



Guía del usuario

# Amazon Fraud Detector



Version latest

Copyright © 2024 Amazon Web Services, Inc. and/or its affiliates. All rights reserved.

# Amazon Fraud Detector: Guía del usuario

Copyright © 2024 Amazon Web Services, Inc. and/or its affiliates. All rights reserved.

Las marcas comerciales y la imagen comercial de Amazon no se pueden utilizar en relación con ningún producto o servicio que no sea de Amazon, de ninguna manera que pueda causar confusión entre los clientes y que menosprecie o desacredite a Amazon. Todas las demás marcas comerciales que no son propiedad de Amazon son propiedad de sus respectivos propietarios, que pueden o no estar afiliados, relacionados o patrocinados por Amazon.

---

# Table of Contents

¿Qué es Amazon Fraud Detector? .....	1
Ventajas .....	1
Conceptos y términos principales .....	3
Cómo funciona Amazon Fraud Detector .....	6
Detección de fraudes con Amazon Fraud Detector .....	8
Acceso a Amazon Fraud Detector .....	10
Disponibilidad .....	10
Interfaces .....	10
Precios .....	11
Configurar Amazon Fraud Detector .....	12
Registrarse en AWS .....	12
Registro para obtener una Cuenta de AWS .....	12
Crear un usuario administrativo .....	13
Configurar permisos para acceder a las interfaces de Amazon Fraud Detector .....	14
Configure las interfaces para acceder a Amazon Fraud Detector con .....	15
Acceda a la consola Amazon Fraud Detector .....	16
Configuración de AWS CLI .....	16
Configurar SDK AWS .....	16
Introducción a Amazon Fraud Detector .....	18
Obtener y cargar un conjunto de datos de ejemplo .....	18
Tutorial: Comience a utilizar la consola Amazon Fraud Detector .....	20
Parte A: Cree, entrene e implemente un modelo de Fraud Detector Amazon .....	20
Parte B: Generar predicciones de fraude .....	25
Tutorial: Empezar a utilizarAWS SDK for Python (Boto3) .....	30
Requisitos previos .....	31
Introducción .....	31
(Opcional) Explore las API de Amazon Fraud Detector con un cuaderno Jupyter (IPython) ....	41
Pasos siguientes .....	41
Conjunto de datos de eventos .....	42
Estructura de conjunto de datos de eventos .....	43
Obtenga los requisitos del conjunto de datos de eventos mediante el explorador de modelos de datos .....	44
Explorador de modelos de datos. ....	44
Recopila datos de eventos .....	45

Validación de conjunto de datos .....	51
Almacenamiento de conjuntos de datos .....	53
Tipo de evento .....	54
Crear un tipo de evento .....	54
Cree un tipo de evento en la consola de Amazon Fraud Detector .....	55
Cree un tipo de evento mediante el AWS SDK for Python (Boto3) .....	56
Eliminar un evento o un tipo de evento .....	57
Almacenamiento de datos de eventos .....	59
Almacene los datos de sus eventos de forma externa con Amazon S3 .....	60
Crear archivo CSV CSV .....	60
Cargue los datos de su evento en un bucket de Amazon S3 .....	63
Almacene los datos de sus eventos internamente con Amazon Fraud Detector .....	64
Preparar los datos de eventos para su almacenamiento .....	65
Almacene los datos de eventos mediante la importación por lotes .....	66
Almacene los datos de eventos mediante la operación GetEventPredictions de la API .....	82
Almacene los datos de eventos mediante la operación SendEvent de la API .....	82
Obtener detalles de los datos de un evento almacenados .....	84
Ver las métricas del conjunto de datos de eventos almacenado .....	84
Orquestación de eventos .....	86
Configuración de la orquestación de eventos .....	87
Habilite la organización de eventos en Amazon Fraud Detector .....	88
Habilite la organización de eventos en la consola de Amazon Fraud Detector .....	88
Habilite la orquestación de eventos mediante el AWS SDK for Python (Boto3) .....	89
Desactivar la organización de eventos en Amazon Fraud Detector .....	89
Desactivar la organización de eventos en la consola de Amazon Fraud Detector .....	89
Deshabilite la organización de eventos mediante la AWS SDK for Python (Boto3) .....	90
Modelo .....	91
Elija un tipo de modelo .....	91
Información sobre el fraude en línea .....	92
Información sobre el fraude en las transacciones .....	94
Información sobre la apropiación de cuentas .....	96
Creación de un modelo .....	102
Entrene e implemente un modelo utilizando el AWS SDK for Python (Boto3) .....	103
Puntuaciones del modelo .....	105
Métricas de rendimiento del modelo .....	106
Importancia de la variable del modelo .....	108

Uso de valores de importancia de las variables del modelo .....	110
Evaluar los valores de importancia de las variables del modelo .....	111
Ver la clasificación de importancia de las variables del modelo .....	111
Comprender cómo se calcula el valor de importancia de la variable del modelo .....	111
Importa un SageMaker modelo .....	112
Importe un modelo mediante el SageMaker AWS SDK for Python (Boto3) .....	113
Eliminar un modelo o versión de modelo .....	114
Detector .....	116
Crear un detector .....	116
Cree un detector en la consola de Amazon Fraud Detector .....	116
Cree un detector mediante elAWS SDK for Python (Boto3) .....	120
Crear una versión de detector .....	120
Modo de ejecución de reglas .....	120
Cree una versión de detector mediante elAWS SDK for Python (Boto3) .....	121
Eliminar un detector, una versión del detector o una versión de regla .....	122
Recursos .....	124
Variables .....	124
Tipos de datos .....	124
Valor predeterminado .....	125
Tipos de variables .....	125
Enriquecimientos variables .....	138
Crear una variable .....	145
Eliminar una variable .....	147
Etiquetas .....	148
Crear etiqueta .....	149
Actualizar etiqueta .....	150
Actualización de las etiquetas de eventos en los datos de eventos almacenados en Amazon Fraud Detector .....	151
Eliminar etiqueta .....	151
Reglas .....	152
Referencia al lenguaje de las reglas .....	153
Crear reglas .....	158
Actualizar regla .....	161
Lists .....	162
Crear una lista .....	162
Añadir entradas a una lista .....	164

Asignar un tipo de variable a una lista .....	165
Eliminar una lista .....	166
Eliminar entradas de una lista .....	167
Eliminar todas las entradas de una lista .....	168
Resultados .....	169
Crea un resultado .....	169
Eliminar un resultado .....	170
Entidad .....	171
Crear un tipo de entidad .....	172
Eliminar un tipo de entidad .....	173
Gestione los recursos medianteAWS CloudFormation .....	174
Amazon DetDetDetDetDetDetDetDetDetDet .....	174
Amazon DetDetDetDetDetDetDetDetDetDetDet .....	174
Amazon CloudFormation DetDetDetDetDetDetDetDetDet .....	175
Amazon Fraud DetectorAWS CloudFormation .....	176
Obtener más información sobre AWS CloudFormation .....	177
Predicciones de fraude .....	178
Predicción en tiempo real .....	179
Cómo funciona la predicción de fraudes en tiempo real .....	179
Obtener una predicción de fraude en tiempo real .....	180
Predicciones por lotes .....	181
Cómo funcionan las predicciones por lotes .....	181
archivos de entrada y salida .....	182
Obtener predicciones de lotes .....	182
Guía sobre las funciones de IAM .....	184
Obtenga predicciones de fraude por lotes mediante el AWS SDK for Python (Boto3) .....	184
Explicaciones de predicción .....	185
Ver las explicaciones de las predicciones .....	187
Comprender cómo se calculan las explicaciones de las predicciones .....	189
Seguridad .....	190
Protección de los datos .....	190
Cifrado en reposo .....	192
Cifrado en tránsito .....	192
Administración de claves .....	192
Puntos de conexión de VPC (AWS PrivateLink) .....	194
Desactivación .....	197

Administración de identidades y accesos .....	197
Público .....	198
Autenticación con identidades .....	198
Administración de acceso mediante políticas .....	202
Cómo funciona Amazon Fraud Detector con IAM .....	204
Ejemplos de políticas basadas en identidades .....	209
Prevención del suplente confuso .....	217
Solución de problemas .....	220
Supervisión de Amazon Fraud Detector .....	223
Validación de conformidad .....	223
Resiliencia .....	224
Seguridad de infraestructuras .....	225
Supervise Amazon Fraud Detector .....	226
Monitorear con CloudWatch .....	226
Uso de CloudWatch métricas para Amazon Fraud Detector. ....	227
Métricas de Amazon Fraud Detector .....	229
Registro de llamadas a la API de Amazon Fraud Detector con AWS CloudTrail .....	234
Información sobre Amazon Fraud Detector en CloudTrail .....	234
Descripción de las entradas de los archivos de registro de Amazon Fraud Detector .....	235
Solucionar problemas .....	237
Solucione problemas con los datos de formación .....	237
Tasa de fraude inestable en el conjunto de datos dado .....	238
Datos insuficientes .....	238
Faltan valores de EVENT_LABEL o son diferentes .....	241
Faltan valores de EVENT_TIMESTAMP o son incorrectos .....	242
Datos no ingeridos .....	243
Variables insuficientes .....	244
Falta el tipo de variable o es incorrecto .....	245
Faltan valores de variables .....	245
Valores de variables únicas insuficientes .....	246
Expresión de variable incorrecta .....	246
Entidades únicas insuficientes .....	248
Cuotas .....	249
Modelos Fraud Detector de .....	249
Detectores de fraudes de Amazon, variables, resultados, reglas .....	249
API Fraud Detector de .....	250

---

Historial de documentos .....	252
.....	cclvii



# ¿Qué es Amazon Fraud Detector?

Amazon Fraud Detector es un servicio de detección de fraudes totalmente gestionado que automatiza la detección de posibles actividades fraudulentas en línea. Estas actividades incluyen transacciones no autorizadas y la creación de cuentas falsas. Amazon Fraud Detector funciona mediante el aprendizaje automático para analizar sus datos. Lo hace de una manera que se basa en la experiencia acumulada durante más de 20 años en la detección de fraudes en Amazon.

