aws

Guide de l’utilisateur

Amazon Fraud Detector

Version latest

Amazon Fraud Detector: Guide de l’utilisateur

Table of Contents

Qu'est-ce qu'Amazon Fraud Detector ?

Amazon Fraud Detector est un service de détection des fraudes entièrement géré qui automatise la détection des activités potentiellement frauduleuses en ligne. Ces activités incluent des transactions non autorisées et la création de faux comptes. Amazon Fraud Detector utilise le machine learning pour analyser vos données. Pour ce faire, il s'appuie sur l'expertise chevronnée de plus de 20 ans d'expérience dans la détection des fraudes chez Amazon.

Vous pouvez utiliser Amazon Fraud Detector pour créer des modèles de détection des fraudes personnalisés, ajouter une logique décisionnelle pour interpréter les évaluations des fraudes du modèle et attribuer des résultats tels que le passage ou le renvoi pour examen à chaque évaluation de fraude possible. Avec Amazon Fraud Detector, vous n'avez pas besoin d'expertise en machine learning pour détecter les activités frauduleuses.

Pour commencer, collectez et préparez les données sur les fraudes que vous avez collectées au sein de votre organisation. Amazon Fraud Detector utilise ensuite ces données pour former, tester et déployer un modèle de détection des fraudes personnalisé en votre nom. Dans le cadre de ce processus, Amazon Fraud Detector utilise des modèles de machine learning qui ont appris des modèles de AWS fraude grâce à l'expertise d'Amazon en matière de fraude afin d'évaluer vos données sur les fraudes et de générer des scores et des données de performance des modèles. Vous configurez la logique de décision pour interpréter le score du modèle et attribuer des résultats indiquant comment traiter chaque évaluation de fraude.

Avantages

Amazon Fraud Detector offre les avantages suivants. Ces avantages vous permettent de détecter rapidement les fraudes sans avoir à investir le temps et les ressources traditionnellement nécessaires à la création et à la maintenance d'un système de gestion des fraudes.

Création automatique de modèles de fraude

Les modèles de détection des fraudes d'Amazon Fraud Detector sont des modèles d'apprentissage automatique entièrement automatisés personnalisés pour répondre aux besoins spécifiques de votre entreprise. Vous pouvez utiliser les modèles Amazon Fraud Detector pour identifier les fraudes potentielles dans toutes les transactions en ligne, telles que la création de nouveaux comptes, les paiements en ligne et le paiement en tant qu'invité.

Les modèles de fraude étant créés par le biais d'un processus automatisé, vous pouvez renoncer à de nombreuses étapes associées à la création et à la formation d'un modèle. Ces étapes incluent la validation et l'enrichissement des données, l'ingénierie des fonctionnalités, la sélection d'algorithmes, le réglage des hyperparamètres et le déploiement du modèle.

Pour créer un modèle de détection des fraudes à l'aide d'Amazon Fraud Detector, il vous suffit de télécharger l'historique des fraudes de votre entreprise et de sélectionner le type de modèle. Ensuite, Amazon Fraud Detector trouve automatiquement l'algorithme de détection des fraudes le mieux adapté à votre cas d'utilisation et crée le modèle. Il n'est pas nécessaire de connaître le codage ou de posséder une expertise en apprentissage automatique pour créer des modèles de détection des fraudes.

Des modèles de fraude qui évoluent et apprennent

Les modèles de détection des fraudes doivent constamment évoluer pour suivre l'évolution du paysage de la fraude. Amazon Fraud Detector le fait automatiquement en calculant des informations telles que l'âge du compte, le temps écoulé depuis la dernière activité et le nombre d'activités. Votre modèle apprend ainsi à faire la différence entre les clients de confiance qui effectuent fréquemment des transactions et les tentatives continues typiques des fraudeurs. Cela permet de maintenir les performances de votre modèle plus longtemps entre les séances de réentraînement.

Visualisation des performances du modèle de fraude

Une fois que votre modèle a été entraîné à l'aide des données que vous fournissez, Amazon Fraud Detector valide les performances de votre modèle. Il fournit également des outils visuels vous permettant d'évaluer les performances. Pour chaque modèle que vous entraînez, vous pouvez consulter le score de performance du modèle, le graphique de distribution des scores, la matrice de confusion, le tableau des seuils et toutes les entrées que vous avez fournies classées en fonction de leur impact sur les performances du modèle. À l'aide de ces outils de performance, vous pouvez découvrir les performances de votre modèle et les entrées qui déterminent les performances de votre modèle. Si nécessaire, vous pouvez modifier votre modèle pour améliorer ses performances globales.

Prédiction des fraudes

Amazon Fraud Detector génère des prévisions de fraude pour les activités commerciales de votre organisation. La prédiction des fraudes est une évaluation du risque de fraude d'une activité commerciale. Amazon Fraud Detector génère des prédictions en utilisant la logique de prédiction avec les données associées à l'activité. Vous avez fourni ces données lorsque vous avez créé votre

modèle de détection des fraudes. Vous pouvez obtenir des prévisions de fraude pour une seule activité en temps réel ou obtenir des prévisions de fraude hors ligne pour un ensemble d'activités.

Visualisation des explications relatives aux prévisions de fraude

Amazon Fraud Detector génère des explications de prédiction dans le cadre du processus de prédiction des fraudes. Les explications relatives aux prévisions fournissent un aperçu de l'impact de chaque élément de données utilisé pour entraîner votre modèle sur le score de prédiction des fraudes de votre modèle. Les explications des prédictions sont fournies à l'aide d'outils visuels tels que des tableaux et des graphiques. Vous pouvez utiliser ces outils pour identifier visuellement l'influence de chaque élément de données sur les scores de prédiction. Vous pouvez ensuite utiliser ces informations pour analyser les modèles de fraude dans votre ensemble de données et détecter les biais éventuels. Enfin, vous pouvez également utiliser les explications des prédictions pour identifier les principaux indicateurs de risque lors d'un processus manuel d'enquête sur les fraudes. Cela vous aide à identifier les causes profondes qui conduisent à des prédictions faussement positives.

Actions basées sur des règles

Une fois votre modèle de détection des fraudes formé, vous pouvez ajouter des règles pour prendre des mesures sur les données évaluées, telles que l'acceptation des données, l'envoi de données pour examen ou la collecte de données supplémentaires. Une règle est une condition qui indique à Amazon Fraud Detector comment interpréter les données lors de la prédiction des fraudes. Par exemple, vous pouvez créer une règle signalant les comptes clients suspects à examiner. Vous pouvez configurer cette règle pour qu'elle soit initiée si le score du modèle détecté est supérieur à votre seuil prédéterminé et si le code d'autorisation du paiement du compte (AUTH_CODE) n'est pas valide.

Concepts et termes de base

Voici une liste des principaux concepts et termes utilisés dans Amazon Fraud Detector :

Événement

Un événement est l'activité commerciale de votre organisation qui est évaluée en fonction du risque de fraude. Amazon Fraud Detector génère des prédictions de fraude en fonction des événements.

Étiquette

Une étiquette classe un seul événement comme frauduleux ou légitime. Les étiquettes sont utilisées pour entraîner des modèles de machine learning dans Amazon Fraud Detector.

Entité

Une entité représente qui exécute l'événement. Vous fournissez un identifiant d'entité dans le cadre des données de fraude de votre entreprise pour indiquer l'entité spécifique qui a réalisé l'événement.

Type d'événement

Un type d'événement définit la structure d'un événement envoyé à Amazon Fraud Detector. Cela inclut les données envoyées dans le cadre de l'événement, l'entité qui réalise l'événement (comme un client) et les étiquettes qui classent l'événement. Les types d'événements incluent les transactions de paiement en ligne, les enregistrements de comptes et l'authentification.

Type d'entité

Un type d'entité classe l'entité. Les exemples de classifications incluent le client, le vendeur ou le compte.

Ensemble de données d'événements

Le jeu de données d'événements contient les données historiques de votre entreprise concernant une activité commerciale ou un événement spécifique. Par exemple, l'événement de votre entreprise peut être l'enregistrement d'un compte en ligne. Les données d'un seul événement (enregistrement) peuvent inclure l'adresse IP, l'adresse e-mail, l'adresse de facturation et l'horodatage de l'événement associés. Vous fournissez un ensemble de données d'événements à Amazon Fraud Detector pour créer et entraîner des modèles de détection des fraudes.

Modèle

Un modèle est un résultat d'algorithmes d'apprentissage automatique. Ces algorithmes sont implémentés dans le code et exécutés sur les données d'événements que vous fournissez.

Type de modèle

Le type de modèle définit les algorithmes, les enrichissements et les transformations de fonctionnalités utilisés lors de l'entraînement du modèle. Il définit également les exigences en matière de données pour entraîner le modèle. Ces définitions permettent d'optimiser votre modèle pour un type de fraude spécifique. Vous spécifiez le type de modèle à utiliser lors de la création de votre modèle.

Entraînement d'un modèle

L'entraînement des modèles est le processus qui consiste à utiliser un ensemble de données d'événements fourni pour créer un modèle capable de prédire les événements frauduleux. Toutes

les étapes du processus de formation des modèles sont entièrement automatisées. Ces étapes incluent la validation des données, la transformation des données, l'ingénierie des fonctionnalités, la sélection d'algorithmes et l'optimisation du modèle.

Note du modèle

Le score du modèle est le résultat de l'évaluation des données historiques sur les fraudes de votre entreprise. Au cours du processus de formation du modèle, Amazon Fraud Detector évalue l'ensemble de données pour détecter les activités frauduleuses et génère un score compris entre 0 et 1 000. Pour ce score, 0 représente un faible risque de fraude, tandis que 1000 représente le risque de fraude le plus élevé. Le score lui-même est directement lié au taux de faux positifs (FPR).

Version du modèle

Une version de modèle est un résultat de l'entraînement d'un modèle.

Déploiement de modèle

Le déploiement d'un modèle est un processus permettant d'activer une version du modèle et de la rendre disponible pour générer des prévisions de fraude.

Point de terminaison SageMaker du modèle Amazon

Outre la création de modèles à l'aide d'Amazon Fraud Detector, vous pouvez éventuellement utiliser des points de terminaison de modèles SageMaker hébergés dans les évaluations d'Amazon Fraud Detector.

Pour plus d'informations sur la création d'un modèle dans SageMaker, voir Entraîner un modèle avec Amazon SageMaker.

Détecteur

Un détecteur contient la logique de détection, telle que le modèle et les règles d'un événement particulier que vous souhaitez évaluer pour détecter une fraude. Vous créez un détecteur à l'aide d'une version modèle.

Version du détecteur

Un détecteur peut avoir plusieurs versions, chaque version ayant un statut de `DraftActive`, ou`Inactive`. Une seule version du détecteur peut être en `Active` état à la fois.

Variable

Une variable représente un élément de données associé à un événement que vous souhaitez utiliser dans le cadre d'une prédiction de fraude. Les variables peuvent être envoyées avec un

événement dans le cadre d'une prédiction de fraude ou dérivées, comme le résultat d'un modèle Amazon Fraud Detector ouAmazon SageMaker.

Règle

Une règle est une condition qui indique à Amazon Fraud Detector comment interpréter les valeurs des variables lors d'une prédiction de fraude. Une règle comprend une ou plusieurs variables, une expression logique et un ou plusieurs résultats. Les variables utilisées dans la règle doivent faire partie du jeu de données d'événements évalué par le détecteur. De plus, chaque détecteur doit être associé à au moins une règle.

Outcome

Il s'agit du résultat, ou du résultat, d'une prédiction de fraude. Chaque règle utilisée dans une prédiction de fraude doit spécifier un ou plusieurs résultats.

Prédiction des fraudes

La prédiction des fraudes est une évaluation de la fraude pour un événement unique ou un ensemble d'événements. Amazon Fraud Detector génère des prédictions de fraude pour un seul événement en ligne en temps réel en fournissant de manière synchrone un score de modèle et un résultat basés sur les règles. Amazon Fraud Detector génère des prédictions de fraude pour une série d'événements hors ligne. Vous pouvez utiliser les prévisions pour effectuer une analyse hors ligne proof-of-concept ou pour évaluer rétrospectivement le risque de fraude sur une base horaire, quotidienne ou hebdomadaire.

Explication de la prédiction des fraudes

Les explications relatives aux prévisions de fraude fournissent un aperçu de l'impact de chaque variable sur le score de prédiction de fraude de votre modèle. Il fournit des informations sur la façon dont chaque variable influence les scores de risque en termes d'ampleur (allant de 0 à 5, 5 étant le plus élevé) et de direction (augmentation ou baisse du score).

Comment fonctionne Amazon Fraud Detector

Amazon Fraud Detector développe un modèle d'apprentissage automatique personnalisé pour détecter les activités en ligne potentiellement frauduleuses au sein de votre entreprise. Pour commencer, vous accordez à nous fournir votre cas d'utilisation pour l'entreprise. En fonction de votre cas d'utilisation professionnelle, Amazon Fraud Detector recommande le type de modèle qu'il utilisera pour créer un modèle de détection des fraudes adapté à vos besoins. En outre, il fournit également

des informations sur les éléments de données que vous devez fournir dans le cadre des données historiques de votre entreprise. Amazon Fraud Detector utilise le jeu de données historique pour créer et entraîner automatiquement un modèle personnalisé pour vous.

Le processus de formation automatique des modèles implique le choix d'un algorithme d'apprentissage automatique qui détecte les fraudes pour votre cas d'utilisation commercial spécifique, la validation des données que vous avez fournies et l'exécution de manipulations de données pour améliorer les performances du modèle. Après avoir entraîné le modèle, Amazon Fraud Detector génère les scores du modèle et d'autres indicateurs de performance du modèle. Vous pouvez utiliser le score et les indicateurs de performance pour évaluer les performances du modèle. Si nécessaire, vous pouvez ajouter ou supprimer des éléments de données dans le jeu de données que vous avez fourni pour l'entraînement et réentraîner le modèle afin d'améliorer le score du modèle.

Une fois le modèle créé, entraîné et activé, vous devez configurer une logique de décision, également appelée règles, qui indique au modèle comment interpréter les données générées par votre entreprise et attribuer des résultats indiquant comment gérer l'interprétation de chaque activité. Les résultats peuvent représenter des actions telles que l'approbation ou la révision de l'activité, ou ils peuvent représenter les niveaux de risque de l'activité tels que le risque élevé, le risque moyen et le risque faible.

Un détecteur est un conteneur qui contient votre modèle et les règles associées. Vous devrez créer, tester et déployer le détecteur dans votre environnement de production.

Le détecteur déployé dans votre environnement de production fournit la capacité de détection des fraudes à vos applications professionnelles. Pour évaluer la fraude, le modèle compare toutes les données entrantes provenant de votre activité commerciale avec les données historiques de votre entreprise et utilise ses algorithmes d'apprentissage automatique sophistiqués avec les règles que vous avez créées pour analyser les résultats et attribuer des résultats. Avec Amazon Fraud Detector, vous pouvez soit évaluer les données d'une seule activité commerciale en temps réel, soit évaluer les données de plusieurs activités commerciales hors ligne.

Supposons que vous ayez une entreprise dont l'une des activités est le transfert de fonds en ligne. Vous souhaitez utiliser Amazon Fraud Detector pour détecter les demandes frauduleuses de transfert de fonds en temps réel. Pour commencer, vous devez d'abord fournir à Amazon Fraud Detector les données relatives aux demandes de transfert de fonds passées. Amazon Fraud Detector utilise ces données pour créer et développer un modèle personnalisé afin de détecter les demandes frauduleuses de transferts de fonds. Ensuite, vous créez un détecteur en ajoutant le modèle et en

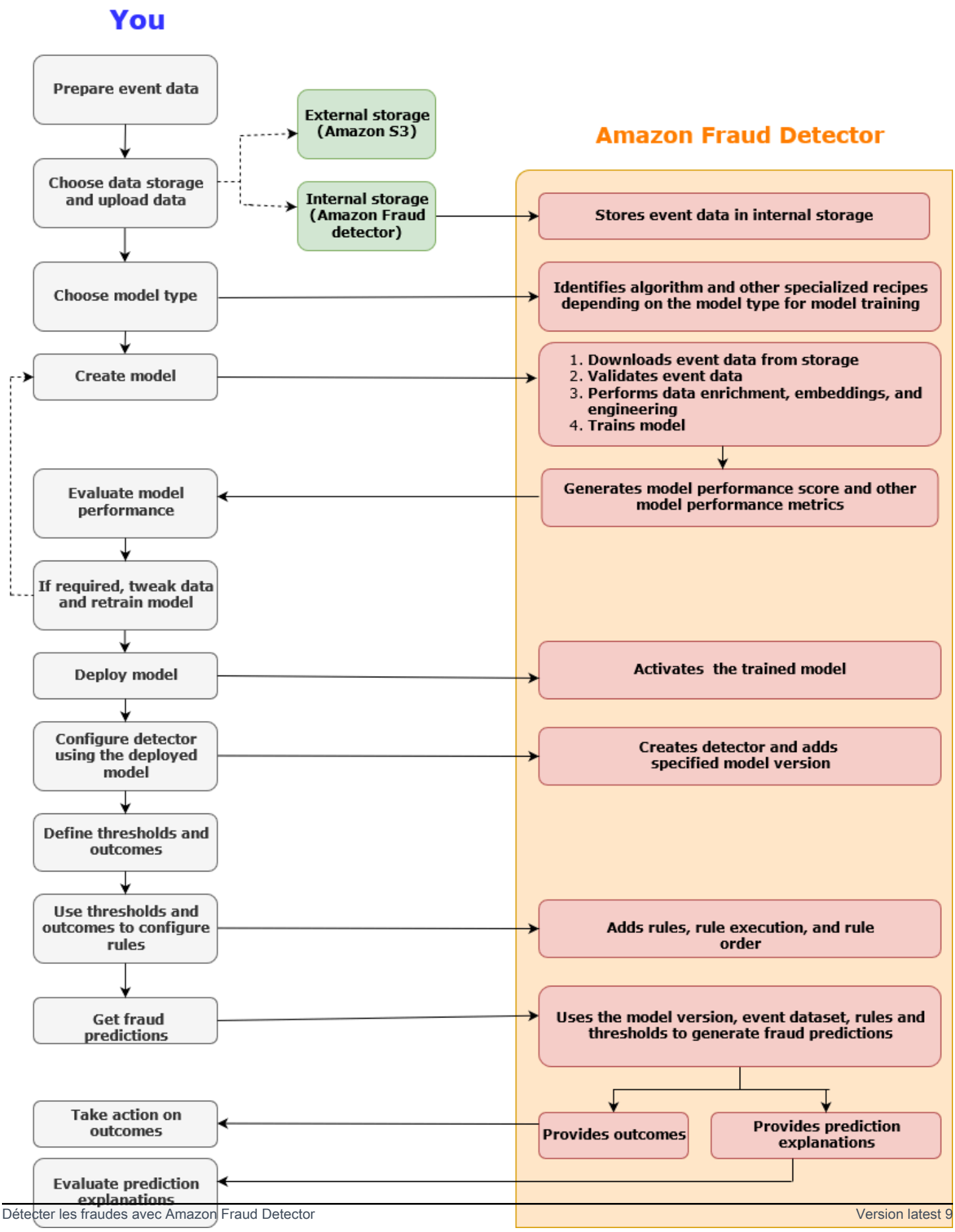
configurant des règles pour que votre modèle interprète les données. Un exemple de règle pour les activités de transfert de fonds en ligne peut être, si la demande de transfert de fonds provient dexyz@example.comadresse e-mail, envoyez la demande de révision. Dans l'environnement de production de votre entreprise, lorsqu'une demande de transfert de fonds arrive, le modèle analyse les données fournies avec la demande et utilise la règle pour attribuer le résultat. Vous pouvez ensuite agir sur la demande en fonction du résultat attribué.

Amazon Fraud Detector utilise des composants tels que l'ensemble de données de formation, le modèle, le détecteur, les règles et les résultats pour fournir à votre entreprise une logique d'évaluation des fraudes.

Pour plus d'informations sur le flux de travail que vous utiliserez pour détecter les fraudes à l'aide d'Amazon Fraud Detector, consultezDétecter les fraudes avec Amazon Fraud Detector

Détecter les fraudes avec Amazon Fraud Detector

Cette section décrit un flux de travail typique pour détecter les fraudes avec Amazon Fraud Detector. Il résume également la manière dont vous pouvez accomplir ces tâches. Le schéma suivant fournit une vue d'ensemble du flux de travail de détection des fraudes avec 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

La détection des fraudes est un processus continu. Après avoir déployé votre modèle, assurez-vous d'évaluer ses scores de performance et ses indicateurs en fonction des explications des prédictions. Ce faisant, vous pouvez identifier les principaux indicateurs de risque, identifier les causes profondes à l'origine des faux positifs, analyser les modèles de fraude dans votre ensemble de données et détecter les biais, le cas échéant. Pour augmenter la précision des prédictions, vous pouvez modifier votre jeu de données pour inclure des données nouvelles ou révisées. Vous pouvez ensuite réentraîner votre modèle avec le jeu de données mis à jour. Au fur et à mesure que de nouvelles données sont disponibles, vous continuez à réentraîner votre modèle pour en augmenter la précision.

Accès à Amazon Fraud Detector

Amazon Fraud Detector est disponible en plusieurs versions Régions AWS et est accessible via AWS des interfaces.

Disponibilité

Amazon Fraud Detector est disponible dans l'est des États-Unis (Virginie du Nord), dans l'est des États-Unis (Ohio), dans l'ouest des États-Unis (Oregon), en Europe (Irlande), en Asie-Pacifique (Singapour) et en Asie-Pacifique (Sydney)Régions AWS.

Interfaces

Vous pouvez créer, former, déployer, tester, exécuter et gérer des modèles et des détecteurs de fraude à l'aide de l'une des interfaces suivantes :

AWS Management Console- Amazon Fraud Detector fournit une interface utilisateur Web, la console Amazon Fraud Detector. Si vous vous êtes inscrit à unCompte AWS, vous pouvez accéder à la console Amazon Fraud Detector. Pour plus d'informations, consultez Configurer Amazon Fraud Detector.

AWS Command Line Interface(AWS CLI) - Fournit une interface que vous pouvez utiliser pour interagir avec un large éventail de personnesServices AWS, y compris Amazon Fraud Detector, à l'aide de commandes dans votre shell de ligne de commande. AWS CLIles commandes d'Amazon Fraud Detector implémentent des fonctionnalités équivalentes à celles fournies par la console Amazon Fraud Detector.

AWSSDK : fournit des API spécifiques au langage et gère de nombreux détails de connexion, tels que le calcul des signatures, le traitement des nouvelles tentatives de demande et le traitement des

erreurs. Pour plus d'informations, rendez-vous sur la AWS page Outils pour créer, faites défiler la page vers le bas jusqu'à la section SDK et choisissez le signe plus (+) pour développer la section.

AWS CloudFormation- Fournit des modèles que vous pouvez utiliser pour définir les ressources et les propriétés de votre Amazon Fraud Detector. Pour plus d'informations, consultez la référence du type de ressource Amazon Fraud Detector dans le guide de AWS CloudFormation l'utilisateur.

Tarification

Avec Amazon Fraud Detector, vous ne payez que pour ce que vous utilisez. Il n'y a pas de tarif minimum ni aucun engagement initial. Vous êtes facturé en fonction des heures de calcul utilisées pour entraîner et héberger vos modèles, de la quantité de stockage que vous utilisez et du nombre de prédictions de fraude que vous effectuez. Pour plus d'informations, consultez les tarifs d'Amazon Fraud Detector.

Configuration d'Amazon Fraud Detector

Pour utiliser Amazon Fraud Detector, vous devez d'abord disposer d'un compte Amazon Web Services (AWS), puis configurer des autorisations vous donnant Compte AWS accès à toutes les interfaces. Plus tard, lorsque vous commencerez à créer vos ressources Amazon Fraud Detector, vous devrez accorder des autorisations permettant à Amazon Fraud Detector d'accéder à votre compte, d'effectuer des tâches en votre nom et d'accéder aux ressources que vous possédez.

Effectuez les tâches suivantes dans cette section pour configurer l'utilisation d'Amazon Fraud Detector :

- Inscrivez-vous pour AWS.
- Configurez des autorisations qui vous permettent Compte AWS d'accéder aux interfaces Amazon Fraud Detector.
- Configurez les interfaces que vous souhaitez utiliser pour accéder à Amazon Fraud Detector.

Une fois ces étapes terminées, consultez Démarrez avec Amazon Fraud Detector pour continuer à démarrer avec Amazon Fraud Detector.

Inscrivez-vous pour AWS

Lorsque vous vous inscrivez à Amazon Web Services (AWS), vous êtes automatiquement Compte AWS inscrit à tous les services AWS, y compris Amazon Fraud Detector. Seuls les services que vous utilisez vous sont facturés. Si vous en avez déjà un Compte AWS, passez à la tâche suivante.

Inscrivez-vous pour un Compte AWS

Si vous n'en avez pas Compte AWS, procédez comme suit pour en créer un.

Pour vous inscrire à un Compte AWS

1. Ouvrez https://portal.aws.amazon.com/billing/signup.
2. Suivez les instructions en ligne.

   Dans le cadre de la procédure d'inscription, vous recevrez un appel téléphonique et vous saisirez un code de vérification en utilisant le clavier numérique du téléphone.

Lorsque vous vous inscrivez à un Compte AWS, un Utilisateur racine d'un compte AWSest créé. Par défaut, seul l'utilisateur racine a accès à l'ensemble des Services AWS et des ressources de ce compte. Pour des raisons de sécurité, attribuez un accès administratif à un utilisateur et utilisez uniquement l'utilisateur root pour effectuer les tâches nécessitant un accès utilisateur root.

AWS vous envoie un e-mail de confirmation une fois le processus d'inscription terminé. Vous pouvez afficher l'activité en cours de votre compte et gérer votre compte à tout moment en accédant à https://aws.amazon.com/ et en choisissant Mon compte.

Création d'un utilisateur doté d'un accès administratif

Après vous être inscrit à un Compte AWS, sécurisez Utilisateur racine d'un compte AWS AWS IAM Identity Center, activez et créez un utilisateur administratif afin de ne pas utiliser l'utilisateur root pour les tâches quotidiennes.

Sécurisez votre Utilisateur racine d'un compte AWS

1. Connectez-vous en AWS Management Consoletant que propriétaire du compte en choisissant Utilisateur root et en saisissant votre adresse Compte AWS e-mail. Sur la page suivante, saisissez votre mot de passe.

   Pour obtenir de l'aide pour vous connecter en utilisant l'utilisateur racine, consultez Connexion en tant qu'utilisateur racine dans le Guide de l'utilisateur Connexion à AWS .
2. Activez l'authentification multifactorielle (MFA) pour votre utilisateur racine.

   Pour obtenir des instructions, voir Activer un périphérique MFA virtuel pour votre utilisateur Compte AWS root (console) dans le guide de l'utilisateur IAM.

Création d'un utilisateur doté d'un accès administratif

1. Activez IAM Identity Center.

   Pour obtenir des instructions, consultez Activation d' AWS IAM Identity Center dans le Guide de l'utilisateur AWS IAM Identity Center .
2. Dans IAM Identity Center, accordez un accès administratif à un utilisateur.

Pour un didacticiel sur l'utilisation du Répertoire IAM Identity Center comme source d'identité, voir Configurer l'accès utilisateur par défaut Répertoire IAM Identity Center dans le Guide de AWS IAM Identity Center l'utilisateur.

Connectez-vous en tant qu'utilisateur disposant d'un accès administratif

- Pour vous connecter avec votre utilisateur IAM Identity Center, utilisez l'URL de connexion qui a été envoyée à votre adresse e-mail lorsque vous avez créé l'utilisateur IAM Identity Center.

  Pour obtenir de l'aide pour vous connecter en utilisant un utilisateur d'IAM Identity Center, consultez la section Connexion au portail AWS d'accès dans le guide de l'Connexion à AWS utilisateur.

Attribuer l'accès à des utilisateurs supplémentaires

1. Dans IAM Identity Center, créez un ensemble d'autorisations conforme aux meilleures pratiques en matière d'application des autorisations du moindre privilège.

   Pour obtenir des instructions, voir Création d'un ensemble d'autorisations dans le guide de AWS IAM Identity Center l'utilisateur.
2. Affectez des utilisateurs à un groupe, puis attribuez un accès d'authentification unique au groupe.

   Pour obtenir des instructions, consultez la section Ajouter des groupes dans le guide de AWS IAM Identity Center l'utilisateur.

Configurez les autorisations pour accéder aux interfaces Amazon Fraud Detector

Pour utiliser Amazon Fraud Detector, configurez les autorisations d'accès à la console Amazon Fraud Detector et aux opérations de l'API.

Conformément aux meilleures pratiques de sécurité, créez un utilisateur AWS Identity and Access Management (IAM) dont l'accès est limité aux opérations d'Amazon Fraud Detector et doté des autorisations requises. Vous pouvez ajouter d'autres autorisations selon vos besoins.

Les politiques suivantes fournissent l'autorisation requise pour utiliser Amazon Fraud Detector :

- `AmazonFraudDetectorFullAccessPolicy`

  Vous permet d'effectuer les actions suivantes :

  - Accédez à toutes les ressources d'Amazon Fraud Detector
  - Répertorier et décrire tous les points de terminaison du modèle dans SageMaker
  - Répertorier tous les rôles IAM du compte
  - Répertorier tous les compartiments Amazon S3
  - Autoriser le rôle IAM Pass à transmettre un rôle à Amazon Fraud Detector
- `AmazonS3FullAccess`

  Permet un accès complet à Amazon Simple Storage Service. Cela est nécessaire si vous devez télécharger des ensembles de données d'entraînement sur Amazon S3.

Ce qui suit décrit comment créer un utilisateur IAM et attribuer les autorisations nécessaires.

Pour créer un utilisateur et attribuer les autorisations requises

1. Connectez-vous à la console IAM AWS Management Console et ouvrez-la à l'adresse https://console.aws.amazon.com/iam/.
2. Dans le panneau de navigation, choisissez Utilisateurs, puis Add user (Ajouter un utilisateur).
3. Dans Nom d'utilisateur, saisissez **`AmazonFraudDetectorUser`**.
4. Cochez la case Accès à la console de AWS gestion, puis configurez le mot de passe utilisateur.
5. (Facultatif) Par défaut, le nouvel utilisateur AWS doit créer un nouveau mot de passe lors de sa première connexion. Désélectionnez la case en regard de User must create a new password at next sign in (L'utilisateur doit créer un nouveau mot de passe à sa prochaine connexion) pour autoriser le nouvel utilisateur à réinitialiser son mot de passe une fois qu'il s'est connecté.
6. Sélectionnez Next: Permissions (Étape suivante : autorisations).
7. Choisissez Créer un groupe.
8. Dans le champ Nom du groupe, entrez**`AmazonFraudDetectorGroup`**.
9. Dans la liste des politiques, cochez la case pour AmazonFraudDetectorFullAccessPolicyet AmazonS3 FullAccess. Choisissez Créer un groupe.
10. Dans la liste des groupes, cochez la case du nouveau groupe. Choisissez Actualiser si le groupe ne figure pas dans la liste.
11. Choisissez Next: Tags (Suivant : Balises).

12. (Facultatif) Ajoutez des métadonnées à l'utilisateur en associant les balises sous forme de paires clé-valeur. Pour obtenir des instructions sur l'utilisation des balises dans IAM, consultez la section Marquage des utilisateurs et des rôles IAM.
13. Choisissez Next : Revoir pour voir les détails de l'utilisateur et le résumé des autorisations du nouvel utilisateur. Lorsque vous êtes prêt à continuer, choisissez Create user.

Configurez des interfaces pour accéder à Amazon Fraud Detector avec

Vous pouvez accéder à Amazon Fraud Detector à l'aide de la console Amazon Fraud Detector AWS CLI, ou AWS SDK. Avant de pouvoir les utiliser, configurez d'abord le AWS SDK AWS CLI et.

Accédez à la console Amazon Fraud Detector

Vous pouvez accéder à la console Amazon Fraud Detector et à d'autres AWS services via le AWS Management Console. Votre Compte AWS, vous donne accès au AWS Management Console.

Pour accéder à la console Amazon Fraud Detector,

1. Accédez https://console.aws.amazon.com/ à votre Compte AWS.
2. Accédez à Amazon Fraud Detector.

Avec la console Amazon Fraud Detector, vous pouvez créer et gérer vos modèles et vos ressources de détection des fraudes, telles que les détecteurs, les variables, les événements, les entités, les étiquettes et les résultats. Vous pouvez générer des prédictions et évaluer les performances et les prévisions de votre modèle.

Configurez AWS CLI

Vous pouvez utiliser AWS Command Line Interface (AWS CLI) pour interagir avec Amazon Fraud Detector en exécutant des commandes dans votre interface de ligne de commande. Avec une configuration minimale, vous pouvez utiliser le AWS CLI pour exécuter des commandes offrant des fonctionnalités similaires à celles fournies par la console Amazon Fraud Detector depuis l'invite de commande de votre terminal.

Pour configurer le AWS CLI

Téléchargez et configurez l'interface AWS CLI. Pour obtenir des instructions, consultez les rubriques suivantes du guide de AWS Command Line Interface l'utilisateur :

- Configuration à l'aide de l'interface de ligne de AWS commande
- Configuration de l'interface AWS de ligne de commande

Pour plus d'informations sur les commandes Amazon Fraud Detector, consultez la section Commandes disponibles

Configurer le AWS SDK

Vous pouvez utiliser les AWS SDK pour écrire du code permettant de créer et de gérer vos ressources de détection des fraudes et d'obtenir des prédictions en matière de fraude. Les AWS SDK prennent en charge Amazon Fraud Detector in JavaScriptet Python (Boto3).

Pour configurer AWS SDK for Python (Boto3)

Vous pouvez l'utiliser AWS SDK for Python (Boto3) pour créer, configurer et gérer AWS des services. Pour obtenir des instructions sur l'installation de Boto, reportez-vous à la section AWS SDK for Python (Boto3). Assurez-vous que vous utilisez la version 1.14.29 ou supérieure du SDK Boto3.

Après l'installation AWS SDK for Python (Boto3), exécutez l'exemple Python suivant pour vérifier que votre environnement est correctement configuré. Si elle est correctement configurée, la réponse contient une liste de détecteurs. Si aucun détecteur n'a été créé, la liste est vide.

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

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

Pour configurer des AWS kits de développement logiciel (SDK) pour Java

Pour obtenir des instructions sur l'installation et le chargement du AWS SDK for JavaScript, consultez la section Configuration du SDK pour JavaScript.

Démarrez avec Amazon Fraud Detector

Avant de commencer, assurez-vous d'avoir luDétecter les fraudes avec Amazon Fraud Detector et terminé les étapes décritesConfiguration d'Amazon Fraud Detector.

Utilisez les didacticiels pratiques figurant dans cette section pour découvrir comment utiliser Amazon Fraud Detector pour créer, entraîner et déployer un modèle de détection des fraudes. Dans ce didacticiel, vous incarnez un analyste des fraudes utilisant un modèle d'apprentissage automatique pour prédire si l'enregistrement d'un nouveau compte est frauduleux. Le modèle doit être entraîné à l'aide des données provenant des enregistrements de comptes. Amazon Fraud Detector fournit un exemple de jeu de données d'enregistrement de compte pour ce didacticiel. L'exemple de jeu de données doit être chargé avant de commencer le didacticiel.

Vous pouvez commencer avec Amazon Fraud Detector à l'aide de l'une des interfaces suivantes. Avant de commencer avec le didacticiel, assurez-vous de suivre les instructions pourObtenir et télécharger un exemple de jeu de données

- Tutoriel : Commencez à utiliser la console Amazon Fraud Detector
- Didacticiel : Premiers pas avecAWS SDK for Python (Boto3)

Obtenir et télécharger un exemple de jeu de données

L'exemple de jeu de données que vous utilisez dans ce didacticiel fournit des informations détaillées sur les enregistrements de comptes en ligne. L'ensemble de données se trouve dans un fichier texte qui utilise des valeurs séparées par des virgules (CSV) au format UTF-8. La première ligne du fichier de données CSV contient les en-têtes. La ligne d'en-tête est suivie de plusieurs lignes de données. Chacune de ces lignes est constituée d'éléments de données provenant de l'enregistrement d'un seul compte. Les données sont étiquetées à titre indicatif. Une colonne de l'ensemble de données indique si l'enregistrement du compte est frauduleux.

Pour obtenir et télécharger un exemple de jeu de données

1. Accédez à la section Échantillons.

   Deux fichiers de données contiennent des données d'enregistrement de comptes en ligne : registration_data_20K_minimum.csv et registration_data_20K_full.csv. Le fichier `neregistration_data_20K_minimum` contient que deux variables : ip_address et email_address. Le fichier`registration_data_20K_full` contient d'autres variables.

Ces variables concernent chaque événement et incluent billing_address, phone_number et user_agent. Les deux fichiers de données contiennent également deux champs obligatoires :

- EVENT_TIMESTAMP — Définit quand l'événement est survenu
- EVENT_LABEL — Classifie l'événement comme frauduleux ou légitime

Vous pouvez utiliser l'un des deux fichiers pour ce didacticiel. Téléchargez le fichier de données que vous souhaitez utiliser.

2. Créez un compartimentAmazon Simple Storage Service (Amazon S3).

   Au cours de cette étape, vous allez créer un stockage externe pour stocker le jeu de données. Ce stockage externe est le compartiment Amazon S3. Pour plus d'informations sur Amazon S3, consultez Qu'est-ce qu'Amazon S3 ?

   a. Connectez-vous à la AWS Management Console et ouvrez la console Amazon S3 à l'adresse https://console.aws.amazon.com/s3/.

   b. Dans Buckets, choisissez Create bucket.

   c. Pour Nom du compartiment, saisissez un nom de compartiment. Assurez-vous de respecter les règles de dénomination des compartiments de la console et de fournir un nom unique au monde entier. Nous vous recommandons d'utiliser un nom qui décrit l'objectif du compartiment.

   d. Pour Région AWS, choisissez l'Région AWSendroit où vous souhaitez créer votre compartiment. La région que vous choisissez doit prendre en charge Amazon Fraud Detector. Pour réduire la latence, choisissez celuiRégion AWS qui est le plus proche de votre position géographique. Pour obtenir la liste des régions compatibles avec Amazon Fraud Detector, consultez le tableau des régions du Global Infrastructure Guide.

   e. Pour ce didacticiel, conservez les paramètres par défaut pour la propriété des objets, les paramètres de compartiment pour bloquer l'accès public, la gestion des versions des compartiments et les balises.

   f. Pour le chiffrement par défaut, choisissez Désactiver pour ce didacticiel.

   g. Vérifiez la configuration de votre compartiment, puis choisissez Créer un compartiment.

3. Chargez l'exemple de fichier de données dans le compartiment Amazon S3.

   Maintenant que vous disposez d'un compartiment, chargez l'un des exemples de fichiers que vous avez précédemment téléchargés dans le compartiment Amazon S3 que vous venez de créer.

a. Dans les compartiments, le nom de votre compartiment est répertorié. Choisissez votre compartiment.

b. Sélectionnez Charger.

c. Dans Fichiers et dossiers, choisissez Ajouter des fichiers.

d. Choisissez l'un des exemples de fichiers de données que vous avez téléchargés sur votre ordinateur, puis choisissez Ouvrir.

e. Conservez les paramètres par défaut pour Destination, Autorisations et Propriétés.

f. Passez en revue les configurations, puis choisissez Charger.

g. L'exemple de fichier de données est chargé dans le compartiment Amazon S3. Notez la position du compartiment. Dans les Objets, choisissez l'exemple de fichier de données que vous venez de télécharger.

h. Dans la vue d'ensemble des objets, copiez l'emplacement sous l'URI S3. Il s'agit de l'emplacement Amazon S3 de votre exemple de fichier de données. Vous l'utiliserez ultérieurement. Vous pouvez également copier l'Amazon Resource Name (ARN) de votre compartiment S3 et l'enregistrer.

Tutoriel : Commencez à utiliser la console Amazon Fraud Detector

Ce didacticiel se compose de deux parties. La première partie décrit comment créer, entraîner et déployer un modèle de détection des fraudes. La deuxième partie explique comment utiliser le modèle pour générer des prévisions de fraude en temps réel. Le modèle est entraîné à l'aide de l'exemple de fichier de données que vous chargez dans un compartiment S3. Au terme de ce didacticiel, vous effectuez les actions suivantes :

- Création et formation d'un modèle Amazon Fraud Detector
- Générez des prévisions de fraude en temps réel

> **Important**
>
> Avant de poursuivre, assurez-vous d'avoir suivi les instructions pourObtenir et télécharger un exemple de jeu de données

Partie A : créer, entraîner et déployer un modèle Amazon Fraud Detector

Dans la partie A, vous définissez votre cas d'utilisation commerciale, définissez votre événement, créez un modèle, formez le modèle, évaluez les performances du modèle et déployez le modèle.

Étape 1 : Choix du cas d'utilisation de votre entreprise

- Au cours de cette étape, vous utilisez l'explorateur de modèles de données pour faire correspondre votre cas d'utilisation commerciale aux types de modèles de détection des fraudes pris en charge par Amazon Fraud Detector. L'explorateur de modèles de données est un outil intégré à la console Amazon Fraud Detector qui recommande un type de modèle à utiliser pour créer et former un modèle de détection des fraudes adapté à votre cas d'utilisation professionnelle. L'explorateur de modèles de données fournit également des informations sur les éléments de données obligatoires, recommandés et facultatifs que vous devrez inclure dans votre ensemble de données. L'ensemble de données sera utilisé pour créer et entraîner votre modèle de détection des fraudes.

  Dans le cadre de ce didacticiel, votre cas d'utilisation professionnelle concerne l'enregistrement de nouveaux comptes. Une fois que vous avez défini votre cas d'utilisation commerciale, l'explorateur de modèles de données recommande un type de modèle pour créer un modèle de détection des fraudes et vous fournit également une liste des éléments de données dont vous aurez besoin pour créer votre ensemble de données. Comme vous avez déjà chargé un exemple de jeu de données contenant des données provenant de nouveaux enregistrements de comptes, il n'est pas nécessaire de créer un nouvel ensemble de données.

  a. Ouvrez la consoleAWS de gestion et connectez-vous à votre compte. Accédez à Amazon Fraud Detector.

  b. Dans le panneau de navigation de gauche, choisissez Explorateur de modèles de données.

  c. Sur la page Explorateur de modèles de données, sous Cas d'utilisation professionnelle, sélectionnez Fraude liée à la création de nouveaux comptes.

  d. Amazon Fraud Detector affiche le type de modèle recommandé à utiliser pour créer un modèle de détection des fraudes pour le cas d'utilisation commercial sélectionné. Le type de modèle définit les algorithmes, les enrichissements et les transformations qu'Amazon Fraud Detector utilisera pour former votre modèle de détection des fraudes.

     Notez le type de modèle recommandé. Vous en aurez besoin ultérieurement lorsque vous créerez votre modèle.

e. Le volet Informations sur les modèles de données fournit un aperçu des éléments de données obligatoires et recommandés nécessaires à la création et à la formation d'un modèle de détection des fraudes.

   Examinez l'exemple de jeu de données que vous avez téléchargé et assurez-vous qu'il contient tous les éléments de données obligatoires et certains éléments recommandés répertoriés dans le tableau.

   Plus tard, lorsque vous créerez un modèle pour votre cas d'utilisation métier spécifique, vous utiliserez les informations fournies pour créer votre ensemble de données.

Étape 2 : créer le type d'événement

- Au cours de cette étape, vous définissez l'activité commerciale (événement) à évaluer pour détecter toute fraude. La définition de l'événement implique la définition des variables qui se trouvent dans votre ensemble de données, de l'entité exécutant l'événement et des étiquettes qui classent l'événement. Pour ce didacticiel, vous allez définir l'événement d'enregistrement du compte.

  a. Ouvrez la consoleAWS de gestion et connectez-vous à votre compte. Accédez à Amazon Fraud Detector.

  b. Dans le panneau de navigation de gauche, choisissez Événements.

  c. Sur la page Type d'événements, choisissez Créer.

  d. Sous Détails du type d'événement, entrez le`sample_registration` nom du type d'événement et, éventuellement, une description de l'événement.

  e. Pour Entité, choisissez Créer une entité.

  f. Sur la page Créer une entité, entrez le`sample_customer` nom du type d'entité. Si vous le souhaitez, saisissez une description du type d'entité.

  g. Choisissez Create entity (Créer une entité).

  h. Sous Variables d'événement, pour Choisir comment définir les variables de cet événement, choisissez Sélectionner les variables d'un jeu de données d'entraînement.

  i. Pour le rôle IAM, choisissez Créer un rôle IAM.

  j. Sur la page Créer un rôle IAM, entrez le nom du compartiment S3 dans lequel vous avez chargé vos exemples de données et choisissez Créer un rôle.

k. Dans Emplacement des données, entrez le chemin d'accès à vos exemples de données. Il s'agit du`S3 URI` chemin que vous avez enregistré après avoir chargé les exemples de données. Le chemin est similaire à celui-ci :`S3://`*`your-bucket-name`*`/`*`example dataset filename`*`.csv`.

l. Sélectionnez Charger.

Amazon Fraud Detector extrait les en-têtes de votre fichier de données d'exemple et les associe à un type de variable. Le mappage s'affiche dans la console.

m. Sous Étiquettes - facultatif, pour Étiquettes, choisissez Créer de nouvelles étiquettes.

n. Dans la page Créer une étiquette, entrez le`fraud` nom. Cette étiquette correspond à la valeur qui représente l'enregistrement frauduleux du compte dans l'exemple de données.

o. Choisissez Créer une étiquette.

p. Créez une deuxième étiquette, puis`legit` saisissez-la comme nom. Cette étiquette correspond à la valeur qui représente l'enregistrement légitime du compte dans l'exemple de données.

q. Choisissez Créer un type d'événement.

Étape 3 : créer le modèle

1. Sur la page Modèles, choisissez Ajouter un modèle, puis choisissez Créer un modèle.
2. Pour l'étape 1 — Définition des détails du modèle, entrez le`sample_fraud_detection_model` nom du modèle. Si vous le souhaitez, ajoutez une description du modèle.
3. Dans Type de modèle, choisissez le modèle Online Fraud Insights.
4. Pour Type d'événement, choisissez sample_registration. Il s'agit du type d'événement que vous avez créé lors de l'étape 1.
5. Dans Données historiques sur les événements,

   a. Dans Source de données d'événements, sélectionnez Données d'événements stockées dans S3.

   b. Pour le rôle IAM, sélectionnez le rôle que vous avez créé lors de l'étape 1.

   c. Dans Emplacement des données d'entraînement, entrez le chemin de l'URI S3 vers votre exemple de fichier de données.

6. Choisissez Suivant.

Étape 4 : Modèle de train

1. Dans les entrées du modèle, laissez toutes les cases cochées. Par défaut, Amazon Fraud Detector utilise toutes les variables de votre ensemble de données d'événements historiques comme entrées de modèle.
2. Dans Classification des étiquettes, pour les étiquettes de fraude, choisissez Fraude, car cette étiquette correspond à la valeur qui représente les événements frauduleux dans l'exemple de jeu de données. Pour les étiquettes légitimes, choisissez Legit car cette étiquette correspond à la valeur qui représente les événements légitimes dans l'exemple de jeu de données.
3. Pour le traitement des événements sans étiquette, conservez la sélection par défaut Ignorer les événements non étiquetés pour cet exemple de jeu de données.
4. Choisissez Suivant.
5. Après avoir vérifié, choisissez Create and train model. Amazon Fraud Detector crée un modèle et commence à entraîner une nouvelle version du modèle.

   Dans les versions du modèle, la colonne Status indique l'état de la formation du modèle. L'entraînement du modèle utilisant l'exemple de jeu de données prend environ 45 minutes. Le statut passe à Prêt à déployer une fois la formation du modèle terminée.

Étape 5 : Examiner les performances du modèle

Une étape importante de l'utilisation d'Amazon Fraud Detector consiste à évaluer la précision de votre modèle à l'aide des scores et des indicateurs de performance du modèle. Une fois la formation du modèle terminée, Amazon Fraud Detector valide les performances du modèle en utilisant les 15 % de données qui n'ont pas été utilisées pour entraîner le modèle et génère un score de performance du modèle et d'autres mesures de performance.

1. Pour consulter les performances du modèle,

   a. Dans le panneau de navigation de gauche de la console Amazon Fraud Detector, choisissez Models.

   b. Sur la page Modèles, choisissez le modèle que vous venez d'entraîner (sample_fraud_detection_model), puis choisissez 1.0. Il s'agit de la version créée par Amazon Fraud Detector à partir de votre modèle.
2. Examinez le score global des performances du modèle et tous les autres indicateurs générés par Amazon Fraud Detector pour ce modèle.

Pour en savoir plus sur le score de performance du modèle et les mesures de performance figurant sur cette page, consultezScores du modèle etIndicateurs de performance du modèle.

Vous pouvez vous attendre à ce que tous vos modèles Amazon Fraud Detector expérimentés disposent de mesures de performance réelles en matière de détection des fraudes similaires à celles que vous pouvez voir pour le modèle dans ce didacticiel.

Étape 6 : Déploiement du modèle

Une fois que vous avez examiné les indicateurs de performance de votre modèle entraîné et que vous êtes prêt à l'utiliser pour générer des prévisions de fraude, vous pouvez déployer le modèle.

1. Dans le panneau de navigation de gauche de la console Amazon Fraud Detector, choisissez Models.
2. Sur la page Modèles, choisissez sample_fraud_detection_model, puis choisissez la version de modèle spécifique que vous souhaitez déployer. Pour ce didacticiel, choisissez 1.0.
3. Sur la page Version du modèle, choisissez Actions, puis choisissez Déployer la version du modèle.
4. Dans les versions du modèle, le statut indique l'état du déploiement. Le statut passe à Actif une fois le déploiement terminé. Cela indique que la version du modèle est activée et disponible pour générer des prévisions de fraude. Poursuivez la procédurePartie B : Générer des prévisions de fraude pour suivre les étapes permettant de générer des prévisions de fraude.

Partie B : Générer des prévisions de fraude

La prédiction de la fraude est une évaluation de la fraude liée à une activité commerciale (événement). Amazon Fraud Detector utilise des détecteurs pour générer des prévisions de fraude. Un détecteur contient une logique de détection, telle que des modèles et des règles, pour un événement spécifique que vous souhaitez évaluer pour détecter une fraude. La logique de détection utilise des règles pour indiquer à Amazon Fraud Detector comment interpréter les données associées au modèle. Dans ce didacticiel, vous allez évaluer l'événement d'enregistrement du compte à l'aide de l'exemple de jeu de données d'enregistrement de compte que vous avez chargé précédemment.

Dans la partie A, vous avez créé, entraîné et déployé votre modèle. Dans la partie B, vous créez un détecteur pour le type d'`sample_registration`événement, ajoutez le modèle déployé, créez des

règles et un ordre d'exécution des règles, puis créez et activez une version du détecteur que vous utilisez pour générer des prévisions de fraude.

Étape 1 : Créer le détecteur

Pour créer un détecteur

1. Dans le panneau de navigation de gauche de la console Amazon Fraud Detector, choisissez Detectors.
2. Choisissez Créer un détecteur.
3. Sur la page Définir les détails du détecteur, saisissez`sample_detector` le nom du détecteur. Si vous le souhaitez, saisissez une description pour le détecteur, par exemple`my sample fraud detector`.
4. Pour Type d'événement, sélectionnez sample_registration. Il s'agit de l'événement que vous avez créé dans la partie A de ce didacticiel.
5. Choisissez Suivant.

Étape 2 : ajouter le modèle

Si vous avez suivi la partie A de ce didacticiel, vous disposez probablement déjà d'un modèle Amazon Fraud Detector que vous pouvez ajouter à votre détecteur. Si vous n'avez pas encore créé de modèle, passez à la partie A et suivez les étapes pour créer, entraîner et déployer un modèle, puis passez à la partie B.

1. Dans le champ Ajouter un modèle - facultatif, choisissez Ajouter un modèle.
2. Sur la page Ajouter un modèle, pour Sélectionner un modèle, choisissez le nom du modèle Amazon Fraud Detector que vous avez déployé précédemment. Pour Sélectionner la version, choisissez la version du modèle déployé.
3. Choisissez Add model.
4. Choisissez Suivant.

Étape 3 : ajouter des règles

Une règle est une condition qui indique à Amazon Fraud Detector comment interpréter le score de performance du modèle lors de l'évaluation à titre de prédiction de fraude. Pour ce didacticiel, vous allez créer trois règles :`high_fraud_risk`,`medium_fraud_risk`, et`low_fraud_risk`.

