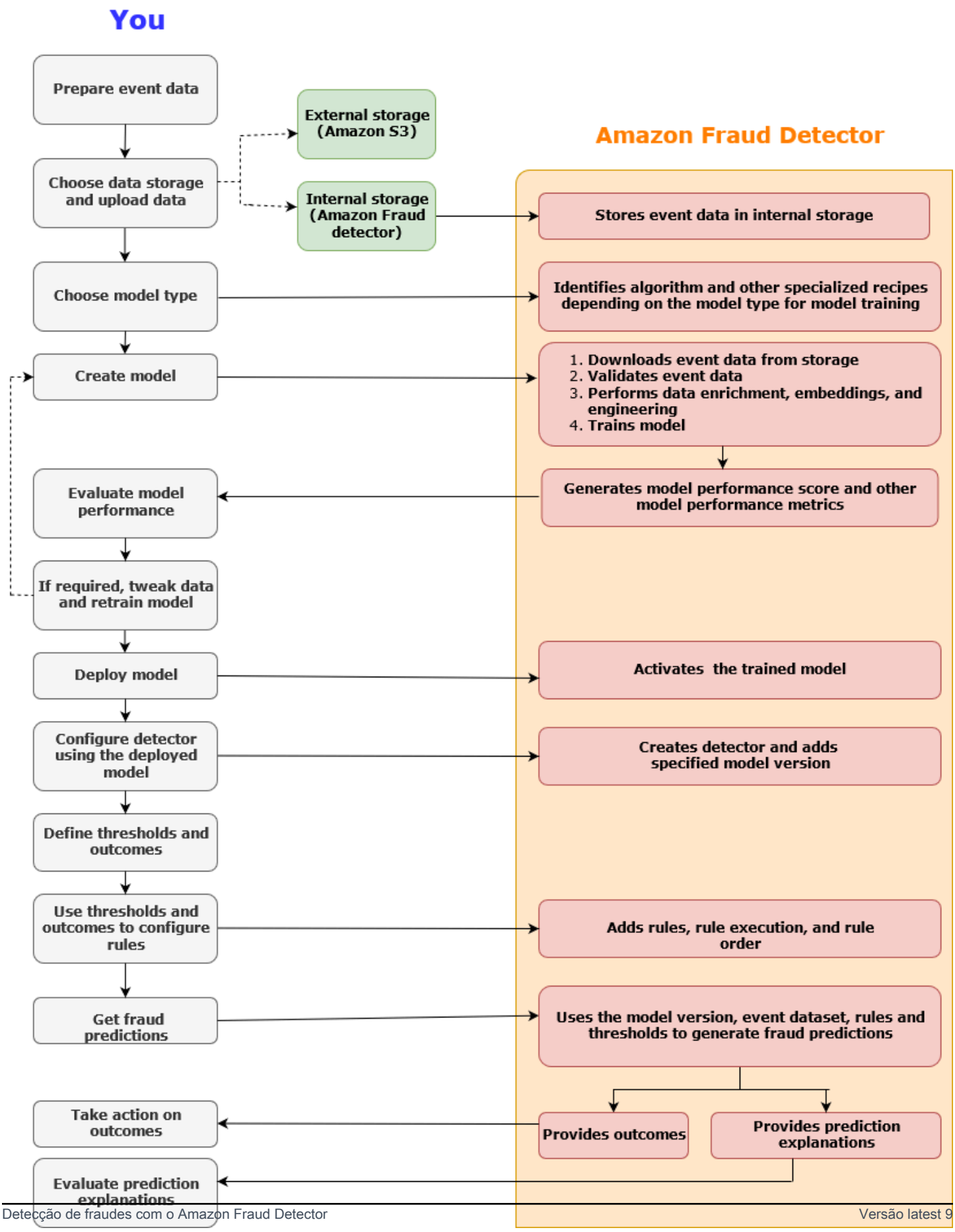
Digamos que você tenha uma empresa que tenha a transferência de fundos on-line como uma de suas atividades. Você quer usar o Amazon Fraud Detector para detectar solicitações fraudulentas de transferência de fundos em tempo real. Para começar, você precisará primeiro fornecer ao Amazon Fraud Detector dados de solicitações anteriores de transferência de fundos. O Amazon Fraud Detector usa esses dados para criar e treinar um modelo personalizado para detectar solicitações fraudulentas de transferências de fundos. Em seguida, você cria um detector adicionando o modelo e configurando regras para que seu modelo interprete os dados. Um exemplo de regra para atividades de transferência de fundos on-line pode ser, se a solicitação de transferência de fundos for proveniente dexyz@example.comendereço de e-mail, envie a solicitação de revisão. No ambiente de produção da sua empresa, quando chega uma solicitação de transferência de fundos, o modelo analisa os dados que vieram com a solicitação e usa a regra para atribuir o resultado. Em seguida, você pode realizar uma ação na solicitação, dependendo do resultado atribuído.

O Amazon Fraud Detector usa componentes como conjunto de dados de treinamento, modelo, detector, regras e resultados para fornecer à sua empresa uma lógica de avaliação de fraudes.

Para obter informações sobre o fluxo de trabalho que você usará para detectar fraudes usando o Amazon Fraud Detector, consulteDetecção de fraudes com o Amazon Fraud Detector

Detecção de fraudes com o Amazon Fraud Detector

Esta seção descreve um fluxo de trabalho típico para detectar fraudes com o Amazon Fraud Detector. Também resume como você pode realizar essas tarefas. O diagrama a seguir fornece uma visão de alto nível do fluxo de trabalho para detectar fraudes com o 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

A detecção de fraudes é um processo contínuo. Depois de implantar seu modelo, certifique-se de avaliar suas pontuações e métricas de desempenho com base nas explicações da previsão. Ao fazer isso, você pode identificar os principais indicadores de risco, restringir as causas-raiz que levam a falsos positivos e analisar padrões de fraude em seu conjunto de dados e detectar preconceitos, se houver. Para aumentar a precisão das previsões, você pode ajustar seu conjunto de dados para incluir dados novos ou revisados. Em seguida, você pode retreinar seu modelo com o conjunto de dados atualizado. À medida que mais dados se tornam disponíveis, você continua treinando seu modelo para aumentar a precisão.

Acessando o Amazon Fraud Detector

O Amazon Fraud Detector está disponível em várias Regiões da AWS versões e pode ser acessado usando AWS interfaces.

Disponibilidade

O Amazon Fraud Detector está disponível no Leste dos EUA (Norte da Virgínia), Leste dos EUA (Ohio), Oeste dos EUA (Oregon), Europa (Irlanda), Ásia-Pacífico (Cingapura) e Ásia-Pacífico (Sydney)Regiões da AWS.

Interfaces

Você pode criar, treinar, implantar, testar, executar e gerenciar modelos e detectores de detecção de fraudes usando qualquer uma das seguintes interfaces:

AWS Management Console- O Amazon Fraud Detector fornece uma interface de usuário baseada na web, o console Amazon Fraud Detector. Se você se inscreveu em umConta da AWS, você pode acessar o console do Amazon Fraud Detector. Para obter mais informações, consulte Configurar o Amazon Fraud Detector.

AWS Command Line Interface(AWS CLI) - Fornece uma interface que você pode usar para interagir com um amplo conjunto de comandosServiços da AWS, incluindo o Amazon Fraud Detector, em seu shell de linha de comando. AWS CLIos comandos do Amazon Fraud Detector implementam uma funcionalidade equivalente à fornecida pelo console do Amazon Fraud Detector.

AWSSDK — fornece APIs específicas de linguagem e gerencia muitos detalhes da conexão, como cálculo de assinatura, tratamento de novas tentativas de solicitação e tratamento de erros. Para obter mais informações, acesse a AWS página Ferramentas para criar, role para baixo até a seção SDK e escolha o sinal de adição (+) para expandir a seção.

AWS CloudFormation- Fornece modelos que você pode usar para definir seus recursos e propriedades do Amazon Fraud Detector. Para obter mais informações, consulte a referência do tipo de recurso do Amazon Fraud Detector no Guia AWS CloudFormation do usuário.

Definição de preço

Com o Amazon Fraud Detector, você paga somente pelo que usa. Não há tarifas mínimas nem compromissos antecipados. Você é cobrado com base nas horas de computação usadas para treinar e hospedar seus modelos, na quantidade de armazenamento que você usa e na quantidade de previsões de fraude que você faz. Para obter mais informações, consulte os preços do Amazon Fraud Detector.

Configurar o Amazon Fraud Detector

Para usar o Amazon Fraud Detector, primeiro você precisa de uma conta da Amazon Web Services (AWS) e, em seguida, deve configurar permissões que dêem Conta da AWS acesso a todas as interfaces. Posteriormente, quando você começar a criar seus recursos do Amazon Fraud Detector, precisará conceder permissões que permitam que o Amazon Fraud Detector acesse sua conta para realizar tarefas em seu nome e acessar recursos que você possui.

Conclua as seguintes tarefas nesta seção para se preparar para usar o Amazon Fraud Detector:

- Inscreva-se em AWS.
- Configure permissões que permitam Conta da AWS acessar as interfaces do Amazon Fraud Detector.
- Configure as interfaces que você deseja usar para acessar o Amazon Fraud Detector.

Depois de concluir essas etapas, consulte Conceitos básicos do Amazon Fraud Detector para continuar começando a usar o Amazon Fraud Detector.

Inscreva-se para AWS

Quando você se inscreve no Amazon Web Services (AWS), você se inscreve automaticamente em todos os serviços AWS, incluindo o Amazon Fraud Detector. Conta da AWS Você será cobrado apenas pelos serviços que usar. Se você já tiver uma Conta da AWS, vá para a próxima tarefa.

Inscreva-se para um Conta da AWS

Se você não tiver um Conta da AWS, conclua as etapas a seguir para criar um.

Para se inscrever em um Conta da AWS

1. Abra https://portal.aws.amazon.com/billing/signup.
2. Siga as instruções on-line.

   Parte do procedimento de inscrição envolve receber uma chamada telefônica e digitar um código de verificação no teclado do telefone.

   Quando você se inscreve em um Conta da AWS, um Usuário raiz da conta da AWSé criado. O usuário-raiz tem acesso a todos os Serviços da AWS e recursos na conta. Como prática

recomendada de segurança, atribua o acesso administrativo a um usuário e use somente o usuário-raiz para executar tarefas que exigem acesso de usuário-raiz.

AWS envia um e-mail de confirmação após a conclusão do processo de inscrição. A qualquer momento, é possível visualizar as atividades da conta atual e gerenciar sua conta acessando https://aws.amazon.com/ e selecionando Minha conta.

Criar um usuário com acesso administrativo

Depois de se inscrever em um Conta da AWS, proteja seu Usuário raiz da conta da AWS AWS IAM Identity Center, habilite e crie um usuário administrativo para que você não use o usuário root nas tarefas diárias.

Proteja seu Usuário raiz da conta da AWS

1. Faça login AWS Management Consolecomo proprietário da conta escolhendo Usuário raiz e inserindo seu endereço de Conta da AWS e-mail. Na próxima página, digite sua senha.

   Para obter ajuda ao fazer login usando o usuário-raiz, consulte Signing in as the root user (Fazer login como usuário-raiz) no Guia do usuário do Início de Sessão da AWS .
2. Habilite a autenticação multifator (MFA) para o usuário-raiz.

   Para obter instruções, consulte Habilitar um dispositivo de MFA virtual para seu usuário Conta da AWS raiz (console) no Guia do usuário do IAM.

Criar um usuário com acesso administrativo

1. Habilitar o IAM Identity Center.

   Para obter instruções, consulte Habilitar AWS IAM Identity Center no Guia do usuário do AWS IAM Identity Center .
2. No Centro de Identidade do IAM, conceda o acesso administrativo para um usuário.

   Para ver um tutorial sobre como usar o Diretório do Centro de Identidade do IAM como fonte de identidade, consulte Configurar o acesso do usuário com o padrão Diretório do Centro de Identidade do IAM no Guia AWS IAM Identity Center do usuário.

Iniciar sessão como o usuário com acesso administrativo

- Para fazer login com seu usuário do Centro de Identidade do IAM, use a URL de login que foi enviada ao seu endereço de e-mail quando você criou o usuário do Centro do Usuário do IAM.

  Para obter ajuda para fazer login usando um usuário do IAM Identity Center, consulte Como fazer login no portal de AWS acesso no Guia Início de Sessão da AWS do usuário.

Atribuir acesso a usuários adicionais

1. No Centro de Identidade do IAM, crie um conjunto de permissões que siga as práticas recomendadas de aplicação de permissões com privilégio mínimo.

   Para obter instruções, consulte Create a permission set no Guia do usuário do AWS IAM Identity Center .
2. Atribua usuários a um grupo e, em seguida, atribua o acesso de autenticação única ao grupo.

   Para obter instruções, consulte Add groups no Guia do usuário do AWS IAM Identity Center .

Configure permissões para acessar as interfaces do Amazon Fraud Detector

Para usar o Amazon Fraud Detector, configure permissões para acessar o console do Amazon Fraud Detector e as operações de API.

Seguindo as melhores práticas de segurança, crie um usuário AWS Identity and Access Management (IAM) com acesso restrito às operações do Amazon Fraud Detector e com as permissões necessárias. Você pode adicionar outras permissões se necessário.

As políticas a seguir fornecem a permissão necessária para usar o Amazon Fraud Detector:

- `AmazonFraudDetectorFullAccessPolicy`

  Permite que você execute as seguintes ações:
  - Acesse todos os recursos do Amazon Fraud Detector
  - Liste e descreva todos os endpoints do modelo em SageMaker
  - Listar todas as funções do IAM na conta
  - Listar todos os buckets do Amazon S3

  - Permita que a função IAM Pass passe uma função para o Amazon Fraud Detector
- `AmazonS3FullAccess`

  Permite acesso total Amazon Simple Storage Service a. Isso é necessário se você precisar carregar conjuntos de dados de treinamento para o Amazon S3.

A seguir, descrevemos como criar um usuário do IAM e atribuir as permissões necessárias.

Para criar um usuário e atribuir as permissões necessárias

1. Faça login AWS Management Console e abra o console do IAM em https://console.aws.amazon.com/iam/.
2. No painel de navegação, escolha Usuários e depois Adicionar usuário.
3. Em User name (Nome do usuário), digite **`AmazonFraudDetectorUser`**.
4. Marque a caixa de seleção Acesso ao AWS Management Console e, em seguida, configure a senha do usuário.
5. (Opcional) Por padrão, AWS exige que o novo usuário crie uma nova senha quando fizer login pela primeira vez. Você pode desmarcar a caixa de seleção próxima de User must create a new password at next sign-in (O usuário deve criar uma senha no próximo login) para permitir que o novo usuário redefina a senha depois de fazer login.
6. Escolha Próximo: Permissões.
7. Escolha Criar grupo.
8. Em Nome do grupo, insira**`AmazonFraudDetectorGroup`**.
9. Na lista de políticas, marque a caixa de seleção para AmazonFraudDetectorFullAccessPolicye AmazonS3 FullAccess. Escolha Criar grupo.
10. Na lista de grupos, marque a caixa de seleção para seu novo grupo. Escolha Atualizar se você não vê o grupo na lista.
11. Escolha Next: Tags (Próximo: etiquetas).
12. (Opcional) Adicione metadados ao usuário anexando tags como pares de chave-valor. Para obter instruções sobre como usar tags no IAM, consulte Como marcar usuários e funções do IAM.
13. Escolha Avançar: Revisar para ver os detalhes do usuário e o resumo das permissões do novo usuário. Quando estiver pronto para continuar, escolha Criar usuário.

Configure interfaces para acessar o Amazon Fraud Detector com

Você pode acessar o Amazon Fraud Detector usando o console do Amazon Fraud Detector ou o AWS SDK. AWS CLI Antes de usá-los, primeiro configure o AWS CLI e AWS SDK.

Acesse o console do Amazon Fraud Detector

Você pode acessar o console do Amazon Fraud Detector e outros AWS serviços por meio do AWS Management Console. Seu Conta da AWS, concede a você acesso ao AWS Management Console.

Para acessar o console do Amazon Fraud Detector,

1. Acesse https://console.aws.amazon.com/ e faça login no seu Conta da AWS.
2. Navegue até o Amazon Fraud Detector.

Com o console Amazon Fraud Detector, você pode criar e gerenciar seus modelos e recursos de detecção de fraudes, como detectores, variáveis, eventos, entidades, rótulos e resultados. Você pode gerar previsões e avaliar o desempenho e as previsões do seu modelo.

Configurar AWS CLI

Você pode usar AWS Command Line Interface (AWS CLI) para interagir com o Amazon Fraud Detector executando comandos em seu shell de linha de comando. Com uma configuração mínima, você pode usar o AWS CLI para executar comandos para obter uma funcionalidade semelhante à fornecida pelo console do Amazon Fraud Detector a partir do prompt de comando em seu terminal.

Para configurar o AWS CLI

Faça download e configure a AWS CLI. Para obter instruções, consulte os seguintes tópicos no Guia AWS Command Line Interface do usuário:

- Configurando a interface de linha de AWS comando
- Configurando a interface de linha de AWS comando

Para obter informações sobre os comandos do Amazon Fraud Detector, consulte Comandos disponíveis

Configurar o AWS SDK

Você pode usar os AWS SDKs para escrever código para criar e gerenciar seus recursos de detecção de fraudes e para obter previsões de fraudes. Os AWS SDKs são compatíveis com Amazon Fraud Detector in JavaScripte Python (Boto3).

Para configurar AWS SDK for Python (Boto3)

Você pode usar AWS SDK for Python (Boto3) para criar, configurar e gerenciar AWS serviços. Para obter instruções sobre como instalar o Boto, consulte AWS SDK para Python (Boto3). Verifique se você está usando o SDK do Boto3 versão 1.14.29 ou superior.

Depois de instalar AWS SDK for Python (Boto3), execute o seguinte exemplo em Python para confirmar se seu ambiente está configurado corretamente. Se estiver configurada corretamente, a resposta conterá uma lista de detectores. Se nenhum detector tiver sido criado, a lista estará vazia.

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

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

Para configurar AWS SDKs para Java

Para obter instruções sobre como instalar e carregar o AWS SDK for JavaScript, consulte Configurando o SDK para JavaScript.

Conceitos básicos do Amazon Fraud Detector

Antes de começar, verifique se você leuDetecção de fraudes com o Amazon Fraud Detector e concluiu as etapas deConfigurar o Amazon Fraud Detector.

Use os tutoriais práticos nesta seção para aprender como usar o Amazon Fraud Detector para criar, treinar e implantar um modelo de detecção de fraude. Neste tutorial, você assume o papel de analista de fraudes usando o modelo de aprendizado de máquina para prever se o registro de uma nova conta é fraudulento. O modelo deve ser treinado usando dados de registros de contas. O Amazon Fraud Detector fornece um exemplo de conjunto de dados de registro de conta para este tutorial. O conjunto de dados de exemplo deve ser carregado antes de você começar com o tutorial.

Você pode começar a usar o Amazon Fraud Detector usando uma das seguintes interfaces. Antes de começar o tutorial, verifique se você segue as instruções paraObtenha e faça upload de um conjunto de dados de exemplo

- Tutorial: Comece a usar o console Amazon Fraud Detector
- Tutorial: Conceitos básicos deAWS SDK for Python (Boto3)

Obtenha e faça upload de um conjunto de dados de exemplo

O exemplo de conjunto de dados que você usa neste tutorial fornece detalhes dos registros de contas on-line. O conjunto de dados está em um arquivo de texto que usa valor separado por vírgula (CSV) no formato UTF-8. A primeira linha do arquivo do conjunto de dados CSV contém os cabeçalhos. A linha do cabeçalho é seguida por várias linhas de dados. Cada uma dessas linhas consiste em elementos de dados de um único registro de conta. Os dados são rotulados para sua conveniência. Uma coluna no conjunto de dados identifica se o registro da conta é fraudulento.

Para obter e carregar um conjunto de dados de exemplo

1. Vá para Amostras.

   Há dois arquivos de dados com dados de registro de conta on-line: registration_data_20K_minimum.csv e registration_data_20K_full.csv. O arquivo`registration_data_20K_minimum` contém apenas duas variáveis: ip_address e email_address. O arquivo`registration_data_20K_full` contém outras variáveis. Essas variáveis são para cada evento e incluem billing_address, phone_number e user_agent. Ambos os arquivos de dados também contêm dois campos obrigatórios:

- EVENT_TIMESTAMP — Define quando o evento ocorreu
- EVENT_LABEL — Classifica o evento como fraudulento ou legítimo

Você pode usar qualquer um dos dois arquivos para este tutorial. Faça o download do arquivo de dados que você deseja usar.

2. Crie um bucketAmazon Simple Storage Service (Amazon S3).

   Nesta etapa, você cria um armazenamento externo para armazenar o conjunto de dados. Esse armazenamento externo é o bucket do Amazon S3. Para obter mais informações sobre o Amazon S3, consulte O que é o Amazon S3?

   a. Faça login no AWS Management Console e abra o console do Amazon S3 em https://console.aws.amazon.com/s3/.

   b. Em Buckets, escolha Create bucket.

   c. Em Nome do bucket, insira um nome de bucket. Certifique-se de seguir as regras de nomenclatura do bucket no console e fornecer um nome globalmente exclusivo. Recomendamos que você use um nome que descreva a finalidade do bucket.

   d. Para Região da AWS, escolha oRegião da AWS local em que você deseja criar o bucket. A região que você escolher deve oferecer suporte ao Amazon Fraud Detector. Para reduzir a latência, escolha oRegião da AWS que está mais próximo da sua localização geográfica. Para obter uma lista das regiões que oferecem suporte ao Amazon Fraud Detector, consulte a tabela de regiões no Guia de infraestrutura global.

   e. Deixe as configurações padrão de Propriedade de Objetos, Configurações de Bucket para Bloquear Acesso Público, Controle de Versão de Bucket e Tags para este tutorial.

   f. Em Criptografia padrão, escolha Desativar neste tutorial.

   g. Revise a configuração do bucket e escolha Create bucket.

3. Faça upload de arquivo de dados de exemplo para o bucket do Amazon S3.

   Agora que você tem um bucket, faça o upload de um dos arquivos de exemplo que você baixou anteriormente para o bucket do Amazon S3 que você acabou de criar.

   a. Nos Buckets, o nome do seu bucket está listado. Escolha o bucket.

   b. Escolha Upload (Carregar).

   c. Em Arquivos e pastas, escolha Adicionar arquivos.

d. Escolha um dos arquivos de dados de exemplo que você baixou no seu computador e escolha Abrir.

e. Deixe as configurações padrão para Destino, Permissões e Propriedades.

f. Revise as configurações e escolha Carregar.

g. O arquivo de dados de exemplo é carregado no bucket do Amazon S3. Anote a localização do balde. Em Objetos, escolha o arquivo de dados de exemplo que você acabou de carregar.

h. Na visão geral do objeto, copie o local em URI do S3. Esse é o local do Amazon S3 do seu arquivo de dados de exemplo. Você o usa mais tarde. Além disso, você pode copiar o nome de recurso da Amazon (ARN) do seu bucket S3 e salvá-lo.

Tutorial: Comece a usar o console Amazon Fraud Detector

Este tutorial consiste em duas partes. A primeira parte descreve como criar, treinar e implantar um modelo de detecção de fraudes. A segunda parte aborda como usar o modelo para gerar previsões de fraudes em tempo real. O modelo é treinado usando o arquivo de dados de exemplo que você carrega em um bucket do S3. Ao final deste tutorial, você concluirá as seguintes ações:

- Crie e treine um modelo de Fraud Detector da Amazon
- Gere previsões de fraude em tempo real

> **Important**
>
> Antes de continuar, verifique se você seguiu as instruções paraObtenha e faça upload de um conjunto de dados de exemplo

Parte A: Crie, treine e implante um modelo do Amazon Fraud Detector

Na parte A, você define seu caso de uso comercial, define seu evento, cria um modelo, treina o modelo, avalia o desempenho do modelo e implanta o modelo.

Etapa 1: Escolher o caso de uso de sua empresa

- Nesta etapa, você usa o explorador de modelos de dados para combinar seu caso de uso comercial com os tipos de modelos de detecção de fraudes suportados pelo Amazon Fraud

Detector. O Data Models Explorer é uma ferramenta integrada ao console Amazon Fraud Detector que recomenda um tipo de modelo a ser usado para criar e treinar um modelo de detecção de fraudes para seu caso de uso comercial. O Data Models Explorer também fornece informações sobre os elementos de dados obrigatórios, recomendados e opcionais que você precisará incluir em seu conjunto de dados. O conjunto de dados será usado para criar e treinar seu modelo de detecção de fraudes.

Para o propósito deste tutorial, seu caso de uso comercial é o registro de novas contas. Depois de especificar seu caso de uso comercial, o explorador de modelos de dados recomendará um tipo de modelo para criar um modelo de detecção de fraudes e também fornecerá uma lista dos elementos de dados necessários para criar seu conjunto de dados. Como você já fez o upload de um conjunto de dados de amostra contendo dados de novos registros de contas, não é necessário criar um novo conjunto de dados.

a. Abra o AWSManagement Console e faça login em sua conta. Navegue até Amazon Fraud Detector.

b. No painel de navegação à esquerda, selecione Explorador de modelos de dados.

c. Na página Explorador de modelos de dados, em Caso de uso comercial, selecione Nova fraude de conta.

d. O Amazon Fraud Detector exibe o tipo de modelo recomendado para criar um modelo de detecção de fraudes para o caso de uso comercial selecionado. O tipo de modelo define os algoritmos, enriquecimentos e transformações que o Amazon Fraud Detector usará para treinar seu modelo de detecção de fraudes.

   Anote o tipo de modelo recomendado. Você precisará disso mais tarde ao criar seu modelo.

e. O painel Informações do modelo de dados fornece informações sobre os elementos de dados obrigatórios e recomendados necessários para criar e treinar um modelo de detecção de fraudes.

   Dê uma olhada no conjunto de dados de amostra que você baixou e verifique se ele tem todos os elementos de dados obrigatórios e alguns recomendados listados na tabela.

   Posteriormente, ao criar um modelo para seu caso de uso comercial específico, você usará os insights fornecidos para criar seu conjunto de dados.

Etapa 2: criar tipo de evento

- Nesta etapa, você define a atividade comercial (evento) a ser avaliada em caso de fraude. Definir o evento envolve definir as variáveis que estão no conjunto de dados, a entidade que executa o evento e os rótulos que classificam o evento. Para este tutorial, você define o evento de registro da conta.

  a. Abra o AWSManagement Console e faça login em sua conta. Navegue até Amazon Fraud Detector.

  b. No painel de navegação esquerdo, escolha Events.

  c. Na página Tipo de eventos, escolha Criar.

  d. Em Detalhes do tipo de evento, insira`sample_registration` como nome do tipo de evento e, opcionalmente, insira uma descrição do evento.

  e. Em Entidade, escolha Criar entidade.

  f. Na página Criar entidade, insira`sample_customer` como o nome do tipo de entidade. Opcionalmente, insira uma descrição do tipo de entidade.

  g. Escolha Create entity (Criar entidade).

  h. Em Variáveis de evento, em Escolher como definir as variáveis desse evento, escolha Selecionar variáveis de um conjunto de dados de treinamento.

  i. Em Função do IAM, escolha Criar função do IAM.

  j. Na página Criar função do IAM, insira o nome do bucket do S3 para o qual você carregou seus dados de exemplo e escolha Criar função.

  k. Em Localização dos dados, insira o caminho para seus dados de exemplo. Esse é o`S3 URI` caminho que você salvou após fazer o upload dos dados de exemplo. O caminho é semelhante a este:`S3://`*`your-bucket-name`*`/`*`example dataset filename`*`.csv`.

  l. Escolha Upload (Carregar).

     O Amazon Fraud Detector extrai os cabeçalhos do seu arquivo de dados de exemplo e os mapeia com um tipo de variável. O mapeamento é exibido no console.

  m. Em Rótulos - opcional, para Rótulos, escolha Criar novos rótulos.

  n. Em Criar página de etiqueta, insira`fraud` como o nome. Esse rótulo corresponde ao valor que representa o registro fraudulento da conta no conjunto de dados de exemplo.

  o. Escolha Criar rótulo.

p. Crie um segundo rótulo e, em seguida, insira`legit` como nome. Esse rótulo corresponde ao valor que representa o registro legítimo da conta no conjunto de dados de exemplo.

q. Escolha Criar tipo de evento.

Etapa 3: criar modelo

1. Na página Modelos, escolha Adicionar modelo e, em seguida, escolha Criar modelo.
2. Para Etapa 1 — Definir detalhes do modelo, insira`sample_fraud_detection_model` como o nome do modelo. Opcionalmente, adicione uma descrição do modelo.
3. Em Tipo de modelo, escolha o modelo Online Fraud Insights.
4. Em Tipo de evento, escolha sample_registration. Esse é o tipo de evento criado na Etapa 1.
5. Em Dados históricos de eventos,

   a. Em Fonte de dados de eventos, escolha Dados de eventos armazenados no S3.

   b. Para a função do IAM, selecione a função criada na Etapa 1.

   c. Em Local de dados de treinamento, insira o caminho do URI do S3 para seu arquivo de dados de exemplo.
6. Escolha Next (Próximo).

Etapa 4: modelo de trem

1. Em Entradas do modelo, deixe todas as caixas de seleção marcadas. Por padrão, o Amazon Fraud Detector usa todas as variáveis do seu conjunto de dados de eventos históricos como entradas de modelo.
2. Em Classificação de rótulos, para rótulos de fraude, escolha fraude, pois esse rótulo corresponde ao valor que representa eventos fraudulentos no conjunto de dados de exemplo. Para rótulos legítimos, escolha legítimo, pois esse rótulo corresponde ao valor que representa eventos legítimos no conjunto de dados de exemplo.
3. Para o tratamento de eventos não rotulados, mantenha a seleção padrão Ignorar eventos não rotulados para este exemplo de conjunto de dados.
4. Escolha Next (Próximo).
5. Depois de revisar, escolha Criar e treinar o modelo. O Amazon Fraud Detector cria um modelo e começa a treinar uma nova versão do modelo.

Nas versões do modelo, a coluna Status indica o status do treinamento do modelo. O treinamento do modelo que usa o conjunto de dados de exemplo leva aproximadamente 45 minutos para ser concluído. O status muda para Pronto para implantação após a conclusão do treinamento do modelo.

Etapa 5: revisar o desempenho do modelo

Uma etapa importante no uso do Amazon Fraud Detector é avaliar a precisão do seu modelo usando pontuações e métricas de desempenho do modelo. Depois que o treinamento do modelo for concluído, o Amazon Fraud Detector valida o desempenho do modelo usando 15% dos seus dados que não foram usados para treinar o modelo e gera uma pontuação de desempenho do modelo e outras métricas de desempenho.

1. Para ver o desempenho do modelo,

   a. No painel de navegação à esquerda do console do Amazon Fraud Detector, selecione Modelos.

   b. Na página Modelos, escolha o modelo que você acabou de treinar (sample_fraud_detection_model) e escolha 1.0. Esta é a versão do Amazon Fraud Detector criada do seu modelo.

2. Veja a pontuação geral de desempenho do modelo e todas as outras métricas que o Amazon Fraud Detector gerou para esse modelo.

   Para saber mais sobre a pontuação de desempenho do modelo e as métricas de desempenho nesta página, consultePontuações do modeloMétricas de desempenho do modelo e.

   Você pode esperar que todos os seus modelos treinados do Amazon Fraud Detector tenham métricas de desempenho de detecção de fraudes no mundo real semelhantes às métricas de desempenho que você vê para o modelo neste tutorial.

Etapa 6: implantar o modelo

Depois de analisar as métricas de desempenho do seu modelo treinado e estar pronto para usá-lo, gerar previsões de fraude, você pode implantar o modelo.

1. No painel de navegação à esquerda do console do Amazon Fraud Detector, selecione Modelos.

2. Na página Modelos, escolha sample_fraud_detection_model e, em seguida, escolha a versão específica do modelo que você deseja implantar. Para este tutorial, escolha 1.0.
3. Na página Versão do modelo, escolha Ações e escolha Implantar versão do modelo.
4. Nas versões do modelo, o Status mostra o status da implantação. O status muda para Ativo após a conclusão da implantação. Isso indica que a versão do modelo está ativada e disponível para gerar previsões de fraude. Continue concluindoParte B: Gere previsões de fraudes as etapas para gerar previsões de fraudes.

Parte B: Gere previsões de fraudes

A previsão de fraudes é uma avaliação da fraude para uma atividade comercial (evento). O Amazon Fraud Detector usa detectores para gerar previsões de fraudes. Um detector contém lógica de detecção, como modelos e regras, para um evento específico que você deseja avaliar como fraude. A lógica de detecção usa regras para informar ao Amazon Fraud Detector como interpretar os dados associados ao modelo. Neste tutorial, você avalia o evento de registro da conta usando o conjunto de dados de exemplo de registro de conta que você carregou anteriormente.

Na Parte A, você criou, treinou e implantou seu modelo. Na Parte B, você cria um detector para o tipo de`sample_registration` evento, adiciona o modelo implantado, cria regras e uma ordem de execução de regras e, em seguida, cria e ativa uma versão do detector que você usa para gerar previsões de fraude.

Etapa 1: construir detector

Para criar um detector

1. No painel de navegação à esquerda do console do Amazon Fraud Detector, selecione Detectores.
2. Escolha Criar detector.
3. Na página Definir detalhes do detector, insira`sample_detector` o nome do detector. Opcionalmente, insira uma descrição para o detector, como`my sample fraud detector`.
4. Em Tipo de evento, selecione sample_registration. Esse é o evento que você criou na Parte A deste tutorial.
5. Escolha Next (Próximo).

Etapa 2: Adicionar modelo

Se você concluiu a Parte A deste tutorial, provavelmente já tem um modelo do Amazon Fraud Detector que está disponível para adicionar ao seu detector. Se você ainda não criou um modelo, vá para a Parte A e conclua as etapas para criar, treinar e implantar um modelo e continue com a Parte B.

1. Em Adicionar modelo - opcional, escolha Adicionar modelo.
2. Na página Adicionar modelo, em Selecionar modelo, escolha o nome do modelo do Amazon Fraud Detector que você implantou anteriormente. Em Selecionar versão, escolha a versão do modelo implantado.
3. Escolha Add model (Adicionar modelo).
4. Escolha Next (Próximo).

Etapa 3: adicionar regras

Uma regra é uma condição que define como o Amazon Fraud Detector como interpretará a pontuação de desempenho do modelo ao avaliar a previsão de fraudes. Para este tutorial, você cria três regras:`high_fraud_risk`,`medium_fraud_risk`,`low_fraud_risk` e.

1. Na página Adicionar regras, em Definir uma regra, insira`high_fraud_risk` o nome da regra e em Descrição - opcional, insira**`This rule captures events with a high ML model score`** como a descrição da regra.
2. Em Expressão, insira a seguinte expressão de regra usando a linguagem de expressão de regras simplificada do Amazon Fraud Detector:

   ```
   $sample_fraud_detection_model_insightscore > 900
   ```
3. Em Resultados, escolha Criar um novo resultado. Um resultado é o resultado de uma previsão de fraude e é retornado se a regra corresponder durante uma avaliação.
4. Em Criar um novo resultado, insira`verify_customer` como o nome do resultado. Opcionalmente, insira uma descrição.
5. Escolha Salvar resultado.
6. Escolha Adicionar regra para executar o verificador de validação de regras e salvar a regra. Depois de criado, o Amazon Fraud Detector disponibiliza a regra para uso em seu detector.
7. Escolha Adicionar outra regra e, em seguida, escolha a guia Criar regra.

8. Repita esse processo mais duas vezes para criar suas`low_fraud_risk` regras`medium_fraud_risk` e usando os seguintes detalhes da regra:

   - risco_de_fraudulento médio

     Nome da regra:`medium_fraud_risk`

     Resultado:`review`

     Expressão:

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

     ```
     $sample_fraud_detection_model_insightscore > 700
     ```

   - baixo risco de fraude

     Nome da regra:`low_fraud_risk`

     Resultado:`approve`

     Expressão:

     ```
     $sample_fraud_detection_model_insightscore <= 700
     ```

   Esses valores são exemplos usados neste tutorial. Ao criar regras para seu próprio detector, use valores apropriados para seu modelo e seu caso de uso,

9. Depois de criar todas as três regras, escolha Avançar.

   Para obter mais informações sobre como criar e escrever regras, consulteRegrasReferência do idioma da regra e.

Etapa 4: configurar a execução e a ordem das regras

O modo de execução de regras para as regras incluídas no detector determina se todas as regras definidas serão avaliadas ou se a avaliação da regra será interrompida na primeira regra correspondente. E a ordem das regras determina a ordem em que você deseja que a regra seja executada.

O modo de execução de regras padrão é`FIRST_MATCHED`.

Combinado pela primeira vez

O modo de execução da primeira regra correspondente retorna os resultados da primeira regra de correspondência com base na ordem definida da regra. Se você especificar `FIRST_MATCHED`, o Amazon Fraud Detector avaliará as regras sequencialmente, da primeiro à última, parando na primeira regra correspondente. Em seguida, o Amazon Fraud Detector fornecerá os resultados para essa única regra.

A ordem em que você executa as regras pode afetar o resultado resultante da previsão de fraudes. Depois de criar suas regras, reordene-as para executá-las na ordem desejada seguindo estas etapas:

Se sua`high_fraud_risk` regra ainda não estiver no topo da sua lista de regras, escolha Pedir e escolha 1. Isso passa`high_fraud_risk` para a primeira posição.

Repita esse processo para que sua`medium_fraud_risk` regra fique na segunda posição e sua`low_fraud_risk` regra esteja na terceira posição.

Tudo combinado

Todo o modo de execução de regras correspondentes retorna resultados para todas as regras correspondentes, independentemente da ordem das regras. Se você especificar`ALL_MATCHED`, o Amazon Fraud Detector avaliará todas as regras e retornará os resultados de todas as regras correspondentes.

Selecione`FIRST_MATCHED` este tutorial e, em seguida, escolha Avançar.

Etapa 5: revisar e criar a versão do detector

Uma versão do detector define os modelos e regras específicos usados para gerar previsões de fraudes.

1. Na página Revisar e criar, revise os detalhes, modelos e regras do detector que você configurou. Se você precisar fazer alguma alteração, escolha Editar ao lado da seção correspondente.
2. Escolha Criar detector. Depois de criado, a primeira versão do seu detector aparece na tabela de versões do detector com`Draft` status.

   Você usa a versão Rascunho para testar seu detector.

Etapa 6: testar e ativar a versão do detector

No console do Amazon Fraud Detector, você pode testar a lógica do seu detector usando dados simulados com o recurso Executar teste. Para este tutorial, você pode usar os dados de registro da conta do conjunto de dados de exemplo.

1. Role até Executar teste na parte inferior da página de detalhes da versão do detector.
2. Para metadados do evento, insira um carimbo de data e hora de quando o evento ocorreu e insira um identificador exclusivo para a entidade que está realizando o evento. Para este tutorial, selecione uma data no seletor de data para carimbo de data e hora e digite “1234” para a ID da entidade.
3. Em Variável de evento, insira os valores das variáveis que você deseja testar. Para este tutorial, você só precisa do`email_address` campo`ip_address` e. Isso ocorre porque eles são os insumos usados para treinar seu modelo Amazon Fraud Detector. Você pode usar os valores de exemplo a seguir. Isso pressupõe que você tenha usado os nomes de variáveis sugeridos:
   - endereço IP:`205.251.233.178`
   - endereço_e-mail:`johndoe@exampledomain.com`
4. Escolha Executar teste.
5. O Amazon Fraud Detector retorna o resultado da previsão de fraudes com base no modo de execução da regra. Se o modo de execução da regra for`FIRST_MATCHED`, o resultado retornado corresponderá à primeira regra correspondente. A primeira regra é a regra com a maior prioridade. É compatível se for avaliado como verdadeiro. Se o modo de execução da regra for`ALL_MATCHED`, o resultado retornado corresponderá a todas as regras correspondentes. Isso significa que todos eles são avaliados como verdadeiros. O Amazon Fraud Detector também retorna a pontuação do modelo para qualquer modelo adicionado ao seu detector.

   Você pode alterar as entradas e executar alguns testes para ver resultados diferentes. Você pode usar os valores ip_address e email_address do seu conjunto de dados de exemplo para os testes e verificar se os resultados são os esperados.
6. Quando estiver satisfeito com o funcionamento do detector, promova-o de`Draft` para`Active`. Isso torna o detector disponível para uso na detecção de fraudes em tempo real.

   Na página de detalhes da versão do Detector, escolha Ações, Publicar, Publicar versão. Isso altera o status do detector de Rascunho para Ativo.

Nesse momento, seu modelo e a lógica do detector associada estão prontos para avaliar atividades on-line em busca de fraudes em tempo real usando a`GetEventPrediction` API Amazon Fraud Detector. Você também pode avaliar eventos off-line usando um arquivo de entrada CSV e a`CreateBatchPredictionJob` API. Para obter mais informações sobre a previsão de fraudes, consultePrevisões de fraude

Ao concluir este tutorial, você fez o seguinte:

- Faça upload de um conjunto de dados de evento de exemplo no Amazon S3.
- Criou e treinou um modelo de detecção de fraudes do Amazon Fraud Detector usando o conjunto de dados de exemplo.
- Visualizou a pontuação de desempenho do modelo e outras métricas de desempenho geradas pelo Amazon Fraud Detector.
- Implantou o modelo de detecção de fraudes.
- Criou um detector e adicionou o modelo implantado.
- Foram adicionadas regras, ordem de execução da regra e resultados ao detector.
- Testei o detector fornecendo diferentes entradas e verificando se as regras e a ordem de execução da regra funcionaram conforme o esperado.
- Ativou o detector publicando-o.

Tutorial: Conceitos básicos deAWS SDK for Python (Boto3)

Este tutorial descreve como criar e treinar um modelo do Amazon Fraud Detector e, em seguida, usar esse modelo para gerar previsões de fraude em tempo real usandoAWS SDK for Python (Boto3) o. O modelo é treinado usando o arquivo de dados de exemplo de registro de conta que você carrega para o bucket do Amazon S3.

Ao final deste tutorial, você concluirá as seguintes ações:

- Crie e treine um modelo de Fraud Detector da Amazon
- Gere previsões de fraude em tempo real

Pré-requisitos

A seguir estão as etapas de pré-requisito para este tutorial.

- ConcluídoConfigurar o Amazon Fraud Detector.

  Se você já o fezConfigurar o AWS SDK, certifique-se de que está usando o SDK do Boto3 versão 1.14.29 ou superior.
- Seguiu as instruções paraObtenha e faça upload de um conjunto de dados de exemplo arquivar o que é necessário para este tutorial.

Conceitos básicos

Etapa 1: Configurar e verificar o ambiente Python

O Boto é o SDK da Amazon Web Services (AWS) para Python. Você pode usá-lo para criar, configurar e gerenciarServiços da AWS. Para obter instruções sobre como instalar o Boto3, consulte AWS SDK for Python (Boto3).

Depois de instalarAWS SDK for Python (Boto3), execute o seguinte comando de exemplo do Python para confirmar se seu ambiente está configurado corretamente. Se seu ambiente estiver configurado corretamente, a resposta conterá uma lista de detectores. Se nenhum detector tiver sido criado, a lista estará vazia.

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

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

Etapa 2: criar variáveis, tipo de entidade e rótulos

Nesta etapa, você cria recursos que são usados para definir modelos, eventos e regras.

Criar variável

Uma variável é um elemento de dados do seu conjunto de dados que você deseja usar para criar tipo de evento, modelo e regras.

No exemplo a seguir, a CreateVariableAPI é usada para criar duas variáveis. As variáveis sãoemail_addressip_address e. Atribua-os aos tipos de variáveis

correspondentes:`EMAIL_ADDRESS`IP_ADDRESS e. Essas variáveis fazem parte do conjunto de dados de exemplo que você enviou. Quando você especifica o tipo de variável, o Amazon Fraud Detector interpreta a variável durante o treinamento do modelo e ao obter previsões. Somente variáveis com um tipo de variável associado podem ser usadas para o treinamento do modelo.

```
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>'
)
```

Criar tipo de entidade

Uma entidade representa quem está realizando o evento e um tipo de entidade classifica a entidade. Exemplos de classificações incluem cliente, comerciante ou conta.

No exemplo a seguir, a PutEntityTypeAPI é usada para criar um tipo de`sample_customer` entidade.

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

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

Criar rótulo

Um rótulo classifica um evento como fraudulento ou legítimo e é usado para treinar o modelo de detecção de fraude. O modelo aprende a classificar eventos usando esses valores de rótulo.

No exemplo a seguir, a API Putlabel é usada para criar dois rótulos,`fraud`legit e.

```
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'
)
```

Etapa 3: Criar tipo de evento

Com o Amazon Fraud Detector, você cria modelos que avaliam riscos e geram previsões de fraude para eventos individuais. Um tipo de evento define a estrutura de um evento individual.

No exemplo a seguir, a PutEventTypeAPI é usada para criar um tipo de eventosample_registration. Você define o tipo de evento especificando as variáveis (email_address,ip_address), tipo de entidade (sample_customer) e rótulos (fraud,legit) que você criou na etapa anterior.

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

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

Etapa 4: criar, treinar e implantar o modelo

O Amazon Fraud Detector treina modelos para aprender a detectar fraudes para um tipo de evento específico. Na etapa anterior, você criou o tipo de evento. Nesta etapa, você cria e treina um modelo para o tipo de evento. O modelo funciona como um contêiner para suas versões de modelo. Cada vez que você treina um modelo, uma nova versão é criada.

Use os códigos de exemplo a seguir para criar e treinar um modelo Online Fraud Insights. Esse modelo é chamado`sample_fraud_detection_model`. É para o tipo de evento`sample_registration` usando o conjunto de dados de exemplo de registro de conta que você enviou para o Amazon S3.

Para obter mais informações sobre os diferentes tipos de modelos compatíveis com o Amazon Fraud Detector, consulteEscolha um tipo de modelo.

Crie um modelo

No exemplo a seguir, a CreateModelAPI é usada para criar um modelo.