Puede utilizar Amazon Fraud Detector para crear modelos de detección de fraudes personalizados, añadir lógica de decisión para interpretar las evaluaciones de fraude del modelo y asignar resultados como aprobar o enviar para su revisión cada posible evaluación de fraude. Con Amazon Fraud Detector, no necesitas experiencia en aprendizaje automático para detectar actividades fraudulentas.

Para empezar, recopile y prepare los datos sobre el fraude que recopiló en su organización. Luego, Amazon Fraud Detector utiliza estos datos para entrenar, probar e implementar un modelo de detección de fraudes personalizado en tu nombre. Como parte de este proceso, Amazon Fraud Detector utiliza modelos de aprendizaje automático que han aprendido los patrones de fraude AWS y de la propia experiencia de Amazon en materia de fraude para evaluar sus datos de fraude y generar puntuaciones y datos de rendimiento de los modelos. Usted configura la lógica de decisiones para interpretar la puntuación del modelo y asignar resultados sobre cómo abordar cada evaluación de fraude.

## Ventajas

Amazon Fraud Detector ofrece las siguientes ventajas. Estos beneficios le permiten detectar el fraude rápidamente sin tener que invertir el tiempo y los recursos que tradicionalmente se requieren para crear y mantener un sistema de gestión del fraude.

### Creación automatizada de modelos de fraude

Los modelos de detección de fraudes de Amazon Fraud Detector son modelos de aprendizaje automático totalmente automatizados y personalizados para satisfacer sus necesidades empresariales específicas. Puedes usar los modelos de Amazon Fraud Detector para identificar posibles fraudes en cualquier transacción en línea, como la creación de nuevas cuentas, los pagos en línea y el proceso de pago como invitado.

Como los modelos de fraude se crean mediante un proceso automatizado, puedes prescindir de muchos de los pasos relacionados con la creación y el entrenamiento de un modelo. Estos pasos

incluyen la validación y el enriquecimiento de los datos, la ingeniería de características, la selección de algoritmos, el ajuste de los hiperparámetros y la implementación del modelo.

Para crear un modelo de detección de fraudes con Amazon Fraud Detector, solo debes cargar el conjunto de datos históricos de fraudes de tu empresa y seleccionar el tipo de modelo. A continuación, Amazon Fraud Detector encuentra automáticamente el algoritmo de detección de fraudes más adecuado para su caso de uso y crea el modelo. No necesita saber programación ni tener experiencia en aprendizaje automático para crear modelos de detección de fraudes.

## Modelos de fraude que evolucionan y aprenden

Los modelos de detección del fraude deben evolucionar constantemente para mantenerse al día con el cambiante panorama del fraude. Amazon Fraud Detector lo hace automáticamente calculando información como la antigüedad de la cuenta, el tiempo transcurrido desde la última actividad y el recuento de actividades. El resultado es que su modelo descubre la diferencia entre los clientes de confianza que realizan transacciones con frecuencia y los intentos continuos típicos de los estafadores. Esto ayuda a mantener el rendimiento del modelo durante más tiempo entre las sesiones de reentrenamiento.

## Visualización del rendimiento del modelo de fraude

Después de entrenar tu modelo con los datos que nos has proporcionado, Amazon Fraud Detector valida el rendimiento de tu modelo. También proporciona herramientas visuales para evaluar el rendimiento. Para cada modelo que entrenes, puedes ver la puntuación de rendimiento del modelo, el gráfico de distribución de puntuaciones, la matriz de confusión, la tabla de umbrales y todas las entradas que proporcionaste clasificadas según su impacto en el rendimiento del modelo. Con estas herramientas de rendimiento, puede conocer el rendimiento de su modelo y qué entradas lo impulsan. Si es necesario, puede ajustar el modelo para mejorar su rendimiento general.

## Predicción de fraudes

Amazon Fraud Detector genera predicciones de fraude para las actividades comerciales de su organización. La predicción del fraude es una evaluación del riesgo de fraude de una actividad empresarial. Amazon Fraud Detector genera predicciones mediante la lógica de predicción con los datos asociados a la actividad. Proporcionaste estos datos cuando creaste tu modelo de detección de fraudes. Puede obtener predicciones de fraude para una sola actividad en tiempo real o desconectarlas para un conjunto de actividades.

## Predicción de fraudes, explicación y visualización

Amazon Fraud Detector genera explicaciones de predicción como parte del proceso de predicción del fraude. Las explicaciones de las predicciones proporcionan información sobre la forma en que cada elemento de datos utilizado para entrenar su modelo ha influido en la puntuación de predicción de fraudes de su modelo. Las explicaciones de las predicciones se proporcionan mediante herramientas visuales, como tablas y gráficos. Puede utilizar estas herramientas para identificar visualmente la influencia que tiene cada elemento de datos en las puntuaciones de predicción. Luego, puede usar esta información para analizar los patrones de fraude en su conjunto de datos y detectar cualquier sesgo, si lo hubiera. Por último, también puede utilizar las explicaciones de las predicciones para identificar los principales indicadores de riesgo durante un proceso manual de investigación de fraudes. Esto le ayuda a reducir las causas fundamentales que conducen a las predicciones de falsos positivos.

### Acciones basadas en reglas

Una vez que haya entrenado su modelo de detección de fraudes, puede añadir reglas para tomar medidas con los datos evaluados, como aceptar los datos, enviarlos para su revisión o recopilar más datos. Una regla es una condición que indica a Amazon Fraud Detector cómo interpretar los datos durante la predicción del fraude. Por ejemplo, puede crear una regla que señale las cuentas de clientes sospechosas para que sean revisadas. Puedes configurar esta regla para que se inicie si la puntuación del modelo detectada es superior a tu umbral predeterminado y si el código de autorización del pago de la cuenta (AUTH\_CODE) no es válido.

## Conceptos y términos principales

La siguiente es una lista de los conceptos y términos principales que se utilizan en Amazon Fraud Detector:

### Evento

Un evento es la actividad empresarial de su organización que se evalúa en función del riesgo de fraude. Amazon Fraud Detector genera predicciones de fraude para eventos.

### Etiqueta

Una etiqueta clasifica un solo evento como fraudulento o legítimo. Las etiquetas se utilizan para entrenar modelos de aprendizaje automático en Amazon Fraud Detector.

## Entidad

Una entidad representa quién está realizando el evento. Usted proporciona el identificador de la entidad como parte de los datos de fraude de su empresa para indicar la entidad específica que llevó a cabo el evento.

## Tipo de evento

Un tipo de evento define la estructura de un evento enviado a Amazon Fraud Detector. Esto incluye los datos enviados como parte del evento, la entidad que organiza el evento (por ejemplo, un cliente) y las etiquetas que clasifican el evento. Los ejemplos de tipos de eventos incluyen las transacciones de pago en línea, los registros de cuentas y la autenticación.

## Tipo de identidad

Un tipo de entidad clasifica la entidad. Las clasificaciones de ejemplo incluyen cliente, comerciante o cuenta.

## Conjunto de datos de eventos

El conjunto de datos de eventos son los datos históricos de su empresa sobre una actividad empresarial o un evento específicos. Por ejemplo, el evento de tu empresa podría ser el registro de una cuenta en línea. Los datos de un solo evento (registro) pueden incluir la dirección IP asociada, la dirección de correo electrónico, la dirección de facturación y la marca horaria del evento. Proporcionas un conjunto de datos de eventos a Amazon Fraud Detector para crear y entrenar modelos de detección de fraudes.

## Modelo

Un modelo es el resultado de algoritmos de aprendizaje automático. Estos algoritmos se implementan en código y se ejecutan con los datos de eventos que usted proporciona.

## Tipo de modelo

El tipo de modelo define los algoritmos, los enriquecimientos y las transformaciones de características que se utilizan durante el entrenamiento del modelo. También define los requisitos de datos para entrenar el modelo. Estas definiciones sirven para optimizar el modelo para un tipo específico de fraude. Usted especifica el tipo de modelo que se utilizará al crear su modelo.

## Entrenamiento de modelos

El entrenamiento del modelo es el proceso de utilizar un conjunto de datos de eventos proporcionado para crear un modelo que pueda predecir eventos fraudulentos. Todos los pasos del proceso de formación del modelo están totalmente automatizados. Estos pasos incluyen la

validación de datos, la transformación de datos, la ingeniería de características, la selección de algoritmos y la optimización del modelo.

### Puntuación del modelo

La puntuación del modelo es el resultado de la evaluación de los datos históricos de fraude de su empresa. Durante el proceso de formación del modelo, Amazon Fraud Detector evalúa el conjunto de datos para detectar actividades fraudulentas y genera una puntuación entre 0 y 1000. Para esta puntuación, 0 representa un riesgo de fraude bajo, mientras que 1000 representa el riesgo de fraude más alto. La puntuación en sí misma está directamente relacionada con la tasa de falsos positivos (FPR).

### Versión del modelo

La versión de un modelo es el resultado del entrenamiento de un modelo.

### Despliegue del modelo

El despliegue del modelo es un proceso para activar una versión del modelo y ponerla a disposición para generar predicciones de fraude.

### Punto final SageMaker del modelo Amazon

Además de crear modelos con Amazon Fraud Detector, también puede utilizar puntos de enlace SageMaker de modelos alojados en las evaluaciones de Amazon Fraud Detector.

Para obtener más información sobre cómo crear un modelo SageMaker, consulte [Entrenar un modelo con](#). Amazon SageMaker

### Detector

Un detector contiene la lógica de detección, como el modelo y las reglas para un evento concreto que desee evaluar como fraude. Para crear un detector, utilice una versión modelo.

### Versión de detector

Un detector puede tener varias versiones, y cada versión tiene un estado de `DraftActive`, o `Inactive`. Solo una versión del detector puede estar en `Active` estado a la vez.