1. Sur la page Ajouter des règles, sous Définir une règle, entrez`high_fraud_risk` le nom de la règle et, dans Description, facultatif, entrez**`This rule captures events with a high ML model score`** la description de la règle.
2. Dans Expression, entrez l'expression de règle suivante à l'aide du langage d'expression de règles simplifié d'Amazon Fraud Detector :

   ```
   $sample_fraud_detection_model_insightscore > 900
   ```
3. Dans Résultats, choisissez Créer un nouveau résultat. Un résultat est le résultat d'une prédiction de fraude et est renvoyé si la règle correspond au cours d'une évaluation.
4. Dans Créer un nouveau résultat, entrez le`verify_customer` nom du résultat. Si vous le souhaitez, saisissez une description.
5. Choisissez Enregistrer le résultat.
6. Choisissez Ajouter une règle pour exécuter le vérificateur de validation des règles et enregistrer la règle. Une fois créée, Amazon Fraud Detector met la règle à disposition de votre détecteur.
7. Choisissez Ajouter une autre règle, puis cliquez sur l'onglet Créer une règle.
8. Répétez cette procédure deux fois de plus pour créer vos`low_fraud_risk` règles`medium_fraud_risk` et en utilisant les détails des règles suivants :

   - risque de fraude moyen

     Nom de la règle :`medium_fraud_risk`

     Résultat :`review`

     Expression :

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

     ```
     $sample_fraud_detection_model_insightscore > 700
     ```
   - faible risque de fraude

     Nom de la règle :`low_fraud_risk`

     Résultat :`approve`

     Expression :

     ```
     $sample_fraud_detection_model_insightscore <= 700
     ```

Ces valeurs sont des exemples utilisés dans ce didacticiel. Lorsque vous créez des règles pour votre propre détecteur, utilisez des valeurs adaptées à votre modèle et à votre cas d'utilisation,

9. Après avoir créé les trois règles, choisissez Suivant.

   Pour plus d'informations sur la création et la rédaction de règles, consultezRègles etRéférence du langage des règles.

Étape 4 : Configuration de l'exécution et de l'ordre des règles

Le mode d'exécution des règles incluses dans le détecteur détermine si toutes les règles que vous définissez sont évaluées ou si l'évaluation des règles s'arrête à la première règle correspondante. Et l'ordre des règles détermine l'ordre dans lequel vous souhaitez que la règle soit exécutée.

Le mode d'exécution des règles par défaut est`FIRST_MATCHED`.

Premier apparié

Le mode d'exécution de la première règle correspondante renvoie les résultats de la première règle correspondante en fonction de l'ordre des règles défini. Si vous spécifiez `FIRST_MATCHED`, Amazon Fraud Detector évalue les règles de manière séquentielle, de la première à la dernière, en s'arrêtant à la première règle correspondante. Amazon Fraud Detector fournit ensuite les résultats pour cette règle unique.

L'ordre dans lequel vous exécutez les règles peut avoir une incidence sur le résultat de la prédiction des fraudes qui en résulte. Après avoir créé vos règles, réorganisez-les pour les exécuter dans l'ordre souhaité en procédant comme suit :

Si votre`high_fraud_risk` règle ne figure pas déjà en haut de votre liste de règles, choisissez Ordre, puis 1. Cela passe`high_fraud_risk` à la première position.

Répétez cette procédure pour placer votre`medium_fraud_risk` règle en deuxième position et votre`low_fraud_risk` règle en troisième position.

Tous assortis

Le mode d'exécution de toutes les règles correspondantes renvoie des résultats pour toutes les règles correspondantes, quel que soit l'ordre des règles. Si vous le spécifiez`ALL_MATCHED`, Amazon Fraud Detector évalue toutes les règles et renvoie les résultats pour toutes les règles correspondantes.

SélectionnezFIRST_MATCHED ce didacticiel, puis choisissez Suivant.

Étape 5 : Examen et création de la version du détecteur

Une version de détecteur définit les modèles et les règles spécifiques utilisés pour générer des prévisions de fraude.

1. Sur la page Réviser et créer, passez en revue les détails, les modèles et les règles du détecteur que vous avez configurés. Si vous devez apporter des modifications, choisissez Modifier à côté de la section correspondante.
2. Choisissez Créer un détecteur. Une fois créée, la première version de votre détecteur apparaît dans le tableau des versions du détecteur avecDraft son statut.

   Vous utilisez la version Draft pour tester votre détecteur.

Étape 6 : Test et activation de la version du détecteur

Dans la console Amazon Fraud Detector, vous pouvez tester la logique de votre détecteur à l'aide de données fictives grâce à la fonction Exécuter un test. Pour ce didacticiel, vous pouvez utiliser les données d'enregistrement de compte issues de l'exemple de jeu de données.

1. Faites défiler la page jusqu'à Exécuter le test en bas de la page de détails de la version du détecteur.
2. Pour les métadonnées de l'événement, entrez l'horodatage de la date à laquelle l'événement s'est produit et entrez un identifiant unique pour l'entité qui l'a réalisé. Pour ce didacticiel, sélectionnez une date dans le sélecteur de dates pour l'horodatage et entrez « 1234 » pour l'ID d'entité.
3. Dans le champ Variable d'événement, entrez les valeurs des variables que vous souhaitez tester. Pour ce didacticiel, vous n'avez besoin queip_address desemail_address champs et. En effet, ce sont les entrées qui sont utilisées pour entraîner votre modèle Amazon Fraud Detector. Vous pouvez utiliser les valeurs d'exemple suivantes. Cela suppose que vous avez utilisé les noms de variables suggérés :

   - adresse_IP :205.251.233.178
   - adresse_e-mail :johndoe@exampledomain.com
4. Choisissez Exécuter le test.
5. Amazon Fraud Detector renvoie le résultat de la prédiction des fraudes en fonction du mode d'exécution de la règle. Si le mode d'exécution de la règle estFIRST_MATCHED, le résultat

renvoyé correspond à la première règle correspondante. La première règle est celle qui a la priorité la plus élevée. Cela correspond s'il est évalué comme vrai. Si le mode d'exécution de la règle est`ALL_MATCHED`, le résultat renvoyé correspond à toutes les règles correspondantes. Cela signifie qu'ils sont tous considérés comme vrais. Amazon Fraud Detector renvoie également le score du modèle pour tous les modèles ajoutés à votre détecteur.

Vous pouvez modifier les entrées et exécuter quelques tests pour obtenir des résultats différents. Vous pouvez utiliser les valeurs ip_address et email_address de votre exemple de jeu de données pour les tests et vérifier si les résultats sont conformes aux attentes.

6. Lorsque vous êtes satisfait du fonctionnement du détecteur, faites-en la promotion de`Draft` à`Active`. Le détecteur peut ainsi être utilisé pour détecter les fraudes en temps réel.

   Sur la page de détails de la version de Detector, sélectionnez Actions, Publier, Publier la version. Cela fait passer le statut du détecteur de Brouillon à Actif.

   À ce stade, votre modèle et la logique de détection associée sont prêts à évaluer les activités en ligne pour détecter les fraudes en temps réel à l'aide de l'`GetEventPrediction`API Amazon Fraud Detector. Vous pouvez également évaluer les événements hors ligne à l'aide d'un fichier d'entrée CSV et de l'`CreateBatchPredictionJob`API. Pour plus d'informations sur la prédiction des fraudes, consultezPrédictions de fraude

En complétant ce didacticiel, vous avez effectué les opérations suivantes :

- Chargement d'un exemple de jeu de données d'événements sur Amazon S3.
- Création et formation d'un modèle de détection des fraudes Amazon Fraud Detector à l'aide de l'exemple de jeu de données.
- Vous avez consulté le score de performance du modèle et d'autres indicateurs de performance générés par Amazon Fraud Detector.
- Déploiement du modèle de détection des fraudes.
- Création d'un détecteur et ajout du modèle déployé.
- Ajout de règles, de l'ordre d'exécution des règles et des résultats au détecteur.
- J'ai testé le détecteur en fournissant différentes entrées et en vérifiant si les règles et l'ordre d'exécution des règles fonctionnaient comme prévu.
- J'ai activé le détecteur en le publiant.

Didacticiel : Premiers pas avecAWS SDK for Python (Boto3)

Ce didacticiel explique comment créer et entraîner un modèle Amazon Fraud Detector, puis comment utiliser ce modèle pour générer des prévisions de fraude en temps réel à l'aide duAWS SDK for Python (Boto3). Le modèle est entraîné à l'aide de l'exemple de fichier de données d'enregistrement de compte que vous chargez dans le compartiment Amazon S3.

Au terme de ce didacticiel, vous aurez effectué les actions suivantes :

- Création et formation d'un modèle Amazon Fraud Detector
- Générez des prédictions de fraude en temps réel

Prérequis

Les étapes préalables à ce didacticiel sont les suivantes.

- TerminéConfiguration d'Amazon Fraud Detector.

  Si vous l'avez déjà faitConfigurer le AWS SDK, assurez-vous d'utiliser la version 1.14.29 ou ultérieure du SDK Boto3.
- J'ai suivi les instructions pour classer lesObtenir et télécharger un exemple de jeu de données fichiers requis pour ce didacticiel.

Mise en route

Étape 1 : Configurer et vérifier votre environnement Python

Boto est le kit SDK Amazon Web Services (AWS) pour Python. Vous pouvez l'utiliser pour créer, configurer et gérerServices AWS. Pour de plus amples informations, veuillez consulter Kit AWS SDK for Python (Boto3).

Après l'installationAWS SDK for Python (Boto3), exécutez l'exemple de commande Python suivant pour vérifier que votre environnement est correctement configuré. Si votre environnement est correctement configuré, la réponse contient une liste de détecteurs. Si aucun détecteur n'a été créé, la liste est vide.

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

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

Étape 2 : Création de variables, de types d'entités et d'étiquettes

Au cours de cette étape, vous créez des ressources qui sont utilisées pour définir le modèle, l'événement et les règles.

Créer une variable

Une variable est un élément de données de votre jeu de données que vous souhaitez utiliser pour créer un type d'événement, un modèle et des règles.

Dans l'exemple suivant, l'CreateVariableAPI est utilisée pour créer deux variables. Les variables sont`email_address` et`ip_address`. Attribuez-les aux types de variables correspondants :`EMAIL_ADDRESS` et`IP_ADDRESS`. Ces variables font partie de l'exemple de jeu de données que vous avez chargé. Lorsque vous spécifiez le type de variable, Amazon Fraud Detector interprète la variable lors de l'entraînement du modèle et lors de l'obtention de prévisions. Seules les variables associées à un type de variable peuvent être utilisées pour l'entraînement du modèle.

```
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>'
```

```
)
```

Créer un type d'entité

Une entité représente qui exécute l'événement et un type d'entité classe l'entité. Les exemples de classifications incluent le client, le commerçant ou le compte.

Dans l'exemple suivant, PutEntityTypel'API est utilisée pour créer un type d'`sample_customer`entité.

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

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

Créer une étiquette

Une étiquette classe un événement comme frauduleux ou légitime et est utilisée pour entraîner le modèle de détection des fraudes. Le modèle apprend à classer les événements à l'aide de ces valeurs d'étiquette.

Dans l'exemple suivant, l'API Putlabel est utilisée pour créer deux étiquettes,`fraud` et`legit`.

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

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

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

Étape 3 : Créer un type d'événement

Avec Amazon Fraud Detector, vous créez des modèles qui évaluent les risques et génèrent des prédictions de fraude pour des événements individuels. Un type d'événement définit la structure d'un événement individuel.

Dans l'exemple suivant, l'PutEventTypeAPI est utilisée pour créer un type d'événement`sample_registration`. Vous définissez le type d'événement en spécifiant les variables (`email_address`,`ip_address`), le type d'entité (`sample_customer`) et les étiquettes (`fraud`,`legit`) que vous avez créés à l'étape précédente.

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

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

Étape 4 : Créer, entraîner et déployer un modèle

Amazon Fraud Detector forme les modèles à apprendre à détecter les fraudes pour un type d'événement spécifique. À l'étape précédente, vous avez créé le type d'événement. Dans cette étape, vous allez créer et entraîner un modèle pour le type d'événement. Le modèle fait office de conteneur pour les versions de votre modèle. Chaque fois que vous entraînez un modèle, une nouvelle version est créée.

Utilisez les exemples de codes suivants pour créer et entraîner un modèle Online Fraud Insights. Ce modèle s'appelle`sample_fraud_detection_model`. Il s'agit du type d'événement`sample_registration` utilisant l'exemple de jeu de données d'enregistrement de compte que vous avez chargé sur Amazon S3.

Pour plus d'informations sur les différents types de modèles pris en charge par Amazon Fraud Detector, consultezChoisissez un type de modèle.

Création d'un modèle

Dans l'exemple suivant, l'CreateModelAPI est utilisée pour créer un modèle.

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

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

Entraînez un mannequin

Dans l'exemple suivant, l'CreateModelVersionAPI est utilisée pour entraîner le modèle. Spécifiez `'EXTERNAL_EVENTS'` le nom`trainingDataSource` et l'emplacement Amazon S3 dans lequel vous avez stocké votre exemple de jeu RoleArnde données et le compartiment Amazon S3 pour lequel vous avez stocké`externalEventsDetail`. En tant que`trainingDataSchema` paramètre, spécifiez la manière dont Amazon Fraud Detector interprète les données d'exemple. Spécifiez plus précisément les variables à inclure et la manière de classer les étiquettes des événements.

```
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'
}
)
```

Vous pouvez entraîner votre modèle plusieurs fois. Chaque fois que vous entraînez un modèle, une nouvelle version est créée. Une fois la formation du modèle terminée, le statut de la version du modèle passe à`TRAINING_COMPLETE`. Vous pouvez consulter le score de performance du modèle et d'autres mesures de performance du modèle.

Passez en revue les performances du modèle

Une étape importante de l'utilisation d'Amazon Fraud Detector consiste à évaluer la précision de votre modèle à l'aide des scores et des indicateurs de performance du modèle. Une fois la formation du modèle terminée, Amazon Fraud Detector valide les performances du modèle en utilisant les 15 % de vos données qui n'ont pas été utilisées pour entraîner le modèle. Il génère un score de performance du modèle et d'autres mesures de performance.

Utilisez l'DescribeModelVersionsAPI pour examiner les performances du modèle. Examinez le score global des performances du modèle et tous les autres indicateurs générés par Amazon Fraud Detector pour ce modèle.

Pour en savoir plus sur le score de performance et les mesures de performance du modèle, consultezScores du modèle etIndicateurs de performance du modèle.

Vous pouvez vous attendre à ce que tous vos modèles Amazon Fraud Detector expérimentés disposent de mesures de performance réelles en matière de détection des fraudes, similaires à celles décrites dans ce didacticiel.

Déployer un modèle

Après avoir examiné les indicateurs de performance de votre modèle entraîné, déployez le modèle et mettez-le à la disposition d'Amazon Fraud Detector pour générer des prévisions de fraude. Pour déployer le modèle entraîné, utilisez l'UpdateModelVersionStatusAPI. Dans l'exemple suivant, il est utilisé pour mettre à jour l'état de la version du modèle à 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'
)
```

Étape 5 : Création du détecteur, des résultats, des règles et de la version du détecteur

Un détecteur contient la logique de détection, telle que les modèles et les règles. Cette logique s'applique à un événement particulier que vous souhaitez évaluer pour détecter une fraude. Une règle est une condition que vous spécifiez pour indiquer à Amazon Fraud Detector comment interpréter les valeurs des variables lors de la prédiction. Et le résultat est le résultat d'une prédiction de fraude. Un détecteur peut avoir plusieurs versions, chaque version ayant le statut BROUILLON, ACTIF ou INACTIF. Une version du détecteur doit avoir au moins une règle associée.

Utilisez les exemples de codes suivants pour créer un détecteur, des règles, des résultats et pour publier le détecteur.

Créer un détecteur

Dans l'exemple suivant, l'PutDetectorAPI est utilisée pour créer un`sample_detector` détecteur pour le type`sample_registration` d'événement.

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

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

Créez des résultats

Des résultats sont créés pour chaque résultat de prédiction de fraude possible. Dans l'exemple suivant, l'PutOutcomeAPI est utilisée pour créer trois résultats :`verify_customer`,`review`, et`approve`. Ces résultats sont ensuite affectés à des règles.

```
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'
)
```

Création de règles

La règle comprend une ou plusieurs variables de votre ensemble de données, une expression logique et un ou plusieurs résultats.

Dans l'exemple suivant, l'CreateRuleAPI est utilisée pour créer trois règles différentes :`high_risk`, `medium_risk`, et`low_risk`. Créez des expressions de règles pour comparer la`sample_fraud_detection_model_insightscore` valeur du score de performance du modèle par rapport à différents seuils. Il s'agit de déterminer le niveau de risque associé à un événement et d'attribuer le résultat défini à l'étape précédente.

```
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']
      )
```

Créer une version du détecteur

Une version de détecteur définit le modèle et les règles utilisés pour prédire les fraudes.

Dans l'exemple suivant, l'CreateDetectorVersionAPI est utilisée pour créer une version de détecteur. Pour ce faire, il fournit des détails sur la version du modèle, des règles et un mode d'exécution des règles FIRST_MATCHED. Un mode d'exécution des règles spécifie la séquence d'évaluation des règles. Le mode d'exécution des règles FIRST_MATCHED indique que les règles sont évaluées de manière séquentielle, de la première à la dernière, en s'arrêtant à la première règle correspondante.

```
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'
)
```

Étape 6 : Créer des prédictions de fraude

La dernière étape de ce didacticiel utilise le détecteur`sample_detector` créé à l'étape précédente pour générer des prévisions de fraude pour le type d'`sample_registration`événement en temps réel. Le détecteur évalue les exemples de données qui sont chargés sur Amazon S3. La réponse inclut les scores de performance du modèle ainsi que tous les résultats associés aux règles correspondantes.

Dans l'exemple suivant, l'GetEventPredictionAPI est utilisée pour fournir des données provenant de l'enregistrement d'un seul compte à chaque demande. Pour ce didacticiel, prenez les données (email_address et ip_address) de l'exemple de fichier de données d'enregistrement du compte. Chaque ligne (ligne) située après la ligne d'en-tête supérieure représente les données d'un seul événement d'enregistrement de compte.

```
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'
}
)
```

Après avoir terminé ce didacticiel, vous avez effectué les opérations suivantes :

- A chargé un exemple de jeu de données d'événements sur Amazon S3.
- Variables, entités et étiquettes créées qui sont utilisées pour créer et entraîner un modèle.
- Création et entraînement d'un modèle à l'aide de l'exemple de jeu de données.

- Vous avez consulté le score de performance du modèle et d'autres indicateurs de performance générés par Amazon Fraud Detector.
- Déploiement du modèle de détection des fraudes.
- Création d'un détecteur et ajout du modèle déployé.
- Ajout de règles, de l'ordre d'exécution des règles et des résultats au détecteur.
- Version du détecteur.
- J'ai testé le détecteur en fournissant différentes entrées et en vérifiant si les règles et l'ordre d'exécution des règles fonctionnaient comme prévu.

(Facultatif) Explorez les API Amazon Fraud Detector avec un bloc-notes Jupyter (IPython)

Pour plus d'exemples d'utilisation des API Amazon Fraud Detector, consultez le aws-fraud-detector-samples GitHub référentiel. Les sujets abordés dans les carnets incluent à la fois la création de modèles et de détecteurs à l'aide des API Amazon Fraud Detector et la création de demandes de prédiction de fraude par lots à l'aide de l'`GetEventPrediction`API.

Étapes suivantes

Maintenant que vous avez créé un modèle et un détecteur, vous pouvez aller plus loin et commencer à créer des modèles et des détecteurs et à générer des prévisions de fraude.

Les sections suivantes du guide de l'utilisateur d'Amazon Fraud Detector décrivent comment votre entreprise ou organisation peut utiliser Amazon Fraud Detector pour détecter les fraudes.

- Préparez et créez votre jeu de données d'événements pour entraîner votre modèle.
- Créer un type d'événement
- Créer un modèle
- Créer un détecteur
- Obtenir des prévisions en matière de fraude
- Gérez vos ressources Amazon Fraud Detector (en particulier, les variables, les entités, les résultats et les étiquettes)
- Configuration d'Amazon Fraud Detector pour atteindre vos objectifs en matière de sécurité et de conformité

- Surveillez Amazon Fraud Detector et enregistrez les appels d'API Amazon Fraud Detector
- Résolvez les problèmes avec Amazon Fraud Detector

Ensemble de données d'événement

Un jeu de données sur les événements est l'historique des fraudes de votre entreprise. Vous fournissez ces données à Amazon Fraud Detector pour créer des modèles de détection des fraudes.

Amazon Fraud Detector utilise des modèles d'apprentissage automatique pour générer des prévisions de fraude. Chaque modèle est entraîné à l'aide d'un type de modèle. Le type de modèle spécifie les algorithmes et les transformations utilisés pour l'entraînement du modèle. L'apprentissage des modèles consiste à utiliser un jeu de données que vous fournissez pour créer un modèle capable de prédire les événements frauduleux. Pour plus d'informations, consultez Utilisation du détecteur de fraude d'Amazon Fraud Detector.

L'ensemble de données utilisé pour créer le modèle de détection des fraudes fournit des détails sur un événement. Un événement est une activité commerciale évaluée pour le risque de fraude. Par exemple, l'enregistrement d'un compte peut être un événement. Les données associées à l'événement d'enregistrement du compte peuvent être un ensemble de données d'événements. Amazon Fraud Detector utilise cet ensemble de données pour évaluer les fraudes liées à l'enregistrement de comptes.

Avant de fournir votre ensemble de données à Amazon Fraud Detector pour créer un modèle, assurez-vous de définir votre objectif de création du modèle. Vous devez également déterminer la manière dont vous souhaitez utiliser le modèle et définir vos mesures pour évaluer si le modèle fonctionne en fonction de vos besoins spécifiques.

Par exemple, vos objectifs en matière de création d'un modèle de détection des fraudes qui évalue les fraudes liées à l'enregistrement de comptes peuvent être les suivants :

- Pour approuver automatiquement les inscriptions légitimes.
- Pour détecter les inscriptions frauduleuses en vue d'une enquête ultérieure.

Une fois que vous avez déterminé votre objectif, l'étape suivante consiste à décider de la manière dont vous souhaitez utiliser le modèle. Voici quelques exemples d'utilisation d'un modèle de détection des fraudes pour évaluer les fraudes à l'enregistrement :

- Pour détecter les fraudes en temps réel pour chaque enregistrement de compte.
- Pour une évaluation hors ligne de toutes les inscriptions de comptes toutes les heures.

Voici quelques exemples de mesures pouvant être utilisées pour mesurer les performances du modèle :

- Performances constamment supérieures à la valeur de référence actuelle en production.
- Capture X % d'enregistrements frauduleux avec un taux de Y % de faux positifs.
- Accepte jusqu'à 5 % des inscriptions approuvées automatiquement qui sont frauduleuses.

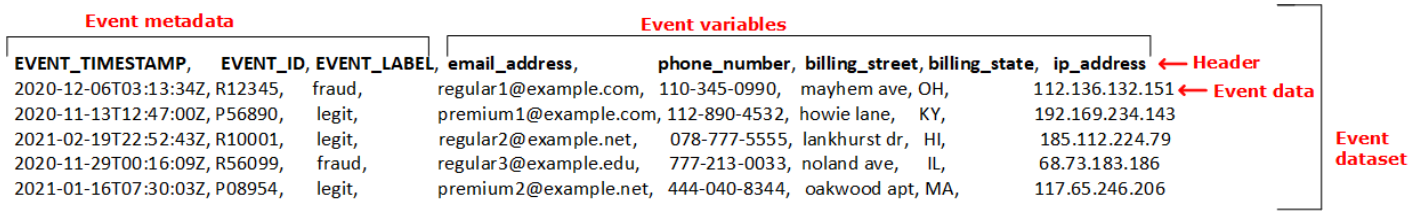
Structure du ensemble de données d'événement

Amazon Fraud Detector nécessite que vous fournissiez votre ensemble de données d'événements dans un fichier texte utilisant des valeurs séparées par des virgules (CSV) au format UTF-8. La première ligne de votre fichier de jeu de données CSV doit contenir des en-têtes de fichier. L'en-tête du fichier se compose de métadonnées d'événement et de variables d'événement qui décrivent chaque élément de données associé à l'événement. L'en-tête est suivi des données relatives à l'événement. Chaque ligne est composée d'éléments de données provenant d'un événement unique.

- Métadonnées de l'événement : fournissent des informations sur l'événement. Par exemple, EVENT_TIMESTAMP est une métadonnée d'événement qui spécifie l'heure à laquelle l'événement s'est produit. En fonction du cas d'utilisation de votre entreprise et du type de modèle utilisé pour créer et former votre modèle de détection des fraudes, Amazon Fraud Detector vous demande de fournir des métadonnées d'événements spécifiques. Lorsque vous spécifiez des métadonnées d'événement dans l'en-tête de votre fichier CSV, utilisez le même nom de métadonnées d'événement que celui spécifié par Amazon Fraud Detector et utilisez uniquement des lettres majuscules.
- Variable d'événement : représente les éléments de données spécifiques à votre événement que vous souhaitez utiliser pour créer et former votre modèle de détection des fraudes. En fonction du cas d'utilisation de votre entreprise et du type de modèle utilisé pour créer et former un modèle de détection des fraudes, Amazon Fraud Detector peut vous demander ou vous recommander de fournir des variables d'événement spécifiques. Vous pouvez également éventuellement fournir d'autres variables d'événement issues de votre événement que vous souhaitez inclure dans l'entraînement du modèle. Voici quelques exemples de variables d'événement pour un événement d'inscription en ligne : adresse e-mail, adresse IP et numéro de téléphone. Lorsque vous spécifiez le nom de la variable d'événement dans l'en-tête de votre fichier CSV, utilisez le nom de variable de votre choix et utilisez uniquement des lettres minuscules.
- Données d'événement : représentent les données collectées à partir de l'événement réel. Dans votre fichier CSV, chaque ligne qui suit l'en-tête du fichier est composée d'éléments de

données provenant d'un seul événement. Par exemple, dans un fichier de données d'événements d'inscription en ligne, chaque ligne contient les données d'une seule inscription. Chaque élément de données de la ligne doit correspondre aux métadonnées d'événement correspondantes ou à la variable d'événement.

Voici un exemple de fichier CSV contenant des données d'un événement d'enregistrement de compte. La ligne d'en-tête contient à la fois les métadonnées d'événement en majuscules et les variables d'événement en minuscules, suivies des données d'événement. Chaque ligne de l'ensemble de données contient des éléments de données associés à l'enregistrement d'un compte unique, chaque élément de données correspondant à l'en-tête.



Obtenez les exigences relatives aux ensembles de données d'événements à l'aide de l'explorateur de modèles

Le type de modèle que vous choisissez pour créer votre modèle définit les exigences de votre jeu de données. Amazon Fraud Detector utilise l'ensemble de données que vous fournissez pour créer et former votre modèle de détection des fraudes. Avant qu'Amazon Fraud Detector ne commence à créer votre modèle, il vérifie si l'ensemble de données répond aux exigences en matière de taille, de format et d'autres exigences. Si le jeu de données ne répond pas aux exigences, la création du modèle et l'apprentissage échouent. Vous pouvez utiliser l'explorateur de modèles de données pour identifier un type de modèle à utiliser pour votre cas d'utilisation commerciale et pour obtenir des informations sur les exigences en matière d'ensembles de données pour le type de modèle identifié.

Explorateur de modèle de données

L'explorateur de modèles de données est un outil intégré à la console Amazon Fraud Detector qui aligne le cas d'utilisation de votre entreprise sur le type de modèle pris en charge par Amazon Fraud Detector. L'explorateur de modèles de données fournit également des informations sur les éléments de données requis par Amazon Fraud Detector pour créer votre modèle de détection des fraudes. Avant de commencer à préparer votre jeu de données d'événements, utilisez l'explorateur de modèles de données pour déterminer le type de modèle recommandé par Amazon Fraud Detector

pour votre entreprise et pour consulter la liste des éléments de données obligatoires, recommandés et facultatifs dont vous aurez besoin pour créer votre jeu de données.

Pour utiliser l'explorateur de modèles de données,

1. Ouvrez la consoleAWS de gestion et connectez-vous à votre compte. Accédez à Amazon Fraud Detector.
2. Dans le panneau de navigation de gauche, choisissez Explorateur de modèle de données.
3. Sur la page Explorateur de modèles de données, sous Cas d'utilisation professionnelle, sélectionnez le cas d'utilisation commerciale que vous souhaitez évaluer en termes de risque de fraude.
4. Amazon Fraud Detector affiche le type de modèle recommandé qui correspond au cas d'utilisation de votre entreprise. Le type de modèle définit les algorithmes, les enrichissements et les transformations qu'Amazon Fraud Detector utilisera pour former votre modèle de détection des fraudes.

   Notez le type de modèle recommandé. Vous en aurez besoin plus tard lorsque vous créerez votre modèle.

   > **Note**
   >
   > Si vous ne trouvez pas votre cas d'utilisation professionnelle, utilisez le lien Nous contacter dans la description pour nous fournir les détails de votre cas d'utilisation professionnelle. Nous vous recommanderons le type de modèle à utiliser pour créer un modèle de détection des fraudes adapté à votre cas d'utilisation professionnelle.

5. Le volet Informations sur les modèles de données fournit un aperçu des éléments de données obligatoires, recommandés et facultatifs requis pour créer et former un modèle de détection des fraudes adapté à votre cas d'utilisation commerciale. Utilisez les informations du volet d'informations pour recueillir les données de vos événements et créer votre ensemble de données.

Collecter des données d'événement

La collecte des données relatives à vos événements est une étape importante dans la création de votre modèle. En effet, les performances de votre modèle en matière de prédiction de la fraude dépendent de la qualité de votre jeu de données. Lorsque vous commencez à recueillir les données

relatives à vos événements, gardez à l'esprit la liste des éléments de données que l'explorateur de modèles de données vous a fourni pour créer votre ensemble de données. Vous devrez rassembler toutes les données obligatoires (métadonnées d'événements) et décider quels éléments de données recommandés et facultatifs (variables d'événement) à inclure en fonction de vos objectifs de création du modèle. Il est également important de décider du format de chaque variable d'événement que vous souhaitez inclure et de la taille totale de votre ensemble de données.

Qualité du jeu de données d'événements

Pour recueillir un ensemble de données de haute qualité pour votre modèle, nous vous recommandons ce qui suit :

- Collectez des données matures : l'utilisation des données les plus récentes permet d'identifier le modèle de fraude le plus récent. Toutefois, pour détecter les cas d'utilisation frauduleuse, laissez les données mûrir. La période d'échéance dépend de votre activité et peut durer de deux semaines à trois mois. Par exemple, si votre événement inclut une transaction par carte de crédit, la maturité des données peut être déterminée par le délai de rétrofacturation de la carte de crédit ou par le temps mis par un enquêteur pour prendre une décision.

  Assurez-vous que l'ensemble de données utilisé pour former le modèle a eu suffisamment de temps pour arriver à maturité, conformément à votre activité.
- Assurez-vous que la distribution des données ne dévie pas de manière significative : le processus de formation du modèle Amazon Fraud Detector échantillonne et partitionne votre ensemble de données en fonction de EVENT_TIMESTAMP. Par exemple, si votre ensemble de données se compose d'événements frauduleux survenus au cours des 6 derniers mois, mais que seul le dernier mois d'événements légitimes est inclus, la distribution des données est considérée comme étant à la dérive et instable. Un jeu de données instable peut entraîner des biais dans l'évaluation des performances du modèle. Si vous constatez une dérive significative de la distribution des données, pensez à équilibrer votre ensemble de données en collectant des données similaires à la distribution des données actuelle.
- Assurez-vous que l'ensemble de données est représentatif du cas d'utilisation dans lequel le modèle est implémenté/testé. Sinon, les performances estimées pourraient être biaisées. Supposons que vous utilisiez un modèle pour refuser automatiquement tous les candidats internes, mais que votre modèle est entraîné à l'aide d'un ensemble de données contenant des données/étiquettes historiques qui ont été précédemment approuvées. L'évaluation de votre modèle peut alors être inexacte, car elle est basée sur l'ensemble de données qui ne contient aucune représentation des candidats refusés.

Format des données de l'événement

Amazon Fraud Detector transforme la plupart de vos données au format requis dans le cadre de son processus de formation des modèles. Cependant, certains formats standard que vous pouvez facilement utiliser pour fournir vos données peuvent vous aider à éviter des problèmes ultérieurs lorsque Amazon Fraud Detector validera votre ensemble de données. Le tableau suivant fournit des conseils sur les formats à utiliser pour fournir les métadonnées d'événements recommandées.

> **Note**
>
> Lorsque vous créez votre fichier CSV, veillez à saisir le nom des métadonnées de l'événement comme indiqué ci-dessous, en lettres majuscules.

Nom des métadonnées	Format	Obligatoire
IDENTIFIANT DE L'ÉVÉNEMENT	S'il est fourni, il doit répondre aux critères suivants : • C'est unique pour cet événement. • Il représente des informations importantes pour votre entreprise. • Il suit le modèle d'expression régulière (par exemple,`^[0-9a-z_-]+$`.) • Outre les exigences ci-dessus, nous vous recommandons de ne pas ajouter d'horodatage à l'EVENT_ID. Cela peut entraîner des problèmes lors de la mise à jour de l'événement. Cela est dû au fait que vous devez	Cela dépend du type de modèle

Nom des métadonnées	Format	Obligatoire
	fournir exactement le même EVENT_ID pour ce faire.	

Nom des métadonnées	Format	Obligatoire

TIMESTAMP DE L'ÉVÉNEMENT	• Il doit être spécifié dans l'un des formats suivants :
	  • %YYYY-%mm-%DDT %Hh : %mm : %SSz (norme ISO 8601 en UTC uniquement, sans millisecondes)
	  Exemple : 2019-11-30T 13:01:01 Z
	  • %yyyy/%mm/%dd %hh : %mm : %ss (AM/PM)
	  Exemples : 2019/11/30 13:01:01, ou 2019/11/30 13:01:01
	  • %mm/%dd/%yyyy %hh : %mm : %ss
	  Exemples : 30/11/201 9 13:01:01, 30/11/2019 13:01:01
	  • %mm/%dd/%yy %hh : %mm : %ss
	  Exemples : 30/11/19 13:01:01, 30/11/19 13:01:01
	• Amazon Fraud Detector part des hypothèses suivantes lors de l'analyse des formats de date/d'horodatage pour les horodatages des événements :
		Oui

Nom des métadonnées	Format	Obligatoire

	• Si vous utilisez la norme ISO 8601, elle doit correspondre exactement à la spécification précédente
	• Si vous utilisez l'un des autres formats, vous bénéficiez d'une flexibilité supplémentaire :
	  • Pour les mois et les jours, vous pouvez fournir un ou deux chiffres. Par exemple, le 1/12/2019 est une date valide.
	  • Vous n'avez pas besoin d'inclure hh:mm:ss si vous ne les avez pas (vous pouvez simplement indiquer une date). Vous pouvez également fournir un sous-ensemble contenant uniquement les heures et les minutes (par exemple, hh:mm). Le simple fait de fournir une heure n'est pas pris en charge. Les millisecondes ne sont pas non plus prises en charge.
	  • Si vous fournissez des étiquettes AM/PM, une	

Nom des métadonnées	Format	Obligatoire
	horloge de 12 heures est supposée. S'il n'y a aucune information AM/PM, une horloge de 24 heures est supposée. • Vous pouvez utiliser «/» ou « - » comme délimiteurs pour les éléments de date. « : » est supposé pour les éléments d'horodatage.	
IDENTITÉ_D'ENTITÉ	• Il doit suivre le modèle d'expression régulière :`^[0-9A-Za-z_.@+-]+$` . • Si l'identifiant de l'entité n'est pas disponible au moment de l'évaluation, spécifiez l'identifiant de l'entité comme inconnu.	Cela dépend du type de modèle
TYPE_ENTITÉ	Vous pouvez utiliser n'importe quelle chaîne	Cela dépend du type de modèle
ÉTIQUETTE DE L'ÉVÉNEMENT	Vous pouvez utiliser n'importe quelle étiquette, telle que « fraude », « légitime », « 1 » ou « 0 ».	Obligatoire si LABEL_TIMESTAMP est inclus
LABEL_TIMESTAMP	Il doit respecter le format d'horodatage.	Obligatoire si EVENT_LABEL est inclus

Pour plus d'informations sur les variables d'événement, consultez la section Variables.

> **Important**
>
> Si vous créez un modèle Account Takeover Insights (ATI), consultez la sectionPréparation des données pour plus de détails sur la préparation et la sélection des données.

Valeurs nulles ou manquantes

Les variables EVENT_TIMESTAMP et EVENT_LABEL ne doivent contenir aucune valeur nulle ou manquante. Vous pouvez avoir des valeurs nulles ou manquantes pour d'autres variables. Toutefois, nous vous recommandons de n'utiliser qu'un petit nombre de valeurs nulles pour ces variables. Si Amazon Fraud Detector détermine qu'il y a trop de valeurs nulles ou manquantes pour une variable d'événement, il omettra automatiquement la variable de votre modèle.

Variables minimales

Lorsque vous créez votre modèle, le jeu de données doit inclure au moins deux variables d'événement en plus des métadonnées d'événements requises. Les deux variables d'événement doivent réussir le contrôle de validation.

Taille du jeu de données d'événements

Obligatoire

Votre jeu de données doit répondre aux exigences de base suivantes pour un apprentissage réussi des modèles.

- Données provenant d'au moins 100 événements.
- L'ensemble de données doit inclure au moins 50 événements (lignes) classés comme frauduleux.

Recommandée

Nous vous recommandons d'inclure dans votre jeu de données les éléments suivants pour un apprentissage réussi du modèle et de bonnes performances du modèle.

- Incluez au moins trois semaines de données historiques, mais au mieux six mois de données.
- Incluez un minimum de 10 000 données d'événements au total.
- Incluez au moins 400 événements (lignes) classés comme frauduleux et 400 événements (lignes) considérés comme légitimes.

- Incluez plus de 100 entités uniques, si votre type de modèle nécessite ENTITY_ID.

Validation des données

Avant de commencer à créer votre modèle, Amazon Fraud Detector vérifie si les variables incluses dans l'ensemble de données pour l'entraînement du modèle répondent à la taille, au format et aux autres exigences. Si le jeu de données ne passe pas la validation, le modèle n'est pas créé. Vous devez d'abord corriger les variables qui n'ont pas passé la validation avant de créer le modèle. Amazon Fraud Detector vous fournit un profileur de données que vous pouvez utiliser pour vous aider à identifier et à résoudre les problèmes liés à votre ensemble de données avant de commencer à entraîner votre modèle.

Profileur de données

Amazon Fraud Detector fournit un outil open source pour le profilage et la préparation de vos données pour la formation des modèles. Ce profileur de données automatisé vous permet d'éviter les erreurs courantes de préparation des données et d'identifier les problèmes potentiels tels que les types de variables mal mappés qui pourraient avoir un impact négatif sur les performances du modèle. Le profileur génère un rapport intuitif et complet de votre ensemble de données, y compris des statistiques sur les variables, la distribution des étiquettes, des analyses catégorielles et numériques, ainsi que des corrélations entre variables et étiquettes. Il fournit des conseils sur les types de variables ainsi qu'une option permettant de transformer l'ensemble de données dans le format requis par Amazon Fraud Detector.

Utilisation du profileur de données

Le profileur de données automatisé est construit avec uneAWS CloudFormation pile que vous pouvez facilement lancer en quelques clics. Tous les codes sont disponibles sur Github. Pour en savoir plus sur l'utilisation du profileur de données, suivez les instructions de notre blog Entraînez les modèles plus rapidement grâce à un profileur de données automatisé pour Amazon Fraud Detector

Erreurs courantes liées aux ensembles de données d'événements

Voici quelques-uns des problèmes courants rencontrés par Amazon Fraud Detector lors de la validation d'un ensemble de données d'événements. Après avoir exécuté le profileur de données, utilisez cette liste pour vérifier l'absence d'erreurs dans votre jeu de données avant de créer votre modèle.

- Le fichier CSV n'est pas au format UTF-8.

- Le nombre d'événements dans l'ensemble de données est inférieur à 100.
- Le nombre d'événements identifiés comme frauduleux ou légitimes est inférieur à 50.
- Le nombre d'entités uniques associées à un événement de fraude est inférieur à 100.
- Plus de 0,1 % des valeurs de EVENT_TIMESTAMP contiennent des valeurs nulles ou des valeurs autres que les formats de date/d'horodatage pris en charge.
- Plus de 1 % des valeurs de EVENT_LABEL contiennent des valeurs nulles ou autres que celles définies dans le type d'événement.
- Moins de deux variables sont disponibles pour l'entraînement des modèles.

Stockage de données

Après avoir rassemblé votre ensemble de données, vous stockant votre ensemble de données en interne à l'aide d'Amazon Fraud Detector Simple Storage Service (Amazon S3). Nous vous recommandons de choisir l'emplacement de stockage de votre ensemble de données en fonction du modèle que vous utilisez pour générer des prévisions de fraude. Pour plus d'informations sur les types de modèles, voir Choisir un type de modèle. Pour plus d'informations sur le stockage de votre jeu de données, consultezStockage des données des événements.

Type d'événement

Avec Amazon Fraud Detector, vous générez des prévisions de fraude pour les événements. Un type d'événement définit la structure d'un événement individuel envoyé à Amazon Fraud Detector. Une fois définis, vous pouvez créer des modèles et des détecteurs qui évaluent le risque associé à des types d'événements spécifiques.

La structure d'un événement comprend les éléments suivants :

- Type d'entité : classe qui organise l'événement. Pendant la prédiction, spécifiez le type d'entité et l'ID de l'entité pour définir qui a réalisé l'événement.
- Variables : définit les variables qui peuvent être envoyées dans le cadre de l'événement. Les variables sont utilisées par les modèles et les règles pour évaluer le risque de fraude. Une fois ajoutées, les variables ne peuvent pas être supprimées d'un type d'événement.
- Libellés : classe un événement comme frauduleux ou légitime. Utilisé lors de l'entraînement des modèles. Une fois ajoutées, les étiquettes ne peuvent pas être supprimées d'un type d'événement.

Création d'un type d'événement

Avant de créer votre modèle de détection des fraudes, vous devez d'abord créer un type d'événement. La création d'un type d'événement implique de définir votre activité commerciale (événement) afin d'évaluer les risques de fraude. La définition de l'événement implique d'identifier les variables d'événement dans votre ensemble de données à inclure pour l'évaluation des fraudes, de spécifier l'entité à l'origine de l'événement et les étiquettes qui classent l'événement.

Conditions préalables à la création d'un type d'événement

Avant de commencer à créer votre type d'événement, assurez-vous d'avoir effectué les opérations suivantes :

- Vous avez utilisé l'Explorateur de modèle de donnéesoutil pour obtenir des informations sur les éléments de données requis par Amazon Fraud Detector pour créer votre modèle de détection des fraudes.
- Vous avez utilisé les informations que vous avez obtenues grâce à l'explorateur de modèles de données pour créer votre jeu de données d'événements et l'avez chargé dans le compartiment Amazon S3.

- Créé VariablesEntité, et Etiquettes vous souhaitez qu'Amazon Fraud Detector l'utilise pour créer un modèle de détection des fraudes pour cet événement. Assurez-vous que les variables, le type d'entité et les étiquettes que vous avez créés sont inclus dans votre jeu de données d'événements.

Vous pouvez créer votre type d'événement dans la console Amazon Fraud Detector, à l'aide de l'APIAWS CLI, du SDK ou du AWS SDK.

Création d'un type d'événement dans la console Amazon Fraud Detector

Pour créer un type d'événement,

1. Ouvrez la console AWS de gestion et connectez-vous à votre compte. Accédez à Amazon Fraud Detector.
2. Dans le volet de navigation de gauche, sélectionnez Événements.
3. Sur la page Type d'événements, choisissez Créer.
4. Sous Détails du type d'événement,
   a. Dans le champ Nom, entrez le nom de votre événement.
   b. Dans la description, entrez éventuellement une description.
   c. Dans l'Entité, sélectionnez le type d'entité que vous avez créé pour votre événement.
5. Sous Variables d'événement,
   - Dans la section Choisissez comment définir les variables de cet événement,
     - Si vous avez déjà créé vos variables d'événement pour cet événement, sélectionnez Sélectionner des variables dans votre liste de variables et, dans la section Variables, sélectionnez les variables que vous avez créées pour cet événement.
     - Si vous n'avez pas créé de variables pour cet événement, sélectionnez Sélectionner des variables à partir d'un ensemble de données d'entraînement,
       - Dans le rôle IAM, sélectionnez le rôle IAM que vous souhaitez qu'Amazon Fraud Detector utilise pour accéder au compartiment Amazon S3 qui contient votre ensemble de données.
       - Dans Emplacement des données, entrez le chemin d'accès à l'emplacement de votre jeu de données. Utilisez le `S3 URI` chemin similaire à celui-ci :`S3://your-bucket-name/example dataset filename.csv`.
       - Sélectionnez Charger.

- Sous Variables, tous les noms de variables d'événement qu'Amazon Fraud Detector a extraits de votre fichier de jeu de données s'affichent.

  Si vous souhaitez que la variable soit incluse pour détecter la fraude, sélectionnez le type de variable dans le champ Type de variable. Choisissez Supprimer pour ne plus inclure les variables dans le cadre de la détection des fraudes. Répétez cette étape pour chaque variable de la liste.

6. Sous Libellés (facultatif), dans les Libellés, sélectionnez les libellés que vous avez créés pour cet événement. Assurez-vous de sélectionner une étiquette pour les événements frauduleux et une étiquette pour les événements légitimes.
7. Si vous souhaitez configurer le traitement automatique en aval pour cet événement, sous Orchestration des événements avec Amazon EventBridge - facultatif, activez l'activation de l'orchestration des événements avec Amazon. EventBridge Pour plus d'informations sur l'orchestration des événements, reportez-vous à la section. Orchestration d'événements

   > **Note**
   >
   > Vous pouvez également activer l'orchestration des événements ultérieurement après avoir créé votre type d'événement.

8. Choisissez Créer un type d'événement.

Créez un type d'événement à l'aide du AWS SDK for Python (Boto3)

L'exemple suivant montre un exemple de demande pour l'`PutEventType`API. L'exemple suppose que vous avez créé les variables `ip_address` et`email_address`, les étiquettes `legit` et`fraud`, ainsi que le type d'entité`sample_customer`. Pour plus d'informations sur la création de ces ressources, reportez-vous à la sectionRessources.

> **Note**
>
> Vous devez d'abord créer des variables, des types d'entités et des étiquettes avant de les ajouter au type d'événement.

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

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

Supprimer un événement ou un type d'événement

Lorsque vous supprimez un événement, Amazon Fraud Detector supprime définitivement cet événement et les données associées à l'événement ne sont plus stockées dans Amazon Fraud Detector.

Pour supprimer un événement qu'Amazon Fraud Detector a évalué via **`GetEventPrediction`** l'API

1. Connectez-vous à la console Amazon Fraud Detector AWS Management Console et ouvrez-la à l'adresse https://console.aws.amazon.com/frauddetector.
2. Dans le volet de navigation de gauche de la console, choisissez Rechercher les prédictions passées.
3. Choisissez l'événement que vous souhaitez supprimer.
4. Choisissez Actions, puis sélectionnez Supprimer l'événement.
5. Entrez**`delete`**, puis choisissez Supprimer l'événement.

> **Note**
>
> Cela supprime tous les enregistrements associés à cet ID d'événement, y compris les données d'événement envoyées à l'`SendEvent`opération et toutes les données de prédiction générées par le biais de l'`GetEventPrediction`opération.

Pour supprimer un événement qui est stocké dans Amazon Fraud Detector mais qui n'a pas été évalué (c'est-à-dire qu'il a été stocké via l'`SendEvent`opération), vous devez faire une `DeleteEvent` demande et spécifier l'ID de l'événement et l'ID du type d'événement. Si vous souhaitez supprimer à la fois l'événement et tout historique des prévisions associé à l'événement, définissez la valeur du `deleteAuditHistory` paramètre sur « true ». Lorsque le `deleteAuditHistory` paramètre est défini sur « true », les données de l'événement sont disponibles par le biais de la recherche jusqu'à 30 secondes après la fin de l'opération de suppression.

Pour supprimer tous les événements associés à un type d'événement

1. Dans le volet de navigation gauche de la console, choisissez Types d'événements
2. Choisissez le type d'événement pour lequel vous souhaitez que tous les événements soient supprimés.
3. Accédez à l'onglet Événements enregistrés et choisissez Supprimer les événements stockés

Selon le nombre d'événements stockés pour le type d'événement, la suppression de tous les événements stockés peut prendre un certain temps. Par exemple, la suppression d'un jeu de données de 1 Go (environ 1 à 2 millions d'événements pour un client moyen) prend environ 2 heures. Pendant ce temps, les nouveaux événements de ce type que vous envoyez à Amazon Fraud Detector ne sont pas stockés, mais vous pouvez continuer à générer des prévisions de fraude via cette `GetEventPrediction` opération.

Pour supprimer un type d'événement

Vous ne pouvez pas supprimer un type d'événement utilisé dans un détecteur ou un modèle, ou auquel des événements sont associés. Avant de supprimer un type d'événement, vous devez supprimer tous les événements associés à ce type d'événement.

Lorsque vous supprimez un type d'événement, Amazon Fraud Detector supprime définitivement ce type d'événement et les données ne sont plus stockées dans Amazon Fraud Detector.

1. Dans le volet de navigation de gauche de la console Amazon Fraud Detector, choisissez Ressources, puis Événements.
2. Choisissez le type d'événement que vous souhaitez supprimer.
3. Choisissez Actions, puis sélectionnez Supprimer le type d'événement.
4. Entrez le nom du type d'événement, puis choisissez Supprimer le type d'événement.

Stockage des données des événements

Après avoir rassemblé votre jeu de données, vous stockez votre jeu de données en interne à l'aide d'Amazon Fraud Detector ou en externe avec Amazon Simple Storage Service (Amazon S3). Nous vous recommandons de choisir l'emplacement de stockage de votre ensemble de données en fonction du modèle que vous utilisez pour générer des prévisions de fraude. Vous trouverez ci-dessous une description détaillée de ces deux options de stockage.

- Stockage interne : votre ensemble de données est stocké dans Amazon Fraud Detector. Toutes les données d'événement associées à un événement sont stockées ensemble. Vous pouvez télécharger le jeu de données d'événements stocké dans Amazon Fraud Detector à tout moment. Vous pouvez soit diffuser des événements un par un vers une API Amazon Fraud Detector, soit importer de grands ensembles de données (jusqu'à 1 Go) à l'aide de la fonction d'importation par lots. Lorsque vous entraînez un modèle à l'aide de l'ensemble de données stocké dans Amazon Fraud Detector, vous pouvez spécifier une plage de temps afin de limiter la taille de votre jeu de données.
- Stockage externe : votre ensemble de données est stocké dans une source de données externe autre qu'Amazon Fraud Detector. Amazon Fraud Detector prend actuellement en charge l'utilisation d'Amazon Simple Storage Service (Amazon S3) à cette fin. Si votre modèle figure dans un fichier chargé sur Amazon S3, ce fichier ne peut pas contenir plus de 5 Go de données non compressées. Si c'est plus que cela, veillez à raccourcir la plage de temps de votre jeu de données.

Le tableau suivant fournit des détails sur le type de modèle et la source de données qu'il prend en charge.

Type de modèle	Source de données d'entraînement compatible
Informations sur la fraude en ligne	Stockage externe, Stockage interne
Informations sur la fraude transactionnelle	Stockage interne
Informations sur le rachat de comptes	Stockage interne

Pour plus d'informations sur le stockage externe de votre jeu de données avec Amazon Simple Storage Service, consultezStockez les données de vos événements en externe avec Amazon S3 .

Pour plus d'informations sur le stockage interne de votre ensemble de données avec Amazon Fraud Detector, consultezStockez les données de vos événements en interne avec Amazon Fraud Detector.

Stockez les données de vos événements en externe avec Amazon S3

Si vous formez un modèle Online Fraud Insights, vous pouvez choisir de stocker les données de vos événements en externe avec Amazon S3. Pour stocker les données de vos événements dans Amazon S3, vous devez d'abord créer un fichier texte au format CSV, ajouter les données de vos événements, puis charger le fichier CSV dans un compartiment Amazon S3.

> **Note**
>
> Les modèles Transaction Fraud Insights et Account Takeover Insights ne prennent pas en charge les ensembles de données stockés en externe avec Amazon S3.

Création d'un fichier CSV

Amazon Fraud Detector nécessite que la première ligne de votre fichier CSV contienne des en-têtes de colonne. Les en-têtes de colonne de votre fichier CSV doivent correspondre aux variables définies dans le type d'événement. Pour un exemple de jeu de données, voirObtenir et télécharger un exemple de jeu de données

Le modèle Online Fraud Insights nécessite un ensemble de données d'entraînement comportant au moins 2 variables et jusqu'à 100 variables. Outre les variables d'événement, le jeu de données d'entraînement doit contenir les en-têtes suivants :

- EVENT_TIMESTAMP - Définit quand l'événement est survenu
- EVENT_LABEL : classe l'événement comme frauduleux ou légitime. Les valeurs de la colonne doivent correspondre aux valeurs définies dans le type d'événement.

Les exemples de données CSV suivants représentent l'historique des événements d'enregistrement d'un commerçant en ligne :

```
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**
>
> Le fichier de données CSV peut contenir des guillemets et des virgules dans le cadre de vos données.