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

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

Treine um modelo

No exemplo a seguir, a CreateModelVersionAPI é usada para treinar o modelo. Especifique`'EXTERNAL_EVENTS'` para o`trainingDataSource` e o local do Amazon S3 em que você armazenou seu conjunto de dados RoleArnde exemplo e para o bucket do Amazon S3`externalEventsDetail`. Como`trainingDataSchema` parâmetro, especifique como o Amazon Fraud Detector interpreta os dados de exemplo. Mais especificamente, especifique quais variáveis incluir e como classificar os rótulos dos eventos.

```
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'
}
)
```

Você pode treinar seu modelo várias vezes. Cada vez que você treina um modelo, uma nova versão é criada. Depois que o treinamento do modelo for concluído, o status da versão do modelo será atualizado para`TRAINING_COMPLETE`. Você pode revisar a pontuação de desempenho do modelo e outras métricas de desempenho do modelo.

Analise o desempenho do modelo

Uma etapa importante no uso do Amazon Fraud Detector é avaliar a precisão do seu modelo usando pontuações e métricas de desempenho do modelo. Depois que o treinamento do modelo for concluído, o Amazon Fraud Detector valida o desempenho do modelo usando 15% dos seus dados que não foram usados para treinar o modelo. Ele gera uma pontuação de performance do modelo e outras métricas de performance.

Use a DescribeModelVersionsAPI para analisar o desempenho do modelo. Veja a pontuação geral de desempenho do modelo e todas as outras métricas geradas pelo Amazon Fraud Detector para esse modelo.

Para saber mais sobre a pontuação de desempenho do modelo e as métricas de desempenho, consultePontuações do modeloMétricas de desempenho do modelo e.

Você pode esperar que todos os seus modelos treinados do Amazon Fraud Detector tenham métricas de desempenho de detecção de fraudes no mundo real, que são semelhantes às métricas deste tutorial.

Implante um modelo

Depois de analisar as métricas de desempenho do seu modelo treinado, implante o modelo e disponibilize-o para o Amazon Fraud Detector para gerar previsões de fraude. Para implantar o modelo treinado, use a UpdateModelVersionStatusAPI. No exemplo a seguir, ele é usado para atualizar o status da versão do modelo para ATIVO.

```
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'
)
```

Etapa 5: criar detector, resultados, regras e versão do detector

Um detector contém a lógica de detecção, como os modelos e as regras. Essa lógica é para um evento específico que você deseja avaliar como fraude. Uma regra é uma condição que você especifica para informar ao Amazon Fraud Detector como interpretará valores de variáveis durante a previsão. E o resultado é o resultado de uma previsão de fraude. Um detector pode ter várias versões, com cada versão tendo um status de RASCUNHO, ATIVO ou INATIVO. Uma versão do detector precisa estar associada a pelo menos uma regra.

Use os códigos de exemplo a seguir para criar detector, regras, resultados e publicar o detector.

Criar um detector

No exemplo a seguir, a PutDetectorAPI é usada para criar um`sample_detector` detector para o tipo de`sample_registration` evento.

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

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

Crie resultados

Os resultados são criados para cada possível resultado de previsão de fraude. No exemplo a seguir, a PutOutcomeAPI é usada para criar três resultados -`verify_customerreview`,`approve` e. Esses resultados são posteriormente atribuídos às regras.

```
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'
)
```

Crie regras

A regra consiste em uma ou mais variáveis do seu conjunto de dados, uma expressão lógica e um ou mais resultados.

No exemplo a seguir, a CreateRuleAPI é usada para criar três regras diferentes:`high_risk`,`medium_risk`,`low_risk` e. Crie expressões de regras para comparar o`sample_fraud_detection_model_insightscore` valor da pontuação de desempenho do modelo com vários limites. Isso é para determinar o nível de risco de um evento e atribuir um resultado que foi definido na etapa anterior.

```
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']
     )
```

Criar uma versão do detector

Uma versão do detector define o modelo e as regras que são usados para obter a previsão de fraudes.

No exemplo a seguir, a CreateDetectorVersionAPI é usada para criar uma versão do detector. Ele faz isso fornecendo detalhes da versão do modelo, regras e um modo de execução de regras FIRST_MATCHED. Um modo de execução de regras especifica a sequência para avaliar as regras. O modo de execução da regra FIRST_MATCHED especifica que as regras sejam avaliadas sequencialmente, da primeiro à última, parando na primeira regra correspondente.

```
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'
)
```

Etapa 6: gerar previsões de fraude

A última etapa deste tutorial usa o detector`sample_detector` criado na etapa anterior para gerar previsões de fraude para o tipo de`sample_registration` evento em tempo real. O detector avalia os dados de exemplo que são enviados para o Amazon S3. A resposta inclui as pontuações de desempenho do modelo, bem como quaisquer resultados associados às regras correspondentes.

No exemplo a seguir, a GetEventPredictionAPI é usada para fornecer dados de um único registro de conta com cada solicitação. Para este tutorial, pegue dados (email_address e ip_address) do arquivo de dados de exemplo de registro da conta. Cada linha (linha) após a linha do cabeçalho superior representa dados de um único evento de registro de conta.

```
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'
}
)
```

Depois de concluir este tutorial, você fez o seguinte:

- Fez upload de um exemplo de conjunto de dados de eventos para o Amazon S3.
- Variáveis, entidades e rótulos criados que são usados para criar e treinar um modelo.
- Criou e treinou um modelo usando o conjunto de dados de exemplo.
- Visualizou a pontuação de desempenho do modelo e outras métricas de desempenho geradas pelo Amazon Fraud Detector.
- Implantou o modelo de detecção de fraudes.
- Criou um detector e adicionou o modelo implantado.
- Foram adicionadas regras, a ordem de execução da regra e os resultados ao detector.
- Versão do detector criada.
- Testei o detector fornecendo diferentes entradas e verificando se as regras e a ordem de execução da regra funcionaram conforme o esperado.

(Opcional) Explore as APIs do Amazon Fraud Detector com um notebook Jupyter (IPython)

Para obter mais exemplos de como usar as APIs do Amazon Fraud Detector, consulte aws-fraud-detector-samples GitHub repositório. Os tópicos abordados pelos notebooks incluem a criação de modelos e detectores usando as APIs do Amazon Fraud Detector e a realização de solicitações de previsão de fraudes em lote usando a`GetEventPrediction` API.

Próximas etapas

Agora que você criou um modelo e um detector, você pode se aprofundar e começar a criar modelos e detectores e gerar previsões de fraudes.

As seções a seguir do Guia do usuário do Amazon Fraud Detector descrevem como sua empresa ou organização pode usar o Amazon Fraud Detector para detectar fraudes.

- Prepare e crie o conjunto de dados do evento para treinar seu modelo.
- Criar tipo de evento
- Criar modelo
- Crie um detector
- Obtenha previsões de fraudes
- Gerencie seus recursos do Amazon Fraud Detector (especificamente, variáveis, entidades, resultados e rótulos)
- configurar o Amazon Fraud Detector para atender aos objetivos de segurança e conformidade
- Monitore o Amazon Fraud Detector e registre chamadas de API do Amazon Fraud Detector
- Solucione problemas com o Amazon Fraud Detector

Conjunto de dados de eventos do

Um conjunto de dados de eventos são os dados históricos de fraudes da sua empresa. Você fornece esses dados ao Amazon Fraud Detector para criar modelos de detecção de fraudes.

O Amazon Fraud Detector usa modelos de aprendizado de máquina para gerar previsões de fraudes. Cada modelo é treinado usando um tipo de modelo. O tipo de modelo especifica os algoritmos e as transformações que são usados para treinar o modelo. O treinamento de modelos é o processo de usar um conjunto de dados que você fornece para criar um modelo capaz de prever eventos fraudulentos. Para obter mais informações, consulte Como funciona o Amazon Fraud Detector

O conjunto de dados usado para criar o modelo de detecção de fraudes fornece detalhes de um evento. Um evento é uma atividade comercial que é avaliada quanto ao risco de fraude. Por exemplo, o registro de uma conta pode ser um evento. Os dados associados ao evento de registro da conta podem ser um conjunto de dados do evento. O Amazon Fraud Detector usa esse conjunto de dados para avaliar fraudes no registro de contas.

Antes de fornecer seu conjunto de dados ao Amazon Fraud Detector para criar um modelo, certifique-se de definir sua meta para criar o modelo. Você também precisa determinar como deseja usar o modelo e definir suas métricas para avaliar se o modelo está funcionando com base em seus requisitos específicos.

Por exemplo, suas metas para criar um modelo de detecção de fraudes que avalia a fraude no registro de contas podem ser as seguintes:

- Para aprovar automaticamente registros legítimos.
- Para capturar registros fraudulentos para investigação posterior.

Depois de determinar sua meta, a próxima etapa é decidir como você deseja usar o modelo. Alguns exemplos de uso do modelo de detecção de fraudes para avaliar fraudes de registro são os seguintes:

- Para detecção de fraudes em tempo real para cada registro de conta.
- Para avaliação off-line de todos os registros de contas a cada hora.

Alguns exemplos de métricas que podem ser usadas para medir o desempenho do modelo incluem o seguinte:

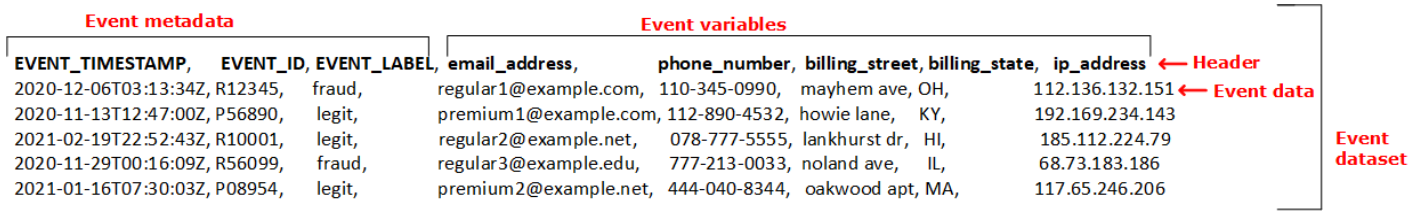
- Tem um desempenho consistentemente melhor do que a linha de base atual na produção.
- Captura X% de registros de fraudes com Y% de taxa de falsos positivos.
- Aceita até 5% dos registros aprovados automaticamente que são fraudulentos.

Estrutura do conjunto de dados de eventos

O Amazon Fraud Detector exige que você forneça seu conjunto de dados de eventos em um arquivo de texto usando valor separado por vírgula (CSV) no formato UTF-8. A primeira linha do seu arquivo de conjunto de dados CSV deve conter cabeçalhos de arquivo. O cabeçalho do arquivo consiste em metadados e variáveis de evento que descrevem cada elemento de dados associado ao evento. O cabeçalho é seguido pelos dados do evento. Cada linha consiste em elementos de dados de um único evento.

- Metadados do evento - fornece informações sobre o evento. Por exemplo, EVENT_TIMESTAMP é um metadado de evento que especifica a hora em que o evento ocorreu. Dependendo do caso de uso da sua empresa e do tipo de modelo usado para criar e treinar seu modelo de detecção de fraudes, o Amazon Fraud Detector exige que você forneça metadados de eventos específicos. Ao especificar metadados de eventos no cabeçalho do arquivo CSV, use o mesmo nome de metadados de evento especificado pelo Amazon Fraud Detector e use somente letras maiúsculas.
- Variável de evento - representa os elementos de dados específicos do seu evento que você deseja usar para criar e treinar seu modelo de detecção de fraudes. Dependendo do caso de uso da sua empresa e do tipo de modelo usado para criar e treinar um modelo de detecção de fraudes, o Amazon Fraud Detector pode exigir ou recomendar que você forneça variáveis de evento específicas. Você também pode, opcionalmente, fornecer outras variáveis de evento do seu evento que você deseja incluir no treinamento do modelo. Alguns exemplos de variáveis de evento para um evento de registro on-line podem ser endereço de e-mail, endereço IP e número de telefone. Ao especificar o nome da variável do evento no cabeçalho do arquivo CSV, use qualquer nome de variável de sua escolha e use somente letras minúsculas.
- Dados do evento - representam os dados coletados do evento real. Em seu arquivo CSV, cada linha após o cabeçalho do arquivo consiste em elementos de dados de um único evento. Por exemplo, em um arquivo de dados de evento de registro on-line, cada linha contém dados de um único registro. Cada elemento de dados na linha deve corresponder aos metadados do evento correspondentes ou à variável do evento.

Veja a seguir um exemplo de um arquivo CSV contendo dados de um evento de registro de conta. A linha do cabeçalho contém metadados do evento em maiúsculas e variáveis de evento em minúsculas, seguidos pelos dados do evento. Cada linha no conjunto de dados contém elementos de dados associados ao registro de uma única conta, com cada elemento de dados correspondente ao cabeçalho.



Obtenha os requisitos do conjunto de dados de eventos usando o Data Models Explorer

O tipo de modelo que você escolhe para criar seu modelo define os requisitos para seu conjunto de dados. O Amazon Fraud Detector usa o conjunto de dados que você fornece para criar e treinar seu modelo de detecção de fraudes. Antes de começar a criar seu modelo, o Amazon Fraud Detector verifica se o conjunto de dados atende ao tamanho, formato e outros requisitos. Se o conjunto de dados não atender aos requisitos, a criação e o treinamento do modelo falharão. Você pode usar o explorador de modelos de dados para identificar um tipo de modelo a ser usado em seu caso de uso comercial e obter informações sobre os requisitos do conjunto de dados para o tipo de modelo identificado.

Explorador de modelos de dados

O explorador de modelos de dados é uma ferramenta no console do Amazon Fraud Detector que alinha seu caso de uso comercial com o tipo de modelo suportado pelo Amazon Fraud Detector. O explorador de modelos de dados também fornece informações sobre os elementos de dados exigidos pelo Amazon Fraud Detector para criar seu modelo de detecção de fraudes. Antes de começar a preparar seu conjunto de dados de eventos, use o explorador de modelos de dados para descobrir o tipo de modelo que o Amazon Fraud Detector recomenda para uso comercial e também para ver uma lista de elementos de dados obrigatórios, recomendados e opcionais que você precisará para criar seu conjunto de dados.

Para usar o explorador de modelos de dados,

1. Abra o AWSManagement Console e faça login em sua conta. Navegue até o Amazon Fraud Detector.

2. No painel de navegação à esquerda, escolha Explorador de modelos de dados.
3. Na página Explorador de modelos de dados, em Caso de uso comercial, selecione o caso de uso comercial que você deseja avaliar quanto ao risco de fraude.
4. O Amazon Fraud Detector exibe o tipo de modelo recomendado que corresponde ao seu caso de uso comercial. O tipo de modelo define os algoritmos, enriquecimentos e transformações que o Amazon Fraud Detector usará para treinar seu modelo de detecção de fraudes.

   Anote o tipo de modelo recomendado. Você precisará disso mais tarde ao criar seu modelo.

   > **Note**
   >
   > Se você não encontrar seu caso de uso comercial, use o link entre em contato conosco na descrição para nos fornecer os detalhes do seu caso de uso comercial. Recomendaremos o tipo de modelo a ser usado para criar um modelo de detecção de fraudes para seu caso de uso comercial.

5. O painel Informações do modelo de dados fornece informações sobre os elementos de dados obrigatórios, recomendados e opcionais necessários para criar e treinar um modelo de detecção de fraudes para seu caso de uso comercial. Use as informações no painel de insights para coletar os dados do seu evento e criar seu conjunto de dados.

Reúna dados de eventos do

Coletar os dados do seu evento é uma etapa importante na criação do seu modelo. Isso ocorre porque o desempenho do seu modelo na previsão de fraudes depende da qualidade do seu conjunto de dados. Ao começar a coletar os dados do evento, lembre-se da lista de elementos de dados que o Data Models Explorer forneceu para você criar seu conjunto de dados. Você precisará reunir todos os dados obrigatórios (metadados do evento) e decidir quais elementos de dados recomendados e opcionais (variáveis de evento) incluir com base em suas metas de criação do modelo. Também é importante decidir o formato de cada variável de evento que você pretende incluir e o tamanho total do seu conjunto de dados.

Qualidade do conjunto de dados de eventos

Para reunir um conjunto de dados de alta qualidade para seu modelo, recomendamos o seguinte:

- Colete dados maduros - Usar os dados mais recentes ajuda a identificar o padrão de fraude mais recente. No entanto, para detectar casos de uso de fraudes, permita que os dados amadureçam.

O período de maturidade depende da sua empresa e pode levar de duas semanas a três meses. Por exemplo, se seu evento incluir uma transação com cartão de crédito, o vencimento dos dados poderá ser determinado pelo período de estorno do cartão de crédito ou pelo tempo gasto pelo investigador para fazer a determinação.

Certifique-se de que o conjunto de dados usado para treinar o modelo tenha tido tempo suficiente para amadurecer de acordo com sua empresa.

- Certifique-se de que a distribuição de dados não varie significativamente: o processo de treinamento do Amazon Fraud Detector modela amostras e particiona seu conjunto de dados com base em EVENT_TIMESTAMP. Por exemplo, se seu conjunto de dados consistir em eventos de fraude retirados dos últimos 6 meses, mas somente o último mês de eventos legítimos for incluído, a distribuição de dados será considerada flutuante e instável. Um conjunto de dados instável pode levar a vieses na avaliação do desempenho do modelo. Se você achar que a distribuição de dados está mudando significativamente, considere equilibrar seu conjunto de dados coletando dados semelhantes à distribuição de dados atual.
- Certifique-se de que o conjunto de dados seja representativo do caso de uso em que o modelo foi implementado/testado. Caso contrário, o desempenho estimado pode ser tendencioso. Digamos que você esteja usando um modelo para recusar automaticamente todos os candidatos internos, mas seu modelo é treinado com um conjunto de dados com dados/rótulos históricos que foram previamente aprovados. Então, a avaliação do seu modelo pode ser imprecisa porque a avaliação é baseada no conjunto de dados que não tem representação de candidatos recusados.

Formato de dados do evento

O Amazon Fraud Detector transforma a maioria dos seus dados no formato necessário como parte de seu processo de treinamento de modelos. No entanto, existem alguns formatos padrão que você pode usar facilmente para fornecer seus dados que podem ajudar a evitar problemas posteriores, quando o Amazon Fraud Detector validar seu conjunto de dados. A tabela a seguir fornece orientação sobre os formatos para fornecer os metadados de eventos recomendados.

> **Note**
>
> Ao criar seu arquivo CSV, certifique-se de inserir o nome dos metadados do evento conforme listado abaixo, em letras maiúsculas.

Nome dos metadados	Formato	Obrigatório
ID DO EVENTO	Se fornecido, ele deve atender aos seguintes requisitos: • É exclusivo para esse evento. • Ela representa informações que são significativas para sua empresa. • Ele segue o padrão de expressão regular (por exemplo,`^[0-9a-z_-]+$.`) • Além dos requisitos acima, recomendamos que você não acrescente um carimbo de data/hora ao EVENT_ID. Fazer isso pode causar problemas ao atualizar o evento. Isso porque você deve fornecer exatamente o mesmo EVENT_ID se fizer isso.	Depende do tipo de modelo
EVENT_TIMESTAMP	• Ele deve ser especific ado em um dos seguintes formatos: • %YYYYY-%MM-%DDT %HH: %mm: %sSz (padrão ISO 8601 em UTC somente sem milissegundos) Exemplo: 2019-11-30T 13:01:01 Z	Sim

Nome dos metadados	Formato	Obrigatório
	• %aaaa/%mm/%dd %h: %mm: %s (AM/PM) Exemplos: 2019/11/30 13:01:01 ou 2019/11/30 13:01:01 • %mm/%dd/%aaaa %h: %mm: %s Exemplos: 30/11/2019 13:01:01, 30/11/2019 13:01:01 • %mm/%dd/%y %h: %mm: %s Exemplos: 30/11/19 13:01:01 PM, 11/30/19 13:01:01 • O Amazon Fraud Detector faz as seguintes suposições ao analisar formatos de data/hora para carimbos de data e hora de eventos: • Se você estiver usando o padrão ISO 8601, ele deve corresponder exatamente à especificação anterior • Se você estiver usando um dos outros formatos, há flexibilidade adicional: • Por meses e dias, você pode fornecer um ou dois dígitos. Por	

Nome dos metadados	Formato	Obrigatório
	exemplo, 1/12/2019 é uma data válida. • Você não precisa incluir hh:mm:ss se não os tiver (ou seja, você pode simplesmente fornecer uma data). Você também pode fornecer um subconjunto de apenas horas e minutos (por exemplo, hh:mm). O simples fornecimento de horas não é suportado. Milissegundos também não são suportados. • Se você fornecer etiquetas AM/PM, presume-se que um relógio de 12 horas. Se não houver informações de AM/PM, presume-se que um relógio de 24 horas. • Você pode usar “/” ou “-” como delimitadores para os elementos de data. “:” é assumido para os elementos de timestamp.	

Nome dos metadados	Formato	Obrigatório
ENTIDADE_ID	• Ele deve seguir o padrão de expressão regular:`^[0-9A-Za-z_.@+-]+$` . • Se o ID da entidade não estiver disponível no momento da avaliação, especifique o ID da entidade como desconhecido.	Depende do tipo de modelo
TIPO_ENTIDADE	Você pode usar qualquer string	Depende do tipo de modelo
RÓTULO DO EVENTO	Você pode usar qualquer rótulo, como “fraude”, “legítimo”, “1" ou “0".	Obrigatório se LABEL_TIMESTAMP estiver incluído
LABEL_TIMESTAMP	Ele deve seguir o formato do carimbo de data/hora.	Obrigatório se EVENT_LABEL estiver incluído

Para obter informações sobre variáveis de evento, consulte Variáveis.

> **Important**
>
> Se você estiver criando o modelo Account Takeover Insights (ATI), consultePreparar dados para obter detalhes sobre como preparar e selecionar dados.

Valores nulos ou faltantes

As variáveis EVENT_TIMESTAMP e EVENT_LABEL não devem conter valores nulos ou ausentes. Você pode ter valores nulos ou ausentes para outras variáveis. No entanto, recomendamos usar apenas um pequeno número nulo para essas variáveis. Se o Amazon Fraud Detector determinar que há muitos valores nulos ou ausentes para uma variável de evento, ele omitirá automaticamente a variável do seu modelo.

Variáveis mínimas

Ao criar seu modelo, o conjunto de dados deve incluir pelo menos duas variáveis de evento além dos metadados de evento necessários. As duas variáveis de evento devem passar pela verificação de validação.

Tamanho do conjunto de dados do evento

Obrigatório

Seu conjunto de dados deve atender aos seguintes requisitos básicos para um treinamento bem-sucedido de modelos.

- Dados de pelo menos 100 eventos.
- O conjunto de dados deve incluir pelo menos 50 eventos (linhas) classificados como fraudulentos.

Recomendado

Recomendamos que seu conjunto de dados inclua o seguinte para um treinamento bem-sucedido do modelo e um bom desempenho do modelo.

- Inclua no mínimo três semanas de dados históricos, mas, no máximo, seis meses de dados.
- Inclua um mínimo de 10 mil dados de eventos no total.
- Inclua pelo menos 400 eventos (linhas) classificados como fraudulentos e 400 eventos (linhas) classificados como legítimos.
- Inclua mais de 100 entidades exclusivas, se seu tipo de modelo exigir ENTITY_ID.

Validação do conjunto de dados

Antes de começar a criar seu modelo, o Amazon Fraud Detector verifica se as variáveis incluídas no conjunto de dados para treinamento do modelo atendem ao tamanho, formato e outros requisitos. Se o conjunto de dados não passar na validação, o modelo não será criado. Você deve primeiro corrigir as variáveis que não passaram na validação antes de criar o modelo. O Amazon Fraud Detector fornece um criador de perfil de dados que você pode usar para ajudá-lo a identificar e corrigir problemas com seu conjunto de dados antes de começar a treinar seu modelo.

Perfilador de dados

O Amazon Fraud Detector fornece uma ferramenta de código aberto para criar perfis e preparar seus dados para o treinamento de modelos. Esse criador de perfil de dados automatizado ajuda

você a evitar erros comuns de preparação de dados e a identificar possíveis problemas, como tipos de variáveis mapeados incorretamente, que afetariam negativamente o desempenho do modelo. O criador de perfil gera um relatório intuitivo e abrangente do seu conjunto de dados, incluindo estatísticas de variáveis, distribuição de rótulos, análise categórica e numérica e correlações de variáveis e rótulos. Ele fornece orientação sobre tipos de variáveis, bem como uma opção para transformar o conjunto de dados em um formato exigido pelo Amazon Fraud Detector.

Usando o criador de perfil de dados

O criador de perfil de dados automatizado é construído com umaAWS CloudFormation pilha, que você pode iniciar facilmente com apenas alguns cliques. Todos os códigos estão disponíveis no Github. Para obter informações sobre como usar o Data Profiler, siga as instruções em nosso blog Treine modelos mais rapidamente com um criador de perfil de dados automatizado para o Amazon Fraud Detector

Erros comuns do conjunto de dados de eventos

A seguir estão alguns dos problemas comuns que o Amazon Fraud Detector encontra ao validar um conjunto de dados de eventos. Depois de executar o criador de perfil de dados, use essa lista para verificar se há erros no conjunto de dados antes de criar seu modelo.

- O arquivo CSV não está no formato UTF-8.
- O número de eventos no conjunto de dados é menor que 100.
- O número de eventos identificados como fraudulentos ou legítimos é inferior a 50.
- O número de entidades exclusivas associadas a um evento de fraude é inferior a 100.
- Mais de 0,1% dos valores em EVENT_TIMESTAMP contêm nulos ou valores diferentes dos formatos de data/timestamp suportados.
- Mais de 1% dos valores em EVENT_LABEL contêm nulos ou valores diferentes dos definidos no tipo de evento.
- Menos de duas variáveis estão disponíveis para o treinamento do modelo.

Armazenamento de conjunto de dados

Depois de reunir o conjunto de dados, você o armazém internamente usando o Amazon Fraud Detector ou externamente com o Amazon Simple Storage Service (Amazon S3). Recomendamos que você escolha onde armazenar seu conjunto de dados com base no modelo usado para gerar previsões de fraude. Para obter mais informações sobre os tipos de modelo, consulte Escolher

um tipo de modelo. Para obter mais informações sobre como armazenar seu conjunto de dados, consulteArmazenamento de dados de eventos.

Tipo de evento

Com o Amazon Fraud Detector, você gera previsões de fraude para eventos. Um tipo de evento define a estrutura de um evento individual enviado ao Amazon Fraud Detector. Uma vez definido, você pode criar modelos e detectores que avaliam o risco de tipos específicos de eventos.

A estrutura de um evento inclui o seguinte:

- Tipo de entidade: classifica quem está realizando o evento. Durante a previsão, especifique o tipo de entidade e o ID da entidade para definir quem realizou o evento.
- Variáveis: define quais variáveis podem ser enviadas como parte do evento. As variáveis são usadas por modelos e regras para avaliar o risco de fraude. Depois de adicionadas, as variáveis não podem ser removidas de um tipo de evento.
- Etiquetas: classifica um evento como fraudulento ou legítimo. Usado durante o treinamento do modelo. Depois de adicionados, os rótulos não podem ser removidos de um tipo de evento.

Crie um tipo de evento

Antes de criar seu modelo de detecção de fraudes, você deve primeiro criar um tipo de evento. A criação de um tipo de evento envolve definir sua atividade comercial (evento) a ser avaliada em caso de fraude. Definir o evento envolve identificar as variáveis do evento em seu conjunto de dados para incluir na avaliação de fraudes, especificar a entidade que está iniciando o evento e os rótulos que classificam o evento.

Pré-requisitos para criar um tipo de evento

Antes de começar a criar seu tipo de evento, certifique-se de ter concluído o seguinte:

- Usou a Explorador de modelos de dados ferramenta para obter informações sobre os elementos de dados exigidos pelo Amazon Fraud Detector para criar seu modelo de detecção de fraudes.
- Usou os insights que você obteve do Data Models Explorer para criar seu conjunto de dados de eventos e carregou seu conjunto de dados para o bucket do Amazon S3.
- CriadoVariáveis,Entidade, e Rótulos você quer que o Amazon Fraud Detector use para criar um modelo de detecção de fraudes para este evento. Certifique-se de que as variáveis, o tipo de entidade e os rótulos que você criou estejam incluídos no conjunto de dados do evento.

Você pode criar seu tipo de evento no console do Amazon Fraud Detector, usando a API, usando ou usando o AWS SDK. AWS CLI

Crie o tipo de evento no console do Amazon Fraud Detector

Para criar um tipo de evento,

1. Abra o AWSManagement Console e faça login na sua conta. Navegue até o Amazon Fraud Detector.
2. No painel de navegação esquerdo, escolha Events.
3. Na página Tipo de eventos, escolha Criar.
4. Em Detalhes do tipo de evento,
   a. Em Nome, insira o nome do seu evento.
   b. Na Descrição, opcionalmente, insira uma descrição.
   c. Na Entidade, selecione o tipo de entidade que você criou para o seu evento.
5. Em Variáveis de evento,
   - Em Escolha como definir as variáveis desse evento,
     - Se você já criou suas variáveis de evento para esse evento, selecione Selecionar variáveis da sua lista de variáveis e, em Variáveis, selecione as variáveis que você criou para esse evento.
     - Se você não criou variáveis para esse evento, selecione Selecionar variáveis de um conjunto de dados de treinamento,
       - Na função do IAM, selecione a função do IAM que você deseja que o Amazon Fraud Detector use para acessar o bucket do Amazon S3 que contém seu conjunto de dados
       - Em Localização dos dados, insira o caminho para a localização do seu conjunto de dados. Use o `S3 URI` caminho semelhante a este:`S3://your-bucket-name/example dataset filename.csv`.
       - Escolha Upload (Carregar).
       - Em Variáveis, todos os nomes de variáveis de evento que o Amazon Fraud Detector extraiu do seu arquivo de conjunto de dados são exibidos.

Se você quiser que a variável seja incluída para detectar fraudes, no Tipo de variável, selecione o tipo de variável. Escolha Remover para remover as variáveis de serem incluídas para detecção de fraudes. Repita essa etapa para cada variável na lista.

6. Em Rótulos (opcional), em Rótulos, selecione os rótulos que você criou para esse evento. Certifique-se de selecionar um rótulo para cada evento fraudulento e legítimo.
7. Se você quiser configurar o processamento automático de downstream para esse evento, em Orquestração de eventos com a Amazon EventBridge - opcional, ative Ativar orquestração de eventos com a Amazon. EventBridge Para obter mais informações sobre orquestração de eventos, consulte. Orquestração de eventos

> **Note**
>
> Você também pode ativar a orquestração de eventos posteriormente, depois de criar seu tipo de evento.

8. Escolha Criar tipo de evento.

Crie um tipo de evento usando o AWS SDK for Python (Boto3)

O exemplo a seguir mostra um exemplo de solicitação para a `PutEventType` API. O exemplo pressupõe que você tenha criado as variáveis `ip_address` e`email_address`, os rótulos `legit` e `fraud` o tipo de `sample_customer` entidade. Para obter informações sobre como criar esses recursos, consulteRecursos.

> **Note**
>
> Você deve primeiro criar variáveis, tipos de entidades e rótulos antes de adicioná-los ao tipo de 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'])
```

Excluir um evento ou tipo de evento

Quando você exclui um evento, o Amazon Fraud Detector exclui permanentemente esse evento e os dados associados ao evento não são mais armazenados no Amazon Fraud Detector.

Para excluir um evento que o Amazon Fraud Detector avaliou por meio da API **`GetEventPrediction`**

1. Faça login AWS Management Console e abra o console do Amazon Fraud Detector em https://console.aws.amazon.com/frauddetector.
2. No painel de navegação esquerdo do console, escolha Pesquisar previsões anteriores.
3. Escolha o evento que você deseja excluir.
4. Escolha Ações e, em seguida, escolha Excluir evento.
5. Digite e**`delete`**, em seguida, escolha Excluir evento.

> **Note**
>
> Isso exclui todos os registros associados a essa ID de evento, incluindo todos os dados de evento enviados para a `SendEvent` operação e quaisquer dados de previsão gerados por meio da `GetEventPrediction` operação.

Para excluir um evento que está armazenado no Amazon Fraud Detector, mas não foi avaliado (ou seja, ele foi armazenado por meio da `SendEvent` operação), você deve fazer uma `DeleteEvent` solicitação e especificar a ID do evento e a ID do tipo de evento. Se você quiser excluir o evento e qualquer histórico de previsão associado ao evento, defina o valor do `deleteAuditHistory` parâmetro como “verdadeiro”. Com o `deleteAuditHistory` parâmetro definido como “verdadeiro”, os dados do evento ficam disponíveis por meio da pesquisa por até 30 segundos após a conclusão da operação de exclusão.

Para excluir todos os eventos associados a um tipo de evento

1. No painel de navegação esquerdo do console, escolha Tipos de eventos
2. Escolha o tipo de evento para o qual você deseja que todos os eventos sejam excluídos.

3. Navegue até a guia Eventos armazenados e escolha Excluir eventos armazenados

Dependendo do número de eventos armazenados para o tipo de evento, pode levar algum tempo para excluir todos os eventos armazenados. Por exemplo, um conjunto de dados de 1 GB (aproximadamente 1 a 2 milhões de eventos para o cliente médio) leva cerca de 2 horas para ser excluído. Durante esse período, novos eventos que você envia para o Amazon Fraud Detector desse tipo de evento não são armazenados, mas você pode continuar gerando previsões de fraude por meio da `GetEventPrediction` operação.

Para excluir um tipo de evento

Você não pode excluir um tipo de evento usado em um detector ou modelo ou que tenha eventos armazenados associados. Antes de excluir um tipo de evento, você deve excluir todos os eventos associados a esse tipo de evento.

Quando você exclui um tipo de evento, o Amazon Fraud Detector exclui permanentemente esse tipo de evento e os dados não são mais armazenados no Amazon Fraud Detector.

1. No painel de navegação esquerdo do console do Amazon Fraud Detector, escolha Recursos e, em seguida, escolha Eventos.
2. Escolha o tipo de evento que você deseja excluir.
3. Escolha Ações e, em seguida, escolha Excluir tipo de evento.
4. Insira o nome do tipo de evento e escolha Excluir tipo de evento.

Armazenamento de dados de eventos

Depois de reunir o conjunto de dados, você o armazena internamente usando o Amazon Simple Storage Service (Amazon Simple Storage Service (Amazon Simple Storage Service (Amazon Simple Storage Service (Amazon Simple Storage Service (Amazon S3) Simple Storage Service Recomendamos que você escolha onde armazenar seu conjunto de dados com base no modelo usado para gerar previsões de fraude. A seguir, é apresentada uma análise detalhada dessas duas opções de armazenamento.

- Armazenamento interno - Seu conjunto de dados é armazenado com o Amazon Fraud Detector. Todos os dados do evento associados a um evento são armazenados juntos. Você pode carregar o conjunto de dados do evento armazenado com o Amazon Fraud Detector a qualquer momento. Você pode transmitir eventos um por vez para uma API Amazon Fraud Detector ou importar grandes conjuntos de dados (até 1 GB) usando o recurso de importação em lote. Ao treinar um modelo usando o conjunto de dados armazenado com o Amazon Fraud Detector, você pode especificar um intervalo de tempo para limitar o tamanho do seu conjunto de dados.
- Armazenamento externo - Seu conjunto de dados é armazenado em uma fonte de dados externa diferente do Amazon Fraud Detector. Atualmente, o Amazon Fraud Detector oferece suporte ao uso do Amazon Fraud Detector (Amazon S3 Detector) para essa finalidade. Se seu modelo estiver em um arquivo enviado para o Amazon S3, esse arquivo não poderá ter mais do que 5 GB de dados não compactados. Se for mais do que isso, certifique-se de encurtar o intervalo de tempo do seu conjunto de dados.

A tabela a seguir fornece detalhes sobre o tipo de modelo e a fonte de dados que ele suporta.

Tipo do modelo	Fonte de dados de treinamento compatível
Insights sobre fraud Insights	Armazenamento externo, armazenamento interno
Insights sobre a fraude de transações	Armazenamento interno
Insights sobre a aquisição de contas	Armazenamento interno

Para obter informações sobre como armazenar seu conjunto de dados externamente com o Amazon Simple Storage Service, consulteArmazene os dados do seu evento externamente com o Amazon

S3 . Para obter informações sobre como armazenar seu conjunto de dados internamente com o Amazon Fraud Detector, consulteArmazene os dados do seu evento internamente com o Amazon Fraud Detector.

Armazene os dados do seu evento externamente com o Amazon S3

Se você estiver treinando um modelo do Online Fraud Insights, você pode optar por armazenar os dados do seu evento externamente com o Amazon S3. Para armazenar os dados do seu evento no Amazon S3, você deve primeiro criar um arquivo de texto no formato CSV, adicionar os dados do evento e, em seguida, fazer o upload do arquivo CSV em um bucket do Amazon S3.

> **Note**
>
> Os tipos de modelo Transaction Fraud Insights e Account Takeover Insights não oferecem suporte a conjuntos de dados armazenados externamente com o Amazon S3

Criar arquivo CSV

O Amazon Fraud Detector exige que a primeira linha do seu arquivo CSV contenha cabeçalhos de coluna. Os cabeçalhos das colunas em seu arquivo CSV devem ser mapeados para as variáveis definidas no tipo de evento. Para obter um exemplo de conjunto de dados, consulteObtenha e faça upload de um conjunto de dados de exemplo

O modelo Online Fraud Insights exige um conjunto de dados de treinamento que tenha pelo menos 2 variáveis e até 100 variáveis. Além das variáveis do evento, o conjunto de dados de treinamento deve conter os seguintes cabeçalhos:

- EVENT_TIMESTAMP - Define quando o evento ocorreu
- EVENT_LABEL - classifica o evento como fraudulento ou legítimo. Os valores na coluna devem corresponder aos valores definidos no tipo de evento.

O exemplo de dados CSV a seguir representa eventos históricos de registro de um comerciante on-line:

```
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**
>
> O arquivo de dados CSV pode conter aspas duplas e vírgulas como parte dos seus dados.

Uma versão simplificada do tipo de evento correspondente está representada abaixo. As variáveis de evento correspondem aos cabeçalhos no arquivo CSV e os valores`EVENT_LABEL` correspondem aos valores na lista de rótulos.

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

Formato de data/hora do evento

Certifique-se de que a data e hora do seu evento esteja no formato exigido. Como parte do processo de criação do modelo, o tipo de modelo Online Fraud Insights ordena seus dados com base na data e hora do evento e divide seus dados para fins de treinamento e teste. Para obter uma estimativa justa do desempenho, o modelo primeiro treina no conjunto de dados de treinamento e depois testa esse modelo no conjunto de dados de teste.

O Amazon Fraud Detector suporta os seguintes formatos de data/hora para os valores apresentados`EVENT_TIMESTAMP` durante o treinamento do modelo:

- %YYYYY-%MM-%DDT%HH: %mm: %sSz (padrão ISO 8601 em UTC somente sem milissegundos)

  Exemplo: 2019-11-30T 13:01:01 Z
- %aaaa/%mm/%dd %h: %mm: %s (AM/PM)

  Exemplos: 2019/11/30 13:01:01 ou 2019/11/30 13:01:01

- %mm/%dd/%aaaa %h: %mm: %s

  Exemplos: 30/11/2019 13:01:01, 30/11/2019 13:01:01
- %mm/%dd/%y %h: %mm: %s

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

O Amazon Fraud Detector faz as seguintes suposições ao analisar formatos de data/hora para carimbos de data e hora de eventos:

- Se você estiver usando o padrão ISO 8601, ele deve corresponder exatamente à especificação anterior
- Se você estiver usando um dos outros formatos, há flexibilidade adicional:
  - Por meses e dias, você pode fornecer um ou dois dígitos. Por exemplo, 1/12/2019 é uma data válida.
  - Você não precisa incluir hh:mm:ss se não os tiver (ou seja, você pode simplesmente fornecer uma data). Você também pode fornecer um subconjunto de apenas horas e minutos (por exemplo, hh:mm). O simples fornecimento de horas não é suportado. Milissegundos também não são suportados.
  - Se você fornecer etiquetas AM/PM, presume-se que um relógio de 12 horas. Se não houver informações de AM/PM, presume-se que um relógio de 24 horas.
  - Você pode usar “/” ou “-” como delimitadores para os elementos de data. “:” é assumido para os elementos de timestamp.

Amostragem de seu conjunto de dados ao longo do tempo

Recomendamos que você forneça exemplos de fraudes e amostras legítimas no mesmo intervalo de tempo. Por exemplo, se você fornecer eventos de fraude dos últimos 6 meses, você também deve fornecer eventos legítimos que abranjam uniformemente o mesmo período. Se seu conjunto de dados contiver uma distribuição altamente desigual de fraudes e eventos legítimos, você poderá receber o seguinte erro: “A distribuição da fraude ao longo do tempo é inaceitavelmente flutuante. Não é possível dividir o conjunto de dados corretamente.” Normalmente, a solução mais fácil para esse erro é garantir que os eventos de fraude e os eventos legítimos sejam amostrados uniformemente no mesmo período de tempo. Talvez você também precise remover dados caso tenha ocorrido um grande aumento de fraudes em um curto período de tempo.

Se você não conseguir gerar dados suficientes para criar um conjunto de dados distribuído uniformemente, uma abordagem é randomizar o EVENT_TIMESTAMP de seus eventos de forma que eles sejam distribuídos uniformemente. No entanto, isso geralmente resulta em métricas de desempenho irrealistas porque o Amazon Fraud Detector usa EVENT_TIMESTAMP para avaliar modelos no subconjunto apropriado de eventos em seu conjunto de dados.

Valores nulos e faltantes

O Amazon Fraud Detector lida com valores nulos e faltantes. No entanto, a porcentagem de nulos para variáveis deve ser limitada. As colunas EVENT_TIMESTAMP e EVENT_LABEL não devem conter valores ausentes.

Validação de arquivos

O Amazon Fraud Detector não treinará um modelo se uma das seguintes condições for acionada:

- Se o CSV não puder ser analisado
- Se o tipo de dados de uma coluna estiver incorreto

Carregar os dados do evento para um bucket do Amazon S3

Depois de criar um arquivo CSV com os dados do evento, faça upload do arquivo no bucket do Amazon S3.

Para carregar para um bucket do Amazon S3

1. Faça login no AWS Management Console e abra o console do Amazon S3 em https://console.aws.amazon.com/s3/.
2. Selecione Create bucket (Criar bucket).

   O assistente Create bucket (Criar bucket) é aberto.
3. Em Bucket name (Nome do bucket), insira um nome compatível com o DNS para seu bucket.

   O nome do bucket deve:

   - Seja exclusivo em todo o Amazon S3.
   - Ter entre 3 e 63 caracteres.
   - Não contém caracteres maiúsculos.

- Começar com uma letra minúscula ou um número.

Depois de criado o bucket, você não pode mudar seu nome. Para obter informações sobre a nomenclatura de buckets, consulte Regras de nomeação de bucket no Guia do usuário do Amazon Simple Storage Service.

> **Important**
>
> Evite incluir informações confidenciais, como números de conta, no nome do bucket. O nome do bucket é visível nos URLs que apontam para os objetos no bucket.

4. Em Region (Região), escolha a região da AWS onde deseja que o bucket resida. Você deve selecionar a mesma região em que está usando o Amazon Fraud Detector (N.) (Norte da) (Norte da) (Oregon) (Ohio) (Ohio) (Ohio) (Ohio) (Oregon) (Oregon) (Oregon) (Oregon) (Oregon) (Oregon) (Oregon) (Oregon) (Oregon) (Oregon) (Oregon) (Oregon) (Oregon) (Oregon) (Oregon) (
5. Em Bucket settings for Block Public Access (Configurações de bucket para o Bloqueio de acesso público), escolha as configurações de bloqueio de acesso público que deseja aplicar ao bucket.

   Recomendamos deixar todas as configurações habilitadas. Para obter mais informações sobre como bloquear o acesso público, consulte Bloquear o acesso Amazon S3 ao armazenamento do Amazon Simple Storage Service.
6. Selecione Create bucket (Criar bucket).
7. Carregar o arquivo de dados de treinamento para o seu bucket do Amazon S3. Observe o caminho de localização do Amazon S3 para seu arquivo de treinamento (por exemplo, s3://bucketname/object.csv).

Armazene os dados do seu evento internamente com o Amazon Fraud Detector

Você pode optar por armazenar dados de eventos no Amazon Fraud Detector e usar os dados armazenados posteriormente para treinar seus modelos. Ao armazenar dados de eventos no Amazon Fraud Detector, você pode treinar modelos que usam variáveis computadas automaticamente para melhorar o desempenho, simplificar a reciclagem de modelos e atualizar rótulos de fraude para fechar o ciclo de feedback do aprendizado de máquina. Os eventos são

armazenados no nível do recurso Tipo de evento, portanto, todos os eventos do mesmo tipo de evento são armazenados juntos em um único conjunto de dados do tipo de evento. Como parte da definição de um tipo de evento, você pode, opcionalmente, especificar se deseja armazenar eventos para esse tipo de evento alternando a configuração de ingestão de eventos no console do Amazon Fraud Detector.

Você pode armazenar eventos únicos ou importar um grande número de conjuntos de dados de eventos no Amazon Fraud Detector. Eventos individuais podem ser transmitidos usando a GetEventPredictionAPI ou a SendEventAPI. Grandes conjuntos de dados podem ser importados de forma rápida e fácil para o Amazon Fraud Detector usando o recurso de importação em lote no console do Amazon Fraud Detector ou usando a CreateBatchImportJobAPI.

Você pode usar o console Amazon Fraud Detector a qualquer momento para verificar o número de eventos já armazenados para cada tipo de evento.

Prepare os dados do evento para armazenamento

Os dados de eventos armazenados internamente com o Amazon Fraud Detector são armazenados no nível do`Event Type` recurso. Portanto, todos os dados do evento que são do mesmo evento são armazenados em um único evento`Event Type`. Posteriormente, os eventos armazenados podem ser usados para treinar um novo modelo ou treinar novamente um modelo existente. Ao treinar um modelo usando os dados de eventos armazenados, você pode, opcionalmente, especificar um intervalo de tempo de eventos para limitar o tamanho do seu conjunto de dados de treinamento.