### Variable

Una variable representa un elemento de datos asociado a un evento que se desea utilizar en una predicción de fraude. Las variables pueden enviarse con un evento como parte de una predicción de fraude o derivarse, como la salida de un modelo de Amazon Fraud Detector o Amazon SageMaker.

## Regla

Una regla es una condición que indica a Amazon Fraud Detector cómo interpretar los valores de las variables durante una predicción de fraude. Una regla consta de una o más variables, una expresión lógica y uno o más resultados. Las variables utilizadas en la regla deben formar parte del conjunto de datos de eventos que evalúa el detector. Además, cada detector debe tener al menos una regla asociada.

## Resultado

Este es el resultado, o resultado, de una predicción de fraude. Cada regla que se utilice en una predicción de fraude debe especificar uno o más resultados.

## Predicción de fraude

La predicción del fraude es una evaluación del fraude, ya sea para un solo evento o para un conjunto de eventos. Amazon Fraud Detector genera predicciones de fraude para un solo evento en línea en tiempo real al proporcionar de forma sincronizada una puntuación del modelo y un resultado en función de las reglas. Amazon Fraud Detector genera predicciones de fraude para una serie de eventos fuera de línea. Puede utilizar las predicciones para realizar una evaluación offline proof-of-concept o retrospectiva del riesgo de fraude cada hora, día o semana.

## Explicación de la predicción del fraude

Las explicaciones de la predicción del fraude proporcionan información sobre el impacto de cada variable en la puntuación de predicción del fraude de su modelo. Proporciona información sobre la forma en que cada variable influye en las puntuaciones de riesgo en términos de magnitud (de 0 a 5, siendo 5 la puntuación más alta) y de dirección (elevando o bajando la puntuación).

# Cómo funciona Amazon Fraud Detector

Amazon Fraud Detector crea un modelo de aprendizaje automático personalizado para detectar posibles actividades fraudulentas en línea en su empresa. Para comenzar, conceda a su caso de uso empresarial. Según el caso de uso empresarial, Amazon Fraud Detector recomienda un tipo de modelo que utilizará para crear un modelo de detección de fraudes para ti. Además, también proporciona información sobre los elementos de datos que debe proporcionar como parte de los datos históricos de su empresa. Amazon Fraud Detector utiliza el conjunto de datos históricos para crear y entrenar automáticamente un modelo personalizado para usted.

El proceso de capacitación sobre modelos automatizados implica elegir un algoritmo de aprendizaje automático que detecte el fraude para su caso de uso empresarial específico, validar los datos

que proporcionó y realizar manipulaciones de datos para mejorar el rendimiento del modelo. Tras entrenar el modelo, Amazon Fraud Detector genera las puntuaciones del modelo y otras métricas de rendimiento del modelo. Puede utilizar la puntuación y las métricas de rendimiento para evaluar el rendimiento del modelo. Si es necesario, puede añadir o eliminar elementos de datos del conjunto de datos que proporcionó para el entrenamiento y volver a entrenar el modelo para mejorar la puntuación del modelo.

Una vez creado, entrenado y activado el modelo, debe configurar la lógica de decisiones, también conocida como reglas, que indique al modelo cómo interpretar los datos generados por su empresa y asignar resultados para abordar la interpretación de cada actividad. Los resultados pueden representar acciones como la aprobación o revisión de la actividad, o pueden representar los niveles de riesgo de la actividad, como el riesgo alto, el riesgo medio y el riesgo bajo.

Un detector es un contenedor que contiene el modelo y las reglas asociadas. Deberá crear, probar e implementar el detector en su entorno de producción.

El detector instalado en su entorno de producción proporciona la capacidad de detección de fraudes a sus aplicaciones empresariales. Para realizar una evaluación del fraude, el modelo compara todos los datos entrantes de su actividad empresarial con los datos históricos de su empresa y utiliza sus sofisticados algoritmos de aprendizaje automático con las reglas que creó para analizar los resultados y asignarlos. Con Amazon Fraud Detector, puede evaluar los datos de una sola actividad empresarial en tiempo real o evaluar los datos de varias actividades empresariales fuera de línea.

Supongamos que tiene una empresa que tiene la transferencia de fondos en línea como una de sus actividades. Quiere usar Amazon Fraud Detector para detectar solicitudes fraudulentas de transferencia de fondos en tiempo real. Para empezar, primero tendrás que proporcionar a Amazon Fraud Detector los datos de las solicitudes de transferencia de fondos anteriores. Amazon Fraud Detector utiliza estos datos para crear y entrenar un modelo personalizado para detectar solicitudes fraudulentas de transferencias de fondos. A continuación, se crea un detector añadiendo el modelo y configurando las reglas para que el modelo interprete los datos. Un ejemplo de regla para la actividad de transferencia de fondos en línea puede ser si la solicitud de transferencia de fondos proviene de `dexyz@example.com` dirección de correo electrónico, envíe la solicitud de revisión. En el entorno de producción de su empresa, cuando llega una solicitud de transferencia de fondos, el modelo analiza los datos incluidos en la solicitud y utiliza la regla para asignar el resultado. A continuación, puede realizar una acción en relación con la solicitud en función del resultado asignado.

Amazon Fraud Detector utiliza componentes como el conjunto de datos de formación, el modelo, el detector, las reglas y los resultados para proporcionar a su empresa una lógica de evaluación del fraude.

Para obtener información sobre el flujo de trabajo que utilizarás para detectar el fraude con Amazon Fraud Detector, consulta [Detección de fraudes con Amazon Fraud Detector](#)

## Detección de fraudes con Amazon Fraud Detector

En esta sección se describe un flujo de trabajo típico para detectar el fraude con Amazon Fraud Detector. También resume cómo puede realizar esas tareas. El siguiente diagrama proporciona una vista general del flujo de trabajo para detectar el fraude con Amazon Fraud Detector.





La detección del fraude es un proceso continuo. Después de implementar el modelo, asegúrese de evaluar sus puntuaciones y métricas de rendimiento en función de las explicaciones de las predicciones. De este modo, puede identificar los principales indicadores de riesgo, reducir las causas fundamentales que conducen a los falsos positivos y analizar los patrones de fraude en todo su conjunto de datos para detectar sesgos, si los hay. Para aumentar la precisión de las predicciones, puedes modificar tu conjunto de datos para incluir datos nuevos o revisados. Luego, puedes volver a entrenar tu modelo con el conjunto de datos actualizado. A medida que haya más datos disponibles, seguirá reentrenando el modelo para aumentar la precisión.

## Acceso a Amazon Fraud Detector

Amazon Fraud Detector está disponible en varios formatos Regiones de AWS y se puede acceder a él mediante AWS interfaces.

### Disponibilidad

Amazon Fraud Detector está disponible en EE. UU. Este (Norte de Virginia), EE. UU. Este (Ohio), EE. UU. Oeste (Oregón), Europa (Irlanda), Asia Pacífico (Singapur) y Asia Pacífico (Sídney)Regiones de AWS.

### Interfaces

Puede crear, entrenar, implementar, probar, ejecutar y gestionar modelos y detectores de detección de fraude mediante cualquiera de las siguientes interfaces:

**AWS Management Console-** Amazon Fraud Detector proporciona una interfaz de usuario basada en la web, la consola Amazon Fraud Detector. Si te has registrado en unaCuenta de AWS, puedes acceder a la consola de Amazon Fraud Detector. Para obtener más información, consulta [Cómo configurar Amazon Fraud Detector](#).

**AWS Command Line Interface(AWS CLI) -** Proporciona una interfaz que puede utilizar para interactuar con un amplio conjunto de comandosServicios de AWS, incluido Amazon Fraud Detector, mediante comandos de la consola de línea de comandos. AWS CLIllos comandos de Amazon Fraud Detector implementan una funcionalidad equivalente a la proporcionada por la consola Amazon Fraud Detector.

**AWSSDK:** proporciona API específicas para cada idioma y gestiona muchos de los detalles de la conexión, como el cálculo de firmas, la gestión de reintentos de solicitudes y la gestión de errores.

Para obtener más información, ve a la AWS página [Herramientas para crear](#), desplázate hacia abajo hasta la sección SDK y selecciona el signo más (+) para ampliar la sección.

AWS CloudFormation- Proporciona plantillas que puede utilizar para definir sus recursos y propiedades de Amazon Fraud Detector. Para obtener más información, consulta la [referencia sobre el tipo de recurso de Amazon Fraud Detector](#) en la Guía del AWS CloudFormation usuario.

## Precios

Con Amazon Fraud Detector, solo pagas por lo que usas. No se requieren pagos mínimos ni compromisos iniciales. Se le cobrará en función de las horas de procesamiento que se utilicen para entrenar y alojar sus modelos, la cantidad de almacenamiento que utilice y la cantidad de predicciones de fraude que haga. Para obtener más información, consulta los [precios de Amazon Fraud Detector](#).

# Configurar Amazon Fraud Detector

Para utilizar Amazon Fraud Detector, primero necesita una cuenta de Amazon Web Services (AWS) y, a continuación, debe configurar los permisos que le permitan Cuenta de AWS acceder a todas las interfaces. Más adelante, cuando empiece a crear sus recursos de Amazon Fraud Detector, tendrá que conceder permisos que permitan a Amazon Fraud Detector acceder a su cuenta para realizar tareas en su nombre y acceder a los recursos de su propiedad.

Complete las siguientes tareas de esta sección para configurar el uso de Amazon Fraud Detector:

- Regístrese en AWS.
- Configura permisos que te permitan acceder Cuenta de AWS a las interfaces de Amazon Fraud Detector.
- Configura las interfaces que quieras usar para acceder a Amazon Fraud Detector.

Una vez que hayas completado estos pasos, continúa con Amazon Fraud Detector [Introducción a Amazon Fraud Detector](#) para continuar con Amazon Fraud Detector.

## Registrarse en AWS

Cuando te registras en Amazon Web Services (AWS), Cuenta de AWS se suscribe automáticamente a todos los servicios de AmazonAWS, incluido Amazon Fraud Detector. Solo se le cobrará por los servicios que utilice. Si ya dispone de una Cuenta de AWS, pase a la siguiente tarea.