Une version simplifiée du type d'événement correspondant est représentée ci-dessous. Les variables d'événement correspondent aux en-têtes du fichier CSV et les valeurs correspondantesEVENT_LABEL aux valeurs de la liste des étiquettes.

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

Formats d'horodatage des événements

Assurez-vous que l'horodatage de votre événement est au format requis. Dans le cadre du processus de création du modèle, le type de modèle Online Fraud Insights organise vos données en fonction de l'horodatage de l'événement et divise vos données à des fins de formation et de test. Pour obtenir une estimation juste des performances, le modèle s'entraîne d'abord sur l'ensemble de données d'apprentissage, puis teste ce modèle sur l'ensemble de données de test.

Amazon Fraud Detector prend en charge les formats de date et d'horodatage suivants pour les valeurs saisiesEVENT_TIMESTAMP lors de la formation du modèle :

- %YYYY-%mm-%DDT%Hh : %mm : %SSz (norme ISO 8601 en UTC uniquement, sans millisecondes)

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

Exemples : 2019/11/30 13:01:01, ou 2019/11/30 13:01:01

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

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

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

  Exemples : 30/11/19 13:01:01, 30/11/19 13:01:01

Amazon Fraud Detector part des hypothèses suivantes lors de l'analyse des formats de date/d'horodatage pour les horodatages des événements :

- Si vous utilisez la norme ISO 8601, elle doit correspondre exactement à la spécification précédente
- Si vous utilisez l'un des autres formats, vous bénéficiez d'une flexibilité supplémentaire :
  - Pour les mois et les jours, vous pouvez fournir un ou deux chiffres. Par exemple, le 1/12/2019 est une date valide.
  - Vous n'avez pas besoin d'inclure hh:mm:ss si vous ne les avez pas (vous pouvez simplement indiquer une date). Vous pouvez également fournir un sous-ensemble contenant uniquement les heures et les minutes (par exemple, hh:mm). Le simple fait de fournir une heure n'est pas pris en charge. Les millisecondes ne sont pas non plus prises en charge.
  - Si vous fournissez des étiquettes AM/PM, une horloge de 12 heures est supposée. S'il n'y a aucune information AM/PM, une horloge de 24 heures est supposée.
  - Vous pouvez utiliser «/» ou « - » comme délimiteurs pour les éléments de date. « : » est supposé pour les éléments d'horodatage.

Échantillonner votre ensemble de données au fil du temps

Nous vous recommandons de fournir des exemples de fraude et des échantillons légitimes datant de la même période. Par exemple, si vous signalez des événements de fraude survenus au cours des 6 derniers mois, vous devez également fournir des événements légitimes qui s'étendent uniformément sur la même période. Si votre jeu de données contient une distribution très inégale des fraudes et des événements légitimes, le message d'erreur suivant peut s'afficher : « La distribution de la fraude dans le temps fluctue de manière inacceptable. Impossible de diviser correctement l'ensemble de données. » En général, la solution la plus simple à cette erreur consiste à s'assurer que les événements frauduleux et les événements légitimes sont échantillonnés de manière uniforme au

cours de la même période. Il se peut également que vous deviez supprimer des données si vous avez été confronté à une forte recrudescence de fraudes dans un court laps de temps.

Si vous ne pouvez pas générer suffisamment de données pour créer un jeu de données réparti de manière uniforme, une approche consiste à randomiser l'EVENT_TIMESTAMP de vos événements de manière à ce qu'ils soient répartis de manière uniforme. Toutefois, cela se traduit souvent par des indicateurs de performance irréalistes, car Amazon Fraud Detector utilise EVENT_TIMESTAMP pour évaluer les modèles sur le sous-ensemble d'événements approprié de votre ensemble de données.

Valeurs nulles et manquantes

Amazon Fraud Detector gère les valeurs nulles et manquantes. Toutefois, le pourcentage de valeurs nulles pour les variables doit être limité. Les colonnes EVENT_TIMESTAMP et EVENT_LABEL ne doivent contenir aucune valeur manquante.

Validation de fichiers

Amazon Fraud Detector ne parviendra pas à entraîner un modèle si l'une des conditions suivantes est remplie :

- Si le fichier CSV ne peut pas être analysé
- Si le type de données d'une colonne est incorrect

Chargez les données de vos événements dans un compartiment Amazon S3

Après avoir créé un fichier CSV avec les données de vos événements, chargez-le dans votre compartiment Amazon S3.

Pour charger vers un compartiment Amazon S3

1. Connectez-vous à la AWS Management Console et ouvrez la console Simple Storage Service (Amazon S3) à la page https://console.aws.amazon.com/s3/.
2. Choisissez Créer un compartiment.

   L'Assistant Create bucket (Créer un compartiment) s'ouvre.
3. Dans Bucket name (Nom du compartiment), saisissez un nom compatible DNS pour votre compartiment.

Les nom du compartiment doit présenter les caractéristiques suivantes :

- Il doit être unique sur l'ensemble d'Amazon S3.
- Il doit comporter entre 3 et 63 caractères.
- Ne contient pas de majuscules.
- Il doit commencer par une minuscule ou un chiffre.

Une fois le compartiment créé, vous ne pouvez pas changer son nom. Pour plus d'informations sur l'attribution de noms de compartiments, veuillez consulter Règles relatives à l'attribution des noms de compartiments dans le Guide de l'utilisateur Amazon Simple Storage Service.

> **Important**
>
> Évitez d'inclure des informations sensibles, notamment des numéros de compte, dans le nom du compartiment. Le nom de compartiment est visible dans les URL qui pointent vers les objets du compartiment.

4. Dans Region (Région), choisissez la région AWS dans laquelle le compartiment doit résider. Vous devez sélectionner la région dans laquelle vous utilisez Amazon Fraud Detector, à savoir USA Est (Virginie du Nord), USA Est (Ohio), USA Ouest (Oregon), Europe (Irlande), Asie-Pacifique (Singapour) et Asie-Pacifique (Sydney).
5. Dans Bucket settings for Block Public Acces (Paramètres de compartiment pour Bloquer l'accès public), choisissez les paramètres de blocage de l'accès public que vous souhaitez appliquer au compartiment.

   Nous vous recommandons de laisser tous les paramètres activés. Pour de plus amples informations sur le blocage de l'accès public, veuillez consulter dans le Manuel de l'accès public Amazon S3 dans le Manuel de l'USA Storage Storage Storage Storage Storage Storage Storage Storage Storage Storage Storage Storage Stor
6. Choisissez Create bucket (Créer un compartiment).
7. Téléchargez le fichier de données d'entraînement dans votre compartiment Amazon S3. Notez le chemin de localisation Amazon S3 de votre fichier de formation (par exemple, s3://bucketname/object.csv).

Stockez les données de vos événements en interne avec Amazon Fraud Detector

Vous pouvez choisir de stocker les données relatives aux événements dans Amazon Fraud Detector et de les utiliser ultérieurement pour entraîner vos modèles. En stockant les données relatives aux événements dans Amazon Fraud Detector, vous pouvez entraîner des modèles qui utilisent des variables calculées automatiquement afin d'améliorer les performances, de simplifier la reconversion des modèles et de mettre à jour les étiquettes de fraude afin de boucler la boucle de rétroaction du machine learning. Les événements sont stockés au niveau de la ressource Event Type, de sorte que tous les événements du même type d'événement sont stockés ensemble dans un ensemble de données de type d'événement unique. Dans le cadre de la définition d'un type d'événement, vous pouvez éventuellement spécifier si vous souhaitez stocker les événements pour ce type d'événement en activant le paramètre d'ingestion d'événements dans la console Amazon Fraud Detector.

Vous pouvez stocker des événements uniques ou importer un grand nombre d'ensembles de données d'événements dans Amazon Fraud Detector. Des événements individuels peuvent être diffusés à l'aide de l'GetEventPredictionAPI ou de l'SendEventAPI. Les grands ensembles de données peuvent être importés rapidement et facilement dans Amazon Fraud Detector à l'aide de la fonctionnalité d'importation par lots de la console Amazon Fraud Detector ou à l'aide de l'CreateBatchImportJobAPI.

Vous pouvez utiliser la console Amazon Fraud Detector à tout moment pour vérifier le nombre d'événements déjà enregistrés pour chaque type d'événement.

Préparer les données d'événements pour le stockage

Les données d'événements stockées en interne avec Amazon Fraud Detector sont stockées au niveau`Event Type` des ressources. Ainsi, toutes les données d'événement provenant du même événement sont stockées dans un seul événement`Event Type`. Les événements stockés peuvent ensuite être utilisés pour entraîner un nouveau modèle ou réentraîner un modèle existant. Lorsque vous entraînez un modèle à l'aide des données d'événements stockées, vous pouvez éventuellement spécifier une plage temporelle d'événements afin de limiter la taille de votre jeu de données d'entraînement.

Chaque fois que vous stockez vos données dans Amazon Fraud Detector, à l'aide de la console Amazon Fraud Detector, de l'`SendEvent`API ou de l'`CreateBatchImportJob`API, Amazon Fraud Detector valide vos données avant de les stocker. Si la validation de vos données échoue, les données de l'événement ne sont pas stockées.

Conditions requises pour stocker des données en interne avec Amazon Fraud Detector

- Pour vous assurer que les données de vos événements passent la validation et que l'ensemble de données est correctement stocké, assurez-vous d'avoir utilisé les informations fournies par l'explorateur de modèles de données pour préparer votre ensemble de données.
- Vous avez créé un type d'événement pour les données d'événement que vous souhaitez stocker avec Amazon Fraud Detector. Si ce n'est pas le cas, suivez les instructions pour créer un type d'événement.

Validation intelligente

Lorsque vous chargez votre ensemble de données dans la console Amazon Fraud Detector pour l'importer par lots, Amazon Fraud Detector utilise la validation intelligente des données (SDV) pour valider votre ensemble de données avant de les importer. SDV analyse le fichier de données chargé et identifie les problèmes tels que les données manquantes, le format ou les types de données incorrects. Outre la validation de votre ensemble de données, SDV fournit également un rapport de validation qui répertorie tous les problèmes identifiés et suggère des actions pour résoudre les problèmes les plus importants. Certains des problèmes identifiés par SDV peuvent être critiques et doivent être résolus avant qu'Amazon Fraud Detector puisse importer correctement votre jeu de données. Pour plus d'informations, veuillez consulter Rapport de validation des données intelligentes.

Le SDV valide votre ensemble de données au niveau du fichier et au niveau des données (lignes). Au niveau du fichier, SDV analyse votre fichier de données et identifie les problèmes tels que des autorisations d'accès inadéquates, une taille de fichier, un format de fichier et des en-têtes (métadonnées d'événements et variables d'événement) incorrects. Au niveau des données, SDV analyse les données de chaque événement (ligne) et identifie les problèmes tels que le format de données, la longueur des données, le format d'horodatage et les valeurs nulles incorrects.

La validation intelligente des données est actuellement disponible uniquement dans la console Amazon Fraud Detector et la validation est activée par défaut. Si vous ne souhaitez pas qu'Amazon Fraud Detector utilise la validation intelligente des données avant d'importer votre jeu de données, désactivez la validation dans la console Amazon Fraud Detector lorsque vous chargez votre jeu de données.

Validation des données stockées lors de l'utilisation d'API ou d'unAWS SDK

Lorsque vous chargez des événements via l'opération`SendEvent`,`GetEventPrediction`, ou`CreateBatchImportJob` API, Amazon Fraud Detector valide les éléments suivants :

- Le EventIngestion paramètre pour ce type d'événement est ACTIVÉ.
- Les horodatages des événements ne peuvent pas être mis à jour. Un événement avec un ID d'événement répété et un EVENT_TIMESTAMP différent sera traité comme une erreur.
- Les noms et les valeurs des variables correspondent au format attendu. Pour de plus amples informations, consultez Création d'une variable.
- Les variables obligatoires sont renseignées avec une valeur.
- Tous les horodatages des événements ne datent pas de plus de 18 mois et ne sont pas future.

Stockez les données d'événements grâce à l'importation par lots

La fonctionnalité d'importation par lots vous permet de charger rapidement et facilement de grands ensembles de données historiques sur les événements dans Amazon Fraud Detector à l'aide de la console, de l'API ou du SDK AWS. Pour utiliser l'importation par lots, créez un fichier d'entrée au format CSV contenant toutes les données de vos événements, chargez le fichier CSV dans le compartiment Amazon S3 et lancez une tâche d'importation. Amazon Fraud Detector valide d'abord les données en fonction du type d'événement, puis importe automatiquement l'ensemble de données. Une fois les données importées, elles sont prêtes à être utilisées pour entraîner de nouveaux modèles ou pour réentraîner des modèles existants.

Fichiers d'entrée et de sortie

Le fichier CSV d'entrée doit contenir des en-têtes correspondant aux variables définies dans le type d'événement associé, ainsi que quatre variables obligatoires. Pour en savoir plus, consultez Préparer les données d'événements pour le stockage. La taille maximale du fichier de données d'entrée est de 20 gigaoctets (Go), soit environ 50 millions d'événements. Le nombre d'événements varie en fonction de la taille de votre événement. Si la tâche d'importation a réussi, le fichier de sortie est vide. Si l'importation a échoué, le fichier de sortie contient les journaux d'erreurs.

Création d'un fichier CSV

Amazon Fraud Detector importe les données uniquement depuis les fichiers au format CSV (valeurs séparées par des virgules). La première ligne de votre fichier CSV doit contenir des en-têtes de colonne qui correspondent exactement aux variables définies dans le type d'événement associé, ainsi que quatre variables obligatoires : EVENT_ID, EVENT_TIMESTAMP, ENTITY_ID et ENTITY_TYPE. Vous pouvez également éventuellement inclure EVENT_LABEL et LABEL_TIMESTAMP (LABEL_TIMESTAMP est requis si EVENT_LABEL est inclus).

Définir les variables obligatoires

Les variables obligatoires sont considérées comme des métadonnées d'événements et doivent être spécifiées en majuscules. Les métadonnées des événements sont automatiquement incluses pour la formation des modèles. Le tableau suivant répertorie les variables obligatoires, la description de chaque variable et le format requis pour la variable.

Name (Nom)	Description	Prérequis
IDENTIFIANT DE L'ÉVÉNEMENT	Un identifiant pour l'événement. Par exemple, si votre événement est une transaction en ligne, l'EVENT_ID peut être le numéro de référence de transaction qui a été fourni à votre client.	• L'EVENT_ID est requis pour les tâches d'importation par lots. • Il doit être unique pour cet événement. • Il doit représenter des informations pertinentes pour votre entreprise. • Il doit satisfaire au modèle d'expression régulière (par exemple,`^[0-9a-z_-]+$`.) • Nous vous déconseillons d'ajouter un horodatage à l'EVENT_ID. Cela peut entraîner des problèmes lors de la mise à jour de l'événement. Cela est dû au fait que vous devez fournir exactement le même EVENT_ID pour ce faire.
TIMESTAMP DE L'ÉVÉNEMENT	Horodatage de l'événement. L'horodatage doit être conforme à la norme ISO 8601 en UTC.	• Le EVENT_TIMESTAMP est requis pour les tâches d'importation par lots. • Il doit être spécifié dans l'un des formats suivants :

Name (Nom)	Description	Prérequis
		• %YYYY-%mm-%DDT %Hh : %mm : %SSz (norme ISO 8601 en UTC uniquement, sans millisecondes) Exemple : 2019-11-30T 13:01:01 Z • %yyyy/%mm/%dd %hh : %mm : %ss (AM/PM) Exemples : 2019/11/30 13:01:01, ou 2019/11/30 13:01:01 • %mm/%dd/%yyyy %hh : %mm : %ss Exemples : 30/11/201 9 13:01:01, 30/11/2019 13:01:01 • %mm/%dd/%yy %hh : %mm : %ss Exemples : 30/11/19 13:01:01, 30/11/19 13:01:01 • Amazon Fraud Detector part des hypothèses suivantes lors de l'analyse des formats de date/d'horodatage pour les horodatages des événements : • Si vous utilisez la norme ISO 8601, elle doit correspondre exactemen

Name (Nom)	Description	Prérequis
		t à la spécification précédente • Si vous utilisez l'un des autres formats, vous bénéficiez d'une flexibilité supplémentaire : • Pour les mois et les jours, vous pouvez fournir un ou deux chiffres. Par exemple, le 1/12/2019 est une date valide. • Vous n'avez pas besoin d'inclure hh:mm:ss si vous ne les avez pas (vous pouvez simplement indiquer une date). Vous pouvez également fournir un sous-ensemble contenant uniquemen t les heures et les minutes (par exemple, hh:mm). Le simple fait de fournir une heure n'est pas pris en charge. Les milliseco ndes ne sont pas non plus prises en charge. • Si vous fournissez des étiquettes AM/PM, une horloge de 12 heures est supposée. S'il n'y a aucune information AM/

Name (Nom)	Description	Prérequis
		PM, une horloge de 24 heures est supposée. • Vous pouvez utiliser «/» ou « - » comme délimiteurs pour les éléments de date. « : » est supposé pour les éléments d'horodatage.
IDENTITÉ_D'ENTITÉ	Un identifiant pour l'entité qui exécute l'événement.	• ENTITY_ID est requis pour les tâches d'importation par lots • Il doit suivre le modèle d'expression régulière :`^[0-9A-Za-z_.@+-]+$` . • Si l'identifiant de l'entité n'est pas disponible au moment de l'évaluation, spécifiez l'identifiant de l'entité comme inconnu.
TYPE_ENTITÉ	L'entité qui organise l'événement, telle qu'un commerçant ou un client	ENTITY_TYPE est requis pour les tâches d'importation par lots
ÉTIQUETTE DE L'ÉVÉNEMENT	Classifie l'événement comme`fraudulent` ou`legitimate`	EVENT_LABEL est requis si LABEL_TIMESTAMP est inclus
LABEL_TIMESTAMP	Horodatage de la dernière saisie ou mise à jour du libellé de l'événement	• LABEL_TIMESTAMP est obligatoire si EVENT_LABEL est inclus. • Il doit respecter le format d'horodatage.

Téléchargement du fichier CSV sur Amazon S3 pour l'importation par lots

Après avoir créé un fichier CSV avec vos données, chargez-le dans votre compartiment Amazon Simple Storage Service (Amazon S3).

Pour charger les données d'événements dans un compartiment Amazon S3

1. Connectez-vous à la AWS Management Console et ouvrez la console Simple Storage Service (Amazon S3) à la page https://console.aws.amazon.com/s3/.
2. Choisissez Créer un compartiment.

   L'Assistant Create bucket (Créer un compartiment) s'ouvre.
3. Dans Bucket name (Nom du compartiment), saisissez un nom compatible DNS pour votre compartiment.

   Les nom du compartiment doit présenter les caractéristiques suivantes :

   - Il doit être unique sur l'ensemble d'Amazon S3.
   - Il doit comporter entre 3 et 63 caractères.
   - Ne contient pas de majuscules.
   - Il doit commencer par une minuscule ou un chiffre.

   Une fois le compartiment créé, vous ne pouvez pas changer son nom. Pour plus d'informations sur l'attribution de noms de compartiments, veuillez consulter Règles relatives à l'attribution des noms de compartiments dans le Guide de l'utilisateur Amazon Simple Storage Service.

   > **Important**
   >
   > Évitez d'inclure des informations sensibles, notamment des numéros de compte, dans le nom du compartiment. Le nom de compartiment est visible dans les URL qui pointent vers les objets du compartiment.
4. Dans Region (Région), choisissez la région AWS dans laquelle le compartiment doit résider. Vous devez sélectionner la région dans laquelle vous utilisez Amazon Fraud Detector, à savoir USA Est (Virginie du Nord), USA Est (Ohio), USA Ouest (Oregon), Europe (Irlande), Asie-Pacifique (Singapour) et Asie-Pacifique (Sydney).

5. Dans Bucket settings for Block Public Acces (Paramètres de compartiment pour Bloquer l'accès public), choisissez les paramètres de blocage de l'accès public que vous souhaitez appliquer au compartiment.

   Nous vous recommandons de laisser tous les paramètres activés. Pour de plus amples informations sur le blocage de l'accès public, veuillez consulter dans le Manuel de l'accès public Amazon S3 dans le Manuel de l'USA Storage Storage Storage Storage Storage Storage Storage Storage Storage Storage Storage Storage Stor
6. Choisissez Create bucket (Créer un compartiment).
7. Téléchargez le fichier de données d'entraînement dans votre compartiment Amazon S3. Notez le chemin de localisation Amazon S3 de votre fichier de formation (par exemple, s3://bucketname/object.csv).

Importation Batch de données d'événements dans la console Amazon Fraud Detector

Vous pouvez facilement importer un grand nombre de vos ensembles de données d'événements dans la console Amazon Fraud Detector, à l'aide de l'`CreateBatchImportJob`API ou du SDK AWS. Avant de poursuivre, assurez-vous d'avoir suivi les instructions pour préparer votre ensemble de données sous forme de fichier CSV. Assurez-vous d'avoir également chargé le fichier CSV dans un compartiment Amazon S3.

Utilisation de la console Amazon Fraud Detector

Pour importer des données d'événements par lots dans la console

1. Ouvrez la console AWS, connectez-vous à votre compte, puis accédez à Amazon Fraud Detector.
2. Dans le panneau de navigation de gauche, choisissez Events.
3. Choisissez votre type d'événement.
4. Sélectionnez l'onglet Événements enregistrés.
5. Dans le volet Détails des événements stockés, assurez-vous que l'ingestion d'événements est activée.
6. Dans le volet Importer les données des événements, choisissez Nouvelle importation.
7. Sur la page d'importation de nouveaux événements, fournissez les informations suivantes :

   - [Recommandé] Laissez le paramètre Activer la validation intelligente des données pour cet ensemble de données. Il est désormais réglé sur le paramètre par défaut.

- Pour le rôle IAM pour les données, sélectionnez le rôle IAM que vous avez créé pour le compartiment Amazon S3 qui contient le fichier CSV que vous prévoyez d'importer.
- Dans Emplacement des données d'entrée, entrez l'emplacement S3 où se trouve votre fichier CSV.
- Si vous souhaitez spécifier un emplacement distinct pour stocker les résultats de vos importations, cliquez sur le bouton Séparer l'emplacement des données pour les entrées et les résultats et indiquez un emplacement de compartiment Amazon S3 valide.

> **Important**
>
> Assurez-vous que le rôle IAM que vous avez sélectionné dispose d'autorisations de lecture sur votre compartiment Amazon S3 d'entrée et d'autorisations d'écriture sur votre compartiment Amazon S3 de sortie.

8. Sélectionnez Démarrer.
9. La colonne État du volet de données d'importation des événements affiche l'état de votre tâche de validation et d'importation. La bannière en haut fournit une description détaillée de l'état de votre jeu de données au fur et à mesure de la validation, puis de l'importation.
10. Suivez les instructions fournies pourSurveiller la progression de la validation et d'importation des jeux de données.

Surveiller la progression de la validation et d'importation des jeux de données

Si vous utilisez la console Amazon Fraud Detector pour effectuer une tâche d'importation par lots, Amazon Fraud Detector valide par défaut votre ensemble de données avant l'importation. Vous pouvez suivre la progression et l'état des tâches de validation et d'importation sur la page d'importation de nouveaux événements de la console Amazon Fraud Detector. Une bannière en haut de la page fournit une brève description des résultats de validation et de l'état de la tâche d'importation. En fonction des résultats de validation et de l'état de votre tâche d'importation, il se peut que vous deviez prendre des mesures pour garantir la réussite de la validation et de l'importation de votre ensemble de données.

Le tableau suivant fournit des informations détaillées sur les actions que vous devez effectuer en fonction du résultat des opérations de validation et d'importation.

Message de bannière	État	Ce que cela signifie	Que dois-je faire
La validation des données a commencé	Validation en cours	SDV a commencé à valider votre jeu de données	Patientez jusqu'à ce que le statut change
La validation des données ne peut pas avoir lieu en raison d'erreurs dans votre jeu de données. Corrigez les erreurs dans votre fichier de données et lancez une nouvelle tâche d'importation. Consultez le rapport de validation pour plus d'informations	Échec de la validation	SDV a identifié des problèmes dans votre fichier de données. Ces problèmes doivent être résolus pour que l'importation de votre jeu de données soit réussie.	Dans le volet Importer les données des événements, sélectionnez l'ID de Job et consultez le rapport de validation. Suivez les recommandations du rapport pour corriger toutes les erreurs répertoriées. Pour plus d'informations, veuillez consulter Utilisation du rapport de validation.
L'importation des données a commencé. La validation est réussie	Importation en cours	Votre jeu de données a passé la validation. L'AFD a commencé à importer votre jeu de données	Patientez jusqu'à ce que le statut change

Message de bannière	État	Ce que cela signifie	Que dois-je faire
Validation terminée avec avertissements. L'importation de données a commencé	Importation en cours	Certaines données de votre jeu de données n'ont pas été validées. Toutefois, les données qui ont passé la validation répondent aux exigences de taille de données minimales pour l'importation.	Surveillez le message dans la bannière et attendez que le statut change

Message de bannière	État	Ce que cela signifie	Que dois-je faire
Vos données ont été partiellement importées. Certaines données ont échoué à la validation et n'ont pas été importées. Consultez le rapport de validation pour plus d'informations.	Importé. L'état affiche une icône d'avertissement.	Certaines des données de votre fichier de données dont la validation a échoué n'ont pas été importées. Le reste des données validées a été importé.	Dans le volet Importer les données des événements, sélectionnez l'ID de Job et consultez le rapport de validation. Suivez les recommandations du tableau des avertissements au niveau des données pour répondre aux avertissements répertoriés. Il n'est pas nécessaire de répondre à tous les avertissements. Assurez-vous toutefois que plus de 50 % des données de votre jeu de données sont validées pour une importation réussie. Après avoir répondu aux avertissements, lancez une nouvelle tâche d'importation. Pour plus d'informations, veuillez consulter Utilisation du rapport de validation.
L'importation des données a échoué en raison d'une erreur de traitement. Lancer une nouvelle tâche d'importation de données	Échec	L'importation a échoué en raison d'une erreur d'exécution passagère	Commencer une nouvelle tâche d'importation

Message de bannière	État	Ce que cela signifie	Que dois-je faire
Les données ont été importées avec succès	Importé	La validation et l'importation se sont terminées avec succès	Sélectionnez le numéro de Job de votre tâche d'importation pour afficher les détails, puis passez à la formation du modèle.

> **Note**
>
> Nous vous recommandons d'attendre 10 minutes après l'importation réussie de l'ensemble de données dans Amazon Fraud Detector pour vous assurer qu'il est entièrement ingéré par le système.

Rapport de validation des données intelligentes

La validation intelligente des données crée un rapport de validation une fois la validation terminée. Le rapport de validation fournit des détails sur tous les problèmes identifiés par le SDV dans votre ensemble de données, avec des suggestions d'actions pour résoudre les problèmes les plus importants. Vous pouvez utiliser le rapport de validation pour déterminer quels sont les problèmes, leur localisation dans l'ensemble de données, leur gravité et la manière de les résoudre. Le rapport de validation est créé même lorsque la validation est réussie. Dans ce cas, vous pouvez consulter le rapport pour voir si des problèmes sont répertoriés et, le cas échéant, décider si vous souhaitez les résoudre.

> **Note**
>
> La version actuelle de SDV analyse votre jeu de données à la recherche de problèmes susceptibles d'entraîner l'échec de l'importation par lots. Si la validation et l'importation par lots aboutissent, votre jeu de données peut toujours présenter des problèmes susceptibles d'entraîner l'échec de l'entraînement du modèle. Nous vous recommandons de consulter votre rapport de validation même si la validation et l'importation se sont déroulées avec succès, et de résoudre tous les problèmes répertoriés dans le rapport pour réussir la

formation des modèles. Après avoir résolu les problèmes, créez une nouvelle tâche d'importation par lots.

Accès au rapport de validation

Vous pouvez accéder au rapport de validation à tout moment une fois la validation terminée à l'aide de l'une des options suivantes :

1. Une fois la validation terminée et pendant que la tâche d'importation est en cours, dans la bannière supérieure, choisissez Afficher le rapport de validation.
2. Une fois la Job importation terminée, dans le volet de données des événements d'importation, choisissez l'ID de la tâche d'importation qui vient de se terminer.

Utilisation du rapport de validation

La page du rapport de validation de votre tâche d'importation fournit les détails de cette tâche d'importation, une liste des erreurs critiques, le cas échéant, une liste d'avertissements concernant des événements spécifiques (lignes) dans votre jeu de données, le cas échéant, et un bref résumé de votre ensemble de données qui inclut des informations telles que des valeurs non valides et des valeurs manquantes pour chaque variable.

- Importer les détails de la tâche

  Fournit des détails sur la tâche d'importation. Si votre tâche d'importation a échoué ou si votre jeu de données a été partiellement importé, choisissez Accéder au fichier de résultats pour consulter les journaux d'erreurs des événements qui n'ont pas pu être importés.
- Erreurs critiques

  Fournit des informations détaillées sur les problèmes les plus importants de votre ensemble de données identifiés par SDV. Tous les problèmes répertoriés dans ce volet sont critiques et vous devez les résoudre avant de procéder à l'importation. Si vous essayez d'importer votre jeu de données sans résoudre les problèmes critiques, votre tâche d'importation risque d'échouer.

  Pour résoudre les problèmes critiques, suivez les recommandations fournies pour chaque avertissement. Après avoir résolu tous les problèmes répertoriés dans le volet Erreurs critiques, créez une nouvelle tâche d'importation par lots.
- Avertissements relatifs au niveau des données

Fournit un résumé des avertissements relatifs à des événements spécifiques (lignes) de votre ensemble de données. Si le volet Avertissements au niveau des données est renseigné, certains événements de votre jeu de données n'ont pas été validés et n'ont pas été importés.

Pour chaque avertissement, la colonne Description affiche le nombre d'événements à l'origine du problème. Et les exemples d'ID d'événements fournissent une liste partielle d'exemples d'ID d'événements que vous pouvez utiliser comme point de départ pour localiser les autres événements présentant le problème. Utilisez la recommandation fournie pour l'avertissement pour résoudre le problème. Utilisez également les journaux d'erreurs de votre fichier de sortie pour obtenir des informations supplémentaires sur le problème. Les journaux d'erreurs sont générés pour tous les événements qui ont échoué à l'importation par lots. Pour accéder aux journaux d'erreurs, dans le volet Importer les détails de la tâche, sélectionnez Accéder au fichier de résultats.

> **Note**
>
> Si plus de 50 % des événements (lignes) de votre jeu de données n'ont pas été validés, la tâche d'importation échoue également. Dans ce cas, vous devez corriger les données avant de commencer une nouvelle tâche d'importation.

- Résumé du jeu de données

  Fournit un résumé du rapport de validation de votre ensemble de données. Si la colonne Nombre d'avertissements contient plus de 0 avertissements, décidez si vous devez corriger ces avertissements. Si la colonne Nombre d'avertissements indique 0, continuez à entraîner votre modèle.

Importation Batch des données d'événements à l'aide du kit AWS SDK for Python (Boto3)

L'exemple suivant montre un exemple de demande d'CreateBatchImportJobAPI. Une tâche d'importation par lots doit inclure un JobID, un InputPath, un OutputPath eventTypeNameet iamRoleArn. Le JobID ne peut pas contenir le même ID que celui d'une tâche précédente, sauf si la tâche existe dans l'état CREATE_FAILED. Les chemins InputPath et OutputPath doivent être des chemins S3 valides. Vous pouvez choisir de ne pas spécifier le nom du fichier dans OutputPath, mais vous devrez toujours fournir un emplacement de compartiment S3 valide. Le eventTypeName et

iamRoleArn doit exister. Le rôle IAM doit accorder des autorisations de lecture pour entrer dans le compartiment Amazon S3 et des autorisations d'écriture pour sortir le compartiment Amazon S3.

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

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

Annuler la tâche d'importation par lots

Vous pouvez annuler une tâche d'importation par lots en cours à tout moment dans la console Amazon Fraud Detector, à l'aide de l'`CancelBatchImportJob`API ou du SDK AWS.

Pour annuler une tâche d'importation par lots dans la console,

1. Ouvrez la console AWS, connectez-vous à votre compte, puis accédez à Amazon Fraud Detector.
2. Dans le panneau de navigation de gauche, choisissez Events.
3. Choisissez votre type d'événement.
4. Sélectionnez l'onglet Événements enregistrés.
5. Dans le volet Importer les données des événements, choisissez l'ID d'une tâche d'importation en cours que vous souhaitez annuler.
6. Sur la page de la tâche événementielle, cliquez sur Actions et sélectionnez Annuler l'importation d'événements.
7. Choisissez Arrêter l'importation des événements pour annuler la tâche d'importation par lots.

Annulation d'une tâche d'importation par lots à l'aide du kit AWS SDK for Python (Boto3)

L'exemple suivant montre un exemple de demande pour l'`CancelBatchImportJob`API. La tâche d'annulation de l'importation doit inclure l'identifiant d'une tâche d'importation par lots en cours.

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

Stocker les données d'événements à l'aide de GetEventPredictions l'opération API

Par défaut, tous les événements envoyés à l'`GetEventPrediction`API pour évaluation sont stockés dans Amazon Fraud Detector. Cela signifie qu'Amazon Fraud Detector enregistre automatiquement les données relatives aux événements lorsque vous générez une prédiction et utilise ces données pour mettre à jour les variables calculées en temps quasi réel. Vous pouvez désactiver le stockage des données en accédant au type d'événement dans la console Amazon Fraud Detector et en réglant l'ingestion d'événements sur OFF ou en mettant à jour la EventIngestion valeur sur DISABLED à l'aide de l'opération`PutEventType` API. Pour plus d'informations sur le fonctionnement de l'`GetEventPrediction`API, consultezPrédictions de fraude.

> **Important**
>
> Nous vous recommandons vivement de la maintenir activée une fois que vous avez activé l'ingestion d'événements pour un type d'événement. La désactivation de l'ingestion d'événements pour le même type d'événement, puis la génération de prédictions, peuvent entraîner un comportement incohérent.

Stocker les données d'événements à l'aide de SendEvent l'opération API

Vous pouvez utiliser l'opération d'`SendEvent`API pour stocker des événements dans Amazon Fraud Detector sans générer de prévisions de fraude pour ces événements. Par exemple, vous pouvez utiliser l'`SendEvent`opération pour télécharger un jeu de données historique, que vous pourrez ensuite utiliser pour entraîner un modèle.

Formats d'horodatage des événements pour SendEvent l'API

Lorsque vous stockez des données d'événements à l'aide de l'`SendEvent`API, vous devez vous assurer que l'horodatage de votre événement est au format requis. Amazon Fraud Detector prend en charge les formats de date et d'horodatage suivants :

- %YYYY-%mm-%DDT%Hh : %mm : %SSz (norme ISO 8601 en UTC uniquement, sans millisecondes)

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

  Exemples : 2019/11/30 13:01:01, ou 2019/11/30 13:01:01
- %mm/%dd/%yyyy %hh : %mm : %ss

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

  Exemples : 30/11/19 13:01:01, 30/11/19 13:01:01

Amazon Fraud Detector part des hypothèses suivantes lors de l'analyse des formats de date/d'horodatage pour les horodatages des événements :

- Si vous utilisez la norme ISO 8601, elle doit correspondre exactement à la spécification précédente
- Si vous utilisez l'un des autres formats, vous bénéficiez d'une flexibilité supplémentaire :
  - Pour les mois et les jours, vous pouvez fournir un ou deux chiffres. Par exemple, le 1/12/2019 est une date valide.
  - Vous n'avez pas besoin d'inclure hh:mm:ss si vous ne les avez pas (vous pouvez simplement indiquer une date). Vous pouvez également fournir un sous-ensemble contenant uniquement les heures et les minutes (par exemple, hh:mm). Le simple fait de fournir une heure n'est pas pris en charge. Les millisecondes ne sont pas non plus prises en charge.
  - Si vous fournissez des étiquettes AM/PM, une horloge de 12 heures est supposée. S'il n'y a aucune information AM/PM, une horloge de 24 heures est supposée.
  - Vous pouvez utiliser «/» ou « - » comme délimiteurs pour les éléments de date. « : » est supposé pour les éléments d'horodatage.

Voici un exemple d'appel`SendEvent` d'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'}],

)
```

Obtenir les détails des données d'un événement stockées

Après avoir enregistré les données d'un événement dans Amazon Fraud Detector, vous pouvez vérifier les dernières données stockées pour un événement à l'aide de l'GetEventAPI. L'exemple de code suivant vérifie les dernières données stockées pour l'`sample_registration`événement.

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

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

Afficher les mesures du jeu de données d'événements stocké

Pour chaque type d'événement, vous pouvez consulter des indicateurs tels que le nombre d'événements stockés, la taille totale de vos événements stockés et l'horodatage des événements enregistrés les plus anciens et les plus récents, dans la console Amazon Fraud Detector.

Pour afficher les statistiques d'événements stockées d'un type d'événement,

1. Ouvrez laAWS console et connectez-vous à votre compte. Accédez à Amazon Fraud Detector.
2. Dans le panneau de navigation de gauche, choisissez Events.
3. Choisissez votre type d'événement.
4. Sélectionnez l'onglet Événements enregistrés.
5. Le volet Détails des événements stockés affiche les mesures. Ces statistiques sont automatiquement mises à jour une fois par jour.
6. Cliquez éventuellement sur Actualiser les statistiques des événements pour mettre à jour manuellement vos statistiques.

> **Note**
>
> Si vous venez d'importer vos données, nous vous recommandons d'attendre 5 à 10 minutes après avoir fini d'importer les données pour actualiser et consulter les statistiques.

Orchestration d'événements

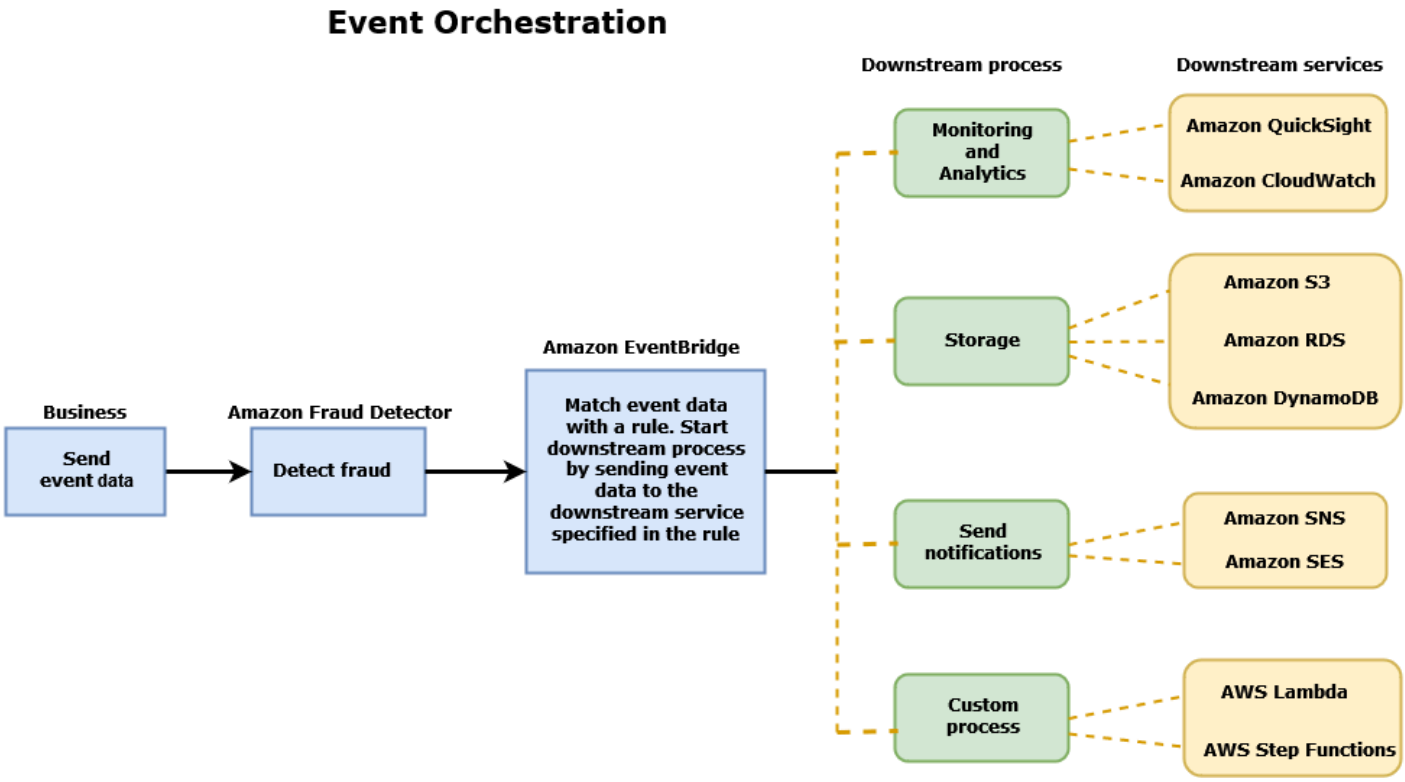
L'orchestration d'événements vous permet d'envoyer facilement des événements à des Services AWS fins de traitement en aval, à l'aide d'Amazon EventBridge. Amazon Fraud Detector vous fournit des règles simples que vous pouvez utiliser pour automatiser le traitement des événements après la détection d'une fraude. Grâce à l'orchestration des événements, vous pouvez automatiser les processus liés aux événements en aval, tels que l'envoi d'événements vers des tableaux de bord pour obtenir des informations à partir des données d'événements, la génération de notifications basées sur les résultats de la détection des fraudes et la mise à jour des événements avec une étiquette basée sur les enseignements tirés de la détection des fraudes.

L'orchestration d'événements permet d'accéder facilement aux services de l'AWSenvironnement via Amazon EventBridge. Vous pouvez configurer Amazon EventBridge pour envoyer des événements directement Services AWS ou indirectement à l'aide de destinations d'API. Les outils Services AWS que vous utilisez pour orchestrer vos processus en aval sont également appelés cibles. Certaines des cibles que vous pouvez utiliser pour orchestrer le traitement en aval sont les suivantes :

- Pour la surveillance et l'analyse — Amazon QuickSight, Amazon CloudWatch
- Pour le stockage : Amazon S3, Amazon RDS, Amazon DynamoDB
- Pour envoyer des notifications — Amazon SNS, Amazon SES
- Pour un traitement personnalisé — AWS Lambda, AWS Step Functions

Pour plus d'informations sur les cibles d'orchestration prises en charge par Amazon EventBridge, consultez la section Amazon EventBridge targets.

Le schéma suivant fournit une vue d'ensemble du fonctionnement de l'orchestration d'événements.



Configuration de l'orchestration des événements

Pour configurer l'orchestration des événements pour vos événements, vous devez configurer des processus dans votre service cible, configurer Amazon EventBridge pour recevoir et envoyer des données d'événements, et créer des règles dans Amazon EventBridge qui spécifient les conditions de démarrage des processus en aval. Procédez comme suit pour configurer l'orchestration des événements :

Pour configurer l'orchestration des événements

1. Consultez le guide de EventBridge l'utilisateur Amazon et découvrez comment utiliser Amazon EventBridge. Assurez-vous de savoir comment créer des règles dans Amazon EventBridge pour votre cas d'utilisation.
2. Suivez les instructions pourActivez l'orchestration des événements dans Amazon Fraud Detector.

> **Note**
>
> L'orchestration des événements de votre événement est désactivée par défaut.

3. Configurez votre service cible pour recevoir et traiter les données de l'événement. Par exemple, si votre processus en aval implique l'envoi de notifications et que vous souhaitez utiliser Amazon SNS, accédez à la console Amazon SNS, créez une rubrique SNS, puis abonnez un point de terminaison à cette rubrique.
4. Suivez les instructions pour créer des EventBridge règles Amazon.

> **Important**
>
> Lorsque vous créez le modèle d'événement dans Amazon EventBridge, assurez-vous `aws.frauddetector` de fournir le champ source et le champ `Event Prediction Result Returned` de type détaillé.

Activez l'orchestration des événements dans Amazon Fraud Detector

Vous pouvez activer l'orchestration d'événements pour un événement soit lorsque vous créez votre type d'événement, soit après avoir créé votre type d'événement. L'orchestration des événements peut être activée dans la console Amazon Fraud Detector à l'aide de la `put-event-type` commande, de l'`PutEventType`API ou duAWS SDK for Python (Boto3).

Activez l'orchestration des événements dans la console Amazon Fraud Detector

Cet exemple active l'orchestration d'événements pour un type d'événement déjà créé. Si vous créez un nouveau type d'événement et souhaitez activer l'orchestration, suivez les instructions pourCréation d'un type d'événement.

Pour activer l'orchestration des événements

1. Ouvrez la console AWS de gestion et connectez-vous à votre compte. Accédez à Amazon Fraud Detector.
2. Dans le volet de navigation de gauche, sélectionnez Events.
3. Sur la page Type d'événement, choisissez votre type d'événement.
4. Activez Activer l'orchestration des événements avec Amazon EventBridge.

5. Continuez avec les instructions de l'étape 3 pourConfiguration de l'orchestration des événements.

Activez l'orchestration d'événements à l'aide du AWS SDK for Python (Boto3)

L'exemple suivant montre un exemple de demande de mise à jour d'un type d'événement afin de `sample_registration` permettre l'orchestration des événements. L'exemple utilise l'`PutEventType`API et suppose que vous avez créé les variables `ip_address``email_address`, les étiquettes `legit` et `fraud` le type d'entité`sample_customer`. Pour plus d'informations sur la création de ces ressources, consultez la section Ressources.

```
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'])
```

Désactiver l'orchestration des événements dans Amazon Fraud Detector

Vous pouvez désactiver l'orchestration d'événements pour un événement à tout moment dans la console Amazon Fraud Detector, à l'aide de la `put-event-type` commande, de l'`PutEventType`API ou duAWS SDK for Python (Boto3).

Désactiver l'orchestration des événements dans la console Amazon Fraud Detector

Pour désactiver l'orchestration des événements

1. Ouvrez la console AWS de gestion et connectez-vous à votre compte. Accédez à Amazon Fraud Detector.
2. Dans le volet de navigation de gauche, sélectionnez Events.

3. Sur la page Type d'événement, choisissez votre type d'événement.
4. Désactivez Activer l'orchestration des événements avec Amazon EventBridge.

Désactivez l'orchestration d'événements à l'aide du AWS SDK for Python (Boto3)

L'exemple suivant montre un exemple de demande de mise à jour d'un type d'événement `sample_registration` afin de désactiver l'orchestration d'événements à l'aide de l'`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'])
```

Modèle

Amazon Fraud Detector utilise des modèles d'apprentissage automatique pour générer des prédictions de fraude. Chaque modèle est entraîné à l'aide d'un type de modèle. Le type de modèle spécifie les algorithmes et les transformations utilisés pour l'entraînement du modèle. L'entraînement des modèles consiste à utiliser un ensemble de données que vous fournissez pour créer un modèle capable de prédire les événements frauduleux.

Pour créer un modèle, vous devez d'abord choisir un type de modèle, puis préparer et fournir les données qui seront utilisées pour entraîner le modèle.

Choisissez un type de modèle

Les types de modèles suivants sont disponibles dans Amazon Fraud Detector. Choisissez un type de modèle adapté à votre cas d'utilisation.

- Informations sur la fraude en ligne

  Le type de modèle Online Fraud Insights est optimisé pour détecter les fraudes lorsque peu de données historiques sont disponibles sur l'entité évaluée, par exemple lorsqu'un nouveau client s'enregistre en ligne pour un nouveau compte.
- Informations sur les fraudes transactionnelles

  Le type de modèle Transaction Fraud Insights est le mieux adapté pour détecter les cas d'utilisation frauduleuse dans lesquels l'entité évaluée peut avoir un historique d'interactions que le modèle peut analyser pour améliorer la précision des prédictions (par exemple, un client existant ayant un historique d'achats antérieurs).
- Informations sur le rachat de comptes

  Le modèle Account Takeover Insights détecte si un compte a été compromis par hameçonnage ou par un autre type d'attaque. Les données de connexion d'un compte compromis, telles que le navigateur et l'appareil utilisés lors de la connexion, sont différentes des données de connexion historiques associées au compte.

Informations sur la fraude en ligne

Online Fraud Insights est un modèle d'apprentissage automatique supervisé, ce qui signifie qu'il utilise des exemples historiques de transactions frauduleuses et légitimes pour entraîner le modèle. Le modèle Online Fraud Insights permet de détecter les fraudes sur la base de peu de données historiques. Les entrées du modèle sont flexibles, vous pouvez donc l'adapter pour détecter divers risques de fraude, notamment les faux avis, les abus de promotion et les fraudes liées au paiement des clients.

Le modèle Online Fraud Insights utilise un ensemble d'algorithmes d'apprentissage automatique pour l'enrichissement, la transformation et la classification des fraudes des données. Dans le cadre du processus de formation modèle, Online Fraud Insights enrichit les éléments de données brutes tels que l'adresse IP et le numéro BIN avec des données tierces telles que la géolocalisation de l'adresse IP ou la banque émettrice d'une carte de crédit. Outre les données de tiers, Online Fraud Insights utilise des algorithmes d'apprentissage en profondeur qui prennent en compte les modèles de fraude observés sur Amazon etAWS. Ces modèles de fraude deviennent des éléments d'entrée de votre modèle à l'aide d'un algorithme de renforcement de l'arborescence des dégradés.

Pour améliorer les performances, Online Fraud Insights optimise les hyperparamètres de l'algorithme de renforcement de l'arbre à gradient via un processus d'optimisation bayésien. Il entraîne de manière séquentielle des dizaines de modèles différents avec différents paramètres de modèle (tels que le nombre d'arbres, la profondeur des arbres et le nombre d'échantillons par feuille). Il utilise également différentes stratégies d'optimisation, telles que la surpondération de la population minoritaire de fraudeurs afin de réduire les taux de fraude.

Sélection de la source de données

Lorsque vous entraînez un modèle Online Fraud Insights, vous pouvez choisir d'entraîner le modèle sur des données d'événements stockées en externe (en dehors d'Amazon Fraud Detector) ou stockées dans Amazon Fraud Detector. Le stockage externe actuellement pris en charge par Amazon Fraud Detector est Amazon Simple Storage Service (Amazon S3). Si vous utilisez un stockage externe, votre ensemble de données d'événements doit être chargé au format CSV (valeurs séparées par des virgules) dans un compartiment Amazon S3. Dans la configuration d'apprentissage du modèle, ces options de stockage de données sont appelées EXTERNAL_EVENTS (pour le stockage externe) et INGESTED_EVENTS (pour le stockage interne). Pour plus d'informations sur les sources de données disponibles et sur la manière d'y stocker des données, consultezStockage des données des événements.

Préparation des données

Quel que soit l'endroit où vous choisissez de stocker les données de vos événements (Amazon S3 ou Amazon Fraud Detector), les exigences relatives au type de modèle Online Fraud Insights sont les mêmes.

Votre ensemble de données doit contenir l'en-tête de colonne EVENT_LABEL. Cette variable classe un événement comme frauduleux ou légitime. Lorsque vous utilisez un fichier CSV (stockage externe), vous devez inclure EVENT_LABEL pour chaque événement du fichier. Pour le stockage interne, le champ EVENT_LABEL est facultatif, mais tous les événements doivent être étiquetés pour être inclus dans un ensemble de données d'entraînement. Lorsque vous configurez votre modèle d'entraînement, vous pouvez choisir d'ignorer les événements non étiquetés, d'utiliser une étiquette légitime pour les événements non étiquetés ou d'utiliser une étiquette frauduleuse pour tous les événements non étiquetés.