Sempre que você armazena seus dados no Amazon Fraud Detector, usando o console do Amazon Fraud Detector, a`SendEvent` API ou a`CreateBatchImportJob` API, o Amazon Fraud Detector valida seus dados antes de armazená-los. Se seus dados falharem na validação, os dados do evento não serão armazenados.

Pré-requisitos para armazenar dados internamente com o Amazon Fraud Detector

- Para garantir que os dados do seu evento passem pela validação e que o conjunto de dados seja armazenado com êxito, certifique-se de ter usado os insights fornecidos pelo Data models explorer para preparar seu conjunto de dados.
- Criou um tipo de evento para os dados do evento que você deseja armazenar com o Amazon Fraud Detector. Caso contrário, siga as instruções para criar um tipo de evento.

Validação de dados inteligente

Quando você carrega seu conjunto de dados no console do Amazon Fraud Detector para importação em lote, o Amazon Fraud Detector usa Smart Data Validation (SDV) para validar seu conjunto de dados antes de importar seus dados. O SDV verifica o arquivo de dados carregado e identifica problemas como dados ausentes e formatos ou tipos de dados incorretos. Além de validar seu conjunto de dados, o SDV também fornece um relatório de validação que lista todos os problemas que foram identificados e sugere ações para corrigir os problemas mais impactantes. Alguns dos problemas identificados pelo SDV podem ser críticos e devem ser resolvidos antes que o Amazon Fraud Detector possa importar seu conjunto de dados com sucesso. Para obter mais informações, consulte Relatório de validação de dados inteligentes.

O SDV valida seu conjunto de dados no nível do arquivo e no nível dos dados (linha). No nível do arquivo, o SDV verifica seu arquivo de dados e identifica problemas como permissões inadequadas para acessar o arquivo, tamanho incorreto do arquivo, formato do arquivo e cabeçalhos (metadados de eventos e variáveis de evento). No nível dos dados, o SDV verifica os dados de cada evento (linha) e identifica problemas como formato de dados incorreto, tamanho dos dados, formato de data e hora e valores nulos.

No momento, a validação inteligente de dados está disponível somente no console do Amazon Fraud Detector e a validação está ativada por padrão. Se você não quiser que o Amazon Fraud Detector use a Smart Data Validation antes de importar seu conjunto de dados, desative a validação no console do Amazon Fraud Detector ao fazer o upload do seu conjunto de dados.

Validando dados armazenados ao usar APIs ouAWS SDK

Ao fazer o upload de eventos por meio da operação`SendEvent`,`GetEventPrediction`, ou`CreateBatchImportJob` API, o Amazon Fraud Detector valida o seguinte:

- A EventIngestion configuração para esse tipo de evento é ATIVADA.
- Os carimbos de data/hora do evento não podem ser atualizados. Um evento com um ID de evento repetido e um EVENT_TIMESTAMP diferente será tratado como um erro.
- Os nomes e valores das variáveis correspondem ao formato esperado. Para obter mais informações, consulte Crie uma variável.
- As variáveis obrigatórias são preenchidas com um valor.
- Todos os registros de data e hora do evento não têm mais de 18 meses e não estão no future.

Armazene dados de eventos usando importação em lote

Com o recurso de importação em lote, você pode carregar de forma rápida e fácil grandes conjuntos de dados históricos de eventos no Amazon Fraud Detector usando o console, a API ou o AWS SDK. Para usar a importação em lote, crie um arquivo de entrada no formato CSV que contenha todos os dados do seu evento, faça o upload do arquivo CSV no bucket do Amazon S3 e inicie um trabalho de importação. O Amazon Fraud Detector primeiro valida os dados com base no tipo de evento e depois importa automaticamente todo o conjunto de dados. Depois que os dados forem importados, eles estarão prontos para serem usados no treinamento de novos modelos ou no treinamento de modelos existentes.

Arquivos de entrada e saída

O arquivo CSV de entrada deve conter cabeçalhos que correspondam às variáveis definidas no tipo de evento associado, além de quatro variáveis obrigatórias. Consulte Prepare os dados do evento para armazenamento para obter mais informações. O tamanho máximo do arquivo de dados de entrada é de 20 Gigabytes (GB), ou cerca de 50 milhões de eventos. O número de eventos variará de acordo com o tamanho do seu evento. Se o trabalho de importação for bem-sucedido, o arquivo de saída estará vazio. Se a importação não for bem-sucedida, o arquivo de saída conterá os registros de erros.

Criar um arquivo CSV

O Amazon Fraud Detector importa dados somente de arquivos no formato CSV (valores separados por vírgula). A primeira linha do seu arquivo CSV deve conter cabeçalhos de coluna que correspondam exatamente às variáveis definidas no tipo de evento associado, além de quatro variáveis obrigatórias: EVENT_ID, EVENT_TIMESTAMP, ENTITY_ID e ENTITY_TYPE. Você também pode incluir opcionalmente EVENT_LABEL e LABEL_TIMESTAMP (LABEL_TIMESTAMP é necessário se EVENT_LABEL estiver incluído).

Definir variáveis obrigatórias

As variáveis obrigatórias são consideradas metadados de eventos e devem ser especificadas em letras maiúsculas. Os metadados do evento são incluídos automaticamente para o treinamento do modelo. A tabela a seguir lista as variáveis obrigatórias, a descrição de cada variável e o formato necessário para a variável.

Name (Nome)	Descrição	Requisitos
ID DO EVENTO	Um identificador para o evento. Por exemplo, se seu evento for uma transação on-line, o EVENT_ID pode ser o número de referência da transação que foi fornecido ao seu cliente.	• O EVENT_ID é necessário para trabalhos de importaçã o em lote. • Essa opção deve ser exclusiva para esse evento. • Ela deve representar informações que sejam significativas para sua empresa. • Essa opção deve satisfazer ao padrão de expressão regular (por exemplo`^[0-9a-z_-]+ $.`) • Não recomendamos que você acrescente um carimbo de data/hora ao EVENT_ID. Fazer isso pode causar problemas ao atualizar o evento. Isso porque você deve fornecer exatamente o mesmo EVENT_ID se fizer isso.
EVENT_TIMESTAMP	o carimbo de data/hora em que o evento ocorreu. O carimbo de data/hora deve estar no padrão ISO 8601 em UTC.	• O EVENT_TIMESTAMP é necessário para trabalhos de importação em lote. • Essa opção deve ser especificada em um dos seguintes formatos: • %YYYYY-%MM-%DDT %HH: %mm: %sSz (padrão ISO 8601 em

Name (Nome)	Descrição	Requisitos
		UTC somente sem milissegundos) Exemplo: 2019-11-30T 13:01:01 Z • %aaaa/%mm/%dd %h: %mm: %s (AM/PM) Exemplos: 2019/11/30 13:01:01 ou 2019/11/30 13:01:01 • %mm/%dd/%aaaa %h: %mm: %s Exemplos: 30/11/2019 13:01:01, 30/11/2019 13:01:01 • %mm/%dd/%y %h: %mm: %s Exemplos: 30/11/19 13:01:01 PM, 11/30/19 13:01:01 • O Amazon Fraud Detector faz as seguintes suposições ao analisar formatos de data/hora para carimbos de data e hora de eventos: • Se você estiver usando o padrão ISO 8601, ele deve corresponder exatamente à especificação anterior

Name (Nome)	Descrição	Requisitos

		• Se você estiver usando um dos outros formatos, há flexibilidade adicional:
		  • Por meses e dias, você pode fornecer um ou dois dígitos. Por exemplo, 1/12/2019 é uma data válida.
		  • Você não precisa incluir hh:mm:ss se não os tiver (ou seja, você pode simplesmente fornecer uma data). Você também pode fornecer um subconjunto de apenas horas e minutos (por exemplo, hh:mm). O simples fornecimento de horas não é suportado. Milissegundos também não são suportados.
		  • Se você fornecer etiquetas AM/PM, presume-se que um relógio de 12 horas. Se não houver informações de AM/PM, presume-se que um relógio de 24 horas.
		  • Você pode usar “/” ou “-” como delimitadores para os elementos de data. “:” é assumido

Name (Nome)	Descrição	Requisitos
		para os elementos de timestamp.
ENTIDADE_ID	Um identificador para a entidade que executa o evento.	• ENTITY_ID é necessário para trabalhos de importaçã o em lote • Ele deve seguir o padrão de expressão regular:`^[0-9A-Za-z_.@+-]+$` . • Se o ID da entidade não estiver disponível no momento da avaliação, especifique o ID da entidade como desconhecido.
TIPO_ENTIDADE	A entidade que realiza o evento, como um comerciante ou um cliente	ENTITY_TYPE é necessário para trabalhos de importação em lote
RÓTULO DO EVENTO	Classifica o evento como`fraudulent` ou`legitimate`	EVENT_LABEL é necessári o se LABEL_TIMESTAMP estiver incluído
LABEL_TIMESTAMP	A data e hora em que o rótulo do evento foi preenchido ou atualizado pela última vez	• LABEL_TIMESTAMP é necessário se EVENT_LAB EL estiver incluído. • Essa opção deve seguir o formato do carimbo de data/ hora.

Carregar o arquivo CSV no Amazon S3

Após criar um arquivo CSV com seus dados (Amazon Simple Storage Service (Amazon Simple Storage Service (Amazon Simple Storage Service (Amazon Simple Storage Service (Amazon Simple Storage Service (Amazon Simple Storage Service (Amazon Simple

Para carregar dados de eventos em um bucket do Amazon S3

1. Faça login no AWS Management Console e abra o console do Amazon S3 em https://console.aws.amazon.com/s3/.
2. Selecione Create bucket (Criar bucket).

   O assistente Create bucket (Criar bucket) é aberto.
3. Em Bucket name (Nome do bucket), insira um nome compatível com o DNS para seu bucket.

   O nome do bucket deve:

   - Seja exclusivo em todo o Amazon S3.
   - Ter entre 3 e 63 caracteres.
   - Não contém caracteres maiúsculos.
   - Começar com uma letra minúscula ou um número.

   Depois de criado o bucket, você não pode mudar seu nome. Para obter informações sobre a nomenclatura de buckets, consulte Regras de nomeação de bucket no Guia do usuário do Amazon Simple Storage Service.

   > **Important**
   >
   > Evite incluir informações confidenciais, como números de conta, no nome do bucket. O nome do bucket é visível nos URLs que apontam para os objetos no bucket.
4. Em Region (Região), escolha a região da AWS onde deseja que o bucket resida. Você deve selecionar a mesma região em que está usando o Amazon Fraud Detector (N.) (Norte da) (Norte da) (Oregon) (Ohio) (Ohio) (Ohio) (Ohio) (Oregon) (Oregon) (Oregon) (Oregon) (Oregon) (Oregon) (Oregon) (Oregon) (Oregon) (Oregon) (Oregon) (Oregon) (Oregon) (Oregon) (Oregon) (
5. Em Bucket settings for Block Public Access (Configurações de bucket para o Bloqueio de acesso público), escolha as configurações de bloqueio de acesso público que deseja aplicar ao bucket.

   Recomendamos deixar todas as configurações habilitadas. Para obter mais informações sobre como bloquear o acesso público, consulte Bloquear o acesso Amazon S3 ao armazenamento do Amazon Simple Storage Service.
6. Selecione Create bucket (Criar bucket).

7. Carregar o arquivo de dados de treinamento para o seu bucket do Amazon S3. Observe o caminho de localização do Amazon S3 para seu arquivo de treinamento (por exemplo, s3://bucketname/object.csv).

Importação Batch de dados de eventos no console do Amazon Fraud Detector

Você pode importar facilmente um grande número de seus conjuntos de dados de eventos no console do Amazon Fraud Detector, usando a`CreateBatchImportJob` API ou usando o AWS SDK. Antes de continuar, certifique-se de ter seguido as instruções para preparar seu conjunto de dados como um arquivo CSV. Certifique-se de também carregar o arquivo CSV para um bucket do Amazon S3.

Usando o console Amazon Fraud Detector

Para importar dados de eventos em lote no console

1. Abra o console da AWS, faça login em sua conta e navegue até o Amazon Fraud Detector.
2. No painel de navegação esquerdo, escolha Events.
3. Escolha o tipo de evento.
4. Selecione a guia Eventos armazenados.
5. No painel de detalhes de eventos armazenados, verifique se a ingestão de eventos está ATIVADA.
6. No painel Importar dados de eventos, escolha Nova importação.
7. Na página de importação de novos eventos, forneça as seguintes informações:
   - [Recomendado] Deixe a opção Ativar a Validação Inteligente de Dados para este conjunto de dados - novo definido com a configuração padrão.
   - Para a função do IAM para dados, selecione a função do IAM que você criou para o bucket do Amazon S3 que contém o arquivo CSV que você planeja importar.
   - Em Local de entrada de dados, insira o local S3 onde você tem seu arquivo CSV.
   - Se você quiser especificar um local separado para armazenar seus resultados de importação, clique no botão Separar local de dados para entradas e resultados e forneça um local válido de bucket do Amazon S3.

> **Important**
>
> Certifique-se de que a função do IAM que você selecionou tenha permissões de leitura para seu bucket Amazon S3 de entrada e permissões de gravação para seu bucket Amazon S3 de saída.

8. Escolha Start (Iniciar).
9. A coluna Status no painel Dados de eventos de importação exibe o status do seu trabalho de validação e importação. O banner na parte superior fornece uma descrição de alto nível do status, pois seu conjunto de dados passa primeiro pela validação e depois pela importação.
10. Siga as orientações fornecidas paraMonitore o progresso do trabalho de validação e importação do conjunto de dados.

Monitore o progresso do trabalho de validação e importação do conjunto de dados

Se você estiver usando o console do Amazon Fraud Detector para realizar um trabalho de importação em lote, por padrão, o Amazon Fraud Detector valida seu conjunto de dados antes da importação. Você pode monitorar o progresso e o status dos trabalhos de validação e importação na página de importação de novos eventos do console do Amazon Fraud Detector. Um banner na parte superior da página fornece uma breve descrição das descobertas de validação e o status do trabalho de importação. Dependendo das descobertas da validação e do status do seu trabalho de importação, talvez seja necessário tomar medidas para garantir a validação e a importação bem-sucedidas do seu conjunto de dados.

A tabela a seguir fornece detalhes das ações que você deve realizar, dependendo do resultado das operações de validação e importação.

Mensagem de banner	Status	O que significa	O que devo fazer
A validação de dados foi iniciada	Validação em andamento	O SDV começou a validar seu conjunto de dados	Aguarde até que o status mude

Mensagem de banner	Status	O que significa	O que devo fazer
A validação de dados não pode continuar devido a erros no seu conjunto de dados. Corrija erros em seu arquivo de dados e inicie um novo trabalho de importação. Consulte o relatório de validação para obter mais informações	Falha na validação	O SDV identificou problemas em seu arquivo de dados. Esses problemas devem ser resolvidos para que a importação bem-sucedida do seu conjunto de dados seja importada.	No painel Importar dados de eventos, selecione o ID do Job e visualize o relatório de validação. Siga as recomendações no relatório para resolver todos os erros listados. Para obter mais informações, consulte Usando o relatório de validação.
A importação de dados foi iniciada. Validação concluída	Importação em andamento	Seu conjunto de dados passou pela validação. O AFD começou a importar seu conjunto de dados	Aguarde até que o status mude

Mensagem de banner	Status	O que significa	O que devo fazer
Validação concluída com avisos. A importação de dados foi iniciada	Importação em andamento	Alguns dos dados em seu conjunto de dados falharam na validação. No entanto, os dados que passaram pela validação atendem aos requisitos mínimos de tamanho de dados para importação.	Monitore a mensagem no banner e espere que o status mude

Mensagem de banner	Status	O que significa	O que devo fazer
Seus dados foram parcialmente importados. Alguns dos dados falharam na validação e não foram importados. Consulte o relatório de validação para obter mais informações.	Importado. O status mostra um ícone de aviso.	Alguns dos dados em seu arquivo de dados que falharam na validação não foram importados. O restante dos dados que passaram pela validação foi importado.	No painel Importar dados de eventos, selecione o ID do Job e visualize o relatório de validação. Siga as recomendações na tabela de avisos em nível de dados para abordar os avisos listados. Você não precisa abordar todos os avisos. No entanto, certifique-se de que seu conjunto de dados tenha mais de 50% dos dados passados pela validação para uma importação bem-sucedida. Depois de resolver os avisos, inicie um novo trabalho de importação. Para obter mais informações, consulte Usando o relatório de validação.
A importação de dados falhou devido a um erro de processamento. Iniciar um novo trabalho de importação de dados	Falha na importação	A importação falhou devido a um erro transitório de tempo de execução	Iniciar um novo trabalho de importação

Mensagem de banner	Status	O que significa	O que devo fazer
Os dados foram importados com sucesso	Importado	A validação e a importação foram concluídas com êxito	Selecione o ID do Job de importação para ver os detalhes e, em seguida, prossiga com o treinamento do modelo

> **Note**
>
> Recomendamos esperar 10 minutos após a importação bem-sucedida do conjunto de dados para o Amazon Fraud Detector para garantir que eles sejam totalmente ingeridos pelo sistema.

Relatório de validação de dados inteligentes

A Validação Inteligente de Dados cria um relatório de validação após a conclusão da validação. O relatório de validação fornece detalhes de todos os problemas que o SDV identificou em seu conjunto de dados, com sugestões de ações para corrigir os problemas mais impactantes. Você pode usar o relatório de validação para determinar quais são os problemas, onde eles estão localizados no conjunto de dados, a gravidade dos problemas e como corrigi-los. O relatório de validação é criado mesmo quando a validação é concluída com êxito. Nesse caso, você pode visualizar o relatório para ver se há algum problema listado e, se houver, decidir se deseja corrigir algum deles.

> **Note**
>
> A versão atual do SDV verifica seu conjunto de dados em busca de problemas que possam causar falha na importação do lote. Se a validação e a importação em lote forem bem-sucedidas, seu conjunto de dados ainda poderá ter problemas que podem fazer com que o treinamento do modelo falhe. Recomendamos que você visualize seu relatório de validação, mesmo que a validação e a importação tenham sido bem-sucedidas, e resolva quaisquer

problemas listados no relatório para um treinamento bem-sucedido do modelo. Depois de resolver os problemas, crie um novo trabalho de importação em lote.

Acessando o relatório de validação

Você pode acessar o relatório de validação a qualquer momento após a conclusão da validação usando uma das seguintes opções:

1. Depois que a validação for concluída e enquanto o trabalho de importação estiver em andamento, no banner superior, escolha Exibir relatório de validação.
2. Depois que o Job de importação for concluído, no painel Dados de eventos de importação, escolha o ID do trabalho de importação que acabou de ser concluído.

Usando o relatório de validação

A página do relatório de validação do seu trabalho de importação fornece os detalhes dessa tarefa de importação, uma lista de erros críticos, se houver, uma lista de avisos sobre eventos específicos (linhas) em seu conjunto de dados, se encontrados, e um breve resumo do seu conjunto de dados que inclui informações como valores que não são válidos e valores faltantes para cada variável.

- Importar detalhes do trabalho

  Fornece detalhes do trabalho de importação. Se sua tarefa de importação falhou ou seu conjunto de dados foi parcialmente importado, escolha Ir para o arquivo de resultados para ver os registros de erros dos eventos que falharam na importação.

- Erros críticos

  Fornece detalhes dos problemas mais impactantes em seu conjunto de dados identificado pelo SDV. Todos os problemas listados nesse painel são essenciais e você deve resolvê-los antes de prosseguir com a importação. Se você tentar importar seu conjunto de dados sem resolver os problemas críticos, sua tarefa de importação poderá falhar.

  Para resolver os problemas críticos, siga as recomendações fornecidas para cada aviso. Depois de resolver todos os problemas listados no painel Erros críticos, crie um novo trabalho de importação em lote.

- Avisos em nível de dados

Fornece um resumo dos avisos para eventos específicos (linhas) em seu conjunto de dados. Se o painel Avisos de nível de dados estiver preenchido, alguns dos eventos em seu conjunto de dados falharam na validação e não foram importados.

Para cada aviso, a coluna Descrição exibe o número de eventos que têm o problema. Além disso, os IDs de eventos de amostra fornecem uma lista parcial de exemplos de IDs de eventos que você pode usar como ponto de partida para localizar o restante dos eventos que têm o problema. Use a recomendação fornecida no aviso para corrigir o problema. Use também os registros de erros do seu arquivo de saída para obter informações adicionais sobre o problema. Os registros de erros são gerados para todos os eventos que falharam na importação do lote. Para acessar os registros de erros, no painel Importar detalhes da tarefa, escolha Ir para o arquivo de resultados.

> **Note**
>
> Se mais de 50% dos eventos (linhas) em seu conjunto de dados falharem na validação, a tarefa de importação também falhará. Nesse caso, você deve corrigir os dados antes de iniciar um novo trabalho de importação.

- Resumo do conjunto de dados

  Fornece um resumo do relatório de validação do seu conjunto de dados. Se a coluna Número de avisos mostrar mais de 0 avisos, decida se você precisa corrigir esses avisos. Se a coluna Número de avisos mostrar 0s, continue treinando seu modelo.

Importar dados de eventos Batch usando o AWS SDK for Python (Boto3)

O exemplo a seguir mostra uma solicitação de exemplo para CreateBatchImportJobAPI. Um trabalho de importação em lote deve incluir um JobId, InputPath, OutputPath eventTypeNameiamRoleArne. O jobID não pode conter o mesmo ID de um trabalho anterior, a menos que o trabalho exista no estado CREATE_FAILED. O InputPath e o OutputPath devem ser caminhos S3 válidos. Você pode optar por não especificar o nome do arquivo no OutputPath, mas ainda precisará fornecer um local válido do bucket do S3. A eventTypeName terra iamRoleArn deve existir. A função do IAM deve conceder permissões de leitura para inserir o bucket do Amazon S3 e permissões de gravação para o bucket Amazon S3 de saída.

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

Cancelar trabalho de importação em lote

Você pode cancelar um trabalho de importação em lote em andamento a qualquer momento no console do Amazon Fraud Detector, usando a`CancelBatchImportJob` API ou o AWS SDK.

Para cancelar um trabalho de importação em lote no console

1. Abra o console da AWS, faça login em sua conta e navegue até o Amazon Fraud Detector.
2. No painel de navegação esquerdo, escolha Events.
3. Escolha o tipo de evento.
4. Selecione a guia Eventos armazenados.
5. No painel Importar dados de eventos, escolha o ID do trabalho de um trabalho de importação em andamento que você deseja cancelar.
6. Na página de trabalho do evento, clique em Ações e selecione Cancelar importação de eventos.
7. Escolha Interromper importação de eventos para cancelar a tarefa de importação em lote.

Cancelamento do trabalho de importação em lote usando o AWS SDK for Python (Boto3)

O exemplo a seguir mostra uma solicitação de exemplo para a`CancelBatchImportJob` API. O trabalho de cancelamento de importação deve incluir o ID do trabalho de um trabalho de importação em lote em andamento.

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

Armazene dados de eventos usando a operação GetEventPredictions da API

Por padrão, todos os eventos enviados à`GetEventPrediction` API para avaliação são armazenados no Amazon Fraud Detector. Isso significa que o Amazon Fraud Detector armazenará automaticamente os dados do evento quando você gerar uma previsão e usará esses dados para atualizar variáveis calculadas quase em tempo real. Você pode desativar o armazenamento de dados navegando até o tipo de evento no console do Amazon Fraud Detector e desativando a ingestão de eventos ou atualizando o EventIngestion valor para DESATIVADO usando a operação da`PutEventType` API. Para obter mais informações sobre a operação`GetEventPrediction` da API, consultePrevisões de fraude.

> **Important**
>
> É altamente recomendável que, depois de ativar a ingestão de eventos para um tipo de evento, mantenha-a ativada. Desabilitar a ingestão de eventos para o mesmo tipo de evento e gerar previsões pode resultar em um comportamento inconsistente.

Armazene dados de eventos usando a operação SendEvent da API

Você pode usar a operação da`SendEvent` API para armazenar eventos no Amazon Fraud Detector sem gerar previsões de fraude para esses eventos. Por exemplo, você pode usar a`SendEvent` operação para carregar um conjunto de dados histórico, que poderá ser usado posteriormente para treinar um modelo.

Formatos de data e hora do evento para SendEvent API

Ao armazenar dados de eventos usando a`SendEvent` API, você deve garantir que a data e hora do evento esteja no formato exigido. O Amazon Fraud Detector é compatível com os seguintes formatos de data/hora:

- %YYYYY-%MM-%DDT%HH: %mm: %sSz (padrão ISO 8601 em UTC somente sem milissegundos)

  Exemplo: 2019-11-30T 13:01:01 Z

- %aaaa/%mm/%dd %h: %mm: %s (AM/PM)

  Exemplos: 2019/11/30 13:01:01 ou 2019/11/30 13:01:01

- %mm/%dd/%aaaa %h: %mm: %s

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

- %mm/%dd/%y %h: %mm: %s

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

O Amazon Fraud Detector faz as seguintes suposições ao analisar formatos de data/hora para carimbos de data e hora de eventos:

- Se você estiver usando o padrão ISO 8601, ele deve corresponder exatamente à especificação anterior
- Se você estiver usando um dos outros formatos, há flexibilidade adicional:
  - Por meses e dias, você pode fornecer um ou dois dígitos. Por exemplo, 1/12/2019 é uma data válida.
  - Você não precisa incluir hh:mm:ss se não os tiver (ou seja, você pode simplesmente fornecer uma data). Você também pode fornecer um subconjunto de apenas horas e minutos (por exemplo, hh:mm). O simples fornecimento de horas não é suportado. Milissegundos também não são suportados.
  - Se você fornecer etiquetas AM/PM, presume-se que um relógio de 12 horas. Se não houver informações de AM/PM, presume-se que um relógio de 24 horas.
  - Você pode usar “/” ou “-” como delimitadores para os elementos de data. “:” é assumido para os elementos de timestamp.

Veja a seguir um exemplo de chamada de`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'}],

)
```

Obtenha detalhes dos dados de um evento armazenado

Depois de armazenar dados de eventos no Amazon Fraud Detector, você pode verificar os dados mais recentes que foram armazenados para um evento usando a GetEventAPI. O código de exemplo a seguir verifica os dados mais recentes armazenados para o`sample_registration` evento.

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

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

Exibir métricas do conjunto de dados de eventos armazenados

Para cada tipo de evento, você pode visualizar métricas como número de eventos armazenados, tamanho total de seus eventos armazenados e registros de data e hora dos eventos armazenados mais antigos e mais recentes, no console do Amazon Fraud Detector.

Para visualizar métricas de eventos armazenadas de um tipo de evento,

1. Abra oAWS console e faça login em sua conta. Navegue até o Amazon Fraud Detector.
2. No painel de navegação esquerdo, escolha Events.
3. Escolha o tipo de evento.
4. Selecione a guia Eventos armazenados.
5. O painel de detalhes de eventos armazenados exibe as métricas. Essas métricas são atualizadas automaticamente uma vez por dia.

6. Opcionalmente, clique em Atualizar métricas de eventos para atualizar manualmente suas métricas.

> **Note**
>
> Se você acabou de importar seus dados, recomendamos esperar de 5 a 10 minutos após concluir a importação dos dados para atualizar e visualizar as métricas.

Orquestração de eventos

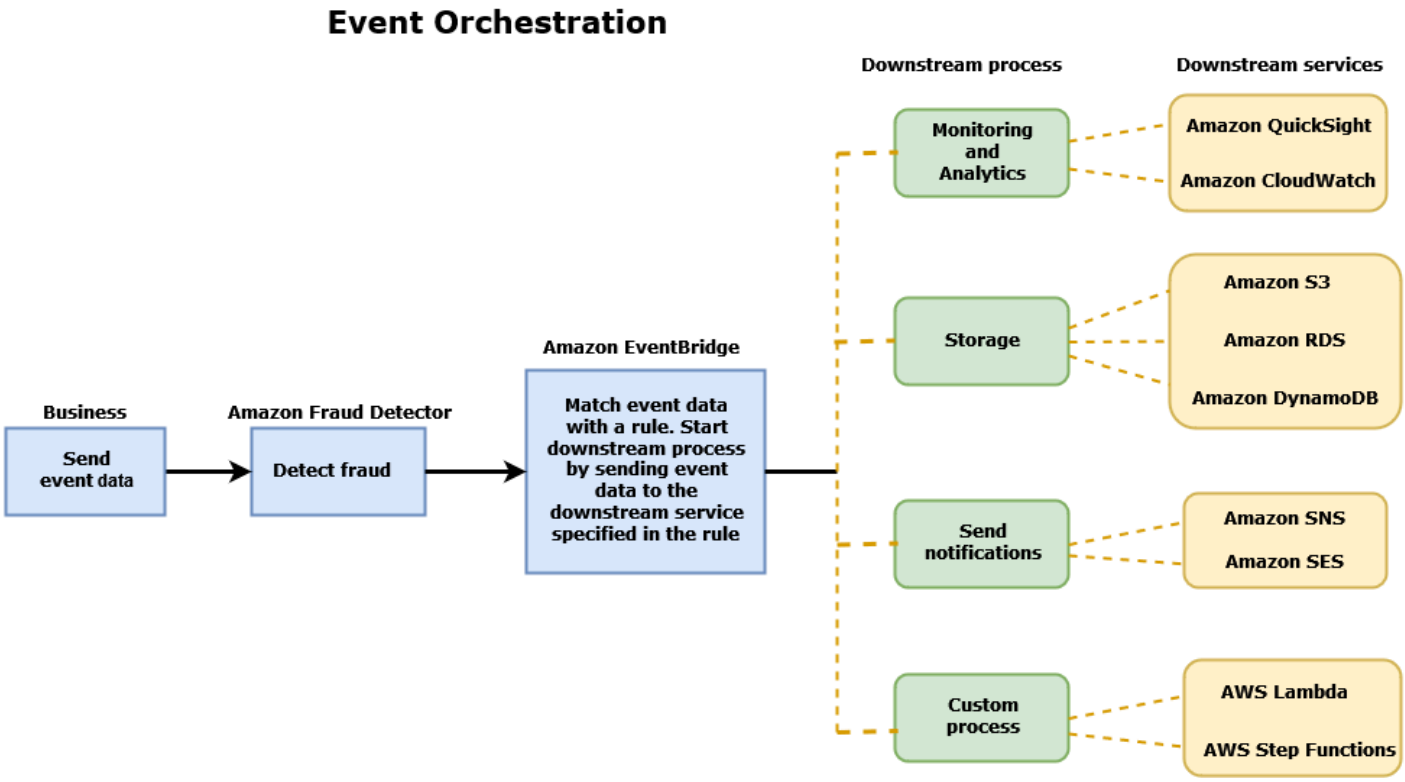
A orquestração de eventos facilita o envio de eventos Serviços da AWS para processamento posterior, usando a Amazon. EventBridge O Amazon Fraud Detector fornece regras simples que você pode usar para automatizar o processamento de eventos após a detecção de fraudes. Com a orquestração de eventos, você pode automatizar processos posteriores de eventos, como enviar eventos para painéis para obter insights dos dados do evento, gerar notificações com base nos resultados da detecção de fraudes e atualizar eventos com um rótulo baseado no aprendizado da detecção de fraudes.

A orquestração de eventos fornece acesso fácil aos serviços no AWS ambiente, por meio da Amazon. EventBridge Você pode configurar EventBridge a Amazon para enviar eventos diretamente Serviços da AWS ou indiretamente usando destinos de API. Os Serviços da AWS que você usa para orquestrar seus processos downstream também são chamados de destinos. Alguns dos alvos que você pode usar para orquestrar o processamento downstream são os seguintes:

- Para monitoramento e análise — Amazon QuickSight, Amazon CloudWatch
- Para armazenamento — Amazon S3, Amazon RDS, Amazon DynamoDB
- Para enviar notificações — Amazon SNS, Amazon SES
- Para processamento personalizado — AWS Lambda, AWS Step Functions

Para obter mais informações sobre as metas de orquestração suportadas pela Amazon EventBridge, consulte Destinos da Amazon EventBridge .

O diagrama a seguir fornece uma visão geral de como a orquestração de eventos funciona.



Configurando a orquestração de eventos

Configurar a orquestração de eventos para seus eventos exige que você configure processos em seu serviço de destino, configure EventBridge a Amazon para receber e enviar dados de eventos e crie regras na Amazon EventBridge que especifiquem as condições para iniciar os processos posteriores. Conclua as etapas a seguir para configurar a orquestração de eventos:

Para configurar a orquestração de eventos

1. Acesse o Guia EventBridge do usuário da Amazon e saiba como usar a Amazon EventBridge. Certifique-se de aprender como criar regras na Amazon EventBridge para seu caso de uso.
2. Siga as instruções paraHabilite a orquestração de eventos no Amazon Fraud Detector.

> **Note**
>
> A orquestração de eventos do seu evento está desativada por padrão.

3. Configure seu serviço de destino para receber e processar os dados do evento. Por exemplo, se seu processo de downstream envolver o envio de notificações e você quiser usar o Amazon

SNS, acesse o console do Amazon SNS, crie um tópico do SNS e, em seguida, inscreva um endpoint no tópico.

4. Siga as instruções para criar EventBridge regras da Amazon.

> **Important**
>
> Ao criar o padrão de evento na Amazon EventBridge, certifique-se de fornecer o campo `aws.frauddetector` de origem e o campo `Event Prediction Result Returned` de tipo de detalhe.

Habilite a orquestração de eventos no Amazon Fraud Detector

Você pode ativar a orquestração de eventos para um evento ao criar seu tipo de evento ou depois de criar seu tipo de evento. A orquestração de eventos pode ser habilitada no console do Amazon Fraud Detector, usando o `put-event-type` comando, usando a `PutEventType` API ou usando o. AWS SDK for Python (Boto3)

Habilite a orquestração de eventos no console do Amazon Fraud Detector

Este exemplo permite a orquestração de eventos para um tipo de evento que já foi criado. Se você estiver criando um novo tipo de evento e quiser ativar a orquestração, siga as instruções para. Crie um tipo de evento

Para habilitar a orquestração de eventos

1. Abra o AWSManagement Console e faça login na sua conta. Navegue até o Amazon Fraud Detector.
2. No painel de navegação esquerdo, escolha Events.
3. Na página Tipo de eventos, escolha seu tipo de evento.
4. Ative a opção Ativar orquestração de eventos com a Amazon. EventBridge
5. Continue com as instruções da etapa 3 paraConfigurando a orquestração de eventos.

Habilite a orquestração de eventos usando o AWS SDK for Python (Boto3)

O exemplo a seguir mostra um exemplo de solicitação para atualizar um tipo de evento para permitir `sample_registration` a orquestração de eventos. O exemplo usa a `PutEventType` API e

pressupõe que você tenha criado as variáveis `ip_addressemail_address`, os rótulos `legit` e `fraud` o tipo de `sample_customer` entidade. Para obter informações sobre como criar esses recursos, consulte Recursos.

```
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'])
```

Desative a orquestração de eventos no Amazon Fraud Detector

Você pode desativar a orquestração de eventos para um evento a qualquer momento no console do Amazon Fraud Detector, usando o `put-event-type` comando, usando a `PutEventType` API ou usando o. AWS SDK for Python (Boto3)

Desative a orquestração de eventos no console do Amazon Fraud Detector

Para desativar a orquestração de eventos

1. Abra o AWSManagement Console e faça login na sua conta. Navegue até o Amazon Fraud Detector.
2. No painel de navegação esquerdo, escolha Events.
3. Na página Tipo de eventos, escolha seu tipo de evento.
4. Desative a opção Ativar orquestração de eventos com a Amazon. EventBridge

Desative a orquestração de eventos usando o AWS SDK for Python (Boto3)

O exemplo a seguir mostra um exemplo de solicitação de atualização de um tipo de evento `sample_registration` para desativar a orquestração de eventos usando a `PutEventType` API.