## Registro para obtener una Cuenta de AWS

Si no dispone de una Cuenta de AWS, siga estos pasos para crear una.

Cómo registrarse en una Cuenta de AWS

1. Abra <https://portal.aws.amazon.com/billing/signup>.
2. Siga las instrucciones que se le indiquen.

Parte del procedimiento de registro consiste en recibir una llamada telefónica e indicar un código de verificación en el teclado del teléfono.

Al registrarse en una Cuenta de AWS, se crea un Usuario raíz de la cuenta de AWS. El usuario raíz tendrá acceso a todos los Servicios de AWS y recursos de esa cuenta. Como práctica

recomendada de seguridad, [asigne acceso administrativo a un usuario administrativo](#) y utilice únicamente el usuario raíz para realizar [tareas que requieran acceso de usuario raíz](#).

AWS le enviará un correo electrónico de confirmación luego de completar el proceso de registro. Puede ver la actividad de la cuenta y administrar la cuenta en cualquier momento entrando en <https://aws.amazon.com/> y seleccionando Mi cuenta.

## Crear un usuario administrativo

Después de suscribirse a un usuario Cuenta de AWS, Usuario raíz de la cuenta de AWS asegúrelo AWS IAM Identity Center, habilite y cree un usuario administrativo para no usar el usuario root en las tareas diarias.

### Protección de su Usuario raíz de la cuenta de AWS

1. Inicie sesión en la [AWS Management Console](#) como propietario de cuenta, elija Usuario raíz e ingrese el email de su Cuenta de AWS. En la siguiente página, escriba su contraseña.

Para obtener ayuda para iniciar sesión con el usuario raíz, consulte [Iniciar sesión como usuario raíz](#) en la Guía del usuario de AWS Sign-In.

2. Active la autenticación multifactor (MFA) para el usuario raíz.

Para obtener instrucciones, consulte [Habilitar un dispositivo MFA virtual para el usuario raíz de la Cuenta de AWS \(consola\)](#) en la Guía del usuario de IAM.

### Creación de un usuario administrativo

1. Activar IAM Identity Center

Para obtener instrucciones, consulte [Habilitación AWS IAM Identity Center](#) en la Guía AWS IAM Identity Center del usuario.

2. En el Centro de identidades de IAM, conceda acceso administrativo a un usuario administrativo.

Para ver un tutorial sobre su uso Directorio de IAM Identity Center como fuente de identidad, consulte [Configurar el acceso de los usuarios con la configuración predeterminada Directorio de IAM Identity Center](#) en la Guía del AWS IAM Identity Center usuario.

## Cómo iniciar sesión como usuario administrativo

- Para iniciar sesión con el usuario del IAM Identity Center, utilice la URL de inicio de sesión que se envió a la dirección de correo electrónico cuando creó el usuario del Centro de identidades de IAM.

Para obtener ayuda para iniciar sesión con un usuario del IAM Identity Center, consulte [Iniciar sesión en el portal de acceso de AWS](#) en la Guía del usuario de AWS Sign-In.

## Configurar permisos para acceder a las interfaces de Amazon Fraud Detector

Para usar Amazon Fraud Detector, configura los permisos para acceder a la consola de Amazon Fraud Detector y a las operaciones de la API.

Siguiendo las prácticas recomendadas de seguridad, cree un usuario AWS Identity and Access Management (IAM) con acceso restringido a las operaciones de Amazon Fraud Detector y con los permisos necesarios. Puede añadir otros permisos según sea necesario.

Las siguientes políticas proporcionan el permiso necesario para utilizar Amazon Fraud Detector:

- `AmazonFraudDetectorFullAccessPolicy`

Le permite realizar las siguientes acciones:

- Accede a todos los recursos de Amazon Fraud Detector
  - Enumere y describa todos los puntos finales del modelo en SageMaker
  - Enumere todas las funciones de IAM de la cuenta
  - Listar todos los buckets de Amazon S3
  - Permita que IAM Pass Role pase una función a Amazon Fraud Detector
- `AmazonS3FullAccess`

Permite el acceso completo a Amazon Simple Storage Service. Esto es obligatorio si necesita cargar conjuntos de datos de entrenamiento en Amazon S3.

A continuación, se describe cómo crear un usuario de IAM y asignar los permisos necesarios.

Para crear un usuario y asignar los permisos necesarios

1. Inicie sesión en la AWS Management Console y abra la consola de IAM en <https://console.aws.amazon.com/iam/>.
2. En el panel de navegación, elija Users (Usuarios) y, a continuación, elija Add user (Añadir usuario).
3. En User name (Nombre de usuario), escriba **AmazonFraudDetectorUser**.
4. Seleccione la casilla de verificación de acceso a la consola de AWS administración y, a continuación, configure la contraseña de usuario.
5. (Opcional) De forma predeterminada, AWS requiere que el nuevo usuario cree una contraseña nueva cuando inicia sesión por primera vez. Puede quitar la marca de selección de la casilla de verificación situada junto a User must create a new password at next sign-in (El usuario debe crear una nueva contraseña en el siguiente inicio de sesión) para permitir al nuevo usuario restablecer su contraseña después de iniciar sesión.
6. Elija Next: Permissions.
7. Elija Crear grupo.
8. Introduzca el nombre del grupo. **AmazonFraudDetectorGroup**
9. En la lista de políticas, seleccione la casilla de verificación correspondiente AmazonFraudDetectorFullAccessPolicy Amazon S3 FullAccess. Elija Crear grupo.
10. En la lista de grupos, active la casilla de verificación del nuevo grupo. Seleccione Actualizar si no ve el grupo en la lista.
11. Elija Next: Tags (Siguiente: Etiquetas).
12. (Opcional) Añadir metadatos al rol asociando las etiquetas como pares de clave-valor. Para obtener instrucciones sobre cómo usar las etiquetas en IAM, consulte [Etiquetar usuarios y roles de IAM](#).
13. Seleccione Siguiente: revise para ver los detalles del usuario y el resumen de los permisos del nuevo usuario. Cuando esté listo para continuar, elija Crear usuario.

## Configure las interfaces para acceder a Amazon Fraud Detector con

Puedes acceder a Amazon Fraud Detector mediante la consola o el AWS SDK de Amazon Fraud Detector. AWS CLI Antes de poder utilizarlos, primero configure el AWS SDK AWS CLI y.

## Acceda a la consola Amazon Fraud Detector

Puede acceder a la consola de Amazon Fraud Detector y a otros AWS servicios a través de la AWS Management Console. Su Cuenta de AWS, le otorga acceso a la AWS Management Console.

Para acceder a la consola de Amazon Fraud Detector,

1. Ve a <https://console.aws.amazon.com/> e inicia sesión en tu Cuenta de AWS.
2. Dirígete a Amazon Fraud Detector.

Con la consola Amazon Fraud Detector, puede crear y gestionar sus modelos y sus recursos de detección de fraudes, como detectores, variables, eventos, entidades, etiquetas y resultados. Puede generar predicciones y evaluar el rendimiento y las predicciones de su modelo.

## Configuración de AWS CLI

Puedes usar AWS Command Line Interface (AWS CLI) para interactuar con Amazon Fraud Detector ejecutando comandos en el shell de tu línea de comandos. Con una configuración mínima, puede utilizar los comandos AWS CLI para ejecutar comandos con una funcionalidad similar a la proporcionada por la consola de Amazon Fraud Detector desde la línea de comandos de su terminal.

Para configurar el AWS CLI

Descargue y configure la AWS CLI. Para obtener instrucciones, consulte los siguientes temas de la Guía del AWS Command Line Interface usuario:

- [Configuración inicial de la AWS Command Line Interface](#)
- [Configuración de la AWS Command Line Interface](#)

Para obtener información sobre los comandos de Amazon Fraud Detector, consulta [Comandos disponibles](#)

## Configurar SDK AWS

Puede usar los AWS SDK para escribir código para crear y administrar sus recursos de detección de fraudes y para obtener predicciones de fraudes. Los AWS SDK son compatibles con Amazon Fraud Detector [JavaScript](#) [Python \(Boto3\)](#).

Para configurar AWS SDK for Python (Boto3)



Se puede utilizar AWS SDK for Python (Boto3) para crear, configurar y administrar AWS servicios. Para obtener instrucciones sobre cómo instalar Boto, consulta [AWSSDK para Python \(Boto3\)](#). Asegúrese de utilizar la versión 1.14.29 o superior del SDK de Boto3.

Tras la instalación AWS SDK for Python (Boto3), ejecute el siguiente ejemplo de Python para confirmar que el entorno está configurado correctamente. Si está configurado correctamente, la respuesta contiene una lista de detectores. Si no se creó ningún detector, la lista está vacía.

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

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

Para configurar los AWS SDK para Java

Para obtener instrucciones sobre cómo instalar y cargar el AWS SDK for JavaScript, consulte [Configuración del SDK para JavaScript](#).

# Introducción a Amazon Fraud Detector

Antes de comenzar, asegúrese de haber leído [Detección de fraudes con Amazon Fraud Detector](#) y completado los pasos de [Configurar Amazon Fraud Detector](#).

Utilice los tutoriales prácticos de esta sección para obtener información sobre Amazon Fraud Detector para crear, entrenar e implementar un modelo de detección de fraude. En este tutorial, asumirá el papel de un analista de fraudes que utiliza un modelo de aprendizaje automático para predecir si el registro de una cuenta nueva es fraudulento. El modelo debe entrenarse con los datos de los registros de cuentas. Amazon Fraud Detector proporciona un ejemplo de conjunto de datos de registro de cuentas para este tutorial. El conjunto de datos de ejemplo debe cargarse antes de empezar con el tutorial.