Sélection de données

Consultez la section Collecter des données sur les événements pour obtenir des informations sur la sélection des données pour la formation de votre modèle Online Fraud Insights.

Le processus de formation Online Fraud Insights échantillonne et partitionne les données historiques en fonction d'EVENT_TIMESTAMP. Il n'est pas nécessaire d'échantillonner les données manuellement, ce qui peut avoir un impact négatif sur les résultats de votre modèle.

Variables d'événement

Le modèle Online Fraud Insights nécessite au moins deux variables, outre les métadonnées d'événement requises, qui ont passé avec succès la validation des données pour l'entraînement du modèle et autorisent jusqu'à 100 variables par modèle. En général, plus vous fournissez de variables, mieux le modèle peut différencier la fraude des événements légitimes. Bien que le modèle Online Fraud Insights puisse prendre en charge des dizaines de variables, y compris des variables personnalisées, nous recommandons d'inclure l'adresse IP et l'adresse e-mail, car ces variables sont généralement les plus efficaces pour identifier l'entité évaluée.

Validation des données

Dans le cadre du processus de formation, Online Fraud Insights validera l'ensemble de données pour détecter les problèmes de qualité des données susceptibles d'avoir une incidence sur la formation des modèles. Après avoir validé les données, Amazon Fraud Detector prendra les mesures appropriées pour créer le meilleur modèle possible. Cela inclut l'émission d'avertissements en

cas de problèmes potentiels de qualité des données, la suppression automatique des variables présentant des problèmes de qualité des données ou l'émission d'une erreur et l'arrêt du processus d'apprentissage du modèle. Pour plus d'informations, consultez la section Validation du jeu de données.

Informations sur les fraudes transactionnelles

Le modèle Transaction Fraud Insights est conçu pour détecter les fraudes en ligne ou card-not-present les fraudes transactionnelles. Transaction Fraud Insights est un modèle d'apprentissage automatique supervisé, ce qui signifie qu'il utilise des exemples historiques de transactions frauduleuses et légitimes pour entraîner le modèle.

Le modèle Transaction Fraud Insights utilise un ensemble d'algorithmes d'apprentissage automatique pour l'enrichissement, la transformation et la classification des fraudes des données. Il utilise un moteur d'ingénierie des fonctionnalités pour créer des agrégats au niveau de l'entité et au niveau des événements. Dans le cadre du processus de formation modèle, Transaction Fraud Insights enrichit les éléments de données brutes tels que l'adresse IP et le numéro BIN avec des données tierces telles que la géolocalisation de l'adresse IP ou la banque émettrice d'une carte de crédit. Outre les données tierces, Transaction Fraud Insights utilise des algorithmes d'apprentissage en profondeur qui prennent en compte les modèles de fraude observés sur Amazon. AWS Ces modèles de fraude deviennent des éléments d'entrée de votre modèle à l'aide d'un algorithme de renforcement de l'arborescence des dégradés.

Pour améliorer les performances, Transaction Fraud Insights optimise les hyperparamètres de l'algorithme de renforcement de l'arbre à gradient via un processus d'optimisation bayésien, en formant séquentiellement des dizaines de modèles différents avec différents paramètres de modèle (tels que le nombre d'arbres, la profondeur des arbres, le nombre d'échantillons par feuille) ainsi que différentes stratégies d'optimisation, telles que la surpondération de la population de fraudeurs minoritaire pour réduire les taux de fraude.

Dans le cadre du processus de formation du modèle, le moteur d'ingénierie des fonctionnalités du modèle de fraude transactionnelle calcule des valeurs pour chaque entité unique de votre ensemble de données de formation afin d'améliorer les prévisions de fraude. Par exemple, pendant le processus de formation, Amazon Fraud Detector calcule et enregistre la date du dernier achat effectué par une entité et met à jour cette valeur de manière dynamique chaque fois que vous appelez l'`SendEvent`API `GetEventPrediction` or. Lors d'une prédiction de fraude, les variables d'événement sont combinées avec d'autres métadonnées d'entités et d'événements pour prédire si la transaction est frauduleuse.

Sélection de la source de données

Les modèles Transaction Fraud Insights sont entraînés uniquement sur un ensemble de données stocké en interne avec Amazon Fraud Detector (INGESTED_EVENTS). Cela permet à Amazon Fraud Detector de mettre à jour en permanence les valeurs calculées concernant les entités que vous évaluez. Pour plus d'informations sur les sources de données disponibles, voir Stockage des données des événements

Préparation des données

Avant de former un modèle Transaction Fraud Insights, assurez-vous que votre fichier de données contient tous les en-têtes, comme indiqué dans Préparation du jeu de données d'événements. Le modèle Transaction Fraud Insights compare les nouvelles entités reçues aux exemples d'entités frauduleuses et légitimes figurant dans l'ensemble de données. Il est donc utile de fournir de nombreux exemples pour chaque entité.

Amazon Fraud Detector transforme automatiquement le jeu de données d'événements enregistré dans le format approprié pour la formation. Une fois l'entraînement du modèle terminé, vous pouvez consulter les indicateurs de performance et déterminer si vous devez ajouter des entités à votre jeu de données d'entraînement.

Sélection de données

Par défaut, Transaction Fraud Insights s'entraîne sur l'intégralité de votre ensemble de données stocké pour le type d'événement que vous sélectionnez. Vous pouvez éventuellement définir une plage de temps afin de réduire le nombre d'événements utilisés pour entraîner votre modèle. Lorsque vous définissez une plage de temps, assurez-vous que les enregistrements utilisés pour entraîner le modèle ont eu suffisamment de temps pour arriver à maturité. En d'autres termes, suffisamment de temps s'est écoulé pour garantir que les dossiers légitimes et frauduleux ont été correctement identifiés. Par exemple, dans le cas d'une fraude liée à la rétrofacturation, il faut souvent 60 jours ou plus pour identifier correctement les événements frauduleux. Pour optimiser les performances du modèle, assurez-vous que tous les enregistrements de votre jeu de données d'entraînement sont matures.

Il n'est pas nécessaire de sélectionner un intervalle de temps qui représente un taux de fraude idéal. Amazon Fraud Detector échantillonne automatiquement vos données pour trouver un équilibre entre les taux de fraude, la période et le nombre d'entités.

Amazon Fraud Detector renvoie une erreur de validation lors de l'entraînement du modèle si vous sélectionnez une plage de temps pendant laquelle il n'y a pas suffisamment d'événements

pour entraîner un modèle avec succès. Pour les ensembles de données stockés, le champ EVENT_LABEL est facultatif, mais les événements doivent être étiquetés pour être inclus dans votre ensemble de données d'entraînement. Lorsque vous configurez votre modèle d'entraînement, vous pouvez choisir d'ignorer les événements non étiquetés, d'utiliser une étiquette légitime pour les événements non étiquetés ou d'utiliser une étiquette frauduleuse pour les événements non étiquetés.

Variables d'événement

Le type d'événement utilisé pour entraîner le modèle doit contenir au moins 2 variables, outre les métadonnées d'événement requises, qui ont passé avec succès la validation des données et peuvent contenir jusqu'à 100 variables. En général, plus vous fournissez de variables, mieux le modèle peut différencier la fraude des événements légitimes. Bien que le modèle Transaction Fraud Insight puisse prendre en charge des dizaines de variables, y compris des variables personnalisées, nous vous recommandons d'inclure l'adresse IP, l'adresse e-mail, le type d'instrument de paiement, le prix de la commande et le BIN de la carte.

Validation des données

Dans le cadre du processus de formation, Transaction Fraud Insights valide l'ensemble de données de formation pour détecter les problèmes de qualité des données susceptibles d'avoir une incidence sur la formation des modèles. Après avoir validé les données, Amazon Fraud Detector prend les mesures appropriées pour créer le meilleur modèle possible. Cela inclut l'émission d'avertissements en cas de problèmes potentiels de qualité des données, la suppression automatique des variables présentant des problèmes de qualité des données ou l'émission d'une erreur et l'arrêt du processus d'apprentissage du modèle. Pour plus d'informations, consultez la section Validation du jeu de données.

Amazon Fraud Detector émettra un avertissement mais continuera à entraîner un modèle si le nombre d'entités uniques est inférieur à 1 500, car cela peut avoir un impact sur la qualité des données de formation. Si vous recevez un avertissement, passez en revue l'indicateur de performance.

Informations sur le rachat de comptes

Le type de modèle Account Takeover Insights (ATI) identifie les activités frauduleuses en ligne en détectant si les comptes ont été compromis par des prises de contrôle malveillantes, par hameçonnage ou par le vol d'informations d'identification. Account Takeover Insights est un modèle d'apprentissage automatique qui utilise les événements de connexion de votre entreprise en ligne pour entraîner le modèle.

Vous pouvez intégrer un modèle Account Takeover Insights expérimenté dans votre flux de connexion en temps réel afin de détecter si un compte est compromis. Le modèle évalue différents types d'authentification et de connexion. Ils incluent les connexions aux applications Web, les authentifications basées sur les API et single-sign-on (SSO). Pour utiliser le modèle Account Takeover Insights, appelez l'GetEventPredictionAPI après avoir présenté des informations de connexion valides. L'API génère un score qui quantifie le risque de compromission du compte. Amazon Fraud Detector utilise le score et les règles que vous avez définis pour renvoyer un ou plusieurs résultats pour les événements de connexion. Les résultats sont ceux que vous avez configurés. En fonction des résultats que vous recevez, vous pouvez prendre les mesures appropriées pour chaque connexion. En d'autres termes, vous pouvez approuver ou contester les informations d'identification présentées pour la connexion. Par exemple, vous pouvez contester les informations d'identification en demandant un code PIN de compte à titre de vérification supplémentaire.

Vous pouvez également utiliser le modèle Account Takeover Insights pour évaluer les connexions aux comptes de manière asynchrone et prendre des mesures sur les comptes à haut risque. Par exemple, un compte à haut risque peut être ajouté à la file d'attente d'investigation pour qu'un réviseur humain puisse déterminer si d'autres mesures doivent être prises, telles que la suspension du compte.

Le modèle Account Takeover Insights est formé à l'aide d'un ensemble de données contenant l'historique des événements de connexion de votre entreprise. Vous fournissez ces données. Vous pouvez éventuellement étiqueter les comptes comme légitimes ou frauduleux. Cependant, cela n'est pas nécessaire pour entraîner le modèle. Le modèle Account Takeover Insights détecte les anomalies sur la base de l'historique des connexions réussies à un compte. Il apprend également à détecter les anomalies dans le comportement d'un utilisateur qui suggèrent un risque accru de prise de contrôle de compte par un acte malveillant. Par exemple, un utilisateur qui se connecte généralement à partir du même ensemble d'appareils et d'adresses IP. Un fraudeur se connecte généralement à partir d'un autre appareil et d'une autre géolocalisation. Cette technique produit un score de risque indiquant qu'une activité est anormale, ce qui est généralement l'une des principales caractéristiques des prises de contrôle de comptes par des personnes malveillantes.

Avant de former un modèle Account Takeover Insights, Amazon Fraud Detector utilise une combinaison de techniques d'apprentissage automatique pour enrichir, agréger et transformer les données. Ensuite, pendant le processus de formation, Amazon Fraud Detector enrichit les éléments de données brutes que vous fournissez. Les exemples d'éléments de données brutes incluent l'adresse IP et l'agent utilisateur. Amazon Fraud Detector utilise ces éléments pour créer des entrées supplémentaires décrivant les données de connexion. Ces entrées incluent l'appareil, le navigateur et

les entrées de géolocalisation. Amazon Fraud Detector utilise également les données de connexion que vous fournissez pour calculer en continu des variables agrégées décrivant le comportement passé des utilisateurs. Parmi les exemples de comportement des utilisateurs, citons le nombre de fois où l'utilisateur s'est connecté à partir d'une adresse IP spécifique. Grâce à ces enrichissements et agrégats supplémentaires, Amazon Fraud Detector peut générer de solides performances de modèle à partir d'un petit nombre d'entrées issues de vos événements de connexion.

Le modèle Account Takeover Insights détecte les cas où un mauvais acteur accède à un compte légitime, qu'il s'agisse d'un humain ou d'un robot. Le modèle produit un score unique qui indique le risque relatif de compromission du compte. Les comptes susceptibles d'avoir été compromis sont signalés comme des comptes à haut risque. Vous pouvez traiter les comptes à haut risque de deux manières. Vous pouvez soit imposer une vérification d'identité supplémentaire. Vous pouvez également envoyer le compte dans une file d'attente pour un examen manuel.

Sélection de la source de données

Les modèles Account Takeover Insights sont formés sur un ensemble de données stocké en interne, dans Amazon Fraud Detector. Pour stocker les données de vos événements de connexion avec Amazon Fraud Detector, créez un fichier CSV contenant les événements de connexion des utilisateurs. Pour chaque événement, incluez des données de connexion telles que l'horodatage de l'événement, l'ID utilisateur, l'adresse IP, l'agent utilisateur et indiquez si les données de connexion sont valides. Après avoir créé le fichier CSV, téléchargez-le d'abord sur Amazon Fraud Detector, puis utilisez la fonction d'importation pour stocker les données. Vous pouvez ensuite entraîner votre modèle à l'aide des données enregistrées. Pour plus d'informations sur le stockage de votre ensemble de données d'événements avec Amazon Fraud Detector, consultez Stockez les données de vos événements en interne avec Amazon Fraud Detector

Préparation des données

Amazon Fraud Detector exige que vous fournissiez les données de connexion de votre compte utilisateur dans un fichier de valeurs séparées par des virgules (CSV) codé au format UTF-8. La première ligne de votre fichier CSV doit contenir un en-tête de fichier. L'en-tête du fichier comprend des métadonnées d'événement et des variables d'événement qui décrivent chaque élément de données. Les données de l'événement suivent l'en-tête. Chaque ligne des données d'événement comprend les données d'un seul événement de connexion.

Pour le modèle Accounts Takeover Insights, vous devez fournir les métadonnées et variables d'événement suivantes dans la ligne d'en-tête de votre fichier CSV.

Métadonnées de l'événement

Nous vous recommandons de fournir les métadonnées suivantes dans l'en-tête de votre fichier CSV. Les métadonnées de l'événement doivent être en majuscules.

- EVENT_ID - Identifiant unique pour l'événement de connexion.
- ENTITY_TYPE - Entité qui exécute l'événement de connexion, telle qu'un commerçant ou un client.
- ENTITY_ID - Identifiant de l'entité effectuant l'événement de connexion.
- EVENT_TIMESTAMP - L'horodatage auquel l'événement de connexion s'est produit. L'horodatage doit être conforme à la norme ISO 8601 en UTC.
- EVENT_LABEL (recommandé) : étiquette qui classe l'événement comme frauduleux ou légitime. Vous pouvez utiliser n'importe quelle étiquette, telle que « fraude », « légitime », « 1 » ou « 0 ».

> **Note**
>
> - Les métadonnées des événements doivent être en majuscules. Cela fait la distinction majuscules et minuscules.
> - Les étiquettes ne sont pas obligatoires pour les événements de connexion. Cependant, nous vous recommandons d'inclure les métadonnées EVENT_LABEL et de fournir des étiquettes pour vos événements de connexion. Ce n'est pas grave si les étiquettes sont incomplètes ou sporadiques. Si vous fournissez des étiquettes, Amazon Fraud Detector les utilisera pour calculer automatiquement le taux de découverte d'un compte et l'affichera dans le graphique et le tableau des performances du modèle.

Variables d'événement

Pour le modèle Accounts Takeover Insights, vous devez fournir des variables obligatoires (obligatoires) et des variables facultatives. Lorsque vous créez vos variables, assurez-vous de les affecter au bon type de variable. Dans le cadre du processus de formation du modèle, Amazon Fraud Detector utilise le type de variable associé à la variable pour effectuer l'enrichissement des variables et l'ingénierie des fonctionnalités.

> **Note**
>
> Les noms des variables d'événement doivent être en minuscules. Ils font la distinction majuscules et minuscules.

Variables obligatoires

Les variables suivantes sont requises pour former un modèle Accounts Takeover Insights.

Catégorie	Type de variable	Description
Adresse IP	IP_ADDRESS	Adresse IP utilisée lors de l'événement de connexion
Navigateur et appareil	AGENT UTILISATEUR	Le navigateur, l'appareil et le système d'exploitation utilisés lors de l'événement de connexion
Informations d'identification valides	VALIDCRED	Indique si les informations d'identification utilisées pour la connexion sont valides

Variables facultatives

Les variables suivantes sont facultatives pour la formation d'un modèle Accounts Takeover Insights.

Catégorie	Type	Description
Navigateur et appareil	EMPREINTE DIGITALE	L'identifiant unique pour l'empreinte digitale d'un navigateur ou d'un appareil
Identifiant de session	SESSION_ID	Identifiant d'une session d'authentification

Catégorie	Type	Description
Étiquette	ÉTIQUETTE D'ÉVÉNEMENT	Une étiquette qui classe l'événement comme frauduleux ou légitime. Vous pouvez utiliser n'importe quelle étiquette, telle que « fraude », « légitime », « 1 » ou « 0 ».
Horodatage	LABEL_TIMESTAMP	Horodatage de la dernière mise à jour de l'étiquette. Cela est obligatoire si EVENT_LABEL est fourni.

> **Note**
>
> - Vous pouvez fournir n'importe quel nom de variable pour les deux variables obligatoires (variables facultatives). Il est important que chaque variable obligatoire et facultative soit affectée au type de variable approprié.
> - Vous pouvez fournir des variables supplémentaires. Cependant, Amazon Fraud Detector n'inclura pas ces variables pour la formation d'un modèle Accounts Takeover Insights.

Sélection de données

La collecte de données est une étape importante de la création de votre modèle Account Takeover Insights. Lorsque vous commencez à collecter vos données de connexion, tenez compte des exigences et recommandations suivantes :

Obligatoire

- Fournissez au moins 1 500 exemples de comptes utilisateur, chacun étant associé à au moins deux événements de connexion.
- Votre jeu de données doit couvrir au moins 30 jours d'événements de connexion. Vous pouvez ultérieurement spécifier la plage de temps spécifique des événements à utiliser pour entraîner le modèle.

Recommandée

- Votre jeu de données inclut des exemples d'événements de connexion infructueux. Vous pouvez éventuellement étiqueter ces connexions infructueuses comme « frauduleuses » ou « légitimes ».
- Préparez des données historiques avec des événements de connexion s'étalant sur plus de six mois et incluant 100 000 entités.

Si vous ne disposez pas d'un ensemble de données répondant déjà aux exigences minimales, envisagez de diffuser les données d'événements vers Amazon Fraud Detector en appelant l'opération SendEventAPI.

Validation des données

Avant de créer votre modèle Account Takeover Insights, Amazon Fraud Detector vérifie si les métadonnées et les variables que vous avez incluses dans votre ensemble de données pour entraîner le modèle répondent aux exigences de taille et de format. Pour plus d'informations, consultez Validation des données. Il vérifie également les autres exigences. Si le jeu de données ne passe pas la validation, le modèle n'est pas créé. Pour que le modèle soit correctement créé, assurez-vous de corriger les données qui n'ont pas été validées avant de vous entraîner à nouveau.

Erreurs courantes dans les ensembles de données

Lors de la validation d'un ensemble de données pour la formation d'un modèle Account Takeover Insights, Amazon Fraud Detector analyse ces problèmes et d'autres et génère une erreur s'il rencontre un ou plusieurs de ces problèmes.

- Le fichier CSV n'est pas au format UTF-8.
- L'en-tête du fichier CSV ne contient pas au moins l'une des métadonnées suivantes : `EVENT_IDENTITY_ID`, ou`EVENT_TIMESTAMP`.
- L'en-tête du fichier CSV ne contient pas au moins une variable des types de variables suivants : `IP_ADDRESSUSERAGENT`, ou`VALIDCRED`.
- Plusieurs variables sont associées au même type de variable.
- Plus de 0,1 % des valeurs `EVENT_TIMESTAMP` contiennent des valeurs nulles ou autres que les formats de date et d'horodatage pris en charge.
- Le nombre de jours entre le premier et le dernier événement est inférieur à 30 jours.
- Plus de 10 % des `IP_ADDRESS` variables de ce type ne sont pas valides ou sont nulles.
- Plus de 50 % des variables de ce `USERAGENT` type contiennent des valeurs nulles.

- Toutes les variables du type de `VALIDCRED` variable sont définies sur`false`.

Créer un modèle

Les modèles Amazon Fraud Detector apprennent à détecter les fraudes liées à un type d'événement spécifique. Dans Amazon Fraud Detector, vous devez d'abord créer un modèle, qui sert de conteneur pour les versions de votre modèle. Chaque fois que vous entraînez un modèle, une nouvelle version est créée. Pour plus de détails sur la création et l'entraînement d'un modèle à l'aide de la AWS console, reportez-vous àÉtape 3 : créer le modèle.

Chaque modèle possède une variable de score correspondante. Amazon Fraud Detector crée cette variable en votre nom lorsque vous créez un modèle. Vous pouvez utiliser cette variable dans vos expressions de règles pour interpréter les scores de votre modèle lors d'une évaluation de fraude.

Entraînez et déployez un modèle à l'aide du AWS SDK for Python (Boto3)

Une version du modèle est créée en appelant les `CreateModelVersion` opérations `CreateModel` et. `CreateModel`lance le modèle, qui agit comme un conteneur pour les versions de votre modèle. `CreateModelVersion`lance le processus de formation, qui aboutit à une version spécifique du modèle. Une nouvelle version de la solution est créée chaque fois que vous appelez `CreateModelVersion`.

L'exemple suivant montre un exemple de demande pour l'`CreateModel`API. Cet exemple crée le type de modèle Online Fraud Insights et suppose que vous avez créé un type d'événement`sample_registration`. Pour plus de détails sur la création d'un type d'événement, consultezCréation d'un type d'événement.

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

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

Entraînez votre première version à l'aide de l'CreateModelVersionAPI. Pour `TrainingDataSource` et `ExternalEventsDetail` spécifiez la source et l'emplacement Amazon S3 de l'ensemble de données d'entraînement. Pour cela, `TrainingDataSchema` spécifiez la manière dont

Amazon Fraud Detector doit interpréter les données d'entraînement, en particulier les variables d'événement à inclure et la manière de classer les étiquettes des événements. Par défaut, Amazon Fraud Detector ignore les événements non étiquetés. Cet exemple de code utilise `AUTO` for `unlabeledEventsTreatment` pour spécifier qu'Amazon Fraud Detector décide comment utiliser les événements non étiquetés.

```
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'
}
)
```

Une demande réussie donnera lieu à une nouvelle version du modèle avec statut`TRAINING_IN_PROGRESS`. À tout moment pendant la formation, vous pouvez annuler la formation en appelant `UpdateModelVersionStatus` et en mettant à jour le statut sur`TRAINING_CANCELLED`. Une fois la formation terminée, le statut de la version du modèle passe à`TRAINING_COMPLETE`. Vous pouvez consulter les performances du modèle à l'aide de la console Amazon Fraud Detector ou en appelant`DescribeModelVersions`. Pour plus d'informations sur la façon d'interpréter les scores et les performances des modèles, reportez-vous Scores du modèle aux sections etIndicateurs de performance du modèle.

Après avoir examiné les performances du modèle, activez-le pour que les détecteurs puissent l'utiliser dans le cadre de prévisions de fraude en temps réel. Amazon Fraud Detector déploiera le modèle dans plusieurs zones de disponibilité à des fins de redondance, l'auto-scaling étant

activé pour garantir que le modèle évolue en fonction du nombre de prédictions de fraude que vous effectuez. Pour activer le modèle, appelez l'`UpdateModelVersionStatus`API et mettez à jour le statut sur`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'
)
```

Scores du modèle

Amazon Fraud Detector génère les scores des modèles différemment selon les types de modèles.

Pour les modèles Account Takeover Insights (ATI), Amazon Fraud Detector utilise uniquement une valeur agrégée (une valeur calculée en combinant un ensemble de variables brutes) pour générer le score du modèle. Un score de -1 est généré pour le premier événement d'une nouvelle entité, indiquant un risque inconnu. En effet, pour une nouvelle entité, les valeurs utilisées pour calculer l'agrégat seront nulles ou nulles. Le modèle Account Takeeover Insights (ATI) génère des scores compris entre 0 et 1 000 pour tous les événements ultérieurs pour la même entité et pour les entités existantes, où 0 indique un faible risque de fraude et 1 000 un risque de fraude élevé. Pour les modèles ATI, les scores du modèle sont directement liés au taux de défi (CR). Par exemple, un score de 500 correspond à un taux de défi estimé à 5 %, tandis qu'un score de 900 correspond à un taux de défi estimé à 0,1 %.

Pour les modèles Online Fraud Insights (OFI) et Transaction Fraud Insights (TFI), Amazon Fraud Detector utilise à la fois une valeur agrégée (une valeur calculée en combinant un ensemble de variables brutes) et une valeur brute (la valeur fournie pour la variable) pour générer les scores du modèle. Les scores du modèle peuvent être compris entre 0 et 1 000, 0 indiquant un faible risque de fraude et 1 000 un risque de fraude élevé. Pour les modèles OFI et TFI, les scores du modèle sont directement liés au taux de faux positifs (FPR). Par exemple, un score de 600 correspond à un taux de faux positifs estimé à 10 %, tandis qu'un score de 900 correspond à un taux de faux positifs estimé à 2 %. Le tableau suivant fournit des détails sur la corrélation entre les scores de certains modèles et les taux de faux positifs estimés.

Note du modèle	FPR estimé
975	0,50 %
950	1 %
900	2 %
860	3 %
775	5 %
700	7 %
600	10 %

Indicateurs de performance du modèle

Une fois la formation du modèle terminée, Amazon Fraud Detector valide les performances du modèle en utilisant 15 % de vos données qui n'ont pas été utilisées pour entraîner le modèle. Vous pouvez vous attendre à ce que votre modèle Amazon Fraud Detector entraîné présente des performances de détection des fraudes réelles similaires aux indicateurs de performance de validation.

En tant qu'entreprise, vous devez trouver un équilibre entre la détection d'un plus grand nombre de fraudes et l'augmentation des tensions pour les clients légitimes. Pour vous aider à trouver le bon équilibre, Amazon Fraud Detector fournit les outils suivants pour évaluer les performances du modèle :

- Tableau de distribution des scores : un histogramme des distributions de scores du modèle suppose un exemple de population de 100 000 événements. L'axe Y de gauche représente les événements légitimes et l'axe Y de droite représente les événements de fraude. Vous pouvez sélectionner un seuil de modèle spécifique en cliquant sur la zone du graphique. Cela mettra à jour les vues correspondantes dans la matrice de confusion et le graphique ROC.
- Matrice de confusion — Résume la précision du modèle pour un seuil de score donné en comparant les prévisions du modèle aux résultats réels. Amazon Fraud Detector part d'une population d'exemple de 100 000 événements. La diffusion de fraudes et d'événements légitimes simule le taux de fraude dans vos entreprises.

  - Les vrais points positifs — Le modèle prédit la fraude et l'événement est en fait une fraude.
  - Faux positifs : le modèle prédit la fraude, mais l'événement est en fait légitime.
  - Les vrais points négatifs — Le modèle prédit la légitimité de l'événement, alors qu'il est en fait légitime.
  - Faux points négatifs — Le modèle prédit des événements légitimes, mais il s'agit en fait d'une fraude.
  - Taux positif réel (TPR) : pourcentage du total des fraudes détectées par le modèle. Également connu sous le nom de taux de capture.
  - Taux de faux positifs (FPR) : pourcentage du total des événements légitimes qui sont faussement considérés comme des fraudes.
- Courbe du récepteur et de l'opérateur (ROC) : trace le taux de vrais positifs en fonction du taux de faux positifs sur tous les seuils de score possibles du modèle. Consultez ce graphique en choisissant Advanced Metrics.
- Zone sous la courbe (AUC) — Résume le TPR et le FPR sur tous les seuils de score possibles du modèle. Un modèle sans pouvoir prédictif a une AUC de 0,5, alors qu'un modèle parfait a un score de 1,0.
- Plage d'incertitude — Elle indique la plage d'AUC attendue du modèle. Une plage plus grande (différence entre les bornes supérieure et inférieure de l'AUC > 0,1) signifie une plus grande incertitude du modèle. Si la plage d'incertitude est large (>0,1), envisagez de fournir davantage d'événements étiquetés et réentraînez le modèle.

Pour utiliser les indicateurs de performance du modèle

1. Commencez par le tableau de distribution des scores pour examiner la distribution des scores des modèles pour vos fraudes et vos événements légitimes. Idéalement, vous aurez une distinction claire entre la fraude et les événements légitimes. Cela indique que le modèle peut identifier avec précision les événements frauduleux et ceux qui sont légitimes. Sélectionnez un seuil de modèle en cliquant sur la zone du graphique. Vous pouvez voir l'impact de l'ajustement du seuil de score du modèle sur vos taux de vrais positifs et de faux positifs.

> **Note**
>
> Le tableau de distribution des scores trace les fraudes et les événements légitimes sur deux axes Y différents. L'axe Y de gauche représente les événements légitimes et l'axe Y de droite représente les événements de fraude.

2. Consultez la matrice de confusion. En fonction du seuil de score du modèle que vous avez sélectionné, vous pouvez voir l'impact simulé sur la base d'un échantillon de 100 000 événements. La diffusion de fraudes et d'événements légitimes simule le taux de fraude dans vos entreprises. Utilisez ces informations pour trouver le juste équilibre entre le taux de vrais positifs et le taux de faux positifs.
3. Pour plus de détails, choisissez Advanced Metrics. Utilisez le graphique ROC pour comprendre la relation entre le taux de vrais positifs et le taux de faux positifs pour n'importe quel seuil de score du modèle. La courbe ROC peut vous aider à affiner le compromis entre un taux de vrais positifs et un taux de faux positifs.

> **Note**
>
> Vous pouvez également consulter les métriques sous forme de tableau en choisissant Tableau.
> La vue du tableau montre également la métrique Precision. La précision est le pourcentage d'événements de fraude correctement prédits comme frauduleux par rapport à tous les événements prédits comme frauduleux.

4. Utilisez les indicateurs de performance pour déterminer les seuils de modèle optimaux pour vos entreprises en fonction de vos objectifs et de votre cas d'utilisation en matière de détection des fraudes. Par exemple, si vous envisagez d'utiliser le modèle pour classer les nouveaux enregistrements de comptes comme présentant un risque élevé, moyen ou faible, vous devez identifier deux seuils afin de pouvoir rédiger les trois conditions de règle suivantes :

   - Les scores > X indiquent un risque élevé
   - Les scores < X but > Y correspondent à un risque moyen
   - Les scores < Y indiquent un faible risque

Importance des variables du modèle

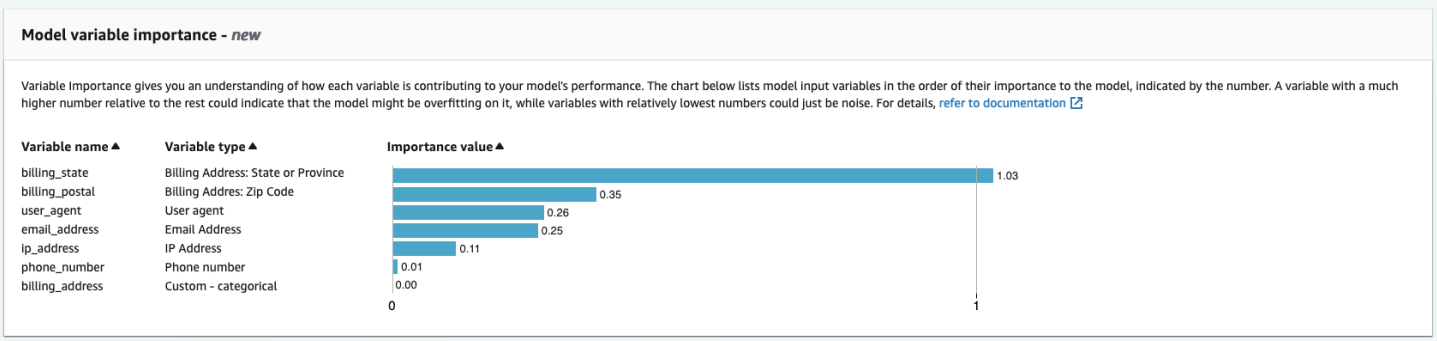
L'importance des variables du modèle est une fonctionnalité d'Amazon Fraud Detector qui classe les variables du modèle au sein d'une version du modèle. Chaque variable de modèle reçoit une valeur basée sur son importance relative par rapport aux performances globales de votre modèle. La variable de modèle ayant la valeur la plus élevée est plus importante pour le modèle que les autres variables de modèle du jeu de données pour cette version du modèle et est répertoriée en haut par défaut. De même, la variable de modèle présentant la valeur la plus faible est répertoriée en bas par défaut et est la moins importante par rapport aux autres variables du modèle. À l'aide des valeurs d'importance des variables du modèle, vous pouvez avoir un aperçu des entrées qui déterminent les performances de votre modèle.

Vous pouvez consulter les valeurs d'importance des variables du modèle pour votre version de modèle entraînée dans la console Amazon Fraud Detector ou à l'aide de l'DescribeModelVersionAPI.

L'importance des variables du modèle fournit l'ensemble de valeurs suivant pour chaque variable utilisée pour entraîner la version du modèle.

- Type de variable : type de variable (par exemple, adresse IP ou e-mail). Pour plus d'informations, consultez Types de variables. Pour les modèles Account Takeover Insights (ATI), Amazon Fraud Detector fournit une valeur d'importance variable pour le type de variable brut et agrégé. Les types de variables bruts sont affectés aux variables que vous fournissez. Le type de variable agrégée est attribué à un ensemble de variables brutes qu'Amazon Fraud Detector a combinées pour calculer une valeur d'importance agrégée.
- Nom de la variable : nom de la variable d'événement utilisée pour entraîner la version du modèle (par exemple`ip_address`,`email_address`,`are_creadentials_valid`). Pour le type de variable agrégée, les noms de toutes les variables utilisées pour calculer la valeur d'importance de la variable agrégée sont répertoriés.
- Valeur d'importance de la variable : nombre qui représente l'importance relative de la variable brute ou agrégée par rapport aux performances du modèle. Plage typique : 0 à 10

Dans la console Amazon Fraud Detector, les valeurs d'importance des variables du modèle sont affichées comme suit pour un modèle Online Fraud Insights (OFI) ou Transaction Fraud Insights (TFI). Un modèle ATI (Account Takeover Insight) fournira des valeurs d'importance des variables agrégées en plus des valeurs d'importance des variables brutes. Le graphique visuel permet de voir facilement l'importance relative entre les variables, la ligne pointillée verticale faisant référence à la valeur d'importance de la variable la mieux classée.



Amazon Fraud Detector génère des valeurs d'importance variables pour chaque version du modèle Fraud Detector, sans frais supplémentaires.

> **Important**
>
> Les versions du modèle créées avant le 9 juillet 2021 n'ont pas de valeurs d'importance variables. Vous devez entraîner une nouvelle version de votre modèle pour générer les valeurs d'importance des variables du modèle.

Utilisation des valeurs d'importance des variables du modèle

Vous pouvez utiliser les valeurs d'importance des variables du modèle pour avoir un aperçu de ce qui fait augmenter ou diminuer les performances de votre modèle et des variables qui y contribuent le plus. Ensuite, modifiez votre modèle pour améliorer les performances globales.

Plus précisément, pour améliorer les performances de votre modèle, examinez les valeurs d'importance des variables par rapport à vos connaissances du domaine et corrigez les problèmes liés aux données d'entraînement. Par exemple, si l'identifiant de compte a été utilisé comme entrée dans le modèle et qu'il est répertorié en haut, examinez sa valeur d'importance variable. Si la valeur d'importance de la variable est nettement supérieure aux autres valeurs, votre modèle est peut-être trop adapté à un modèle de fraude spécifique (par exemple, tous les événements de fraude proviennent du même identifiant de compte). Cependant, il se peut également qu'il y ait une fuite d'étiquette si la variable dépend des étiquettes frauduleuses. Selon le résultat de votre analyse basée sur vos connaissances du domaine, vous souhaiterez peut-être supprimer la variable et vous entraîner avec un ensemble de données plus diversifié, ou conserver le modèle tel quel.

De même, jetez un œil aux variables classées en dernier. Si la valeur d'importance de la variable est nettement inférieure aux autres valeurs, cette variable du modèle peut ne pas avoir d'importance

dans l'entraînement de votre modèle. Vous pouvez envisager de supprimer la variable pour entraîner une version de modèle plus simple. Si votre modèle comporte peu de variables, par exemple deux variables seulement, Amazon Fraud Detector fournit toujours les valeurs d'importance des variables et classe les variables. Cependant, les informations disponibles dans ce cas seront limitées.

⚠ Important

1. Si vous remarquez l'absence de variables dans le tableau d'importance des variables du modèle, cela peut être dû à l'une des raisons suivantes. Pensez à modifier la variable dans votre jeu de données et à réentraîner votre modèle.
   - Le nombre de valeurs uniques pour la variable dans le jeu de données d'apprentissage est inférieur à 100.
   - Plus de 0,9 % des valeurs de la variable sont absentes de l'ensemble de données d'apprentissage.
2. Vous devez entraîner une nouvelle version du modèle chaque fois que vous souhaitez ajuster les variables d'entrée de votre modèle.

Évaluation des valeurs d'importance des variables du modèle

Nous vous recommandons de prendre en compte les points suivants lorsque vous évaluez les valeurs d'importance des variables du modèle :

- Les valeurs d'importance des variables doivent toujours être évaluées en combinaison avec les connaissances du domaine.
- Examinez la valeur d'importance d'une variable par rapport à la valeur d'importance variable des autres variables dans la version du modèle. Ne considérez pas la valeur d'importance d'une variable pour une seule variable indépendamment.
- Comparez les valeurs d'importance des variables au sein de la même version du modèle. Ne comparez pas les valeurs d'importance des mêmes variables entre les versions du modèle, car la valeur d'importance d'une variable dans une version de modèle peut être différente de la valeur de la même variable dans une version de modèle différente. Si vous utilisez les mêmes variables et le même jeu de données pour entraîner différentes versions du modèle, cela ne génère pas nécessairement les mêmes valeurs d'importance des variables.

Affichage du classement par importance des variables du modèle

Une fois la formation du modèle terminée, vous pouvez consulter le classement par importance des variables du modèle de votre version entraînée dans la console Amazon Fraud Detector ou en utilisant l'DescribeModelVersionAPI.

Pour consulter le classement d'importance des variables du modèle à l'aide de la console,

1. Ouvrez la AWS console et connectez-vous à votre compte. Accédez à Amazon Fraud Detector.
2. Dans le volet de navigation de gauche, choisissez Models (Modèles).
3. Choisissez votre modèle, puis la version de votre modèle.
4. Assurez-vous que l'onglet Aperçu est sélectionné.
5. Faites défiler la page vers le bas pour afficher le volet Importance des variables du modèle.

Comprendre comment la valeur d'importance de la variable du modèle est calculée

À la fin de la formation sur chaque version de modèle, Amazon Fraud Detector génère automatiquement des valeurs d'importance des variables du modèle et des indicateurs de performance du modèle. Pour cela, Amazon Fraud Detector utilise Shapley Additive Explanations (SHAP). Le SHAP est essentiellement la contribution moyenne attendue d'une variable de modèle une fois que toutes les combinaisons possibles de toutes les variables du modèle ont été prises en compte.

SHAP affecte d'abord la contribution de chaque variable du modèle pour la prédiction d'un événement. Il agrège ensuite ces prédictions pour créer un classement des variables au niveau du modèle. Pour attribuer les contributions de chaque variable de modèle à une prédiction, SHAP prend en compte les différences entre les sorties du modèle parmi toutes les combinaisons de variables possibles. En incluant toutes les possibilités d'inclusion ou de suppression d'un ensemble spécifique de variables pour générer une sortie de modèle, SHAP peut accéder avec précision à l'importance de chaque variable de modèle. Cela est particulièrement important lorsque les variables du modèle sont fortement corrélées entre elles.

Dans la plupart des cas, les modèles ML ne vous permettent pas de supprimer des variables. Vous pouvez à la place remplacer une variable supprimée ou manquante dans le modèle par les valeurs de variable correspondantes issues d'une ou de plusieurs lignes de base (par exemple, des

événements non liés à une fraude). Choisir des instances de référence appropriées peut s'avérer difficile, mais Amazon Fraud Detector vous facilite la tâche en définissant cette base de référence comme la moyenne de la population pour vous.

Importer un SageMaker modèle

Vous pouvez éventuellement importer des modèles SageMaker hébergés dans Amazon Fraud Detector. Tout comme les modèles, SageMaker les modèles peuvent être ajoutés aux détecteurs et générer des prédictions de fraude à l'aide de l'`GetEventPrediction`API. Dans le cadre de la `GetEventPrediction` demande, Amazon Fraud Detector invoquera votre SageMaker terminal et transmettra les résultats à vos règles.

Vous pouvez configurer Amazon Fraud Detector pour utiliser les variables d'événement envoyées dans le cadre de la `GetEventPrediction` demande. Si vous choisissez d'utiliser des variables d'événement, vous devez fournir un modèle de saisie. Amazon Fraud Detector utilisera ce modèle pour transformer vos variables d'événement en la charge utile d'entrée requise pour appeler le SageMaker point de terminaison. Vous pouvez également configurer votre SageMaker modèle pour utiliser un ByteBuffer envoyé dans le cadre de la `GetEventPrediction` demande.

Amazon Fraud Detector prend en charge l'importation d' SageMaker algorithmes utilisant les formats d'entrée JSON ou CSV et les formats de sortie JSON ou CSV. Parmi les SageMaker algorithmes pris en charge, citons XGBoost, Linear Learner et Random Cut Forest.

Importez un SageMaker modèle à l'aide du AWS SDK for Python (Boto3)

Pour importer un SageMaker modèle, utilisez l'`PutExternalModel`API. L'exemple suivant suppose que le SageMaker point de terminaison `sagemaker-transaction-model` a été déployé, qu'il est en `InService` état et qu'il utilise l'algorithme XGBoost.

La configuration d'entrée indique qui utilisera les variables d'événement pour construire l'entrée du modèle (`useEventVariables`définie sur`TRUE`). Le format d'entrée est TEXT_CSV, étant donné que XGBoost nécessite une entrée CSV. csvInputTemplate Spécifie comment construire l'entrée CSV à partir des variables envoyées dans le cadre de la `GetEventPrediction` demande. Cet exemple suppose que vous avez créé les variables `order_amt`prev_amt, `hist_amt` et`payment_type`.

La configuration de sortie spécifie le format de réponse du SageMaker modèle et associe l'index CSV approprié à la variable Amazon Fraud Detector`sagemaker_output_score`. Une fois configurée, vous pouvez utiliser la variable de sortie dans les règles.

> **Note**
>
> La sortie d'un SageMaker modèle doit être mappée à une variable avec sourceEXTERNAL_MODEL_SCORE. Vous ne pouvez pas créer ces variables dans la console à l'aide de variables. Vous devez plutôt les créer lorsque vous configurez l'importation de votre modèle.

```
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'
)
```

Suppression d'un modèle ou d'une version de modèle

Vous pouvez supprimer des modèles et des versions de modèles dans Amazon Fraud Detector, à condition qu'ils ne soient pas associés à une version de détecteur. Lorsque vous supprimez un modèle, Amazon Fraud Detector supprime définitivement ce modèle et les données ne sont plus stockées dans Amazon Fraud Detector.

Vous pouvez également supprimer SageMaker des modèles Amazon s'ils ne sont pas associés à une version de détecteur. La suppression d'un SageMaker modèle le déconnecte d'Amazon Fraud Detector, mais le modèle reste disponible dans SageMaker.

Suppression d'une version de modèle

Vous ne pouvez supprimer que les versions du modèle dont le`Ready to deploy` statut est indiqué. Pour modifier le`Ready to deploy` statut d'une version`ACTIVE` de modèle, annulez le déploiement de la version du modèle.

1. Connectez-vous àAWS Management Console et ouvrez la console Amazon Fraud Detector à l'adresse https://console.aws.amazon.com/frauddetector.
2. Dans le panneau de navigation gauche de la console Amazon Fraud Detector, choisissez Models.
3. Choisissez le modèle qui contient la version de modèle que vous voulez supprimer.
4. Choisissez la version de modèle que vous voulez supprimer.
5. Choisissez Actions, puis Delete (Supprimer).
6. Entrez le nom de la version du modèle, puis choisissez Supprimer la version du modèle.

Pour annuler le déploiement d'une version de modèle

Vous ne pouvez pas annuler le déploiement d'une version de modèle utilisée par n'importe quelle version de détecteur (`ACTIVE`,`INACTIVE`,`DRAFT`). Par conséquent, pour annuler le déploiement d'une version de modèle utilisée par une version de détecteur, supprimez d'abord la version du modèle de la version de détecteur.

1. Dans le panneau de navigation gauche de la console Amazon Fraud Detector, choisissez Models.
2. Choisissez le modèle qui contient la version du modèle que vous souhaitez annuler le déploiement.
3. Choisissez la version de modèle que vous voulez supprimer.
4. Choisissez Actions, puis choisissez Annuler le déploiement de la version du modèle.

Suppression d'un modèle

Avant de supprimer un modèle, vous devez d'abord supprimer toutes les versions de modèle et toutes les versions associées au modèle.

1. Dans le panneau de navigation gauche de la console Amazon Fraud Detector, choisissez Models.
2. Choisissez le modèle que vous voulez supprimer.
3. Choisissez Actions, puis Delete (Supprimer).
4. Entrez le nom du modèle, puis choisissez Supprimer le modèle.

Pour supprimer un SageMaker modèle Amazon

1. Dans le panneau de navigation gauche de la console Amazon Fraud Detector, choisissez Models.
2. Choisissez le SageMaker modèle que vous voulez supprimer.
3. Choisissez Actions, puis choisissez Supprimer le modèle.
4. Entrez le nom du modèle, puis choisissez Supprimer le SageMaker modèle.

Détecteur

Un détecteur est un conteneur qui contient une logique de détection des fraudes, telle que les modèles et les règles, pour un événement commercial spécifique que vous souhaitez évaluer pour détecter une fraude. Vous créez d'abord un détecteur en spécifiant l'événement que vous avez déjà défini et vous pouvez éventuellement ajouter une version du modèle qui a déjà été créée et entraînée par Amazon Fraud Detector pour l'événement.

Vous ajoutez ensuite des règles et un ordre d'exécution des règles à un détecteur pour créer une version du détecteur. Une version du détecteur définit les règles et éventuellement un modèle qui sera exécuté dans le cadre de la demande de génération de prévisions de fraude. Vous pouvez ajouter n'importe laquelle des règles définies dans un détecteur à la version du détecteur. Vous pouvez également ajouter n'importe quel modèle entraîné sur le type d'événement évalué à la version du détecteur. Un détecteur peut avoir plusieurs versions, chaque version ayant des règles et un ordre d'exécution des règles différents pour répondre à de multiples cas d'utilisation.

Chaque version du détecteur doit avoir un statut de`DRAFT`,`ACTIVE`, ou`INACTIVE`. Il ne peut y avoir qu'une seule version de détecteur`ACTIVE`statut à la fois. Amazon Fraud Detector utilise la version du détecteur avec`ACTIVE`statut pour générer des prévisions de fraude.

Création d'un détecteur

Vous créez un détecteur en spécifiant le type d'événement que vous avez déjà défini. Vous pouvez éventuellement ajouter un modèle déjà entraîné et déployé par Amazon Fraud Detector. Si vous ajoutez un modèle, vous pouvez utiliser le score du modèle généré par Amazon Fraud Detector dans l'expression de votre règle lors de la création d'une règle (par exemple,`$model score < 90`).

Vous pouvez créer un détecteur dans la console Amazon Fraud Detector en utilisantPutDetectorAPI, à l'aide dudétecteur de putcommande, ou à l'aide deAWSSDK. Si vous utilisez une API, une commande ou un SDK pour créer un détecteur, suivez les instructions pourCréation d'une version du détecteur.

Créez un détecteur dans la console Amazon Fraud Detector

Cet exemple suppose que vous avez créé un type d'événement et que vous avez également créé et déployé une version du modèle que vous souhaitez utiliser pour la prévision des fraudes.

Étape 1 : Construire un détecteur

1. Dans le volet de navigation de gauche de la console Amazon Fraud Detector, choisissezDétecteurs.
2. ChoisissezCréer un détecteur.
3. Dans leDéfinir les détails du détecteurpage, entrez`sample_detector`pour le nom du détecteur. Entrez éventuellement une description du détecteur, telle que`my sample fraud detector`.
4. PourType d'événement, sélectionnez le type d'événement que vous avez créé pour la prévision des fraudes.
5. Choisissez Suivant.

Étape 2 : Ajouter une version de modèle déployée

1. Notez qu'il s'agit d'une étape facultative. Il n'est pas nécessaire d'ajouter un modèle à votre détecteur. Pour sauter cette étape, choisissez Next (Suivant).
2. Dans leAjouter un modèle - facultatif, choisissezAjouter un modèle.
3. Dans leAjouter un modèlepage, pourSélectionnez le modèle, choisissez le nom du modèle Amazon Fraud Detector que vous avez déployé précédemment. PourSélectionnez la version, choisissez la version du modèle déployé.
4. Choisissez Add model.
5. Choisissez Suivant.

Étape 3 : Ajouter des règles

Une règle est une condition qui indique à Amazon Fraud Detector comment interpréter les valeurs des variables lors de l'évaluation à des fins de prédiction des fraudes.
Cet exemple va créer trois règles en utilisant les scores du modèle comme valeurs variables :`high_fraud_risk`,`medium_fraud_risk`, et`low_fraud_risk`. Pour créer vos propres règles, expressions de règles, ordre d'exécution des règles et résultats, utilisez des valeurs adaptées à votre modèle et à votre cas d'utilisation.

1. Dans leAjouter des règlespage, sousDéfinir une règle, entrez`high_fraud_risk`pour le nom de la règle et sousDescription : optionnel, entrez**`This rule captures events with a high ML model score`**comme description de la règle.

2. DansExpression, entrez l'expression de règle suivante à l'aide du langage d'expression de règles simplifié d'Amazon Fraud Detector :

   ```
   $sample_fraud_detection_model_insightscore > 900
   ```

3. DansRésultats, choisissezCréation d'un nouveau résultat. Un résultat est le résultat d'une prédiction de fraude et est renvoyé si la règle correspond lors d'une évaluation.
4. DansCréation d'un nouveau résultat, entrez`verify_customer`comme nom du résultat. Entrez éventuellement une description.
5. ChoisissezEnregistrer le résultat.
6. ChoisissezAjouter une règlepour exécuter le vérificateur de validation des règles et enregistrer la règle. Une fois la règle créée, Amazon Fraud Detector met la règle à votre disposition pour qu'elle puisse être utilisée dans votre détecteur.
7. ChoisissezAjouter une autre règle, puis choisissezCréer une règleonglet.
8. Répétez ce processus deux fois de plus pour créer votre`medium_fraud_risk`et`low_fraud_risk`règles en utilisant les détails suivants :

   - risque_frauduleux moyen

     Nom de la règle :`medium_fraud_risk`

     Résultat :`review`

     Expression :

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

     ```
     $sample_fraud_detection_model_insightscore > 700
     ```

   - risque_de fraude faible

     Nom de la règle :`low_fraud_risk`

     Résultat :`approve`

     Expression :

     ```
     $sample_fraud_detection_model_insightscore <= 700
     ```

9. Après avoir créé toutes les règles pour votre cas d'utilisation, choisissezSuivant.

Pour plus d'informations sur la création et la rédaction de règles, voirRèglesetRéférence du langage des règles.

Étape 4 : Configuration de l'exécution des règles et de l'ordre des règles

Le mode d'exécution des règles incluses dans le détecteur détermine si toutes les règles que vous définissez sont évaluées ou si l'évaluation des règles s'arrête à la première règle correspondante. Et l'ordre des règles détermine l'ordre dans lequel vous souhaitez que la règle soit exécutée.

Le mode d'exécution des règles par défaut est`FIRST_MATCHED`.

Premier match

Le mode d'exécution de la première règle correspondante renvoie les résultats de la première règle correspondante en fonction de l'ordre des règles défini. Si vous spécifiez `FIRST_MATCHED`, Amazon Fraud Detector évalue les règles de manière séquentielle, de la première à la dernière, en s'arrêtant à la première règle correspondante. Amazon Fraud Detector fournit ensuite les résultats pour cette règle unique.

L'ordre dans lequel vous exécutez les règles peut affecter le résultat de la prédiction de fraude qui en résulte. Après avoir créé vos règles, réorganisez-les pour les exécuter dans l'ordre souhaité en procédant comme suit :

Si votre`high_fraud_risk`la règle ne figure pas déjà en haut de votre liste de règles, choisissezOrdre, puis choisissez1. Cela bouge`high_fraud_risk`à la première position.

Répétez ce processus pour que votre`medium_fraud_risk`la règle se trouve en deuxième position et votre`low_fraud_risk`la règle est en troisième position.

Tous correspondent

Le mode d'exécution de toutes les règles correspondantes renvoie des résultats pour toutes les règles correspondantes, quel que soit l'ordre des règles. Si vous spécifiez`ALL_MATCHED`, Amazon Fraud Detector évalue toutes les règles et renvoie les résultats pour toutes les règles correspondantes.

SélectionnezFIRST_MATCHEDpour ce didacticiel, puis choisissezSuivant.

Étape 5 : Révision et création de la version du détecteur

Une version de détection définit les modèles et les règles spécifiques utilisés pour générer des prévisions de fraude.

1. Dans leRévision et créationpage, passez en revue les détails, les modèles et les règles du détecteur que vous avez configurés. Si vous devez apporter des modifications, choisissezModifierà côté de la section correspondante.
2. ChoisissezCréer un détecteur. Une fois créée, la première version de votre détecteur apparaît dans le tableau des versions du détecteur avec`Draft`statut.

   Vous utilisez leBrouillonversion pour tester votre détecteur.

Créez un détecteur à l'aide duAWS SDK for Python (Boto3)

L'exemple suivant montre un exemple de demande pour`PutDetector`API. Un détecteur fait office de conteneur pour les versions de vos détecteurs. Le`PutDetector`L'API spécifie le type d'événement que le détecteur évaluera. L'exemple suivant suppose que vous avez créé un type d'événement`sample_registration`.

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

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

Création d'une version du détecteur

Une version de détecteur définit les règles, l'ordre d'exécution des règles et, éventuellement, une version du modèle, qui seront utilisés dans le cadre de la demande pour générer des prévisions de fraude. Vous pouvez ajouter n'importe laquelle des règles définies dans un détecteur à la version du détecteur. Vous pouvez également ajouter n'importe quel modèle entraîné sur le type d'événement évalué.

L'état de chaque version du détecteur estDRAFT,ACTIVE, ouINACTIVE. Il ne peut y avoir qu'une seule version de détecteurACTIVEstatut à la fois. Au cours duGetEventPredictiondemande, Amazon Fraud Detector utiliseraACTIVEdétecteur si nonDetectorVersionest spécifié.

Mode d'exécution des règles

Amazon Fraud Detector prend en charge deux modes d'exécution de règles différents :FIRST_MATCHEDetALL_MATCHED.

- Si le mode d'exécution des règles estFIRST_MATCHED, Amazon Fraud Detector évalue les règles de manière séquentielle, de la première à la dernière, en s'arrêtant à la première règle correspondante. Amazon Fraud Detector fournit ensuite les résultats pour cette règle unique. Si le résultat d'une règle est faux (non concordant), la règle suivante de la liste est évaluée.
- Si le mode d'exécution des règles estALL_MATCHED, toutes les règles d'une évaluation sont alors exécutées en parallèle, quel que soit leur ordre. Amazon Fraud Detector exécute toutes les règles et renvoie les résultats définis pour chaque règle correspondante.

Créez une version du détecteur à l'aide duAWS SDK for Python (Boto3)

L'exemple suivant montre un exemple de demande pourCreateDetectorVersionAPI. Le mode d'exécution des règles est défini surFIRST_MATCHED, Amazon Fraud Detector évaluera donc les règles de manière séquentielle, de la première à la dernière, en s'arrêtant à la première règle correspondante. Amazon Fraud Detector fournit ensuite les résultats de cette règle unique au cours deGetEventPrediction 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'
)
```

Pour mettre à jour l'état d'une version du détecteur, utilisez`UpdateDetectorVersionStatus`API. L'exemple suivant met à jour l'état de la version du détecteur depuis`DRAFT`pour`ACTIVE`. Au cours d'une`GetEventPrediction`demande, si aucun identifiant de détecteur n'est spécifié, Amazon Fraud Detector utilisera`ACTIVE`version du détecteur.