```
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'])
```

Modelo

O Amazon Fraud Detector usa modelos de aprendizado de máquina para gerar previsões de fraudes. Cada modelo é treinado usando um tipo de modelo. O tipo de modelo especifica os algoritmos e as transformações usados para treinar o modelo. O treinamento de modelos é o processo de usar um conjunto de dados fornecido por você para criar um modelo capaz de prever eventos fraudulentos.

Para criar um modelo, você deve primeiro escolher um tipo de modelo e, em seguida, preparar e fornecer dados que serão usados para treinar o modelo.

Escolha um tipo de modelo

Os seguintes tipos de modelo estão disponíveis no Amazon Fraud Detector. Escolha um tipo de modelo que funcione para seu caso de uso.

- Informações sobre fraudes on-line

  O tipo de modelo Online Fraud Insights é otimizado para detectar fraudes quando há poucos dados históricos disponíveis sobre a entidade que está sendo avaliada, por exemplo, um novo cliente se registrando on-line para uma nova conta.
- Informações sobre fraudes em transações

  O tipo de modelo Transaction Fraud Insights é mais adequado para detectar casos de uso de fraude em que a entidade que está sendo avaliada pode ter um histórico de interações que o modelo pode analisar para melhorar a precisão da previsão (por exemplo, um cliente existente com histórico de compras anteriores).
- Insights sobre aquisição de contas

  O tipo de modelo Account Takeover Insights detecta se uma conta foi comprometida por phishing ou outro tipo de ataque. Os dados de login de uma conta comprometida, como o navegador e o dispositivo usados no login, são diferentes dos dados históricos de login associados à conta.

Informações sobre fraudes on-line

O Online Fraud Insights é um modelo de aprendizado de máquina supervisionado, o que significa que ele usa exemplos históricos de transações fraudulentas e legítimas para treinar o modelo. O

modelo Online Fraud Insights pode detectar fraudes com base em poucos dados históricos. As entradas do modelo são flexíveis, então você pode adaptá-lo para detectar uma variedade de riscos de fraude, incluindo avaliações falsas, abuso de promoções e fraudes no check-out de hóspedes.

O modelo Online Fraud Insights usa um conjunto de algoritmos de aprendizado de máquina para enriquecimento, transformação e classificação de fraudes de dados. Como parte do processo de treinamento do modelo, o Online Fraud Insights enriquece elementos de dados brutos, como endereço IP e número BIN, com dados de terceiros, como a geolocalização do endereço IP ou o banco emissor de um cartão de crédito. Além de dados de terceiros, o Online Fraud Insights usa algoritmos de aprendizado profundo que levam em consideração os padrões de fraude observados na Amazon AWS e. Esses padrões de fraude se tornam recursos de entrada para seu modelo usando um algoritmo de aumento de árvore de gradiente.

Para aumentar o desempenho, o Online Fraud Insights otimiza os hiperparâmetros do algoritmo de aumento da árvore de gradiente por meio de um processo de otimização bayesiano. Ele treina sequencialmente dezenas de modelos diferentes com parâmetros de modelo variados (como número de árvores, profundidade das árvores e número de amostras por folha). Ele também usa diferentes estratégias de otimização, como aumentar a população minoritária de fraudes, para lidar com taxas de fraude muito baixas.

Seleção da fonte de dados

Ao treinar um modelo do Online Fraud Insights, você pode escolher treinar o modelo em dados de eventos armazenados externamente (fora do Amazon Fraud Detector) ou armazenados no Amazon Fraud Detector. O armazenamento externo que o Amazon Fraud Detector suporta atualmente é o Amazon Simple Storage Service (Amazon S3). Se você estiver usando armazenamento externo, seu conjunto de dados do evento deve ser carregado no formato de valores separados por vírgula (CSV) em um bucket do Amazon S3. Essas opções de armazenamento de dados são chamadas na configuração de treinamento do modelo como EXTERNAL_EVENTS (para armazenamento externo) e INGESTED_EVENTS (para armazenamento interno). Para obter mais informações sobre as fontes de dados disponíveis e como armazenar dados nelas, consulteArmazenamento de dados de eventos.

Preparar dados

Independentemente de onde você escolher armazenar os dados do seu evento (Amazon S3 ou Amazon Fraud Detector), os requisitos para o tipo de modelo do Online Fraud Insights são os mesmos.

Seu conjunto de dados deve conter o cabeçalho da coluna EVENT_LABEL. Essa variável classifica um evento como fraudulento ou legítimo. Ao usar um arquivo CSV (armazenamento externo), você deve incluir EVENT_LABEL para cada evento no arquivo. Para armazenamento interno, o campo EVENT_LABEL é opcional, mas todos os eventos devem ser rotulados para serem incluídos em um conjunto de dados de treinamento. Ao configurar seu modelo de treinamento, você pode escolher se deseja ignorar eventos não rotulados, assumir um rótulo legítimo para eventos não rotulados ou assumir um rótulo fraudulento para todos os eventos não rotulados.

Seleção de dados

Consulte Coletar dados de eventos para obter informações sobre como selecionar dados para treinar seu modelo Online Fraud Insights.

O processo de treinamento do Online Fraud Insights mostra e divide dados históricos com base em EVENT_TIMESTAMP. Não há necessidade de amostrar manualmente os dados, e isso pode afetar negativamente os resultados do seu modelo.

Variáveis do evento

O modelo Online Fraud Insights exige pelo menos duas variáveis, além dos metadados de eventos necessários, que passaram pela validação de dados para o treinamento do modelo e permitem até 100 variáveis por modelo. Geralmente, quanto mais variáveis você fornece, melhor o modelo pode diferenciar entre fraude e eventos legítimos. Embora o modelo Online Fraud Insights possa suportar dezenas de variáveis, incluindo variáveis personalizadas, recomendamos incluir endereço IP e endereço de e-mail, pois essas variáveis geralmente são mais eficazes na identificação da entidade que está sendo avaliada.

Validando dados

Como parte do processo de treinamento, o Online Fraud Insights validará o conjunto de dados para problemas de qualidade de dados que possam afetar o treinamento do modelo. Depois de validar os dados, o Amazon Fraud Detector tomará as medidas apropriadas para criar o melhor modelo possível. Isso inclui emitir avisos sobre possíveis problemas de qualidade de dados, remover automaticamente variáveis com problemas de qualidade de dados ou emitir um erro e interromper o processo de treinamento do modelo. Para obter mais informações, consulte validação do conjunto de dados.

Informações sobre fraudes em transações

O tipo de modelo Transaction Fraud Insights foi projetado para detectar fraudes on-line ou card-not-present em transações. O Transaction Fraud Insights é um modelo de aprendizado de máquina supervisionado, o que significa que ele usa exemplos históricos de transações fraudulentas e legítimas para treinar o modelo.

O modelo Transaction Fraud Insights usa um conjunto de algoritmos de aprendizado de máquina para enriquecimento, transformação e classificação de fraudes de dados. Ele utiliza um mecanismo de engenharia de recursos para criar agregados em nível de entidade e de evento. Como parte do processo de treinamento do modelo, o Transaction Fraud Insights enriquece elementos de dados brutos, como endereço IP e número BIN, com dados de terceiros, como a geolocalização do endereço IP ou o banco emissor de um cartão de crédito. Além de dados de terceiros, o Transaction Fraud Insights usa algoritmos de aprendizado profundo que levam em conta os padrões de fraude observados na Amazon. AWS Esses padrões de fraude se tornam recursos de entrada para seu modelo usando um algoritmo de aumento de árvore de gradiente.

Para aumentar o desempenho, o Transaction Fraud Insights otimiza os hiperparâmetros do algoritmo de aumento da árvore de gradiente por meio de um processo de otimização bayesiano, treinando sequencialmente dezenas de modelos diferentes com parâmetros de modelo variados (como número de árvores, profundidade das árvores, número de amostras por folha), bem como diferentes estratégias de otimização, como aumentar a população minoritária de fraudes para lidar com taxas de fraude muito baixas.

Como parte do processo de treinamento do modelo, o mecanismo de engenharia de recursos do modelo Transaction Fraud calcula os valores de cada entidade exclusiva em seu conjunto de dados de treinamento para ajudar a melhorar as previsões de fraudes. Por exemplo, durante o processo de treinamento, o Amazon Fraud Detector calcula e armazena a última vez que uma entidade fez uma compra e atualiza dinamicamente esse valor sempre que você chama a API `GetEventPrediction` ou`SendEvent`. Durante uma previsão de fraude, as variáveis do evento são combinadas com outros metadados da entidade e do evento para prever se a transação é fraudulenta.

Seleção da fonte de dados

Os modelos do Transaction Fraud Insights são treinados em conjuntos de dados armazenados internamente somente com o Amazon Fraud Detector (INGESTED_EVENTS). Isso permite que o Amazon Fraud Detector atualize continuamente os valores calculados sobre as entidades que você está avaliando. Para obter mais informações sobre as fontes de dados disponíveis, consulte Armazenamento de dados de eventos

Preparar dados

Antes de treinar um modelo do Transaction Fraud Insights, certifique-se de que seu arquivo de dados contenha todos os cabeçalhos, conforme mencionado em Prepare o conjunto de dados do evento. O modelo Transaction Fraud Insights compara novas entidades que são recebidas com os exemplos de entidades fraudulentas e legítimas no conjunto de dados, por isso é útil fornecer muitos exemplos para cada entidade.

O Amazon Fraud Detector transforma automaticamente o conjunto de dados de eventos armazenado no formato correto para treinamento. Depois que o modelo concluir o treinamento, você poderá revisar as métricas de desempenho e determinar se deve adicionar entidades ao seu conjunto de dados de treinamento.

Seleção de dados

Por padrão, o Transaction Fraud Insights treina todo o seu conjunto de dados armazenado para o tipo de evento selecionado. Opcionalmente, você pode definir um intervalo de tempo para reduzir os eventos usados para treinar seu modelo. Ao definir um intervalo de tempo, certifique-se de que os registros usados para treinar o modelo tenham tido tempo suficiente para amadurecer. Ou seja, já passou tempo suficiente para garantir que registros legítimos e fraudulentos tenham sido identificados corretamente. Por exemplo, para fraudes de estorno, geralmente são necessários 60 dias ou mais para identificar corretamente eventos fraudulentos. Para obter o melhor desempenho do modelo, certifique-se de que todos os registros em seu conjunto de dados de treinamento estejam maduros.

Não há necessidade de selecionar um intervalo de tempo que represente uma taxa de fraude ideal. O Amazon Fraud Detector coleta amostras automaticamente de seus dados para alcançar o equilíbrio entre taxas de fraude, intervalo de tempo e contagem de entidades.

O Amazon Fraud Detector retornará um erro de validação durante o treinamento do modelo se você selecionar um intervalo de tempo no qual não haja eventos suficientes para treinar um modelo com sucesso. Para conjuntos de dados armazenados, o campo EVENT_LABEL é opcional, mas os eventos devem ser rotulados para serem incluídos em seu conjunto de dados de treinamento. Ao configurar seu modelo de treinamento, você pode escolher se deseja ignorar eventos não rotulados, assumir um rótulo legítimo para eventos não rotulados ou assumir um rótulo fraudulento para eventos não rotulados.

Variáveis do evento

O tipo de evento usado para treinar o modelo deve conter pelo menos 2 variáveis, além dos metadados de eventos obrigatórios, que passaram pela validação de dados e podem conter até 100 variáveis. Geralmente, quanto mais variáveis você fornece, melhor o modelo pode diferenciar entre fraude e eventos legítimos. Embora o modelo Transaction Fraud Insight possa suportar dezenas de variáveis, incluindo variáveis personalizadas, recomendamos que você inclua endereço IP, endereço de e-mail, tipo de instrumento de pagamento, preço do pedido e BIN do cartão.

Validando dados

Como parte do processo de treinamento, o Transaction Fraud Insights valida o conjunto de dados de treinamento para problemas de qualidade de dados que possam afetar o treinamento do modelo. Depois de validar os dados, o Amazon Fraud Detector toma as medidas apropriadas para criar o melhor modelo possível. Isso inclui emitir avisos sobre possíveis problemas de qualidade de dados, remover automaticamente variáveis com problemas de qualidade de dados ou emitir um erro e interromper o processo de treinamento do modelo. Para obter mais informações, consulte Validação do conjunto de dados.

O Amazon Fraud Detector emitirá um aviso, mas continuará treinando um modelo se o número de entidades exclusivas for inferior a 1.500, pois isso pode afetar a qualidade dos dados de treinamento. Se você receber um aviso, revise a métrica de desempenho.

Insights sobre aquisição de contas

O tipo de modelo Account Takeover Insights (ATI) identifica atividades on-line fraudulentas detectando se as contas foram comprometidas por invasões maliciosas, phishing ou roubo de credenciais. O Account Takeover Insights é um modelo de aprendizado de máquina que usa eventos de login da sua empresa on-line para treinar o modelo.

Você pode incorporar um modelo treinado do Account Takeover Insights ao seu fluxo de login em tempo real para detectar se uma conta está comprometida. O modelo avalia uma variedade de tipos de autenticação e login. Eles incluem logins de aplicativos web, autenticações baseadas em API e single-sign-on (SSO). Para usar o modelo Account Takeover Insights, chame a GetEventPredictionAPI depois que uma credencial de login válida for apresentada. A API gera uma pontuação que quantifica o risco de comprometimento da conta. O Amazon Fraud Detector usa a pontuação e as regras que você definiu para retornar um ou mais resultados para os eventos de login. Os resultados são aqueles que você configurou. Com base nos resultados que você recebe, você pode tomar as medidas apropriadas para cada login. Ou seja, você pode aprovar ou

contestar as credenciais apresentadas para o login. Por exemplo, você pode contestar as credenciais solicitando um PIN da conta como verificação adicional.

Você também pode usar o modelo Account Takeover Insights para avaliar logins de contas de forma assíncrona e realizar ações em contas de alto risco. Por exemplo, uma conta de alto risco pode ser adicionada à fila de investigação para que um revisor humano determine se outras medidas precisam ser tomadas, como suspender a conta.

O modelo Account Takeover Insights é treinado usando um conjunto de dados que contém os eventos históricos de login da sua empresa. Você fornece esses dados. Opcionalmente, você pode rotular as contas como legítimas ou fraudulentas. No entanto, isso não é necessário para treinar o modelo. O modelo Account Takeover Insights detecta anomalias com base no histórico de logins bem-sucedidos de uma conta. Ele também aprende a detectar anomalias no comportamento de um usuário que sugerem um risco maior de um evento de invasão maliciosa da conta. Por exemplo, um usuário que normalmente faz login a partir do mesmo conjunto de dispositivos e endereços IP. Um fraudador normalmente faz login usando um dispositivo e uma localização geográfica diferentes. Essa técnica produz uma pontuação de risco de uma atividade ser anômala, o que normalmente é a principal característica das invasões de contas mal-intencionadas.

Antes de treinar um modelo do Account Takeover Insights, o Amazon Fraud Detector usa uma combinação de técnicas de aprendizado de máquina para realizar o enriquecimento, a agregação e a transformação de dados. Então, durante o processo de treinamento, o Amazon Fraud Detector enriquece os elementos de dados brutos que você fornece. Exemplos de elementos de dados brutos incluem endereço IP e agente de usuário. O Amazon Fraud Detector usa esses elementos para criar entradas adicionais que descrevem os dados de login. Essas entradas incluem o dispositivo, o navegador e as entradas de geolocalização. O Amazon Fraud Detector também usa os dados de login que você fornece para calcular continuamente variáveis agregadas que descrevem o comportamento anterior do usuário. Exemplos de comportamento do usuário incluem o número de vezes que o usuário fez login a partir de um endereço IP específico. Usando esses enriquecimentos e agregados adicionais, o Amazon Fraud Detector pode gerar um forte desempenho do modelo a partir de um pequeno conjunto de entradas de seus eventos de login.

O modelo Account Takeover Insights detecta casos em que uma conta legítima é acessada por um agente mal-intencionado, independentemente de o agente mal-intencionado ser humano ou robô. O modelo produz uma pontuação única que indica o risco relativo de comprometimento da conta. As contas que podem ter sido comprometidas são marcadas como contas de alto risco. Você pode processar contas de alto risco de duas maneiras. Você também pode impor uma verificação de identidade adicional. Ou você pode enviar a conta para uma fila para investigação manual.

Seleção da fonte de dados

Os modelos do Account Takeover Insights são treinados em um conjunto de dados armazenado internamente, no Amazon Fraud Detector. Para armazenar seus dados de eventos de login com o Amazon Fraud Detector, crie um arquivo CSV com os eventos de login dos usuários. Para cada evento, inclua dados de login, como data e hora do evento, ID do usuário, endereço IP, agente do usuário e se os dados de login são válidos. Depois de criar o arquivo CSV, primeiro faça o upload do arquivo para o Amazon Fraud Detector e, em seguida, use o recurso de importação para armazenar os dados. Em seguida, você pode treinar seu modelo usando os dados armazenados. Para obter mais informações sobre como armazenar seu conjunto de dados de eventos com o Amazon Fraud Detector, consulte Armazene os dados do seu evento internamente com o Amazon Fraud Detector

Preparar dados

O Amazon Fraud Detector exige que você forneça os dados de login da sua conta de usuário em um arquivo de valores separados por vírgula (CSV) codificado no formato UTF-8. A primeira linha do seu arquivo CSV deve conter um cabeçalho de arquivo. O cabeçalho do arquivo consiste em metadados de eventos e variáveis de eventos que descrevem cada elemento de dados. Os dados do evento seguem o cabeçalho. Cada linha nos dados do evento consiste em dados de um único evento de login.

Para o modelo Accounts Takeover Insights, você deve fornecer os seguintes metadados de eventos e variáveis de eventos na linha de cabeçalho do seu arquivo CSV.

Metadados do evento

Recomendamos que você forneça os seguintes metadados no cabeçalho do arquivo CSV. Os metadados do evento devem estar em letras maiúsculas.

- EVENT_ID - Um identificador exclusivo para o evento de login.
- ENTITY_TYPE - A entidade que realiza o evento de login, como um lojista ou um cliente.
- ENTITY_ID - Um identificador para a entidade que está executando o evento de login.
- EVENT_TIMESTAMP - A data e hora em que o evento de login ocorreu. O carimbo de data/hora deve estar no padrão ISO 8601 em UTC.
- EVENT_LABEL (recomendado) - Um rótulo que classifica o evento como fraudulento ou legítimo. Você pode usar qualquer rótulo, como “fraude”, “legítimo”, “1" ou “0".

> **Note**
>
> - Os metadados do evento devem estar em letras maiúsculas. É sensível a maiúsculas e minúsculas.
> - Os rótulos não são necessários para eventos de login. No entanto, recomendamos que você inclua os metadados EVENT_LABEL e forneça rótulos para seus eventos de login. Tudo bem se os rótulos estiverem incompletos ou esporádicos. Se você fornecer etiquetas, o Amazon Fraud Detector as usará para calcular automaticamente uma taxa de descoberta de aquisição de contas e exibi-la no gráfico e na tabela de desempenho do modelo.

Variáveis do evento

Para o modelo Accounts Takeover Insights, há variáveis obrigatórias (obrigatórias) que você deve fornecer e variáveis opcionais. Ao criar suas variáveis, certifique-se de atribuir a variável ao tipo correto de variável. Como parte do processo de treinamento do modelo, o Amazon Fraud Detector usa o tipo de variável associado à variável para realizar o enriquecimento de variáveis e a engenharia de recursos.

> **Note**
>
> Os nomes das variáveis do evento devem estar em letras minúsculas. Eles diferenciam maiúsculas de minúsculas.

Variáveis obrigatórias

As variáveis a seguir são necessárias para treinar um modelo do Accounts Takeover Insights.

Categoria	Tipo de variável	Descrição
Endereço IP	IP_ADDRESS	O endereço IP usado no evento de login
Navegador e dispositivo	AGENTE DE USUÁRIO	O navegador, o dispositivo e o sistema operacional usados no evento de login

Categoria	Tipo de variável	Descrição
Credenciais válidas	CREDENCIADO VÁLIDO	Indica se as credenciais usadas para login são válidas

Variáveis opcionais

As variáveis a seguir são opcionais para treinar um modelo do Accounts Takeover Insights.

Categoria	Tipo	Descrição
Navegador e dispositivo	IMPRESSÃO DIGITAL	O identificador exclusivo da impressão digital de um navegador ou dispositivo
ID da sessão	SESSION_ID	O identificador de uma sessão de autenticação
Rótulo	RÓTULO_EVENTO	Uma etiqueta que classific a o evento como fraudulen to ou legítimo. Você pode usar qualquer rótulo, como “fraude”, “legítimo”, “1" ou “0".
Timestamp	LABEL_TIMESTAMP	O carimbo de data e hora da última atualização do rótulo. Isso é necessário se EVENT_LABEL for fornecido.

Note

- Você pode fornecer qualquer nome de variável para ambas as variáveis obrigatórias opcionais. É importante que cada variável obrigatória e opcional seja atribuída ao tipo correto de variável.

- Você pode fornecer variáveis adicionais. No entanto, o Amazon Fraud Detector não incluirá essas variáveis para treinar um modelo do Accounts Takeover Insights.

Seleção de dados

A coleta de dados é uma etapa importante para criar seu modelo Account Takeover Insights. Ao começar a coletar seus dados de login, considere os seguintes requisitos e recomendações:

Obrigatório

- Forneça pelo menos 1.500 exemplos de contas de usuário, cada uma com pelo menos dois eventos de login associados.
- Seu conjunto de dados deve abranger pelo menos 30 dias de eventos de login. Posteriormente, você pode especificar o intervalo de tempo específico dos eventos a serem usados para treinar o modelo.

Recomendado

- Seu conjunto de dados inclui exemplos de eventos de login malsucedidos. Opcionalmente, você pode rotular esses logins malsucedidos como “fraudulentos” ou “legítimos”.
- Prepare dados históricos com eventos de login que abrangem mais de seis meses e inclua 100 mil entidades.

Se você não tiver um conjunto de dados que já atenda aos requisitos mínimos, considere transmitir dados de eventos para o Amazon Fraud Detector chamando a operação da SendEventAPI.

Validando dados

Antes de criar seu modelo Account Takeover Insights, o Amazon Fraud Detector verifica se os metadados e variáveis que você incluiu em seu conjunto de dados para treinar o modelo atendem aos requisitos de tamanho e formato. Para obter mais informações, consulte Validação do conjunto de dados. Ele também verifica outros requisitos. Se o conjunto de dados não passar pela validação, o modelo não será criado. Para que o modelo seja criado com sucesso, certifique-se de corrigir os dados que não passaram na validação antes de treinar novamente.

Erros comuns do conjunto de dados

Ao validar um conjunto de dados para treinar um modelo do Account Takeover Insights, o Amazon Fraud Detector verifica esses e outros problemas e gera um erro se encontrar um ou mais dos problemas.

- O arquivo CSV não está no formato UTF-8.
- O cabeçalho do arquivo CSV não contém pelo menos um dos seguintes metadados:`EVENT_ID`,`ENTITY_ID`, ou. `EVENT_TIMESTAMP`
- O cabeçalho do arquivo CSV não contém pelo menos uma variável dos seguintes tipos de variáveis:`IP_ADDRESS`,`USERAGENT`, ou`VALIDCRED`.
- Há mais de uma variável associada ao mesmo tipo de variável.
- Mais de 0,1% dos valores em `EVENT_TIMESTAMP` contêm valores nulos ou valores diferentes dos formatos de data e hora suportados.
- O número de dias entre o primeiro e o último evento é inferior a 30 dias.
- Mais de 10% das variáveis do tipo `IP_ADDRESS` variável são inválidas ou nulas.
- Mais de 50% das variáveis do tipo `USERAGENT` variável contêm nulos.
- Todas as variáveis do tipo de `VALIDCRED` variável são definidas como`false`.

Criar um modelo

Os modelos do Amazon Fraud Detector aprendem a detectar fraudes em um tipo específico de evento. No Amazon Fraud Detector, primeiro você cria um modelo, que funciona como um contêiner para as versões do seu modelo. Cada vez que você treina um modelo, uma nova versão é criada. Para obter detalhes sobre como criar e treinar um modelo usando o AWS console, consulteEtapa 3: criar modelo.

Cada modelo tem uma variável de pontuação do modelo correspondente. O Amazon Fraud Detector cria essa variável em seu nome quando você cria um modelo. Você pode usar essa variável em suas expressões de regras para interpretar as pontuações do modelo durante uma avaliação de fraude.

Treine e implante um modelo usando o AWS SDK for Python (Boto3)

Uma versão do modelo é criada chamando `CreateModel` as `CreateModelVersion` operações e. `CreateModel`inicia o modelo, que atua como um contêiner para as versões do seu modelo. `CreateModelVersion`oninicia o processo de treinamento, que resulta em uma versão específica do modelo. Uma nova versão da solução é criada cada vez que você chama `CreateModelVersion`.

O exemplo a seguir mostra um exemplo de solicitação para a `CreateModel` API. Este exemplo cria o tipo de modelo do Online Fraud Insights e pressupõe que você tenha criado um tipo de `sample_registration` evento. Para obter detalhes adicionais sobre a criação de um tipo de evento, consulteCrie um tipo de evento.

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

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

Treine sua primeira versão usando a CreateModelVersionAPI. Para o `TrainingDataSource` e `ExternalEventsDetail` especifique a origem e a localização do Amazon S3 do conjunto de dados de treinamento. Para isso, `TrainingDataSchema` especifique como o Amazon Fraud Detector deve interpretar os dados de treinamento, especificamente quais variáveis do evento incluir e como classificar os rótulos dos eventos. Por padrão, o Amazon Fraud Detector ignora os eventos não identificados. Esse código de exemplo usa `AUTO` for `unlabeledEventsTreatment` para especificar que o Amazon Fraud Detector decide como usar os eventos não identificados.

```
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'
```

```
}
)
```

Uma solicitação bem-sucedida resultará em uma nova versão do modelo com status`TRAINING_IN_PROGRESS`. A qualquer momento durante o treinamento, você pode cancelar o treinamento ligando `UpdateModelVersionStatus` e atualizando o status para`TRAINING_CANCELLED`. Quando o treinamento for concluído, o status da versão do modelo será atualizado para`TRAINING_COMPLETE`. Você pode analisar o desempenho do modelo usando o console do Amazon Fraud Detector ou ligando`DescribeModelVersions`. Para obter mais informações sobre como interpretar as pontuações e o desempenho do modelo, consulte Pontuações do modelo Métricas de desempenho do modelo e.

Depois de analisar o desempenho do modelo, ative o modelo para disponibilizá-lo para uso pelos Detectores em previsões de fraudes em tempo real. O Amazon Fraud Detector implantará o modelo em várias zonas de disponibilidade para redundância com o auto-scaling ativado para garantir que o modelo seja escalado de acordo com o número de previsões de fraude que você está fazendo. Para ativar o modelo, chame a `UpdateModelVersionStatus` API e atualize o status para`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'
)
```

Pontuações do modelo

O Amazon Fraud Detector gera pontuações de modelos de forma diferente para diferentes tipos de modelo.

Para modelos do Account Takeover Insights (ATI), o Amazon Fraud Detector usa somente o valor agregado (um valor calculado pela combinação de um conjunto de variáveis brutas) para gerar a pontuação do modelo. Uma pontuação de -1 é gerada para o primeiro evento de uma nova entidade, indicando um risco desconhecido. Isso ocorre porque, para uma nova entidade, os valores usados para calcular a agregação serão zero ou nulos. O modelo Account Takeeover Insights (ATI) gera pontuações de modelo entre 0 e 1000 para todos os eventos subsequentes para a mesma entidade

e para entidades existentes, onde 0 indica baixo risco de fraude e 1000 indica alto risco de fraude. Para modelos ATI, as pontuações do modelo estão diretamente relacionadas à taxa de desafio (CR). Por exemplo, uma pontuação de 500 corresponde a uma taxa de desafio estimada de 5%, enquanto uma pontuação de 900 corresponde a uma taxa de desafio estimada de 0,1%.

Para os modelos Online Fraud Insights (OFI) e Transaction Fraud Insights (TFI), o Amazon Fraud Detector usa tanto o valor agregado (um valor calculado pela combinação de um conjunto de variáveis brutas) quanto o valor bruto (o valor fornecido para a variável) para gerar as pontuações do modelo. As pontuações do modelo podem estar entre 0 e 1000, onde 0 indica baixo risco de fraude e 1000 indica alto risco de fraude. Para os modelos OFI e TFI, as pontuações do modelo estão diretamente relacionadas à taxa de falsos positivos (FPR). Por exemplo, uma pontuação de 600 corresponde a uma taxa estimada de 10% de falsos positivos, enquanto uma pontuação de 900 corresponde a uma taxa estimada de 2% de falsos positivos. A tabela a seguir fornece detalhes de como determinadas pontuações do modelo se correlacionam com as taxas estimadas de falsos positivos.

Pontuação do modelo	FPR estimado
975	0,50%
950	1%
900	2%
860	3%
775	5%
700	7%
600	10%

Métricas de desempenho do modelo

Após a conclusão do treinamento do modelo, o Amazon Fraud Detector valida o desempenho do modelo usando 15% dos seus dados que não foram usados para treinar o modelo. Você pode esperar que seu modelo treinado do Amazon Fraud Detector tenha um desempenho real de detecção de fraudes semelhante às métricas de desempenho de validação.

Como empresa, você deve equilibrar entre detectar mais fraudes e adicionar mais atrito aos clientes legítimos. Para ajudar na escolha do equilíbrio certo, o Amazon Fraud Detector fornece as seguintes ferramentas para avaliar o desempenho do modelo:

- Gráfico de distribuição de pontuação — Um histograma das distribuições de pontuação do modelo pressupõe um exemplo de população de 100.000 eventos. O eixo Y esquerdo representa os eventos legítimos e o eixo Y direito representa os eventos de fraude. Você pode selecionar um limite de modelo específico clicando na área do gráfico. Isso atualizará as visualizações correspondentes na matriz de confusão e no gráfico ROC.
- Matriz de confusão — resume a precisão do modelo para um determinado limite de pontuação comparando as previsões do modelo com os resultados reais. O Amazon Fraud Detector pressupõe um exemplo de população de 100.000 eventos. A distribuição de fraudes e eventos legítimos simula a taxa de fraude em seus negócios.
  - Verdadeiros pontos positivos — O modelo prevê fraudes e o evento é, na verdade, uma fraude.
  - Falsos positivos — O modelo prevê fraudes, mas o evento é realmente legítimo.
  - Verdadeiros negativos — O modelo prevê que é legítimo e o evento é realmente legítimo.
  - Falsos negativos — O modelo prevê que seja legítimo, mas o evento é na verdade uma fraude.
  - Taxa positiva verdadeira (TPR) — Porcentagem do total de fraudes detectadas pelo modelo. Também conhecida como taxa de captura.
  - Taxa de falsos positivos (FPR) — Porcentagem do total de eventos legítimos previstos incorretamente como fraude.
- Curva do operador do receptor (ROC) — traça a taxa de verdadeiros positivos em função da taxa de falsos positivos em todos os limites possíveis de pontuação do modelo. Veja esse gráfico escolhendo Métricas avançadas.
- Área sob a curva (AUC) — Resume o TPR e o FPR em todos os limites possíveis de pontuação do modelo. Um modelo sem poder preditivo tem uma AUC de 0,5, enquanto um modelo perfeito tem uma pontuação de 1,0.
- Faixa de incerteza — Mostra a faixa de AUC esperada do modelo. Uma faixa maior (diferença no limite superior e inferior da AUC > 0,1) significa maior incerteza do modelo. Se a faixa de incerteza for grande (>0,1), considere fornecer mais eventos rotulados e retreinar o modelo.

Para usar as métricas de desempenho do modelo

1. Comece com o gráfico de distribuição de pontuação para analisar a distribuição das pontuações do modelo para suas fraudes e eventos legítimos. Idealmente, você terá uma separação clara

entre a fraude e os eventos legítimos. Isso indica que o modelo pode identificar com precisão quais eventos são fraudulentos e quais são legítimos. Selecione um limite de modelo clicando na área do gráfico. Você pode ver como o ajuste do limite de pontuação do modelo afeta suas taxas de verdadeiros positivos e falsos positivos.

> **Note**
>
> O gráfico de distribuição de pontuação traça a fraude e os eventos legítimos em dois eixos Y diferentes. O eixo Y esquerdo representa os eventos legítimos e o eixo Y direito representa os eventos de fraude.

2. Revise a matriz de confusão. Dependendo do limite de pontuação do modelo selecionado, você pode ver o impacto simulado com base em uma amostra de 100.000 eventos. A distribuição de fraudes e eventos legítimos simula a taxa de fraude em seus negócios. Use essas informações para encontrar o equilíbrio certo entre a taxa de verdadeiros positivos e a taxa de falsos positivos.
3. Para obter detalhes adicionais, escolha Métricas avançadas. Use a carta ROC para entender a relação entre a taxa de verdadeiros positivos e a taxa de falsos positivos para qualquer limite de pontuação do modelo. A curva ROC pode ajudá-lo a ajustar a compensação entre a taxa de verdadeiros positivos e a taxa de falsos positivos.

> **Note**
>
> Você também pode revisar as métricas em forma de tabela escolhendo Tabela.
> A exibição da tabela também mostra a precisão métrica. Precisão é a porcentagem de eventos de fraude previstos corretamente como fraudulentos em comparação com todos os eventos previstos como fraudulentos.

4. Use as métricas de desempenho para determinar os limites ideais do modelo para seus negócios com base em suas metas e no caso de uso de detecção de fraudes. Por exemplo, se você planeja usar o modelo para classificar novos registros de contas como de alto, médio ou baixo risco, precisará identificar duas pontuações de limite para poder elaborar três condições de regra da seguinte forma:

   - Pontuações > X são de alto risco
   - Os escores < X but > Y são de risco médio
   - Pontuações < Y são de baixo risco

Importância da variável do modelo

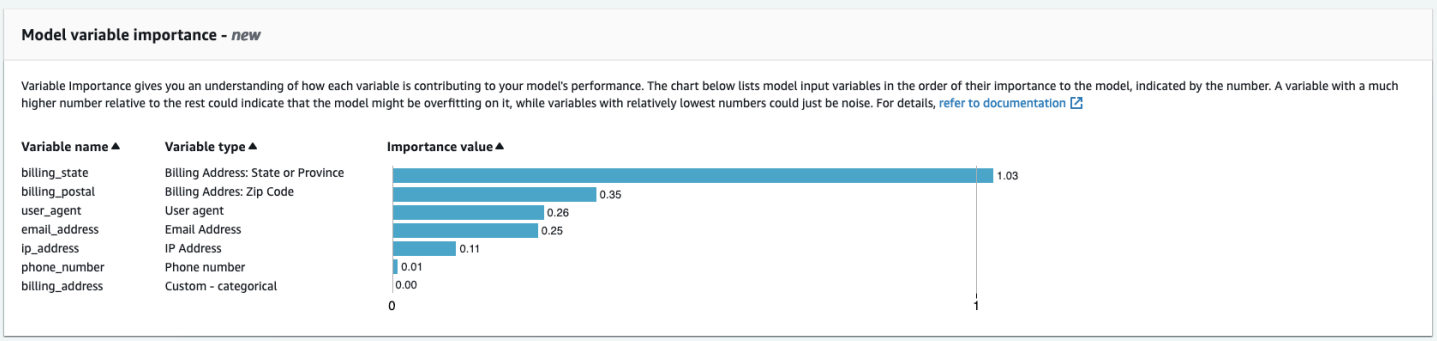
A importância da variável do modelo é um recurso do Amazon Fraud Detector que classifica as variáveis do modelo em uma versão do modelo. Cada variável do modelo recebe um valor com base em sua importância relativa para o desempenho geral do seu modelo. A variável do modelo com o valor mais alto é mais importante para o modelo do que as outras variáveis do modelo no conjunto de dados dessa versão do modelo e está listada na parte superior por padrão. Da mesma forma, a variável do modelo com o menor valor é listada na parte inferior por padrão e é menos importante em comparação com as outras variáveis do modelo. Usando os valores de importância das variáveis do modelo, você pode obter informações sobre quais entradas estão impulsionando o desempenho do seu modelo.

Você pode visualizar os valores de importância das variáveis do modelo para sua versão treinada no console do Amazon Fraud Detector ou usando a DescribeModelVersionAPI.

A importância da variável do modelo fornece o seguinte conjunto de valores para cada variável usada para treinar a versão do modelo.

- Tipo de variável: Tipo de variável (por exemplo, endereço IP ou e-mail). Para obter mais informações, consulte Tipos de variáveis. Para os modelos Account Takeover Insights (ATI), o Amazon Fraud Detector fornece um valor de importância variável para o tipo de variável bruta e agregada. Os tipos de variáveis brutas são atribuídos às variáveis que você fornece. O tipo de variável agregada é atribuído a um conjunto de variáveis brutas que o Amazon Fraud Detector combinou para calcular um valor de importância agregada.
- Nome da variável: Nome da variável de evento usada para treinar a versão do modelo (por exemplo,`ip_address`,`email_address`,`are_creadentials_valid`). Para o tipo de variável agregada, os nomes de todas as variáveis que foram usadas para calcular o valor de importância da variável agregada são listados.
- Valor de importância da variável: um número que representa a importância relativa da variável bruta ou agregada para o desempenho do modelo. Intervalo típico: 0—10

No console do Amazon Fraud Detector, os valores de importância das variáveis do modelo são exibidos da seguinte forma para um modelo Online Fraud Insights (OFI) ou Transaction Fraud Insights (TFI). Um modelo Account Takeover Insight (ATI) fornecerá valores agregados de importância variável, além dos valores de importância da variável bruta. O gráfico visual facilita a visualização da importância relativa entre as variáveis, com a linha pontilhada vertical fornecendo referência ao valor de importância da variável mais bem classificada.



O Amazon Fraud Detector gera valores de importância variáveis para cada versão do modelo do Fraud Detector sem custo adicional.

> **Important**
>
> As versões do modelo criadas antes de 9 de julho de 2021 não têm valores de importância variáveis. Você deve treinar uma nova versão do seu modelo para gerar os valores de importância das variáveis do modelo.

Usando valores de importância da variável do modelo

Você pode usar os valores de importância das variáveis do modelo para obter informações sobre o que está aumentando ou diminuindo o desempenho do seu modelo e quais variáveis contribuem mais. Em seguida, ajuste seu modelo para melhorar o desempenho geral.

Mais especificamente, para melhorar o desempenho do modelo, examine os valores de importância das variáveis em relação ao seu conhecimento de domínio e depure os problemas nos dados de treinamento. Por exemplo, se o ID da conta foi usado como entrada para o modelo e está listado na parte superior, dê uma olhada no valor de importância variável. Se o valor de importância da variável for significativamente maior do que o restante dos valores, seu modelo pode estar se ajustando demais a um padrão de fraude específico (por exemplo, todos os eventos de fraude são do mesmo ID de conta). No entanto, também pode ocorrer um vazamento de etiquetas se a variável depender das etiquetas fraudulentas. Dependendo do resultado da análise com base no conhecimento do seu domínio, talvez você queira remover a variável e treinar com um conjunto de dados mais diversificado ou manter o modelo como está.

Da mesma forma, dê uma olhada nas variáveis classificadas por último. Se o valor de importância da variável for significativamente menor do que o restante dos valores, essa variável do modelo

pode não ter nenhuma importância no treinamento do seu modelo. Você pode considerar remover a variável para treinar uma versão mais simples do modelo. Se seu modelo tiver poucas variáveis, como apenas duas variáveis, o Amazon Fraud Detector ainda fornecerá os valores de importância das variáveis e classificará as variáveis. No entanto, os insights nesse caso serão limitados.

⚠ Important

1. Se você notar que faltam variáveis no gráfico de importância das variáveis do modelo, isso pode ser devido a um dos seguintes motivos. Considere modificar a variável em seu conjunto de dados e retreinar seu modelo.
   - A contagem de valores exclusivos para a variável no conjunto de dados de treinamento é menor que 100.
   - Mais de 0,9 dos valores da variável estão ausentes no conjunto de dados de treinamento.
2. Você precisa treinar uma nova versão do modelo sempre que quiser ajustar as variáveis de entrada do seu modelo.

Avaliação dos valores de importância das variáveis do modelo

Recomendamos que você considere o seguinte ao avaliar os valores de importância das variáveis do modelo:

- Os valores de importância das variáveis devem sempre ser avaliados em combinação com o conhecimento do domínio.
- Examine o valor de importância variável de uma variável em relação ao valor de importância variável das outras variáveis na versão do modelo. Não considere o valor de importância da variável para uma única variável de forma independente.
- Compare os valores de importância das variáveis na mesma versão do modelo. Não compare os valores de importância variável das mesmas variáveis nas versões do modelo porque o valor da importância variável de uma variável em uma versão do modelo pode ser diferente do valor da mesma variável em uma versão diferente do modelo. Se você usar as mesmas variáveis e o mesmo conjunto de dados para treinar diferentes versões do modelo, isso não gerará necessariamente os mesmos valores de importância da variável.

Visualizando a classificação de importância das variáveis do modelo

Depois que o treinamento do modelo for concluído, você poderá visualizar a classificação de importância variável do modelo da sua versão treinada no console do Amazon Fraud Detector ou usando a DescribeModelVersionAPI.

Para visualizar a classificação de importância da variável do modelo usando o console,

1. Abra o AWS console e faça login na sua conta. Navegue até o Amazon Fraud Detector.
2. No painel de navegação à esquerda, selecione Modelos.
3. Escolha seu modelo e depois a versão do modelo.
4. Certifique-se de que a guia Visão geral esteja selecionada.
5. Role para baixo para ver o painel Importância da variável do modelo.

Entendendo como o valor de importância da variável do modelo é calculado

Após a conclusão do treinamento de cada versão do modelo, o Amazon Fraud Detector gera automaticamente os valores de importância das variáveis do modelo e as métricas de desempenho do modelo. Para isso, o Amazon Fraud Detector usa o SHaPley Additive Explanations (SHAP). O SHAP é essencialmente a contribuição média esperada de uma variável do modelo após todas as combinações possíveis de todas as variáveis do modelo terem sido consideradas.

O SHAP primeiro atribui a contribuição de cada variável do modelo para a previsão de um evento. Em seguida, ele agrega essas previsões para criar uma classificação das variáveis no nível do modelo. Para atribuir contribuições de cada variável do modelo para uma previsão, o SHAP considera as diferenças nas saídas do modelo entre todas as combinações possíveis de variáveis. Ao incluir todas as possibilidades de incluir ou remover um conjunto específico de variáveis para gerar uma saída de modelo, o SHAP pode acessar com precisão a importância de cada variável do modelo. Isso é particularmente importante quando as variáveis do modelo estão altamente correlacionadas entre si.

Os modelos de ML, na maioria dos casos, não permitem que você remova variáveis. Em vez disso, você pode substituir uma variável removida ou ausente no modelo pelos valores correspondentes de uma ou mais linhas de base (por exemplo, eventos não fraudulentos). Escolher instâncias básicas adequadas pode ser difícil, mas o Amazon Fraud Detector facilita isso definindo essa linha de base como a média da população para você.

Importar um SageMaker modelo

Opcionalmente, você pode importar modelos SageMaker hospedados para o Amazon Fraud Detector. Assim como os modelos, SageMaker os modelos podem ser adicionados aos detectores e gerar previsões de fraudes usando a `GetEventPrediction` API. Como parte da `GetEventPrediction` solicitação, o Amazon Fraud Detector invocará seu SageMaker endpoint e transmitirá os resultados às suas regras.

Você pode configurar o Amazon Fraud Detector para usar as variáveis de evento enviadas como parte da `GetEventPrediction` solicitação. Se você optar por usar variáveis de evento, deverá fornecer um modelo de entrada. O Amazon Fraud Detector usará esse modelo para transformar suas variáveis de evento na carga de entrada necessária para invocar o SageMaker endpoint. Como alternativa, você pode configurar seu SageMaker modelo para usar um ByteBuffer enviado como parte da solicitação. `GetEventPrediction`

O Amazon Fraud Detector suporta SageMaker algoritmos de importação que usam formatos de entrada JSON ou CSV e formatos de saída JSON ou CSV. Exemplos de SageMaker algoritmos compatíveis incluem XGBoost, Linear Learner e Random Cut Forest.

Importe um SageMaker modelo usando o AWS SDK for Python (Boto3)

Para importar um SageMaker modelo, use a `PutExternalModel` API. O exemplo a seguir pressupõe que o SageMaker endpoint `sagemaker-transaction-model` foi implantado, está em `InService` status e usa o algoritmo XGBoost.

A configuração de entrada especifica que usará as variáveis de evento para construir a entrada do modelo (`useEventVariables`está definida como`TRUE`). O formato de entrada é TEXT_CSV, já que o XGBoost requer uma entrada CSV. csvInputTemplate Especifica como construir a entrada CSV a partir das variáveis enviadas como parte da `GetEventPrediction` solicitação. Este exemplo pressupõe que você tenha criado as variáveis `order_amt`prev_amt, `hist_amt` e. `payment_type`

A configuração de saída especifica o formato de resposta do SageMaker modelo e mapeia o índice CSV apropriado para a variável Amazon Fraud Detector. `sagemaker_output_score` Depois de configurada, você pode usar a variável de saída nas regras.

> **Note**
>
> A saída de um SageMaker modelo deve ser mapeada para uma variável com origem`EXTERNAL_MODEL_SCORE`. Você não pode criar essas variáveis no console usando Variáveis. Em vez disso, você deve criá-los ao configurar a importação do modelo.

```
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'
)
```

Excluir um modelo ou versão de modelo

Você pode excluir modelos e versões de modelos no Amazon Fraud Detector, desde que não estejam associados a uma versão do detector. Quando você exclui um modelo, o Amazon Fraud Detector exclui permanentemente esse modelo e os dados não são mais armazenados no Amazon Fraud Detector.

Você também pode remover SageMaker modelos da Amazon se eles não estiverem associados a uma versão do detector. A remoção de um SageMaker modelo o desconecta do Amazon Fraud Detector, mas o modelo permanece disponível em SageMaker.

Para excluir uma versão do modelo

Você só pode excluir versões do modelo que estão no`Ready to deploy` status. Para alterar uma versão do modelo de`ACTIVE` para`Ready to deploy` status, desimplante a versão do modelo.

1. Faça login noAWS Management Console e abra o console do Amazon Fraud Detector em https://console.aws.amazon.com/frauddetector.
2. No painel de navegação à esquerda do console do Amazon Fraud Detector, selecione Modelos.
3. Escolha o modelo que contém a versão do modelo que você deseja excluir.
4. Escolha a versão do modelo que você deseja excluir.
5. Escolha Actions (Ações) e, em seguida, escolha Delete (Excluir).
6. Insira o nome da versão do modelo e escolha Excluir versão do modelo.

Para desimplantar uma versão do modelo

Você não pode desimplantar uma versão do modelo que esteja sendo usada por qualquer versão do detector (`ACTIVE`,`INACTIVE`,`DRAFT`). Portanto, para desimplantar uma versão do modelo que está sendo usada por uma versão do detector, primeiro remova a versão do modelo da versão do detector.

1. No painel de navegação à esquerda do console do Amazon Fraud Detector, selecione Modelos.
2. Escolha o modelo que contém a versão do modelo que você deseja desimplantar.
3. Escolha a versão do modelo que você deseja excluir.
4. Escolha Ações e, em seguida, escolha Desimplantar versão do modelo.

Para excluir um modelo

Antes de excluir um modelo, você deve excluir todas as versões do modelo e estão associadas a ele.

1. No painel de navegação à esquerda do console do Amazon Fraud Detector, selecione Modelos.
2. Escolha o modelo que você deseja excluir.
3. Escolha Actions (Ações) e, em seguida, escolha Delete (Excluir).

4. Insira o nome do modelo e escolha Excluir modelo.

Para remover um SageMaker modelo da Amazon

1. No painel de navegação à esquerda do console do Amazon Fraud Detector, selecione Modelos.
2. Escolha o SageMaker modelo que você deseja remover.
3. Escolha Ações e escolha Remover modelo.
4. Insira o nome do modelo e escolha Remover SageMaker modelo.

Detector

Um detector é um contêiner que contém a lógica de detecção de fraudes, como modelos e regras, para um evento comercial específico que você deseja avaliar se há fraude. Primeiro, você cria um detector especificando o evento que você já definiu e, opcionalmente, adiciona uma versão do modelo que já foi criada e treinada pelo Amazon Fraud Detector para o evento.

Em seguida, você adiciona regras e ordem de execução de regras a um detector para criar uma versão do detector. Uma versão de detector define as regras e, opcionalmente, um modelo que será executado como parte da solicitação para gerar previsões de fraude. Você pode adicionar qualquer uma das regras definidas em um detector à versão do detector. Você também pode adicionar qualquer modelo treinado no tipo de evento avaliado à versão do detector. Um detector pode ter várias versões, com cada versão tendo regras e ordens de execução de regras diferentes para atender a vários casos de uso.

Cada versão do detector deve ter um status de`DRAFT`,`ACTIVE`, ou`INACTIVE`. Somente uma versão do detector pode estar em`ACTIVE`status por vez. O Amazon Fraud Detector usa a versão do detector com`ACTIVE`status para gerar previsões de fraude.

Crie um detector

Você cria um detector especificando o tipo de evento que você já definiu. Opcionalmente, você pode adicionar um modelo que já foi treinado e implantado pelo Amazon Fraud Detector. Se você adicionar um modelo, poderá usar a pontuação do modelo gerada pelo Amazon Fraud Detector em sua expressão de regra ao criar uma regra (por exemplo,`$model score < 90`).

Você pode criar um detector no console do Amazon Fraud Detector, usando oPutDetectorAPI, usando odetector put-detectorcomando, ou usando oAWSSDK. Se você estiver usando API, comando ou SDK para criar um detector, depois de criar o detector, siga as instruções paraCrie uma versão do detector.

Crie um detector no console do Amazon Fraud Detector

Este exemplo pressupõe que você criou um tipo de evento e também criou e implantou uma versão do modelo que deseja usar para previsão de fraudes.

Etapa 1: Construir detector

1. No painel de navegação esquerdo do console do Amazon Fraud Detector, escolhaDetectores.

2. EscolhaCrie um detector.
3. NoDefina os detalhes do detectorpágina, insira`sample_detector`para o nome do detector. Opcionalmente, insira uma descrição para o detector, como`my sample fraud detector`.
4. ParaTipo de evento, selecione o tipo de evento que você criou para previsão de fraudes.
5. Escolha Next (próximo).

Etapa 2: Adicionar uma versão do modelo implantado

1. Observe que essa é uma etapa opcional. Você não precisa adicionar um modelo ao seu detector. Para pular esta etapa, escolha, escolha Next (Próximo).
2. NoAdicionar modelo - opcional, escolhaAdicionar modelo.
3. NoAdicionar modelopágina, paraSelecione o modelo, escolha o nome do modelo do Amazon Fraud Detector que você implantou anteriormente. ParaSelecione a versão, escolha a versão do modelo implantado.
4. Escolha Add model (Adicionar modelo).
5. Escolha Next (próximo).

Etapa 3: adicionar regras

Uma regra é uma condição que informa ao Amazon Fraud Detector como interpretar valores variáveis ao avaliar a previsão de fraudes. Este exemplo criará três regras usando as pontuações do modelo como valores variáveis:`high_fraud_risk`,`medium_fraud_risk`, `elow_fraud_risk`. Para criar suas próprias regras, expressões de regras, ordem de execução de regras e resultados, use valores que sejam apropriados para seu modelo e seu caso de uso.

1. NoAdicionar regraspágina, abaixoDefinir uma regra, insira`high_fraud_risk`para o nome e abaixo da regraDescrição - opcional, insira**`This rule captures events with a high ML model score`**como descrição da regra.
2. EmExpressão, insira a seguinte expressão de regra usando a linguagem simplificada de expressão de regras do Amazon Fraud Detector:

   ```
   $sample_fraud_detection_model_insightscore > 900
   ```

3. EmResultados, escolhaCrie um novo resultado. Um resultado é o resultado de uma previsão de fraude e é retornado se a regra coincidir durante uma avaliação.

4. EmCrie um novo resultado, insira`verify_customer`como nome do resultado. Opcionalmente, insira uma descrição.
5. EscolhaSalvar resultado.
6. EscolhaAdicionar regrapara executar o verificador de validação de regras e salvar a regra. Depois de criado, o Amazon Fraud Detector disponibiliza a regra para uso em seu detector.
7. EscolhaAdicionar outra regrae, em seguida, escolha oCriar regraaba.
8. Repita esse processo mais duas vezes para criar seu`medium_fraud_risk`e`low_fraud_risk`regras usando os seguintes detalhes da regra:

   - risco_fraude_médio

     Nome da regra:`medium_fraud_risk`

     Resultado:`review`

     Expressão:

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

     ```
     $sample_fraud_detection_model_insightscore > 700
     ```

   - baixo risco de fraude

     Nome da regra:`low_fraud_risk`

     Resultado:`approve`

     Expressão:

     ```
     $sample_fraud_detection_model_insightscore <= 700
     ```

9. Depois de criar todas as regras para seu caso de uso, escolhaPróximo.

   Para obter mais informações sobre como criar e escrever regras, consulteRegraseReferência do idioma da regra.

Etapa 4: Configurar a execução e a ordem das regras

O modo de execução das regras incluídas no detector determina se todas as regras definidas são avaliadas ou se a avaliação da regra é interrompida na primeira regra correspondente. E a ordem da regra determina a ordem em que você deseja que a regra seja executada.

O modo de execução de regras padrão éFIRST_MATCHED.

Combinado pela primeira vez

O primeiro modo de execução de regra correspondente retorna os resultados da primeira regra de correspondência com base na ordem de regra definida. Se você especificar FIRST_MATCHED, o Amazon Fraud Detector avaliará as regras sequencialmente, da primeiro à última, parando na primeira regra correspondente. Em seguida, o Amazon Fraud Detector fornece os resultados dessa única regra.

A ordem em que você executa as regras pode afetar o resultado resultante da previsão de fraude. Depois de criar suas regras, reordene as regras para executá-las na ordem desejada seguindo estas etapas:

Se o seuhigh_fraud_riska regra ainda não está no topo da sua lista de regras, escolhaPedire, em seguida, escolha1. Isso se movehigh_fraud_riskpara a primeira posição.

Repita esse processo para que seumedium_fraud_riska regra está na segunda posição e sualow_fraud_riska regra está na terceira posição.

Tudo combinado

Todos os modos de execução de regras correspondentes retornam resultados para todas as regras correspondentes, independentemente da ordem das regras. Se você especificarALL_MATCHED, o Amazon Fraud Detector avalia todas as regras e retorna os resultados de todas as regras correspondentes.

SelecionarFIRST_MATCHEDpara este tutorial e, em seguida, escolhaPróximo.

Etapa 5: revisar e criar a versão do detector

Uma versão de detector define os modelos e regras específicos que são usados para gerar previsões de fraude.

1. NoRevise e criepágina, revise os detalhes, modelos e regras do detector que você configurou. Se você precisar fazer alguma alteração, escolhaEditarao lado da seção correspondente.
2. EscolhaCrie um detector. Depois de criada, a primeira versão do seu detector aparece na tabela Versões do detector comDraftstatus.

   Você usa oEsboçoversão para testar seu detector.

Crie um detector usando oAWS SDK for Python (Boto3)

O exemplo a seguir mostra um exemplo de solicitação para o`PutDetector`API. Um detector atua como um contêiner para suas versões do detector. O`PutDetector`A API especifica qual tipo de evento o detector avaliará. O exemplo a seguir pressupõe que você tenha criado um tipo de evento.`sample_registration`.

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

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

Crie uma versão do detector

Uma versão do detector define as regras, a ordem de execução da regra e, opcionalmente, uma versão do modelo, que será usada como parte da solicitação para gerar previsões de fraude. Você pode adicionar qualquer uma das regras definidas em um detector à versão do detector. Você também pode adicionar qualquer modelo treinado no tipo de evento avaliado.

Cada versão do detector tem um status de`DRAFT`,`ACTIVE`, ou`INACTIVE`. Somente uma versão do detector pode estar em`ACTIVE`status por vez. Durante o`GetEventPrediction`solicitação, o Amazon Fraud Detector usará o`ACTIVE`detector se não`DetectorVersion`é especificado.

Modo de execução de regras

O Amazon Fraud Detector oferece suporte a dois modos diferentes de execução de regras:`FIRST_MATCHED`e`ALL_MATCHED`.

- Se o modo de execução da regra for`FIRST_MATCHED`, o Amazon Fraud Detector avalia as regras sequencialmente, do primeiro ao último, parando na primeira regra correspondente. Em seguida, o Amazon Fraud Detector fornece os resultados dessa única regra. Se uma regra for avaliada como falsa (sem correspondência), a próxima regra na lista será avaliada.
- Se o modo de execução da regra for`ALL_MATCHED`, então todas as regras em uma avaliação são executadas em paralelo, independentemente de sua ordem. O Amazon Fraud Detector executa todas as regras e retorna os resultados definidos para cada regra correspondente.