Amazon Fraud Detector puede comenzar a utilizar una de las siguientes interfaces. Antes de comenzar con el tutorial, asegúrese de seguir las instrucciones de [Obtener y cargar un conjunto de datos de ejemplo](#)

- [Tutorial: Comience a utilizar la consola Amazon Fraud Detector](#)
- [Tutorial: Empezar a utilizar AWS SDK for Python \(Boto3\)](#)

## Obtener y cargar un conjunto de datos de ejemplo

El conjunto de datos de ejemplo que utiliza en este tutorial proporciona detalles sobre los registros de cuentas en línea. El conjunto de datos se encuentra en un archivo de texto que usa valores separados por comas (CSV) en formato UTF-8. La primera fila del archivo del conjunto de datos CSV contiene los encabezados. La fila del encabezado va seguida de varias filas de datos. Cada una de estas filas se compone de elementos de datos de un único registro de cuenta. Los datos están etiquetados para mayor comodidad. Una columna del conjunto de datos identifica si el registro de la cuenta es fraudulento.

Para obtener y cargar un conjunto de datos de ejemplo

1. Ve a [Muestras](#).

Hay dos archivos de datos que contienen datos de registro de cuentas en línea: `registration_data_20K_minimum.csv` y `registration_data_20K_full.csv`. El archivo `registration_data_20K_minimum` contiene solo dos variables: `ip_address` y

email\_address. El archivo `registration_data_20K_full` contiene otras variables. Estas variables son para cada evento e incluyen `billing_address`, `phone_number` y `user_agent`. Ambos archivos de datos también contienen dos campos obligatorios:

- `EVENT_TIMESTAMP` — Define cuándo se produjo el evento
- `EVENT_LABEL` — Clasifica el evento como fraudulento o legítimo

Puede utilizar cualquiera de los dos archivos de este tutorial. Descarga el archivo de datos que quieras usar.

## 2. Cree un bucket Amazon Simple Storage Service (Amazon S3)

En este paso, crea un almacenamiento externo para almacenar el conjunto de datos. Este almacenamiento externo es un bucket de Amazon S3. Para obtener más información acerca de Amazon S3, consulte [¿Qué es Amazon S3?](#)

- a. Inicie sesión en la AWS Management Console y abra la consola de Amazon S3 en <https://console.aws.amazon.com/s3/>.
  - b. En Depósitos, selecciona Crear depósito.
  - c. En Bucket name (Nombre del bucket), introduzca un nombre de bucket. Asegúrese de seguir las reglas de nomenclatura de depósitos de la consola y proporcione un nombre único a nivel mundial. Le recomendamos que utilice un nombre que describa el propósito del depósito.
  - d. En Región de AWS este caso, elija la Región de AWS en la que desea crear el bucket. La región que elija debe ser compatible con Amazon Fraud Detector. Para reducir la latencia, elige el Región de AWS que esté más cerca de tu ubicación geográfica. Para obtener una lista de las regiones que admiten Amazon Fraud Detector, consulte la [tabla de regiones](#) de la Guía de infraestructura global.
  - e. Deje la configuración predeterminada para la propiedad del objeto, la configuración del bucket para bloquear el acceso público, el control de versiones del bucket y las etiquetas para este tutorial.
  - f. Para el cifrado predeterminado, seleccione Desactivar en este tutorial.
  - g. Revisa la configuración del depósito y, a continuación, selecciona Crear depósito.
- ## 3. Cargue un archivo de datos de ejemplo en un bucket de Amazon S3.

Ahora que tiene un bucket, suba uno de los archivos de ejemplo que descargó anteriormente al bucket de Amazon S3 que acaba de crear.

- a. En los Buckets, aparece el nombre del bucket. Elija el bucket.
- b. Seleccione Upload (Cargar).
- c. En Archivos y carpetas, selecciona Agregar archivos.
- d. Elija uno de los archivos de datos de ejemplo que descargó en su equipo y, a continuación, elija Abrir.
- e. Deje la configuración predeterminada para Destino, Permisos y Propiedades.
- f. Revise las configuraciones y, a continuación, seleccione Cargar.
- g. El archivo de datos de ejemplo se carga en un bucket de Amazon S3. Anote la ubicación del bucket. En Objetos, elige el archivo de datos de ejemplo que acabas de cargar.
- h. En la descripción general del objeto, copie la ubicación en el URI de S3. Esta es la ubicación de Amazon S3 de su archivo de datos de ejemplo. Lo usará más adelante. También, puede copiar el nombre de recurso de Amazon (ARN) de su bucket S3 y guardarlo.

## Tutorial: Comience a utilizar la consola Amazon Fraud Detector

Este tutorial consta de dos partes. La primera parte describe cómo crear, entrenar e implementar un modelo de detección de fraudes. La segunda parte trata sobre cómo utilizar el modelo para generar predicciones de fraude en tiempo real. El modelo se entrena con el archivo de datos de ejemplo que se carga en un bucket de S3. Al final de este tutorial, deberá realizar las siguientes acciones:

- Cree y entrene un modelo de Fraud Detector Amazon
- Genere predicciones de fraude en tiempo real

### Important

Antes de continuar, asegúrese de haber seguido las instrucciones de [Obtener y cargar un conjunto de datos de ejemplo](#)

## Parte A: Cree, entrene e implemente un modelo de Fraud Detector Amazon

En la parte A, define su caso de uso empresarial, define su evento, crea un modelo, entrena el modelo, evalúa el rendimiento del modelo e implementa el modelo.

## Paso 1: Elegir un caso de uso empresarial

- En este paso, utilizará el explorador de modelos de datos para hacer coincidir su caso de uso empresarial con los tipos de modelos de detección de fraudes compatibles con Amazon Fraud Detector. El explorador de modelos de datos es una herramienta integrada en la consola de Amazon Fraud Detector que recomienda un tipo de modelo para crear y entrenar un modelo de detección de fraudes para su caso práctico empresarial. El explorador de modelos de datos también proporciona información sobre los elementos de datos obligatorios, recomendados y opcionales que deberá incluir en su conjunto de datos. El conjunto de datos se utilizará para crear y entrenar su modelo de detección de fraudes.

A los efectos de este tutorial, su caso de uso empresarial son los registros de cuentas nuevas. Tras especificar su caso de uso empresarial, el explorador de modelos de datos le recomendará un tipo de modelo para crear un modelo de detección de fraudes y también le proporcionará una lista de los elementos de datos que necesitará para crear su conjunto de datos. Como ya ha cargado un conjunto de datos de muestra que contiene datos de nuevos registros de cuentas, no necesita crear un conjunto de datos nuevo.

- a. Abre la [consolaAWS de administración](#) e inicia sesión en tu cuenta. Navegue hasta Amazon Fraud Detector.
- b. En el panel de navegación izquierdo, elija Explorador de modelos de datos.
- c. En la página del explorador de modelos de datos, en Caso de uso empresarial, seleccione Fraude en una cuenta nueva.
- d. Amazon Fraud Detector muestra el tipo de modelo recomendado para crear un modelo de detección de fraudes para el caso de uso empresarial seleccionado. El tipo de modelo define los algoritmos, los enriquecimientos y las transformaciones que Amazon Fraud Detector utilizará para entrenar su modelo de detección de fraudes.

Anote el tipo de modelo recomendado. Lo necesitará más adelante cuando cree su modelo.

- e. El panel de información del modelo de datos proporciona información sobre los elementos de datos obligatorios y recomendados necesarios para crear y entrenar un modelo de detección de fraudes.

Eche un vistazo al conjunto de datos de ejemplo que ha descargado y asegúrese de que contiene todos los elementos de datos obligatorios y algunos recomendados en la tabla.

Más adelante, cuando cree un modelo para su caso de uso empresarial específico, utilizará la información proporcionada para crear su conjunto de datos.

## Paso 2: Crear un tipo de evento

- En este paso, definirá la actividad empresarial (evento) que se va a evaluar para detectar el fraude. Definir el evento implica establecer las variables que se encuentran en el conjunto de datos, la entidad que inicia el evento y las etiquetas que clasifican el evento. Para este tutorial, defina el evento de registro de la cuenta.
  - a. Abra la [consolaAWS de administración](#) e inicia sesión en tu cuenta. Navegue hasta Amazon Fraud Detector.
  - b. En el panel de navegación izquierdo, elija Events.
  - c. En la página Tipo de eventos, selecciona Crear.
  - d. En Detalles del tipo de evento, introduzca `sample_registration` el nombre del tipo de evento y, si lo desea, introduzca una descripción del evento.
  - e. En Entidad, elija Crear entidad.
  - f. En la página Crear entidad, introduzca `sample_customer` el nombre del tipo de entidad. De manera opcional, ingrese una descripción del tipo de entidad.
  - g. Seleccione Create entity (Crear entidad).
  - h. En Variables de eventos, en Elegir cómo definir las variables de este evento, elija Seleccionar variables de un conjunto de datos de entrenamiento.
  - i. Para el rol de IAM, elija Crear rol de IAM.
  - j. En la página Crear rol de IAM, introduzca el nombre del bucket de S3 en el que cargó los datos de ejemplo y seleccione Crear rol.
  - k. En Ubicación de datos, introduce la ruta a los datos de ejemplo. Esta es la S3 URI ruta que guardó después de cargar los datos del ejemplo. La ruta es similar a esta: `S3://your-bucket-name/example dataset filename.csv`.
  - l. Seleccione Upload (Cargar).

Amazon Fraud Detector extrae los encabezados del archivo de datos de ejemplo y los asigna con un tipo de variable. El mapeo aparece en la consola.
  - m. En Etiquetas (opcional), en Etiquetas, selecciona Crear etiquetas nuevas.
  - n. En Crear página de etiquetas, introduzca `fraud` el nombre. Esta etiqueta corresponde al valor que representa el registro de una cuenta fraudulenta en el conjunto de datos de ejemplo.
  - o. Seleccione Crear etiqueta.

- p. Crea una segunda etiqueta y, a continuación, `legit` introdúcela como nombre. Esta etiqueta corresponde al valor que representa el registro legítimo de la cuenta en el conjunto de datos de ejemplo.
- q. Elige Crear tipo de evento.