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

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

Supprimer un détecteur, une version de détecteur ou une version de règle

Avant de supprimer un détecteur dans Amazon Fraud Detector, vous devez d'abord supprimer toutes les versions de détecteur et toutes les versions de règle associées au détecteur.

Lorsque vous supprimez un détecteur, une version de détecteur ou une version de règle, Amazon Fraud Detector supprime définitivement cette ressource et les données ne sont plus stockées dans Amazon Fraud Detector.

Pour supprimer une version de détecteur

Vous pouvez uniquement supprimer les versions du détecteur qui sont dans l'`INACTIVE`état`DRAFT` ou qui sont dans l'état.

1. Connectez-vous àAWS Management Console et ouvrez la console Amazon Fraud Detector à l'adresse https://console.aws.amazon.com/frauddetector.
2. Dans le panneau de navigation gauche de la console Amazon Fraud Detector, choisissez Detectors.
3. Choisissez le détecteur qui contient la version du détecteur que vous souhaitez supprimer.
4. Choisissez la version de détecteur que vous souhaitez supprimer.
5. Choisissez Actions, puis Delete (Supprimer).
6. Entrez**`delete`**, puis choisissez Supprimer le détecteur.

Pour supprimer une version de règle

Vous ne pouvez supprimer une version de règle que si elle n'est utilisée par`ACTIVE` aucune version du`INACTIVE` détecteur. Si nécessaire, avant de supprimer une version de règle, déplacez d'abord la version du`ACTIVE` détecteur vers`INACTIVE`, puis supprimez la version du`INACTIVE` détecteur.

1. Dans le panneau de navigation gauche de la console Amazon Fraud Detector, choisissez Detectors.
2. Choisissez le détecteur qui contient la version de règle que vous souhaitez supprimer.
3. Choisissez l'onglet Règles associées et choisissez la règle que vous souhaitez supprimer.
4. Choisissez la version de règle que vous souhaitez supprimer.
5. Choisissez Actions, puis choisissez Supprimer la version de la règle.
6. Entrez**`delete`**, puis choisissez Supprimer la version.

Pour supprimer un détecteur

Avant de supprimer un détecteur, vous devez d'abord supprimer toutes les versions de détecteur et toutes les versions de règle associées au détecteur.

1. Dans le panneau de navigation gauche de la console Amazon Fraud Detector, choisissez Detectors.
2. Choisissez le détecteur que vous souhaitez supprimer.

3. Choisissez Actions, puis choisissez Supprimer le détecteur.
4. Entrez**`delete`**, puis choisissez Supprimer le détecteur.

Ressources

Les modèles, les règles et les détecteurs utilisent des ressources telles que des variables, des résultats, des étiquettes, des listes et des entités pour évaluer les risques de fraude. Cette section fournit des informations sur la création et la gestion des ressources.

Rubriques

Variables

Les variables représentent les éléments de données que vous souhaitez utiliser dans une prévision de fraude. Ces variables peuvent être extraites de l'ensemble de données d'événements que vous avez préparé pour entraîner votre modèle, des résultats des scores de risque de votre modèle Amazon Fraud Detector ou des SageMaker modèles Amazon. Pour plus d'informations sur les variables extraites du jeu de données d'événements, consultezObtenez les exigences relatives aux ensembles de données d'événements à l'aide de l'explorateur de modèles.

Les variables que vous souhaitez utiliser dans vos prévisions de fraude doivent d'abord être créées, puis ajoutées à l'événement lors de la création de votre type d'événement. Chaque variable que vous créez doit se voir attribuer un type de données, une valeur par défaut et éventuellement un type de variable. Amazon Fraud Detector enrichit certaines des variables que vous fournissez, telles que les adresses IP, les numéros d'identification bancaire (BIN) et les numéros de téléphone, afin de créer des entrées supplémentaires et d'améliorer les performances des modèles qui utilisent ces variables.

Types de données

Les variables doivent avoir un type de données pour l'élément de données qu'elles représentent et peuvent éventuellement se voir attribuer l'un des types prédéfinisTypes de variables. Pour les

variables affectées à un type de variable, le type de données est présélectionné. Les types de données possibles incluent les types suivants :

Type de données	Description	Valeur par défaut	Exemples de valeur
Chaîne	N'importe quelle combinaison de lettres, de chiffres entiers ou des deux	<empty>	abc, 123 ans, 1D3B
Entier	Nombres entiers positifs ou négatifs	0	1, -1
Booléen	Vrai ou faux	False	Vrai, Faux
DateTime	Date et heure spécifiées uniquement au format UTC de la norme ISO 8601	<empty>	2019-11-30T 13:01:01 Z
Float	Nombres avec virgule décimale	0.0	4,01, 0,10

Valeur par défaut

Les variables doivent avoir une valeur par défaut. Lorsqu'Amazon Fraud Detector génère des prévisions de fraude, cette valeur par défaut est utilisée pour exécuter une règle ou un modèle si Amazon Fraud Detector ne reçoit aucune valeur pour une variable. Les valeurs par défaut que vous fournissez doivent correspondre au type de données sélectionné. Dans la console AWS, Amazon Fraud Detector attribue la valeur par défaut `0` pour les entiers, pour les booléens, `false` pour les flottants et (vide) `0.0` pour les chaînes. Vous pouvez définir une valeur par défaut personnalisée pour n'importe lequel de ces types de données.

Types de variables

Lorsque vous créez une variable, vous pouvez éventuellement l'affecter à un type de variable. Le type de variable représente les éléments de données courants utilisés pour former des modèles et générer des prévisions de fraude. Seules les variables associées à un type de variable peuvent être utilisées pour l'apprentissage du modèle. Dans le cadre du processus de formation du

modèle, Amazon Fraud Detector utilise le type de variable associé à la variable pour effectuer des enrichissements variables, une ingénierie des fonctionnalités et une évaluation des risques.

Amazon Fraud Detector a prédéfini les types de variables suivants qui peuvent être utilisés pour les attribuer à vos variables.

Ca	Type de variable	Description	Type de donn	Ex
Session	IP_ADDRESS	L'adresse IP collectée lors de l'événement	Cha	192,2.0 Remarque : Amazon Fraud Detector enrichit ces données. Pour de plus amples informations, consultez Enrichissement de la géolocalisation.
	AGENT UTILISATEUR	L'agent utilisateur collecté lors de l'événement	Cha	Mozilla 5.0 (Windows NT 10.0,

Ca	Type de variable	Description	Type de donn	Ex
				Win64, x64, rv:68.0) Gecko 20100101
	EMPREINTE DIGITALE	L'identifiant unique d'un appareil utilisé pour l'événement	Cha	sadfow987u234
	SESSION_ID	L'ID de session pour la session active de l'événement	Cha	sid123456789
	LES INFORMATONS D'IDENTIFICATION SONT-ELLES VALIDES	Indique si les informations d'identification utilisées pour la connexion aux événements sont valides	Bool	True
Uti ur	ADRESSE_-MAIL	L'adresse e-mail collectée lors de l'événement	Cha	abc@domain.com

Ca	Type de variable	Description	Type de donn	Ex
	PHONE_NUMBER	Le numéro de téléphone collecté lors de l'événement	Cha	+1 555-0100 Remarque : Amazon Fraud Detector enrichit ces données. Pour de plus amples informations, consultez Enrichissement du numéro de téléphone.
Fa on	NOM_DE FACTURATION	Le nom associé à l'adresse de facturation	Cha	Jean Dupont

Ca	Type de variable	Description	Type de donn	Ex
	TÉLÉPHONE DE FACTURATION	Le numéro de téléphone associé à l'adresse de facturation	Cha	+1 555-0100 Remarque : Amazon Fraud Detector enrichit ces données. Pour de plus amples informations, consultez Enrichissement du numéro de téléphone.
	ADRESSE_E FACTURATION_L1	La première ligne de l'adresse de facturation	Cha	N'importe quelle rue

Ca	Type de variable	Description	Type de donn	Ex
	ADRESSE_E FACTURATON_L2	La deuxième ligne de l'adresse de facturation	Cha	N'importe quelle unité 123
	BILLING_CITY	La ville indiquée dans l'adresse de facturation	Cha	N'importe quelle ville
	ÉTAT DE FACTURATON	État ou province indiqué dans l'adresse de facturation	Cha	N'importe quel État ou province

Ca	Type de variable	Description	Type de donn	Ex
	PAYS_DE_F ACTURATIO N	Le pays indiqué dans l'adresse de facturation	Cha	N'importe quel pays Remarque : Amazon Fraud Detector enrichit ces données. Pour de plus amples informations, consultez Enrichissement de la géolocalisation.

Ca	Type de variable	Description	Type de donn	Ex
	ZIP DE FACTURATION	Le code postal qui se trouve dans l'adresse de facturation	Cha	01234 Remarque : Amazon Fraud Detector enrichit ces données. Pour de plus amples informations, consultez Enrichissement de la géolocalisation.
Ex n	NOM_D'EXÉDITION	Le nom associé à l'adresse de livraison	Cha	Jean Dupont

Ca	Type de variable	Description	Type de donn	Ex
	TÉLÉPHONE D'EXPÉDITION	Le numéro de téléphone associé à l'adresse de livraison	Cha	+1 555-0100 Remarque : Amazon Fraud Detector enrichit ces données. Pour de plus amples informations, consultez Enrichissement du numéro de téléphone.
	ADRESSE_E LIVRAISON_L1	La première ligne de l'adresse de livraison	Cha	123 Any Street

Ca	Type de variable	Description	Type de donn	Ex
	ADRESSE_E LIVRAISON_L2	La deuxième ligne de l'adresse de livraison	Cha	Unité 123
	VILLE_D'EXPÉDITION	La ville indiquée dans l'adresse de livraison	Cha	N'importe quelle ville
	ÉTAT_D'EXPÉDITION	État ou province indiqué dans l'adresse de livraison	Cha	N'importe quel État

Ca	Type de variable	Description	Type de donn	Ex
	PAYS_D'EXPÉDITION	Le pays dans lequel se trouve l'adresse de livraison	Cha	N'importe quel pays Remarque : Amazon Fraud Detector enrichit ces données. Pour de plus amples informations, consultez Enrichissement de la géolocalisation.

Ca	Type de variable	Description	Type de donn	Ex
	ZIP_D'EXPÉDITION	Le code postal qui se trouve dans l'adresse de livraison	Cha	01234 Remarque : Amazon Fraud Detector enrichit ces données. Pour de plus amples informations, consultez Enrichissement de la géolocalisation.
Paie	IDENTIFIANT_COMMANDE	L'identifiant unique de la transaction	Cha	LUX60
	PRIX	Le prix total de la commande	Cha	560,00
	CODE_DEVISE	Le code de devise ISO 4217	Cha	USD

Ca	Type de variable	Description	Type de donn	Ex
	TYPE_DE PAIEMENT	Le mode de paiement utilisé pour le paiement lors de l'événeme nt	Cha	Carte de crédit
	CODE D'AUTHEN IFICATION	Le code alphanumé rique envoyé par l'émetteur de la carte de crédit ou la banque émettrice	Cha	0000
	AVS	Le code de réponse du système de vérification d'adresse (AVS) émis par le processeur de la carte	Cha	Y
Pr	CATÉGORI _PRODUIT	La catégorie de produit de l'article commandé	Cha	Cuisine
Pe isé	NUMERIC	Toute variable pouvant être représentée sous forme de nombre réel	Floa	1,224

Ca	Type de variable	Description	Type de donn	Ex
	CATEGORICAL (catégorie)	Toute variable décrivant des catégories, des segments ou des groupes	Cha	Large
	TEXTE_FORMULAIRE_LIBRE	Tout texte en format libre capturé dans le cadre de l'événement (par exemple, un avis ou un commentaire d'un client)	Cha	Exemple de saisie de texte sous forme libre

Affectation d'une variable à un type de variable

Si vous envisagez d'utiliser une variable pour entraîner votre modèle, il est important que vous choisissiez le type de variable approprié à affecter à la variable. Une attribution incorrecte du type de variable peut avoir un impact négatif sur les performances de votre modèle. Il peut également s'avérer très difficile de modifier l'affectation ultérieurement, en particulier si plusieurs modèles et événements ont utilisé la variable.

Vous pouvez attribuer à votre variable l'un des types de variables prédéfinis ou l'un des types de variables personnalisés —`FREE_FORM_TEXT`,`CATEGORICAL`, ou`NUMERIC`.

Remarques importantes concernant l'affectation de variables aux bons types de variables

1. Si la variable correspond à l'un des types de variables prédéfinis, utilisez-la. Assurez-vous que le type de variable correspond à la variable. Par exemple, si vous attribuez une variable ip_address à un type de variable, la `EMAIL_ADDRESS` variable ip_address ne sera pas enrichie par des enrichissements tels que l'ASN, l'ISP, la géolocalisation et le score de risque. Pour plus d'informations, veuillez consulter Enrichissements variables.

2. Si la variable ne correspond à aucun type de variable prédéfini, suivez les recommandations ci-dessous pour attribuer l'un des types de variables personnalisés.
3. Attribuez un type de `CATEGORICAL` variable à des variables qui n'ont généralement pas d'ordre naturel et qui peuvent être placées dans des catégories, des segments ou des groupes. Le jeu de données que vous utilisez pour entraîner votre modèle peut contenir des variables d'identification telles que merchant_id, campaign_id ou policy_id. Ces variables représentent des groupes (par exemple, tous les clients ayant le même policy_id représentent un groupe). Les variables contenant les données suivantes doivent se voir attribuer le type de variable CATEGORICAL -
   - Variables contenant des données telles que Customer_ID, Segment_ID, Color_ID, department_code ou Product_ID.
   - Variables contenant des données booléennes avec des valeurs vraies, fausses ou nulles.
   - Variables pouvant être placées dans des groupes ou des catégories telles que le nom de l'entreprise, la catégorie de produit, le type de carte ou le support de référence.

   > **Note**
   >
   > `ENTITY_ID`Dest un type de variable réservé utilisé par Amazon Fraud Detector pour attribuer à la variable ENTITY_ID. La variable ENTITY_ID est l'ID de l'entité qui lance l'action que vous souhaitez évaluer. Si vous créez un type de modèle Transaction Fraud Insight (TFI), vous devez fournir la variable ENTITY_ID. Vous devrez décider quelle variable de vos données identifie de manière unique l'entité à l'origine de l'action et la transmettre en tant que variable ENTITY_ID. Attribuez le type de variable CATEGORICAL à tous les autres ID de votre jeu de données, s'ils sont présents et si vous les utilisez pour l'apprentissage du modèle. Parmi les autres identifiants qui ne constituent pas une entité dans votre jeu de données, citons Merchant_ID, Policy_ID et Campaign_ID.

4. Attribuez un type de `FREE_FORM_TEXT` variable aux variables qui contiennent un bloc de texte. Voici des exemples de types de variables FREE_FORM_TEXT : les avis des utilisateurs, les commentaires, les dates et les codes de référence. Les données FREE_FORM_TEXT contiennent plusieurs jetons séparés par un délimiteur. Les délimiteurs peuvent être n'importe quel caractère autre que le caractère alphanumérique et le trait de soulignement. Par exemple, les avis et les commentaires des utilisateurs peuvent être séparés par un séparateur « espace », tandis que les dates et les codes de référence peuvent utiliser des traits d'union comme délimiteurs pour séparer le préfixe, le suffixe et les parties intermédiaires. Amazon Fraud Detector utilise les délimiteurs pour extraire les données des variables FREE_FORM_TEXT.

5. Attribuez le type de variable NUMÉRIQUE aux variables qui sont des nombres réels et qui ont un ordre inhérent. Des exemples de variables NUMERIC incluent day_of_the_week, incident_severity, customer_rating. Bien que vous puissiez attribuer le type de variable CATEGORICAL à ces variables, nous vous recommandons vivement d'attribuer toutes les variables numériques avec un ordre inhérent au type de variable NUMÉRIQUE.

Enrichissements variables

Amazon Fraud Detector enrichit certains éléments de données brutes que vous fournissez, tels que les adresses IP, les numéros d'identification bancaire (BIN) et les numéros de téléphone, afin de créer des entrées supplémentaires et d'améliorer les performances des modèles qui utilisent ces éléments de données. L'enrichissement permet d'identifier les situations potentiellement suspectes et aide les modèles à détecter davantage de fraudes.

Enrichissement du numéro de téléphone

Amazon Fraud Detector enrichit les données relatives aux numéros de téléphone avec des informations supplémentaires relatives à la géolocalisation, à l'opérateur d'origine et à la validité du numéro de téléphone. L'enrichissement des numéros de téléphone est automatiquement activé pour tous les modèles qui sont formés le 13 décembre 2021 ou après cette date et dont le numéro de téléphone inclut un code de pays (+xxx). Si vous avez inclus une variable de numéro de téléphone dans votre modèle et que vous l'avez entraînée avant le 13 décembre 2021, réentraînez votre modèle afin qu'il puisse tirer parti de cet enrichissement.

Nous vous recommandons vivement d'utiliser le format suivant pour les variables de numéro de téléphone afin de garantir un enrichissement réussi de vos données.

Variable	Format	Description
PHONE_NUMBER	La norme E.164	Assurez-vous d'inclure le code du pays (+xxx) avec le numéro de téléphone.
BILLING_PHONE et SHIPPING_PHONE	La norme E.164	Assurez-vous d'inclure le code du pays (+xxx) avec le numéro de téléphone.

Enrichissement de la géolocalisation

À compter du 8 février 2022, Amazon Fraud Detector calcule la distance physique entre les valeurs IP_ADDRESS, BILLING_ZIP et SHIPPING_ZIP que vous fournissez pour un événement. Les distances calculées sont utilisées comme entrées dans votre modèle de détection des fraudes.

Pour permettre l'enrichissement de la géolocalisation, les données de votre événement doivent inclure au moins deux des trois variables : IP_ADDRESS, BILLING_ZIP ou SHIPPING_ZIP. En outre, chaque valeur BILLING_ZIP et SHIPPING_ZIP doit comporter respectivement un code BILLING_COUNTRY et un code SHIPPING_COUNTRY valides. Si votre modèle a été entraîné avant le 8 février 2022 et qu'il inclut ces variables, vous devez réentraîner le modèle pour permettre l'enrichissement par géolocalisation.

Si Amazon Fraud Detector ne parvient pas à déterminer l'emplacement associé aux valeurs IP_ADDRESS, BILLING_ZIP ou SHIPPING_ZIP pour un événement en raison de la non-validité des données, une valeur d'espace réservé spéciale est utilisée à la place. Supposons, par exemple, qu'un événement possède des valeurs IP_ADDRESS et BILLING_ZIP valides, mais que la valeur SHIPPING_ZIP ne l'est pas. Dans ce cas, l'enrichissement est effectué uniquement pour IP_ADDRESS—> BILLING_ZIP. L'enrichissement n'est pas effectué pour IP_ADDRESS—>SHIPPING_ZIP et BILLING_ZIP—>SHIPPING_ZIP. Au lieu de cela, les valeurs des espaces réservés sont utilisées à leur place. Que l'enrichissement par géolocalisation soit activé ou non pour votre modèle, les performances de votre modèle ne changent pas.

Vous pouvez désactiver l'enrichissement par géolocalisation en mappant vos variables BILLING_ZIP et SHIPPING_ZIP au type de variable CUSTOM_CATEGORICAL. La modification du type de variable n'affecte pas les performances de votre modèle.

Format variable de géolocalisation

Nous vous recommandons vivement d'utiliser le format suivant pour les variables de géolocalisation afin de vous assurer que vos données de localisation sont correctement enrichies.

Variable	Format	Description
IP_ADDRESS	Adresse IPv4	Par exemple - 1.1.1.1
BILLING_ZIP et SHIPPING_ZIP	Le code postal ISO 3166-1 alpha-2 du pays spécifié	Pour plus d'informations, consultez la section Codes de pays

Variable	Format	Description
		et de territoires de cette rubrique.
BILLING_COUNTRY et SHIPPING_COUNTRY	Le code de pays standard à deux lettres ISO 3166-1 alpha-2	Pour plus d'informations, consultez la section Codes de pays et de territoires de cette rubrique. Amazon Fraud Detector essaie de faire correspondre toutes les variantes courantes du nom d'un pays à son code de pays standard à deux lettres ISO 3166-1. Cependant, nous ne pouvons pas garantir qu'ils seront correctement mis en correspondance.

Codes de pays et de territoires

Le tableau suivant fournit une liste complète des pays et territoires pris en charge par Amazon Fraud Detector pour l'enrichissement de la géolocalisation. Chaque pays et territoire est associé à un code de pays (en particulier, le code de pays à deux lettres ISO 3166-1 alpha-2) et à un code postal.

Format du code postal

- 9 - numéro
- une - lettre
- [X] - X est facultatif. Par exemple, « GY9 [9] 9aa » de Guersney signifie que « GY9 9aa » et « GY99 9aa » sont valides. Utilisez un seul format.
- [X/XX] : vous pouvez utiliser X ou XX. Par exemple, « aa [aa/99] » des Bermudes signifie que « aa aa » et « aa 99 » sont valides. Utilisez l'un de ces formats, mais pas les deux.

- Certains pays ont un préfixe fixe. Par exemple, le code postal d'Andorre est AD999. Cela signifie que le code du pays doit commencer par les lettres AD suivies de trois chiffres.

Code	Nom	Code postal
AD	Andorre	ANNONCE 999
AR	Antilles néerlandaises	9999
AT	Autriche	9999
AU	Australie	9999
AZ	Azerbaïdjan	COMME 9999
BD	Bangladesh	9999
ÊTRE	Belgique	9999
SAC	Bulgarie	9999
BM	Bermudes	aa [aa/99]
BY	Biélorussie	999999
CA	Canada	a9a 9a9
CHAP	Suisse	9999
CL	Chili	9999999
CO	Colombie	999999
CR	Costa Rica	99999
CY	Chypre	9999
RÉPUBLIQUE TCHÈQUE	Tchéquie	99 99
DE	Allemagne	99999

Code	Nom	Code postal
DK	Danemark	9999
DO	République Dominicaine	99999
DZ	Algérie	99999
EE	Estonie	99999
ES	Espagne	99999
FI	Finlande	99999
FM	États fédérés de Micronésie	99999
POUR	Iles Féroé	999
FR	France	99999
Go	Royaume-Uni	[a] 9 [a/9] 9aa
GG	Guernesey	GY9 [9] 9aa
GRAND LIVRE	Groenland	9999
GRAND PRIX	Guadeloupe	99999
GT	Guatemala	99999
GU	Guam	99999
HR	Croatie	99999
HU	Hongrie	9999
IE	Irlande	a99 [a/9] [a/9] [a/9]
IM	Île de Man	IM9 [9] 9aa
IN	Inde	999999

Code	Nom	Code postal
IS	Islande	999
IL	Italie	99999
JE	Jersey	JE9 [9] 9aa
JP	Japon	999-9999
KR	République de Corée	99999
LI	Liechtenstein	9999
LK	Sri Lanka	99999
LT	Lituanie	99999
LU	Luxembourg	L-9999
LV	Lettonie	LV-9999
MAÎTRE DES CÉRÉMONIES	Monaco	99999
MARYLAND	République de Moldova	9999
MH	Îles Marshall	99999
MK	Macédoine du Nord	9999
MP	Îles Mariannes du Nord	99999
MQ	Matinique	99999
MT	Malte	aaa 999
MX	Mexique	99999
MON	Malaisie	99999
NL	Pays-Bas	999 aa

Code	Nom	Code postal
NO	Norvège	9999
NZ	Nouvelle-Zélande	9999
PH	Philippines	9999
PK	Pakistan	99999
PL	Pologne	99-999
PR	Porto Rico	99999
PT	Portugal	9999-999
PW	Palaos	99999
RE	Réunion	99999
RO	Roumanie	999999
RU	Fédération de Russie	999999
SE	Suède	99 99
SG	Singapour	999999
SI	Slovénie	9999
SK	Slovaquie	99 99
HM	Saint-Marin	99999
TH	Thaïlande	99999
TR	Turquie	99999
UA	Ukraine	99999
ETATS-UNIS	États-Unis	99999

Code	Nom	Code postal
BUY	Uruguay	99999
VI	Iles Vierges américaines	99999
WF	Wallis-et-Futuna	99999
YT	Mayotte	99999
ZA	Afrique du Sud	9999

Enrichissement des agents utilisateurs

Si vous créez le modèle Account Takeover Insights (ATI), vous devez fournir une variable du type de `useragent` variable dans votre jeu de données. Cette variable contient les données du navigateur, de l'appareil et du système d'exploitation d'un événement de connexion. Amazon Fraud Detector enrichit les données utilisateur/agent avec des informations supplémentaires telles que `user_agent_family`OS_family, et. `device_family`

Création d'une variable

Vous pouvez créer des variables dans la console Amazon Fraud Detector, à l'aide de la commande create-variable, à l'aide du CreateVariableou du AWS SDK for Python (Boto3)

Création d'une variable à l'aide de la console Amazon Fraud Detector

Cet exemple crée deux variables `email_address` et`ip_address`, et les affecte aux types de variables correspondants (`EMAIL_ADDRESS`et`IP_ADDRESS`). Ces variables sont utilisées à titre d'exemple. Si vous créez des variables à utiliser pour l'apprentissage de votre modèle, utilisez les variables de votre jeu de données qui conviennent à votre cas d'utilisation. Assurez-vous de lire à propos de vos variables Types de variables et Enrichissements variables avant de les créer.

Pour créer une variable,

1. Ouvrez la console AWS de gestion et connectez-vous à votre compte.
2. Accédez à Amazon Fraud Detector, choisissez Variables dans le volet de navigation de gauche, puis choisissez Créer.

3. Sur la page Nouvelle variable, entrez le `email_address` nom de la variable. Entrez éventuellement une description de la variable.
4. Dans le type de variable, choisissez Adresse e-mail.
5. Amazon Fraud Detector sélectionne automatiquement le type de données pour ce type de variable car ce type de variable est prédéfini. Si aucun type de variable n'est automatiquement attribué à votre variable, sélectionnez un type de variable dans la liste. Pour plus d'informations, veuillez consulter Types de variables.
6. Si vous souhaitez fournir une valeur par défaut pour votre variable, sélectionnez Définir une valeur par défaut personnalisée et entrez une valeur par défaut pour votre variable. Ignorez cette étape si vous suivez cet exemple.
7. Sélectionnez Create (Créer).
8. Sur la page d'aperçu email_address, confirmez les détails de la variable que vous venez de créer.

   Si vous devez effectuer une mise à jour, choisissez Modifier et fournissez les mises à jour. Choisissez Save Changes (Enregistrer les modifications).
9. Répétez le processus pour créer une autre variable `ip_address` et choisissez Adresse IP pour le type de variable.
10. La page Variables affiche les variables récemment créées.

> **Important**
>
> Nous vous recommandons de créer autant de variables que vous le souhaitez à partir de votre jeu de données. Vous pouvez décider ultérieurement, lors de la création de votre type d'événement, quelles variables vous souhaitez inclure pour entraîner votre modèle à détecter les fraudes et à générer des détections de fraude.

Créez une variable à l'aide du AWS SDK for Python (Boto3)

L'exemple suivant montre les demandes pour l'CreateVariableAPI. L'exemple crée deux variables `email_address` et`ip_address`, et les affecte aux types de variables correspondants (`EMAIL_ADDRESS`et`IP_ADDRESS`).

Ces variables sont utilisées à titre d'exemple. Si vous créez des variables à utiliser pour l'apprentissage de votre modèle, utilisez les variables de votre jeu de données qui conviennent

à votre cas d'utilisation. Assurez-vous de lire à propos de vos variables Types de variables et Enrichissements variables avant de les créer.

Veillez à spécifier une source variable. Cela permet d'identifier d'où provient la valeur de la variable. Si la source de la variable est EVENT, la valeur de la variable est envoyée dans le cadre de la GetEventPredictiondemande. Si la valeur de la variable est`MODEL_SCORE`, elle est renseignée par un détecteur de fraude Amazon. Si`EXTERNAL_MODEL_SCORE`, la valeur de la variable est renseignée par un SageMaker modèle importé.

```
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>'
     )
```

Supprimer une variable

Lorsque vous supprimez une variable, Amazon Fraud Detector supprime définitivement cette variable et les données ne sont plus stockées dans Amazon Fraud Detector.

Vous ne pouvez pas supprimer les variables incluses dans un type d'événement dans Amazon Fraud Detector. Vous devez d'abord supprimer le type d'événement auquel la variable est associée, puis supprimer la variable.

Vous ne pouvez pas supprimer manuellement les variables de sortie du modèle Amazon Fraud Detector et les variables de sortie du SageMaker modèle. Amazon Fraud Detector supprime automatiquement les variables de sortie du modèle lorsque vous supprimez le modèle.

Vous pouvez supprimer une variable dans la console Amazon Fraud Detector, à l'aide de la commande CLI delete-variable, à l'aide de l'DeleteVariableAPI ou à l'aide du AWS SDK for Python (Boto3)

Supprimer une variable à l'aide de la console

Pour supprimer une variable,

1. Connectez-vous à la console Amazon Fraud Detector AWS Management Console et ouvrez-la à l'adresse https://console.aws.amazon.com/frauddetector.
2. Dans le volet de navigation de gauche de la console Amazon Fraud Detector, choisissez Ressources, puis Variables.
3. Choisissez la variable que vous souhaitez supprimer.
4. Choisissez Actions, puis Delete (Supprimer).
5. Entrez le nom de la variable, puis choisissez Supprimer la variable.

Supprimer une variable à l'aide du AWS SDK for Python (Boto3)

L'exemple de code suivant supprime une variable customer_name à l'aide de l'API. DeleteVariable

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

fraudDetector.delete_variable (

name = 'customer_name'

)
```

Etiquettes

Une étiquette classe un événement comme frauduleux ou légitime. Les étiquettes sont associées à des types d'événements et sont utilisées pour entraîner des modèles de machine learning dans

Amazon Fraud Detector. Si vous envisagez de former un modèle Online Fraud Insights (OFI) ou Transaction Fraud Insights (TFI), au moins 400 événements de votre ensemble de données de formation doivent être considérés comme frauduleux ou légitimes. Vous pouvez utiliser n'importe quel libellé tel que fraude, légitime, 1 ou 0 pour classer les événements dans votre jeu de données d'entraînement. Une fois la formation terminée, le modèle formé évalue les événements pour détecter des fraudes et utilise ces valeurs pour classer les événements comme frauduleux ou légitimes.

Vous devrez d'abord créer les étiquettes avec les valeurs utilisées dans votre jeu de données d'apprentissage, puis associer les étiquettes au type d'événement utilisé pour créer et entraîner votre modèle de détection des fraudes.

Créer une étiquette

Vous pouvez créer des étiquettes dans la console Amazon Fraud Detector, à l'aide de la commande put-label, de l'PutLabelAPI ou duAWS SDK for Python (Boto3).

Création d'une étiquette à l'aide de la console Amazon Fraud Detector

Pour créer des étiquettes,

1. Ouvrez la consoleAWS de gestion et connectez-vous à votre compte.
2. Accédez à Amazon Fraud Detector, choisissez Labels dans le menu de navigation de gauche, puis choisissez Créer.
3. Sur la page Créer une étiquette, saisissez le nom de votre étiquette pour l'événement frauduleux comme nom d'étiquette. Le nom de l'étiquette doit correspondre à l'étiquette qui représente une activité frauduleuse dans votre ensemble de données d'entraînement. Si vous le souhaitez, saisissez une description de l'étiquette.
4. Choisissez Créer une étiquette.
5. Créez une deuxième étiquette et entrez un nom d'étiquette pour un événement légitime. Assurez-vous que le nom de l'étiquette correspond à la valeur qui représente l'activité légitime dans votre jeu de données d'entraînement.

Créez une étiquette à l'aide duAWS SDK for Python (Boto3)

L'AWS SDK for Python (Boto3)exemple de code suivant crée deux étiquettes (frauduleuse, légitime) à l'aide de l'PutLabelAPI. Après avoir créé les étiquettes, vous pouvez les ajouter à un type d'événement pour classer des événements spécifiques.

```
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'
)
```

Mettre à jour l'étiquette

Si votre ensemble de données d'événements est stocké dans Amazon Fraud Detector, vous devrez peut-être ajouter ou mettre à jour des étiquettes pour les événements stockés, par exemple lorsque vous menez une enquête de fraude hors ligne pour un événement et que vous souhaitez fermer la boucle de retour d'informations en matière d'apprentissage automatique.

Vous pouvez ajouter ou mettre à jour des étiquettes pour les événements stockés à l'aide de la update-event-labelcommande, de l'UpdateEventLabelAPI ou duAWS SDK for Python (Boto3)

L'AWS SDK for Python (Boto3)exemple de code suivant ajoute une fraude d'étiquette associée à l'enregistrement du type d'événement à l'aide de l'`UpdateEventLabel`API.

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

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

Mettre à jour les libellés des événements dans les données d'événements stockées dans Amazon Fraud Detector

Il se peut que vous deviez ajouter ou mettre à jour des étiquettes de fraude pour des événements déjà enregistrés dans Amazon Fraud Detector, par exemple lorsque vous menez une enquête de fraude hors ligne pour un événement et que vous souhaitez fermer la boucle de retour d'information liée à l'apprentissage automatique. Pour mettre à jour l'étiquette d'un événement déjà enregistré dans Amazon Fraud Detector, utilisez l'opération`UpdateEventLabel` API. Voici un exemple d'appel UpdateEventLabel d'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'
)
```

Supprimer l'étiquette

Lorsque vous supprimez une étiquette, Amazon Fraud Detector supprime définitivement cette étiquette et les données ne sont plus stockées dans Amazon Fraud Detector.

Vous ne pouvez pas supprimer une étiquette incluse dans un type d'événement dans Amazon Fraud Detector. De plus, vous ne pouvez pas supprimer une étiquette affectée à un ID d'événement. Vous devez d'abord supprimer l'ID d'événement correspondant.

Vous pouvez supprimer des étiquettes dans la console Amazon Fraud Detector à l'aide de la commande delete-label, de l'DeleteLabelAPI ou duAWS SDK for Python (Boto3)

Supprimer une étiquette à l'aide de la console

Pour supprimer une étiquette

1. Connectez-vous auAWS Management Console et ouvrez la console Amazon Fraud Detector à l'adresse https://console.aws.amazon.com/frauddetector.

2. Dans le volet de navigation gauche de la console Amazon Fraud Detector, choisissez Ressources, puis Libellés.
3. Choisissez l'étiquette que vous voulez supprimer.
4. Choisissez Actions, puis Delete (Supprimer).
5. Entrez le nom de l'étiquette, puis choisissez Supprimer l'étiquette.

Supprimer une étiquette à l'aide duAWS SDK for Python (Boto3)

L'AWS SDK for Python (Boto3)exemple de code suivant supprime une étiquette légitime à l'aide de l'DeleteLabelAPI.

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

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

Règles

Une règle est une condition qui indique à Amazon Fraud Detector comment interpréter les valeurs variables lors d'une prédiction de fraude. Une règle fait partie de la logique d'un détecteur et comprend les éléments suivants :

- Variable ou liste : la variable représente un élément de données de votre jeu de données d'événements que vous souhaitez utiliser dans une prévision de fraude. Une liste est un ensemble d'éléments de données d'entrée pour une variable de votre jeu de données d'événements. Les variables utilisées dans une règle doivent être prédéfinies dans le type d'événement évalué et les listes utilisées dans une règle doivent être associées à un type de variable. Pour plus d'informations, consultez Variables et Listes.
- Expression : une expression contenue dans une règle reflète votre logique métier. Si vous utilisez une variable dans votre règle, une expression de règle simple est créée à l'aide d'une variable, d'un opérateur de comparaison tel que >, <, <=, >=. == et d'une valeur. Si vous utilisez une liste, l'expression de la règle est construite sous la forme d'une entrée de liste et du nom de la liste. `in` Pour plus d'informations, veuillez consulter Référence du langage des règles. Vous pouvez combiner plusieurs expressions à l'aide de `and` et`or`. Toutes les expressions doivent correspondre

à une valeur booléenne (vrai ou faux) et comporter moins de 4 000 caractères. Les conditions de type If-else ne sont pas prises en charge.

- Résultat : un résultat est une réponse renvoyée par Amazon Fraud Detector lorsqu'une règle correspond. Le résultat indique le résultat d'une prédiction de fraude. Vous pouvez créer des résultats pour chaque prédiction de fraude possible et les ajouter à une règle. Pour plus d'informations, veuillez consulter Résultats.

Un détecteur doit être associé à au moins une règle. Une règle peut comporter jusqu'à 3 listes et un détecteur peut en avoir jusqu'à 30. Vous créez une règle dans le cadre du processus de création du détecteur. Vous pouvez également créer et associer de nouvelles règles à un détecteur existant.

Référence du langage des règles

La section suivante décrit les fonctionnalités d'expression (c'est-à-dire de rédaction de règles) dans Amazon Fraud Detector.

Utilisation de variables

Vous pouvez utiliser n'importe quelle variable définie dans le type d'événement évalué dans le cadre de votre expression. Utilisez le signe du dollar pour indiquer une variable :

```
$example_variable < 100
```

Utiliser des listes

Vous pouvez utiliser n'importe quelle liste associée à un type de variable et remplie d'entrées dans le cadre de votre expression de règle. Utilisez le signe dollar pour indiquer la valeur d'une entrée de liste :

```
$example_list_variable in @list_name
```

Opérateurs de comparaison, d'adhésion et d'identité

Amazon Fraud Detector inclut les opérateurs de comparaison suivants : >, >=, <, <=, ! =, ==, dans, pas dans

Voici quelques exemples :

Exemple : <

```
$variable < 100
```

Exemple : dans, pas dans

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

Exemple : ! =

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

Exemple : ==

```
$variable == 1000
```

Tableaux d'opérateurs

Opérateur	Opérateur du détecteur de fraude Amazon
Egal à	==
Non égal à	!=
Supérieure à	>
Inférieur à	<
Supérieur ou égal à	>=
Inférieur ou égal à	<=
Entrée	dans
And	and
Ou	or
Not	!

Mathématiques de base

Vous pouvez utiliser des opérateurs mathématiques de base dans votre expression (par exemple, +, -, *,/). Un cas d'utilisation typique est celui où vous devez combiner des variables au cours de votre évaluation.

Dans la règle ci-dessous, nous ajoutons la variable `$variable_1` avec `$variable_2` et vérifions si le total est inférieur à 10.

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

Données de base des tables mathématiques

Opérateur	Opérateur du détecteur de fraude Amazon
Plus	+
Moins	-
Multiplication	*
Division	/
Modulo	%

Expression régulière (regex)

Vous pouvez utiliser regex pour rechercher des modèles spécifiques dans le cadre de votre expression. Cela est particulièrement utile si vous souhaitez faire correspondre une chaîne ou une valeur numérique spécifique à l'une de vos variables. Amazon Fraud Detector ne prend en charge la correspondance que lorsque vous travaillez avec des expressions régulières (par exemple, il renvoie True/False selon que la chaîne fournie correspond ou non à l'expression régulière). La prise en charge des expressions régulières par Amazon Fraud Detector est basée sur .matches () dans Java (à l'aide de la bibliothèque d'expressions régulières RE2J). Il existe plusieurs sites Web utiles sur Internet qui permettent de tester différents modèles d'expressions régulières.

Dans le premier exemple ci-dessous, nous transformons d'abord la variable `email` en minuscules. Nous vérifions ensuite si le modèle `@gmail.com` se trouve dans la `email` variable. Notez que le second point est omis afin que nous puissions vérifier explicitement la présence de la chaîne`.com`.

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

Dans le second exemple, nous vérifions si la variable `phone_number` contient le code du pays +1 pour déterminer si le numéro de téléphone provient des États-Unis. Le symbole plus est supprimé afin que nous puissions vérifier explicitement la présence de la chaîne+1.

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

Tableau Regex

Opérateur	Exemple de détecteur de fraude Amazon
Correspond à n'importe quelle chaîne commençant par	regex_match (« ^mystring », $variable)
Correspond exactement à la chaîne entière	regex_match (« mystring », $variable)
Correspond à n'importe quel caractère sauf à la nouvelle ligne	regex_match (» . «, $variable)
Faire correspondre n'importe quel nombre de caractères sauf la nouvelle ligne précédant « mystring »	regex_match (»). *mystring », $variable)
Échappez aux caractères spéciaux	\

Vérification des valeurs manquantes

Il est parfois utile de vérifier si la valeur est manquante. Dans Amazon Fraud Detector, cela est représenté par une valeur nulle. Pour ce faire, utilisez la syntaxe suivante :

```
$variable != null
```

De même, si vous souhaitez vérifier si une valeur n'est pas présente, vous pouvez procéder comme suit :

```
$variable == null
```

Affections multiples

Vous pouvez combiner plusieurs expressions à l'aide de `and` et`or`. Amazon Fraud Detector s'arrête dans une `OR` expression lorsqu'une seule valeur vraie est trouvée, et s'arrête dans une `AND` lorsqu'une seule fausse valeur est détectée.

Dans l'exemple ci-dessous, nous vérifions deux conditions à l'aide de la `and` condition. Dans la première instruction, nous vérifions si la variable 1 est inférieure à 100. Dans le second, nous vérifions si la variable 2 ne correspond pas aux États-Unis.

Étant donné que la règle utilise un`and`, les deux doivent être VRAIS pour que l'ensemble de la condition soit évalué comme VRAI.

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

Vous pouvez utiliser des parenthèses pour regrouper les opérations booléennes, comme indiqué ci-dessous :

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

Autres types d'expressions

DateTimefonctions

Fonction	Description	Exemple
getcurren tdatetime ()	Indique l'heure actuelle de l'exécuti on de la règle au format UTC ISO8601. Vous pouvez utiliser getepochmilliseconds (getcurre ntdatetime ()) pour effectuer des opérations supplémentaires	getcurrentdatetime () = « 28/03/2023 T 18:34:02 Z »
est avant (DateTime1, DateTime 2)	Renvoie une valeur booléenne (True/ False) si l'appelant DateTime 1 est antérieur à 2 DateTime	is before (getcurrentdatetime (), « 2019-11-30T 01:01:01 Z ») == « Faux »

Fonction	Description	Exemple
		is before (getcurrentdatetime (), « 2050-11-30T 01:05:01 Z ») == « Vrai »
est après (DateTime1, DateTime 2)	Renvoie un booléen (True/False) si l'appelant DateTime 1 est après 2 DateTime	isafter (getcurrentdatetime (), « 2019-11-30T 01:01:01 Z ») == « Vrai » isafter (getcurrentdatetime (), « 2050-11-30T 01:05:01 Z ») == « Faux »
getepochm illisecondes () DateTime	Prend un DateTime et le renvoie DateTime en millisecondes d'époque. Utile pour effectuer des opérations mathématiques sur la date	getepochmillisecondes (« 2019-11-30T 01:01:01 Z ») = 1575032461

Opérateurs de chaîne

Opérateur	Exemple
Transformer la chaîne en majuscules	majuscules ($variable)
Transformer la chaîne en minuscules	minuscules ($variable)

Autre

Opérateur	Comment
Ajouter un commentaire	# mon commentaire

Création de règles

Vous pouvez créer des règles dans la console Amazon Fraud Detector, à l'aide de la commande create-rule, à l'aide de l'CreateRuleAPI ou à l'aide du. AWS SDK for Python (Boto3)

Chaque règle doit contenir une expression unique qui reflète votre logique métier. Toutes les expressions doivent correspondre à une valeur booléenne (vrai ou faux) et comporter moins de 4 000 caractères. Les conditions de type If-else ne sont pas prises en charge. Toutes les variables utilisées dans l'expression doivent être prédéfinies dans le type d'événement évalué. De même, toutes les listes utilisées dans l'expression doivent être prédéfinies, associées à un type de variable et être renseignées avec des entrées.

L'exemple suivant crée une règle `high_risk` pour un détecteur existant`payments_detector`. La règle associe une expression et un résultat `verify_customer` à la règle.

Prérequis

Pour suivre les étapes décrites ci-dessous, veillez à effectuer les opérations suivantes avant de créer des règles :

- Création d'un détecteur
- Créer un résultat

Si vous créez un détecteur, une règle et un résultat pour votre cas d'utilisation, remplacez les exemples de nom de détecteur, de nom de règle, d'expression de règle et de nom de résultat par les noms et expressions correspondant à votre cas d'utilisation.

Créez une nouvelle règle dans la console Amazon Fraud Detector

1. Ouvrez la console AWS de gestion et connectez-vous à votre compte. Accédez à Amazon Fraud Detector.
2. Dans le volet de navigation de gauche, choisissez Détecteurs et sélectionnez le détecteur que vous avez créé pour votre cas d'utilisation, par exemple payments_detector.
3. Sur la page payments_detector, choisissez l'onglet Règles associées, puis choisissez Créer une règle.
4. Sur la page Nouvelle règle, saisissez les informations suivantes :

    a. Dans le champ Nom, entrez le nom de la règle, par exemple **`high_risk`**

b. Dans le champ Description (facultatif), entrez éventuellement une description de la règle, par exemple **`This rule captures events with a high ML model score`**

c. Dans l'Expression, entrez une expression de règle correspondant à votre cas d'utilisation à l'aide du guide de référence rapide Expression. `$sample_fraud_detection_model_insightscore >900` exemple

d. Dans les résultats, choisissez le résultat que vous avez créé pour votre cas d'utilisation, par exemple verify_customer. Un résultat est le résultat d'une prédiction de fraude et est renvoyé si la règle correspond lors d'une évaluation.

5. Choisissez Enregistrer la règle

Vous avez créé une nouvelle règle pour votre détecteur. Il s'agit de la version 1 de la règle qu'Amazon Fraud Detector met automatiquement à la disposition du détecteur pour qu'il puisse l'utiliser.

Créez une règle à l'aide du AWS SDK for Python (Boto3)

L'exemple de code suivant utilise CreateRulel'API pour créer une règle `high_risk` pour un détecteur existant`payments_detector`. L'exemple de code ajoute également une expression de règle et un résultat `verify_customer` à la règle.

Prérequis

Pour utiliser l'exemple de code, assurez-vous d'avoir effectué les opérations suivantes avant de créer des règles :

- Création d'un détecteur
- Créer un résultat

Si vous créez un détecteur, une règle et un résultat pour votre cas d'utilisation, remplacez l'exemple de nom de détecteur, de nom de règle, d'expression de règle et de nom de résultat par des noms et une expression correspondant à votre cas d'utilisation.

```
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']
)
```

Vous avez créé la version 1 de la règle qu'Amazon Fraud Detector met automatiquement à la disposition du détecteur pour qu'il puisse l'utiliser.

Mettre à jour la règle

Vous pouvez mettre à jour une règle à tout moment en ajoutant ou en mettant à jour la description de la règle, en mettant à jour l'expression de la règle ou en ajoutant ou en supprimant le résultat de la règle. Lorsque vous mettez à jour une règle, une nouvelle version de règle est créée.

Vous pouvez mettre à jour une règle dans la console Amazon Fraud Detector, à l'aide de la update-rule-versioncommande, de l'UpdateRuleVersionAPI ou du AWS SDK.

Après avoir mis à jour la règle, veillez à mettre à jour la version de votre détecteur pour utiliser la nouvelle version de la règle.