Crie uma versão do detector usando oAWS SDK for Python (Boto3)

O exemplo a seguir mostra um exemplo de solicitação para o`CreateDetectorVersion`API. O modo de execução da regra está definido como`FIRST_MATCHED`, portanto, o Amazon Fraud Detector avaliará as regras sequencialmente, do primeiro ao último, parando na primeira regra correspondente. Em seguida, o Amazon Fraud Detector fornece os resultados dessa única regra durante o`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'
)
```

Para atualizar o status de uma versão do detector, use o`UpdateDetectorVersionStatus`API. O exemplo a seguir atualiza o status da versão do detector de`DRAFT`para`ACTIVE`. Durante um`GetEventPrediction`solicitação, se um ID de detector não for especificado, o Amazon Fraud Detector usará o`ACTIVE`versão do detector.

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

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

Excluir um detector, versão do detector ou versão da regra

Antes de excluir um detector no Amazon Fraud Detector, você deve primeiro excluir todas as versões do detector e versões de regras associadas ao detector.

Quando você exclui um detector, uma versão do detector ou uma versão de regra, o Amazon Fraud Detector exclui permanentemente esse recurso e os dados não são mais armazenados no Amazon Fraud Detector.

Para excluir uma versão do detector

Você pode excluir versões do detector que estão em`DRAFT` nosso`INACTIVE` status.

1. Faça login no AWS Management Console e abra o console do Amazon Fraud Detector em https://console.aws.amazon.com/frauddetector.
2. No painel de navegação à esquerda do console do Amazon Fraud Detector, selecione Detectors.
3. Escolha o detector que contém a versão do detector que você deseja excluir.
4. Escolha a versão do detector que você deseja excluir.
5. Escolha Actions (Ações) e, em seguida, escolha Delete (Excluir).
6. Digite e**`delete`**, em seguida, escolha Excluir detector.

Para excluir uma versão de regras

Você pode excluir uma versão de regra somente se ela não for usada por nenhuma versão do`ACTIVE`ou`INACTIVE` detector. Se necessário, antes de excluir uma versão de regra, primeiro mova a versão do`ACTIVE` detector para e, em seguida`INACTIVE`, exclua a versão do`INACTIVE` detector.

1. No painel de navegação à esquerda do console do Amazon Fraud Detector, selecione Detectors.
2. Escolha o detector que contém a versão da regra que você deseja excluir.
3. Escolha a guia Regras associadas e escolha a regra que você deseja excluir.
4. Escolha a versão da regra que você deseja excluir.
5. Escolha Ações e, em seguida, escolha Excluir versão da regra.
6. Digite e**`delete`**, em seguida, escolha Excluir versão.

Para excluir um detector

Antes de excluir um detector, você deve primeiro excluir todas as versões do detector e versões de regras associadas ao detector.

1. No painel de navegação à esquerda do console do Amazon Fraud Detector, selecione Detectors.
2. Escolha o detector que você deseja excluir.
3. Escolha Ações e, em seguida, escolha Excluir detector.
4. Digite e**`delete`**, em seguida, escolha Excluir detector.

Recursos

Modelos, regras e detectores usam recursos como variáveis, resultados, rótulos, listas e entidades para avaliar eventos quanto ao risco de fraude. Esta seção fornece informações sobre como e informações sobre como criar e gerenciar recursos.

Tópicos

Variáveis

As variáveis representam elementos de dados que você deseja usar em uma previsão de fraude. Essas variáveis podem ser obtidas do conjunto de dados do evento que você preparou para treinar seu modelo, dos resultados da pontuação de risco do seu modelo do Amazon Fraud Detector ou dos modelos da Amazon. SageMaker Para obter mais informações sobre variáveis retiradas do conjunto de dados do evento, consulteObtenha os requisitos do conjunto de dados de eventos usando o Data Models Explorer.

As variáveis que você deseja usar em sua previsão de fraude devem primeiro ser criadas e depois adicionadas ao evento ao criar seu tipo de evento. Cada variável criada deve receber um tipo de dados, um valor padrão e, opcionalmente, um tipo de variável. O Amazon Fraud Detector enriquece algumas das variáveis que você fornece, como endereços IP, números de identificação bancária (BINs) e números de telefone, para criar entradas adicionais e aumentar o desempenho dos modelos que usam essas variáveis.

Tipos de dados

As variáveis devem ter um tipo de dados para o elemento de dados que a variável representa e, opcionalmente, podem ser atribuídos a um dos predefinidosTipos de variáveis. Para variáveis

atribuídas a um tipo de variável, o tipo de dados é pré-selecionado. Os tipos de dados possíveis incluem os seguintes tipos:

Tipo de dados	Descrição	Valor padrão	Exemplos de valores
String	Qualquer combinação de letras, números inteiros ou ambos	<empty>	abc, 123, 13DB
Inteiro	Números inteiros positivos ou negativos	0	1, -1
Booliano	Verdadeiro ou falso	Falso	Verdadeiro, falso
DateTime	Data e hora especificadas somente no formato UTC padrão ISO 8601	<empty>	30/11/2019 ÀS 13:01:01 Z
Float	Números com pontos decimais	0.0	4,01, 0,10

Valor padrão

As variáveis devem ter um valor padrão. Quando o Amazon Fraud Detector gera previsões de fraude, esse valor padrão é usado para executar uma regra ou modelo se o Amazon Fraud Detector não receber um valor para uma variável. Os valores padrão fornecidos devem corresponder ao tipo de dados selecionado. No console da AWS, o Amazon Fraud Detector atribui o valor padrão de `0` para números inteiros, para booleanos, `false` para flutuadores e (vazio) `0.0` para cadeias de caracteres. Você pode definir um valor padrão personalizado para qualquer um desses tipos de dados.

Tipos de variáveis

Ao criar uma variável, você pode, opcionalmente, atribuir a variável a um tipo de variável. O tipo de variável representa os elementos de dados comuns usados para treinar modelos e gerar previsões de fraude. Somente variáveis com um tipo de variável associado podem ser usadas para o treinamento do modelo. Como parte do processo de treinamento do modelo, o Amazon

Fraud Detector usa o tipo de variável associado à variável para realizar enriquecimentos variáveis, engenharia de recursos e pontuação de risco.

O Amazon Fraud Detector predefiniu os seguintes tipos de variáveis que podem ser usados para atribuir às suas variáveis.

Ca	Tipo de variável	Descrição	Tipo de dado	Ex
Sessão	IP_ADDRESS	O endereço IP que é coletado durante o evento	Strin	192.0.2.0 Nota: O Amazon Fraud Detector enriquece esses dados. Para ter mais informações, consulte Enriquecimento da geolocalização.
	AGENTE DE USUÁRIO	O agente de usuário que é coletado durante o evento	Strin	Mozilla 5.0 (Windows NT 10.0, Win64,

Ca	Tipo de variável	Descrição	Tipo de dado	Ex
				x64, rv: 68.0) Gecko 20100101
	IMPRESSÃ DIGITAL	O identificador exclusivo de um dispositivo usado para o evento	Strin	sadfow987 u234
	SESSION_I D	O ID da sessão ativa do evento	Strin	sid123456 789
	SÃO_CRED NTIALS_VÁ LIDAS	Indica se as credenciais usadas para o login do evento são válidas	Bool	Ver dadeir o
Us	ENDEREÇO DE E-MAIL	O endereço de e-mail coletado durante o evento	Strin	abc@domai n.com

Ca	Tipo de variável	Descrição	Tipo de dado	Ex
	PHONE_NUMBER	O número de telefone coletado durante o evento	Strin	+1 555-0100 Nota: O Amazon Fraud Detector enriquece esses dados. Para ter mais informações, consulte Enriquecimento do número de telefone.
Fato	NOME_DO_ATURAMENTO	O nome associado ao endereço de cobrança	Strin	John Doe

Ca	Tipo de variável	Descrição	Tipo de dado	Ex
	TELEFONE DE COBRANÇA	O número de telefone associado ao endereço de cobrança	Strin	+1 555-0100 Nota: O Amazon Fraud Detector enriquece esses dados. Para ter mais informações, consulte Enriquecimento do número de telefone.
	ENDEREÇO DE_FATURAMENTO_L1	A primeira linha do endereço de cobrança	Strin	Qualquer rua
	ENDEREÇO DE_FATURAMENTO_L2	A segunda linha do endereço de cobrança	Strin	Qualquer unidade 123

Ca	Tipo de variável	Descrição	Tipo de dado	Ex
	CIDADE DE COBRANÇA	A cidade que está no endereço de cobrança	Strin	Qualquer cidade
	ESTADO DE COBRANÇA	O estado ou província que está no endereço de cobrança	Strin	Qualquer estado ou província
	PAÍS_DE_FATURAMENTO	O país que está no endereço de cobrança	Strin	Qualquer país Nota: O Amazon Fraud Detector enriquece esses dados. Para ter mais informações, consulte Enriquecimento da geolocalização.

Ca	Tipo de variável	Descrição	Tipo de dado	Ex
	COBRANÇA ZIP	O código postal que está no endereço de cobrança	Strin	01234 Nota: O Amazon Fraud Detector enriquece esses dados. Para ter mais informações, consulte Enriquecimento da geolocalização.
Re	NOME_DE_ NVIO	O nome associado ao endereço de entrega	Strin	John Doe

Ca	Tipo de variável	Descrição	Tipo de dado	Ex
	TELEFONE_DE_ENVIO	O número de telefone associado ao endereço de entrega	Strin	+1 555-0100 Nota: O Amazon Fraud Detector enriquece esses dados. Para ter mais informações, consulte Enriquecimento do número de telefone.
	ENDEREÇO_DE_FRETE_L1	A primeira linha do endereço de entrega	Strin	123 Any Street
	ENDEREÇO_DE_ENVIO_L2	A segunda linha do endereço de entrega	Strin	Unidade 123

Ca	Tipo de variável	Descrição	Tipo de dad	Ex
	CIDADE_EXPEDIÇÃO	A cidade que está no endereço de entrega	Strin	Qualquer cidade
	ESTADO_DE_ENVIO	O estado ou província que está no endereço de entrega	Strin	Qualquer estado
	PAÍS_DE_ENVIO	O país que está no endereço de entrega	Strin	Qualquer país Nota: O Amazon Fraud Detector enriquece esses dados. Para ter mais informações, consulte Enriquecimento da geolocalização.

Ca	Tipo de variável	Descrição	Tipo de dado	Ex
	SHIPPING_ZIP	O código postal que está no endereço de entrega	Strin	01234 Nota: O Amazon Fraud Detector enriquece esses dados. Para ter mais informações, consulte Enriquecimento da geolocalização.
Pagamento	ID_DO_PEDIDO	O identificador exclusivo da transação	Strin	LUX60
	PREÇO	O preço total do pedido	Strin	560,00
	CÓDIGO_DE_MOEDA	O código de moeda ISO 4217	Strin	USD

Ca	Tipo de variável	Descrição	Tipo de dado	Ex
	TIPO_DE_PAGAMENTO	A forma de pagamento usada para pagamento durante o evento	Strin	Cartão de crédito
	CÓDIGO_FONTE	O código alfanumérico enviado por um emissor de cartão de crédito ou banco emissor	Strin	0000
	AVS	O código de resposta do sistema de verificação de endereço (AVS) do processador do cartão	Strin	Y
Pr	CATEGORIA_PRODUTO	A categoria de produto do item do pedido	Strin	Cozinha
Pe za	NUMERIC	Qualquer variável que possa ser representada como um número real	Floa	1.224

Ca	Tipo de variável	Descrição	Tipo de dad	Ex
	CATEGORICAL	Qualquer variável que descreva categorias, segmentos ou grupos	Strin	Grande
	TEXTO_EM FORMATO LIVRE	Qualquer texto de formato livre que seja capturado como parte do evento (por exemplo, uma avaliação ou comentário de um cliente)	Strin	Exemplo de entrada de texto em formato livre

Atribuindo variável a um tipo de variável

Se você planeja usar uma variável para treinar seu modelo, é importante escolher um tipo de variável correto para atribuir à variável. A atribuição incorreta do tipo de variável pode afetar negativamente o desempenho do seu modelo. Também pode ser muito difícil alterar a atribuição posteriormente, especialmente se vários modelos e eventos tiverem usado a variável.

Você pode atribuir à sua variável qualquer um dos tipos de variáveis predefinidos ou um dos tipos de variáveis personalizadas —`FREE_FORM_TEXT`,`CATEGORICAL`, ou. `NUMERIC`

Notas importantes para atribuir variáveis aos tipos de variáveis corretos

1. Se a variável corresponder a um dos tipos de variáveis predefinidos, use-a. Certifique-se de que o tipo de variável corresponda à variável. Por exemplo, se você atribuir uma variável ip_address ao tipo de variável, a `EMAIL_ADDRESS` variável ip_address não será enriquecida com enriquecimentos como ASN, ISP, localização geográfica e pontuação de risco. Para obter mais informações, consulte Enriquecimentos variáveis.

2. Se a variável não corresponder a nenhum dos tipos de variáveis predefinidos, siga as recomendações listadas abaixo para atribuir um dos tipos de variáveis personalizadas.
3. Atribua o tipo de `CATEGORICAL` variável a variáveis que normalmente não têm ordem natural e podem ser colocadas em categorias, segmentos ou grupos. O conjunto de dados que você está usando para treinar seu modelo pode ter variáveis de ID como merchant_id, campaign_id ou policy_id. Essas variáveis representam grupos (por exemplo, todos os clientes com o mesmo policy_id representam um grupo). As variáveis que têm os seguintes dados devem ser atribuídas ao tipo de variável CATEGÓRICA -
   - Variáveis que contêm dados como Customer_ID, Segment_ID, Color_ID, department_code ou Product_ID.
   - Variáveis que contêm dados booleanos com valores verdadeiros, falsos ou nulos.
   - Variáveis que podem ser colocadas em grupos ou categorias, como nome da empresa, categoria do produto, tipo de cartão ou meio de referência.

   > **Note**
   >
   > `ENTITY_ID`é um tipo de variável reservada usado pelo Amazon Fraud Detector para atribuir à variável ENTITY_ID. A variável ENTITY_ID é a ID da entidade que está iniciando a ação que você deseja avaliar. Se você estiver criando um tipo de modelo Transaction Fraud Insight (TFI), precisará fornecer a variável ENTITY_ID. Você precisará decidir qual variável em seus dados identifica de forma exclusiva a entidade que está iniciando a ação e passá-la como variável ENTITY_ID. Atribua o tipo de variável CATEGÓRICA a todos os outros IDs em seu conjunto de dados, se eles estiverem presentes e se você os estiver usando para treinamento de modelos. Exemplos de outras IDs que não são uma entidade em seu conjunto de dados podem ser Merchant_ID, Policy_ID e Campaign_ID.
4. Atribua o tipo de `FREE_FORM_TEXT` variável às variáveis que contêm um bloco de texto. Exemplos de tipos de variáveis FREE_FORM_TEXT são: avaliações de usuários, comentários, datas e códigos de referência. Os dados FREE_FORM_TEXT contêm vários tokens separados por um delimitador. Os delimitadores podem ser qualquer caractere diferente do símbolo alfanumérico e sublinhado. Por exemplo, avaliações e comentários de usuários podem ser separados por um delimitador de “espaço”, datas e códigos de referência podem usar hífens como delimitadores para separar prefixo, sufixo e partes intermediárias. O Amazon Fraud Detector usa os delimitadores para extrair dados das variáveis FREE_FORM_TEXT.
5. Atribua o tipo de variável NUMERIC a variáveis que são números reais e têm ordenação inerente. Exemplos de variáveis NUMÉRICAS incluem day_of_the_week, incident_severity,

customer_rating. Embora você possa atribuir o tipo de variável CATEGÓRICA a essas variáveis, é altamente recomendável atribuir todas as variáveis de número real com ordem inerente ao tipo de variável NUMERIC.

Enriquecimentos variáveis

O Amazon Fraud Detector enriquece alguns dos elementos de dados brutos que você fornece, como endereços IP, números de identificação bancária (BINs) e números de telefone, para criar entradas adicionais e aumentar o desempenho dos modelos que usam esses elementos de dados. O enriquecimento ajuda a identificar situações potencialmente suspeitas e ajuda os modelos a capturar mais fraudes.

Enriquecimento do número de telefone

O Amazon Fraud Detector enriquece os dados do número de telefone com informações adicionais relacionadas à geolocalização, à operadora original e à validade do número de telefone. O enriquecimento do número de telefone é ativado automaticamente para todos os modelos treinados em ou após 13 de dezembro de 2021 e têm um número de telefone que inclui um código de país (+xxx). Se você incluiu a variável de número de telefone em seu modelo e a treinou antes de 13 de dezembro de 2021, treine novamente seu modelo para que ele possa aproveitar esse enriquecimento.

É altamente recomendável que você use o seguinte formato para variáveis de número de telefone para garantir que seus dados sejam enriquecidos com sucesso.

Variável	Formato	Descrição
PHONE_NUMBER	O padrão E.164	Certifique-se de incluir o código do país (+xxx) com o número de telefone.
BILLING_PHONE e SHIPPING_PHONE	O padrão E.164	Certifique-se de incluir o código do país (+xxx) com o número de telefone.

Enriquecimento da geolocalização

A partir de 8 de fevereiro de 2022, o Amazon Fraud Detector calcula a distância física entre os valores IP_ADDRESS, BILLING_ZIP e SHIPPING_ZIP que você fornece para um evento. As distâncias calculadas são usadas como entradas para seu modelo de detecção de fraudes.

Para habilitar o enriquecimento da geolocalização, os dados do evento devem incluir pelo menos duas das três variáveis: IP_ADDRESS, BILLING_ZIP ou SHIPPING_ZIP. Além disso, cada valor BILLING_ZIP e SHIPPING_ZIP deve ter um código BILLING_COUNTRY e um código SHIPPING_COUNTRY válidos, respectivamente. Se você tem um modelo que foi treinado antes de 8 de fevereiro de 2022 e inclui essas variáveis, você deve treinar novamente o modelo para habilitar o enriquecimento da geolocalização.

Se o Amazon Fraud Detector não conseguir determinar a localização associada aos valores IP_ADDRESS, BILLING_ZIP ou SHIPPING_ZIP de um evento devido à invalidade dos dados, um valor especial de espaço reservado será usado em vez disso. Por exemplo, suponha que um evento tenha valores de IP_ADDRESS e BILLING_ZIP válidos, mas o valor SHIPPING_ZIP não seja válido. Nesse caso, o enriquecimento é feito somente para IP_ADDRESS—> BILLING_ZIP. O enriquecimento não é feito para IP_ADDRESS—>SHIPPING_ZIP e BILLING_ZIP—>SHIPPING_ZIP. Em vez disso, os valores do espaço reservado são usados em seu lugar. Não importa se o enriquecimento de geolocalização está habilitado para seu modelo ou não, o desempenho do seu modelo não muda.

Você pode desativar o enriquecimento de geolocalização mapeando suas variáveis BILLING_ZIP e SHIPPING_ZIP para o tipo de variável CUSTOM_CATEGORICAL. Alterar o tipo de variável não afeta o desempenho do seu modelo.

Formato da variável de geolocalização

É altamente recomendável que você use o seguinte formato para variáveis de geolocalização para garantir que seus dados de localização sejam enriquecidos com sucesso.

Variável	Formato	Descrição
IP_ADDRESS	Endereço IPv4	Por exemplo - 1.1.1.1
BILLING_ZIP e SHIPPING_ZIP	O código postal ISO 3166-1 alfa-2 para o país especificado	Para obter mais informações, consulte a seção Códigos de

Variável	Formato	Descrição
		país e território neste tópico.
BILLING_COUNTRY e SHIPPING_COUNTRY	O código de país padrão ISO 3166-1 alfa-2 de duas letras	Para obter mais informações, consulte a seção Códigos de país e território neste tópico. O Amazon Fraud Detector tenta combinar todas as variações comuns do nome de um país com seu código de país padrão de duas letras ISO 3166-1. No entanto, não podemos garantir que eles serão combinados corretamente.

Códigos de país e território

A tabela a seguir fornece uma lista completa dos países e territórios que são suportados pelo Amazon Fraud Detector para enriquecimento de geolocalização. Cada país e território tem um código de país atribuído (especificamente, o código de país de duas letras ISO 3166-1 alfa-2) e um código postal.

Formato de código postal

- 9 - número
- a - letra
- [X] - X é opcional. Por exemplo, Guersney “GY9 [9] 9aa” significa que tanto “GY9 9aa” quanto “GY99 9aa” são válidos. Use um formato.
- [X/XX] - X ou XX podem ser usados. Por exemplo, Bermuda “aa [aa/99]” significa que tanto “aa aa” quanto “aa 99" são válidos. Use qualquer um desses formatos, mas não os dois.

- Alguns países têm prefixo fixo. Por exemplo, o código postal de Andorra é AD999. Isso significa que o código do país deve começar com as letras AD seguidas por três números.

Código	Name (Nome)	Código postal
AD	Andorra	AD999
AR	Antilhas Holandesas	9999
AT	Áustria	9999
AU	Austrália	9999
AZ	Azerbaijão	COMO 999
CAMA	Bangladesh	9999
SER	Bélgica	9999
POR	Bulgária	9999
BM	Bermudas	aa [aa/99]
BY	Bielorrússia	999999
CA	Canadá	a9a 9a9
CH	Suíça	9999
CL	Chile	9999999
CO	Colômbia	999999
CR	Costa Rica	99999
CHORAR	Chipre	9999
CZ	Tchequia	99 99
DE	Alemanha	99999

Código	Name (Nome)	Código postal
DK	Dinamarca	9999
DO	República Dominicana	99999
DZ	Argélia	99999
EE	Estônia	99999
ES	Espanha	99999
SE	Finlândia	99999
FM	Estados Federados da Micronésia	99999
DE	Ilhas Faroe	999
FR	França	99999
GB	Reino Unido	[a] 9 [a/9] 9aa
GG	Guernsey	GY9 [9] 9aa
GL	Groenlândia	9999
GP	Guadalupe	99999
GT	Guatemala	99999
ARMA	Guam	99999
HR	Croácia	99999
HU	Hungria	9999
IE	Irlanda	a99 [a/9] [a/9] [a/9] [a/9]
EU SOU	Ilha de Man	IM9 [9] 9aa
IN	Índia	999999

Código	Name (Nome)	Código postal
IS	Islândia	999
ISSO	Itália	99999
JE	Jérsei	JE9 [9] 9aa
JP	Japão	999-9999
KR	República da Coreia	99999
MENTIRA	Liechtenstein	9999
LK	Sri Lanka	99999
LT	Lituânia	99999
LU	Luxemburgo	L-9999
LV	Letônia	LV-9999
MC	Mônaco	99999
MD	República da Moldávia	9999
MH	Ilhas Marshall	99999
KM	Macedônia do Norte	9999
MAPA	Ilhas Marianas do Norte	99999
MQ	Matinique	99999
MT	Malta	aaaa 999
MX	México	99999
MEU	Malásia	99999
NL	Holanda	999 aa

Código	Name (Nome)	Código postal
NO	Noruega	9999
NZ	Nova Zelândia	9999
PH	Filipinas	9999
PK	Paquistão	99999
PL	Polônia	99-999
PR	Porto Rico	99999
PT	Portugal	9999-999
PW	Palau	99999
SOBRE	Reunião	99999
OU	Romênia	999999
RU	Federação Russa	999999
SE	Suécia	99 99
SG	Singapura	999999
É	Eslovênia	9999
SK	Eslováquia	99 99
SM	São Marinho	99999
TH	Tailândia	99999
TR	Turquia	99999
UA	Ucrânia	99999
EUA	Estados Unidos	99999

Código	Name (Nome)	Código postal
COMPRAR	Uruguai	99999
VI	Ilhas Virgens Americanas	99999
WF	Wallis e Futuna	99999
AINDA	Mayotte	99999
ZA	África do Sul	9999

Enriquecimento do agente do usuário

Se você criar o modelo Account Takeover Insights (ATI), deverá fornecer uma variável do tipo de `useragent` variável em seu conjunto de dados. Essa variável contém os dados do navegador, dispositivo e sistema operacional de um evento de login. O Amazon Fraud Detector enriquece os dados do agente do usuário com informações adicionais, como e. `user_agent_family` `OS_family` `device_family`

Crie uma variável

Você pode criar variáveis no console do Amazon Fraud Detector, usando o comando create-variable, usando o, ou usando o CreateVariableAWS SDK for Python (Boto3)

Crie uma variável usando o console do Amazon Fraud Detector

Esse exemplo cria duas variáveis `email_address` `eip_address`, e as atribui aos tipos de variáveis correspondentes (`EMAIL_ADDRESS`e`IP_ADDRESS`). Essas variáveis são usadas como exemplos. Se você estiver criando variáveis para usar em seu treinamento de modelo, use as variáveis do seu conjunto de dados que sejam apropriadas para seu caso de uso. Certifique-se de ler sobre Tipos de variáveis e Enriquecimentos variáveis antes de criar suas variáveis.

Para criar uma variável,

1. Abra o AWSManagement Console e faça login na sua conta.
2. Navegue até o Amazon Fraud Detector, escolha Variáveis na navegação à esquerda e escolha Criar.

3. Na página Nova variável, insira `email_address` como nome da variável. Opcionalmente, insira uma descrição da variável.
4. No tipo Variável, escolha Endereço de e-mail.
5. O Amazon Fraud Detector seleciona automaticamente o tipo de dados para esse tipo de variável porque esse tipo de variável é predefinido. Se a variável não for atribuída automaticamente a um tipo de variável, selecione um tipo de variável na lista. Para obter mais informações, consulte Tipos de variáveis.
6. Se você quiser fornecer um valor padrão para sua variável, selecione Definir um valor padrão personalizado e insira um valor padrão para sua variável. Ignore esta etapa se você estiver seguindo este exemplo.
7. Escolha Create (Criar).
8. Na página de visão geral do email_address, confirme os detalhes da variável que você acabou de criar.

   Se precisar atualizar, escolha Editar e forneça as atualizações. Escolha Salvar alterações.
9. Repita o processo para criar outra variável `ip_address` e escolha Endereço IP para o tipo de variável.
10. A página Variáveis mostra as variáveis recém-criadas.

> **Important**
>
> Recomendamos que você crie quantas variáveis quiser do seu conjunto de dados. Posteriormente, ao criar seu tipo de evento, você pode decidir quais variáveis deseja incluir para treinar seu modelo para detectar fraudes e gerar detecções de fraudes.

Crie uma variável usando o AWS SDK for Python (Boto3)

O exemplo a seguir mostra solicitações para a CreateVariableAPI. O exemplo cria duas variáveis `email_address` `eip_address`, e as atribui aos tipos de variáveis correspondentes (`EMAIL_ADDRESSeIP_ADDRESS`).

Essas variáveis são usadas como exemplos. Se você estiver criando variáveis para usar em seu treinamento de modelo, use as variáveis do seu conjunto de dados que sejam apropriadas para seu caso de uso. Certifique-se de ler sobre Tipos de variáveis e Enriquecimentos variáveis antes de criar suas variáveis.

Certifique-se de especificar uma fonte variável. Isso ajuda a identificar de onde o valor da variável é derivado. Se a fonte da variável for EVENT, o valor da variável será enviado como parte da GetEventPredictionsolicitação. Se o valor da variável for`MODEL_SCORE`, ela será preenchida por um Amazon Fraud Detector. Se`EXTERNAL_MODEL_SCORE`, o valor da variável for preenchido por um SageMaker modelo importado.

```
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>'
     )
```

Excluir uma variável

Quando você exclui uma variável, o Amazon Fraud Detector exclui permanentemente essa variável e os dados não são mais armazenados no Amazon Fraud Detector.

Você não pode excluir variáveis que estão incluídas em um tipo de evento no Amazon Fraud Detector. Você precisará primeiro excluir o tipo de evento ao qual a variável está associada e depois excluir a variável.

Você não pode excluir manualmente as variáveis de saída do modelo e SageMaker as variáveis de saída do modelo do Amazon Fraud Detector. O Amazon Fraud Detector exclui automaticamente as variáveis de saída do modelo quando você exclui o modelo.

Você pode excluir a variável no console do Amazon Fraud Detector, usando o comando delete-variable CLI, usando a API ou usando o DeleteVariableAWS SDK for Python (Boto3)

Excluir variável usando o console

Para excluir uma variável,

1. Faça login AWS Management Console e abra o console do Amazon Fraud Detector em https://console.aws.amazon.com/frauddetector.
2. No painel de navegação esquerdo do console do Amazon Fraud Detector, escolha Recursos e, em seguida, escolha Variáveis.
3. Escolha a variável que você deseja excluir.
4. Escolha Actions (Ações) e, em seguida, escolha Delete (Excluir).
5. Insira o nome da variável e escolha Excluir variável.

Exclua a variável usando o AWS SDK for Python (Boto3)

O exemplo de código a seguir exclui uma variável customer_name usando a API. DeleteVariable

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

fraudDetector.delete_variable (

name = 'customer_name'

)
```

Rótulos

Um rótulo classifica um evento como fraudulento ou legítimo. Os rótulos são associados a tipos de eventos e usados para treinar modelos de machine no Amazon Fraud Detector. Se você planeja treinar um modelo do Online Fraud Insights (OFI) ou do Transaction Fraud Insights (TFI), um mínimo de 400 eventos em seu conjunto de dados de treinamento devem ser classificados como fraudulentos ou legítimos. Você pode usar qualquer rótulo, como fraude, legítimo, 1 ou 0, para classificar eventos em seu conjunto de dados de treinamento. Depois que o treinamento é concluído,

o modelo treinado avalia os eventos em busca de fraudes e usa esses valores para classificar os eventos como fraudulentos ou legítimos.

Você precisará primeiro criar os rótulos com os valores usados em seu conjunto de dados de treinamento e depois associá-los ao tipo de evento usado para criar e treinar seu modelo de detecção de fraudes.

Criar etiqueta

Você pode criar rótulos no console do Amazon Fraud Detector, usando o comando put-label, usando a PutLabelAPI ou usandoAWS SDK for Python (Boto3) o.

Crie uma etiqueta usando o console Amazon Fraud Detector

Para criar rótulos,

1. Abra o AWSManagement Console e faça login em sua conta.
2. Navegue até o Amazon Fraud Detector, escolha Rótulos no painel de navegação à esquerda e escolha Criar.
3. Na página Criar etiqueta, insira o nome da etiqueta para o evento fraudulento como o nome da etiqueta. O nome do rótulo deve corresponder ao rótulo que representa a atividade fraudulenta em seu conjunto de dados de treinamento. Opcionalmente, insira uma descrição do rótulo.
4. Escolha Criar etiqueta.
5. Crie um segundo rótulo e insira o nome do rótulo para o evento legítimo. Certifique-se de que o nome do rótulo corresponda ao valor que representa a atividade legítima em seu conjunto de dados de treinamento.

Crie um rótulo usando oAWS SDK for Python (Boto3)

O código deAWS SDK for Python (Boto3) exemplo a seguir cria dois rótulos (fraudulentos, legítimos) usando a PutLabelAPI. Depois de criar os rótulos, você pode adicioná-los a um tipo de evento para classificar eventos específicos.

```
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'
)
```

Atualizar rótulo

Se o conjunto de dados do seu evento estiver armazenado com o Amazon Fraud Detector, talvez seja necessário adicionar ou atualizar rótulos para os eventos armazenados, como quando você realiza uma investigação de fraude off-line para um evento e deseja fechar o ciclo de feedback do aprendizado de máquina.

Você pode adicionar ou atualizar rótulos para eventos armazenados usando o update-event-labelcomando, usando a UpdateEventLabelAPI ou usando oAWS SDK for Python (Boto3)

O código deAWS SDK for Python (Boto3) exemplo a seguir adiciona uma fraude de rótulo associada ao registro do tipo de evento usando a`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'
)
```

Atualização de rótulos de eventos em dados de eventos armazenados no Amazon Fraud Detector

Talvez seja necessário adicionar ou atualizar rótulos de fraude para eventos que já estão armazenados no Amazon Fraud Detector, como quando você realiza uma investigação de fraude offline para um evento e deseja fechar o ciclo de feedback de aprendizado de máquina.

Para atualizar o rótulo de um evento que já está armazenado no Amazon Fraud Detector, use a operaçãoUpdateEventLabel da API. Veja a seguir um exemplo de chamada de 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'
)
```

Excluir rótulo

Quando você exclui uma etiqueta, o Amazon Fraud Detector exclui permanentemente essa etiqueta e os dados não são mais armazenados no Amazon Fraud Detector.

Não é possível excluir um rótulo incluído em um tipo de evento no Amazon Fraud Detector. E você também não pode excluir um rótulo atribuído a um rótulo atribuído a um ID de evento. Primeiro, você precisa excluir o ID de evento relevante.

Você pode excluir rótulos no console do Amazon Fraud Detector, usando o comando delete-label, usando a DeleteLabelAPI ou usando oAWS SDK for Python (Boto3)

Excluir rótulo usando o console

Para excluir um rótulo um rótulo

1. Faça login noAWS Management Console e abra o console do Amazon Fraud Detector em https://console.aws.amazon.com/frauddetector.
2. No painel de navegação esquerdo do console do Amazon Fraud Detector, selecione Recursos e, em seguida, selecione Ajustar.
3. Escolha o rótulo que você deseja excluir.
4. Escolha Actions (Ações) e, em seguida, escolha Delete (Excluir).
5. Insira o nome do rótulo e escolha Excluir rótulo.

Exclua um rótulo usando oAWS SDK for Python (Boto3)

O código deAWS SDK for Python (Boto3) exemplo a seguir exclui um rótulo legítimo usando a DeleteLabelAPI.

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

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

Regras

Uma regra é uma condição que informa ao Amazon Fraud Detector como interpretar valores variáveis durante uma previsão de fraude. Uma regra faz parte da lógica de um detector e consiste nos seguintes elementos:

- Variável ou lista — A variável representa um elemento de dados em seu conjunto de dados de eventos que você deseja usar em uma previsão de fraude. Uma lista é um conjunto de elementos de dados de entrada para uma variável no conjunto de dados do evento. As variáveis usadas em uma regra devem ser predefinidas no tipo de evento avaliado e as listas usadas em uma regra devem estar associadas a um tipo de variável. Para ter mais informações, consulte Variáveis e Listas.
- Expressão — Uma expressão em uma regra captura sua lógica de negócios. Se você estiver usando variável em sua regra, uma expressão de regra simples será construída usando uma variável, um operador de comparação como >, <, <=, >=. == e um valor. Se você estiver usando uma lista, a expressão da regra será construída como entrada da lista e o nome da lista. `in` Para obter mais informações, consulte Referência do idioma da regra. Você pode combinar várias expressões usando `and` `or` e. Todas as expressões devem ser avaliadas como um valor booleano (verdadeiro ou falso) e ter menos de 4.000 caracteres. As condições do tipo If-else não são suportadas.
- Resultado — Um resultado é uma resposta retornada pelo Amazon Fraud Detector quando uma regra é correspondida. O resultado indica o resultado de uma previsão de fraude. Você pode criar resultados para cada possível previsão de fraude e adicioná-los a uma regra. Para obter mais informações, consulte Resultados.

Um detector deve ter pelo menos uma regra associada. Uma regra pode ter até 3 listas e um detector pode ter até 30 listas. Você cria uma regra como parte do processo de criação do detector. Você também pode criar e associar novas regras a um detector existente.

Referência do idioma da regra

A seção a seguir descreve os recursos de expressão (ou seja, elaboração de regras) no Amazon Fraud Detector.

Usando variáveis

Você pode usar qualquer variável definida no tipo de evento avaliado como parte de sua expressão. Use o cifrão para indicar uma variável:

```
$example_variable < 100
```

Usando listas

Você pode usar qualquer lista associada a um tipo de variável e preenchida com entradas como parte de sua expressão de regra. Use o cifrão para indicar um valor de entrada na lista:

```
$example_list_variable in @list_name
```

Operadores de comparação, associação e identidade

O Amazon Fraud Detector inclui os seguintes operadores de comparação: **>**, **>=**, **<**, **<=**,! =, ==, em, não em

Veja os exemplos a seguir:

Exemplo: **<**

```
$variable < 100
```

Exemplo: em, não em

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

Exemplo:! =

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

Exemplo: ==

```
$variable == 1000
```

Tabelas de operadores

Operador	Operador de detector de fraudes da Amazon
Igual a	==
Não é igual a	!=
Maior que	>
Menor que	<
Grande ou igual a	>=
Menor ou igual a	<=
Entrada	em
E	e
Ou	or
Não	!

Matemática básica

Você pode usar operadores matemáticos básicos em sua expressão (por exemplo, +, -, *,/). Um caso de uso típico é quando você precisa combinar variáveis durante sua avaliação.

Na regra abaixo, estamos adicionando a variável `$variable_1` com `$variable_2` e verificando se o total é menor que 10.

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

Dados básicos da tabela matemática

Operador	Operador de detector de fraudes da Amazon
Mais	+
Menos	-
Multiply (Multiplicar)	*
Divide (Dividir)	/
Módulo	%

Expressão regular (regex)

Você pode usar regex para pesquisar padrões específicos como parte de sua expressão. Isso é particularmente útil se você quiser combinar uma string específica ou um valor numérico para uma de suas variáveis. O Amazon Fraud Detector só suporta correspondência ao trabalhar com expressões regulares (por exemplo, ele retorna True/False dependendo se a string fornecida corresponde à expressão regular). O suporte a expressões regulares do Amazon Fraud Detector é baseado em .matches () em java (usando a biblioteca RE2J Regular Expression). Existem vários sites úteis na Internet que são úteis para testar diferentes padrões de expressão regular.

No primeiro exemplo abaixo, primeiro transformamos a variável `email` em minúsculas. Em seguida, verificamos se o padrão `@gmail.com` está na `email` variável. Observe que o segundo ponto é escapado para que possamos verificar explicitamente a string. `.com`

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

No segundo exemplo, verificamos se a variável `phone_number` contém o código do país `+1` para determinar se o número de telefone é dos EUA. O símbolo de mais é escapado para que possamos verificar explicitamente a string. +1

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

Tabela Regex

Operador	Exemplo do Amazon Fraud Detector
Combine qualquer string que comece com	regex_match (“^mystring”, variável $)
Combine exatamente toda a sequência	regex_match (“minha string”, variável $)
Combine qualquer caractere, exceto a nova linha	regex_match (” . “, $variável)
Combine qualquer número de caracteres, exceto a nova linha antes de 'mystring'	regex_match (”). *mystring”, $variável)
Caracteres especiais de escape	\

Verificando valores faltantes

Às vezes, é benéfico verificar se o valor está ausente. No Amazon Fraud Detector, isso é representado por nulo. Você pode fazer isso usando a seguinte sintaxe:

```
$variable != null
```

Da mesma forma, se você quiser verificar se um valor não está presente, você pode fazer o seguinte:

```
$variable == null
```

Múltiplas condições

Você pode combinar várias expressões usando `and` `or` e. O Amazon Fraud Detector para em uma `OR` expressão quando um único valor verdadeiro é encontrado e para em uma `AND` quando um único valor falso é encontrado.

No exemplo abaixo, estamos verificando duas condições usando a `and` condição. Na primeira declaração, estamos verificando se a variável 1 é menor que 100. Na segunda, verificamos se a variável 2 não é os EUA.

Como a regra usa um`and`, ambos devem ser VERDADEIROS para que toda a condição seja avaliada como VERDADEIRA.

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

Você pode usar parênteses para agrupar operações booleanas, conforme mostrado a seguir:

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

Outros tipos de expressão

DateTimefunções

Função	Descrição	Exemplo
obter data e hora atual ()	Fornece a hora atual da execução da regra no formato ISO8601 UTC. Você pode usar getepochmillisecon ds (getcurrentdatetime ()) para realizar operações adicionais	getcurrentdatetime () = “28/03/2021 T 18:34:02 Z”
é antes (DateTime1, DateTime 2)	Retorna um booleano (verdadeiro/ falso) se o chamador DateTime 1 estiver antes de 2 DateTime	isbefore (getcurrentdatetime (), “2019-11-30T 01:01:01 Z”) == “Falso” isbefore (getcurrentdatetime (), “2050-11-30T 01:05:01 Z”) == “Verdadeiro”
é depois (DateTime1, DateTime 2)	Retorna um booleano (verdadeiro/ falso) se o chamador DateTime 1 estiver depois de 2 DateTime	isafter (getcurrentdatetime (), “30/11/2019 T 01:01:01 Z”) == “Verdadeiro” isafter (getcurrentdatetime (), “2050-11-30T 01:05:01 Z”) == “Falso”
getepoch milissegundos () DateTime	Pega um DateTime e retorna isso DateTime em milissegundos de época. Útil para realizar operações matemáticas na data	getepochmilliseconds (“2019-11-30T 01:01:01 Z”) = 1575032461

Operadores de sequência

Operador	Exemplo
Transformar string em maiúsculas	maiúsculas (variável $)
Transformar string em minúsculas	minúsculas (variável $)

Outros

Operador	Comentário
Adicionar um comentário	# meu comentário

Crie regras

Você pode criar regras no console do Amazon Fraud Detector, usando o comando create-rule, usando a CreateRuleAPI ou usando o. AWS SDK for Python (Boto3)

Cada regra deve conter uma única expressão que capture sua lógica de negócios. Todas as expressões devem ser avaliadas como um valor booleano (verdadeiro ou falso) e ter menos de 4.000 caracteres. As condições do tipo If-else não são suportadas. Todas as variáveis usadas na expressão devem ser predefinidas no tipo de evento avaliado. Da mesma forma, todas as listas usadas na expressão devem ser predefinidas, associadas a um tipo de variável e preenchidas com entradas.

O exemplo a seguir cria uma regra `high_risk` para um detector `payments_detector` existente. A regra associa uma expressão e um resultado `verify_customer` à regra.

Pré-requisitos

Para seguir as etapas mencionadas abaixo, certifique-se de concluir o seguinte antes de continuar com a criação de regras:

- Crie um detector
- Crie um resultado

Se você estiver criando um detector, regra e resultado para seu caso de uso, substitua o nome do detector de exemplo, o nome da regra, a expressão da regra e o nome do resultado pelos nomes e expressões relevantes para seu caso de uso.

Crie uma nova regra no console do Amazon Fraud Detector

1. Abra o AWSManagement Console e faça login na sua conta. Navegue até o Amazon Fraud Detector.
2. No painel de navegação esquerdo, escolha Detectores e selecione o detector que você criou para seu caso de uso, por exemplo, payments_detector.
3. Na página payments_detector, escolha a guia Regras associadas e escolha Criar regra.
4. Na página Nova regra, insira o seguinte:
    a. Em Nome, insira um nome para a regra, exemplo **`high_risk`**
    b. Em Descrição - opcional, opcionalmente, insira uma descrição da regra, por exemplo, **`This rule captures events with a high ML model score`**
    c. Na Expressão, insira uma expressão de regra para seu caso de uso usando o guia de referência rápida de expressões. Exemplo `$sample_fraud_detection_model_insightscore >900`
    d. Em Resultados, escolha o resultado que você criou para seu caso de uso, por exemplo, verify_customer. Um resultado é o resultado de uma previsão de fraude e é retornado se a regra coincidir durante uma avaliação.
5. Escolha Salvar regra

Você criou uma nova regra para o seu detector. Essa é a versão 1 da regra que o Amazon Fraud Detector disponibiliza automaticamente para uso do detector.

Crie uma regra usando o AWS SDK for Python (Boto3)

O código de exemplo a seguir usa a CreateRuleAPI para criar uma regra `high_risk` para um detector `payments_detector` existente. O código de exemplo também adiciona uma expressão de regra e um resultado `verify_customer` à regra.

Pré-requisitos

Para usar o código de exemplo, certifique-se de ter concluído o seguinte antes de continuar com a criação de regras:

- Crie um detector
- Crie um resultado

Se você estiver criando um detector, regra e resultado para seu caso de uso, substitua o nome do detector de exemplo, o nome da regra, a expressão da regra e o nome do resultado por nomes e expressões relevantes para seu caso de 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']
)
```

Você criou a versão 1 da regra que o Amazon Fraud Detector a disponibiliza automaticamente para uso do detector.

Regra de atualização

Você pode atualizar uma regra a qualquer momento adicionando ou atualizando a descrição da regra, atualizando a expressão da regra ou adicionando ou removendo o resultado da regra. Quando você atualiza uma regra, uma nova versão da regra é criada.

Você pode atualizar uma regra no console do Amazon Fraud Detector usando o update-rule-versioncomando, usando a UpdateRuleVersionAPI ou usando o AWS SDK.

Depois de atualizar a regra, certifique-se de atualizar a versão do detector para usar a nova versão da regra.

Regra de atualização no console do Amazon Fraud Detector

Para atualizar uma regra,

1. Abra o AWSManagement Console e faça login na sua conta. Navegue até o Amazon Fraud Detector.
2. No painel de navegação esquerdo, escolha Detectores.

3. No painel Detectores, selecione o detector associado à regra que você deseja atualizar.
4. Na página do detector, escolha a guia Regras associadas e selecione a regra que você deseja atualizar.
5. Na sua página de regras, escolha Ações e selecione Criar versão.
6. Observe que a versão foi alterada. Insira a descrição, expressão ou resultado atualizados.
7. Escolha Salvar nova versão

Atualize a regra usando o AWS SDK for Python (Boto3)

O código de exemplo a seguir usa a UpdateRuleVersionAPI para atualizar o limite da regra `high_risk` de 900 para 950. Essa regra está associada ao detector`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']
)
```

Listas

Uma lista é um conjunto de dados de entrada para uma variável em seu conjunto de dados de eventos. Você usa os dados de entrada em uma regra associada ao seu detector. Uma regra é uma condição que define como Amazon Fraud Detector como o Amazon Fraud Detector como o Amazon Fraud Detector como o Amazon Fraud Dettor como o Amazon Fraud Por exemplo, você pode criar uma lista de endereços IP e, em seguida, criar uma regra para negar acesso se um endereço IP específico estiver na lista. As regras que usam listas são expressas no`@list_name` formato`$ip_address_value` in.