### Paso 3: Crear un modelo

1. En la página Modelos, elija Agregar modelo y, a continuación, elija Crear modelo.
2. Para el paso 1: Definir los detalles del modelo, `sample_fraud_detection_model` introdúzcalo como nombre del modelo. De manera opcional, agregue una descripción del modelo.
3. Para el tipo de modelo, elija el modelo Online Fraud Insights.
4. En Tipo de evento, elija `sample_registration`. Este es el tipo de evento que ha creado en el Paso 1.
5. En los datos de eventos históricos,
  - a. En Fuente de datos de eventos, elija Datos de eventos almacenados en S3.
  - b. En el caso del rol de IAM, seleccione el rol que creó en el Paso 1.
  - c. En Ubicación de datos de entrenamiento, introduzca la ruta URI de S3 a su archivo de datos de ejemplo.
6. Elija Siguiente.

### Paso 4: Modelo de tren

1. En las entradas del modelo, deje marcadas todas las casillas de verificación. De forma predeterminada, Amazon Fraud Detector utiliza todas las variables del conjunto de datos de eventos históricos como entradas del modelo.
2. En la clasificación de etiquetas, para las etiquetas de fraude, elija fraude, ya que esta etiqueta corresponde al valor que representa los eventos fraudulentos en el conjunto de datos del ejemplo. Para las etiquetas legítimas, elija legítimo, ya que esta etiqueta corresponde al valor que representa los eventos legítimos en el conjunto de datos de ejemplo.
3. Para el tratamiento de eventos sin etiqueta, mantenga la selección predeterminada Omitir eventos sin etiqueta para este conjunto de datos de ejemplo.
4. Elija Siguiente.

5. Tras revisarlo, seleccione Crear y entrenar el modelo. Amazon Fraud Detector crea un modelo y comienza a entrenar una nueva versión del modelo.

En las versiones del modelo, la columna Estado indica el estado del entrenamiento del modelo. El entrenamiento con modelos que utiliza el conjunto de datos de ejemplo tarda aproximadamente 45 minutos en completarse. El estado cambia a Listo para desplegarse una vez finalizado el entrenamiento del modelo.

### Paso 5: Revisar el rendimiento del modelo

Un paso importante a la hora de utilizar Amazon Fraud Detector es evaluar la precisión del modelo mediante las puntuaciones del modelo y las métricas de rendimiento. Una vez finalizado el entrenamiento del modelo, Amazon Fraud Detector valida el rendimiento del modelo utilizando el 15% de los datos que no se utilizó para entrenar el modelo y genera una puntuación de rendimiento del modelo y otras métricas de rendimiento.

1. Para ver el rendimiento del modelo,
  - a. En el panel de navegación izquierdo de la consola de Amazon Fraud Detector, elija Modelos.
  - b. En la página Modelos, elige el modelo que acabas de entrenar (sample\_fraud\_detection\_model) y, a continuación, elige 1.0. Esta es la versión que Amazon Fraud Detector creó de su modelo.
2. Observe la puntuación general del rendimiento del modelo y todas las demás métricas que Amazon Fraud Detector generó para este modelo.

Para obtener más información sobre la puntuación de rendimiento del modelo y las métricas de rendimiento en esta página, consulte [Puntuaciones del modelo](#) y [Métricas de rendimiento del modelo](#).

Puede esperar que todos sus modelos de Amazon Fraud Detector capacitados tengan métricas de rendimiento de detección de fraudes del mundo real similares a las métricas de rendimiento que ve para el modelo en este tutorial.

### Paso 6: Implementar el modelo

Una vez que haya revisado las métricas de rendimiento de su modelo entrenado y esté listo para usarlo para generar predicciones de fraude, podrá implementar el modelo.



1. En el panel de navegación izquierdo de la consola de Amazon Fraud Detector, seleccione Modelos.
2. En la página Modelos, elija `sample_fraud_detection_model` y, a continuación, elija la versión específica del modelo que desee implementar. Para este tutorial, elija 1.0.
3. En la página Versión del modelo, elija Acciones y, a continuación, elija Implementar versión del modelo.
4. En las versiones del modelo, el estado muestra el estado de la implementación. El estado cambia a Activo una vez finalizada la implementación. Esto indica que la versión del modelo está activada y disponible para generar predicciones de fraude. [Parte B: Generar predicciones de fraude](#) Continúe con los pasos completos para generar predicciones de fraude.

## Parte B: Generar predicciones de fraude

La predicción del fraude es una evaluación del fraude para una actividad empresarial (evento). Amazon Fraud Detector utiliza detectores para generar predicciones de fraude. Un detector contiene la lógica de detección, como modelos y reglas, para un evento específico que se desea evaluar para determinar si es un fraude. La lógica de detección utiliza reglas para indicar a Amazon Fraud Detector cómo interpretar los datos asociados al modelo. En este tutorial, evaluará el evento de registro de la cuenta mediante el conjunto de datos de ejemplo de registro de cuenta que cargó anteriormente.

En la parte A, creó, entrenó e implementó su modelo. En la parte B, crea un detector para el tipo `sample_registration` evento, agrega el modelo implementado, crea reglas y una orden de ejecución de reglas y, a continuación, crea y activa una versión del detector que se utiliza para generar predicciones de fraude.

### Paso 1: Crear un detector

Para crear un detector

1. En el panel de navegación izquierdo de la consola de Amazon Fraud Detector, elija Detectores.
2. Seleccione Crear detector.
3. En la página Definir detalles del detector, introduzca `sample_detector` el nombre del detector. De manera opcional, ingrese una descripción para el detector, como `sample fraud detector`.
4. En Tipo de evento, seleccione `sample_registration`. Este es el evento que creó en la parte A de este tutorial.

## 5. Elija Siguiente.

### Paso 2: Agregar el modelo

Si ha completado la parte A de este tutorial, es probable que ya tenga un modelo de Fraud Detector de Amazon disponible para agregarlo a su detector. Si aún no ha creado un modelo, vaya a la parte A y complete los pasos para crear, entrenar e implementar un modelo y, a continuación, continúe con la parte B.

1. En Añadir modelo (opcional), selecciona Añadir modelo.
2. En la página Agregar modelo, en Seleccionar modelo, elija el nombre del modelo de Amazon Fraud Detector que implementó anteriormente. En Seleccionar versión, elija la versión del modelo implementado.
3. Elija Add model (Añadir modelo).
4. Elija Siguiente.

### Paso 3: Agregar reglas

Una regla es una condición que indica a Amazon Fraud Detector cómo interpretar la puntuación de rendimiento del modelo al evaluar la predicción de fraude. Para este tutorial, debe crear tres reglas: `high_fraud_risk`, `medium_fraud_risk`, y `low_fraud_risk`.

1. En la página Agregar reglas, en Definir una regla, introduzca `high_fraud_risk` el nombre de la regla y, en Descripción (opcional), introduzca **This rule captures events with a high ML model score** la descripción de la regla.
2. En Expresión, introduzca la siguiente expresión de regla mediante el lenguaje de expresiones de reglas simplificado de Amazon Fraud Detector:

```
$sample_fraud_detection_model_insightscore > 900
```

3. En Resultados, selecciona Crear un nuevo resultado. Un resultado es el resultado de una predicción de fraude y se devuelve si la regla coincide durante una evaluación.
4. En Crear un nuevo resultado, introduzca `verify_customer` el nombre del resultado. De manera opcional, ingrese una descripción.
5. Selecciona Guardar resultado.

6. Seleccione Agregar regla para ejecutar el comprobador de validación de reglas y guardar la regla. Una vez creada, Amazon Fraud Detector hace que la regla esté disponible para su uso en su detector.
7. Elija Agregar otra regla y, a continuación, elija la pestaña Crear regla.
8. Repita este proceso dos veces más para crear sus `low_fraud_risk` y `medium_fraud_risk` reglas y utilice los siguientes detalles de la regla:

- riesgo de fraude medio

Nombre de la regla: `medium_fraud_risk`

Resultado: `review`

Expresión:

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

```
$sample_fraud_detection_model_insightscore > 700
```

- bajo riesgo de fraude

Nombre de la regla: `low_fraud_risk`

Resultado: `approve`

Expresión:

```
$sample_fraud_detection_model_insightscore <= 700
```

Estos valores son ejemplos utilizados en este tutorial. Cuando cree reglas para su propio detector, utilice valores que sean apropiados para su modelo y su caso de uso,

9. Después de crear las tres reglas, seleccione Siguiente.

Para obtener más información acerca de cómo crear y escribir reglas, consulte [Reglas y Referencia al lenguaje de las reglas](#).

## Paso 4: Configurar la ejecución de las reglas y el orden de las reglas

El modo de ejecución de reglas de las reglas que se incluyen en el detector determina si se evalúan todas las reglas que defina o si la evaluación de las reglas se detiene en la primera regla coincidente. Y el orden de las reglas determina el orden en el que desea que se ejecute la regla.

El modo de ejecución de reglas predeterminado es `FIRST_MATCHED`.

### Primer emparejado

El modo de ejecución de la primera regla coincidente devuelve los resultados de la primera regla coincidente en función del orden de reglas definido. Si especifica `FIRST_MATCHED`, Amazon Fraud Detector evalúa las reglas secuencialmente, de la primera a la última, y se detiene en la primera regla que coincida. Amazon Fraud Detector proporciona los resultados de esa regla única.

El orden en el que se ejecutan las reglas puede afectar al resultado de la predicción de fraudes resultante. Después de crear las reglas, reordene las reglas para ejecutarlas en el orden deseado siguiendo estos pasos:

Si la `high_fraud_risk` regla aún no aparece en la parte superior de la lista de reglas, selecciona Ordenar y, a continuación, elige 1. Esto pasará `high_fraud_risk` a la primera posición.

Repita este proceso para que la `medium_fraud_risk` regla esté en la segunda posición y la `low_fraud_risk` regla en la tercera posición.