Mettre à jour la règle dans la console Amazon Fraud Detector

Pour mettre à jour une règle,

1. Ouvrez la console AWS de gestion et connectez-vous à votre compte. Accédez à Amazon Fraud Detector.
2. Dans le volet de navigation de gauche, choisissez Détecteurs.
3. Dans le volet Détecteurs, sélectionnez le détecteur associé à la règle que vous souhaitez mettre à jour.
4. Sur la page de votre détecteur, choisissez l'onglet Règles associées et sélectionnez la règle que vous souhaitez mettre à jour.
5. Sur votre page de règles, choisissez Actions, puis sélectionnez Créer une version.
6. Notez que la version a changé. Entrez une description, une expression ou un résultat mis à jour.
7. Choisissez Enregistrer la nouvelle version

Mettre à jour la règle à l'aide du AWS SDK for Python (Boto3)

L'exemple de code suivant utilise l'UpdateRuleVersionAPI pour mettre à jour le seuil de la règle `high_risk` de 900 à 950. Cette règle est associée au détecteur`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']
)
```

Listes

Une liste est un ensemble de données d'entrée pour une variable de votre jeu de données d'événements. Vous utilisez les données d'entrée dans une règle associée à votre détecteur. Une règle est une condition qui indique à Amazon Fraud Detector. Par exemple, vous pouvez créer une liste d'adresses IP, puis créer une règle pour refuser l'accès si une adresse IP spécifique figure dans la liste. Les règles qui utilisent des listes sont exprimées au`@list_name` format`$ip_address_value` in.

Avec Amazon Fraud Detector, vous pouvez gérer une liste en ajoutant ou en supprimant des données sans avoir à mettre à jour une règle associée. Une règle associée à votre liste intègre automatiquement les données récemment ajoutées ou supprimées.

Une liste peut contenir jusqu'à 100 000 entrées uniques et chaque entrée peut comporter jusqu'à 320 caractères. Chaque liste que vous utilisez dans une règle est, par défaut, associée àTypes de variables FREE_FORM_TEXT d'Amazon Fraud Detector. Vous pouvez attribuer un type de variable à votre liste à tout moment. Vous pouvez utiliser jusqu'à 3 listes dans une règle.

Vous pouvez créer une liste, ajouter des entrées à la liste, supprimer une liste ou supprimer une ou plusieurs entrées de la liste, ou attribuer un type de variable à votre liste dans la console Amazon Fraud Detector, à l'aide de l'APIAWS CLI, du ou duAWS SDK.

Création d'une liste

Vous pouvez créer une liste contenant les données d'entrée (entrées) d'une variable dans votre jeu de données d'événements et utiliser cette liste dans l'expression de la règle. Les entrées de la liste peuvent être gérées dynamiquement sans mettre à jour la règle qui utilise la liste.

Pour créer une liste, vous devez d'abord spécifier un nom, puis éventuellement associer la liste à un nomTypes de variables pris en charge par Amazon Fraud Detector. Par défaut, Amazon Fraud Detector suppose que la liste est de type variable FREE_FORM_TEXT.

Vous pouvez créer une liste dans la console Amazon Fraud Detector à l'aide de l'APIAWS CLI, du ou duAWS SDK.

Création d'une liste à l'aide de la console Amazon Fraud Detector

Pour créer une liste

1. Ouvrez la consoleAWS de gestion et connectez-vous à votre compte. Accédez à Amazon Fraud Detector.
2. Dans le volet de navigation, choisissez Listes.
3. Sous Détails des listes
   a. Dans le champ Nom de la liste, entrez un nom pour votre liste.
   b. Dans la zone Description, entrez une description.
   c. (Facultatif) Dans le champ Type de variable, sélectionnez un type de variable pour votre liste.

   > **Important**
   >
   > Si votre liste contient des adresses IP, veillez à sélectionner IP_ADDRESS comme type de variable. Si vous ne sélectionnez aucun type de variable, Amazon Fraud Detector suppose que la liste est du type de variable FREE_FORM_TEXT.

4. Dans le champ Ajouter des données de liste, ajoutez des entrées de liste, une entrée par ligne. Vous pouvez également copier et coller des entrées à partir d'une feuille de calcul.

> **Note**
>
> Assurez-vous que les entrées ne sont pas séparées par une virgule et qu'elles sont uniques dans la liste. Si deux entrées identiques sont saisies, une seule sera ajoutée.

5. Sélectionnez Create (Créer).

Créez une liste à l'aide duAWS SDK for Python (Boto3)

Vous créez une liste en spécifiant un nom de liste. Vous pouvez éventuellement fournir une description, associer un type de variable ou ajouter des entrées à votre liste lorsque vous créez une liste. Vous pouvez également mettre à jour la liste ultérieurement en ajoutant des entrées ou une description. Vous pouvez attribuer un type de variable à la liste ultérieurement si vous ne l'avez pas attribué au moment de la création de la liste. Le type de variable d'une liste ne peut pas être modifié.

> **Important**
>
> Si votre liste contient des adresses IP, veillez à attribuer IP_ADDRESS comme type de variable. Si vous n'attribuez aucun type de variable, Amazon Fraud Detector suppose que la liste est du type de variable FREE_FORM_TEXT.

L'exemple suivant utilise une opération d'CreateListAPI pour créer une`allow_email_ids` liste en fournissant une description, un type de variable et en ajoutant quatre entrées de liste.

```
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']
     )
```

Ajouter des entrées dans une liste

Après avoir créé votre liste, vous pouvez ajouter ou ajouter des entrées à votre liste à tout moment. Lorsque vous ajoutez ou ajoutez des entrées à votre liste, vous n'avez pas besoin de mettre à jour la règle à laquelle la liste est associée. La règle intègre automatiquement les entrées nouvellement ajoutées.

Votre liste peut contenir jusqu'à 100 000 entrées uniques et chaque entrée peut comporter jusqu'à 320 caractères.

Vous pouvez ajouter des entrées dans la console Amazon Fraud Detector, à l'aide de l'APIAWS CLI, du ou à l'aide duAWS SDK.

Ajoutez des entrées à une liste à l'aide de la console Amazon Fraud Detector

Pour ajouter une ou plusieurs entrées dans une liste

1. Ouvrez la consoleAWS de gestion et connectez-vous à votre compte. Accédez à Amazon Fraud Detector.
2. Dans le volet de navigation, choisissez Listes.
3. Sur la page Listes, sélectionnez la liste à laquelle vous souhaitez ajouter des entrées.
4. Sur la page de détails de votre liste, sélectionnez l'onglet Données de liste et choisissez Ajouter des données.
5. Dans la zone Ajouter des données de liste, ajoutez une entrée sur chaque ligne ou copiez-collez des entrées à partir d'une feuille de calcul. Veillez à ne pas utiliser de virgule pour séparer les entrées.
6. Choisissez Add (Ajouter).

Ajoutez des entrées à une liste à l'aide duAWS SDK for Python (Boto3)

L'exemple suivant utilise l'opération d'UpdateListAPI pour ajouter deux nouvelles entrées à la`allow_email_ids` liste. Assurez-vous que les entrées que vous ajoutez sont uniques dans la liste.

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

fraudDetector.update_list (
```

```
    name = 'allow_email_ids',
    updateMode = 'APPEND'
    elements = ['emailId_11','emailId_12']
```

Attribuer un type de variable à une liste

Chaque liste que vous utilisez dans une règle doit être associée au type deTypes de variables variable Amazon Fraud Detector. Par défaut, Amazon Fraud Detector suppose que la liste est de type variable FREE_FORM_TEXT. Il est important de noter qu'une liste composée d'adresses IP doit être associée au type de variable IP_ADDRESS.

Vous pouvez associer votre liste à un type de variable au moment de la création de la liste ou ultérieurement. Si vous avez déjà associé votre liste à un type de variable et que vous souhaitez le modifier ultérieurement, vous devez créer une nouvelle liste. Vous ne pouvez pas modifier le type de variable d'une liste.

Vous pouvez attribuer un type de variable dans la console Amazon Fraud Detector, à l'aide de l'APIAWS CLI, du ou duAWS SDK.

Attribuer un type de variable à une liste à l'aide de la console Amazon Fraud Detector

Pour attribuer un type de variable à une liste

1. Ouvrez la consoleAWS de gestion et connectez-vous à votre compte. Accédez à Amazon Fraud Detector.
2. Dans le volet de navigation, choisissez Listes.
3. Sur la page Listes, sélectionnez la liste à laquelle vous souhaitez attribuer un type de variable.
4. Sur la page de détails de votre liste, choisissez Actions, puis sélectionnez Modifier la liste.
5. Dans la zone de liste Modifier, sélectionnez le type de variable pour votre liste.
6. Choisissez Save (Enregistrer).

Attribuez un type de variable à une liste à l'aide duAWS SDK for Python (Boto3)

L'exemple suivant utilise l'opération UpdateListd'API pour attribuer un type de variable à la`allow_ip_address` liste.

```
import boto3
```

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

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

Supprimer une liste

Vous pouvez supprimer une liste qui n'est utilisée dans aucune règle. Lorsque vous supprimez une liste, Amazon Fraud Detector supprime définitivement cette liste ainsi que toutes les entrées qu'elle contient.

Vous pouvez supprimer une liste dans la console Amazon Fraud Detector, à l'aide de l'APIAWS CLI ou duAWS SDK.

Supprimer la liste à l'aide de la console Amazon Fraud Detector

Pour supprimer une liste

1. Ouvrez la consoleAWS de gestion et connectez-vous à votre compte. Accédez à Amazon Fraud Detector.
2. Dans le volet de navigation, choisissez Listes.
3. Sur la page Listes, sélectionnez la liste que vous souhaitez supprimer.
4. Sur la page de détails de votre liste, choisissez Actions, puis sélectionnez Supprimer la liste.
5. Choisissez Supprimer la liste.

Supprimer la liste à l'aide duAWS SDK for Python (Boto3)

L'exemple suivant utilise l'opération DeleteListd'API pour supprimer`allow_email_ids`.

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

Supprimer des entrées d'une liste

Vous pouvez supprimer une ou plusieurs entrées de vos listes. Lorsque vous supprimez des entrées de votre liste, il n'est pas nécessaire de mettre à jour la règle à laquelle la liste est associée. La règle intègre automatiquement la liste mise à jour.

Vous pouvez supprimer des entrées d'une liste dans la console Amazon Fraud Detector, à l'aide de l'APIAWS CLI ou duAWS SDK.

Supprimer des entrées d'une liste à l'aide de la console Amazon Fraud Detector

Pour supprimer une ou plusieurs entrées d'une liste

1. Ouvrez la consoleAWS de gestion et connectez-vous à votre compte. Accédez à Amazon Fraud Detector.
2. Dans le volet de navigation, choisissez Listes.
3. Sur la page Listes, sélectionnez la liste qui contient les entrées que vous souhaitez supprimer.
4. Sur la page de détails de votre liste, sélectionnez l'onglet Données de la liste et sélectionnez les entrées que vous souhaitez supprimer.
5. Choisissez Supprimer, puis choisissez à nouveau Supprimer pour confirmer.

Supprimez des entrées d'une liste à l'aide duAWS SDK for Python (Boto3)

Dans l'exemple suivant, l'opération UpdateListd'API supprime des entrées de`allow_email_ids` la liste.

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

Supprimer toutes les entrées d'une liste

Vous pouvez supprimer toutes les entrées de votre liste, si la liste n'est pas utilisée dans une règle. Vous pouvez supprimer toutes les entrées de la liste et ajouter ultérieurement des entrées dans la même liste.

Vous pouvez supprimer des entrées d'une liste dans la console Amazon Fraud Detector, à l'aide de l'APIAWS CLI ou duAWS SDK.

Supprimer toutes les entrées d'une liste à l'aide de la console Amazon Fraud Detector

Pour supprimer toutes les entrées d'une liste

1. Ouvrez la consoleAWS de gestion et connectez-vous à votre compte. Accédez à Amazon Fraud Detector.
2. Dans le volet de navigation, choisissez Listes.
3. Sur la page Listes, sélectionnez la liste qui contient les entrées que vous souhaitez supprimer.
4. Sur la page de détails de votre liste, sélectionnez l'onglet Données de liste et choisissez Supprimer tout.
5. Dans la zone Supprimer tout, tapez`delete all` pour confirmer, puis choisissez Supprimer toutes les données de la liste.

Supprimez toutes les entrées d'une liste à l'aide duAWS SDK for Python (Boto3)

Dans l'exemple suivant, l'opération UpdateListd'API supprime toutes les entrées de`allow_email_ids` la liste.

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

Résultats

Un résultat est le résultat d'une prédiction de fraude. Vous pouvez créer un résultat pour chaque résultat de prédiction de fraude possible. Par exemple, vous souhaiterez peut-être que les résultats représentent des niveaux de risque (risque élevé, risque moyen et risque faible) ou des actions (approbation, révision). Après avoir créé un résultat, vous pouvez ajouter un ou plusieurs résultats à une règle. Dans le cadre de la GetEventPredictionréponse, Amazon Fraud Detector renvoie les résultats définis pour toute règle correspondante.

Créer un résultat

Vous pouvez créer des résultats dans la console Amazon Fraud Detector, à l'aide de la commande put-outcome, de l'PutOutcomeAPI ou duAWS SDK for Python (Boto3).

Créez un résultat à l'aide de la console Amazon Fraud Detector

Pour créer un ou plusieurs résultats,

1. Ouvrez la consoleAWS de gestion et connectez-vous à votre compte. Accédez à Fraud Detector.
2. Dans le panneau de navigation de gauche, choisissez Résultats.
3. Sur la page Résultats, choisissez Créer.
4. Dans votre page Nouveau résultat, saisissez les informations suivantes :
    a. Dans le nom du résultat, entrez le nom de votre résultat.
    b. Dans la description du résultat, vous pouvez ajouter une description.
5. Choisissez Enregistrer le résultat.
6. Répétez les étapes 2 à 5 pour créer des résultats supplémentaires.

Créez un résultat à l'aide duAWS SDK for Python (Boto3)

L'exemple suivant utilise l'`PutOutcome`API pour créer trois résultats. Ils sont`verify_customerreview`, et`approve`. Une fois les résultats créés, vous pouvez les attribuer à des règles.

```
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'
)
```

Supprimer un résultat

Vous ne pouvez pas supprimer un résultat utilisé dans une version de règle.

Lorsque vous supprimez un résultat, Amazon Fraud Detector supprime définitivement ce résultat et les données ne sont plus stockées dans Amazon Fraud Detector.

Vous pouvez supprimer un résultat dans la console Amazon Fraud Detector, à l'aide de la commande delete-outcome, de l'DeleteOutcomeAPI ou duAWS SDK for Python (Boto3)

Supprimer un résultat dans la console Amazon Fraud Detector

Pour supprimer un résultat

1. Connectez-vous àAWS Management Console et ouvrez la console Amazon Fraud Detector https://console.aws.amazon.com/frauddetector
2. Dans le volet de navigation gauche de la console Amazon Fraud Detector, choisissez Ressources, puis Résultats.
3. Choisissez le résultat que vous voulez supprimer.
4. Choisissez Actions, puis Delete (Supprimer).
5. Entrez le nom du résultat, puis choisissez Supprimer le résultat.

Supprimer un résultat à l'aide duAWS SDK for Python (Boto3)

L'exemple suivant utilise l'DeleteOutcomeAPI pour supprimer le`verify_customer` résultat. Une fois le résultat supprimé, vous ne pouvez plus l'affecter à une règle.

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

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

Entité

Une entité représente une personne ou un objet qui réalise l'événement. Un type d'entité classe l'entité. Les exemples de classifications incluent le client, le vendeur, l'utilisateur ou le compte. Vous fournissez le type d'entité (ENTITY_TYPE) et un identifiant d'entité (ENTITY_ID) dans le cadre de votre jeu de données d'événements afin d'indiquer l'entité spécifique qui a réalisé l'événement.

Amazon Fraud Detector utilise le type d'entité lors de la génération d'une prédiction de fraude pour un événement afin d'indiquer qui l'a réalisé. Le type d'entité que vous souhaitez utiliser dans vos prévisions de fraude doit d'abord être créé dans Amazon Fraud Detector, puis ajouté à l'événement lors de la création de votre type d'événement.

Création d'un type d'entité

Vous pouvez créer un type d'entité dans la console Amazon Fraud Detector à l'aide de la put-entity-typecommande, de l'PutEntityTypeAPI ou duAWS SDK for Python (Boto3). Les exemples ci-dessous créent un type d'entité`customer` dans la console Amazon Fraud Detector et à l'aide du kit SDK for Python (Boto3). Si vous créez un type d'entité à associer à un type d'événement pour former un modèle de détection des fraudes, utilisez le type d'entité de votre jeu de données d'événements qui convient à votre cas d'utilisation.

Création d'un type d'entité à l'aide de la console Amazon Fraud Detector

Pour créer un type d'entité,

1. Ouvrez la consoleAWS de gestion et connectez-vous à votre compte.
2. Accédez à Amazon Fraud Detector, choisissez Entités dans le menu de navigation de gauche, puis choisissez Créer.
3. Sur la page Créer une entité, saisissez client comme nom de type d'entité. Si vous le souhaitez, saisissez une description de l'entité.

4. Choisissez Create entity (Créer une entité).

Créez un type d'entité à l'aide duAWS SDK for Python (Boto3)

L'exemple deAWS SDK for Python (Boto3) code suivant utilise l'`PutEntityType`API pour créer un type d'entité`customer`. Si vous créez un type d'entité à associer à un type d'événement pour former un modèle de détection des fraudes, utilisez l'entité de votre jeu de données d'événements qui convient à votre cas d'utilisation.

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

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

Supprimer un type d'entité

Dans Amazon Fraud Detector, vous ne pouvez pas supprimer un type d'entité inclus dans un type d'événement. Vous devez d'abord supprimer le type d'événement auquel l'entité est associée, puis supprimer le type d'entité.

Lorsque vous supprimez un type d'entité, Amazon Fraud Detector supprime définitivement ce type d'entité et les données ne sont plus stockées dans Amazon Fraud Detector.

Un type d'entité peut être supprimé dans la console Amazon Fraud Detector à l'aide de la delete-entity-typecommande, de l'DeleteEntityTypeAPI ou duAWS SDK for Python (Boto3)

Supprimer un type d'entité dans la console Amazon Fraud Detector

Pour supprimer un type d'entité,

1. Connectez-vous auAWS Management Console et ouvrez la console Amazon Fraud Detector à l'adresse https://console.aws.amazon.com/frauddetector.
2. Dans le volet de navigation gauche de la console Amazon Fraud Detector, choisissez Ressources, puis Entités.
3. Choisissez le type d'entité que vous voulez supprimer.
4. Choisissez Actions, puis Delete (Supprimer).

5. Entrez le nom du type d'entité, puis choisissez Supprimer le type d'entité.

Supprimez le type d'entité à l'aide duAWS SDK for Python (Boto3)

L'AWS SDK for Python (Boto3)exemple de code suivant supprime le type d'entité client à l'aide de l'DeleteEntityTypeAPI.

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

fraudDetector.delete_entity_type (

name = 'customer'

)
```

Gérez les ressources d'Amazon Fraud Detector avecAWS CloudFormation

Claud Fraud Detector Fraud DetectorAWS CloudFormation Vous créez un modèle qui décrit toutesAWS CloudFormation les ressources Amazon EntityType EventType Vous pouvez réutiliser le modèle pour provisionner et configurer les ressources de manière de manière et de manière répétée dans plusieurs comptes et régions AWS.

L'utilisation d'AWS n'implique aucun coût supplémentaire pour l'utilisation d'AWS CloudFormation.

Fraud Detector

Pour provisionner Fraud Detector configurer des ressources AWS CloudFormationpour Amazon Les modèles sont des fichiers texte formatés en JSON ou YAML. Ces modèles décrivent les ressources que vous souhaitez allouer dans vos piles AWS CloudFormation. Si JSON ou YAML ne vous est pas familier, vous pouvez utiliser AWS CloudFormation Designer pour vous aider à démarrer avec des modèles AWS CloudFormation. Pour plus d'informations, consultez Qu'est-ce que AWS CloudFormation Designer ? dans le AWS CloudFormationGuide de l'utilisateur.

Vous pouvez également créer, mettre à jour et supprimer vosAWS CloudFormation ressources Amazon Pour plus d'informations, y compris des exemples de modèles Jaud aud aud aud aud aud

aud aud aud aud aud aud aud aud aud aud aud aud aud aud aud aud aud aud aud aud aud aud aud aud aud aud aud aud aud aud aud aud aud aud aud aud aud aud aud aud audAWS CloudFormation

Si vous l'utilisez déjà CloudFormation, il n'est pas nécessaire de gérer des politiques IAM ou une CloudTrail journalisation supplémentaires.

Gestion Fraud Detector de Amazon

Vous pouvez créer, mettre à jour et supprimer vos piles Amazon Fraud Detector via la CloudFormation console ou via l'AWS CLI.

Pour créer une pile, vous devez disposer d'un modèle qui décrit les ressources qu'AWS CloudFormation inclura dans votre pile. Vous pouvez également CloudFormation gérer les ressources Amazon Fraud Detector que vous avez déjà créées en les important dans une pile nouvelle ou existante.

Pour obtenir des instructions détaillées sur la gestion de vos piles, consultez le Guide deAWS CloudFormation l'utilisateur pour savoir comment créer, mettre à jour et supprimer des piles.

Claud aud aud aud aud aud aud aud aud aud aud aud aud

La façon dont vous organisez vosAWS CloudFormation piles dépend entièrement de vous. Il est généralement recommandé d'organiser les piles par cycle de vie et par propriété. Cela implique de regrouper les ressources en fonction de leur fréquence de modification ou par équipes chargées de les mettre à jour.

Vous pouvez choisir d'organiser vos piles en créant une pile pour chaque détecteur et sa logique de détection (par exemple, règles, variables, etc.). Si vous utilisez d'autres services, vous devez déterminer si vous souhaitez associer les ressources Amazon Fraud Detector à des ressources provenant d'autres services. Par exemple, vous pouvez créer une pile qui inclut des ressources Kinesis qui aident à collecter des données et des ressources Amazon Fraud Detector qui traitent les données. Cela peut être un moyen efficace de garantir que tous les produits de votre équipe de lutte contre la fraude fonctionnent ensemble.

Présentation des Fraud Detector CloudFormation Amazon

Outre les paramètres standard disponibles dans tous les CloudFormation modèles, Amazon Fraud Detector introduit deux paramètres supplémentaires qui vous aideront à gérer le comportement de déploiement. Si vous n'incluez pas l'un de ces paramètres ou les deux, CloudFormation vous utiliserez la valeur par défaut ci-dessous.

Paramètre	Valeurs	Valeur par défaut
DetectorVersionStatus	ACTIF : Réglez la version actualisée ou mise à jour du détecteur sur le statut Actif BROUILLON : Réglez la version nouvelle/mise à jour du détecteur sur le statut Brouillon	ÉBAUCHE
En ligne	TRaud : permet CloudFormation de créer, mettre à jour ou supprimer la ressource lors de la création, de la mise à jour ou de la suppression de la pile. FALSE : CloudFormation Permet de valider l'existence de l'objet sans y apporter de modifications.	TRUE

ExempleAWS CloudFormation de modèle de modèle pour Amazon

Vous trouverez ci-dessous un exemple de modèleAWS CloudFormation YAML pour gérer un détecteur et les versions de détecteurs qui lui sont associées.

```
# 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'
```

En savoir plus sur AWS CloudFormation

Pour en savoir plus sur AWS CloudFormation, consultez les ressources suivantes :

- AWS CloudFormation
- Guide de l'utilisateur AWS CloudFormation
- Référence API AWS CloudFormation
- Guide de l'utilisateur de l'interface de ligne de commande AWS CloudFormation

Prédictions de fraude

Vous pouvez utiliser Amazon Fraud Detector pour obtenir des prévisions de fraude pour un seul événement en temps réel ou pour obtenir des prévisions de fraude hors ligne pour un ensemble d'événements. Pour générer des prévisions de fraude pour un seul événement ou pour un ensemble d'événements, vous devez fournir à Amazon Fraud Detector les informations suivantes :

- Logique de prédiction des fraudes
- Métadonnées des événements

Logique de détection des fraudes

La logique de prédiction de fraude utilise une ou plusieurs règles pour évaluer les données associées à un événement, puis fournit un résultat et un score de prédiction de fraude. Vous créez votre logique de prédiction des fraudes à l'aide des composants suivants :

- Types d'événements : définit la structure de l'événement
- Modèles - Définit les exigences en matière d'algorithmes et de données pour prévoir la fraude
- Variables : représente un élément de données associé à l'événement
- Règles : indique à Amazon Fraud Detector comment interpréter les valeurs des variables lors d'une prédiction de fraude
- Résultats : résultats générés à partir d'une prédiction de fraude
- Version Detector : contient une logique de prédiction de fraude pour un événement particulier

Pour plus d'informations sur les composants utilisés pour créer une logique de détection des fraudes, consultez les concepts d'Amazon Fraud Detector. Avant de commencer à générer des prévisions de fraude, assurez-vous d'avoir créé et publié la version du détecteur qui contient votre logique de prédiction des fraudes. Vous pouvez créer et publier la version du détecteur à l'aide de la console ou de l'API Fraud Detector. Pour des instructions sur l'utilisation de la console, consultez la section Mise en route (console). Pour obtenir des instructions sur l'utilisation de l'API, voir Créer une version de détecteur.

Métadonnées de l'événement

Les métadonnées de l'événement fournissent des détails sur l'événement en cours d'évaluation. Chaque événement que vous souhaitez évaluer doit inclure une valeur pour chaque variable du type

d'événement associé à la version de votre détecteur. En outre, les métadonnées de votre événement doivent inclure les éléments suivants :

- EVENT_ID — Identifiant de l'événement. Par exemple, si votre événement est une transaction en ligne, l'EVENT_ID peut être le numéro de référence de transaction fourni à votre client.

  Remarques importantes concernant EVENT_ID
  - Doit être unique pour cet événement
  - Doit représenter des informations importantes pour votre entreprise
  - Doit respecter le modèle d'expression régulière :`^[0-9a-z_-]+$.`
  - Doit être enregistré. EVENT_ID est la référence de l'événement et est utilisé pour effectuer des opérations sur l'événement, telles que la suppression de l'événement.
  - Il n'est pas recommandé d'ajouter un horodatage à l'EVENT_ID car cela pourrait entraîner des problèmes lorsque vous souhaiterez ultérieurement mettre à jour l'événement, car vous devrez fournir exactement le même EVENT_ID.
- ENTITY_TYPE — Entité qui réalise l'événement, par exemple un commerçant ou un client.
- ENTITY_ID : identifiant de l'entité exécutant l'événement. L'ENTITY_ID doit satisfaire au modèle d'expression régulière suivant :`^[0-9a-z_-]+$`. Si l'ENTITY_ID n'est pas disponible au moment de l'évaluation, transmettez la chaîne inconnue.
- EVENT_TIMESTAMP - Moment où l'événement est survenu. L'horodatage doit être conforme à la norme ISO 8601 en UTC.

Prédiction en temps réel

Vous pouvez évaluer les activités en ligne pour détecter les fraudes en temps réel en appelant`GetEventPrediction` l'API. Vous fournissez des informations sur un événement unique dans chaque demande et recevez de manière synchrone un score de modèle et un résultat basés sur la logique de prédiction de fraude associée au détecteur spécifié.

Comment fonctionne la prédiction des fraudes en temps réel

L'`GetEventPrediction`API utilise une version de détecteur spécifiée pour évaluer les métadonnées d'événement fournies pour l'événement. Au cours de l'évaluation, Amazon Fraud Detector génère d'abord les scores des modèles ajoutés à la version du détecteur, puis transmet les résultats aux règles pour évaluation. Les règles sont exécutées comme spécifié par le mode d'exécution des règles (voir Création d'une version de détecteur). Dans le cadre de la réponse,

Amazon Fraud Detector fournit les scores des modèles ainsi que tous les résultats associés aux règles correspondantes.

Obtenir des prévisions de fraude en temps réel

Pour obtenir des prévisions de fraude en temps réel, assurez-vous d'avoir créé et publié un détecteur contenant votre modèle et vos règles de prédiction des fraudes, ou simplement un ensemble de règles.

Vous pouvez obtenir des prévisions de fraude pour un événement en temps réel en appelant l'opération d'GetEventPredictionAPI à l'aide de l'interface de ligne deAWS commande (AWSCLI) ou de l'un des SDK Amazon Fraud Detector.

Pour utiliser l'API, fournissez les informations relatives à un événement unique à chaque demande. Dans le cadre de la demande, vous devez spécifier`detectorId` qu'Amazon Fraud Detector utilisera pour évaluer l'événement. Le cas échéant, vous pouvez spécifier un`detectorVersionId`. Si aucun n'`detectorVersionId`est spécifié, Amazon Fraud Detector utilisera la`ACTIVE` version du détecteur.

Vous pouvez éventuellement envoyer des données pour appeler un SageMaker modèle en transmettant les données dans le champ`externalModelEndpointBlobs`.

Obtenez une prévision de fraude à l'aide duAWS SDK for Python (Boto3)

Pour générer une prédiction de fraude, appelez l'`GetEventPrediction`API. L'exemple ci-dessous suppose que vous avez terminéPartie B : Générer des prévisions de fraude. Dans le cadre de la réponse, vous recevrez un score modèle ainsi que toutes les règles correspondantes et les résultats correspondants. Vous trouverez d'autres exemples de`GetEventPrediction` demandes dans le aws-fraud-detector-samples GitHub référentiel.

```
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'
}
)
```

Des prédictions par lots

Vous pouvez utiliser une tâche de prévision par lots dans Amazon Fraud Detector pour obtenir des prévisions pour un ensemble d'événements qui ne nécessitent pas de notation en temps réel. Par exemple, vous pouvez créer une tâche de prévision par lots pour effectuer une tâche hors ligne proof-of-concept ou pour évaluer rétrospectivement le risque d'événements sur une base horaire, quotidienne ou hebdomadaire.

Vous pouvez créer une tâche de prédiction par lots à l'aide de la console Amazon Fraud Detector ou en appelant l'opération d'CreateBatchPredictionJobAPI à l'aide de l'interface de ligne de AWS commande (AWSCLI) ou de l'un des kits SDK Amazon Fraud Detector.

Rubriques

- Comment fonctionnent les prédictions par lots
- Fichiers d'entrée et de sortie
- Obtenir des prévisions par lots
- Guide sur les rôles IAM
- Obtenez des prévisions de fraude par lots à l'aide du AWS SDK for Python (Boto3)

Comment fonctionnent les prédictions par lots

L'opération d'`CreateBatchPredictionJob`API utilise une version de détecteur spécifiée pour effectuer des prédictions sur la base des données fournies dans un fichier CSV d'entrée situé dans un compartiment Amazon S3. L'API renvoie ensuite le fichier ACL dans un compartiment S3.

Les tâches de prédiction Batch calculent les scores du modèle et les résultats des prévisions de la même manière que l'`GetEventPrediction`opération. De la même manière`GetEventPrediction`, pour créer une tâche de prévision par lots, vous devez d'abord créer un type d'événement, éventuellement entraîner un modèle, puis créer une version de détecteur qui évalue les événements de votre travail par lots.

Le prix des scores de risque d'événement évalués par des tâches de prédiction par lots est le même que celui des scores créés par l'`GetEventPrediction`API. Pour en savoir plus, consultez la tarification d'Amazon Fraud Detector.

Vous ne pouvez exécuter qu'une seule tâche de prédiction par lots à la fois.

Fichiers d'entrée et de sortie

Le fichier CSV d'entrée doit contenir des en-têtes correspondant au type d'événement associé à la version du détecteur sélectionnée. Taille maximale du fichier de données en entrée est de 1 Go. Le nombre d'événements varie en fonction de la taille de votre événement.

Amazon Fraud Detector crée le fichier de sortie dans le même compartiment que le fichier d'entrée, sauf si vous spécifiez un emplacement distinct pour les données de sortie. Le fichier de sortie contient les données d'origine du fichier d'entrée et les colonnes ajoutées suivantes :

- `MODEL_SCORES`— Détaille les scores du modèle pour l'événement à partir de chaque modèle associé à la version de détecteur sélectionnée.
- `OUTCOMES`— Détaille les résultats de l'événement tels qu'évalués par la version du détecteur sélectionnée et ses règles.
- `STATUS`— Indique si l'événement a été évalué avec succès. Si l'événement n'a pas été évalué correctement, cette colonne affiche le code de raison de l'échec.
- `RULE_RESULTS`— Liste de toutes les règles correspondantes, en fonction du mode d'exécution des règles.

Obtenir des prévisions par lots

Les étapes suivantes supposent que vous avez déjà créé un type d'événement, entraîné un modèle à l'aide de ce type d'événement (facultatif) et créé une version de détecteur pour ce type d'événement.

Pour une prévision par lots

1. Connectez-vous à la AWS Management Console et ouvrez la console Amazon Fraud Detector Detecket à l'adresse https://console.aws.amazon.com/frauddetector.
2. Dans le volet de navigation de gauche de la console Amazon Fraud Detector, choisissez Prédictions Batch, puis sélectionnez Nouvelle prédiction par lots.
3. Dans Nom de la Job, spécifiez le nom de votre tâche de prédiction par lots. Si vous ne spécifiez pas de nom, Amazon Fraud Detector génère un nom de tâche de manière aléatoire.

4. Dans Detector, choisissez le détecteur pour cette prédiction par lots.
5. Dans Version Detector, choisissez la version du détecteur pour cette prédiction par lots. Vous pouvez choisir une version du détecteur dans n'importe quel statut. Si l'`Active`état de votre détecteur est associé à une version de détecteur, cette version est automatiquement sélectionnée, mais vous pouvez également modifier cette sélection si nécessaire.
6. Dans le rôle IAM, choisissez ou créez un rôle disposant d'un accès en lecture et en écriture à vos compartiments Amazon S3 en entrée et en sortie. Pour en savoir plus, consultez Guide sur les rôles IAM.

   Pour obtenir des prévisions par lots, le rôle IAM qui appelle l'`CreateBatchPredictionJob`opération doit disposer d'autorisations de lecture sur votre compartiment S3 d'entrée et d'autorisations d'écriture sur votre compartiment S3 de sortie. Pour plus d'informations sur les autorisations relatives aux compartiments, consultez des exemples de politique utilisateur dans le Guide de l'utilisateur Amazon S3.
7. Dans Emplacement des données d'entrée, spécifiez l'emplacement Amazon S3 de vos données d'entrée. Si vous souhaitez que le fichier de sortie se trouve dans un autre compartiment S3, sélectionnez Emplacement de données séparé pour la sortie et indiquez l'emplacement Amazon S3 pour vos données de sortie.
8. (Facultatif) Créez des balises pour votre tâche de prédiction par lots.
9. Sélectionnez Démarrer.

   Amazon Fraud Detector crée la tâche de prédiction par lots, et le statut de la tâche est`In progress`. Les délais de traitement des tâches de prédiction par Batch varient en fonction du nombre d'événements et de la configuration de la version de votre détecteur.

Pour arrêter une tâche de prédiction par lots en cours, accédez à la page détaillée de la tâche de prédiction par lots, choisissez Actions, puis choisissez Arrêter la prédiction par lots. Si vous arrêtez une tâche de prédiction par lots, vous ne recevrez aucun résultat pour cette tâche.

Lorsque le statut de la tâche de prédiction par lots passe à`Complete`, vous pouvez récupérer la sortie de la tâche à partir du compartiment de sortie Amazon S3 désigné. Le nom du fichier de sortie est au format`batch prediction job name_file creation timestamp_output.csv`. Par exemple, le fichier de sortie d'une tâche nommée `mybatchjob` est`mybatchjob_1611170650_output.csv`.

Pour rechercher des événements spécifiques évalués par une tâche de prédiction par lots, dans le volet de navigation de gauche de la console Amazon Fraud Detector, sélectionnez Rechercher les prédictions passées.

Pour supprimer une tâche de prédiction par lots terminée, accédez à la page détaillée de la tâche de prédiction par lots, choisissez Actions, puis choisissez Supprimer la prédiction par lots.

Guide sur les rôles IAM

Pour obtenir des prévisions par lots, le rôle IAM qui appelle l'CreateBatchPredictionJobopération doit disposer d'autorisations de lecture sur votre compartiment S3 d'entrée et d'autorisations d'écriture sur votre compartiment S3 de sortie. Pour plus d'informations sur les listes ACL dans le Guide de l'utilisateur Amazon S3. Sur la console Amazon Fraud Detector, vous disposez de trois options pour sélectionner un rôle IAM pour les prévisions Batch :

1. Créez un rôle lors de la création d'une nouvelle tâche de prédiction Batch.
2. Sélectionnez un rôle IAM existant que vous avez précédemment créé dans la console Amazon Fraud Detector. Assurez-vous d'ajouter l'`S3:PutObject`autorisation au rôle avant de procéder à cette étape.
3. Entrez un ARN personnalisé pour un rôle IAM créé précédemment.

Si vous recevez une erreur liée à votre rôle IAM, effectuez les vérifications suivantes :

1. Vos compartiments d'entrée et de sortie Amazon S3 se trouvent dans la même région que votre détecteur.
2. Le rôle IAM que vous utilisez possède l'`s3:GetObject`autorisation pour votre compartiment S3 d'entrée et l'`s3:PutObject`autorisation pour votre compartiment S3 de sortie.
3. Le rôle IAM que vous utilisez est associé à une politique de confiance pour le principal `frauddetector.amazonaws.com` de service.

Obtenez des prévisions de fraude par lots à l'aide du AWS SDK for Python (Boto3)

L'exemple suivant montre un exemple de demande pour l'CreateBatchPredictionJobAPI. Une tâche de prédiction par lots doit inclure les ressources existantes suivantes : détecteur, version du détecteur et nom du type d'événement. L'exemple suivant suppose que vous avez créé un

type d'événementsample_registration, un détecteur sample_detector et une version du détecteur1.

```
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-
**'
)
```

Explications des prédictions

Les explications de prédiction fournissent un aperçu de l'impact de chaque variable d'événement sur le score de prédiction de fraude de votre modèle et sont automatiquement générées dans le cadre de la prédiction de fraude. Chaque prédiction de fraude est assortie d'un score de risque compris entre 1 et 1 000. Les explications relatives aux prévisions vous donnent des détails sur l'influence de chaque variable d'événement sur les scores de risque en termes d'ampleur (0-5, 5 étant le plus élevé) et de direction (score d'entraînement supérieur ou inférieur). Vous pouvez également utiliser les explications des prédictions pour les tâches suivantes :

- Identifier les principaux indicateurs de risque lors d'enquêtes manuelles lorsqu'un événement est signalé pour examen.
- Déterminer les causes profondes qui mènent à des prédictions faussement positives (par exemple, des scores de risque élevés pour des événements légitimes).
- Pour analyser les modèles de fraude dans les données relatives aux événements et détecter les biais éventuels dans votre ensemble de données.

> **Important**
>
> Les explications des prédictions sont générées automatiquement et disponibles uniquement pour les modèles entraînés le 30 juin 2021 ou après cette date. Pour recevoir des explications de prédiction pour les modèles entraînés avant le 30 juin 2021, réentraînez ces modèles.

Les explications de prédiction fournissent l'ensemble de valeurs suivant pour chaque variable d'événement utilisée pour entraîner le modèle.

Impact relatif

Fournit une référence visuelle de l'impact de la variable en termes d'ampleur sur les scores de prédiction des fraudes. Les valeurs d'impact relatives se composent d'une note par étoiles (0-5, 5 étant la valeur la plus élevée) et de l'impact directionnel (augmenté/diminué) du risque de fraude.

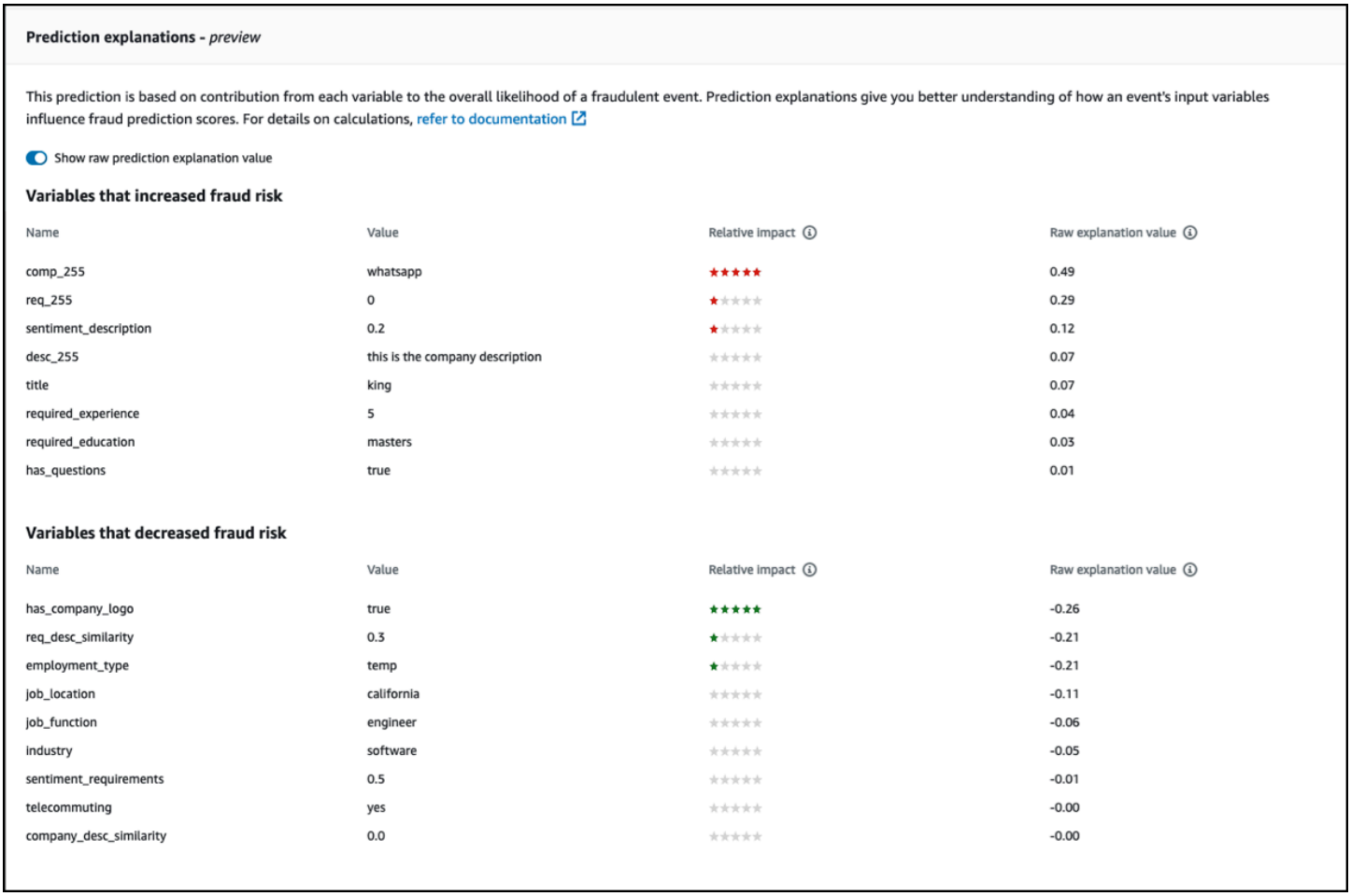
- Les variables qui augmentent le risque de fraude sont indiquées par des étoiles rouges. Plus le nombre d'étoiles rouges est élevé, plus la variable augmente le score de fraude et augmente le risque de fraude.
- Les variables qui réduisent le risque de fraude sont indiquées par des étoiles vertes. Plus le nombre de démarrages de couleur verte est élevé, plus la variable fait baisser le score de risque de fraude et la probabilité de fraude.
- Le zéro étoile pour toutes les variables indique qu'aucune des variables à elle seule n'a modifié de manière significative le risque de fraude.

Valeur explicative brute

Fournit une valeur brute non interprétée, représentée sous forme de cotes logarithmiques de fraude. Ces valeurs sont généralement comprises entre -10 et +10, mais elles vont de - infini à + infini.

- Une valeur positive indique que la variable a fait grimper le score de risque.
- Une valeur négative indique que la variable a fait baisser le score de risque.

Dans la console Amazon Fraud Detector, les valeurs explicatives des prédictions sont affichées comme suit. Le nombre d'étoiles en couleur et les valeurs numériques brutes correspondantes permettent de voir facilement l'influence relative entre les variables.



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

Afficher les explications des prédictions

Après avoir généré des prédictions de fraude, vous pouvez consulter les explications des prédictions dans la console Amazon Fraud Detector. Pour afficher les explications des prédictions à l'aide des API du AWS SDK, vous devez d'abord appeler l'`ListEventPrediction`API pour obtenir l'horodatage de l'événement, puis appeler l'`GetEventPredictionMetadata`API pour obtenir les explications des prédictions.

Afficher les explications relatives aux prédictions à l'aide de la console Amazon Fraud Detector

Pour consulter les explications des prédictions à l'aide de la console,

1. Ouvrez la AWS console et connectez-vous à votre compte. Accédez à Amazon Fraud Detector.
2. Dans le volet de navigation de gauche, choisissez Rechercher dans les prédictions passées.

3. Utilisez les filtres Propriété, Opérateur et Valeur pour sélectionner la prédiction que vous souhaitez examiner.
4. Dans le volet supérieur du filtre, assurez-vous de sélectionner la période pendant laquelle la prédiction que vous souhaitez examiner a été générée.
5. Le volet Résultats affiche la liste de toutes les prédictions générées pendant la période spécifiée. Cliquez sur l'ID d'événement de la prédiction pour afficher les explications de la prédiction.
6. Faites défiler la page vers le bas jusqu'au volet Explications des prédictions.
7. Activez le bouton Afficher la valeur d'explication de prédiction brute pour afficher la valeur d'explication de prédiction brute de toutes les variables.

Afficher les explications relatives aux prédictions à l'aide du kit SDK AWS pour Python (Boto3)

Les exemples suivants présentent des exemples de demandes d'affichage des explications relatives aux prédictions à `ListEventPredictions` l'aide des `GetEventPredictionMetadata` API du AWS SDK.

Exemple 1 : obtenir une liste des prédictions les plus récentes à l'aide de l'**`ListEventPredictions`**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'
    }
 )
```

Exemple 2 ; Obtenir une liste des prédictions passées pour le type d'événement « enregistrement » à l'aide de l'**`ListEventPredictions`**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'
    }
 )
```

Exemple 3 : obtenir les détails d'une prédiction passée pour un ID d'événement, un type d'événement, un ID de détecteur et un ID de version de détecteur spécifiés qui a été générée au cours de la période spécifiée à l'aide de l'**`GetEventPredictionMetadata`**API.

Le `predictionTimestamp` paramètre spécifié pour cette demande est obtenu en appelant d'abord l'`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'
 )
```

Comprendre comment les explications des prédictions sont calculées

Amazon Fraud Detector utilise SHAP (ShapeLey Additive Explanations) pour expliquer les prédictions d'événements individuels en calculant les valeurs explicatives brutes de chaque variable d'événement utilisée pour l'entraînement du modèle. Les valeurs explicatives brutes sont calculées par le modèle dans le cadre de l'algorithme de classification lors de la génération de prédictions. Ces valeurs explicatives brutes représentent la contribution de chaque entrée au logarithme des probabilités de fraude. Les valeurs explicatives brutes (de -infinity à +infinity) sont converties en une valeur d'impact relative (-5 à +5) à l'aide d'un mappage. La valeur d'impact relative dérivée de la valeur d'explication brute représente le nombre de fois où le risque de fraude (positif) ou légitime (négatif) augmente, ce qui facilite la compréhension des explications des prédictions.

Sécurité dans Amazon Fraud Detector

La sécurité du cloud AWS est la priorité absolue. En tant que AWS client, vous bénéficiez de centres de données et d'architectures réseau conçus pour répondre aux exigences des entreprises les plus sensibles en matière de sécurité.

La sécurité est une responsabilité partagée entre vous AWS et vous. Le modèle de responsabilité partagée décrit cela comme la sécurité du cloud et la sécurité dans le cloud :

- Sécurité du cloud : AWS est chargée de protéger l'infrastructure qui exécute les AWS services dans le AWS cloud. AWS vous fournit également des services que vous pouvez utiliser en toute sécurité. Des auditeurs tiers testent et vérifient régulièrement l'efficacité de notre sécurité dans le cadre des programmes de AWS conformité Programmes de de conformité. Pour en savoir plus sur les programmes de conformité applicables à Amazon Fraud Detector, consultez AWS Services in Scope in Scope by Compliance Program .
- Sécurité dans le cloud — Votre responsabilité est déterminée par le AWS service que vous utilisez. Vous êtes également responsable d'autres facteurs, y compris de la sensibilité de vos données, des exigences de votre entreprise, ainsi que de la législation et de la réglementation applicables.

Cette documentation vous aide à comprendre comment appliquer le modèle de responsabilité partagée lors de l'utilisation d'Amazon Fraud Detector. Les rubriques suivantes expliquent comment configurer Amazon Fraud Detector pour atteindre vos objectifs de sécurité et de conformité. Vous apprendrez également à utiliser d'autres AWS services qui vous aident à surveiller et à sécuriser vos ressources Amazon Fraud Detector.

Rubriques

Protection des données dans Amazon Fraud Detector

Le modèle de responsabilité AWS partagée Le modèle s'applique à la protection des données dans Amazon Fraud Detector. Comme décrit dans ce modèle, AWS est chargé de protéger l'infrastructure mondiale qui gère tous les AWS Cloud. La gestion du contrôle de votre contenu hébergé sur cette infrastructure relève de votre responsabilité. Vous êtes également responsable des tâches de configuration et de gestion de la sécurité des Services AWS que vous utilisez. Pour plus d'informations sur la confidentialité des données, consultez Questions fréquentes (FAQ) sur la confidentialité des données. Pour en savoir plus sur la protection des données en Europe, consultez le billet de blog Modèle de responsabilité partagée AWS et RGPD (Règlement général sur la protection des données) sur le Blog de sécuritéAWS .

À des fins de protection des données, nous vous recommandons de protéger les Compte AWS informations d'identification et de configurer les utilisateurs individuels avec AWS IAM Identity Center ou AWS Identity and Access Management (IAM). Ainsi, chaque utilisateur se voit attribuer uniquement les autorisations nécessaires pour exécuter ses tâches. Nous vous recommandons également de sécuriser vos données comme indiqué ci-dessous :

- Utilisez l'authentification multifactorielle (MFA) avec chaque compte.
- Utilisez le protocole SSL/TLS pour communiquer avec les ressources. AWS Nous exigeons TLS 1.2 et recommandons TLS 1.3.
- Configurez l'API et la journalisation de l'activité des utilisateurs avec AWS CloudTrail.
- Utilisez des solutions de AWS chiffrement, ainsi que tous les contrôles de sécurité par défaut qu'ils contiennent Services AWS.
- Utilisez des services de sécurité gérés avancés tels qu'Amazon Macie, qui contribuent à la découverte et à la sécurisation des données sensibles stockées dans Amazon S3.
- Si vous avez besoin de modules cryptographiques validés par la norme FIPS 140-2 pour accéder AWS via une interface de ligne de commande ou une API, utilisez un point de terminaison FIPS. Pour plus d'informations sur les points de terminaison FIPS (Federal Information Processing Standard) disponibles, consultez Federal Information Processing Standard (FIPS) 140-2 (Normes de traitement de l'information fédérale).

Nous vous recommandons fortement de ne jamais placer d'informations confidentielles ou sensibles, telles que les adresses e-mail de vos clients, dans des balises ou des champs de texte libre tels que le champ Name (Nom). Cela inclut lorsque vous travaillez avec Amazon Fraud Detector ou une autre solution Services AWS à l'aide de la console AWS CLI, de l'API ou AWS des SDK. Toutes

les données que vous entrez dans des balises ou des champs de texte de forme libre utilisés pour les noms peuvent être utilisées à des fins de facturation ou dans les journaux de diagnostic. Si vous fournissez une adresse URL à un serveur externe, nous vous recommandons fortement de ne pas inclure d'informations d'identification dans l'adresse URL permettant de valider votre demande adressée à ce serveur.

Chiffrement de données au repos

Amazon Fraud Detector chiffre vos données inactives à l'aide de la clé de chiffrement de votre choix. Vous pouvez choisir l'une des méthodes suivantes.

- Une AWS clé KMS que vous possédez. Si vous ne spécifiez pas de clé de chiffrement, vos données sont chiffrées avec cette clé par défaut.
- Une clé KMS gérée par le client. Vous pouvez contrôler l'accès à votre clé KMS gérée par le client à l'aide de politiques clés. Pour plus d'informations sur la création et la gestion d'une clé KMS gérée par le client, consultezGestion des clés.

chiffrement des données en transit

Amazon Fraud Detector copie les données de votre compte et les traite dans un AWS système interne. Par défaut, Amazon Fraud Detector utilise le protocole TLS 1.2 avec AWS des certificats pour chiffrer les données en transit.

Gestion des clés

Amazon Fraud Detector chiffre vos données à l'aide de l'un des deux types de clés suivants :

- Une AWS clé KMS que vous possédez. Il s'agit de l'option par défaut.
- Une clé KMS gérée par le client.

Création d'une clé KMS gérée par le client

Vous pouvez créer une clé KMS gérée par le client à l'aide de la console AWS KMS ou de l'CreateKeyAPI. Lors de la création de la clé, assurez-vous que

- Sélectionnez une clé KMS de chiffrement symétrique gérée par le client, Amazon Fraud Detector ne prend pas en charge les clés KMS asymétriques. Pour plus d'informations, voir Asymmetric Keys AWS KMS dans le guide du développeur du service de gestion des AWS clés.