Com o Amazon Fraud Detector, você pode gerenciar uma lista adicionando ou removendo dados sem precisar atualizar uma regra associada. Uma regra associada à sua lista incorpora automaticamente dados recém-adicionados ou removidos.

Uma lista pode conter até 100.000 entradas exclusivas e cada entrada pode ter até 320 caracteres. Cada lista que você usa em uma regra é, por padrão, associada aoTipos de variáveis FREE_FORM_TEXT do Amazon Fraud Detector. Você pode atribuir um tipo de variável à sua lista a qualquer momento. Você pode usar até 3 listas em uma regra.

Você pode criar uma lista, adicionar entradas à lista, excluir uma lista ou excluir uma ou mais entradas na lista, ou atribuir um tipo de variável à sua lista no console do Amazon Fraud Detector, usando a API, usando oAWS CLI ou usando oAWS SDK.

Criar uma lista

Você pode criar uma lista contendo dados de entrada (entradas) de uma variável em seu conjunto de dados de eventos e usar a lista na expressão da regra. As entradas na lista podem ser gerenciadas dinamicamente sem atualizar a regra que está usando a lista.

Para criar uma lista, você deve primeiro especificar um nome e, opcionalmente, associar a lista a uma listaTipos de variáveis suportada pelo Amazon Fraud Detector. Por padrão, o Amazon Fraud Detector assume que a lista é do tipo de variável FREE_FORM_TEXT.

Você pode criar uma lista no console do Amazon Fraud Detector, usando a APIAWS CLI, usando o ou usando oAWS SDK.

Crie uma lista usando o console Amazon Fraud Detector

Criar uma lista

1. Abra o AWSManagement Console e faça login em sua conta. Navegue até Amazon Fraud Detector.
2. No painel de navegação.
3. Em Detalhes das listas
    a. No Nome da lista. Insira um nome para a lista.
    b. Em Description (Descrição), opcionalmente, insira uma descrição.
    c. (Opcional) Em Tipo de variável, selecione um tipo de variável para sua lista.

> **Important**
>
> Se sua lista contiver endereços IP, certifique-se de selecionar IP_ADDRESS como o tipo de variável. Se você não selecionar um tipo de variável, o Amazon Fraud Detector presume que a lista seja do tipo de variável FREE_FORM_TEXT.

4. Em Adicionar dados da lista, adicione entradas de lista, uma entrada em cada linha. Você também pode copiar e colar entradas de uma planilha.

> **Note**
>
> Certifique-se de que as entradas não estejam separadas por vírgula e sejam exclusivas na lista. Se duas entradas idênticas forem inseridas, somente uma será adicionada.

5. Escolha Create (Criar).

Crie uma lista usando oAWS SDK for Python (Boto3)

Você cria uma lista especificando um nome de lista. Opcionalmente, você pode fornecer uma descrição, associar um tipo de variável ou adicionar entradas à sua lista ao criar uma lista. Ou você pode atualizar a lista posteriormente adicionando entradas ou uma descrição. Você pode atribuir um tipo de variável à lista posteriormente, caso ainda não a tenha atribuído no momento da criação da lista. O tipo de variável de uma lista não pode ser alterado após sua atribuição.

> **Important**
>
> Se sua lista contiver endereços IP, certifique-se de atribuir IP_ADDRESS como o tipo de variável. Se você não atribuir um tipo de variável, o Amazon Fraud Detector presume que a lista seja do tipo de variável FREE_FORM_TEXT.

O exemplo a seguir usa a operação de CreateListAPI para criar uma`allow_email_ids` lista fornecendo uma descrição, um tipo de variável e adicionando quatro entradas de lista.

```
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']
    )
```

Adicionar entradas em uma lista

Depois de criar sua lista, você pode adicionar ou acrescentar entradas à sua lista a qualquer momento. Ao adicionar ou acrescentar entradas em sua lista, você não precisa atualizar a regra à qual a lista está associada. A regra incorpora automaticamente as entradas recém-adicionadas.

Sua lista pode conter até 100.000 entradas exclusivas e cada entrada pode ter até 320 caracteres.

Você pode adicionar entradas no console do Amazon Fraud Detector usando a API, usando oAWS CLI ou usando oAWS SDK.

Adicione entradas em uma lista usando o console Amazon Fraud Detector

Como adicionar uma ou mais entradas em uma lista

1. Abra o AWSManagement Console e faça login em sua conta. Navegue até Amazon Fraud Detector.
2. No painel de navegação.
3. Na página Listas, selecione a lista à qual você deseja adicionar entradas.
4. Na página de detalhes da sua lista, selecione a guia Dados da lista e escolha Adicionar dados.
5. Na caixa Adicionar dados da lista, adicione uma entrada em cada linha ou copie e cole entradas de uma planilha. Certifique-se de não usar vírgula para separar as entradas.
6. Escolha Add (Adicionar).

Adicione entradas em uma lista usando oAWS SDK for Python (Boto3)

O exemplo a seguir usa a operação UpdateListda API para adicionar duas novas entradas na`allow_email_ids` lista. Certifique-se de que as entradas que você está adicionando sejam exclusivas na lista.

```
import boto3
```

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

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

Atribuir um tipo de variável a uma lista

Cada lista que você usa em uma regra deve estar associada ao tipo deTipos de variáveis variável do Amazon Fraud Detector. Por padrão, o Amazon Fraud Detector assume que a lista é do tipo de variável FREE_FORM_TEXT. É importante observar que uma lista que consiste em endereços IP deve estar associada ao tipo de variável IP_ADDRESS.

Você pode associar sua lista a um tipo de variável no momento da criação da lista ou a qualquer momento posterior. Se você já associou sua lista a um tipo de variável e deseja alterá-la posteriormente, você deve criar uma nova lista. Não é possível alterar o tipo de variável de uma lista.

Você pode atribuir um tipo de variável no console do Amazon Fraud Detector usando a API, usando oAWS CLI ou usando oAWS SDK.

Atribua um tipo de variável a uma lista usando o console Amazon Fraud Detector

Para atribuir um tipo de variável a uma lista

1. Abra o AWSManagement Console e faça login em sua conta. Navegue até Amazon Fraud Detector.
2. No painel de navegação.
3. Na página Listas, selecione a lista à qual você deseja atribuir um tipo de variável.
4. Na página de detalhes da sua lista, escolha Ações e selecione Editar lista.
5. Na caixa Editar lista, selecione o tipo de variável para sua lista.
6. Escolha Save (Salvar).

Atribua um tipo de variável a uma lista usando oAWS SDK for Python (Boto3)

O exemplo a seguir usa a operação UpdateListda API para atribuir um tipo de variável à`allow_ip_address` lista.

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

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

Excluir uma lista

Você pode excluir uma lista que não é usada em nenhuma regra. Quando você exclui uma lista, o Amazon Fraud Detector exclui permanentemente essa lista e todas as entradas na lista.

Você pode excluir uma lista no console do Amazon Fraud Detector, usando a API, usando oAWS CLI ou oAWS SDK.

Exclua a lista usando o console Amazon Fraud Detector

Para excluir uma lista

1. Abra o AWSManagement Console e faça login em sua conta. Navegue até Amazon Fraud Detector.
2. No painel de navegação, escolha Listas
3. Na página Listas. Selecione a lista que você quer excluir.
4. Na página de detalhes da sua lista, escolha Ações e selecione Excluir lista.
5. Escolha Excluir lista.

Excluir lista usando oAWS SDK for Python (Boto3)

O exemplo a seguir usa a operação DeleteListda API para excluir`allow_email_ids`.

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

Excluir entradas de uma lista

É possível excluir uma ou mais entradas de suas listas a qualquer momento. Ao excluir entradas na sua lista, você não precisa atualizar a regra à qual a lista está associada. A regra incorpora automaticamente a lista atualizada.

Você pode excluir entradas de uma lista no console do Amazon Fraud Detector, usando a API, usando oAWS CLI ou oAWS SDK.

Exclua entradas de uma lista usando o console Amazon Fraud Detector

Para excluir uma ou mais entradas de uma lista

1. Abra o AWSManagement Console e faça login em sua conta. Navegue até Amazon Fraud Detector.
2. No painel de navegação, escolha Listas
3. Na página Listas. Selecione a lista que contém entradas que você quer excluir.
4. Na página de detalhes da sua lista, selecione a guia Dados da lista e selecione as entradas que você deseja excluir.
5. Escolha Excluir e escolha Excluir novamente para confirmar.

Exclua entradas de uma lista usando oAWS SDK for Python (Boto3)

No exemplo a seguir, a operação UpdateListda API exclui entradas da`allow_email_ids` lista.

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

Excluir todas as entradas de uma lista

Você pode excluir todas as entradas da sua lista, se a lista não estiver sendo usada em uma regra. Você pode excluir todas as entradas que estão na lista e depois adicionar entradas na mesma lista.

Você pode excluir entradas de uma lista no console do Amazon Fraud Detector, usando a API, usando oAWS CLI ou oAWS SDK.

Exclua todas as entradas de uma lista usando o console Amazon Fraud Detector

Para excluir todas as entradas de uma lista

1. Abra o AWSManagement Console e faça login em sua conta. Navegue até Amazon Fraud Detector.
2. No painel de navegação, escolha Listas
3. Na página Listas. Selecione a lista que contém entradas que você quer excluir.
4. Na página de detalhes da sua lista, selecione a guia Dados da lista e escolha Excluir tudo.
5. Na caixa Excluir tudo, digite`delete all` para confirmar e escolha Excluir todos os dados da lista.

Exclua todas as entradas de uma lista usando oAWS SDK for Python (Boto3)

No exemplo a seguir, a operação UpdateListda API exclui todas as entradas da`allow_email_ids` lista.

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

Resultados

Um resultado é o resultado de uma previsão de fraude. Você pode criar um resultado para cada possível resultado de previsão de fraude. Por exemplo, talvez você queira que os resultados representem níveis de risco (alto_risco, risco_médio e baixo_risco) ou ações (aprovação, revisão). Depois que um resultado é criado, você pode adicionar um ou mais resultados a uma regra. Como parte da GetEventPredictionresposta, o Amazon Fraud Detector retorna os resultados definidos para qualquer regra correspondente.

Crie um resultado

Você pode criar resultados no console do Amazon Fraud Detector, usando o comando put-result, usando a PutOutcomeAPI ou usandoAWS SDK for Python (Boto3) o.

Crie um resultado usando o console Amazon Fraud Detector

Para criar um ou mais resultados,

1. Abra o AWSManagement Console e faça login em sua conta. Navegue até o Amazon Fraud Detector.
2. No painel de navegação esquerdo, escolha Resultados.
3. Na página Resultados, escolha Criar.
4. Na página Novo resultado, insira o seguinte:
   a. No Nome do resultado, insira um nome para seu resultado.
   b. Na descrição do resultado, opcionalmente, insira uma descrição.
5. Escolha Salvar resultado.
6. Repita as etapas 2 a 5 para criar resultados adicionais.

Crie um resultado usando oAWS SDK for Python (Boto3)

O exemplo a seguir usa a`PutOutcome` API para criar três resultados. Eles são`verify_customer`,`review`,`approve` e. Depois que os resultados forem criados, você poderá atribuí-los às regras.

```
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'
)
```

Exclui um resultado

Não é possível excluir um resultado usado em uma versão de regra.

Quando você exclui um resultado, o Amazon Fraud Detector exclui permanentemente esse resultado e os dados não são mais armazenados no Amazon Fraud Detector.

Você pode excluir um resultado no console do Amazon Fraud Detector, usando o comando delete-result, usando a DeleteOutcomeAPI ou usando oAWS SDK for Python (Boto3)

Excluir um resultado no console do Amazon Fraud Detector

Para excluir um resultado

1. Faça login noAWS Management Console e abra o console do Amazon Fraud Detector em https://console.aws.amazon.com/frauddetector.
2. No painel de navegação esquerdo do console do Amazon Fraud Detector, escolha Recursos e, em seguida, escolha Resultados.
3. Escolha o resultado que você deseja excluir.
4. Escolha Actions (Ações) e, em seguida, escolha Delete (Excluir).
5. Insira o nome do resultado e escolha Excluir resultado.

Exclua um resultado usando oAWS SDK for Python (Boto3)

O exemplo a seguir usa a DeleteOutcomeAPI para excluir `overify_customer` resultado. Depois que o resultado for excluído, você não poderá mais atribuí-lo a uma regra.

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

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

```
)
```

Entidade

Uma entidade representa uma pessoa ou coisa que está realizando o evento. Um tipo de entidade classifica a entidade. Classificações de exemplo incluem cliente, comerciante, usuário ou conta. Você fornece o tipo de entidade (ENTITY_TYPE) e um identificador de entidade (ENTITY_ID) como parte do conjunto de dados do evento para indicar a entidade específica que realizou o evento.

O Amazon Fraud Detector usa o tipo de entidade ao gerar uma previsão de fraude para um evento para indicar quem realizou o evento. O tipo de entidade que você deseja usar em suas previsões de fraude deve primeiro ser criado no Amazon Fraud Detector e depois adicionado ao evento ao criar seu tipo de evento.

Criar um tipo de entidade

Você pode criar um tipo de entidade no console do Amazon Fraud Detector, usando o put-entity-typecomando, usando a PutEntityTypeAPI ou usandoAWS SDK for Python (Boto3) o. Os exemplos abaixo criam um tipo de entidade`customer` no console do Amazon Fraud Detector e usando o SDK for Python (Boto3). Se você estiver criando um tipo de entidade para associar a um tipo de evento para treinar um modelo de detecção de fraudes, use o tipo de entidade do seu conjunto de dados de eventos que seja apropriado para seu caso de uso.

Crie um tipo de entidade usando o console Amazon Fraud Detector

Para criar um tipo de entidade,

1. Abra o AWSManagement Console e faça login em sua conta.
2. Navegue até o Amazon Fraud Detector, escolha Entidades no painel de navegação à esquerda e escolha Criar.
3. Na página Criar entidade, insira cliente como o nome do tipo de entidade. Opcionalmente, insira uma descrição da entidade.
4. Escolha Create entity (Criar entidade).

Crie um tipo de entidade usando oAWS SDK for Python (Boto3)

O exemploAWS SDK for Python (Boto3) de código a seguir usa a`PutEntityType` API para criar um tipo de entidade`customer`. Se você estiver criando um tipo de entidade para associar a um tipo de

evento para treinar um modelo de detecção de fraudes, use a entidade do seu conjunto de dados de eventos que seja apropriada para seu caso de uso.

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

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

Excluir um tipo de entidade

No Amazon Fraud Detector, não é possível excluir um tipo de entidade incluído em um tipo de evento. Você precisará primeiro excluir o tipo de evento ao qual a entidade está associada e depois excluir o tipo de entidade.

Quando você exclui um tipo de entidade, o Amazon Fraud Detector exclui permanentemente esse tipo de entidade e os dados não são mais armazenados no Amazon Fraud Detector.

Um tipo de entidade pode ser excluído no console do Amazon Fraud Detector, usando o delete-entity-typecomando, usando a DeleteEntityTypeAPI ou usando oAWS SDK for Python (Boto3)

Excluir um tipo de entidade no console do Amazon Fraud Detector

Para excluir um tipo de entidade,

1. Faça login noAWS Management Console e abra o console do Amazon Fraud Detector em https://console.aws.amazon.com/frauddetector.
2. No painel de navegação esquerdo do console do Amazon Fraud Detector, selecione Recursos e, em seguida, selecione Entidades.
3. Escolha o tipo de entidade do que você deseja excluir.
4. Escolha Actions (Ações) e, em seguida, escolha Delete (Excluir).
5. Insira o nome do tipo de entidade e escolha Excluir tipo de entidade.

Exclua o tipo de entidade usando oAWS SDK for Python (Boto3)

O código deAWS SDK for Python (Boto3) exemplo a seguir exclui o tipo de entidade cliente usando a DeleteEntityTypeAPI.

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

fraudDetector.delete_entity_type (

name = 'customer'

)
```

Gerencie os recursos do Amazon Fraud Detector usandoAWS CloudFormation

O AmazonAWS CloudFormation de Fraud Detector Fraud Detector Você um modelo que descreve todos os recursos desejados do do do do do do do do do do do do do do do do do do do do do do do do do do do do do do do do do do doAWS CloudFormation do do do do do do do do do do do. EntityType EventType Você pode reutilizar o modelo para provisionar e configurar os recursos de forma consistente e repetida em várias contas e regiões da AWS.

Não há cobrança adicional pelo uso da AWS CloudFormation.

Crias ud ud ud ud ud ud ud ud ud ud ud

Para o provisiondo do do o Amazon de do Fraud Detector do do do do do, você deve entender AWS CloudFormationos do. Os modelos são arquivos de texto formatados em JSON ou YAML. Esses modelos descrevem os recursos que você deseja provisionar nas suas pilhas do AWS CloudFormation. Se você não estiver familiarizado com JSON ou YAML, poderá usar o AWS CloudFormation Designer para ajudá-lo a começar a usar os modelos do AWS CloudFormation. Para obter mais informações, consulte O que é o Designer? (O que é o AWS CloudFormation Designer) no Manual do usuário do AWS CloudFormation.

Você você também pode você criar, da da da do Amazon de Fraud DetectorAWS CloudFormation Para obter mais informações, o do do do do do do do do do do do do do do do Amazon de do do do do do do do do do o do do no Guia do o doAWS CloudFormation usuário do do do do do do do do do do do do do do do do.

Se você já estiver usando CloudFormation, não há necessidade de gerenciar políticas ou CloudTrail registros adicionais do IAM.

Como o Amazon de Fraud Detector

Você pode criar, atualizar e excluir suas pilhas do Amazon Fraud Detector por meio do CloudFormation console ou da AWS CLI.

Para criar uma pilha, você deve ter um modelo que descreva quais recursos a AWS CloudFormation incluirá na pilha. Você também pode CloudFormation gerenciar os recursos do Amazon Fraud Detector que você já criou, importando-os para uma pilha nova ou existente.

Para obter instruções detalhadas sobre como gerenciar suas pilhas, consulte o GuiaAWS CloudFormation do usuário para saber como criar, atualizar e excluir pilhas.

Como o Amazon de Fraud Detector

A maneira como você organiza suasAWS CloudFormation pilhas depende inteiramente de você. Geralmente, a melhor prática é organizar as pilhas por ciclo de vida e propriedade. Isso significa agrupar recursos pela frequência com que eles mudam ou pelas equipes responsáveis por atualizá-los.

Você pode escolher organizar suas pilhas criando uma pilha para cada detector e sua lógica de detecção (por exemplo, regras, variáveis etc.). Se você estiver usando outros serviços, considere se deseja combinar os recursos do Amazon Fraud Detector com recursos de outros serviços. Por exemplo, você pode criar uma pilha que inclua recursos do Kinesis que ajudam a coletar dados e recursos do Amazon Fraud Detector que processam os dados. Essa pode ser uma forma eficaz de garantir que todos os produtos da sua equipe de fraude funcionem juntos.

entender os CloudFormation parâmetros do do Fraud Detector

Além dos parâmetros padrão que estão disponíveis em todos os CloudFormation modelos, o Amazon Fraud Detector apresenta dois parâmetros adicionais que ajudarão você a gerenciar o comportamento de implantação. Se você não incluir um ou ambos os parâmetros, CloudFormation usará o valor padrão mostrado abaixo.

Parâmetro	Valores	Valor padrão
DetectorVersionStatus	ATIVO: defina a versão nova/atualizada do detector para o status Ativo RASCUNHO: Defina a versão nova/atualizada do detector para o status de rascunho	RASCUNHO

Parâmetro	Valores	Valor padrão
Em linha	VERDADEIRO: CloudFormation permite criar/excluir o recurso ao criar/excluir o recurso ao criar/excluir a pilha. FALSO: Permite CloudFormation validar se o objeto existe, mas não fazer alterações no objeto.	TRUE

OAWS CloudFormation modelo do do do do do do do do do Fraud Detector

A seguir um exemplo do modelo deAWS CloudFormation YAML para o gerenciamento de um detector e as versões associadas do do detector do.

```
# 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'
```

Saiba mais sobre o AWS CloudFormation

Para saber mais sobre o AWS CloudFormation, consulte os seguintes recursos:

- AWS CloudFormation
- Manual do usuário do AWS CloudFormation
- AWS CloudFormation Referência da API
- Guia do usuário da interface de linha de comando do AWS CloudFormation

Previsões de fraude

Você pode usar o Amazon Fraud Detector para obter previsões de fraude para um único evento em tempo real ou obter previsões de fraudes off-line para um conjunto de eventos. Para gerar previsões de fraude para um único evento ou um conjunto de eventos, você precisará fornecer ao Amazon Fraud Detector as seguintes informações:

- Lógica de previsão de fraude
- Metadados de evento

Lógica de detecção de fraude

A lógica de previsão de fraudes usa uma ou mais regras para avaliar dados associados a um evento e, em seguida, fornece resultados e uma pontuação de previsão de fraudes. Você cria sua lógica de previsão de fraudes usando os seguintes componentes:

- Tipos de evento - Define a estrutura do evento
- Modelos - Define os requisitos de algoritmos e dados para prever fraudes
- Variáveis - Representa um elemento de dados associado ao evento
- Regras - define como o Amazon Fraud Detector como interpretará valores de variáveis durante a previsão de fraude
- Resultados - Resultados gerados a partir de uma previsão de fraude
- Versão do detector - Contém lógica de previsão de fraudes para um evento específico

Para obter mais informações sobre os componentes usados para criar a lógica de detecção de fraudes, consulte os conceitos do Amazon Fraud Detector. Antes de começar a gerar previsões de fraude, certifique-se de ter criado e publicado a versão do detector que contém sua lógica de previsão de fraudes. Você pode criar e publicar a versão do detector usando o Console ou a API do Fraud Detector. Para obter instruções sobre como usar o console, consulte Começar (console). Para obter instruções sobre como usar a API, consulte Criar uma versão do detector.

Metadados do evento

Os metadados do evento fornecem detalhes do evento que está sendo avaliado. Cada evento que você deseja avaliar deve incluir o valor de cada variável no tipo de evento associado à sua versão do detector. Além disso, os metadados de seu evento devem incluir o seguinte:

- EVENT_ID — Um identificador para o evento. Por exemplo, se seu evento for uma transação on-line, o EVENT_ID pode ser o número de referência da transação fornecido ao seu cliente.

  Notas importantes sobre EVENT_ID

  - Deve ser exclusivo para esse evento
  - Deve representar informações que sejam significativas para sua empresa
  - Deve satisfazer o padrão de expressão regular:`^[0-9a-z_-]+$.`
  - Deve ser salvo. EVENT_ID é a referência para o evento e é usado para realizar operações no evento, como excluir o evento.
  - Anexar timestamp ao EVENT_ID não é recomendado, pois isso pode causar problemas quando você quiser atualizar o evento posteriormente, pois você precisará fornecer exatamente o mesmo EVENT_ID.
- ENTITY_TYPE — A entidade que realiza o evento, como um lojista ou um cliente.
- ENTITY_ID - Um identificador para a entidade que executa o evento. O ENTITY_ID deve satisfazer o seguinte padrão de expressão regular:`^[0-9a-z_-]+$`. Se o ENTITY_ID não estiver disponível no momento da avaliação, passe a string unknown.
- EVENT_TIMESTAMP - o carimbo de data/hora em que o evento ocorreu. O carimbo de data/hora deve estar no padrão ISO 8601 em UTC.

Previsão em tempo real

Você pode avaliar atividades on-line em busca de fraudes em tempo real ligando para a`GetEventPrediction` API. Você fornece informações sobre um único evento em cada solicitação e recebe de forma síncrona uma pontuação do modelo e um resultado com base na lógica de previsão de fraudes associada ao detector especificado.

Como funciona a previsão de fraudes em tempo real

A`GetEventPrediction` API usa uma versão específica do detector para avaliar os metadados do evento fornecidos para o evento. Durante a avaliação, o Amazon Fraud Detector primeiro gera pontuações de modelo para modelos que são adicionados à versão do detector e, em seguida, passa os resultados para as regras de avaliação. As regras são executadas conforme especificado pelo modo de execução da regra (consulte Criar uma versão do detector). Como parte da resposta, o Amazon Fraud Detector fornece as pontuações do modelo, bem como quaisquer resultados associados às regras correspondentes.

Obtendo previsões de fraudes em tempo real

Para obter previsões de fraudes em tempo real, certifique-se de ter criado e publicado um detector que contenha seu modelo e regras de previsão de fraudes, ou simplesmente um conjunto de regras.

Você pode obter a previsão de fraudes para um evento em tempo real chamando a operação da GetEventPredictionAPI usando a interface de linha deAWS comando (AWSCLI) ou um dos SDKs do Amazon Fraud Detector.

Para usar a API, forneça informações de um único evento com cada solicitação. Como parte da solicitação, você deve especificar`detectorId` que o Amazon Fraud Detector usará para avaliar o evento. Opcionalmente, você pode especificar um`detectorVersionId`. Se`detectorVersionId` a não for especificado, o Amazon Fraud Detector usará a`ACTIVE` versão do detector.

Opcionalmente, você pode enviar dados para invocar um SageMaker modelo passando os dados no campo`externalModelEndpointBlobs`.

Obtenha uma previsão de fraude usando oAWS SDK for Python (Boto3)

Para gerar uma previsão de fraude, chame a`GetEventPrediction` API. O exemplo abaixo pressupõe que você tenha concluídoParte B: Gere previsões de fraudes. Como parte da resposta, você receberá uma pontuação do modelo, bem como todas as regras correspondentes e os resultados correspondentes. Você pode encontrar exemplos adicionais de`GetEventPrediction` solicitações no aws-fraud-detector-samples GitHub repositório.

```
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'
}
)
```

Previsões em lote

Você pode usar uma tarefa de previsões em lote no Amazon Fraud Detector para obter previsões para um conjunto de eventos que não exigem pontuação em tempo real. Por exemplo, você pode criar um trabalho de previsões em lote para realizar um trabalho off-line proof-of-concept ou para avaliar retrospectivamente o risco de eventos em uma base horária, diária ou semanal.

Você pode criar um trabalho de previsão em lote usando o console do Amazon Fraud Detector ou chamando a operação da CreateBatchPredictionJobAPI usando a interface de linha de AWS comando (AWSCLI) ou um dos SDKs do Amazon Fraud Detector.

Tópicos

Como funcionam as previsões em lote

A operação da `CreateBatchPredictionJob` API usa uma versão específica do detector para fazer previsões com base nos dados fornecidos em um arquivo CSV de entrada localizado em um bucket do Amazon S3. A API então retorna o arquivo CSV resultante em um bucket do S3.

Os trabalhos de previsão Batch calculam as pontuações do modelo e os resultados da previsão da mesma forma que a `GetEventPrediction` operação. Da mesma forma que`GetEventPrediction`, para criar um trabalho de previsões em lote, você primeiro cria um tipo de evento, opcionalmente treina um modelo e, em seguida, cria uma versão do detector que avalia os eventos em seu trabalho em lotes.

O preço das pontuações de risco de eventos avaliadas por trabalhos de previsão em lote é o mesmo que o preço das pontuações criadas pela `GetEventPrediction` API. Para obter detalhes, consulte os preços do Amazon Fraud Detector.

Você pode executar apenas um trabalho de previsão de lote de cada vez.

Arquivos de entrada e saída

O arquivo CSV de entrada deve conter cabeçalhos que correspondam ao tipo de evento associado à versão do detector selecionada. O tamanho máximo do arquivo de dados de entrada é de 1 GB. O número de eventos variará de acordo com o tamanho do seu evento.

O Amazon Fraud Detector cria o arquivo de saída no mesmo bucket do arquivo de entrada, a menos que você especifique um local separado para os dados de saída. O arquivo de saída contém os dados originais do arquivo de entrada e as seguintes colunas anexadas:

- `MODEL_SCORES`— Detalha as pontuações do modelo para o evento de cada modelo associado à versão do detector selecionada.
- `OUTCOMES`— Detalha os resultados do evento conforme avaliados pela versão selecionada do detector e suas regras.
- `STATUS`— Indica se o evento foi avaliado com sucesso. Se o evento não foi avaliado com êxito, essa coluna mostra um código do motivo da falha.
- `RULE_RESULTS`— Uma lista de todas as regras correspondentes, com base no modo de execução da regra.

Obter previsões em lote

As etapas a seguir pressupõem que você já tenha criado um tipo de evento, treinado um modelo usando esse tipo de evento (opcional) e criado uma versão de detector para esse tipo de evento.

Para obter uma previsão de lote

1. Faça login no AWS Management Console e abra o console do Amazon Fraud Detector em https://console.aws.amazon.com/frauddetector.
2. No painel de navegação esquerdo do console do Amazon Fraud Detector, escolha Previsões Batch e, em seguida, escolha Nova previsão em lote.
3. Em Nome do Job, especifique um nome para seu trabalho de previsão em lote. Se você não especificar um nome, o Amazon Fraud Detector gerará aleatoriamente um nome de trabalho.
4. Em Detector, escolha o detector para essa previsão de lote.
5. Na versão do detector, escolha a versão do detector para essa previsão em lote. Você pode escolher uma versão do detector em qualquer status. Se o detector tiver uma versão do detector

em `Active` status, essa versão será selecionada automaticamente, mas você também poderá alterar essa seleção, se necessário.

6. Na função IAM, escolha ou crie uma função que tenha acesso de leitura e gravação aos seus buckets de entrada e saída do Amazon S3. Consulte Orientação sobre funções do IAM para obter mais informações.

   Para obter previsões em lote, a função do IAM que chama a `CreateBatchPredictionJob` operação deve ter permissões de leitura no bucket do S3 de entrada e permissões de gravação no bucket do S3 de saída. Para obter mais informações sobre permissões de bucket, consulte exemplos de políticas de usuário no Guia do usuário do Amazon S3.
7. Em Localização dos dados de entrada, especifique a localização dos dados de entrada no Amazon S3. Se você quiser o arquivo de saída em um bucket S3 diferente, selecione Separar localização de dados para saída e forneça a localização do Amazon S3 para seus dados de saída.
8. (Opcional) Crie etiquetas para seu trabalho de previsão em lote.
9. Escolha Start (Iniciar).

   O Amazon Fraud Detector cria a tarefa de previsão em lote, e o status da tarefa é. `In progress` Os tempos de processamento do trabalho de previsão em Batch variam dependendo do número de eventos e da configuração da versão do detector.

Para interromper um trabalho de previsão em lote que está em andamento, acesse a página de detalhes do trabalho de previsão em lote, escolha Ações e escolha Interromper previsão em lote. Se você interromper um trabalho de previsão em lote, não receberá nenhum resultado do trabalho.

Quando o status do trabalho de previsão em lote muda para`Complete`, você pode recuperar a saída do trabalho do bucket de saída designado do Amazon S3. O nome do arquivo de saída está no formato`batch prediction job name_file creation timestamp_output.csv`. Por exemplo, o arquivo de saída de um trabalho chamado `mybatchjob` é`mybatchjob_1611170650_output.csv`.

Para pesquisar eventos específicos avaliados por um trabalho de previsão em lote, no painel de navegação esquerdo do console do Amazon Fraud Detector, escolha Pesquisar previsões anteriores.

Para excluir um trabalho de previsão em lote concluído, acesse a página de detalhes do trabalho de previsão em lote, escolha Ações e escolha Excluir previsão em lote.

Orientação sobre funções do IAM

Para obter previsões em lote, a função do IAM que chama a CreateBatchPredictionJoboperação deve ter permissões de leitura no bucket do S3 de entrada e permissões de gravação no bucket do S3 de saída. Para obter mais informações sobre permissões de bucket, consulte Exemplos de políticas do usuário no Guia do usuário do Amazon S3. No console do Amazon Fraud Detector, você tem três opções para selecionar uma função do IAM para previsões Batch:

1. Crie uma função ao criar um novo trabalho de previsão em lote.
2. Selecione uma função do IAM existente que você criou anteriormente no console do Amazon Fraud Detector. Certifique-se de adicionar a `S3:PutObject` permissão à função antes de executar essa etapa.
3. Insira um ARN personalizado para uma função do IAM criada anteriormente.

Se você receber um erro relacionado à sua função do IAM, faça o seguinte:

1. Seus bucket de entrada e saída do Amazon S3 estão na mesma região que seu detector.
2. A função do IAM que você está usando tem a `s3:GetObject` permissão para seu bucket de entrada do S3 e a `s3:PutObject` permissão para o bucket do S3 de saída.
3. A função do IAM que você está usando tem uma política de confiança para o responsável pelo serviço`frauddetector.amazonaws.com`.

Obtenha previsões de fraudes em lote usando o AWS SDK for Python (Boto3)

O exemplo a seguir mostra uma solicitação de exemplo para a CreateBatchPredictionJobAPI. Uma tarefa de previsão em lote deve incluir os seguintes recursos existentes: detector, versão do detector e nome do tipo de evento. O exemplo a seguir pressupõe que você tenha criado um tipo de evento`sample_registration`, um detector e uma `sample_detector` versão do detector. 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-
**'
)
```

Explicações de previsão

As explicações de previsão fornecem informações sobre como cada variável de evento afetou a pontuação de previsão de fraude do seu modelo e são geradas automaticamente como parte da previsão de fraude. Cada previsão de fraude vem com uma pontuação de risco entre 1 e 1000. As explicações de previsão fornecem detalhes da influência de cada variável do evento nas pontuações de risco em termos de magnitude (0-5, sendo 5 a mais alta) e direção (a pontuação do impulso é maior ou menor). Você também pode usar explicações de previsão para as seguintes tarefas:

- Identificar os principais indicadores de risco durante as inverstigações manuais, quando um evento é sinalizado para análise.
- Para restringir as causas-raiz que levam a previsões falsas positivas (por exemplo, pontuações de alto risco para eventos legítimos).
- Para analisar padrões de fraude em dados de eventos e detectar preconceitos, se houver, em seu conjunto de dados.

> **Important**
>
> As explicações de previsão são geradas automaticamente e estão disponíveis somente para modelos treinados em ou após 30 de junho de 2021. Para receber explicações de previsão para modelos treinados antes de 30 de junho de 2021, treine novamente esses modelos.

As explicações de predição fornecem o seguinte conjunto de valores para cada variável de evento usada para treinar o modelo.

Impacto relativo

Fornece uma referência visual do impacto da variável em termos de magnitude nas pontuações de previsão de fraudes. Os valores de impacto relativo consistem em uma classificação por estrelas (0-5, sendo 5 a mais alta) e no impacto direcional (aumentado/diminuído) do risco de fraude.

- As variáveis que aumentam o risco de fraude são indicadas por estrelas vermelhas. Quanto maior o número de estrelas vermelhas, mais a variável aumenta a pontuação de fraude e aumenta a probabilidade de fraude.
- As variáveis que diminuíram o risco de fraude são indicadas por estrelas verdes. Quanto maior o número de inícios verdes, mais a variável reduz a pontuação de risco de fraude e diminui a probabilidade de fraude.
- Zero estrelas para todas as variáveis indicam que nenhuma das variáveis, por si só, alterou significativamente o risco de fraude.

Valor bruto da explicação

Fornece valor bruto e não interpretado, representado como probabilidades logarítmicas da fraude. Esses valores geralmente estão entre -10 a +10, mas variam de - infinito a + infinito.

- Um valor positivo indica que a variável aumentou a pontuação de risco.
- Um valor negativo indica que a variável reduziu a pontuação de risco.

No console do Amazon Fraud Detector, os valores da explicação da previsão são exibidos da seguinte forma. As classificações por estrelas coloridas e os valores numéricos brutos correspondentes facilitam a visualização da influência relativa entre as variáveis.

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

Visualizando explicações de previsão

Depois de gerar previsões de fraude, você pode ver as explicações das previsões no console do Amazon Fraud Detector. Para ver as explicações de previsão usando APIs do AWS SDK, você deve primeiro chamar a `ListEventPrediction` API para obter a data e hora da previsão do evento e, em seguida, chamar a `GetEventPredictionMetadata` API para obter as explicações da previsão.

Veja explicações de previsão usando o console Amazon Fraud Detector

Para ver as explicações de previsão usando o console,

1. Abra o AWS console e faça login na sua conta. Navegue até o Amazon Fraud Detector.
2. No painel de navegação esquerdo, escolha Pesquisar previsões anteriores.
3. Use os filtros Propriedade, Operador e Valor para selecionar a previsão que você deseja revisar.

4. No painel superior do Filtro, certifique-se de selecionar o período em que a previsão que você deseja revisar foi gerada.
5. O painel Resultados exibe uma lista de todas as previsões geradas durante o período especificado. Clique no ID do evento da previsão para ver as explicações da previsão.
6. Role para baixo até o painel Explicações de previsão.
7. Defina o botão Mostrar valor bruto da explicação da predição para visualizar o valor bruto da explicação da predição de todas as variáveis.

Veja explicações de previsão usando o AWS SDK para Python (Boto3) (SDK for Python)

Os exemplos a seguir mostram exemplos de solicitações para visualizar explicações de previsão usando `ListEventPredictions` `GetEventPredictionMetadata` APIs do AWS SDK.

Exemplo 1: obtenha uma lista das previsões mais recentes usando **`ListEventPredictions`** a API

```
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'
    }
 )
```

Exemplo 2; Obtenha uma lista de previsões anteriores para o tipo de evento “registro” usando **`ListEventPredictions`** a API

```
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'
    }
 )
```

Exemplo 3: Obtenha detalhes de uma previsão anterior para um ID de evento específico, tipo de evento, ID do detector e ID da versão do detector que foi gerado no período especificado usando a **`GetEventPredictionMetadata`** API.

O `predictionTimestamp` especificado para essa solicitação é obtido chamando primeiro a `ListEventPredictions` API.

```
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'
 )
```

Entendendo como as explicações de previsão são calculadas

O Amazon Fraud Detector usa SHAP (ShapeLey Additive Explanations) para explicar previsões de eventos individuais, calculando os valores brutos de explicação de cada variável de evento usada para treinamento de modelos. Os valores brutos da explicação são calculados pelo modelo como parte do algoritmo de classificação ao gerar previsões. Esses valores brutos de explicação representam a contribuição de cada entrada para o logaritmo das chances de fraude. Os valores brutos da explicação (de -infinito a +infinito) são convertidos em um valor de impacto relativo (-5 a +5) usando um mapeamento. O valor de impacto relativo derivado do valor bruto da explicação representa o aumento do número de vezes nas chances de fraude (positiva) ou legítima (negativa), facilitando a compreensão das explicações da previsão.

Segurança no Amazon Fraud Detector

A segurança na nuvem AWS é a maior prioridade. Como AWS cliente, você se beneficia de data centers e arquiteturas de rede criados para atender aos requisitos das organizações mais sensíveis à segurança.

A segurança é uma responsabilidade compartilhada entre você AWS e você. O modelo de responsabilidade compartilhada descreve isso como a segurança da nuvem e segurança na nuvem:

- Segurança da nuvem — AWS é responsável por proteger a infraestrutura que executa AWS os serviços na AWS nuvem. AWS também fornece serviços que você pode usar com segurança. Auditores terceirizados testam e verificam regularmente a eficácia de nossa segurança como parte dos Programas de Conformidade Programas de AWS de . Para saber mais sobre os programas de conformidade que se aplicam ao Amazon Fraud Detector, consulte AWS Services in Scope by Compliance Program .
- Segurança na nuvem — Sua responsabilidade é determinada pelo AWS serviço que você usa. Você também é responsável por outros fatores, incluindo a confidencialidade de seus dados, os requisitos da empresa e as leis e regulamentos aplicáveis.

Essa documentação ajuda você a entender como aplicar o modelo de responsabilidade compartilhada ao usar o Amazon Fraud Detector. Os tópicos a seguir mostram como configurar o Amazon Fraud Detector para atender aos seus objetivos de segurança e conformidade. Você também aprenderá a usar outros AWS serviços que ajudam a monitorar e proteger seus recursos do Amazon Fraud Detector.

Tópicos

Proteção de dados no Amazon Fraud Detector

O modelo de responsabilidade AWS compartilhada se aplica à proteção de dados no Amazon Fraud Detector. Conforme descrito neste modelo, AWS é responsável por proteger a infraestrutura global que executa todos os Nuvem AWS. Você é responsável por manter o controle sobre seu conteúdo hospedado nessa infraestrutura. Você também é responsável pelas tarefas de configuração e gerenciamento de segurança dos Serviços da AWS que usa. Para ter mais informações sobre a privacidade de dados, consulte as Perguntas frequentes sobre privacidade de dados. Para ter mais informações sobre a proteção de dados na Europa, consulte a AWS postagem do blog Shared Responsibility Model and GDPR no AWS Blog de segurança da.

Para fins de proteção de dados, recomendamos que você proteja Conta da AWS as credenciais e configure usuários individuais com AWS IAM Identity Center ou AWS Identity and Access Management (IAM). Dessa maneira, cada usuário receberá apenas as permissões necessárias para cumprir suas obrigações de trabalho. Recomendamos também que você proteja seus dados das seguintes formas:

- Use uma autenticação multifator (MFA) com cada conta.
- Use SSL/TLS para se comunicar com os recursos. AWS Exigimos TLS 1.2 e recomendamos TLS 1.3.
- Configure a API e o registro de atividades do usuário com AWS CloudTrail.
- Use soluções de AWS criptografia, juntamente com todos os controles de segurança padrão Serviços da AWS.
- Use serviços gerenciados de segurança avançada, como o Amazon Macie, que ajuda a localizar e proteger dados sigilosos armazenados no Amazon S3.
- Se você precisar de módulos criptográficos validados pelo FIPS 140-2 ao acessar AWS por meio de uma interface de linha de comando ou de uma API, use um endpoint FIPS. Para ter mais informações sobre endpoints do FIPS, consulte Federal Information Processing Standard (FIPS) 140-2.

É altamente recomendável que nunca sejam colocadas informações de identificação confidenciais, como endereços de email dos seus clientes, em marcações ou campos de formato livre, como um campo Name (Nome). Isso inclui quando você trabalha com o Amazon Fraud Detector ou outro Serviços da AWS usando o console, a API ou AWS os SDKs. AWS CLI Quaisquer dados inseridos em tags ou campos de texto de formato livre usados para nomes podem ser usados para logs de faturamento ou de diagnóstico. Se você fornecer um URL para um servidor externo, recomendemos

fortemente que não sejam incluídas informações de credenciais no URL para validar a solicitação a esse servidor.

Criptografar dados em repouso

O Amazon Fraud Detector criptografa seus dados em repouso com a chave de criptografia de sua escolha. Você pode escolher uma das seguintes opções:

- Uma AWS chave KMS própria. Se você não especificar uma chave de criptografia, os dados serão criptografados com essa chave por padrão.
- Uma chave KMS gerenciada pelo cliente. Você pode controlar o acesso à sua chave KMS gerenciada pelo cliente usando as principais políticas. Para obter informações sobre como criar e gerenciar a chave KMS gerenciada pelo cliente, consulteGerenciamento de chaves.

Criptografia de dados em trânsito

O Amazon Fraud Detector copia dados da sua conta e os processa em um AWS sistema interno. Por padrão, o Amazon Fraud Detector usa o TLS 1.2 com AWS certificados para criptografar dados em trânsito.

Gerenciamento de chaves

O Amazon Fraud Detector criptografa seus dados usando um dos dois tipos de chaves:

- Uma AWS chave KMS própria. Esse é o padrão.
- Uma chave KMS gerenciada pelo cliente.

Criação de uma chave KMS gerenciada pelo cliente

Você pode criar uma chave KMS gerenciada pelo cliente usando o console AWS KMS ou a CreateKeyAPI. Ao criar a chave, certifique-se de

- Selecione uma chave KMS de criptografia simétrica gerenciada pelo cliente. O Amazon Fraud Detector não suporta chaves KMS assimétricas. Para obter mais informações, consulte Chaves assimétricas AWS KMS no Guia do desenvolvedor do AWS Key Management Service.
- Crie uma chave KMS de região única. O Amazon Fraud Detector não oferece suporte a chaves KMS multirregionais. Para obter mais informações, consulte Chaves multirregionais AWS KMS no Guia do desenvolvedor do AWS Key Management Service.

- Forneça a seguinte política de chaves para conceder permissões ao Amazon Fraud Detector para usar a chave.

```
        {
    "Effect": "Allow",
    "Principal": {
        "Service": "frauddetector.amazonaws.com"
    },
    "Action": [
        "kms:Encrypt",
        "kms:Decrypt",
        "kms:ReEncrypt*",
        "kms:GenerateDataKey*",
        "kms:DescribeKey",
        "kms:CreateGrant",
        "kms:RetireGrant"
    ],
    "Resource": "*"
}
```

  Para obter informações sobre as principais políticas, consulte Usando políticas de chaves no AWS KMS no Guia do desenvolvedor do AWS Key Management Service.

Criptografando dados usando a chave KMS gerenciada pelo cliente

Use a EncryptionKey API putKMS do Amazon Fraud Detector para criptografar seus dados do Amazon Fraud Detector em repouso usando a chave KMS gerenciada pelo cliente. Você pode alterar a configuração de criptografia a qualquer momento usando a `PutKMSEncryptionKey` API.

Notas importantes sobre dados criptografados

- Os dados gerados após a configuração da chave KMS gerenciada pelo cliente são criptografados. Os dados gerados antes da configuração da chave KMS gerenciada pelo cliente permanecerão sem criptografia.
- Se a chave KMS gerenciada pelo cliente for alterada, os dados que foram criptografados usando a configuração de criptografia anterior não serão criptografados novamente.

Visualizar dados

Quando você usa a chave KMS gerenciada pelo cliente para criptografar seus dados do Amazon Fraud Detector, os dados criptografados usando esse método não podem ser pesquisados usando filtros na área Pesquisar previsões passadas do console do Amazon Fraud Detector. Para garantir resultados de pesquisa completos, use uma ou mais das seguintes propriedades para filtrar os resultados:

- ID do evento
- Carimbo de data/hora da avaliação
- Status do detector
- Versão do detector
- Versão do modelo
- Tipo do modelo
- Status de avaliação da regra
- Modo de execução de regras
- Status da correspondência de regras
- Versão da regra
- Fonte de dados variável

Se a chave KMS gerenciada pelo cliente foi excluída ou está programada para exclusão, seus dados podem não estar disponíveis. Para obter mais informações, consulte Excluindo a chave KMS.