### Todos coincidentes

El modo de ejecución de todas las reglas coincidentes devuelve los resultados de todas las reglas coincidentes, independientemente del orden de las reglas. Si lo especifica `ALL_MATCHED`, Amazon Fraud Detector evalúa todas las reglas y devuelve los resultados de todas las reglas coincidentes.

Seleccione `FIRST_MATCHED` este tutorial y, a continuación, elija Siguiente.

## Paso 5: Revisar y Crear la versión del detector

Una versión de detector define los modelos y reglas específicos que se utilizan para generar predicciones de fraude.

1. En la página Revisar y crear, revise los detalles, los modelos y las reglas del detector que configuró. Si necesitas hacer algún cambio, selecciona Editar junto a la sección correspondiente.
2. Selecciona Crear detector. Una vez creado, la primera versión del detector aparece en la tabla de versiones del detector con el `Draft` estado.

Utiliza la versión preliminar para probar el detector.

## Paso 6: Probar y activar la versión del detector

En la consola de Amazon Fraud Detector, puede probar la lógica del detector mediante datos simulados con la función Ejecutar prueba. Para este tutorial, puede utilizar los datos de registro de la cuenta del conjunto de datos de ejemplo.

1. Desplázate hasta Ejecutar prueba en la parte inferior de la página de detalles de la versión de Detector.
2. Para los metadatos del evento, introduzca una marca de tiempo en la que se produjo el evento e introduzca un identificador único para la entidad que realiza el evento. Para este tutorial, seleccione una fecha en el selector de fechas para la marca de tiempo e introduzca «1234» como ID de entidad.
3. En Variable de evento, introduzca los valores de la variable que desee probar. Para este tutorial, solo necesitas `ip_address` y `email_address`. Esto se debe a que son las entradas que se utilizan para entrenar su modelo de Fraud Detector Amazon. Puede realizar una prueba con los siguientes valores de ejemplo. Esto supone que ha utilizado los nombres de variables sugeridos:
  - dirección\_IP:205.251.233.178
  - dirección\_de\_correo electrónico:john.doe@exampledomain.com
4. Selecciona Ejecutar prueba.
5. Amazon Fraud Detector devuelve el resultado de la predicción del fraude en función del modo de ejecución de la regla. Si el modo de ejecución de la regla es `FIRST_MATCHED`, el resultado devuelto corresponde a la primera regla que coincidió. La primera regla es la regla con la prioridad más alta. Coincide si se evalúa como verdadera. Si el modo de ejecución de la regla es `ALL_MATCHED`, el resultado devuelto corresponde a todas las reglas que coincidieron. Eso significa que todos se evalúan como verdaderos. Amazon Fraud Detector también devuelve la puntuación del modelo de todos los modelos añadidos al detector.

Puede cambiar las entradas y ejecutar un par de pruebas para ver diferentes resultados. Puedes usar los valores `ip_address` y `email_address` de tu conjunto de datos de ejemplo para las pruebas y comprobar si los resultados son los esperados.

6. Cuando esté satisfecho con el funcionamiento del detector, promuévalo de `Draft` a `Active`. De este modo, el detector estará disponible para su uso en la detección de fraudes en tiempo real.

En la página de detalles de la versión de Detector, elija `Acciones`, `Publicar`, `Publicar versión`. Esto cambia el estado del detector de `Borrador` a `Activo`.

En este punto, su modelo y la lógica de detección asociada están listos para evaluar las actividades en línea en busca de fraude en tiempo real mediante la `GetEventPrediction` API de Fraud Detector de Amazon. También puedes evaluar los eventos sin conexión mediante un archivo de entrada CSV y la `CreateBatchPredictionJob` API. Para obtener más información acerca de la predicción de fraudes, consulte [Predicciones de fraude](#)

Al completar este tutorial, ha hecho lo siguiente:

- Cargué un conjunto de datos de eventos de ejemplo en Amazon S3.
- Creé y entrené un modelo de detección de fraudes de Amazon Fraud Detector utilizando el conjunto de datos de ejemplo.
- Consultó la puntuación de rendimiento del modelo y otras métricas de rendimiento que generó Amazon Fraud Detector.
- Implementé el modelo de detección de fraudes.
- Creó un detector y agregó el modelo implementado.
- Se agregaron reglas, el orden de ejecución de las reglas y los resultados al detector.
- Probé el detector proporcionando diferentes entradas y comprobando si las reglas y el orden de ejecución de las reglas funcionaban según lo esperado.
- Se activó el detector publicándolo.

## Tutorial: Empezar a utilizar AWS SDK for Python (Boto3)

Este tutorial describe cómo crear y entrenar un modelo de Fraud Detector de Amazon y, a continuación, cómo utilizar este modelo para generar predicciones de fraude en tiempo real mediante

elAWS SDK for Python (Boto3). El modelo se entrena mediante el archivo de datos de ejemplo de registro de cuentas que se sube al bucket de Amazon S3.

Al final de este tutorial, aprenderá a completar las siguientes acciones:

- Cree y entrene un modelo de Fraud Detector Amazon
- Genere predicciones de fraude en tiempo real

## Requisitos previos

Los pasos siguientes son requisitos previos para este tutorial.

- Completado [Configurar Amazon Fraud Detector](#).

Si ya lo has hecho [Configurar SDK AWS](#), asegúrate de utilizar la versión 1.14.29 o superior del SDK de Boto3.

- He seguido las instrucciones para [Obtener y cargar un conjunto de datos de ejemplo](#) archivar las necesarias para este tutorial.

## Introducción

### Paso 1: Configuración y verificación del entorno de Python

Boto es el SDK de Amazon Web Services (AWS) para Python. Puede usarlo para crear, configurar y administrar Servicios de AWS. Para obtener instrucciones sobre cómo instalar Boto3, consulte [AWS para Python \(Boto3\)](#).

Tras la instalaciónAWS SDK for Python (Boto3), ejecute el siguiente comando de ejemplo de Python para confirmar que el entorno está configurado correctamente. Si el entorno está configurado correctamente, la respuesta contiene una lista de detectores. Si no se creó ningún detector, la lista está vacía.

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

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

## Paso 2: Crear variables, tipos de entidad y etiquetas

En este paso, crea recursos que se utilizan para definir el modelo, el evento y las reglas.

### Crear una variable

Una variable es un elemento de datos de tu conjunto de datos que deseas usar para crear tipos de eventos, modelos y reglas.

En el siguiente ejemplo, la [CreateVariable](#) API se usa para crear dos variables. Las variables son `email_address` y `ip_address`. Asígnelas a los tipos de variables correspondientes: `EMAIL_ADDRESS` y `IP_ADDRESS`. Estas variables forman parte del conjunto de datos de ejemplo que has subido. Al especificar el tipo de variable, Amazon Fraud Detector interpreta la variable durante el entrenamiento del modelo y al obtener las predicciones. Solo las variables con un tipo de variable asociado se pueden utilizar para el entrenamiento del modelo.

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

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

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

### Crear tipo de entidad

Una entidad representa quién está realizando el evento y un tipo de entidad clasifica la entidad. Entre las clasificaciones de ejemplo se incluyen el cliente, el comerciante o la cuenta.



En el siguiente ejemplo, la [PutEntityType](#) API se usa para crear un tipo `sample_customer` entidad.

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

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

### Crear etiqueta

Una etiqueta clasifica un evento como fraudulento o legítimo y se utiliza para formar el modelo de detección del fraude. El modelo aprende a clasificar los eventos mediante estos valores de etiqueta.

En el siguiente ejemplo, la API [Putlabel](#) se usa para crear dos etiquetas, `fraud` y `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'
)
```

### Paso 3: crear un tipo de evento

Con Amazon Fraud Detector, genere modelos que evalúen los riesgos y genere predicciones de fraude para eventos individuales. Un tipo de evento define la estructura de un evento individual.

En el siguiente ejemplo, la [PutEventType](#) API se usa para crear un tipo de evento `sample_registration`. Para definir el tipo de evento, especifique las variables

(`email_address`,`ip_address`), el tipo de entidad (`sample_customer`) y las etiquetas (`fraud`,`legit`) que creó en el paso anterior.

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

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

#### Paso 4: Crear, entrenar e implementar el modelo

Amazon Fraud Detector entrena a los modelos para que aprendan a detectar el fraude para un tipo de evento específico. En el paso anterior, creó el tipo de evento. En este paso, creará y formó un modelo para el tipo de evento. El modelo actúa como un contenedor para las versiones del modelo. Cada vez que entrene un modelo, se crea una nueva versión.

Utilice los siguientes códigos de ejemplo para crear y entrenar un modelo de Online Fraud Insights. Este modelo se llama `sample_fraud_detection_model`. Es para el tipo de evento `sample_registration` utiliza el conjunto de datos de ejemplo de registro de cuentas que ha subido a Amazon S3.

Para obtener más información sobre los diferentes tipos de modelos compatibles con Amazon Fraud Detector, consulte [Elija un tipo de modelo](#).

#### Crear un modelo

En el siguiente ejemplo, la [CreateModel](#) API se usa para crear un modelo.

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

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

## Entrena a un modelo

En el siguiente ejemplo, se utiliza la [CreateModelVersion](#) API para formar el modelo.

'EXTERNAL\_EVENTS' Especifique la ubicación de Amazon S3 `trainingDataSource` y la ubicación en la que almacenó su conjunto de datos `RoleArnde` ejemplo y el bucket de Amazon S3 `externalEventsDetail`. Para el `trainingDataSchema` parámetro, especifique cómo interpreta Amazon Fraud Detector los datos del ejemplo. Más específicamente, especifique qué variables incluir y cómo clasificar las etiquetas de eventos.

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

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

Puedes entrenar tu modelo varias veces. Cada vez que entrene un modelo, se crea una nueva versión. Una vez finalizado el entrenamiento del modelo, el estado de la versión del modelo se actualiza a `TRAINING_COMPLETE`. Puede revisar la puntuación de rendimiento del modelo y otras métricas de rendimiento del modelo.

## Revise el rendimiento del modelo

Un paso importante a la hora de utilizar Amazon Fraud Detector es evaluar la precisión del modelo mediante las puntuaciones del modelo y las métricas de rendimiento. Una vez finalizado el

entrenamiento del modelo, Amazon Fraud Detector valida el rendimiento del modelo utilizando el 15% de los datos que no se utilizó para entrenar el modelo. Genera una puntuación de rendimiento del modelo y otras métricas de rendimiento.

Utilice la [DescribeModelVersions](#) API para revisar el rendimiento del modelo. Observe la puntuación general del rendimiento del modelo y todas las demás métricas generadas por Amazon Fraud Detector para este modelo.

Para obtener más información sobre la puntuación de rendimiento y las métricas de rendimiento del modelo, consulte [Puntuaciones del modelo](#) y [Métricas de rendimiento del modelo](#).

Puede esperar que todos sus modelos de Amazon Fraud Detector capacitados cuenten con métricas de rendimiento de detección de fraudes reales, similares a las métricas de este tutorial.

## Implementar un modelo

Tras revisar las métricas de rendimiento de su modelo entrenado, implemente el modelo y póngalo a disposición de Amazon Fraud Detector para generar predicciones de fraude. Para implementar el modelo entrenado, utilice la [UpdateModelVersionStatus](#) API. En el siguiente ejemplo, se usa para actualizar el estado de la versión del modelo a 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'
)
```