- Créez une clé KMS pour une seule région. Amazon Fraud Detector ne prend pas en charge les clés KMS multirégionales. Pour plus d'informations, consultez la section Clés multirégionales AWS KMS dans le Guide du développeur du service de gestion des AWS clés.
- Fournissez la politique clé suivante pour autoriser Amazon Fraud Detector à utiliser la clé.

```
        {
    "Effect": "Allow",
    "Principal": {
        "Service": "frauddetector.amazonaws.com"
    },
    "Action": [
        "kms:Encrypt",
        "kms:Decrypt",
        "kms:ReEncrypt*",
        "kms:GenerateDataKey*",
        "kms:DescribeKey",
        "kms:CreateGrant",
        "kms:RetireGrant"
    ],
    "Resource": "*"
}
```

Pour plus d'informations sur les politiques clés, consultez la section Utilisation des politiques clés dans AWS KMS dans le Guide du développeur du service de gestion des AWS clés.

Chiffrement des données à l'aide d'une clé KMS gérée par le client

Utilisez l'EncryptionKeyAPI PutKMS d'Amazon Fraud Detector pour chiffrer vos données Amazon Fraud Detector au repos à l'aide de la clé KMS gérée par le client. Vous pouvez modifier la configuration du chiffrement à tout moment à l'aide de l'`PutKMSEncryptionKey`API.

Remarques importantes concernant les données cryptées

- Les données générées après la configuration de la clé KMS gérée par le client sont cryptées. Les données générées avant la configuration de la clé KMS gérée par le client ne seront pas chiffrées.
- Si la clé KMS gérée par le client est modifiée, les données chiffrées à l'aide de la configuration de chiffrement précédente ne seront pas rechiffrées.

Affichage des données

Lorsque vous utilisez une clé KMS gérée par le client pour chiffrer vos données Amazon Fraud Detector, les données chiffrées à l'aide de cette méthode ne sont pas consultables à l'aide de filtres dans la zone Search Past Predictions de la console Amazon Fraud Detector. Pour garantir des résultats de recherche complets, utilisez une ou plusieurs des propriétés suivantes pour filtrer les résultats :

- ID de l'événement
- Horodatage de l'évaluation
- État du détecteur
- Version du détecteur
- Version du modèle
- Type de modèle
- État de l'évaluation des règles
- Mode d'exécution des règles
- État de correspondance des règles
- Version de la règle
- Source de données variable

Si la clé KMS gérée par le client a été supprimée ou doit être supprimée, il est possible que vos données ne soient pas disponibles. Pour plus d'informations, consultez la section Suppression de la clé KMS.

Amazon Fraud Detector et points de terminaison VPC d'interface ()AWS PrivateLink

Vous pouvez établir une connexion privée entre votre VPC et Amazon Fraud Detector en créant un point de terminaison VPC d'interface. Les points de terminaison de l'interface sont alimentés par AWS PrivateLinkune technologie qui vous permet d'accéder en privé aux API Amazon Fraud Detector sans passerelle Internet, appareil NAT, connexion VPN ou connexion AWS Direct Connect. Les instances de votre VPC n'ont pas besoin d'adresses IP publiques pour communiquer avec les API Amazon Fraud Detector. Le trafic entre votre VPC et Amazon Fraud Detector ne quitte pas le réseau Amazon.

Chaque point de terminaison d'interface est représenté par une ou plusieurs interfaces réseau Elastic dans vos sous-réseaux.

Pour plus d'informations, consultez la section Interface VPC endpoints (AWS PrivateLink) dans le guide de l'utilisateur Amazon VPC.

Considérations relatives aux points de terminaison VPC Amazon Fraud Detector

Avant de configurer un point de terminaison VPC d'interface pour Amazon Fraud Detector, assurez-vous de consulter les propriétés et les limites du point de terminaison d'interface dans le guide de l'utilisateur Amazon VPC.

Amazon Fraud Detector permet d'appeler toutes ses actions d'API depuis votre VPC.

Les politiques relatives aux points de terminaison VPC sont prises en charge pour Amazon Fraud Detector. Par défaut, l'accès complet à Amazon Fraud Detector est autorisé via le terminal. Pour plus d'informations, consultez Contrôle de l'accès aux services avec points de terminaison d'un VPC dans le Guide de l'utilisateur Amazon VPC.

Création d'un point de terminaison VPC d'interface pour Amazon Fraud Detector

Vous pouvez créer un point de terminaison VPC pour le service Amazon Fraud Detector à l'aide de la console Amazon VPC ou du (). AWS Command Line Interface AWS CLI Pour plus d'informations, consultez Création d'un point de terminaison d'interface dans le Guide de l'utilisateur Amazon VPC.

Créez un point de terminaison VPC pour Amazon Fraud Detector en utilisant le nom de service suivant :

- com.amazonaws.*region*.frauddetector

Si vous activez le DNS privé pour le point de terminaison, vous pouvez envoyer des demandes d'API à Amazon Fraud Detector en utilisant son nom DNS par défaut pour la région, par exemple,`frauddetector.us-east-1.amazonaws.com`.

Pour plus d'informations, consultez Accès à un service via un point de terminaison d'interface dans le Guide de l'utilisateur Amazon VPC.

Création d'une politique de point de terminaison VPC pour Amazon Fraud Detector

Vous pouvez créer une politique pour les points de terminaison VPC d'interface pour Amazon Fraud Detector afin de spécifier les éléments suivants :

- Le principal qui peut exécuter des actions.
- Les actions qui peuvent être effectuées.
- Les ressources sur lesquelles les actions peuvent être exécutées.

Pour en savoir plus, consultez Contrôle de l'accès aux services avec des points de terminaison d'un VPC dans le guide de l'utilisateur Amazon VPC.

L'exemple de politique de point de terminaison VPC suivant indique que tous les utilisateurs ayant accès au point de terminaison de l'interface VPC sont autorisés à accéder au détecteur Amazon Fraud Detector nommé. `my_detector`

```
{
  "Statement": [
      {
          "Action": "frauddetector:*Detector",
          "Effect": "Allow",
          "Resource": "arn:aws:frauddetector:us-east-1:123456789012:detector/
my_detector",
          "Principal": "*"
      }
  ]
}
```

Dans cet exemple, les éléments suivants sont refusés :

- Autres actions de l'API Amazon Fraud Detector
- Invocation de l'API Amazon Fraud Detector `GetEventPrediction`

> **Note**
>
> Dans cet exemple, les utilisateurs peuvent toujours effectuer d'autres actions de l'API Amazon Fraud Detector en dehors du VPC. Pour obtenir des informations sur la façon de restreindre les appels d'API à ceux situés dans le VPC, veuillez consulter Politiques basées sur l'identité d'Amazon Fraud Detector.

Refus d'utiliser vos données pour améliorer le service

Les données historiques des événements que vous fournissez pour entraîner les modèles et générer des prévisions sont utilisées uniquement pour fournir et maintenir votre service. Ces données peuvent également être utilisées pour améliorer la qualité d'Amazon Fraud Detector. Votre confiance, votre confidentialité et la sécurité de votre contenu sont nos priorités absolues et garantissent que notre utilisation est conforme à nos engagements envers vous. Consultez la FAQ sur la confidentialité des données pour plus d'informations

Vous pouvez choisir de ne pas utiliser les données de votre événement pour développer ou améliorer la qualité d'Amazon Fraud Detector en consultant la page des politiques de désinscription des services d'intelligence artificielle dans le guide de l'utilisateur d'AWS Organizations et en suivant le processus qui y est expliqué.

> **Note**
>
> Vos comptes AWS devront être gérés de manière centralisée par AWS Organizations pour que vous puissiez utiliser la politique de désinscription. Si vous n'avez pas encore créé d'organisation pour vos comptes AWS, consultez la page Création et gestion d'une organisation et suivez le processus qui y est expliqué.

Gestion des identités et des accès pour Amazon Fraud Detector

AWS Identity and Access Management (IAM) est un outil Service AWS qui permet à un administrateur de contrôler en toute sécurité l'accès aux AWS ressources. Les administrateurs IAM contrôlent qui peut être authentifié (connecté) et autorisé (autorisé) à utiliser les ressources Amazon Fraud Detector. IAM est un Service AWS outil que vous pouvez utiliser sans frais supplémentaires.

Rubriques

Public ciblé

La façon dont vous utilisez AWS Identity and Access Management (IAM) varie en fonction du travail que vous effectuez dans Amazon Fraud Detector.

Utilisateur du service — Si vous utilisez le service Amazon Fraud Detector dans le cadre de votre travail, votre administrateur vous fournit les informations d'identification et les autorisations dont vous avez besoin. Au fur et à mesure que vous utilisez les fonctionnalités d'Amazon Fraud Detector dans le cadre de votre travail, il se peut que vous ayez besoin d'autorisations supplémentaires. En comprenant bien la gestion des accès, vous saurez demander les autorisations appropriées à votre administrateur. Si vous ne parvenez pas à accéder à une fonctionnalité d'Amazon Fraud Detector, consultezRésolution des problèmes d'identité et d'accès à Amazon Fraud Detector.

Administrateur du service — Si vous êtes responsable des ressources Amazon Fraud Detector au sein de votre entreprise, vous avez probablement un accès complet à Amazon Fraud Detector. C'est à vous de déterminer les fonctionnalités et les ressources d'Amazon Fraud Detector auxquelles les utilisateurs de votre service doivent accéder. Vous devez ensuite soumettre les demandes à votre administrateur IAM pour modifier les autorisations des utilisateurs de votre service. Consultez les informations sur cette page pour comprendre les concepts de base d'IAM. Pour en savoir plus sur la manière dont votre entreprise peut utiliser l'IAM avec Amazon Fraud Detector, consultezComment Amazon Fraud Detector fonctionne avec IAM.

Administrateur IAM — Si vous êtes administrateur IAM, vous souhaiterez peut-être en savoir plus sur la manière dont vous pouvez rédiger des politiques pour gérer l'accès à Amazon Fraud Detector. Pour consulter des exemples de politiques basées sur l'identité d'Amazon Fraud Detector que vous pouvez utiliser dans IAM, consultez. Exemples de politiques basées sur l'identité d'Amazon Fraud Detector

Authentification par des identités

L'authentification est la façon dont vous vous connectez à AWS l'aide de vos informations d'identification. Vous devez être authentifié (connecté à AWS) en tant qu'utilisateur IAM ou en assumant un rôle IAM. Utilisateur racine d'un compte AWS

Vous pouvez vous connecter en AWS tant qu'identité fédérée en utilisant les informations d'identification fournies par le biais d'une source d'identité. AWS IAM Identity Center Les utilisateurs (IAM Identity Center), l'authentification unique de votre entreprise et vos informations d'identification Google ou Facebook sont des exemples d'identités fédérées. Lorsque vous vous connectez avec une identité fédérée, votre administrateur aura précédemment configuré une fédération d'identités avec

des rôles IAM. Lorsque vous accédez à AWS l'aide de la fédération, vous assumez indirectement un rôle.

Selon le type d'utilisateur que vous êtes, vous pouvez vous connecter au portail AWS Management Console ou au portail AWS d'accès. Pour plus d'informations sur la connexion à AWS, consultez la section Comment vous connecter à votre compte Compte AWS dans le guide de Connexion à AWS l'utilisateur.

Si vous y accédez AWS par programmation, AWS fournit un kit de développement logiciel (SDK) et une interface de ligne de commande (CLI) pour signer cryptographiquement vos demandes à l'aide de vos informations d'identification. Si vous n'utilisez pas d' AWS outils, vous devez signer vous-même les demandes. Pour plus d'informations sur l'utilisation de la méthode recommandée pour signer vous-même les demandes, consultez la section Signature des demandes AWS d'API dans le guide de l'utilisateur IAM.

Quelle que soit la méthode d'authentification que vous utilisez, vous devrez peut-être fournir des informations de sécurité supplémentaires. Par exemple, il vous AWS recommande d'utiliser l'authentification multifactorielle (MFA) pour renforcer la sécurité de votre compte. Pour en savoir plus, consultez Authentification multifactorielle dans le Guide de l'utilisateur AWS IAM Identity Center et Utilisation de l'authentification multifactorielle (MFA) dans l'interface AWS dans le Guide de l'utilisateur IAM.

Compte AWS utilisateur root

Lorsque vous créez un Compte AWS, vous commencez par une identité de connexion unique qui donne un accès complet à toutes Services AWS les ressources du compte. Cette identité est appelée utilisateur Compte AWS root et est accessible en vous connectant avec l'adresse e-mail et le mot de passe que vous avez utilisés pour créer le compte. Il est vivement recommandé de ne pas utiliser l'utilisateur racine pour vos tâches quotidiennes. Protégez vos informations d'identification d'utilisateur racine et utilisez-les pour effectuer les tâches que seul l'utilisateur racine peut effectuer. Pour obtenir la liste complète des tâches qui vous imposent de vous connecter en tant qu'utilisateur racine, veuillez consulter Tâches nécessitant les informations d'identification de l'utilisateur racine dans le Guide de l'utilisateur IAM.

Utilisateurs et groupes

Un utilisateur IAM est une identité au sein de vous Compte AWS qui possède des autorisations spécifiques pour une seule personne ou une seule application. Dans la mesure du possible, nous vous recommandons de vous appuyer sur des informations d'identification temporaires plutôt que

de créer des utilisateurs IAM ayant des informations d'identification à long terme tels que les clés d'accès. Toutefois, si certains cas d'utilisation spécifiques nécessitent des informations d'identification à long terme avec les utilisateurs IAM, nous vous recommandons de faire pivoter les clés d'accès. Pour plus d'informations, consultez Rotation régulière des clés d'accès pour les cas d'utilisation nécessitant des informations d'identification dans le Guide de l'utilisateur IAM.

Un groupe IAM est une identité qui concerne un ensemble d'utilisateurs IAM. Vous ne pouvez pas vous connecter en tant que groupe. Vous pouvez utiliser les groupes pour spécifier des autorisations pour plusieurs utilisateurs à la fois. Les groupes permettent de gérer plus facilement les autorisations pour de grands ensembles d'utilisateurs. Par exemple, vous pouvez avoir un groupe nommé IAMAdmins et accorder à ce groupe les autorisations d'administrer des ressources IAM.

Les utilisateurs sont différents des rôles. Un utilisateur est associé de manière unique à une personne ou une application, alors qu'un rôle est conçu pour être endossé par tout utilisateur qui en a besoin. Les utilisateurs disposent d'informations d'identification permanentes, mais les rôles fournissent des informations d'identification temporaires. Pour en savoir plus, consultez Quand créer un utilisateur IAM (au lieu d'un rôle) dans le Guide de l'utilisateur IAM.

Rôles IAM

Un rôle IAM est une identité au sein de vous Compte AWS dotée d'autorisations spécifiques. Le concept ressemble à celui d'utilisateur IAM, mais le rôle IAM n'est pas associé à une personne en particulier. Vous pouvez assumer temporairement un rôle IAM dans le en AWS Management Console changeant de rôle. Vous pouvez assumer un rôle en appelant une opération d' AWS API AWS CLI ou en utilisant une URL personnalisée. Pour plus d'informations sur les méthodes d'utilisation des rôles, consultez Utilisation de rôles IAM dans le Guide de l'utilisateur IAM.

Les rôles IAM avec des informations d'identification temporaires sont utiles dans les cas suivants :

- Accès utilisateur fédéré – Pour attribuer des autorisations à une identité fédérée, vous créez un rôle et définissez des autorisations pour le rôle. Quand une identité externe s'authentifie, l'identité est associée au rôle et reçoit les autorisations qui sont définies par celui-ci. Pour obtenir des informations sur les rôles pour la fédération, consultez Création d'un rôle pour un fournisseur d'identité tiers (fédération) dans le Guide de l'utilisateur IAM. Si vous utilisez IAM Identity Center, vous configurez un jeu d'autorisations. IAM Identity Center met en corrélation le jeu d'autorisations avec un rôle dans IAM afin de contrôler à quoi vos identités peuvent accéder après leur authentification. Pour plus d'informations sur les jeux d'autorisations, consultez la rubrique Jeux d'autorisations dans le Guide de l'utilisateur AWS IAM Identity Center .

- Autorisations d'utilisateur IAM temporaires : un rôle ou un utilisateur IAM peut endosser un rôle IAM pour profiter temporairement d'autorisations différentes pour une tâche spécifique.
- Accès intercompte : vous pouvez utiliser un rôle IAM pour permettre à un utilisateur (principal de confiance) d'un compte différent d'accéder aux ressources de votre compte. Les rôles constituent le principal moyen d'accorder l'accès intercompte. Toutefois, dans certains Services AWS cas, vous pouvez associer une politique directement à une ressource (au lieu d'utiliser un rôle comme proxy). Pour en savoir plus sur la différence entre les rôles et les politiques basées sur les ressources pour l'accès intercompte, consultez Différence entre les rôles IAM et les politiques basées sur les ressources dans le Guide de l'utilisateur IAM.
- Accès multiservices — Certains Services AWS utilisent des fonctionnalités dans d'autres Services AWS. Par exemple, lorsque vous effectuez un appel dans un service, il est courant que ce service exécute des applications dans Amazon EC2 ou stocke des objets dans Amazon S3. Un service peut le faire en utilisant les autorisations d'appel du principal, un rôle de service ou un rôle lié au service.
  - Sessions d'accès direct (FAS) : lorsque vous utilisez un utilisateur ou un rôle IAM pour effectuer des actions AWS, vous êtes considéré comme un mandant. Lorsque vous utilisez certains services, vous pouvez effectuer une action qui initie une autre action dans un autre service. FAS utilise les autorisations du principal appelant et Service AWS, associées Service AWS à la demande, pour adresser des demandes aux services en aval. Les demandes FAS ne sont effectuées que lorsqu'un service reçoit une demande qui nécessite des interactions avec d'autres personnes Services AWS ou des ressources pour être traitée. Dans ce cas, vous devez disposer d'autorisations nécessaires pour effectuer les deux actions. Pour plus de détails sur la politique relative à la transmission de demandes FAS, consultez Sessions de transmission d'accès.
  - Rôle de service : il s'agit d'un rôle IAM attribué à un service afin de réaliser des actions en votre nom. Un administrateur IAM peut créer, modifier et supprimer une fonction du service à partir d'IAM. Pour plus d'informations, consultez Création d'un rôle pour la délégation d'autorisations à un Service AWS dans le Guide de l'utilisateur IAM.
  - Rôle lié à un service — Un rôle lié à un service est un type de rôle de service lié à un. Service AWS Le service peut endosser le rôle afin d'effectuer une action en votre nom. Les rôles liés à un service apparaissent dans votre Compte AWS répertoire et appartiennent au service. Un administrateur IAM peut consulter, mais ne peut pas modifier, les autorisations concernant les rôles liés à un service.
- Applications exécutées sur Amazon EC2 : vous pouvez utiliser un rôle IAM pour gérer les informations d'identification temporaires pour les applications qui s'exécutent sur une instance EC2 et qui envoient des demandes d'API. AWS CLI AWS Cette solution est préférable au stockage

des clés d'accès au sein de l'instance EC2. Pour attribuer un AWS rôle à une instance EC2 et le mettre à la disposition de toutes ses applications, vous devez créer un profil d'instance attaché à l'instance. Un profil d'instance contient le rôle et permet aux programmes qui s'exécutent sur l'instance EC2 d'obtenir des informations d'identification temporaires. Pour plus d'informations, consultez Utilisation d'un rôle IAM pour accorder des autorisations à des applications s'exécutant sur des instances Amazon EC2 dans le Guide de l'utilisateur IAM.

Pour savoir dans quel cas utiliser des rôles ou des utilisateurs IAM, consultez Quand créer un rôle IAM (au lieu d'un utilisateur) dans le Guide de l'utilisateur IAM.

Gestion des accès à l'aide de politiques

Vous contrôlez l'accès en AWS créant des politiques et en les associant à AWS des identités ou à des ressources. Une politique est un objet AWS qui, lorsqu'il est associé à une identité ou à une ressource, définit leurs autorisations. AWS évalue ces politiques lorsqu'un principal (utilisateur, utilisateur root ou session de rôle) fait une demande. Les autorisations dans les politiques déterminent si la demande est autorisée ou refusée. La plupart des politiques sont stockées AWS sous forme de documents JSON. Pour plus d'informations sur la structure et le contenu des documents de politique JSON, consultez Vue d'ensemble des politiques JSON dans le Guide de l'utilisateur IAM.

Les administrateurs peuvent utiliser les politiques AWS JSON pour spécifier qui a accès à quoi. C'est-à-dire, quel principal peut effectuer des actions sur quelles ressources et dans quelles conditions.

Par défaut, les utilisateurs et les rôles ne disposent d'aucune autorisation. Pour octroyer aux utilisateurs des autorisations d'effectuer des actions sur les ressources dont ils ont besoin, un administrateur IAM peut créer des politiques IAM. L'administrateur peut ensuite ajouter les politiques IAM aux rôles et les utilisateurs peuvent assumer les rôles.

Les politiques IAM définissent les autorisations d'une action, quelle que soit la méthode que vous utilisez pour exécuter l'opération. Par exemple, supposons que vous disposiez d'une politique qui autorise l'action `iam:GetRole`. Un utilisateur appliquant cette politique peut obtenir des informations sur le rôle à partir de AWS Management Console AWS CLI, de ou de l' AWS API.

Politiques basées sur l'identité

Les politiques basées sur l'identité sont des documents de politique d'autorisations JSON que vous pouvez attacher à une identité telle qu'un utilisateur, un groupe d'utilisateurs ou un rôle IAM. Ces

politiques contrôlent quel type d'actions des utilisateurs et des rôles peuvent exécuter, sur quelles ressources et dans quelles conditions. Pour découvrir comment créer une politique basée sur l'identité, consultez Création de politiques IAM dans le Guide de l'utilisateur IAM.

Les politiques basées sur l'identité peuvent être classées comme des politiques en ligne ou des politiques gérées. Les politiques en ligne sont intégrées directement à un utilisateur, groupe ou rôle. Les politiques gérées sont des politiques autonomes que vous pouvez associer à plusieurs utilisateurs, groupes et rôles au sein de votre Compte AWS. Les politiques gérées incluent les politiques AWS gérées et les politiques gérées par le client. Pour découvrir comment choisir entre une politique gérée et une politique en ligne, consultez Choix entre les politiques gérées et les politiques en ligne dans le Guide de l'utilisateur IAM.

politiques basées sur les ressources

Les politiques basées sur les ressources sont des documents de politique JSON que vous attachez à une ressource. Des politiques basées sur les ressources sont, par exemple, les politiques de confiance de rôle IAM et des politiques de compartiment. Dans les services qui sont compatibles avec les politiques basées sur les ressources, les administrateurs de service peuvent les utiliser pour contrôler l'accès à une ressource spécifique. Pour la ressource dans laquelle se trouve la politique, cette dernière définit quel type d'actions un principal spécifié peut effectuer sur cette ressource et dans quelles conditions. Vous devez spécifier un principal dans une politique basée sur les ressources. Les principaux peuvent inclure des comptes, des utilisateurs, des rôles, des utilisateurs fédérés ou. Services AWS

Les politiques basées sur les ressources sont des politiques en ligne situées dans ce service. Vous ne pouvez pas utiliser les politiques AWS gérées par IAM dans une stratégie basée sur les ressources.

Listes de contrôle d'accès (ACL)

Les listes de contrôle d'accès (ACL) vérifie quels principals (membres de compte, utilisateurs ou rôles) ont l'autorisation d'accéder à une ressource. Les listes de contrôle d'accès sont similaires aux politiques basées sur les ressources, bien qu'elles n'utilisent pas le format de document de politique JSON.

Amazon S3 et Amazon VPC sont des exemples de services qui prennent en charge les ACL. AWS WAF Pour en savoir plus sur les listes de contrôle d'accès, consultez Vue d'ensemble des listes de contrôle d'accès (ACL) dans le Guide du développeur Amazon Simple Storage Service.

Autres types de politique

AWS prend en charge d'autres types de politiques moins courants. Ces types de politiques peuvent définir le nombre maximum d'autorisations qui vous sont accordées par des types de politiques plus courants.

- Limite d'autorisations : une limite d'autorisations est une fonctionnalité avancée dans laquelle vous définissez le nombre maximal d'autorisations qu'une politique basée sur l'identité peut accorder à une entité IAM (utilisateur ou rôle IAM). Vous pouvez définir une limite d'autorisations pour une entité. Les autorisations en résultant représentent la combinaison des politiques basées sur l'identité d'une entité et de ses limites d'autorisation. Les politiques basées sur les ressources qui spécifient l'utilisateur ou le rôle dans le champ `Principal` ne sont pas limitées par les limites d'autorisations. Un refus explicite dans l'une de ces politiques remplace l'autorisation. Pour plus d'informations sur les limites d'autorisations, consultez Limites d'autorisations pour des entités IAM dans le Guide de l'utilisateur IAM.
- Politiques de contrôle des services (SCP) — Les SCP sont des politiques JSON qui spécifient les autorisations maximales pour une organisation ou une unité organisationnelle (UO) dans. AWS Organizations AWS Organizations est un service permettant de regrouper et de gérer de manière centralisée Comptes AWS les multiples propriétés de votre entreprise. Si vous activez toutes les fonctionnalités d'une organisation, vous pouvez appliquer les politiques de contrôle des services (SCP) à l'un ou à l'ensemble de vos comptes. Le SCP limite les autorisations pour les entités figurant dans les comptes des membres, y compris chacune Utilisateur racine d'un compte AWS d'entre elles. Pour plus d'informations sur les organisations et les SCP, consultez Fonctionnement des SCP dans le Guide de l'utilisateur AWS Organizations .
- Politiques de séance : les politiques de séance sont des politiques avancées que vous utilisez en tant que paramètre lorsque vous créez par programmation une séance temporaire pour un rôle ou un utilisateur fédéré. Les autorisations de séance en résultant sont une combinaison des politiques basées sur l'identité de l'utilisateur ou du rôle et des politiques de séance. Les autorisations peuvent également provenir d'une politique basée sur les ressources. Un refus explicite dans l'une de ces politiques annule l'autorisation. Pour plus d'informations, consultez politiques de séance dans le Guide de l'utilisateur IAM.

Plusieurs types de politique

Lorsque plusieurs types de politiques s'appliquent à la requête, les autorisations en résultant sont plus compliquées à comprendre. Pour savoir comment AWS déterminer s'il faut autoriser

une demande lorsque plusieurs types de politiques sont impliqués, consultez la section Logique d'évaluation des politiques dans le guide de l'utilisateur IAM.

Comment Amazon Fraud Detector fonctionne avec IAM

Avant d'utiliser IAM pour gérer l'accès à Amazon Fraud Detector, vous devez connaître les fonctionnalités IAM disponibles avec Amazon Fraud Detector. Pour obtenir une vue d'ensemble de la manière dont Amazon Fraud Detector et les autres AWS services fonctionnent avec IAM, consultez la section AWS Services That Work with IAM dans le guide de l'utilisateur d'IAM.

Rubriques

- Politiques basées sur l'identité d'Amazon Fraud Detector
- Politiques basées sur les ressources d'Amazon Fraud Detector
- Autorisation basée sur les tags Amazon Fraud Detector
- Rôles IAM chez Amazon Fraud Detector

Politiques basées sur l'identité d'Amazon Fraud Detector

Avec les politiques IAM basées sur l'identité, vous pouvez spécifier des actions et ressources autorisées ou refusées, ainsi que les conditions dans lesquelles les actions sont autorisées ou refusées. Amazon Fraud Detector prend en charge des actions, des ressources et des clés de condition spécifiques. Pour en savoir plus sur tous les éléments que vous utilisez dans une politique JSON, consultez Références des éléments de politique JSON IAM dans le Guide de l'utilisateur IAM.

Pour commencer à utiliser Amazon Fraud Detector, nous vous recommandons de créer un utilisateur dont l'accès est limité aux opérations d'Amazon Fraud Detector et avec les autorisations requises. Vous pouvez ajouter d'autres autorisations selon vos besoins. Les politiques suivantes fournissent l'autorisation requise pour utiliser Amazon Fraud Detector : `AmazonFraudDetectorFullAccessPolicy` et`AmazonS3FullAccess`. Pour plus d'informations sur la configuration d'Amazon Fraud Detector à l'aide de ces politiques, consultezConfiguration d'Amazon Fraud Detector.

Actions

Les administrateurs peuvent utiliser les politiques AWS JSON pour spécifier qui a accès à quoi. C'est-à-dire, quel principal peut effectuer des actions sur quelles ressources et dans quelles conditions.

L'élément `Action` d'une politique JSON décrit les actions que vous pouvez utiliser pour autoriser ou refuser l'accès à une politique. Les actions de stratégie portent généralement le même nom que l'opération AWS d'API associée. Il existe quelques exceptions, telles que les actions avec autorisations uniquement qui n'ont pas d'opération API correspondante. Certaines opérations nécessitent également plusieurs actions dans une politique. Ces actions supplémentaires sont nommées actions dépendantes.

Intégration d'actions dans une stratégie afin d'accorder l'autorisation d'exécuter les opérations associées.

Les actions politiques dans Amazon Fraud Detector utilisent le préfixe suivant avant l'action :`frauddetector:`. Par exemple, pour créer une règle avec l'opération d'`CreateRule`API Amazon Fraud Detector, vous devez inclure l'`frauddetector:CreateRule`action dans la politique. Les déclarations de politique doivent inclure un élément `Action` ou `NotAction`. Amazon Fraud Detector définit son propre ensemble d'actions décrivant les tâches que vous pouvez effectuer avec ce service.

Pour spécifier plusieurs actions dans une seule déclaration, séparez-les par des virgules comme suit :

```
"Action": [
      "frauddetector:action1",
      "frauddetector:action2"
```

Vous pouvez aussi spécifier plusieurs actions à l'aide de caractères génériques (*). Par exemple, pour spécifier toutes les actions qui commencent par le mot `Describe`, incluez l'action suivante :

```
"Action": "frauddetector:Describe*"
```

Pour consulter la liste des actions d'Amazon Fraud Detector, consultez la section Actions définies par Amazon Fraud Detector dans le guide de l'utilisateur IAM.

Ressources

Les administrateurs peuvent utiliser les politiques AWS JSON pour spécifier qui a accès à quoi. C'est-à-dire, quel principal peut effectuer des actions sur quelles ressources et dans quelles conditions.

L'élément de politique JSON `Resource` indique le ou les objets auxquels l'action s'applique. Les instructions doivent inclure un élément `Resource` ou `NotResource`. Il est recommandé de définir

une ressource à l'aide de son Amazon Resource Name (ARN). Vous pouvez le faire pour des actions qui prennent en charge un type de ressource spécifique, connu sous la dénomination autorisations de niveau ressource.

Pour les actions qui ne sont pas compatibles avec les autorisations de niveau ressource, telles que les opérations de liste, utilisez un caractère générique (*) afin d'indiquer que l'instruction s'applique à toutes les ressources.

```
"Resource": "*"
```

Les types de ressources définis par Amazon Fraud Detector répertorie tous les ARN des ressources Amazon Fraud Detector.

Par exemple, pour spécifier le `my_detector` détecteur dans votre instruction, utilisez l'ARN suivant :

```
"Resource": "arn:aws:frauddetector:us-east-1:123456789012:detector/my_detector"
```

Pour plus d'informations sur le format des ARN, consultez Amazon Resource Names (ARN) et AWS Service Namespaces.

Pour spécifier tous les détecteurs appartenant à un compte spécifique, utilisez le caractère générique (*) :

```
"Resource": "arn:aws:frauddetector:us-east-1:123456789012:detector/*"
```

Certaines actions d'Amazon Fraud Detector, telles que celles relatives à la création de ressources, ne peuvent pas être effectuées sur une ressource spécifique. Dans ces cas-là, vous devez utiliser le caractère générique (*).

```
"Resource": "*"
```

Pour consulter la liste des types de ressources Amazon Fraud Detector et de leurs ARN, consultez la section Resources Defined by Amazon Fraud Detector dans le guide de l'utilisateur IAM. Pour savoir quelles actions vous pouvez spécifier l'ARN de chaque ressource, consultez Actions définies par Amazon Fraud Detector.

Clés de condition

Les administrateurs peuvent utiliser les politiques AWS JSON pour spécifier qui a accès à quoi. C'est-à-dire, quel principal peut effectuer des actions sur quelles ressources et dans quelles conditions.

L'élément `Condition` (ou le bloc `Condition`) vous permet de spécifier des conditions lorsqu'une instruction est appliquée. L'élément `Condition` est facultatif. Vous pouvez créer des expressions conditionnelles qui utilisent des opérateurs de condition, tels que les signes égal ou inférieur à, pour faire correspondre la condition de la politique aux valeurs de la demande.

Si vous spécifiez plusieurs éléments `Condition` dans une instruction, ou plusieurs clés dans un seul élément `Condition`, AWS les évalue à l'aide d'une opération `AND` logique. Si vous spécifiez plusieurs valeurs pour une seule clé de condition, AWS évalue la condition à l'aide d'une `OR` opération logique. Toutes les conditions doivent être remplies avant que les autorisations associées à l'instruction ne soient accordées.

Vous pouvez aussi utiliser des variables d'espace réservé quand vous spécifiez des conditions. Par exemple, vous pouvez accorder à un utilisateur IAM l'autorisation d'accéder à une ressource uniquement si elle est balisée avec son nom d'utilisateur IAM. Pour plus d'informations, consultez Éléments d'une politique IAM : variables et identifications dans le Guide de l'utilisateur IAM.

AWS prend en charge les clés de condition globales et les clés de condition spécifiques au service. Pour voir toutes les clés de condition AWS globales, voir les clés de contexte de condition AWS globales dans le guide de l'utilisateur IAM.

Amazon Fraud Detector définit son propre ensemble de clés de condition et prend également en charge l'utilisation de certaines clés de condition globales. Pour voir toutes les clés de condition AWS globales, consultez la section Clés contextuelles de condition AWS globale dans le guide de l'utilisateur IAM.

Pour consulter la liste des clés de condition d'Amazon Fraud Detector, consultez la section Condition Keys for Amazon Fraud Detector dans le guide de l'utilisateur IAM. Pour savoir quelles actions et ressources vous pouvez utiliser une clé de condition, consultez Actions Defined by Amazon Fraud Detector.

Exemples

Pour consulter des exemples de politiques basées sur l'identité d'Amazon Fraud Detector, consultez. Exemples de politiques basées sur l'identité d'Amazon Fraud Detector

Politiques basées sur les ressources d'Amazon Fraud Detector

Amazon Fraud Detector ne prend pas en charge les politiques basées sur les ressources.

Autorisation basée sur les tags Amazon Fraud Detector

Vous pouvez joindre des tags aux ressources Amazon Fraud Detector ou transmettre des tags dans une demande adressée à Amazon Fraud Detector. Pour contrôler l'accès basé sur des étiquettes, vous devez fournir les informations d'étiquette dans l'élément de condition d'une politique utilisant les clés de condition `aws:ResourceTag/key-name`, `aws:RequestTag/key-name` ou `aws:TagKeys`.

Rôles IAM chez Amazon Fraud Detector

Un rôle IAM est une entité de votre AWS compte qui possède des autorisations spécifiques.

Utilisation d'informations d'identification temporaires avec Amazon Fraud Detector

Vous pouvez utiliser des informations d'identification temporaires pour vous connecter à l'aide de la fédération, endosser un rôle IAM ou encore pour endosser un rôle intercompte. Vous obtenez des informations d'identification de sécurité temporaires en appelant des opérations d' AWS STS API telles que AssumeRoleou GetFederationToken.

Amazon Fraud Detector prend en charge l'utilisation d'informations d'identification temporaires.

Rôles liés à un service

Les rôles liés aux AWS services permettent aux services d'accéder aux ressources d'autres services pour effectuer une action en votre nom. Les rôles liés à un service s'affichent dans votre compte IAM et sont la propriété du service. Un administrateur IAM peut consulter, mais ne peut pas modifier, les autorisations concernant les rôles liés à un service.

Amazon Fraud Detector ne prend pas en charge les rôles liés à un service.

Rôles de service

Cette fonction permet à un service d'endosser une fonction du service en votre nom. Ce rôle autorise le service à accéder à des ressources d'autres services pour effectuer une action en votre nom. Les rôles de service s'affichent dans votre compte et sont la propriété du compte. Cela signifie qu'un administrateur peut modifier les autorisations associées à ce rôle. Toutefois, une telle action peut perturber le bon fonctionnement du service.

Amazon Fraud Detector prend en charge les rôles de service.

Exemples de politiques basées sur l'identité d'Amazon Fraud Detector

Par défaut, les utilisateurs et les rôles IAM ne sont pas autorisés à créer ou à modifier les ressources Amazon Fraud Detector. Ils ne peuvent pas non plus effectuer de tâches à l'aide de l' AWS API AWS Management Console AWS CLI, ou. Un administrateur doit créer des politiques IAM autorisant les utilisateurs et les rôles à exécuter des opérations d'API spécifiques sur les ressources spécifiées dont ils ont besoin. Il doit ensuite attacher ces stratégies aux utilisateurs ou aux groupes ayant besoin de ces autorisations.

Pour savoir comment créer une politique IAM basée sur l'identité à l'aide de ces exemples de documents de politique JSON, consultez Création de politiques dans l'onglet JSON dans le Guide de l'utilisateur IAM.

Rubriques

Bonnes pratiques en matière de politiques

Les politiques basées sur l'identité déterminent si quelqu'un peut créer, accéder ou supprimer les ressources Amazon Fraud Detector de votre compte. Ces actions peuvent entraîner des frais pour votre Compte AWS. Lorsque vous créez ou modifiez des politiques basées sur l'identité, suivez ces instructions et recommandations :

- Commencez AWS par les politiques gérées et passez aux autorisations du moindre privilège : pour commencer à accorder des autorisations à vos utilisateurs et à vos charges de travail, utilisez les politiques AWS gérées qui accordent des autorisations pour de nombreux cas d'utilisation courants. Ils sont disponibles dans votre Compte AWS. Nous vous recommandons de réduire

davantage les autorisations en définissant des politiques gérées par les AWS clients spécifiques à vos cas d'utilisation. Pour plus d'informations, consultez politiques gérées par AWS ou politiques gérées par AWS pour les activités professionnelles dans le Guide de l'utilisateur IAM.

- Accorder les autorisations de moindre privilège : lorsque vous définissez des autorisations avec des politiques IAM, accordez uniquement les autorisations nécessaires à l'exécution d'une seule tâche. Pour ce faire, vous définissez les actions qui peuvent être entreprises sur des ressources spécifiques dans des conditions spécifiques, également appelées autorisations de moindre privilège. Pour plus d'informations sur l'utilisation de IAM pour appliquer des autorisations, consultez politiques et autorisations dans IAM dans le Guide de l'utilisateur IAM.
- Utiliser des conditions dans les politiques IAM pour restreindre davantage l'accès : vous pouvez ajouter une condition à vos politiques afin de limiter l'accès aux actions et aux ressources. Par exemple, vous pouvez écrire une condition de politique pour spécifier que toutes les demandes doivent être envoyées via SSL. Vous pouvez également utiliser des conditions pour accorder l'accès aux actions de service si elles sont utilisées par le biais d'un service spécifique Service AWS, tel que AWS CloudFormation. Pour plus d'informations, consultez Conditions pour éléments de politique JSON IAM dans le Guide de l'utilisateur IAM.
- Utilisez IAM Access Analyzer pour valider vos politiques IAM afin de garantir des autorisations sécurisées et fonctionnelles : IAM Access Analyzer valide les politiques nouvelles et existantes de manière à ce que les politiques IAM respectent le langage de politique IAM (JSON) et les bonnes pratiques IAM. IAM Access Analyzer fournit plus de 100 vérifications de politiques et des recommandations exploitables pour vous aider à créer des politiques sécurisées et fonctionnelles. Pour plus d'informations, consultez Validation de politique IAM Access Analyzer dans le Guide de l'utilisateur IAM.
- Exiger l'authentification multifactorielle (MFA) : si vous avez un scénario qui nécessite des utilisateurs IAM ou un utilisateur root, activez l'authentification MFA pour une sécurité accrue. Compte AWS Pour exiger le MFA lorsque des opérations d'API sont appelées, ajoutez des conditions MFA à vos politiques. Pour plus d'informations, consultez Configuration de l'accès aux API protégé par MFA dans le Guide de l'utilisateur IAM.

Pour plus d'informations sur les bonnes pratiques dans IAM, consultez Bonnes pratiques de sécurité dans IAM dans le Guide de l'utilisateur IAM.

Politique (prédéfinie) gérée par AWS pour Amazon Fraud Detector

AWS répond à de nombreux cas d'utilisation courants en fournissant des politiques IAM autonomes créées et administrées par. AWS Ces politiques AWS gérées accordent les autorisations nécessaires

pour les cas d'utilisation courants afin que vous puissiez éviter d'avoir à rechercher les autorisations nécessaires. Pour plus d'informations, consultez les politiques gérées par AWS dans le guide AWS Identity and Access Management de l'utilisateur de gestion.

La politique AWS gérée suivante, que vous pouvez associer aux utilisateurs de votre compte, est spécifique à Amazon Fraud Detector :

`AmazonFraudDetectorFullAccess`: accorde un accès complet aux ressources, aux actions et aux opérations prises en charge par Amazon Fraud Detector, notamment :

- Répertorier et décrire tous les points de terminaison du modèle sur Amazon SageMaker
- Répertorier tous les rôles IAM du compte
- Répertorier tous les compartiments Amazon S3
- Autoriser le rôle IAM Pass à transmettre un rôle à Amazon Fraud Detector

Cette politique ne fournit pas un accès illimité à S3. Si vous devez télécharger des ensembles de données d'entraînement de modèles vers S3, la politique `AmazonS3FullAccess` gérée (ou la politique d'accès Amazon S3 personnalisée et délimitée) est également requise.

Vous pouvez consulter les autorisations de la politique en vous connectant à la console IAM et en effectuant une recherche par nom de politique. Vous pouvez également créer vos propres politiques IAM personnalisées pour autoriser les actions et les ressources d'Amazon Fraud Detector selon vos besoins. Vous pouvez attacher ces stratégies personnalisées aux utilisateurs ou groupes qui les nécessitent.

Autorisation accordée aux utilisateurs pour afficher leurs propres autorisations

Cet exemple montre comment créer une politique qui permet aux utilisateurs IAM d'afficher les politiques en ligne et gérées attachées à leur identité d'utilisateur. Cette politique inclut les autorisations permettant d'effectuer cette action sur la console ou par programmation à l'aide de l'API AWS CLI or 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": "*"
        }
    ]
}
```

Autoriser un accès complet aux ressources d'Amazon Fraud Detector

L'exemple suivant donne à un utilisateur un accès Compte AWS complet à toutes les ressources et actions d'Amazon Fraud Detector.

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Action": [
                "frauddetector:*"
            ],
            "Resource": "*"
        }
    ]
```

```
}
```

Autoriser l'accès en lecture seule aux ressources d'Amazon Fraud Detector

Dans cet exemple, vous accordez à un utilisateur un accès en Compte AWS lecture seule à vos ressources 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": "*"
        }
    ]
}
```

Autoriser l'accès à une ressource spécifique

Dans cet exemple de politique au niveau des ressources, vous accordez à un utilisateur l' Compte AWS accès à toutes les actions et ressources, à l'exception d'une ressource Detector en particulier.

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Action": [
                "frauddetector:*"
            ],
            "Resource": "*"
        },
        {
            "Effect": "Deny",
            "Action": [
                "frauddetector:*Detector"
            ],
            "Resource": "arn:${Partition}:frauddetector:${Region}:${Account}:detector/
${detector-name}"
        }
    ]
}
```

Autoriser l'accès à des ressources spécifiques lors de l'utilisation de l'API bimode

Amazon Fraud Detector fournit des API Get bimode qui fonctionnent à la fois comme des opérations List et Describe. Une API bimode, lorsqu'elle est appelée sans aucun paramètre, renvoie une liste des ressources spécifiées associées à votre Compte AWS. Lorsqu'elle est appelée avec un paramètre, une API bimode renvoie les détails de la ressource spécifiée. Les ressources peuvent être des modèles, des variables, des types d'événements ou des types d'entités.

Les API bimodes prennent en charge les autorisations au niveau des ressources dans les politiques IAM. Toutefois, les autorisations au niveau des ressources ne sont appliquées que lorsqu'un ou plusieurs paramètres sont fournis dans le cadre de la demande. Par exemple, si l'utilisateur appelle l'GetVariablesAPI et fournit un nom de variable et si une politique IAM Deny est attachée à la ressource variable ou au nom de variable, l'utilisateur recevra `AccessDeniedException` une erreur. Si l'utilisateur appelle `GetVariables` l'API sans spécifier de nom de variable, toutes les variables sont renvoyées, ce qui peut entraîner une fuite d'informations.

Pour permettre aux utilisateurs de consulter les détails de ressources spécifiques uniquement, utilisez un élément de `NotResource` stratégie IAM dans une stratégie IAM Deny. Une fois que vous avez ajouté cet élément de stratégie à une stratégie IAM Deny, les utilisateurs peuvent uniquement

consulter les détails des ressources spécifiées dans le `NotResource` bloc. Pour plus d'informations, voir Éléments de politique IAM JSON : NotResource dans le guide de l'utilisateur IAM.

L'exemple de politique suivant permet aux utilisateurs d'accéder à toutes les ressources d'Amazon Fraud Detector. Cependant, l'élément de `NotResource` politique est utilisé pour limiter les appels d'GetVariablesAPI aux seuls noms de variables avec les préfixes `user*job_*`, et`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*"
    ]
  }
 ]
}
```

Réponse

Pour cet exemple de politique, la réponse présente le comportement suivant :

- Un GetVariables appel qui n'inclut pas les noms de variables génère une `AccessDeniedException` erreur car la demande correspond à l'instruction Deny.
- Un GetVariables appel qui inclut un nom de variable non autorisé génère une `AccessDeniedException` erreur car le nom de la variable ne correspond pas au nom de la variable dans le `NotResource` bloc. Par exemple, un GetVariables appel avec un nom de variable `email_address` entraîne une `AccessDeniedException` erreur.
- Un GetVariables appel qui inclut un nom de variable correspondant à un nom de variable dans le `NotResource` bloc est renvoyé comme prévu. Par exemple, un GetVariables appel qui inclut le nom d'une variable `job_cpa` renvoie les détails de la `job_cpa` variable.

Limiter l'accès en fonction des balises

Cet exemple de politique montre comment limiter l'accès à Amazon Fraud Detector en fonction des balises de ressources. Cet exemple suppose que :

- Dans votre, Compte AWS vous avez défini deux groupes différents, nommés Team1 et Team2
- Vous avez créé quatre détecteurs
- Vous souhaitez autoriser les membres de Team1 à effectuer des appels d'API sur 2 détecteurs
- Vous souhaitez autoriser les membres de Team2 à effectuer des appels d'API sur les 2 autres détecteurs

Pour contrôler l'accès aux appels d'API (exemple)

1. Ajoutez une étiquette avec la clé `Project` et la valeur `A` aux détecteurs utilisés par Team1.
2. Ajoutez une étiquette avec la clé `Project` et la valeur `B` aux détecteurs utilisés par Team2.
3. Créez une politique IAM avec une `ResourceTag` condition interdisant l'accès aux détecteurs dotés de balises contenant une clé `Project` et une valeurB, et associez cette politique à Team1.
4. Créez une politique IAM avec une `ResourceTag` condition interdisant l'accès aux détecteurs dotés de balises contenant une clé `Project` et une valeurA, et associez cette politique à Team2.

Voici un exemple de politique interdisant des actions spécifiques sur toute ressource Amazon Fraud Detector dont le tag comporte une clé `Project` et une valeur 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"
        }
      }
    }
  ]
}
```

Prévention de l'adjoint confus

Le problème des adjoints confus se produit lorsqu'une entité qui n'est pas autorisée à effectuer une action peut contraindre une entité plus privilégiée à effectuer l'action. AWS fournit des outils qui vous aident à protéger votre compte si vous fournissez à des tiers (comptes croisés) ou à d'autres AWS services (appelés interservices) un accès aux ressources de votre compte.

Un problème de confusion entre les services peut survenir lorsqu'un service (le service appelant) appelle un autre service (le service appelé). Le service appelant peut être manipulé et ses autorisations utilisées pour agir sur les ressources d'un autre client auxquelles on ne serait pas autorisé d'accéder autrement. Pour éviter cela, vous pouvez créer des politiques qui vous aident à protéger vos données pour tous les services dont les principaux responsables ont obtenu l'accès aux ressources de votre service.

Amazon Fraud Detector prend en charge l'utilisation de rôles de service dans vos politiques d'autorisation afin de permettre à un service d'accéder aux ressources d'un autre service en votre nom. Un rôle nécessite deux politiques : une politique d'approbation de rôle qui spécifie le principal autorisé à endosser le rôle et une politique d'autorisations qui spécifie ce qui peut être fait avec le rôle. Lorsqu'un service endosse un rôle en votre nom, le principal du service doit être autorisé à effectuer l'action `sts:AssumeRole` dans la politique d'approbation des rôles. Lorsqu'un service appelle`sts:AssumeRole`, AWS STS renvoie un ensemble d'informations d'identification de sécurité

temporaires que le principal du service utilise pour accéder aux ressources autorisées par la politique d'autorisation du rôle.

Pour éviter tout problème de confusion entre les services, Amazon Fraud Detector recommande d'utiliser les clés contextuelles `aws:SourceArn`et les clés de contexte de condition `aws:SourceAccount`globale dans votre politique de confiance en matière de rôle afin de limiter l'accès au rôle aux seules demandes générées par les ressources attendues.

`aws:SourceAccount`Spécifie l'ID de compte et l'`aws:SourceArn`ARN de la ressource associée à l'accès interservices. Le `aws:SourceArn` doit être spécifié à l'aide du format ARN. Assurez-vous que `aws:SourceAccount` les deux `aws:SourceArn` utilisent le même identifiant de compte lorsqu'il est utilisé dans la même déclaration de politique.

Le moyen le plus efficace de se protéger contre le problème de député confus consiste à utiliser la clé de contexte de condition globale `aws:SourceArn` avec l'ARN complet de la ressource. Si vous ne connaissez pas l'ARN complet de la ressource ou si vous spécifiez plusieurs ressources, utilisez la clé de condition de contexte `aws:SourceArn` global avec un caractère générique (*) pour les parties inconnues de l'ARN. Par exemple, `arn:aws:`*`servicename`*`:*:`*`123456789012`*`:*`. Pour plus d'informations sur les ressources et les actions d'Amazon Fraud Detector que vous pouvez utiliser dans le cadre de vos politiques d'autorisation, consultez Actions, ressources et clés de condition pour Amazon Fraud Detector.

L'exemple de politique de confiance dans les rôles suivant utilise un caractère générique (*) dans la clé de `aws:SourceArn` condition pour permettre à Amazon Fraud Detector d'accéder à plusieurs ressources associées à l'identifiant de compte.

```
{
        "Version": "2012-10-17",
        "Statement": [
             {
               "Effect": "Allow",
               "Principal": {
               "Service": [
                   "frauddetector.amazonaws.com"
                   ]
               },
               "Action": "sts:AssumeRole",
               "Condition": {
               "StringEquals": {
                   "aws:SourceAccount": "123456789012"
               },
```

```
                "StringLike": {
                   "aws:SourceArn": "arn:aws:frauddetector:us-west-2:123456789012:*"
        }
      }
    }
  ]
}
```

La politique de confiance des rôles suivante permet à Amazon Fraud Detector d'accéder uniquement aux `external-model` ressources. Notez le `aws:SourceArn` paramètre dans le bloc Condition. Le qualificatif de ressource est créé à l'aide du point de terminaison du modèle fourni pour effectuer l'appel `PutExternalModel` d'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"
        }
      }
    }
  ]
}
```

Résolution des problèmes d'identité et d'accès à Amazon Fraud Detector

Utilisez les informations suivantes pour vous aider à diagnostiquer et à résoudre les problèmes courants que vous pouvez rencontrer lorsque vous travaillez avec Amazon Fraud Detector et IAM.

Rubriques

Je ne suis pas autorisé à effectuer une action dans Amazon Fraud Detector

S'il vous AWS Management Console indique que vous n'êtes pas autorisé à effectuer une action, vous devez contacter votre administrateur pour obtenir de l'aide. Votre administrateur est la personne qui vous a fourni vos informations de connexion.

L'exemple d'erreur suivant se produit lorsque l'`mateojackson`utilisateur essaie d'utiliser la console pour afficher les détails d'un *`détecteur`* mais ne dispose pas des `frauddetector:`*`GetDetectors`* autorisations nécessaires.