Amazon Fraud Detector e interface de VPC endpoints ()AWS PrivateLink

Você pode estabelecer uma conexão privada entre sua VPC e o Amazon Fraud Detector criando uma interface VPC endpoint. Os endpoints de interface são alimentados por AWS PrivateLinkuma tecnologia que permite acessar de forma privada as APIs do Amazon Fraud Detector sem um gateway de internet, dispositivo NAT, conexão VPN ou conexão com o AWS Direct Connect. As instâncias em sua VPC não precisam de endereços IP públicos para se comunicarem com as APIs do Amazon Fraud Detector. O tráfego entre sua VPC e o Amazon Fraud Detector não sai da rede Amazon.

Cada endpoint de interface é representado por uma ou mais Interfaces de Rede Elástica nas sub-redes.

Para obter mais informações, consulte Interface VPC endpoints (AWS PrivateLink) no Guia do usuário da Amazon VPC.

Considerações sobre os endpoints VPC do Amazon Fraud Detector

Antes de configurar uma interface VPC endpoint para o Amazon Fraud Detector, certifique-se de revisar as propriedades e limitações do endpoint da interface no Guia do usuário do Amazon VPC.

O Amazon Fraud Detector oferece suporte para fazer chamadas para todas as suas ações de API a partir de sua VPC.

As políticas de VPC endpoint são compatíveis com o Amazon Fraud Detector. Por padrão, o acesso total ao Amazon Fraud Detector é permitido por meio do endpoint. Para mais informações, consulte Controlar o acesso a serviços com VPC endpoints no Guia do usuário da Amazon VPC.

Criação de uma interface VPC endpoint para o Amazon Fraud Detector

Você pode criar um VPC endpoint para o serviço Amazon Fraud Detector usando o console Amazon VPC ou o (). AWS Command Line Interface AWS CLI Para mais informações, consulte Criar um endpoint de interface no Guia do usuário da Amazon VPC.

Crie um VPC endpoint para o Amazon Fraud Detector usando o seguinte nome de serviço:

- com.amazonaws.*region*.frauddetector

Se você habilitar o DNS privado para o endpoint, poderá fazer solicitações de API ao Amazon Fraud Detector usando seu nome DNS padrão para a região, por exemplo,. `frauddetector.us-east-1.amazonaws.com`

Para mais informações, consulte Acessar um serviço por um endpoint de interface no Guia do usuário da Amazon VPC.

Criação de uma política de VPC endpoint para o Amazon Fraud Detector

Você pode criar uma política para endpoints VPC de interface para o Amazon Fraud Detector para especificar o seguinte:

- A entidade principal que pode executar ações
- As ações que podem ser executadas
- Os recursos nos quais as ações podem ser executadas

Para obter mais informações, consulte Controlar o acesso a serviços com VPC endpoints no Guia do usuário da Amazon VPC.

O exemplo de política de VPC endpoint a seguir especifica que todos os usuários que têm acesso ao endpoint da interface VPC têm permissão para acessar o detector de Fraud Detector da Amazon chamado. `my_detector`

```
{
  "Statement": [
      {
          "Action": "frauddetector:*Detector",
          "Effect": "Allow",
          "Resource": "arn:aws:frauddetector:us-east-1:123456789012:detector/
my_detector",
          "Principal": "*"
      }
  ]
}
```

Neste exemplo, as opções a seguir são negadas:

- Outras ações da API Amazon Fraud Detector
- Invocando a API Amazon Fraud Detector `GetEventPrediction`

> **Note**
>
> Neste exemplo, os usuários ainda podem realizar outras ações da API Amazon Fraud Detector de fora da VPC. Para obter informações sobre como restringir chamadas de API àquelas da VPC, consulte Políticas baseadas em identidade do Amazon Fraud Detector.

Optar por não usar seus dados para melhorar o serviço

Os dados históricos de eventos que você fornece para treinar modelos e gerar previsões são usados exclusivamente para fornecer e manter seu serviço. Esses dados também podem ser usados para melhorar a qualidade do Amazon Fraud Detector. Sua confiança, privacidade e segurança de seu conteúdo são nossa maior prioridade e garantem que nosso uso esteja em conformidade com nossos compromissos com você. Consulte Perguntas frequentes sobre privacidade de dados para obter mais informações

Você pode optar por não ter os dados do seu evento usados para desenvolver ou melhorar a qualidade do Amazon Fraud Detector visitando a página de políticas de exclusão de serviços de IA no Guia do Usuário do AWS Organizations e seguindo o processo explicado lá.

> **Note**
>
> Suas contas da AWS precisarão ser gerenciadas centralmente pelo AWS Organizations para que você possa usar a política de exclusão. Se você ainda não criou uma organização para suas contas da AWS, acesse a página Criar e gerenciar uma organização e siga o processo explicado lá.

Gerenciamento de identidade e acesso para o Amazon Fraud Detector

AWS Identity and Access Management (IAM) é uma ferramenta AWS service (Serviço da AWS) que ajuda o administrador a controlar com segurança o acesso aos AWS recursos. Os administradores do IAM controlam quem pode ser autenticado (conectado) e autorizado (tem permissões) para usar os recursos do Amazon Fraud Detector. O IAM é um AWS service (Serviço da AWS) que você pode usar sem custo adicional.

Tópicos

Público

A forma como você usa AWS Identity and Access Management (IAM) é diferente, dependendo do trabalho que você faz no Amazon Fraud Detector.

Usuário do serviço — Se você usa o serviço Amazon Fraud Detector para fazer seu trabalho, seu administrador fornecerá as credenciais e as permissões de que você precisa. À medida que você usa mais recursos do Amazon Fraud Detector para fazer seu trabalho, talvez precise de permissões adicionais. Entender como o acesso é gerenciado pode ajudar você a solicitar as permissões corretas ao seu administrador. Se você não conseguir acessar um recurso no Amazon Fraud Detector, consulteSolução de problemas de identidade e acesso ao Amazon Fraud Detector.

Administrador de serviços — Se você é responsável pelos recursos do Amazon Fraud Detector em sua empresa, provavelmente tem acesso total ao Amazon Fraud Detector. É seu trabalho determinar quais recursos e recursos do Amazon Fraud Detector seus usuários do serviço devem acessar. Assim, você deve enviar solicitações ao administrador do IAM para alterar as permissões dos usuários de seu serviço. Revise as informações nesta página para entender os Introdução ao IAM. Para saber mais sobre como sua empresa pode usar o IAM com o Amazon Fraud Detector, consulteComo o Amazon Fraud Detector funciona com o IAM.

Administrador do IAM — Se você for administrador do IAM, talvez queira saber detalhes sobre como criar políticas para gerenciar o acesso ao Amazon Fraud Detector. Para ver exemplos de políticas baseadas em identidade do Amazon Fraud Detector que você pode usar no IAM, consulte. Exemplos de políticas baseadas em identidade do Amazon Fraud Detector

Autenticando com identidades

A autenticação é como você faz login AWS usando suas credenciais de identidade. Você deve estar autenticado (conectado AWS) como o Usuário raiz da conta da AWS, como usuário do IAM ou assumindo uma função do IAM.

Você pode entrar AWS como uma identidade federada usando credenciais fornecidas por meio de uma fonte de identidade. AWS IAM Identity Center Usuários (IAM Identity Center), a autenticação de login único da sua empresa e suas credenciais do Google ou do Facebook são exemplos de identidades federadas. Quando você faz login como uma identidade federada, o administrador já configurou anteriormente a federação de identidades usando perfis do IAM. Ao acessar AWS usando a federação, você está assumindo indiretamente uma função.

Dependendo do tipo de usuário que você é, você pode entrar no AWS Management Console ou no portal de AWS acesso. Para obter mais informações sobre como fazer login em AWS, consulte Como fazer login Conta da AWS no Guia do Início de Sessão da AWS usuário.

Se você acessar AWS programaticamente, AWS fornece um kit de desenvolvimento de software (SDK) e uma interface de linha de comando (CLI) para assinar criptograficamente suas solicitações

usando suas credenciais. Se você não usa AWS ferramentas, você mesmo deve assinar as solicitações. Para obter mais informações sobre como usar o método recomendado para assinar solicitações por conta própria, consulte Assinatura de solicitações de AWS API no Guia do usuário do IAM.

Independentemente do método de autenticação usado, também pode ser exigido que você forneça informações adicionais de segurança. Por exemplo, AWS recomenda que você use a autenticação multifator (MFA) para aumentar a segurança da sua conta. Para saber mais, consulte Autenticação multifator no Guia do usuário do AWS IAM Identity Center . Usar a autenticação multifator (MFA) na AWS no Guia do usuário do IAM.

Conta da AWS usuário root

Ao criar uma Conta da AWS, você começa com uma identidade de login que tem acesso completo a todos Serviços da AWS os recursos da conta. Essa identidade é chamada de usuário Conta da AWS raiz e é acessada fazendo login com o endereço de e-mail e a senha que você usou para criar a conta. É altamente recomendável não usar o usuário-raiz para tarefas diárias. Proteja as credenciais do usuário-raiz e use-as para executar as tarefas que somente ele pode executar. Para obter a lista completa das tarefas que exigem login como usuário-raiz, consulte Tarefas que exigem credenciais de usuário-raiz no Guia do usuário do IAM.

Usuários e grupos

Um usuário do IAM é uma identidade dentro da sua Conta da AWS que tem permissões específicas para uma única pessoa ou aplicativo. Sempre que possível, recomendamos depender de credenciais temporárias em vez de criar usuários do IAM com credenciais de longo prazo, como senhas e chaves de acesso. No entanto, se você tiver casos de uso específicos que exijam credenciais de longo prazo com usuários do IAM, recomendamos alternar as chaves de acesso. Para obter mais informações, consulte Alterne as chaves de acesso regularmente para casos de uso que exijam credenciais de longo prazo no Guia do usuário do IAM.

Um grupo do IAM é uma identidade que especifica uma coleção de usuários do IAM. Não é possível fazer login como um grupo. É possível usar grupos para especificar permissões para vários usuários de uma vez. Os grupos facilitam o gerenciamento de permissões para grandes conjuntos de usuários. Por exemplo, você pode ter um grupo chamado IAMAdmins e atribuir a esse grupo permissões para administrar atributos do IAM.

Usuários são diferentes de perfis. Um usuário é exclusivamente associado a uma pessoa ou a uma aplicação, mas um perfil pode ser assumido por qualquer pessoa que precisar dele. Os usuários

têm credenciais permanentes de longo prazo, mas os perfis fornecem credenciais temporárias. Para saber mais, consulte Quando criar um usuário do IAM (em vez de um perfil) no Guia do usuário do IAM.

Perfis do IAM

Uma função do IAM é uma identidade dentro da sua Conta da AWS que tem permissões específicas. Ele é semelhante a um usuário do IAM, mas não está associado a uma pessoa específica. Você pode assumir temporariamente uma função do IAM no AWS Management Console trocando de funções. Você pode assumir uma função chamando uma operação de AWS API AWS CLI ou usando uma URL personalizada. Para obter mais informações sobre métodos para o uso de perfis, consulte Usar perfis do IAM no Guia do usuário do IAM.

Perfis do IAM com credenciais temporárias são úteis nas seguintes situações:

- Acesso de usuário federado: para atribuir permissões a identidades federadas, você pode criar um perfil e definir permissões para ele. Quando uma identidade federada é autenticada, essa identidade é associada ao perfil e recebe as permissões definidas pelo mesmo. Para obter mais informações sobre perfis para federação, consulte Criar um perfil para um provedor de identidades de terceiros no Guia do usuário do IAM. Se você usar o IAM Identity Center, configure um conjunto de permissões. Para controlar o que suas identidades podem acessar após a autenticação, o IAM Identity Center correlaciona o conjunto de permissões a um perfil no IAM. Para obter informações sobre conjuntos de permissões, consulte Conjuntos de permissões noAWS IAM Identity Center Guia do usuário do .
- Permissões temporárias para usuários do IAM: um usuário ou um perfil do IAM pode assumir um perfil do IAM para obter temporariamente permissões diferentes para uma tarefa específica.
- Acesso entre contas: é possível usar um perfil do IAM para permitir que alguém (uma entidade principal confiável) em outra conta acesse recursos em sua conta. Os perfis são a principal forma de conceder acesso entre contas. No entanto, com alguns Serviços da AWS, você pode anexar uma política diretamente a um recurso (em vez de usar uma função como proxy). Para saber a diferença entre perfis e políticas baseadas em atributo para acesso entre contas, consulte Como os perfis do IAM diferem das políticas baseadas em atributo no Guia do usuário do IAM.
- Acesso entre serviços — Alguns Serviços da AWS usam recursos em outros Serviços da AWS. Por exemplo, quando você faz uma chamada em um serviço, é comum que esse serviço execute aplicações no Amazon EC2 ou armazene objetos no Amazon S3. Um serviço pode fazer isso usando as permissões da entidade principal de chamada, usando um perfil de serviço ou uma função vinculada ao serviço.

- Sessões de acesso direto (FAS) — Quando você usa um usuário ou uma função do IAM para realizar ações AWS, você é considerado principal. Ao usar alguns serviços, você pode executar uma ação que inicia outra ação em um serviço diferente. O FAS usa as permissões do diretor chamando um AWS service (Serviço da AWS), combinadas com a solicitação AWS service (Serviço da AWS) para fazer solicitações aos serviços posteriores. As solicitações do FAS são feitas somente quando um serviço recebe uma solicitação que requer interações com outros Serviços da AWS ou com recursos para ser concluída. Nesse caso, você precisa ter permissões para executar ambas as ações. Para obter detalhes da política ao fazer solicitações de FAS, consulte Encaminhar sessões de acesso.
- Perfil de serviço: um perfil de serviço é um perfil do IAMhttps://docs.aws.amazon.com/IAM/latest/UserGuide/id_roles.html que um serviço assume para realizar ações em seu nome. Um administrador do IAM pode criar, modificar e excluir um perfil de serviço do IAM. Para obter mais informações, consulte Criar um perfil para delegar permissões a um AWS service (Serviço da AWS) no Guia do usuário do IAM.
- Função vinculada ao serviço — Uma função vinculada ao serviço é um tipo de função de serviço vinculada a um. AWS service (Serviço da AWS) O serviço pode assumir o perfil de executar uma ação em seu nome. As funções vinculadas ao serviço aparecem em você Conta da AWS e são de propriedade do serviço. Um administrador do IAM pode visualizar, mas não pode editar as permissões para perfis vinculados ao serviço.

- Aplicativos em execução no Amazon EC2 — Você pode usar uma função do IAM para gerenciar credenciais temporárias para aplicativos que estão sendo executados em uma instância do EC2 e fazendo AWS CLI solicitações de API. AWS É preferível fazer isso a armazenar chaves de acesso na instância do EC2. Para atribuir uma AWS função a uma instância do EC2 e disponibilizá-la para todos os seus aplicativos, você cria um perfil de instância anexado à instância. Um perfil de instância contém a perfil e permite que os programas em execução na instância do EC2 obtenham credenciais temporárias. Para mais informações, consulte Usar um perfil do IAM para conceder permissões a aplicações em execução nas instâncias do Amazon EC2 no Guia do usuário do IAM.

Para saber se deseja usar as funções do IAM, consulte Quando criar um perfil do IAM (em vez de um usuário) no Guia do usuário do IAM.

Gerenciamento do acesso usando políticas

Você controla o acesso AWS criando políticas e anexando-as a AWS identidades ou recursos. Uma política é um objeto AWS que, quando associada a uma identidade ou recurso, define suas permissões. AWS avalia essas políticas quando um principal (usuário, usuário raiz ou sessão de

função) faz uma solicitação. As permissões nas políticas determinam se a solicitação será permitida ou negada. A maioria das políticas é armazenada AWS como documentos JSON. Para obter mais informações sobre a estrutura e o conteúdo de documentos de políticas JSON, consulte Visão geral das políticas JSON no Guia do usuário do IAM.

Os administradores podem usar políticas AWS JSON para especificar quem tem acesso ao quê. Ou seja, qual entidade principal pode executar ações em quais recursos e em que condições.

Por padrão, usuários e funções não têm permissões. Para conceder aos usuários permissão para executar ações nos recursos de que eles precisam, um administrador do IAM pode criar políticas do IAM. O administrador pode então adicionar as políticas do IAM a perfis, e os usuários podem assumir os perfis.

As políticas do IAM definem permissões para uma ação, independentemente do método usado para executar a operação. Por exemplo, suponha que você tenha uma política que permite a ação `iam:GetRole`. Um usuário com essa política pode obter informações de função da AWS Management Console AWS CLI, da ou da AWS API.

Políticas baseadas em identidade

As políticas baseadas em identidade são documentos de políticas de permissões JSON que você pode anexar a uma identidade, como usuário do IAM, grupo de usuários ou perfil do IAM. Essas políticas controlam quais ações os usuários e funções podem realizar, em quais recursos e em que condições. Para saber como criar uma política baseada em identidade, consulte Criar políticas do IAM no Guia do usuário do IAM.

As políticas baseadas em identidade podem ser categorizadas ainda mais como políticas em linha ou políticas gerenciadas. As políticas em linha são anexadas diretamente a um único usuário, grupo ou perfil. As políticas gerenciadas são políticas autônomas que você pode associar a vários usuários, grupos e funções em seu Conta da AWS. As políticas AWS gerenciadas incluem políticas gerenciadas e políticas gerenciadas pelo cliente. Para saber como escolher entre uma política gerenciada ou uma política em linha, consulte Escolher entre políticas gerenciadas e políticas em linha no Guia do usuário do IAM.

Políticas baseadas em recursos

Políticas baseadas em recursos são documentos de políticas JSON que você anexa a um recurso. São exemplos de políticas baseadas em recursos as políticas de confiança de perfil do IAM e as políticas de bucket do Amazon S3. Em serviços compatíveis com políticas baseadas em recursos,

os administradores de serviço podem usá-las para controlar o acesso a um recurso específico. Para o atributo ao qual a política está anexada, a política define quais ações uma entidade principal especificada pode executar nesse atributo e em que condições. Você deve especificar uma entidade principal em uma política baseada em recursos. Os diretores podem incluir contas, usuários, funções, usuários federados ou. Serviços da AWS

Políticas baseadas em atributos são políticas em linha que estão localizadas nesse serviço. Você não pode usar políticas AWS gerenciadas do IAM em uma política baseada em recursos.

Listas de controle de acesso (ACLs)

As listas de controle de acesso (ACLs) controlam quais entidades principais (membros, usuários ou funções da conta) têm permissões para acessar um recurso. As ACLs são semelhantes às políticas baseadas em recursos, embora não usem o formato de documento de política JSON.

O Amazon S3 e o Amazon VPC são exemplos de serviços que oferecem suporte a ACLs. AWS WAF Para saber mais sobre ACLs, consulte Visão geral da lista de controle de acesso (ACL) no Guia do desenvolvedor do Amazon Simple Storage Service.

Outros tipos de política

AWS oferece suporte a tipos de políticas adicionais menos comuns. Esses tipos de política podem definir o máximo de permissões concedidas a você pelos tipos de política mais comuns.

- Limites de permissões: um limite de permissões é um recurso avançado no qual você define o máximo de permissões que uma política baseada em identidade pode conceder a uma entidade do IAM (perfil ou usuário do IAM). É possível definir um limite de permissões para uma entidade. As permissões resultantes são a interseção das políticas baseadas em identidade de uma entidade e dos seus limites de permissões. As políticas baseadas em atributo que especificam o usuário ou o perfil no campo `Principal` não são limitadas pelo limite de permissões. Uma negação explícita em qualquer uma dessas políticas substitui a permissão. Para obter mais informações sobre limites de permissões, consulte Limites de permissões para identidades do IAM no Guia do usuário do IAM.
- Políticas de controle de serviço (SCPs) — SCPs são políticas JSON que especificam as permissões máximas para uma organização ou unidade organizacional (OU) em. AWS Organizations AWS Organizations é um serviço para agrupar e gerenciar centralmente vários Contas da AWS que sua empresa possui. Se você habilitar todos os atributos em uma organização, poderá aplicar políticas de controle de serviço (SCPs) a qualquer uma ou a todas

as contas. O SCP limita as permissões para entidades nas contas dos membros, incluindo cada uma Usuário raiz da conta da AWS. Para obter mais informações sobre o Organizações e SCPs, consulte Como os SCPs funcionam no Guia do usuário do AWS Organizations .

- Políticas de sessão: são políticas avançadas que você transmite como um parâmetro quando cria de forma programática uma sessão temporária para um perfil ou um usuário federado. As permissões da sessão resultante são a interseção das políticas baseadas em identidade do usuário ou do perfil e das políticas de sessão. As permissões também podem ser provenientes de uma política baseada em atributo. Uma negação explícita em qualquer uma dessas políticas substitui a permissão. Para obter mais informações, consulte Políticas de sessão no Guia do usuário do IAM.

Vários tipos de política

Quando vários tipos de política são aplicáveis a uma solicitação, é mais complicado compreender as permissões resultantes. Para saber como AWS determinar se uma solicitação deve ser permitida quando vários tipos de políticas estão envolvidos, consulte Lógica de avaliação de políticas no Guia do usuário do IAM.

Como o Amazon Fraud Detector funciona com o IAM

Antes de usar o IAM para gerenciar o acesso ao Amazon Fraud Detector, você deve entender quais recursos do IAM estão disponíveis para uso com o Amazon Fraud Detector. Para ter uma visão de alto nível de como o Amazon Fraud Detector e outros AWS serviços funcionam com o IAM, consulte AWS Services That Work with IAM no Guia do usuário do IAM.

Tópicos

- Políticas baseadas em identidade do Amazon Fraud Detector
- Políticas baseadas em recursos do Amazon Fraud Detector
- Autorização baseada nas etiquetas do Amazon Fraud Detector
- Funções do Amazon Fraud Detector IAM

Políticas baseadas em identidade do Amazon Fraud Detector

Com as políticas baseadas em identidade do IAM, é possível especificar ações ou atributos permitidos ou negados, bem como as condições sob as quais as ações são permitidas ou negadas. O Amazon Fraud Detector oferece suporte a ações, recursos e chaves de condição específicos. Para

conhecer todos os elementos usados em uma política JSON, consulte Referência de elementos de política JSON do IAM no Guia do usuário do IAM.

Para começar a usar o Amazon Fraud Detector, recomendamos criar um usuário com acesso restrito às operações do Amazon Fraud Detector e às permissões necessárias. Você pode adicionar outras permissões se necessário. As políticas a seguir fornecem a permissão necessária para usar o Amazon Fraud Detector: `AmazonFraudDetectorFullAccessPolicy` `AmazonS3FullAccess` e. Para obter mais informações sobre como configurar o Amazon Fraud Detector usando essas políticas, consulteConfigurar o Amazon Fraud Detector.

Ações

Os administradores podem usar políticas AWS JSON para especificar quem tem acesso ao quê. Ou seja, qual entidade principal pode executar ações em quais recursos, e em que condições.

O elemento `Action` de uma política JSON descreve as ações que você pode usar para permitir ou negar acesso em uma política. As ações de política geralmente têm o mesmo nome da operação de AWS API associada. Existem algumas exceções, como ações somente de permissão, que não têm uma operação de API correspondente. Há também algumas operações que exigem várias ações em uma política. Essas ações adicionais são chamadas de ações dependentes.

Incluem ações em uma política para conceder permissões para executar a operação associada.

As ações políticas no Amazon Fraud Detector usam o seguinte prefixo antes da ação:`frauddetector:`. Por exemplo, para criar uma regra com a operação da `CreateRule` API Amazon Fraud Detector, você inclui a `frauddetector:CreateRule` ação na política. As instruções de política devem incluir um elemento `Action` ou `NotAction`. O Amazon Fraud Detector define seu próprio conjunto de ações que descrevem as tarefas que você pode realizar com esse serviço.

Para especificar várias ações em uma única instrução, separe-as com vírgulas, como segue:

```
"Action": [
      "frauddetector:action1",
      "frauddetector:action2"
```

Você também pode especificar várias ações usando caracteres curinga (*). Por exemplo, para especificar todas as ações que começam com a palavra `Describe`, inclua a seguinte ação:

```
"Action": "frauddetector:Describe*"
```

Para ver uma lista das ações do Amazon Fraud Detector, consulte Ações definidas pelo Amazon Fraud Detector no Guia do usuário do IAM.

Recursos

Os administradores podem usar políticas AWS JSON para especificar quem tem acesso ao quê. Ou seja, qual entidade principal pode executar ações em quais recursos, e em que condições.

O elemento `Resource` de política JSON especifica o objeto ou os objetos aos quais a ação se aplica. As instruções devem incluir um elemento `Resource` ou um elemento `NotResource`. Como prática recomendada, especifique um recurso usando Nome do recurso da Amazon (ARN). Isso pode ser feito para ações que oferecem suporte a um tipo de atributo específico, conhecido como permissões em nível de atributo.

Para ações não compatíveis com permissões no nível de recurso, como operações de listagem, use um curinga (*) para indicar que a instrução se aplica a todos os recursos.

```
"Resource": "*"
```

Os tipos de recursos definidos pelo Amazon Fraud Detector listam todos os ARNs de recursos do Amazon Fraud Detector.

Por exemplo, para especificar o `my_detector` detector em sua declaração, use o seguinte ARN:

```
"Resource": "arn:aws:frauddetector:us-east-1:123456789012:detector/my_detector"
```

Para obter mais informações sobre o formato dos ARNs, consulte Amazon Resource Names (ARNs) e AWS Service Namespaces.

Para especificar todos os detectores que pertencem a uma conta específica, use o caractere curinga (*):

```
"Resource": "arn:aws:frauddetector:us-east-1:123456789012:detector/*"
```

Algumas ações do Amazon Fraud Detector, como aquelas para criar recursos, não podem ser executadas em um recurso específico. Nesses casos, você deve utilizar o caractere curinga (*).

```
"Resource": "*"
```

Para ver uma lista dos tipos de recursos do Amazon Fraud Detector e seus ARNs, consulte Resources Defined by Amazon Fraud Detector no Guia do usuário do IAM. Para saber quais ações você pode especificar o ARN de cada recurso, consulte Ações definidas pelo Amazon Fraud Detector.

Chaves de condição

Os administradores podem usar políticas AWS JSON para especificar quem tem acesso ao quê. Ou seja, qual principal pode executar ações em quais recursos, e em que condições.

O elemento `Condition` (ou `Condition` bloco de) permite que você especifique condições nas quais uma instrução está em vigor. O elemento `Condition` é opcional. É possível criar expressões condicionais que usam agentes de condição, como “igual a” ou “menor que”, para fazer a condição da política corresponder aos valores na solicitação.

Se você especificar vários elementos `Condition` em uma instrução ou várias chaves em um único `Condition` elemento, a AWS os avaliará usando uma operação lógica `AND`. Se você especificar vários valores para uma única chave de condição, AWS avalia a condição usando uma `OR` operação lógica. Todas as condições devem ser atendidas para que as permissões da instrução sejam concedidas.

Você também pode usar variáveis de espaço reservado ao especificar as condições. Por exemplo, é possível conceder a um usuário do IAM permissão para acessar um atributo somente se ele estiver marcado com seu nome de usuário do IAM. Para obter mais informações, consulte Elementos de política do IAM: variáveis e tags no Guia do usuário do IAM.

AWS suporta chaves de condição globais e chaves de condição específicas do serviço. Para ver todas as chaves de condição AWS globais, consulte as chaves de contexto de condição AWS global no Guia do usuário do IAM.

O Amazon Fraud Detector define seu próprio conjunto de chaves de condição e também suporta o uso de algumas chaves de condição globais. Para ver todas as chaves de condição AWS globais, consulte Chaves de contexto de condição AWS global no Guia do usuário do IAM.

Para ver uma lista das chaves de condição do Amazon Fraud Detector, consulte Chaves de condição do Amazon Fraud Detector no Guia do usuário do IAM. Para saber quais ações e recursos você pode usar uma chave de condição, consulte Ações definidas pelo Amazon Fraud Detector.

Exemplos

Para ver exemplos de políticas baseadas em identidade do Amazon Fraud Detector, consulte. Exemplos de políticas baseadas em identidade do Amazon Fraud Detector

Políticas baseadas em recursos do Amazon Fraud Detector

O Amazon Fraud Detector não oferece suporte a políticas baseadas em recursos.

Autorização baseada nas etiquetas do Amazon Fraud Detector

Você pode anexar tags aos recursos do Amazon Fraud Detector ou passar tags em uma solicitação para o Amazon Fraud Detector. Para controlar o acesso baseado em tags, forneça informações sobre as tags no elemento de condição de uma política usando as chaves de condição `aws:ResourceTag/key-name`, `aws:RequestTag/key-name` ou `aws:TagKeys`.

Funções do Amazon Fraud Detector IAM

Uma função do IAM é uma entidade dentro da sua AWS conta que tem permissões específicas.

Usando credenciais temporárias com o Amazon Fraud Detector

É possível usar credenciais temporárias para fazer login com federação, assumir um perfil do IAM ou assumir um perfil entre contas. Você obtém credenciais de segurança temporárias chamando operações de AWS STS API, como AssumeRoleou GetFederationToken.

O Amazon Fraud Detector suporta o uso de credenciais temporárias.

Perfis vinculados ao serviço

As funções vinculadas ao serviço permitem que AWS os serviços acessem recursos em outros serviços para concluir uma ação em seu nome. Os perfis vinculados a serviço aparecem na sua conta do IAM e são de propriedade do serviço. Um administrador do IAM pode visualizar, mas não pode editar as permissões para perfis vinculados a serviço.

O Amazon Fraud Detector não oferece suporte a funções vinculadas a serviços.

Perfis de serviço

Esse atributo permite que um serviço assuma um perfil de serviço em seu nome. O perfil permite que o serviço acesse recursos em outros serviços para concluir uma ação em seu nome. As funções de serviço aparecem em sua conta do e são de propriedade da conta. Isso significa que um administrador do pode alterar as permissões para essa função. Porém, fazer isso pode alterar a funcionalidade do serviço.

O Amazon Fraud Detector suporta funções de serviço.

Exemplos de políticas baseadas em identidade do Amazon Fraud Detector

Por padrão, usuários e funções do IAM não têm permissão para criar ou modificar recursos do Amazon Fraud Detector. Eles também não podem realizar tarefas usando a AWS API AWS Management Console AWS CLI, ou. Um administrador deve criar as políticas do IAM que concedam aos usuários e aos perfis permissões para executar operações de API específicas nos recursos especificados que precisam. O administrador deve anexar essas políticas aos usuários ou grupos que exigem essas permissões.

Para saber como criar uma política baseada em identidade do IAM usando esses exemplos de documentos de política JSON, consulte Criar políticas na guia JSON no Guia do usuário do IAM.

Tópicos

Melhores práticas de política

As políticas baseadas em identidade determinam se alguém pode criar, acessar ou excluir recursos do Amazon Fraud Detector em sua conta. Essas ações podem incorrer em custos para a Conta da AWS. Ao criar ou editar políticas baseadas em identidade, siga estas diretrizes e recomendações:

- Comece com as políticas AWS gerenciadas e avance para as permissões de privilégios mínimos — Para começar a conceder permissões aos seus usuários e cargas de trabalho, use as políticas AWS gerenciadas que concedem permissões para muitos casos de uso comuns. Eles estão disponíveis no seu Conta da AWS. Recomendamos que você reduza ainda mais as permissões definindo políticas gerenciadas pelo AWS cliente que sejam específicas para seus casos de uso. Para obter mais informações, consulte Políticas gerenciadas pela AWS ou Políticas gerenciadas pela AWS para perfis de trabalho no Guia do usuário do IAM.

- Aplique permissões de privilégio mínimo: ao definir permissões com as políticas do IAM, conceda apenas as permissões necessárias para executar uma tarefa. Você faz isso definindo as ações que podem ser executadas em atributos específicos sob condições específicas, também conhecidas como permissões de privilégio mínimo. Para obter mais informações sobre como usar o IAM para aplicar permissões, consulte Políticas e permissões no IAM no Guia do usuário do IAM.
- Use condições nas políticas do IAM para restringir ainda mais o acesso: você pode adicionar uma condição às políticas para limitar o acesso a ações e atributos. Por exemplo, você pode escrever uma condição de política para especificar que todas as solicitações devem ser enviadas usando SSL. Você também pode usar condições para conceder acesso às ações de serviço se elas forem usadas por meio de uma ação específica AWS service (Serviço da AWS), como AWS CloudFormation. Para obter mais informações, consulte Elementos de política JSON do IAM: condições no Manual do usuário do IAM.
- Use o IAM Access Analyzer para validar suas políticas do IAM a fim de garantir permissões seguras e funcionais: o IAM Access Analyzer valida as políticas novas e existentes para que elas sigam a linguagem de política do IAM (JSON) e as práticas recomendadas do IAM. O IAM Access Analyzer oferece mais de cem verificações de política e recomendações acionáveis para ajudar você a criar políticas seguras e funcionais. Para obter mais informações, consulte Validação de políticas do IAM Access Analyzer no Guia do usuário do IAM.
- Exigir autenticação multifator (MFA) — Se você tiver um cenário que exija usuários do IAM ou um usuário root, ative Conta da AWS a MFA para obter segurança adicional. Para exigir a MFA quando as operações de API forem chamadas, adicione condições de MFA às suas políticas. Para obter mais informações, consulte Configuração de acesso à API protegido por MFA no Guia do usuário do IAM.

Para mais informações sobre as práticas recomendadas do IAM, consulte Práticas recomendadas de segurança no IAM no Guia do usuário do IAM.

Política gerenciada pela AWS (predefinida) para o Amazon Fraud Detector

AWS aborda muitos casos de uso comuns fornecendo políticas autônomas do IAM que são criadas e administradas pela AWS. Essas políticas AWS gerenciadas concedem as permissões necessárias para casos de uso comuns, para que você não precise investigar quais permissões são necessárias. Para obter mais informações, consulte as políticas gerenciadas da AWS no Guia do usuário AWS Identity and Access Management de gerenciamento.

A seguinte política AWS gerenciada, que você pode anexar aos usuários em sua conta, é específica do Amazon Fraud Detector:

`AmazonFraudDetectorFullAccess`: Concede acesso total aos recursos, ações e operações apoiadas do Amazon Fraud Detector, incluindo:

- Liste e descreva todos os endpoints do modelo na Amazon SageMaker
- Listar todas as funções do IAM na conta
- Listar todos os buckets do Amazon S3
- Permita que a função IAM Pass passe uma função para o Amazon Fraud Detector

Essa política não fornece acesso irrestrito ao S3. Se você precisar carregar conjuntos de dados de treinamento de modelos para o S3, a política `AmazonS3FullAccess` gerenciada (ou a política de acesso personalizada do Amazon S3 com escopo reduzido) também é necessária.

Você pode revisar as permissões da política fazendo login no console do IAM e pesquisando pelo nome da política. Você também pode criar suas próprias políticas personalizadas do IAM para permitir permissões para ações e recursos do Amazon Fraud Detector conforme necessário. É possível anexar essas políticas personalizadas aos usuários ou grupos que necessitam delas.

Permitir que os usuários visualizem suas próprias permissões

Este exemplo mostra como você pode criar uma política que permite que os usuários do IAM visualizem as políticas gerenciadas e em linha anexadas a sua identidade de usuário. Essa política inclui permissões para concluir essa ação no console ou programaticamente usando a API AWS CLI ou 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": "*"
        }
    ]
}
```

Permita acesso total aos recursos do Amazon Fraud Detector

O exemplo a seguir dá a um usuário acesso Conta da AWS total a todos os recursos e ações do Amazon Fraud Detector.

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Action": [
                "frauddetector:*"
            ],
            "Resource": "*"
        }
    ]
}
```

Permita acesso somente para leitura aos recursos do Amazon Fraud Detector

Neste exemplo, você concede a um usuário em seu acesso Conta da AWS somente para leitura aos recursos do 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": "*"
        }
    ]
}
```

Permitir acesso a um recurso específico

Neste exemplo de política em nível de recurso, você concede a um usuário Conta da AWS acesso a todas as ações e recursos, exceto a um recurso específico do 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}"
        }
    ]
}
```

Permita o acesso a recursos específicos ao usar a API de modo duplo

O Amazon Fraud Detector fornece APIs de obtenção de modo duplo que funcionam como operações de lista e descrição. Uma API de modo duplo, quando chamada sem nenhum parâmetro, retorna uma lista do recurso especificado associado ao seu Conta da AWS. Uma API de modo duplo, quando chamada com o parâmetro, retorna os detalhes do recurso especificado. O recurso pode ser modelos, variáveis, tipos de eventos ou tipos de entidades.

As APIs de modo duplo oferecem suporte a permissões em nível de recurso nas políticas do IAM. No entanto, as permissões em nível de recurso são aplicadas somente quando um ou mais parâmetros são fornecidos como parte da solicitação. Por exemplo, se o usuário chamar a GetVariablesAPI e fornecer um nome de variável e se houver uma política do IAM Deny anexada ao recurso da variável ou ao nome da variável, o usuário receberá `AccessDeniedException` um erro. Se o usuário chamar a `GetVariables` API e não especificar um nome de variável, todas as variáveis serão retornadas, o que pode causar vazamento de informações.

Para permitir que os usuários visualizem somente detalhes de recursos específicos, use um elemento de `NotResource` política do IAM em uma política do IAM Deny. Depois de adicionar esse elemento de política a uma política do IAM Deny, os usuários só podem visualizar os detalhes dos recursos especificados no `NotResource` bloco. Para obter mais informações, consulte Elementos da política JSON do IAM: NotResource no Guia do usuário do IAM.

O exemplo de política a seguir permite que os usuários acessem todos os recursos do Amazon Fraud Detector. No entanto, o elemento de `NotResource` política é usado para limitar as chamadas de GetVariablesAPI somente aos nomes das variáveis com os prefixos `user*job_*`, e. `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*"
    ]
  }
 ]
}
```

Resposta

Para este exemplo de política, a resposta apresenta o seguinte comportamento:

- Uma GetVariables chamada que não inclui nomes de variáveis resulta em um `AccessDeniedException` erro porque a solicitação é mapeada para a instrução Deny.
- Uma GetVariables chamada que inclui um nome de variável que não é permitido resulta em um `AccessDeniedException` erro porque o nome da variável não é mapeado para o nome da variável no `NotResource` bloco. Por exemplo, uma GetVariables chamada com um nome de variável `email_address` resulta em um `AccessDeniedException` erro.
- Uma GetVariables chamada que inclui um nome de variável que corresponda a um nome de variável no `NotResource` bloco é retornada conforme o esperado. Por exemplo, uma GetVariables chamada que inclui o nome da variável `job_cpa` retorna os detalhes da `job_cpa` variável.

Limitar o acesso com base em tags

Este exemplo de política demonstra como limitar o acesso ao Amazon Fraud Detector com base em tags de recursos. Este exemplo pressupõe que:

- No seu, Conta da AWS você definiu dois grupos diferentes, chamados Equipe1 e Equipe2
- Você criou quatro detectores

- Você deseja permitir que os membros do Team1 façam chamadas de API em 2 detectores
- Você deseja permitir que os membros do Team2 façam chamadas de API nos outros 2 detectores

Para controlar o acesso a chamadas de APIs (exemplo)

1. Adicione uma tag com a chave `Project` e o valor `A` aos detectores usados pelo Team1.
2. Adicione uma tag com a chave `Project` e o valor `B` aos detectores usados pelo Team2.
3. Crie uma política do IAM com uma `ResourceTag` condição que negue o acesso a detectores que tenham tags com chave `Project` e valor `B` e anexe essa política ao Team1.
4. Crie uma política do IAM com uma `ResourceTag` condição que negue o acesso a detectores que tenham tags com chave `Project` e valor `A` e anexe essa política ao Team2.

Veja a seguir um exemplo de uma política que nega ações específicas em qualquer recurso do Amazon Fraud Detector que tenha uma tag com uma chave de `Project` e um valor de`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"
        }
```

```
      }
    }
  ]
}
```

Prevenção contra representante confuso

O problema confuso do deputado ocorre quando uma entidade que não tem permissão para realizar uma ação pode coagir uma entidade mais privilegiada a realizar a ação. AWS fornece ferramentas que ajudam você a proteger sua conta se você fornecer acesso a terceiros (chamado de contas cruzadas) ou outros AWS serviços (chamado de serviços cruzados) aos recursos em sua conta.

O problema confuso de delegação entre serviços pode ocorrer quando um serviço (o serviço de chamada) liga para outro serviço (o serviço chamado). O serviço de chamada pode ser manipulado para utilizar as suas permissões para atuar nos recursos de outro cliente em que, de outra forma, ele não teria permissão para acessar. Para evitar isso, você pode criar políticas que ajudem a proteger seus dados para todos os serviços com diretores de serviço que receberam acesso aos recursos do seu serviço.

O Amazon Fraud Detector suporta o uso de funções de serviço em suas políticas de permissão para permitir que um serviço acesse os recursos de outro serviço em seu nome. Uma função requer duas políticas: uma política de confiança de função que especifica qual entidade principal tem permissão para assumir a função e uma política de permissões que especifica o que pode ser feito com a função. Quando um serviço assume uma função em seu nome, a entidade principal de serviço deve ter permissão para executar a ação `sts:AssumeRole` na política de confiança de função. Quando um serviço é chamado`sts:AssumeRole`, AWS STS retorna um conjunto de credenciais de segurança temporárias que o responsável pelo serviço usa para acessar os recursos permitidos pela política de permissões da função.

Para evitar problemas confusos entre serviços, o Amazon Fraud Detector recomenda usar `aws:SourceArn`as chaves de contexto de condições `aws:SourceAccount`globais em sua política de confiança de função para limitar o acesso à função somente às solicitações geradas pelos recursos esperados.

`aws:SourceAccount`Especifica a ID da conta e `aws:SourceArn` especifica o ARN do recurso associado ao acesso entre serviços. O `aws:SourceArn` deve ser especificado usando o formato ARN. Certifique-se de que ambos `aws:SourceAccount` `aws:SourceArn` estejam usando o mesmo ID de conta quando usados na mesma declaração de política.

A maneira mais eficaz de se proteger contra o problema do substituto confuso é usar a chave de contexto de condição global `aws:SourceArn` com o ARN completo do recurso. Se você não souber o ARN completo do recurso ou se estiver especificando vários recursos, use a chave de condição de contexto `aws:SourceArn` global com um curinga (*) para as partes desconhecidas do ARN. Por exemplo, `arn:aws:`*`servicename`*`:*:`*`123456789012`*`:*`. Para obter informações sobre os recursos e ações do Amazon Fraud Detector que você pode usar em suas políticas de permissão, consulte Ações, recursos e chaves de condição do Amazon Fraud Detector.

O exemplo de política de confiança de função a seguir usa o caractere curinga (*) na chave de `aws:SourceArn` condição para permitir que o Amazon Fraud Detector acesse vários recursos associados à ID da conta.

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

A política de confiança de funções a seguir permite que o Amazon Fraud Detector acesse somente `external-model` recursos. Observe o `aws:SourceArn` parâmetro no bloco de condições. O qualificador de recursos é criado usando o endpoint do modelo fornecido para fazer a chamada à `PutExternalModel` API.

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

Solução de problemas de identidade e acesso ao Amazon Fraud Detector

Use as informações a seguir para ajudá-lo a diagnosticar e corrigir problemas comuns que você pode encontrar ao trabalhar com o Amazon Fraud Detector e o IAM.

Tópicos

- Não estou autorizado a realizar uma ação no Amazon Fraud Detector
- Não estou autorizado a realizar iam: PassRole
- Quero permitir que pessoas fora da minha AWS conta acessem meus recursos do Amazon Fraud Detector
- O Amazon Fraud Detector não pôde assumir a função determinada

Não estou autorizado a realizar uma ação no Amazon Fraud Detector

Se isso AWS Management Console indicar que você não está autorizado a realizar uma ação, entre em contato com o administrador para obter ajuda. Caso seu administrador seja a pessoa que forneceu suas credenciais de início de sessão.

O exemplo de erro a seguir ocorre quando o `mateojackson` usuário tenta usar o console para ver detalhes sobre um *`detector`*, mas não tem `frauddetector:`*`GetDetectors`* permissões.

```
User: arn:aws:iam::123456789012:user/mateojackson is not authorized to perform:
 frauddetector:GetDetectors on resource: my-example-detector
```

Neste caso, Mateo pede ao administrador para atualizar suas políticas para permitir a ele o acesso ao recurso *`my-example-detector`* usando a ação `frauddetector:`*`GetDetectors`*.

Não estou autorizado a realizar iam: PassRole

Se você receber um erro informando que não está autorizado a realizar a `iam:PassRole` ação, suas políticas devem ser atualizadas para permitir que você passe uma função para o Amazon Fraud Detector.

Alguns Serviços da AWS permitem que você passe uma função existente para esse serviço em vez de criar uma nova função de serviço ou uma função vinculada ao serviço. Para fazer isso, é preciso ter permissões para passar o perfil para o serviço.

O exemplo de erro a seguir ocorre quando um usuário do IAM chamado `marymajor` tenta usar o console para realizar uma ação no Amazon Fraud Detector. No entanto, a ação exige que o serviço tenha permissões concedidas por um perfil de serviço. Mary não tem permissões para passar o perfil para o serviço.

```
User: arn:aws:iam::123456789012:user/marymajor is not authorized to perform:
 iam:PassRole
```

Nesse caso, as políticas de Mary devem ser atualizadas para permitir que ela realize a ação `iam:PassRole`.

Se precisar de ajuda, entre em contato com seu AWS administrador. Seu administrador é a pessoa que forneceu suas credenciais de login.

Quero permitir que pessoas fora da minha AWS conta acessem meus recursos do Amazon Fraud Detector

Você pode criar uma função que os usuários de outras contas ou pessoas fora da organização podem usar para acessar seus recursos. Você pode especificar quem é confiável para assumir o perfil. Para serviços compatíveis com políticas baseadas em recursos ou listas de controle de acesso (ACLs), você pode usar essas políticas para conceder às pessoas acesso aos seus recursos.

Para saber mais, consulte:

- Para saber se o Amazon Fraud Detector é compatível com esses recursos, consulteComo o Amazon Fraud Detector funciona com o IAM.
- Para saber como fornecer acesso aos seus recursos em todos os Contas da AWS que você possui, consulte Como fornecer acesso a um usuário do IAM em outro Conta da AWS que você possui no Guia do usuário do IAM.
- Para saber como fornecer acesso aos seus recursos a terceiros Contas da AWS, consulte Como fornecer acesso Contas da AWS a terceiros no Guia do usuário do IAM.
- Para saber como conceder acesso por meio da federação de identidades, consulte Conceder acesso a usuários autenticados externamente (federação de identidades) no Guia do usuário do IAM.
- Para saber a diferença entre usar perfis e políticas baseadas em recursos para acesso entre contas, consulte Como os perfis do IAM diferem de políticas baseadas em recursos no Guia do usuário do IAM.

O Amazon Fraud Detector não pôde assumir a função determinada

Se você receber um erro informando que o Amazon Fraud Detector não pôde assumir a função especificada, você deverá atualizar a relação de confiança da função especificada. Ao especificar o Amazon Fraud Detector como uma entidade confiável, o serviço pode assumir a função. Quando você usa o Amazon Fraud Detector para criar uma função, essa relação de confiança é definida automaticamente. Você só precisa estabelecer essa relação de confiança para funções do IAM que não foram criadas pelo Amazon Fraud Detector.

Estabelecer uma relação de confiança para uma função existente no Amazon Fraud Detector

1. Abra o console do IAM em https://console.aws.amazon.com/iam/
2. No painel de navegação, escolha Funções.

3. Escolha o nome da função que você deseja modificar e escolha a guia Relações de confiança.
4. Selecione Edit trust relationship (Editar relação de confiança).
5. Em Policy Document, cole o seguinte e selecione Update Trust Policy.

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

Registro e monitoramento no Amazon Fraud Detector

A AWS fornece as seguintes ferramentas de monitoramento para observar o Amazon Fraud Detector, relatar quando algo está errado e realizar ações automáticas quando apropriado:

- A Amazon CloudWatch monitora seus AWS recursos e os aplicativos em que você executa AWS em tempo real. Para obter mais informações sobre CloudWatch, consulte o Guia CloudWatch do usuário da Amazon.
- AWS CloudTrailcaptura chamadas de API e eventos relacionados feitos por ou em nome de sua AWS conta e entrega os arquivos de log para um bucket do Amazon S3 que você especificar. Para obter mais informações CloudTrail, consulte o Guia AWS CloudTrail do usuário.

Para obter mais informações sobre o monitoramento do Amazon Fraud Detector, consulteMonitore o Amazon Fraud Detector.

Validação de conformidade para o Amazon Fraud Detector

Auditores terceirizados avaliam a segurança e a conformidade dos AWS serviços como parte de vários programas de AWS conformidade, como SOC, PCI, FedRAMP e HIPAA.

Para saber se um AWS service (Serviço da AWS) está dentro do escopo de programas de conformidade específicos, consulte Serviços da AWS Escopo por Programa de Conformidade Serviços da AWS e escolha o programa de conformidade em que você está interessado. Para obter informações gerais, consulte Programas de AWS conformidade Programas AWS de .

Você pode baixar relatórios de auditoria de terceiros usando AWS Artifact. Para obter mais informações, consulte Baixar relatórios em AWS Artifact .

Sua responsabilidade de conformidade ao usar Serviços da AWS é determinada pela confidencialidade de seus dados, pelos objetivos de conformidade de sua empresa e pelas leis e regulamentações aplicáveis. AWS fornece os seguintes recursos para ajudar na conformidade:

- Guias de início rápido sobre segurança e conformidade — Esses guias de implantação discutem considerações arquitetônicas e fornecem etapas para a implantação de ambientes básicos AWS focados em segurança e conformidade.
- Arquitetura para segurança e conformidade com a HIPAA na Amazon Web Services — Este whitepaper descreve como as empresas podem usar AWS para criar aplicativos qualificados para a HIPAA.

  > **Note**
  >
  > Nem todos Serviços da AWS são elegíveis para a HIPAA. Para obter mais informações, consulte a Referência dos serviços qualificados pela HIPAA.

- AWS Recursos de https://aws.amazon.com/compliance/resources/ de conformidade — Essa coleção de pastas de trabalho e guias pode ser aplicada ao seu setor e local.
- AWS Guias de conformidade do cliente — Entenda o modelo de responsabilidade compartilhada sob a ótica da conformidade. Os guias resumem as melhores práticas de proteção Serviços da AWS e mapeiam as diretrizes para controles de segurança em várias estruturas (incluindo o Instituto Nacional de Padrões e Tecnologia (NIST), o Conselho de Padrões de Segurança do Setor de Cartões de Pagamento (PCI) e a Organização Internacional de Padronização (ISO)).
- Avaliação de recursos com regras no Guia do AWS Config desenvolvedor — O AWS Config serviço avalia o quão bem suas configurações de recursos estão em conformidade com as práticas internas, as diretrizes e os regulamentos do setor.
- AWS Security Hub— Isso AWS service (Serviço da AWS) fornece uma visão abrangente do seu estado de segurança interno AWS. O Security Hub usa controles de segurança para avaliar os atributos da AWS e verificar a conformidade com os padrões e as práticas recomendadas do setor

de segurança. Para obter uma lista dos serviços e controles aceitos, consulte a Referência de controles do Security Hub.

- Amazon GuardDuty — Isso AWS service (Serviço da AWS) detecta possíveis ameaças às suas cargas de trabalho Contas da AWS, contêineres e dados monitorando seu ambiente em busca de atividades suspeitas e maliciosas. GuardDuty pode ajudá-lo a atender a vários requisitos de conformidade, como o PCI DSS, atendendo aos requisitos de detecção de intrusões exigidos por determinadas estruturas de conformidade.
- AWS Audit Manager— Isso AWS service (Serviço da AWS) ajuda você a auditar continuamente seu AWS uso para simplificar a forma como você gerencia o risco e a conformidade com as regulamentações e os padrões do setor.

Resiliência no Amazon Fraud Detector

A infraestrutura global da AWS é criada com base em regiões e zonas de disponibilidade da AWS. As regiões da AWS fornecem várias zonas de disponibilidade separadas e fisicamente isoladas, que são conectadas com redes de baixa latência, throughput alto e altamente redundantes. Com as zonas de disponibilidade, é possível projetar e operar aplicações e bancos de dados que automaticamente executam o failover entre as zonas sem interrupção. As zonas de disponibilidade são mais altamente disponíveis, tolerantes a falhas e escaláveis que uma ou várias infraestruturas de datacenter tradicionais.

Para obter mais informações sobre as regiões e as zonas de disponibilidade da AWS, consulte Infraestrutura global da AWS.

Segurança de infraestrutura no Amazon Fraud Detector

Como um serviço gerenciado, o Amazon Fraud Detector é protegido pela segurança de rede AWS global. Para obter informações sobre serviços AWS de segurança e como AWS proteger a infraestrutura, consulte AWS Cloud Security. Para projetar seu AWS ambiente usando as melhores práticas de segurança de infraestrutura, consulte Proteção de infraestrutura no Security Pillar AWS Well-Architected Framework.

Você usa chamadas de API AWS publicadas para acessar o Amazon Fraud Detector pela rede. Os clientes devem ser compatíveis com:

- Transport Layer Security (TLS). Exigimos TLS 1.2 e recomendamos TLS 1.3.

- Conjuntos de criptografia com sigilo de encaminhamento perfeito (perfect forward secrecy, ou PFS) como DHE (Ephemeral Diffie-Hellman, ou Efêmero Diffie-Hellman) ou ECDHE (Ephemeral Elliptic Curve Diffie-Hellman, ou Curva elíptica efêmera Diffie-Hellman). A maioria dos sistemas modernos, como Java 7 e versões posteriores, são compatíveis com esses modos.

Além disso, as solicitações devem ser assinadas utilizando um ID da chave de acesso e uma chave de acesso secreta associada a uma entidade principal do IAM. Ou é possível usar o AWS Security Token Service (AWS STS) para gerar credenciais de segurança temporárias para assinar solicitações.

Monitore o Amazon Fraud Detector

O monitoramento é uma parte importante da manutenção da confiabilidade, disponibilidade e desempenho do Amazon Fraud Detector e de suas outras soluções da AWS. A AWS fornece as seguintes ferramentas de monitoramento para observar o Amazon Fraud Detector, relatar quando algo está errado e realizar ações automáticas quando apropriado:

- A Amazon CloudWatch monitora seus AWS recursos e os aplicativos em que você executa AWS em tempo real. É possível coletar e rastrear métricas, criar painéis personalizados e definir alarmes que o notificam ou que realizam ações quando uma métrica especificada atinge um limite definido. Para obter mais informações, consulte o Guia CloudWatch do usuário da Amazon.
- AWS CloudTrailcaptura chamadas de API e eventos relacionados feitos por ou em nome de sua AWS conta e entrega os arquivos de log para um bucket do Amazon S3 que você especificar. Você pode identificar quais usuários e contas chamaram a AWS, o endereço IP de origem no qual as chamadas foram feitas e quando elas ocorreram. Para mais informações, consulte o Guia do usuário do AWS CloudTrail.

Tópicos

Monitorando o Amazon Fraud Detector com a Amazon CloudWatch

Você pode monitorar o Amazon Fraud Detector usando o Amazon Fraud Detector CloudWatch, que coleta dados brutos e os processa em métricas legíveis, quase em tempo real. Essas estatísticas são mantidas por 15 meses, de maneira que você possa acessar informações históricas e ter uma perspectiva melhor de como o aplicativo web ou o serviço está se saindo. Você também pode definir alarmes que observam determinados limites e enviam notificações ou realizam ações quando esses limites são atingidos. Para obter mais informações, consulte o Guia CloudWatch do usuário da Amazon.

Tópicos

Usando CloudWatch métricas para o Amazon Fraud Detector.

Para usar métricas, você deve especificar as seguintes informações:

- O namespace métrico. Um namespace é um contêiner que o CloudWatch Amazon Fraud Detector usa para publicar suas métricas. Se você estiver usando a CloudWatch ListMetricsAPI ou o comando list-metrics para visualizar as métricas do Amazon Fraud Detector, especifique `AWS/FraudDetector` o namespace.
- A dimensão da métrica. Uma dimensão é um par nome-valor que ajuda você a identificar de forma exclusiva uma métrica, por exemplo, `DetectorId` pode ser um nome de dimensão. Especificar uma dimensão métrica é opcional.
- O nome da métrica, como `GetEventPrediction`.

Você pode obter dados de monitoramento para o Amazon Fraud Detector usando o AWS Management Console AWS CLI, o ou a CloudWatch API. Você também pode usar a CloudWatch API por meio de um dos kits de desenvolvimento de software (SDKs) da Amazon AWS ou das ferramentas de CloudWatch API. O console exibe uma série de gráficos com base nos dados brutos da CloudWatch API. Dependendo das necessidades, você pode preferir usar os gráficos exibidos no console ou recuperados da API.

A lista a seguir mostra alguns usos comuns para as métricas. Essas são sugestões para você começar, e não uma lista abrangente.

Como eu faço para...	Métricas relevantes
Como faço para rastrear o número de previsões que foram realizadas?	Monitorar a métrica `GetEventPrediction` .
Como posso monitorar os `GetEventPrediction` erros?	Use as `GetEventPrediction4xxError` métricas `GetEventPrediction5xxError` e as.
Como posso monitorar a latência das chamadas `GetEventPrediction` ?	Use a métrica `GetEventPrediction Latency` .

Você deve ter as CloudWatch permissões apropriadas para monitorar o Amazon Fraud Detector com CloudWatch. Para obter mais informações, consulte Autenticação e controle de acesso para a Amazon CloudWatch.

Acesse as métricas do Amazon Fraud Detector

As etapas a seguir mostram como acessar as métricas do Amazon Fraud Detector usando o CloudWatch console.

Para visualizar métricas (console)

1. Abra o CloudWatch console em https://console.aws.amazon.com/cloudwatch/.
2. Escolha Métricas, escolha a guia Todas as métricas e, em seguida, escolha Fraud Detector.
3. Escolha a dimensão da métrica.
4. Escolha a métrica desejada na lista e um período para o gráfico.

Criar um alarme

Você pode criar um CloudWatch alarme que envia uma mensagem do Amazon Simple Notification Service (Amazon SNS) quando o alarme muda de estado. Um alarme observa uma única métrica por um período tempo que você especifica. Ele executa uma ou mais ações com base no valor da métrica em relação a um limite especificado ao longo de vários períodos. A ação é uma notificação enviada a um tópico do Amazon SNS ou a uma política de Auto Scaling.

Os alarmes invocam ações somente para mudanças de estado sustentadas. CloudWatch os alarmes não invocam ações simplesmente porque estão em um estado específico. O estado deve ter sido alterado e mantido por um período especificado.

Para definir um alarme (console)

1. Faça login no AWS Management Console e abra o CloudWatch console em https://console.aws.amazon.com/cloudwatch/.
2. No painel de navegação, escolha Alarmes e escolha Criar alarme. Isso abre o Assistente de Criação de Alarmes.
3. Escolha Selecionar métrica.
4. Na guia Todas as métricas, escolha Fraud Detector.
5. Escolha Por ID do detector e, em seguida, escolha a GetEventPredictionmétrica.

6. Escolha a guia Graphed metrics (Métricas em gráfico).
7. Em Estatística, selecione Soma.
8. Escolha Selecionar métrica.
9. Em Condições, escolha Estático para o tipo Limite e Maior para Sempre que... e, em seguida, insira um valor máximo de sua escolha. Escolha Próximo.
10. Para enviar alarmes para um tópico existente do Amazon SNS, em Enviar notificação para:, escolha um tópico existente do SNS. Para definir o nome e os endereços de e-mail para uma nova lista de assinaturas de e-mail, escolha Nova lista. CloudWatch salva a lista e a exibe no campo para que você possa usá-la para definir futuros alarmes.

   > **Note**
   >
   > Se você usar Nova lista para criar um novo tópico do Amazon SNS, os endereços de e-mail deverão ser verificados antes que os destinatários desejados recebam as notificações. O Amazon SNS envia só e-mails quando o alarme entra em um estado de alarme. Se essa alteração no estado do alarme ocorrer antes da verificação dos endereços de e-mail, os destinatários pretendidos não receberão uma notificação.

11. Escolha Próximo. Adicione um nome e uma descrição opcional para seu alarme. Escolha Próximo.
12. Escolha Create Alarm.

Métricas do Amazon Fraud Detector

O Amazon Fraud Detector envia as seguintes métricas para CloudWatch. Todas as métricas suportam essas estatísticas:`Average`,`Minimum`,`Maximum`,`Sum`.

Métrica	Descrição
`GetEventPrediction`	O número de solicitações de GetEventPrediction API. Dimensões válidas: `DetectorID`
`GetEventPredictionLatency`	O intervalo de tempo necessário para responder a uma solicitação do cliente a partir da GetEventPrediction solicitação.

Métrica	Descrição
	Dimensões válidas: `DetectorID` Unidade: milissegundos
`GetEventPrediction4XXError`	O número de GetEventPrediction solicitações em que o Amazon Fraud Detector retornou um código de resposta HTTP 4xx. Para cada resposta 4xx, 1 é enviada. Dimensões válidas: `DetectorID`
`GetEventPrediction5XXError`	O número de GetEventPrediction solicitações em que o Amazon Fraud Detector retornou um código de resposta HTTP 5xx. Para cada resposta 5xx, 1 é enviada. Dimensões válidas: `DetectorID`
`Prediction`	O número de previsões. 1 é enviado em caso de sucesso. Dimensões válidas:`DetectorID` , `DetectorVersionID`
`PredictionLatency`	O intervalo de tempo gasto para uma operação de previsão. Dimensões válidas:`DetectorID` , `DetectorVersionID` Unidade: milissegundos
`PredictionError`	O número de previsões em que o Amazon Fraud Detector encontrou um erro. 1 é enviado se um erro for encontrado. Dimensões válidas:`DetectorID` , `DetectorVersionID`

Métrica	Descrição
`VariableUsed`	O número de GetEventPrediction solicitações em que a variável foi usada como parte da avaliação. Dimensões válidas:`DetectorID` ,`DetectorVersionID` , `VariableName`
`VariableDefaultReturned`	O número de GetEventPrediction solicitações em que a variável não estava presente como parte dos atributos do evento e, portanto, o valor padrão da variável foi usado durante a avaliação. Dimensões válidas:`DetectorID` ,`DetectorVersionID` , `VariableName`
`RuleNotEvaluated`	O número de GetEventPrediction solicitações em que a regra não foi avaliada porque uma regra anterior correspondeu. Dimensões válidas:`DetectorID` ,`DetectorVersionID` , `RuleID`
`RuleEvaluateTrue`	O número de GetEventPrediction solicitações em que a regra foi acionada como verdadeira e o resultado da regra foi retornado. Dimensões válidas:`DetectorID` ,`DetectorVersionID` , `RuleID`
`RuleEvaluateFalse`	O número de GetEventPrediction solicitações em que a regra foi avaliada como False. Dimensões válidas:`DetectorID` ,`DetectorVersionID` , `RuleID`

Métrica	Descrição
`RuleEvaluateError`	O número de GetEventPrediction solicitações em que a regra é avaliada com erro Dimensões válidas:`DetectorID` ,`DetectorVersionID` , `RuleID`
`OutcomeReturned`	O número de GetEventPrediction chamadas em que o resultado especificado foi retornado. Dimensões válidas:`DetectorID` ,`DetectorVersionID` , `OutcomeName`
`ModelInvocation (Amazon SageMaker model endpoint)`	O número de GetEventPrediction solicitações em que o endpoint do SageMaker modelo foi invocado como parte da avaliação. Dimensões válidas:`DetectorID` ,`DetectorVersionID` , `ModelEndpoint`
`ModelInvocationError (Amazon SageMaker model endpoint)`	O número de GetEventPrediction solicitações em que o endpoint do SageMaker modelo invocado retornou um erro durante a avaliação. Dimensões válidas:`DetectorID` ,`DetectorVersionID` , `ModelEndpoint`
`ModelInvocationLatency (Amazon SageMaker model endpoint)`	O intervalo de tempo gasto pelo modelo importado para responder, conforme visualizado pelo Amazon Fraud Detector. Esse intervalo inclui somente a invocação do modelo. Dimensões válidas:`DetectorID` ,`DetectorVersionID` , `ModelEndpoint` Unidade: milissegundos

Métrica	Descrição
`ModelInvocation`	O número de GetEventPrediction solicitações em que o modelo foi invocado como parte da avaliação. Dimensões válidas:`DetectorID` ,`DetectorVersionID` ,`ModelType` , `ModelID`
`ModelInvocationError`	O número de GetEventPrediction solicitações em que o modelo Amazon Fraud Detector retornou um erro durante a avaliação. Dimensões válidas:`DetectorID` ,`DetectorVersionID` ,`ModelType` , `ModelID`
`ModelInvocationLatency`	O intervalo de tempo gasto pelo modelo Amazon Fraud Detector para responder, conforme visualizado pelo Amazon Fraud Detector. Esse intervalo inclui somente a invocação do modelo. Dimensões válidas:`DetectorID` ,`DetectorVersionID` ,`ModelType` , `ModelID` Unidade: milissegundos

Registrando chamadas da API do Amazon Fraud Detector com AWS CloudTrail

O Amazon Fraud Detector é integrado com AWS CloudTrail, um serviço que fornece um registro das ações realizadas por um usuário, função ou AWS serviço no Amazon Fraud Detector. CloudTrail captura todas as chamadas de API para o Amazon Fraud Detector como eventos, incluindo chamadas do console do Amazon Fraud Detector e chamadas de código para as APIs do Amazon Fraud Detector.

Se você criar uma trilha, poderá habilitar a entrega contínua de CloudTrail eventos para um bucket do Amazon S3, incluindo eventos para o Amazon Fraud Detector. Se você não configurar uma trilha, ainda poderá ver os eventos mais recentes no CloudTrail console no Histórico de eventos. Usando as informações coletadas por CloudTrail, você pode determinar a solicitação que foi feita ao Amazon

Fraud Detector, o endereço IP a partir do qual a solicitação foi feita, quem fez a solicitação, quando ela foi feita e detalhes adicionais.

Para saber mais sobre isso CloudTrail, consulte o Guia AWS CloudTrail do usuário.

Informações sobre o Amazon Fraud Detector em CloudTrail

CloudTrail é ativado em sua AWS conta quando você cria a conta. Quando ocorre uma atividade no Amazon Fraud Detector, essa atividade é registrada em um CloudTrail evento junto com outros eventos AWS de serviço no histórico de eventos. Você pode visualizar, pesquisar e baixar eventos recentes em sua AWS conta. Para obter mais informações, consulte Visualização de eventos com histórico de CloudTrail eventos.

Para um registro contínuo dos eventos em sua AWS conta, incluindo eventos do Amazon Fraud Detector, crie uma trilha. Uma trilha permite CloudTrail entregar arquivos de log para um bucket do Amazon S3. Por padrão, quando você cria uma trilha no console, ela é aplicada a todas as regiões da AWS. A trilha registra eventos de todas as regiões na AWS partição e entrega os arquivos de log ao bucket do Amazon S3 que você especificar. Além disso, você pode configurar outros AWS serviços para analisar e agir com base nos dados de eventos coletados nos CloudTrail registros. Para mais informações, consulte:

- Visão Geral para Criar uma Trilha
- CloudTrail Serviços e integrações compatíveis
- Configurando notificações do Amazon SNS para CloudTrail
- Recebendo arquivos de CloudTrail log de várias regiões e recebendo arquivos de CloudTrail log de várias contas

O Amazon Fraud Detector suporta o registro de cada ação (operação de API) como um evento em arquivos de CloudTrail log. Para obter mais informações, consulte Ações.

Cada entrada de log ou evento contém informações sobre quem gerou a solicitação. As informações de identidade ajudam a determinar:

- Se a solicitação foi feita com credenciais de usuário da raiz ou do .
- Se a solicitação foi feita com credenciais de segurança temporárias de um perfil ou de um usuário federado.
- Se a solicitação foi feita por outro AWS serviço.

Para obter mais informações, consulte o elemento CloudTrail UserIdentity.

Compreendendo as entradas do arquivo de log do Amazon Fraud Detector

Uma trilha é uma configuração que permite a entrega de eventos como arquivos de log para um bucket do Amazon S3 que você especificar. CloudTrail os arquivos de log contêm uma ou mais entradas de log. Um evento representa uma única solicitação de qualquer fonte e inclui informações sobre a operação solicitada, a data e a hora da operação, os parâmetros da solicitação e assim por diante. CloudTrail os arquivos de log não são um rastreamento de pilha ordenado das chamadas públicas de API, portanto, eles não aparecem em nenhuma ordem específica.

O exemplo a seguir mostra uma entrada de CloudTrail registro que demonstra a `GetDetectors` operação.

```
{
    "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"
}
```

Solução de problemas

As seções a seguir ajudam você a solucionar problemas que você pode encontrar ao trabalhar com o Amazon Fraud Detector

Solucionar problemas com dados de treinamento

Use as informações desta seção para ajudar a diagnosticar e resolver problemas que você possa ver no painel de diagnóstico de treinamento de modelos no console do Amazon Fraud Detector ao treinar seu modelo.

Os problemas exibidos no painel de diagnóstico de treinamento do modelo são categorizados da seguinte forma. O requisito para resolver o problema depende da categoria do problema.

- Erro - faz com que o treinamento do modelo falhe. Esses problemas devem ser resolvidos para que o modelo seja treinado com sucesso.
- Aviso - faz com que o treinamento do modelo continue, no entanto, algumas das variáveis podem estar sendo excluídas do processo de treinamento. Consulte as orientações relevantes nesta seção para melhorar a qualidade do seu conjunto de dados.
- Informa (Informações) - não tem impacto no treinamento do modelo e todas as variáveis são usadas para treinamento. Recomendamos que você verifique as orientações relevantes nesta seção para melhorar ainda mais a qualidade do seu conjunto de dados e do desempenho do modelo.

Tópicos

- Valores de variáveis ausentes
- Valores variáveis exclusivos insuficientes
- Expressão de variável incorreta
- Entidades exclusivas insuficientes

Taxa de fraude instável no conjunto de dados fornecido

Tipo de problema: Erro

Descrição

A taxa de fraude nos dados fornecidos é muito instável ao longo do tempo. Certifique-se de que suas fraudes e eventos legítimos sejam amostrados uniformemente ao longo do tempo.

Causa

Esse erro ocorre se a fraude e os eventos legítimos em seu conjunto de dados forem distribuídos de forma desigual e forem retirados de diferentes horários. O processo de treinamento do modelo Amazon Fraud Detector amostra e particiona seu conjunto de dados com base em EVENT_TIMESTAMP. Por exemplo, se seu conjunto de dados consistir em eventos de fraude retirados dos últimos 6 meses, mas somente o último mês de eventos legítimos for incluído, o conjunto de dados será considerado instável. Um conjunto de dados instável pode levar a vieses na avaliação do desempenho do modelo.

Solução

Certifique-se de fornecer os dados de eventos fraudulentos e legítimos no mesmo horário, para que a taxa de fraude não mude drasticamente com o tempo.

Dados insuficientes

1. Tipo de problema: Erro

   Descrição

   Menos de 50 linhas são rotuladas como eventos fraudulentos. Garanta que eventos fraudulentos e legítimos excedam a contagem mínima de 50 e treine novamente o modelo.

   Causa

Esse erro ocorre se seu conjunto de dados tiver menos eventos rotulados como fraudulentos do que o necessário para o treinamento do modelo. O Amazon Fraud Detector exige pelo menos 50 eventos fraudulentos para treinar seu modelo.

Solução

Certifique-se de que seu conjunto de dados inclua no mínimo 50 eventos fraudulentos. Você pode garantir isso cobrindo um período de tempo mais longo, se necessário.

2. Tipo de problema: Erro

   Descrição

   Menos de 50 linhas são rotuladas como eventos legítimos. Garanta que eventos fraudulentos e legítimos excedam a contagem mínima de $ threshold e treine novamente o modelo.

   Causa

   Esse erro ocorre se seu conjunto de dados tiver menos eventos rotulados como legítimos do que o necessário para o treinamento do modelo. O Amazon Fraud Detector exige pelo menos 50 eventos legítimos para treinar seu modelo.

   Solução

   Certifique-se de que seu conjunto de dados inclua no mínimo 50 eventos legítimos. Você pode garantir isso cobrindo um período de tempo mais longo, se necessário.

3. Tipo de problema: Erro

   Descrição

   O número de entidades exclusivas associadas à fraude é inferior a 100. Considere incluir mais exemplos de entidades fraudulentas para melhorar o desempenho.

   Causa

   Esse erro ocorre se seu conjunto de dados tiver menos entidades com eventos fraudulentos do que o necessário para o treinamento do modelo. O modelo Transaction Fraud Insights (TFI) exige pelo menos 100 entidades com eventos de fraude para garantir a cobertura máxima do espaço de fraude. O modelo pode não se generalizar bem se todos os eventos de fraude forem realizados por um pequeno grupo de entidades.

Solução

Certifique-se de que seu conjunto de dados inclua pelo menos 100 entidades com eventos fraudulentos. Você pode garantir que isso cubra um período de tempo mais longo, se necessário.

4. Tipo de problema: Erro

   Descrição

   O número de entidades exclusivas associadas a entidades legítimas é inferior a 100. Considere incluir mais exemplos de entidades legítimas para melhorar o desempenho.

   Causa

   Esse erro ocorre se seu conjunto de dados tiver menos entidades com eventos legítimos do que o necessário para o treinamento do modelo. O modelo Transaction Fraud Insights (TFI) exige pelo menos 100 entidades com eventos legítimos para garantir a cobertura máxima do espaço de fraude. O modelo pode não se generalizar bem se todos os eventos legítimos forem executados por um pequeno grupo de entidades.

   Solução

   Certifique-se de que seu conjunto de dados inclua pelo menos 100 entidades com eventos legítimos. Você pode garantir que isso cubra um período de tempo mais longo, se necessário.

5. Tipo de problema: Erro

   Descrição

   Menos de 100 linhas estão no conjunto de dados. Certifique-se de que haja mais de 100 linhas no conjunto de dados total e que pelo menos 50 linhas sejam rotuladas como fraudulentas.

   Causa

   Esse erro ocorre se seu conjunto de dados contiver menos de 100 registros. O Amazon Fraud Detector exige dados de pelo menos 100 eventos (registros) em seu conjunto de dados para treinamento de modelos.

   Solução

   Verifique se você tem dados de mais de 100 eventos em seu conjunto de dados.

Valores de EVENT_LABEL ausentes ou diferentes

1. Tipo de problema: Erro

   Descrição

   Mais de 1% da coluna EVENT_LABEL são nulos ou são valores diferentes dos definidos na configuração do modelo. **`$label_values`** Verifique se você tem menos de 1% dos valores ausentes na coluna EVENT_LABEL e se os valores são aqueles definidos na configuração do modelo. **`$label_values`**

   Causa

   Esse erro ocorre devido a um dos seguintes motivos:

   - Mais de 1% dos registros no arquivo CSV contendo seus dados de treinamento têm valores ausentes na coluna EVENT_LABEL.
   - Mais de 1% dos registros no arquivo CSV contendo seus dados de treinamento têm valores na coluna EVENT_LABEL que são diferentes daqueles associados ao seu tipo de evento.

   O modelo Online Fraud Insights (OFI) exige que a coluna EVENT_LABEL em cada registro seja preenchida com um dos rótulos associados ao seu tipo de evento (ou mapeado). `CreateModelVersion`

   Solução

   Se esse erro for devido aos valores ausentes de EVENT_LABEL, considere atribuir rótulos adequados a esses registros ou excluí-los do seu conjunto de dados. Se esse erro ocorrer porque os rótulos de alguns registros não estão entre eles**`label_values`**, certifique-se de adicionar todos os valores na coluna EVENT_LABEL aos rótulos do tipo de evento e mapeados como fraudulentos ou legítimos (fraudulentos, legítimos) na criação do modelo.

2. Tipo de problema: Informações

   Descrição

   Sua coluna EVENT_LABEL contém valores nulos ou valores de rótulo diferentes dos definidos na configuração do modelo. **`$label_values`** Esses valores inconsistentes foram convertidos em “não fraudulentos” antes do treinamento.

   Causa

Você obtém essas informações por um dos seguintes motivos:

- Menos de 1% dos registros no arquivo CSV contendo seus dados de treinamento têm valores ausentes na coluna EVENT_LABEL
- Menos de 1% dos registros no arquivo CSV contendo seus dados de treinamento têm valores na coluna EVENT_LABEL que são diferentes daqueles associados ao seu tipo de evento.

O treinamento do modelo em ambos os casos será bem-sucedido. No entanto, os valores de rótulo desses eventos que têm valores de rótulo ausentes ou não mapeados são convertidos em legítimos. Se você considerar que isso é um problema, siga a solução fornecida abaixo.

Solução

Se houver valores de EVENT_LABEL ausentes em seu conjunto de dados, considere eliminar esses registros do seu conjunto de dados. Se os valores fornecidos para esses EVENT_LABELS não forem mapeados, certifique-se de que todos esses valores sejam mapeados como fraudulentos ou legítimos (fraudulentos, legítimos) para cada evento.

Valores de EVENT_TIMESTAMP ausentes ou incorretos

1. Tipo de problema: Erro

   Descrição

   Seu conjunto de dados de treinamento contém EVENT_TIMESTAMP com timestamps que não estão em conformidade com os formatos aceitos. Verifique se o formato é um dos formatos de data e hora aceitos.

   Causa

   Esse erro ocorre se a coluna EVENT_TIMESTAMP contiver um valor que não esteja em conformidade com os formatos de timestamp compatíveis com o Amazon Fraud Detector.

   Solução

   Certifique-se de que os valores fornecidos para a coluna EVENT_TIMESTAMP estejam em conformidade com os formatos de carimbo de data/hora compatíveis. Se você tiver valores ausentes na coluna EVENT_TIMESTAMP, você pode preenchê-los com valores usando o formato

de carimbo de data/hora compatível ou considerar descartar completamente o evento em vez de inserir cadeias de caracteres como, ou. `none` `null` `missing`

2. Tipo de problema: Erro

   Seu conjunto de dados de treinamento contém EVENT_TIMESTAMP com valores ausentes. Certifique-se de que você não tenha valores faltantes.

   Causa

   Esse erro ocorre se a coluna EVENT_TIMESTAMP em seu conjunto de dados tiver valores ausentes. O Amazon Fraud Detector exige que a coluna EVENT_TIMESTAMP em seu conjunto de dados tenha valores.

   Solução

   Certifique-se de que a coluna EVENT_TIMESTAMP em seu conjunto de dados tenha valores e que esses valores estejam em conformidade com os formatos de carimbo de data/hora compatíveis. Se você tiver valores ausentes na coluna EVENT_TIMESTAMP, você pode preenchê-los com valores usando o formato de carimbo de data/hora compatível ou considerar descartar completamente o evento em vez de inserir cadeias de caracteres como, ou. `none` `null` `missing`

Dados não ingeridos

Tipo de problema: Erro

Descrição

Nenhum evento ingerido foi encontrado para treinamento. Verifique sua configuração de treinamento.

Causa

Esse erro ocorre se você estiver criando um modelo com dados de eventos armazenados com o Amazon Fraud Detector, mas não importou seu conjunto de dados para o Amazon Fraud Detector antes de começar a treinar seu modelo.

Solução

Use a operação da `SendEvent` API, a operação da `CreateBatchImportJob` API ou o recurso de importação em lote no console do Amazon Fraud Detector para primeiro importar os dados do evento

e depois treinar seu modelo. Consulte Conjuntos de dados de eventos armazenados para obter mais informações.

> **Note**
>
> Recomendamos esperar 10 minutos depois de terminar de importar seus dados antes de usá-los para treinar seu modelo.

Você pode usar o console Amazon Fraud Detector para verificar o número de eventos já armazenados para cada tipo de evento. Consulte Visualização de métricas de seus eventos armazenados para obter mais informações.

Variáveis insuficientes

Tipo de problema: Erro

Descrição

O conjunto de dados deve conter pelo menos 2 variáveis adequadas para treinamento.

Causa

Esse erro ocorre se o conjunto de dados contiver menos de duas variáveis adequadas para o treinamento do modelo. O Amazon Fraud Detector considera uma variável adequada para o treinamento de modelos somente se ela for aprovada em todas as validações. Se uma variável falhar na validação, ela será excluída no treinamento do modelo e você verá uma mensagem no Diagnóstico do treinamento do modelo.

Solução

Certifique-se de que seu conjunto de dados tenha pelo menos duas variáveis preenchidas com valores e aprovado em todas as validações de dados. Observe que a linha de metadados do evento em que você forneceu os cabeçalhos das colunas (EVENT_TIMESTAMP, EVENT_ID, ENTITY_ID, EVENT_LABEL etc.) não é considerada variável.

Tipo de variável ausente ou incorreto

Tipo de problema: Aviso

Descrição

O tipo de dados esperado para **$variable_name** é NUMERIC. Revise e **$variable_name** atualize seu conjunto de dados e treine novamente o modelo.

Causa

Você receberá esse aviso se uma variável for definida como uma variável NUMERIC, mas no conjunto de dados ela tiver valores que não podem ser convertidos em NUMERIC. Como resultado, essa variável é excluída no treinamento do modelo.

Solução

Se você quiser mantê-la como uma variável NUMERIC, certifique-se de que os valores fornecidos possam ser convertidos em números flutuantes. Observe que, se a variável contiver valores ausentes, não os preencha com cadeias de caracteres como `nonenenull`, ou`missing`. Se a variável contiver valores não numéricos, recrie-a como um tipo de variável CATEGÓRICA ou FREE_FORM_TEXT.

Valores de variáveis ausentes

Tipo de problema: Aviso

Descrição

Maiores do que **$threshold** valores para **$variable_name** estão faltando em seu conjunto de dados de treinamento. Considere modificar seu conjunto **$variable_name** de dados e treinar novamente para melhorar o desempenho.

Causa

Você receberá esse aviso se a variável especificada estiver sendo descartada devido a muitos valores ausentes. O Amazon Fraud Detector permite valores faltantes para uma variável. No entanto, se uma variável tiver muitos valores ausentes, ela não contribui muito para o modelo e essa variável é descartada no treinamento do modelo.

Solução

Primeiro, verifique se esses valores faltantes não se devem a erros na coleta e preparação dos dados. Se forem erros, considere retirá-los do treinamento de modelos. No entanto, se você acredita que esses valores ausentes são valiosos e ainda deseja manter essa variável, pode preencher manualmente os valores ausentes com uma constante no treinamento do modelo e na inferência em tempo real.

Valores variáveis exclusivos insuficientes

Tipo de problema: Aviso

Descrição

A contagem de valores exclusivos de **$variable_name** é menor que 100. Revise e **$variable_name** atualize seu conjunto de dados e treine novamente o modelo.

Causa

Você receberá esse aviso se o número de valores exclusivos da variável especificada for menor que 100. Os limites variam de acordo com o tipo de variável. Com poucos valores exclusivos, existe o risco de o conjunto de dados não ser geral o suficiente para cobrir o espaço de recursos dessa variável. Como resultado, o modelo pode não se generalizar bem nas previsões em tempo real.

Solução

Primeiro, certifique-se de que a distribuição variável seja representativa do tráfego comercial real. Em seguida, você pode adotar mais variáveis bem treinadas com maior cardinalidade, como usar `full_customer_name` em vez de `first_name` e `last_name` separadamente, ou alterar o tipo de variável para CATEGÓRICO, o que permite menor cardinalidade.

Expressão de variável incorreta

1. Tipo de problema: Informações

   Descrição

   Mais de 50% dos **$email_variable_name** valores não correspondem à expressão regular esperada http://emailregex.com. Considere modificar seu conjunto **$email_variable_name** de dados e treinar novamente para melhorar o desempenho.

   Causa

   Essas informações serão exibidas se mais de 50% dos registros em seu conjunto de dados tiverem valores de e-mail que não estejam em conformidade com uma expressão de e-mail regular e, portanto, falharem na validação.

   Solução

Formate os valores das variáveis de e-mail para que estejam em conformidade com a expressão regular. Se faltarem valores de e-mail, recomendamos deixá-los vazios em vez de preenchê-los com cadeias de caracteres como `nonenull`, ou`missing`.

2. Tipo de problema: Informações

   Descrição

   Mais de 50% dos **`$IP_variable_name`** valores não correspondem à expressão regular para endereços IPv4 ou IPv6 https://digitalfortress.tech/tricks/top-15 - /. commonly-used-regex Considere modificar seu conjunto **`$IP_variable_name`** de dados e treinar novamente para melhorar o desempenho.

   Causa

   Essas informações serão exibidas se mais de 50% dos registros em seu conjunto de dados tiverem valores de IP que não estejam em conformidade com uma expressão de IP regular e, portanto, falharem na validação.

   Solução

   Formate os valores de IP para que estejam em conformidade com a expressão regular. Se faltarem valores de IP, recomendamos deixá-los vazios em vez de preenchê-los com cadeias de caracteres como `nonenull`, ou`missing`.

3. Tipo de problema: Informações

   Descrição

   Mais de 50% dos **`$phone_variable_name`** valores não correspondem à expressão regular básica do telefone /$pattern/. Considere modificar seu conjunto **`$phone_variable_name`** de dados e treinar novamente para melhorar o desempenho.

   Causa

   Essas informações serão exibidas se mais de 50% dos registros em seu conjunto de dados tiverem números de telefone que não estejam em conformidade com uma expressão normal de número de telefone e, portanto, falharem na validação.

   Solução

Formate os números de telefone de acordo com a expressão regular. Se faltarem números de telefone, recomendamos deixá-los vazios em vez de preenchê-los com sequências de caracteres comonone,`null`, ou`missing`.

Entidades exclusivas insuficientes

Tipo de problema: Informações

Descrição

O número de entidades exclusivas é inferior a 1500. Considere incluir mais dados para melhorar o desempenho.

Causa

Essas informações são exibidas se seu conjunto de dados tiver um número menor de entidades exclusivas do que o número recomendado. O modelo Transaction Fraud Insights (TFI) usa agregados de séries temporais e recursos genéricos de transação para fornecer o melhor desempenho. Se seu conjunto de dados tiver poucas entidades exclusivas, a maioria dos seus dados genéricos, como IP_ADDRESS, EMAIL_ADDRESS, talvez não tenha valores exclusivos. Então, também existe o risco de que esse conjunto de dados não seja geral o suficiente para cobrir o espaço de recursos dessa variável. Como resultado, o modelo pode não se generalizar bem em transações de novas entidades.

Solução

Inclua mais entidades. Estenda o intervalo de tempo dos dados de treinamento, se necessário.

Cotas

SuaConta da AWS tem cotas padrão, anteriormente chamadas de limites, para cada serviço da. A menos que especificado de outra forma, cada cota é específica da região. É possível solicitar um aumento de cota para todas cotas ajustpor da. Para obter mais informações, consulte Solicitar um aumento de cota

As tabelas a seguir descrevem as cotas do Amazon Fraud Detector por componente.

Modelos por Amazon Frarararararapor

Nome da cota	Cota padrão	Ajustável
Tamanho dos dados de treinamento	5 GB	Não
Modelos por conta	50	Não
Verpor conta por conta da	200	Não
Versões de modelo implantadas por conta	5	Não
Trabalhos de treinamento simultâneos por conta	3	Não
Trabalhos de treinamento simultâneos por modelo	1	Não

Fraud Detector da Amazon/variáveis/ resultados/regras

Nome da cota	Cota padrão	Ajustável
Varipor conta por conta da	5000	Não
Regras por conta da	5000	Não

Nome da cota	Cota padrão	Ajustável
Listas por regra	3	Não
Resultados por conta por conta da	5000	Não
Detpor conta por conta da	100	Não
Listas por detector	30	Não
Versões de rascunho por detector	100	Não
Modelos por versão de detector	10	Não
Rpor conta por conta da	100	Não
Tipos por conta da	100	Não
Tipos por conta da	100	Não

Amazon Frarapor Amazon Frararapor

Nome da cota	Cota padrão	Ajustável
GetEventPrediction Champor conta por conta da	200 TPS	Sim
Tamanho da carga útil por chamada GetEventPrediction de API	256 KB	Não
Número de entradas por chamada GetEventPrediction de API	5000	Não

Histórico do documento

A tabela a seguir descreve mudanças importantes no Guia do usuário do Amazon Fraud Detector. Também atualizamos o Guia do usuário do Amazon Fraud Detector com frequência para abordar o feedback que você nos envia.

Alteração	Descrição	Data
Novos tipos de variáveis e dados	O Amazon Fraud Detector apresenta novos tipos de variáveis e um tipo de dados que você pode usar para extrair informações úteis.	5 de junho de 2023
Orquestração de eventos	A orquestração de eventos facilita o envio de eventos Serviços da AWS para processamento posterior usando a Amazon. EventBrid ge	30 de maio de 2023
Listas	O recurso Listas permite que você faça referência a um conjunto de valores, como endereços IP ou endereços de e-mail, como parte de uma regra. Use listas em uma regra para permitir ou negar acesso ou transação.	14 de fevereiro de 2023
Explorador de modelos de dados	O Data Models Explorer fornece informações sobre os elementos de dados exigidos pelo Amazon Fraud Detector para criar seu modelo de detecção de fraudes. Use o explorador de modelos de	15 de dezembro de 2022

	dados antes de preparar seu conjunto de dados de eventos.	
Modelo Account Takeover Insights	Use o modelo Account Takeover Insights (ATI) para detectar contas comprometidas por meio de aquisições maliciosas, phishing ou roubo de credenciais.	21 de julho de 2022
Atualização do capítulo	Atualizou o capítulo introdutório com informações adicionais sobre o Amazon Fraud Detector	11 de abril de 2022
Enriquecimento variável	Ative o enriquecimento de alguns dos dados brutos que você fornece para aumentar o desempenho dos modelos que usam esses elementos de dados e que foram treinados antes de 8 de fevereiro de 2022.	8 de fevereiro de 2022
Políticas de exclusão	Use políticas de exclusão para optar por não usar seus dados de eventos para desenvolver ou melhorar a qualidade do Amazon Fraud Detector.	6 de janeiro de 2022
Prevenção confusa de adjuntos	Crie políticas para impedir que uma entidade terceirizada ou de serviços cruzados manipule uma entidade com permissão para agir em seu nome para obter acesso aos recursos em sua conta.	6 de dezembro de 2021

Criar conjunto de dados do evento	Use a orientação fornecida em Criar conjunto de dados de eventos para preparar e coletar dados para treinar seu modelo.	22 de novembro de 2021
Explicações de previsão	Use as explicações de previsão para obter informaçõ es sobre como cada variável de evento impactou as pontuações de previsão de fraudes do seu modelo.	10 de novembro de 2021
Solucionar problemas	Use as informações em Solucionar problemas de dados de treinamento para ajudar a diagnosticar e resolver problemas que você pode ver no console do Amazon Fraud Detector ao treinar seu modelo.	11 de outubro de 2021
Modelo de insights sobre fraudes em transações	Use o modelo Transaction Fraud Insights (TFI) para detectar fraudes on-line ou em card-not-present transações.	11 de outubro de 2021

Eventos armazenados	Armazene seus dados de eventos no Amazon Fraud Detector e use os dados armazenados para treinar seus modelos posteriormente. Ao armazenar dados de eventos no Amazon Fraud Detector, você pode treinar modelos que usam variáveis computadas automaticamente para melhorar o desempenho, simplificar o treinamento de modelos e atualizar rótulos de fraude para fechar o ciclo de feedback do aprendizado de máquina.	11 de outubro de 2021
Importância da variável do modelo	Use a importância da variável do modelo para obter informações sobre o que está impulsionando o desempenho do seu modelo para cima ou para baixo e quais variáveis do seu modelo contribuem mais. Em seguida, ajuste seu modelo para melhorar o desempenho geral.	09 de julho de 2021
Integração com AWS CloudFormation	Use AWS CloudFormation para gerenciar seus recursos do Amazon Fraud Detector.	10 de maio de 2021
Previsões em lote	Use as previsões em lote para obter previsões para um conjunto de eventos que não exigem pontuação em tempo real.	31 de março de 2021

Reformulação do capítulo	Reformulação de Get started e de outras seções	17 de julho de 2020
Versão inicial	Versão inicial	2 de dezembro de 2019

As traduções são geradas por tradução automática. Em caso de conflito entre o conteúdo da tradução e da versão original em inglês, a versão em inglês prevalecerá.