```
User: arn:aws:iam::123456789012:user/mateojackson is not authorized to perform:
 frauddetector:GetDetectors on resource: my-example-detector
```

Dans ce cas, Mateo demande à son administrateur de mettre à jour ses politiques pour lui permettre d'accéder à la ressource *`my-example-detector`* à l'aide de l'action `frauddetector:`*`GetDetectors`*.

Je ne suis pas autorisé à effectuer iam : PassRole

Si vous recevez un message d'erreur indiquant que vous n'êtes pas autorisé à effectuer l'`iam:PassRole`action, vos politiques doivent être mises à jour pour vous permettre de transmettre un rôle à Amazon Fraud Detector.

Certains vous Services AWS permettent de transmettre un rôle existant à ce service au lieu de créer un nouveau rôle de service ou un rôle lié à un service. Pour ce faire, un utilisateur doit disposer des autorisations nécessaires pour transmettre le rôle au service.

L'exemple d'erreur suivant se produit lorsqu'un utilisateur IAM nommé `marymajor` essaie d'utiliser la console pour effectuer une action dans Amazon Fraud Detector. Toutefois, l'action nécessite que le service ait des autorisations accordées par un rôle de service. Mary ne dispose pas des autorisations nécessaires pour transférer le rôle au service.

```
User: arn:aws:iam::123456789012:user/marymajor is not authorized to perform:
 iam:PassRole
```

Dans ce cas, les politiques de Mary doivent être mises à jour pour lui permettre d'exécuter l'action `iam:PassRole`.

Si vous avez besoin d'aide, contactez votre AWS administrateur. Votre administrateur vous a fourni vos informations d'identification de connexion.

Je souhaite autoriser des personnes extérieures à mon AWS compte à accéder à mes ressources Amazon Fraud Detector

Vous pouvez créer un rôle que les utilisateurs provenant d'autres comptes ou les personnes extérieures à votre organisation pourront utiliser pour accéder à vos ressources. Vous pouvez spécifier qui est autorisé à assumer le rôle. Pour les services qui prennent en charge les politiques basées sur les ressources ou les listes de contrôle d'accès (ACL), vous pouvez utiliser ces politiques pour donner l'accès à vos ressources.

Pour en savoir plus, consultez les éléments suivants :

- Pour savoir si Amazon Fraud Detector prend en charge ces fonctionnalités, consultezComment Amazon Fraud Detector fonctionne avec IAM.
- Pour savoir comment fournir l'accès à vos ressources sur celles Comptes AWS que vous possédez, consultez la section Fournir l'accès à un utilisateur IAM dans un autre utilisateur Compte AWS que vous possédez dans le Guide de l'utilisateur IAM.
- Pour savoir comment fournir l'accès à vos ressources à des tiers Comptes AWS, consultez la section Fournir un accès à des ressources Comptes AWS détenues par des tiers dans le guide de l'utilisateur IAM.
- Pour savoir comment fournir un accès par le biais de la fédération d'identité, consultez Fournir un accès à des utilisateurs authentifiés en externe (fédération d'identité) dans le Guide de l'utilisateur IAM.
- Pour découvrir quelle est la différence entre l'utilisation des rôles et l'utilisation des politiques basées sur les ressources pour l'accès entre comptes, consultez Différence entre les rôles IAM et les politiques basées sur les ressources dans le Guide de l'utilisateur IAM.

Amazon Fraud Detector n'a pas pu assumer le rôle indiqué

Si vous recevez un message d'erreur indiquant qu'Amazon Fraud Detector n'a pas pu assumer le rôle donné, vous devez mettre à jour la relation de confiance pour le rôle spécifié. En désignant Amazon Fraud Detector comme entité de confiance, le service peut assumer ce rôle. Lorsque vous utilisez Amazon Fraud Detector pour créer un rôle, cette relation de confiance est automatiquement définie. Vous devez uniquement établir cette relation de confiance pour les rôles IAM qui ne sont pas créés par Amazon Fraud Detector.

Pour établir une relation de confiance pour un rôle existant avec Amazon Fraud Detector

1. Ouvrez la console IAM à l'adresse https://console.aws.amazon.com/iam/
2. Dans le volet de navigation, sélectionnez Rôles.
3. Choisissez le nom du rôle que vous souhaitez modifier, puis cliquez sur l'onglet Relations de confiance.
4. Choisissez Modifier la relation d'approbation.
5. Sous Document de stratégie, collez les informations suivantes, puis choisissez Mettre à jour la stratégie de confiance.

```
{
    "Version": "2012-10-17",
    "Statement": [ {
        "Effect": "Allow",
        "Principal": {
            "Service": "frauddetector.amazonaws.com"
        },
        "Action": "sts:AssumeRole"
    } ]
}
```

Enregistrement et surveillance dans Amazon Fraud Detector

AWS fournit les outils de surveillance suivants pour surveiller Amazon Fraud Detector, signaler un problème et prendre des mesures automatiques le cas échéant :

- Amazon CloudWatch surveille vos AWS ressources et les applications que vous utilisez AWS en temps réel. Pour plus d'informations CloudWatch, consultez le guide de CloudWatch l'utilisateur Amazon.
- AWS CloudTrailcapture les appels d'API et les événements associés effectués par ou pour le compte de votre AWS compte et envoie les fichiers journaux dans un compartiment Amazon S3 que vous spécifiez. Pour plus d'informations CloudTrail et consultez le guide de AWS CloudTrail l'utilisateur.

Pour plus d'informations sur la surveillance d'Amazon Fraud Detector, consultezSurveillez Amazon Fraud Detector.

Validation de conformité pour Amazon Fraud Detector

Des auditeurs tiers évaluent la sécurité et la conformité des AWS services dans le cadre de plusieurs programmes de AWS conformité, tels que SOC, PCI, FedRAMP et HIPAA.

Pour savoir si un programme Services AWS de conformité Service AWS s'inscrit dans le champ d'application de programmes de conformité spécifiques, consultez Services AWS la section de conformité et sélectionnez le programme de conformité qui vous intéresse. Pour des informations générales, voir Programmes de AWS conformité Programmes AWS de .

Vous pouvez télécharger des rapports d'audit tiers à l'aide de AWS Artifact. Pour plus d'informations, voir Téléchargement de rapports dans AWS Artifact .

Votre responsabilité en matière de conformité lors de l'utilisation Services AWS est déterminée par la sensibilité de vos données, les objectifs de conformité de votre entreprise et les lois et réglementations applicables. AWS fournit les ressources suivantes pour faciliter la mise en conformité :

- Guides de démarrage rapide sur la sécurité et la conformité : ces guides de déploiement abordent les considérations architecturales et indiquent les étapes à suivre pour déployer des environnements de base axés sur AWS la sécurité et la conformité.
- Architecture axée sur la sécurité et la conformité HIPAA sur Amazon Web Services : ce livre blanc décrit comment les entreprises peuvent créer des applications AWS conformes à la loi HIPAA.

> **Note**
>
> Tous ne Services AWS sont pas éligibles à la loi HIPAA. Pour plus d'informations, consultez le HIPAA Eligible Services Reference.

- AWS Ressources de https://aws.amazon.com/compliance/resources/ de conformité — Cette collection de classeurs et de guides peut s'appliquer à votre secteur d'activité et à votre région.
- AWS Guides de conformité destinés aux clients — Comprenez le modèle de responsabilité partagée sous l'angle de la conformité. Les guides résument les meilleures pratiques en matière de sécurisation Services AWS et décrivent les directives relatives aux contrôles de sécurité dans plusieurs cadres (notamment le National Institute of Standards and Technology (NIST), le Payment Card Industry Security Standards Council (PCI) et l'Organisation internationale de normalisation (ISO)).
- Évaluation des ressources à l'aide des règles du guide du AWS Config développeur : le AWS Config service évalue dans quelle mesure les configurations de vos ressources sont conformes aux pratiques internes, aux directives du secteur et aux réglementations.
- AWS Security Hub— Cela Service AWS fournit une vue complète de votre état de sécurité interne AWS. Security Hub utilise des contrôles de sécurité pour évaluer vos ressources AWS et vérifier votre conformité par rapport aux normes et aux bonnes pratiques du secteur de la sécurité. Pour obtenir la liste des services et des contrôles pris en charge, consultez Référence des contrôles Security Hub.
- Amazon GuardDuty — Cela Service AWS détecte les menaces potentielles qui pèsent sur vos charges de travail Comptes AWS, vos conteneurs et vos données en surveillant votre environnement pour détecter toute activité suspecte et malveillante. GuardDuty peut vous aider à répondre à diverses exigences de conformité, telles que la norme PCI DSS, en répondant aux exigences de détection des intrusions imposées par certains cadres de conformité.
- AWS Audit Manager— Cela vous Service AWS permet d'auditer en permanence votre AWS utilisation afin de simplifier la gestion des risques et la conformité aux réglementations et aux normes du secteur.

Résilience dans Amazon Fraud Detector

L'infrastructure mondiale d'AWS repose sur les régions AWS et les zones de disponibilité. Les régions AWS fournissent plusieurs zones de disponibilité physiquement séparées et isolées, reliées par un réseau à latence faible, à débit élevé et à forte redondance. Avec les zones de

disponibilité, vous pouvez concevoir et exploiter des applications et des bases de données qui basculent automatiquement d'une zone à l'autre sans interruption. Les zones de disponibilité sont davantage disponibles, tolérantes aux pannes et ont une plus grande capacité de mise à l'échelle que les infrastructures traditionnelles à un ou plusieurs centres de données.

Pour de plus amples informations sur les régions et les zones de disponibilité AWS, veuillez consulter Infrastructure mondiale AWS.

Sécurité de l'infrastructure dans Amazon Fraud Detector

En tant que service géré, Amazon Fraud Detector est protégé par la sécurité du réseau AWS mondial. Pour plus d'informations sur les services AWS de sécurité et sur la manière dont AWS l'infrastructure est protégée, consultez la section Sécurité du AWS cloud. Pour concevoir votre AWS environnement en utilisant les meilleures pratiques en matière de sécurité de l'infrastructure, consultez la section Protection de l'infrastructure dans le cadre AWS bien architecturé du pilier de sécurité.

Vous utilisez des appels d'API AWS publiés pour accéder à Amazon Fraud Detector via le réseau. Les clients doivent prendre en charge les éléments suivants :

- Protocole TLS (Transport Layer Security). Nous exigeons TLS 1.2 et recommandons TLS 1.3.
- Ses suites de chiffrement PFS (Perfect Forward Secrecy) comme DHE (Ephemeral Diffie-Hellman) ou ECDHE (Elliptic Curve Ephemeral Diffie-Hellman). La plupart des systèmes modernes tels que Java 7 et les versions ultérieures prennent en charge ces modes.

En outre, les demandes doivent être signées à l'aide d'un ID de clé d'accès et d'une clé d'accès secrète associée à un principal IAM. Vous pouvez également utiliser AWS Security Token Service (AWS STS) pour générer des informations d'identification de sécurité temporaires et signer les demandes.

Surveillez Amazon Fraud Detector

La surveillance joue un rôle important dans le maintien de la fiabilité, de la disponibilité et des performances d'Amazon Fraud Detector et de vos autres solutions AWS. AWS fournit les outils de surveillance suivants pour surveiller Amazon Fraud Detector, signaler un problème et prendre des mesures automatiques le cas échéant :

- Amazon CloudWatch surveille vos AWS ressources et les applications que vous utilisez AWS en temps réel. Vous pouvez collecter et suivre les métriques, créer des tableaux de bord personnalisés, et définir des alarmes qui vous informent ou prennent des mesures lorsqu'une métrique spécifique atteint un seuil que vous spécifiez. Pour plus d'informations, consultez le guide de CloudWatch l'utilisateur Amazon.
- AWS CloudTrailcapture les appels d'API et les événements associés effectués par ou pour le compte de votre AWS compte et envoie les fichiers journaux dans un compartiment Amazon S3 que vous spécifiez. Vous pouvez identifier les utilisateurs et les comptes qui ont appelé AWS, l'adresse IP source à partir de laquelle les appels ont été émis, ainsi que le moment où les appels ont eu lieu. Pour de plus amples informations, veuillez consulter le Guide de l'utilisateur AWS CloudTrail.

Rubriques

Surveillance d'Amazon Fraud Detector avec Amazon CloudWatch

Vous pouvez surveiller Amazon Fraud Detector à l'aide d'Amazon CloudWatch, qui collecte des données brutes et les traite en indicateurs lisibles en temps quasi réel. Ces statistiques sont enregistrées pour une durée de 15 mois ; par conséquent, vous pouvez accéder aux informations historiques et acquérir un meilleur point de vue de la façon dont votre service ou application web s'exécute. Vous pouvez également définir des alarmes qui surveillent certains seuils et envoient des notifications ou prennent des mesures lorsque ces seuils sont atteints. Pour plus d'informations, consultez le guide de CloudWatch l'utilisateur Amazon.

Rubriques

- Métriques d'Amazon Fraud Detector

Utilisation CloudWatch des métriques pour Amazon Fraud Detector.

Pour utiliser les métriques, vous devez spécifier les informations suivantes :

- L'espace de noms de la métrique. Un espace de noms est un CloudWatch conteneur dans lequel Amazon Fraud Detector publie ses métriques. Si vous utilisez l' CloudWatch ListMetricsAPI ou la commande list-metrics pour afficher les métriques d'Amazon Fraud Detector, spécifiez l'espace de `AWS/FraudDetector` noms.
- La dimension de métrique. Une dimension est une paire nom-valeur qui vous aide à identifier de manière unique une métrique. Par exemple, il `DetectorId` peut s'agir d'un nom de dimension. La spécification d'une dimension métrique est facultative.
- Le nom de la métrique, par exemple `GetEventPrediction`.

Vous pouvez obtenir des données de surveillance pour Amazon Fraud Detector en utilisant l' AWS Management Console API AWS CLI, ou l' CloudWatch API. Vous pouvez également utiliser l' CloudWatch API via l'un des kits de développement logiciel (SDK) Amazon AWS ou les outils d' CloudWatch API. La console affiche une série de graphiques basés sur les données brutes de l' CloudWatch API. En fonction de vos besoins, vous pouvez utiliser les graphiques affichés dans la console ou extraits de l'API.

La liste suivante présente certaines utilisations courantes des métriques. Voici quelques suggestions pour vous aider à démarrer, qui ne forment pas une liste exhaustive.

Comment... ?	Métriques pertinentes
Comment suivre le nombre de prédictions effectuées ?	Surveiller la métrique `GetEventPrediction` .
Comment puis-je surveiller les `GetEventPrediction` erreurs ?	Utilisez les indicateurs `GetEventPrediction5xxError` et les `GetEventPrediction4xxError` indicateurs.
Comment puis-je surveiller la latence des appels `GetEventPrediction` ?	Utilisez la métrique `GetEventPrediction Latency` .

Vous devez disposer des CloudWatch autorisations appropriées pour surveiller Amazon Fraud Detector avec CloudWatch. Pour plus d'informations, consultez Authentification et contrôle d'accès pour Amazon CloudWatch.

Accédez aux métriques d'Amazon Fraud Detector

Les étapes suivantes indiquent comment accéder aux métriques d'Amazon Fraud Detector à l'aide de la CloudWatch console.

Pour consulter les métriques (console)

1. Ouvrez la CloudWatch console à l'adresse https://console.aws.amazon.com/cloudwatch/.
2. Choisissez Metrics, cliquez sur l'onglet All Metrics, puis sélectionnez Fraud Detector.
3. Choisissez la dimension de métrique.
4. Choisissez la métrique souhaitée dans la liste, puis une période pour le graphique.

Créer une alarme

Vous pouvez créer une CloudWatch alarme qui envoie un message Amazon Simple Notification Service (Amazon SNS) lorsque l'état de l'alarme change. Une alarme surveille une seule métrique pendant la période que vous spécifiez. Elle réalise une ou plusieurs actions en fonction de la valeur de la métrique par rapport à un seuil donné sur un certain nombre de périodes. L'action est une notification envoyée à une rubrique Amazon SNS ou à une stratégie Auto Scaling.

Les alarmes déclenchent des actions uniquement pour les changements d'état prolongés. CloudWatch les alarmes n'invoquent pas d'actions simplement parce qu'elles sont dans un état particulier. L'état doit avoir changé et avoir été maintenu pendant un nombre de périodes spécifié.

Pour définir une alarme (console)

1. Connectez-vous à la CloudWatch console AWS Management Console et ouvrez-la à l'adresse https://console.aws.amazon.com/cloudwatch/.
2. Dans le volet de navigation, choisissez Alarms, puis Create Alarm. Cela ouvre l'assistant de création d'alarme.
3. Choisissez Select metric (Sélectionner une métrique).
4. Dans l'onglet All metrics, sélectionnez Fraud Detector.
5. Choisissez Par identifiant de détecteur, puis choisissez la GetEventPredictionmétrique.

6. Sélectionnez l'onglet Graphed metrics (Graphiques des métriques).
7. Pour Statistics (Statistique), choisissez Sum (Somme).
8. Choisissez Select metric (Sélectionner une métrique).
9. Pour Conditions, choisissez Static pour le type de seuil et Greater pour Whenever..., puis entrez la valeur maximale de votre choix. Choisissez Suivant.
10. Afin d'envoyer des alarmes à une rubrique Amazon SNS existante, pour Envoyer une notification à : choisissez une rubrique SNS existante. Pour définir le nom et les adresses e-mail d'une nouvelle liste d'abonnement par e-mail, choisissez Nouvelle liste. CloudWatch enregistre la liste et l'affiche sur le terrain afin que vous puissiez l'utiliser pour définir de futures alarmes.

> **Note**
>
> Si vous utilisez Nouvelle liste pour créer une nouvelle rubrique Amazon SNS, les adresses e-mail doivent être vérifiées avant que les destinataires ne reçoivent de notifications. Amazon SNS n'envoie les e-mails que lorsque l'alarme passe à l'état d'alarme. Si ce changement d'état d'alarme se produit avant que les adresses e-mail ne soient vérifiées, les destinataires prévus ne reçoivent aucune notification.

11. Choisissez Suivant. Ajoutez un nom et une description facultative pour votre alarme. Choisissez Suivant.
12. Sélectionnez Create Alarm (Créer une alerte).

Métriques d'Amazon Fraud Detector

Amazon Fraud Detector envoie les statistiques suivantes à CloudWatch. Toutes les mesures soutiennent ces statistiques :`Average`,`Minimum`,`Maximum`,`Sum`.

Métrique	Description
`GetEventPrediction`	Le nombre de demandes GetEventPrediction d'API. Dimensions valides : `DetectorID`
`GetEventPredictionLatency`	Intervalle de temps nécessaire pour répondre à une demande du client par rapport à la GetEventPrediction demande.

Métrique	Description
	Dimensions valides : `DetectorID` Unité : millisecondes
`GetEventPrediction4XXError`	Le nombre de GetEventPrediction demandes pour lesquelles Amazon Fraud Detector a renvoyé un code de réponse HTTP 4xx. Pour chaque réponse 4xx, 1 est envoyée. Dimensions valides : `DetectorID`
`GetEventPrediction5XXError`	Le nombre de GetEventPrediction demandes pour lesquelles Amazon Fraud Detector a renvoyé un code de réponse HTTP 5xx. Pour chaque réponse 5xx, 1 est envoyée. Dimensions valides : `DetectorID`
`Prediction`	Le nombre de prédictions. 1 est envoyé en cas de succès. Dimensions valides :`DetectorID` , `DetectorVersionID`
`PredictionLatency`	Intervalle de temps nécessaire à une opération de prédiction. Dimensions valides :`DetectorID` , `DetectorVersionID` Unité : millisecondes
`PredictionError`	Le nombre de prédictions pour lesquelles Amazon Fraud Detector a rencontré une erreur. 1 est envoyé en cas d'erreur. Dimensions valides :`DetectorID` , `DetectorVersionID`

Métrique	Description
`VariableUsed`	Le nombre de GetEventPrediction demandes pour lesquelles la variable a été utilisée dans le cadre de l'évaluation. Dimensions valides :`DetectorID` ,`DetectorVersionID` , `VariableName`
`VariableDefaultReturned`	Le nombre de GetEventPrediction demandes pour lesquelles la variable n'était pas présente dans les attributs d'événement et, par conséquent, la valeur par défaut de la variable a été utilisée lors de l'évaluation. Dimensions valides :`DetectorID` ,`DetectorVersionID` , `VariableName`
`RuleNotEvaluated`	Le nombre de GetEventPrediction demandes pour lesquelles la règle n'a pas été évaluée parce qu'une règle précédente correspondait. Dimensions valides :`DetectorID` ,`DetectorVersionID` , `RuleID`
`RuleEvaluateTrue`	Le nombre de GetEventPrediction demandes pour lesquelles la règle s'est déclenchée comme True et le résultat de la règle a été renvoyé. Dimensions valides :`DetectorID` ,`DetectorVersionID` , `RuleID`
`RuleEvaluateFalse`	Nombre de GetEventPrediction demandes pour lesquelles la règle a été évaluée à False. Dimensions valides :`DetectorID` ,`DetectorVersionID` , `RuleID`

Métrique	Description
`RuleEvaluateError`	Le nombre de GetEventPrediction demandes pour lesquelles la règle est évaluée par erreur Dimensions valides :`DetectorID` ,`DetectorVersionID` , `RuleID`
`OutcomeReturned`	Le nombre d' GetEventPrediction appels pour lesquels le résultat spécifié a été renvoyé. Dimensions valides :`DetectorID` ,`DetectorVersionID` , `OutcomeName`
`ModelInvocation (Amazon SageMaker model endpoint)`	Le nombre de GetEventPrediction demandes pour lesquelles le point de terminaison du SageMaker modèle a été invoqué dans le cadre de l'évaluation. Dimensions valides :`DetectorID` ,`DetectorVersionID` , `ModelEndpoint`
`ModelInvocationError (Amazon SageMaker model endpoint)`	Nombre de GetEventPrediction demandes pour lesquelles le point de terminaison du SageMaker modèle invoqué a renvoyé une erreur lors de l'évaluation. Dimensions valides :`DetectorID` ,`DetectorVersionID` , `ModelEndpoint`
`ModelInvocationLatency (Amazon SageMaker model endpoint)`	Intervalle de temps nécessaire au modèle importé pour répondre, tel qu'il est affiché sur Amazon Fraud Detector. Cet intervalle inclut uniquement l'invocation du modèle. Dimensions valides :`DetectorID` ,`DetectorVersionID` , `ModelEndpoint` Unité : millisecondes

Métrique	Description
`ModelInvocation`	Le nombre de GetEventPrediction demandes pour lesquelles le modèle a été invoqué dans le cadre de l'évaluation. Dimensions valides : `DetectorID DetectorVersionID ,ModelType , ModelID`
`ModelInvocationError`	Le nombre de GetEventPrediction demandes pour lesquelles le modèle Amazon Fraud Detector a renvoyé une erreur lors de l'évaluation. Dimensions valides : `DetectorID DetectorVersionID ,ModelType , ModelID`
`ModelInvocationLatency`	Intervalle de temps nécessaire au modèle Amazon Fraud Detector pour répondre, tel qu'il est affiché sur Amazon Fraud Detector. Cet intervalle inclut uniquement l'invocation du modèle. Dimensions valides : `DetectorID DetectorVersionID ,ModelType , ModelID` Unité : millisecondes

Enregistrement des appels d'API Amazon Fraud Detector avec AWS CloudTrail

Amazon Fraud Detector est intégré à AWS CloudTrail un service qui fournit un enregistrement des actions effectuées par un utilisateur, un rôle ou un AWS service dans Amazon Fraud Detector. CloudTrail capture tous les appels d'API pour Amazon Fraud Detector sous forme d'événements, y compris les appels depuis la console Amazon Fraud Detector et les appels depuis le code vers les API Amazon Fraud Detector.

Si vous créez un suivi, vous pouvez activer la diffusion continue des CloudTrail événements vers un compartiment Amazon S3, y compris les événements pour Amazon Fraud Detector. Si vous ne configurez pas de suivi, vous pouvez toujours consulter les événements les plus récents dans

la CloudTrail console dans Historique des événements. À l'aide des informations collectées par CloudTrail, vous pouvez déterminer la demande envoyée à Amazon Fraud Detector, l'adresse IP à partir de laquelle la demande a été faite, l'auteur de la demande, la date à laquelle elle a été faite, ainsi que des informations supplémentaires.

Pour en savoir plus CloudTrail, consultez le guide de AWS CloudTrail l'utilisateur.

Informations sur Amazon Fraud Detector dans CloudTrail

CloudTrail est activé sur votre AWS compte lorsque vous le créez. Lorsqu'une activité se produit dans Amazon Fraud Detector, cette activité est enregistrée dans un CloudTrail événement avec d'autres événements liés au AWS service dans l'historique des événements. Vous pouvez consulter, rechercher et télécharger les événements récents dans votre AWS compte. Pour plus d'informations, consultez la section Affichage des événements à l'aide de l'historique des CloudTrail événements.

Pour un enregistrement continu des événements de votre AWS compte, y compris des événements pour Amazon Fraud Detector, créez une trace. Un suivi permet CloudTrail de fournir des fichiers journaux à un compartiment Amazon S3. Par défaut, lorsque vous créez un journal d'activité dans la console, il s'applique à toutes les régions AWS. Le journal enregistre les événements de toutes les régions de la AWS partition et transmet les fichiers journaux au compartiment Amazon S3 que vous spécifiez. En outre, vous pouvez configurer d'autres AWS services pour analyser plus en détail les données d'événements collectées dans les CloudTrail journaux et agir en conséquence. Pour plus d'informations, consultez les ressources suivantes :

- Vue d'ensemble de la création d'un journal d'activité
- CloudTrail Services et intégrations pris en charge
- Configuration des notifications Amazon SNS pour CloudTrail
- Réception de fichiers CloudTrail journaux de plusieurs régions et réception de fichiers CloudTrail journaux de plusieurs comptes

Amazon Fraud Detector prend en charge l'enregistrement de chaque action (opération d'API) sous forme d'événement dans des fichiers CloudTrail journaux. Pour plus d'informations, consultez Actions.

Chaque événement ou entrée de journal contient des informations sur la personne ayant initié la demande. Les informations relatives à l'identité permettent de déterminer les éléments suivants :

- Si la demande a été effectuée avec les informations d'identification utilisateur racine ou .

- Si la demande a été effectuée avec les informations d'identification de sécurité temporaires d'un rôle ou d'un utilisateur fédéré.
- Si la demande a été faite par un autre AWS service.

Pour plus d'informations, consultez l'élément CloudTrail UserIdentity.

Comprendre les entrées du fichier journal Amazon Fraud Detector

Un suivi est une configuration qui permet de transmettre des événements sous forme de fichiers journaux à un compartiment Amazon S3 que vous spécifiez. CloudTrail les fichiers journaux contiennent une ou plusieurs entrées de journal. Un événement représente une demande unique provenant de n'importe quelle source et inclut des informations sur l'opération demandée, la date et l'heure de l'opération, les paramètres de la demande, etc. CloudTrail les fichiers journaux ne constituent pas une trace ordonnée des appels d'API publics, ils n'apparaissent donc pas dans un ordre spécifique.

L'exemple suivant montre une entrée de CloudTrail journal illustrant l'`GetDetectors`opération.


```
{
    "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"
```

```
}
```

Dépannage

Les sections suivantes vous aident à résoudre les problèmes que vous pouvez rencontrer lors de l'utilisation d'Amazon Fraud Detector

Résoudre les problèmes liés aux données d'entraînement

Utilisez les informations de cette section pour diagnostiquer et résoudre les problèmes que vous pourriez rencontrer dans le volet de diagnostic de l'entraînement des modèles de la console Amazon Fraud Detector lorsque vous entraînez votre modèle.

Les problèmes affichés dans le volet de diagnostic de Model Training sont classés comme suit. L'obligation de régler le problème dépend de la catégorie du problème.

- Erreur
  
  entraîne l'échec de l'entraînement du modèle. Ces problèmes doivent être résolus pour que le modèle s'entraîne avec succès.
- Avertis
  
  entraîne la poursuite de l'entraînement du modèle, mais certaines variables peuvent être exclues du processus de formation. Consultez les instructions pertinentes dans cette section pour améliorer la qualité de votre ensemble de données.
- Informa
  
  (Info) - n'a aucun impact sur l'entraînement du modèle et toutes les variables sont utilisées pour l'entraînement. Nous vous recommandons de consulter les instructions pertinentes de cette section afin d'améliorer encore la qualité de votre jeu de données et les performances de votre modèle.

Rubriques

- Type de variable manquant ou incorrect
- Valeurs de variables manquantes
- Valeurs de variables uniques insuffisantes
- Expression de variable incorrecte
- Entités uniques insuffisantes

Taux de fraude instable dans l'ensemble de données donné

Type de problème : Erreur

Description

Le taux de fraude dans les données fournies est trop instable dans le temps. Assurez-vous que votre fraude et vos événements légitimes sont échantillonnés de manière uniforme au fil du temps.

Cause

Cette erreur se produit si les fraudes et les événements légitimes de votre ensemble de données sont répartis de manière inégale et proviennent de plages horaires différentes. Le processus de formation du modèle Amazon Fraud Detector échantillonne et partitionne votre ensemble de données en fonction de EVENT_TIMESTAMP. Par exemple, si votre ensemble de données contient des événements de fraude extraits des 6 derniers mois, mais que seul le dernier mois d'événements légitimes est inclus, l'ensemble de données est considéré comme instable. Un jeu de données instable peut entraîner des biais dans l'évaluation des performances du modèle.

Solution

Assurez-vous de fournir les données relatives aux événements frauduleux et légitimes à partir du même créneau horaire afin que le taux de fraude ne change pas radicalement au fil du temps.

Données insuffisantes

1. Type de problème : Erreur

   Description

   Moins de 50 lignes sont considérées comme des événements frauduleux. Assurez-vous que les événements frauduleux et légitimes dépassent le nombre minimum de 50 et réentraînez le modèle.

Cause

Cette erreur se produit si votre jeu de données contient moins d'événements considérés comme frauduleux que ce qui est requis pour l'entraînement du modèle. Amazon Fraud Detector nécessite au moins 50 événements frauduleux pour entraîner votre modèle.

Solution

Assurez-vous que votre ensemble de données inclut au moins 50 événements frauduleux. Vous pouvez vous en assurer en couvrant une période plus longue, si nécessaire.

2. Type de problème : Erreur

   Description

   Moins de 50 lignes sont considérées comme des événements légitimes. Assurez-vous que les événements frauduleux et légitimes dépassent le seuil minimum de dollars et réentraînez le modèle.

   Cause

   Cette erreur se produit si votre jeu de données contient moins d'événements étiquetés comme légitimes que ce qui est requis pour l'entraînement du modèle. Amazon Fraud Detector nécessite au moins 50 événements légitimes pour entraîner votre modèle.

   Solution

   Assurez-vous que votre ensemble de données inclut au moins 50 événements légitimes. Vous pouvez vous en assurer en couvrant une période plus longue, si nécessaire.

3. Type de problème : Erreur

   Description

   Le nombre d'entités uniques associées à la fraude est inférieur à 100. Envisagez d'inclure d'autres exemples d'entités frauduleuses afin d'améliorer les performances.

   Cause

   Cette erreur se produit si votre jeu de données contient moins d'entités présentant des événements frauduleux que ce qui est requis pour la formation du modèle. Le modèle Transaction Fraud Insights (TFI) nécessite au moins 100 entités présentant des cas de fraude pour garantir

une couverture maximale de l'espace frauduleux. Le modèle risque de ne pas bien se généraliser si tous les événements de fraude sont réalisés par un petit groupe d'entités.

Solution

Assurez-vous que votre ensemble de données inclut au moins 100 entités présentant des événements frauduleux. Vous pouvez vous assurer que cela couvre une période plus longue, si nécessaire.

4. Type de problème : Erreur

   Description

   Le nombre d'entités uniques associées à des entités légitimes est inférieur à 100. Envisagez d'inclure d'autres exemples d'entités légitimes afin d'améliorer les performances.

   Cause

   Cette erreur se produit si votre jeu de données contient moins d'entités présentant des événements légitimes que ce qui est requis pour l'entraînement du modèle. Le modèle Transaction Fraud Insights (TFI) nécessite au moins 100 entités présentant des événements légitimes pour garantir une couverture maximale de l'espace frauduleux. Le modèle risque de ne pas bien se généraliser si tous les événements légitimes sont réalisés par un petit groupe d'entités.

   Solution

   Assurez-vous que votre ensemble de données inclut au moins 100 entités présentant des événements légitimes. Vous pouvez vous assurer que cela couvre une période plus longue, si nécessaire.

5. Type de problème : Erreur

   Description

   Le jeu de données contient moins de 100 lignes. Assurez-vous qu'il y a plus de 100 lignes dans le jeu de données total et qu'au moins 50 lignes sont considérées comme frauduleuses.

   Cause

   Cette erreur se produit si votre ensemble de données contient moins de 100 enregistrements. Amazon Fraud Detector a besoin de données provenant d'au moins 100 événements (enregistrements) de votre ensemble de données pour l'entraînement des modèles.

Solution

Assurez-vous que votre jeu de données contient des données provenant de plus de 100 événements.

Valeurs EVENT_LABEL manquantes ou différentes

1. Type de problème : Erreur

   Description

   Plus de 1 % de votre colonne EVENT_LABEL sont nulles ou sont des valeurs autres que celles définies dans la configuration du modèle. **`$label_values`** Assurez-vous qu'il manque moins de 1 % de valeurs dans votre colonne EVENT_LABEL et que les valeurs sont celles définies dans la configuration du modèle. **`$label_values`**

   Cause

   Cette erreur se produit pour l'une des raisons suivantes :

   - Plus de 1 % des enregistrements du fichier CSV contenant vos données d'entraînement comportent des valeurs manquantes dans la colonne EVENT_LABEL.
   - Plus de 1 % des enregistrements du fichier CSV contenant vos données d'entraînement contiennent des valeurs dans la colonne EVENT_LABEL différentes de celles associées à votre type d'événement.

   Le modèle Online Fraud Insights (OFI) exige que la colonne EVENT_LABEL de chaque enregistrement soit remplie avec l'une des étiquettes associées à votre type d'événement (ou mappées). `CreateModelVersion`

   Solution

   Si cette erreur est due à l'absence de valeurs EVENT_LABEL, pensez à attribuer des étiquettes appropriées à ces enregistrements ou à supprimer ces enregistrements de votre ensemble de données. Si cette erreur est due au fait que les étiquettes de certains enregistrements ne figurent pas dans la **`label_values`** liste, assurez-vous d'ajouter toutes les valeurs de la colonne EVENT_LABEL aux étiquettes du type d'événement et de les associer à des valeurs frauduleuses ou légitimes (fraude, légitimité) lors de la création du modèle.
2. Type de problème : Informations

Description

Votre colonne EVENT_LABEL contient des valeurs nulles ou des valeurs d'étiquette autres que celles définies dans la configuration du modèle. **`$label_values`** Ces valeurs incohérentes ont été converties en « valeurs non frauduleuses » avant la formation.

Cause

Vous obtenez ces informations pour l'une des raisons suivantes :

- Moins de 1 % des enregistrements du fichier CSV contenant vos données d'entraînement comportent des valeurs manquantes dans la colonne EVENT_LABEL
- Moins de 1 % des enregistrements du fichier CSV contenant vos données d'entraînement contiennent des valeurs dans la colonne EVENT_LABEL différentes de celles associées à votre type d'événement.

Dans les deux cas, le modèle de formation sera couronné de succès. Toutefois, les valeurs d'étiquette des événements pour lesquels des valeurs d'étiquette sont manquantes ou non mappées sont converties en valeurs légitimes. Si vous considérez qu'il s'agit d'un problème, suivez la solution ci-dessous.

Solution

Si des valeurs EVENT_LABEL sont manquantes dans votre ensemble de données, pensez à supprimer ces enregistrements de votre ensemble de données. Si les valeurs fournies pour ces EVENT_LABELS ne sont pas mappées, assurez-vous que toutes ces valeurs sont mappées de manière frauduleuse ou légitime (fraude, légitime) pour chaque événement.

Valeurs EVENT_TIMESTAMP manquantes ou incorrectes

1. Type de problème : Erreur

   Description

   Votre ensemble de données d'entraînement contient EVENT_TIMESTAMP avec des horodatages non conformes aux formats acceptés. Assurez-vous que le format est l'un des formats de date/horodatage acceptés.

   Cause

Cette erreur se produit si la colonne EVENT_TIMESTAMP contient une valeur non conforme aux formats d'horodatage pris en charge par Amazon Fraud Detector.

Solution

Assurez-vous que les valeurs fournies pour la colonne EVENT_TIMESTAMP sont conformes aux formats d'horodatage pris en charge. S'il manque des valeurs dans la colonne EVENT_TIMESTAMP, vous pouvez soit les remplacer par des valeurs utilisant le format d'horodatage pris en charge, soit envisager de supprimer complètement l'événement au lieu de saisir des chaînes telles que, ou. `none` `null` `missing`

2. Type de problème : Erreur

   Votre ensemble de données d'entraînement contient EVENT_TIMESTAMP avec des valeurs manquantes. Assurez-vous qu'il n'y a aucune valeur manquante.

   Cause

   Cette erreur se produit si des valeurs sont manquantes dans la colonne EVENT_TIMESTAMP de votre ensemble de données. Amazon Fraud Detector exige que la colonne EVENT_TIMESTAMP de votre ensemble de données contienne des valeurs.

   Solution

   Assurez-vous que la colonne EVENT_TIMESTAMP de votre ensemble de données contient des valeurs et que ces valeurs sont conformes aux formats d'horodatage pris en charge. S'il manque des valeurs dans la colonne EVENT_TIMESTAMP, vous pouvez soit les remplacer par des valeurs utilisant le format d'horodatage pris en charge, soit envisager de supprimer complètement l'événement au lieu de saisir des chaînes telles que, ou. `none` `null` `missing`

Données non ingérées

Type de problème : Erreur

Description

Aucun événement ingéré n'a été trouvé pour l'entraînement, veuillez vérifier votre configuration d'entraînement.

Cause

Cette erreur se produit si vous créez un modèle avec des données d'événements stockées avec Amazon Fraud Detector mais que vous n'avez pas importé votre ensemble de données dans Amazon Fraud Detector avant de commencer à entraîner votre modèle.

Solution

Utilisez l'opération d'`SendEvent`API, l'opération d'`CreateBatchImportJob`API ou la fonctionnalité d'importation par lots dans la console Amazon Fraud Detector pour d'abord importer les données de vos événements, puis entraîner votre modèle. Voir Ensembles de données d'événements stockés pour plus d'informations.

> **Note**
>
> Nous vous recommandons d'attendre 10 minutes après avoir fini d'importer vos données avant de les utiliser pour entraîner votre modèle.

Vous pouvez utiliser la console Amazon Fraud Detector pour vérifier le nombre d'événements déjà enregistrés pour chaque type d'événement. Consultez la section Affichage des statistiques de vos événements enregistrés pour plus d'informations.

Variables insuffisantes

Type de problème : Erreur

Description

L'ensemble de données doit contenir au moins 2 variables adaptées à l'entraînement.

Cause

Cette erreur se produit si votre ensemble de données contient moins de 2 variables adaptées à l'entraînement du modèle. Amazon Fraud Detector considère qu'une variable convient à la formation des modèles uniquement si elle passe toutes les validations. Si la validation d'une variable échoue, elle est exclue de l'entraînement du modèle et un message s'affiche dans le diagnostic de l'entraînement du modèle.

Solution

Assurez-vous que votre ensemble de données comporte au moins deux variables remplies de valeurs et que toutes les validations de données ont été validées. Notez que la ligne de métadonnées

d'événement dans laquelle vous avez fourni les en-têtes de colonne (EVENT_TIMESTAMP, EVENT_ID, ENTITY_ID, EVENT_LABEL, etc.) n'est pas considérée comme une variable.

Type de variable manquant ou incorrect

Type de problème : Avertissement

Description

Le type de données attendu pour **`$variable_name`** est NUMERIC. Passez en revue et mettez **`$variable_name`** à jour votre jeu de données et réentraînez le modèle.

Cause

Cet avertissement s'affiche si une variable est définie en tant que variable NUMERIC, mais que dans l'ensemble de données, elle contient des valeurs qui ne peuvent pas être converties en NUMERIC. Par conséquent, cette variable est exclue de l'entraînement du modèle.

Solution

Si vous souhaitez la conserver sous forme de variable NUMÉRIQUE, assurez-vous que les valeurs que vous fournissez peuvent être converties en nombres flottants. Notez que si la variable contient des valeurs manquantes, ne les remplissez pas avec des chaînes telles que `nonenenull`, ou`missing`. Si la variable contient des valeurs non numériques, recréez-la en tant que variable de type CATEGORICAL ou FREE_FORM_TEXT.

Valeurs de variables manquantes

Type de problème : Avertissement

Description

Des **`$threshold`** valeurs supérieures à **`$variable_name`** sont absentes de votre jeu de données d'entraînement. Envisagez de modifier **`$variable_name`** votre ensemble de données et de vous entraîner à nouveau pour améliorer les performances.

Cause

Cet avertissement s'affiche si la variable spécifiée est supprimée en raison d'un trop grand nombre de valeurs manquantes. Amazon Fraud Detector autorise les valeurs manquantes pour une variable.

Cependant, si une variable comporte trop de valeurs manquantes, elle ne contribue pas beaucoup au modèle et cette variable est supprimée lors de l'apprentissage du modèle.

Solution

Tout d'abord, vérifiez que ces valeurs manquantes ne sont pas dues à des erreurs de collecte et de préparation des données. S'il s'agit d'erreurs, vous pouvez envisager de les supprimer de votre formation sur les modèles. Toutefois, si vous pensez que ces valeurs manquantes sont utiles et que vous souhaitez conserver cette variable, vous pouvez remplir manuellement les valeurs manquantes avec une constante à la fois dans l'apprentissage du modèle et dans l'inférence en temps réel.

Valeurs de variables uniques insuffisantes

Type de problème : Avertissement

Description

Le nombre de valeurs uniques de **`$variable_name`** est inférieur à 100. Passez en revue et mettez **`$variable_name`** à jour votre jeu de données et réentraînez le modèle.

Cause

Cet avertissement s'affiche si le nombre de valeurs uniques de la variable spécifiée est inférieur à 100. Les seuils varient en fonction du type de variable. Avec très peu de valeurs uniques, le jeu de données risque de ne pas être suffisamment général pour couvrir l'espace caractéristique de cette variable. Par conséquent, le modèle risque de ne pas bien se généraliser sur les prévisions en temps réel.

Solution

Tout d'abord, assurez-vous que la distribution des variables est représentative du trafic commercial réel. Ensuite, vous pouvez soit adopter des variables plus fines avec une cardinalité plus élevée, par exemple en les utilisant `full_customer_name` au lieu de `first_name` et `last_name` séparément, soit changer le type de variable en CATEGORICAL, ce qui permet une cardinalité plus faible.

Expression de variable incorrecte

1. Type de problème : Informations

   Description

Plus de 50 % des **$email_variable_name** valeurs ne correspondent pas à l'expression régulière attendue http://emailregex.com. Envisagez de modifier **$email_variable_name** votre ensemble de données et de vous entraîner à nouveau pour améliorer les performances.

Cause

Ces informations sont affichées si plus de 50 % des enregistrements de votre ensemble de données contiennent des valeurs d'e-mail qui ne sont pas conformes à une expression d'e-mail régulière et ne sont donc pas validées.

Solution

Formatez les valeurs des variables d'e-mail conformément à l'expression régulière. Si des valeurs d'e-mail sont manquantes, nous vous recommandons de les laisser vides au lieu de les remplir avec des chaînes telles que `nonenull`, ou`missing`.

2. Type de problème : Informations

   Description

   Plus de 50 % des **$IP_variable_name** valeurs ne correspondent pas à l'expression régulière pour les adresses IPv4 ou IPv6 https://digitalfortress.tech/tricks/top-15 - /. commonly-used-regex Envisagez de modifier **$IP_variable_name** votre ensemble de données et de vous entraîner à nouveau pour améliorer les performances.

   Cause

   Ces informations sont affichées si plus de 50 % des enregistrements de votre ensemble de données contiennent des valeurs IP non conformes à une expression IP régulière et ne sont donc pas validées.

   Solution

   Formatez les valeurs IP conformément à l'expression régulière. Si des valeurs IP sont manquantes, nous vous recommandons de les laisser vides au lieu de les remplir avec des chaînes telles que `nonenull`, ou`missing`.

3. Type de problème : Informations

   Description

Plus de 50 % des **$phone_variable_name** valeurs ne correspondent pas à l'expression régulière de base du téléphone /$pattern/. Envisagez de modifier **$phone_variable_name** votre ensemble de données et de vous entraîner à nouveau pour améliorer les performances.

Cause

Ces informations sont affichées si plus de 50 % des enregistrements de votre ensemble de données contiennent des numéros de téléphone qui ne correspondent pas à une expression de numéro de téléphone normale et ne sont donc pas validés.

Solution

Formatez les numéros de téléphone conformément à l'expression régulière. S'il manque des numéros de téléphone, nous vous recommandons de les laisser vides au lieu de les remplir avec des chaînes telles que `nonenull`, ou`missing`.

Entités uniques insuffisantes

Type de problème : Informations

Description

Le nombre d'entités uniques est inférieur à 1 500. Envisagez d'inclure davantage de données pour améliorer les performances.

Cause

Ces informations sont affichées si votre jeu de données comporte un nombre d'entités uniques inférieur au nombre recommandé. Le modèle Transaction Fraud Insights (TFI) utilise à la fois des agrégats de séries chronologiques et des fonctionnalités de transaction génériques pour fournir les meilleures performances. Si votre ensemble de données comporte trop peu d'entités uniques, il est possible que la plupart de vos données génériques, telles que IP_ADDRESS, EMAIL_ADDRESS, n'aient pas de valeurs uniques. Il existe alors un risque que ce jeu de données ne soit pas suffisamment général pour couvrir l'espace caractéristique de cette variable. Par conséquent, le modèle risque de ne pas bien se généraliser aux transactions provenant de nouvelles entités.

Solution

Incluez davantage d'entités. Étendez la plage de temps de vos données d'entraînement, si nécessaire.

Quotas

VotreCompte AWS dispose de quotas par défaut, anciennement appelés limites, pour chaque Amazon Amazon Fraud Detector. Sauf indication contraire, chaque quota est spécifique à la région. Vous pouvez demander une augmentation pour tous les quotas ajustables mentionnés dans les tableaux ci-dessous. Pour de plus amples informations, veuillez consulter consulter Demande d'augmentation de quota

Les tableaux suivants présentent les quotas d'Amazon Fraud Detector par composant.

Amazon Fraud Detector

Nom du quota	Quota par défaut	Ajustable
Taille des données de formation	5 Go	Non
Modèles par compte	50	Non
Versions par modèle	200	Non
Versions de modèles déployées par compte	5	Non
Tâches de formation simultanées par compte	3	Non
Tâches de formation simultanées par modèle	1	Non

Détecteurs de fraude Amazon, variables, résultats, règles

Nom du quota	Quota par défaut	Ajustable
Variables par compte	5000	Non

Nom du quota	Quota par défaut	Ajustable
Règles par compte	5000	Non
Listes par règle	3	Non
Résultats par compte	5000	Non
Fraud Detector par compte	100	Non
Listes par détecteur	30	Non
Versions préliminaires par détecteur	100	Non
Modèles par version de détecteur	10	Non
Étiquettes par compte	100	Non
Types d'événements par compte	100	Non
Types d'entités par compte	100	Non

Amazon Fraud Detector

Nom du quota	Quota par défaut	Ajustable
GetEventPrediction Appels d'API par seconde	200 TPS	Oui
Taille de la charge utile par appel GetEventPrediction d'API	256 Ko	Non
Nombre d'entrées par appel GetEventPrediction d'API	5000	Non

Historique du document

Le tableau suivant décrit les modifications importantes apportées au guide de l'utilisateur d'Amazon Fraud Detector. Nous mettons également régulièrement à jour le guide de l'utilisateur d'Amazon Fraud Detector afin de répondre aux commentaires que vous nous envoyez.

Modification	Description	Date
Nouveaux types de variables et de données	Amazon Fraud Detector introduit de nouveaux types de variables et un type de données que vous pouvez utiliser pour extraire des informations utiles.	5 juin 2023
Orchestration d'événements	L'orchestration des événement s vous permet d'envoyer facilement des événements à des Services AWS fins de traitement en aval, à l'aide d'Amazon. EventBridge	30 mai 2023
Listes	La ressource Listes vous permet de référencer un ensemble de valeurs telles que des adresses IP ou des adresses e-mail, dans le cadre d'une règle. Utilisez des listes dans une règle pour autoriser ou refuser l'accès ou une transaction.	14 février 2023
Explorateur de modèles de données	L'explorateur de modèles de données fournit des informati ons sur les éléments de données requis par Amazon Fraud Detector pour créer	15 décembre 2022

	votre modèle de détection des fraudes. Utilisez l'explorateur de modèles de données avant de préparer votre jeu de données d'événements.	
Modèle Account Takeover Insights	Utilisez le modèle ATI (Account Takeover Insights) pour détecter les comptes compromis à la suite d'une prise de contrôle malveillante, d'un hameçonnage ou d'un vol d'informations d'identification.	21 juillet 2022
Mise à jour du chapitre	Mise à jour du chapitre d'introduction avec des informations supplémentaires sur Amazon Fraud Detector	11 avril 2022
Enrichissement variable	Activez l'enrichissement de certaines des données brutes que vous fournissez pour améliorer les performances des modèles qui utilisent ces éléments de données et qui ont été entraînés avant le 8 février 2022.	8 février 2022
Politiques de désabonnement	Utilisez des politiques de désinscription pour refuser que les données de vos événements soient utilisées pour développer ou améliorer la qualité d'Amazon Fraud Detector.	6 janvier 2022

Prévention confuse des adjoints	Créez des politiques pour empêcher un tiers ou une entité interservices de manipuler une entité autorisée à agir en son nom afin d'accéder aux ressources de votre compte.	6 décembre 2021
Créer un jeu de données d'événements	Suivez les instructions fournies dans la section Créer un jeu de données d'événements pour préparer et collecter des données pour entraîner votre modèle.	22 novembre 2021
Explications des prévisions	Utilisez les explications des prévisions pour mieux comprendre l'impact de chaque variable d'événement sur les scores de prédiction des fraudes de votre modèle.	10 novembre 2021
Résoudre les problèmes	Utilisez les informations de la section Résoudre les problèmes liés aux données d'entraînement pour vous aider à diagnostiquer et à résoudre les problèmes que vous pourriez rencontrer dans la console Amazon Fraud Detector lorsque vous entraînez votre modèle.	11 octobre 2021

Modèle d'analyse des fraudes transactionnelles	Utilisez le modèle Transacti on Fraud Insights (TFI) pour détecter les fraudes en ligne ou card-not-present transacti onnelles.	11 octobre 2021
Événements enregistrés	Stockez les données de vos événements dans Amazon Fraud Detector et utilisez-les pour entraîner ultérieurement vos modèles. En stockant les données d'événements dans Amazon Fraud Detector, vous pouvez entraîner des modèles qui utilisent des variables calculées automatiquement pour améliorer les performan ces, simplifier le recyclage des modèles et mettre à jour les étiquettes de fraude afin de fermer la boucle de feedback du machine learning.	11 octobre 2021
Importance des variables du modèle	Utilisez l'importance des variables du modèle pour mieux comprendre ce qui fait augmenter ou diminuer les performances de votre modèle et quelles variables de votre modèle y contribuent le plus. Modifiez ensuite votre modèle pour améliorer les performan ces globales.	9 juillet 2021
Intégration à AWS CloudForm ation	AWS CloudFormationÀ utiliser pour gérer vos ressources Amazon Fraud Detector.	10 mai 2021

Prédictions par lots	Utilisez les prédictions par lots pour obtenir des prévisions pour un ensemble d'événements qui ne nécessitent pas de notation en temps réel.	31 mars 2021
Refonte du chapitre	Refonte de Get Started et d'autres sections	17 juillet 2020
Première version	Première version	2 décembre 2019

Les traductions sont fournies par des outils de traduction automatique. En cas de conflit entre le contenu d'une traduction et celui de la version originale en anglais, la version anglaise prévaudra.