## Paso 5: Crear el detector, los resultados, las reglas y la versión del detector

Un detector contiene la lógica de detección, como los modelos y las reglas. Esta lógica es para un evento en particular que desee evaluar para determinar si es un fraude. Una regla es una condición que especifica para indicar a Amazon Fraud Detector cómo interpretar los valores de las variables durante la predicción. Y el resultado es el resultado de una predicción de fraude. Un detector puede tener varias versiones y cada versión tiene un estado de BORRADOR, ACTIVO o INACTIVO. Una versión del detector debe tener una regla asociada como mínimo como mínimo.

Utilice los siguientes códigos de ejemplo para crear el detector, las reglas, el resultado y publicar el detector.

### Crear un detector

En el siguiente ejemplo, la [PutDetector](#) API se usa para crear un `sample_detector` detector para el tipo `sample_registration` evento.

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

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

### Crear resultados

Los resultados se crean para cada posible resultado de predicción de fraude. En el siguiente ejemplo, la [PutOutcome](#) API se usa para crear tres resultados: `verify_customerreview`, `yapprove`. Estos resultados se asignan posteriormente a las reglas.

```
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'
)
```

## Crear reglas

La regla se compone de una o más variables del conjunto de datos, una expresión lógica y uno o más resultados.

En el siguiente ejemplo, la [CreateRuleAPI](#) se usa para crear tres reglas diferentes: `high_risk`, `medium_risk`, y `low_risk`. Cree expresiones de reglas para comparar el `sample_fraud_detection_model_insightscore` valor de la puntuación de rendimiento del modelo con varios umbrales. Esto sirve para determinar el nivel de riesgo de un evento y asignar el resultado que se definió en el paso anterior.

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

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

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

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

## Crear una versión del detector

Una versión de detector define el modelo y las reglas que se utilizan para predecir el fraude.

En el siguiente ejemplo, la [CreateDetectorVersion](#) API se usa para crear una versión de detector. Para ello, proporciona detalles de la versión del modelo, reglas y un modo de ejecución de reglas `FIRST_MATCHED`. Un modo de ejecución de reglas especifica la secuencia para evaluar las reglas. El modo de ejecución de reglas `FIRST_MATCHED` especifica que las reglas se evalúen secuencialmente, de la primera a la última, y se detiene en la primera regla que coincida.

```
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'
)
```

## Paso 6: generar predicciones de fraude

El último paso de este tutorial utiliza el `sample_detector` creado en el paso anterior para generar predicciones de fraude para el tipo `sample_registration` evento en tiempo real. El detector evalúa los datos de ejemplo que se cargan en Amazon S3. La respuesta incluye las puntuaciones de rendimiento del modelo, así como cualquier resultado asociado a las reglas coincidentes.

En el siguiente ejemplo, la [GetEventPrediction](#) API se utiliza para proporcionar datos del registro de una sola cuenta con cada solicitud. Para este tutorial, tome datos (`email_address` e `ip_address`) del archivo de datos de ejemplo de registro de la cuenta. Cada línea (fila) después de la línea superior del encabezado representa los datos de un único evento de registro de cuenta.

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

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

Una vez formado este tutorial, aprenderá a hacer lo siguiente:

- Cargué un conjunto de datos de eventos de ejemplo en Amazon S3.
- Se crearon variables, entidades y etiquetas que se utilizan para crear y entrenar un modelo.
- Creé y entrené un modelo utilizando el conjunto de datos de ejemplo.
- Consultó la puntuación de rendimiento del modelo y otras métricas de rendimiento que generó Amazon Fraud Detector.
- Implementé el modelo de detección de fraudes.
- Creó un detector y agregó el modelo implementado.
- Se agregaron reglas, el orden de ejecución de las reglas y los resultados al detector.



- Versión del detector creado.
- Probé el detector proporcionando diferentes entradas y comprobando si las reglas y el orden de ejecución de las reglas funcionaban según lo esperado.

## (Opcional) Explore las API de Amazon Fraud Detector con un cuaderno Jupyter (IPython)

Para obtener más ejemplos sobre cómo utilizar las API de Amazon Fraud Detector, consulte el [aws-fraud-detector-samples GitHub repositorio](#). Los temas que abordan los cuadernos incluyen la creación de modelos y detectores mediante las API de Amazon Fraud Detector y la realización de solicitudes de predicción de fraudes por lotes mediante la `GetEventPrediction` API.

## Pasos siguientes

Ahora que ha creado un modelo y un detector, puede profundizar más y empezar a crear modelos y detectores y a generar predicciones de fraude.

En las siguientes secciones de la Guía del usuario de Amazon Fraud Detector se describe cómo su empresa u organización puede utilizar Amazon Fraud Detector para detectar el fraude.

- Prepare y cree el conjunto de datos de eventos para entrenar el modelo.
- Crear tipo de evento
- Crear un modelo
- Crear detector
- Obtenga predicciones de fraude
- Gestione sus recursos de Amazon Fraud Detector (específicamente, variables, entidades, resultados y etiquetas)
- Configurar Amazon Fraud Detector para satisfacer sus objetivos de seguridad y conformidad
- Supervise Amazon Fraud Detector y registre las llamadas a la API de Amazon Fraud Detector
- Solución de problemas de Amazon Fraud Detector

# Conjunto de datos de eventos

Un conjunto de datos de eventos es el historial de fraude de su empresa. Usted proporciona estos datos a Amazon Fraud Detector para crear modelos de detección de fraudes.

Amazon Fraud Detector utiliza modelos de aprendizaje automático para generar predicciones de fraude. Cada modelo se entrena con un tipo de modelo. El tipo de modelo especifica los algoritmos y las transformaciones que se utilizan para entrenar el modelo. El entrenamiento con modelos es el proceso de utilizar un conjunto de datos que usted proporciona para crear un modelo que pueda predecir eventos fraudulentos. Para obtener más información, consulte [Cómo funciona Amazon Fraud Detector](#).

El conjunto de datos utilizado para crear el modelo de detección de fraudes proporciona detalles de un evento. Un evento es una actividad empresarial que se evalúa para detectar el riesgo de fraude. Por ejemplo, el registro de una cuenta puede ser un evento. Los datos asociados al evento de registro de la cuenta pueden ser un conjunto de datos de eventos. Amazon Fraud Detector utiliza este conjunto de datos para evaluar el fraude en el registro de cuentas.

Antes de proporcionar su conjunto de datos a Amazon Fraud Detector para crear un modelo, asegúrese de definir su objetivo para crear el modelo. También debe determinar cómo desea utilizar el modelo y definir sus métricas para evaluar si el modelo funciona en función de sus requisitos específicos.

Por ejemplo, sus objetivos para crear un modelo de detección de fraudes que evalúe el fraude en el registro de cuentas pueden ser los siguientes:

- Para aprobar automáticamente los registros legítimos.
- Capturar registros fraudulentos para su posterior investigación.

Una vez que haya determinado su objetivo, el siguiente paso es decidir cómo desea utilizar el modelo. Algunos ejemplos de uso del modelo de detección de fraudes para evaluar el fraude de registro son los siguientes:

- Para detectar fraudes en tiempo real para cada registro de cuenta.
- Para evaluar sin conexión todos los registros de cuentas cada hora.

Algunos ejemplos de métricas que se pueden utilizar para medir el rendimiento del modelo son los siguientes:

- Su rendimiento es consistentemente mejor que el valor base actual en producción.
- Captura el X% de registros fraudulentos con una tasa de falsos positivos del Y%.
- Acepta hasta un 5% de los registros fraudulentos con aprobación automática.

## Estructura de conjunto de datos de eventos

Amazon Fraud Detector requiere que proporcione su conjunto de datos de eventos en un archivo de texto con valores separados por comas (CSV) en formato UTF-8. La primera línea del archivo de conjunto de datos CSV debe contener los encabezados de los archivos. El encabezado del archivo se compone de metadatos de eventos y variables de eventos que describen cada elemento de datos asociado al evento. El encabezado va seguido de los datos del evento. Cada línea se compone de elementos de datos de un solo evento.

- **Metadatos del evento:** proporcionan información sobre el evento. Por ejemplo, `EVENT_TIMESTAMP` es un metadato de evento que especifica la hora en que se produjo el evento. Dependiendo de su caso de uso empresarial y del tipo de modelo utilizado para crear y entrenar su modelo de detección de fraudes, Amazon Fraud Detector requiere que proporcione metadatos de eventos específicos. Al especificar los metadatos de eventos en el encabezado del archivo CSV, utilice el mismo nombre de metadatos de eventos que el especificado por Amazon Fraud Detector y utilice únicamente mayúsculas.
- **Variable de evento:** representa los elementos de datos específicos de su evento y que desea utilizar para crear y entrenar su modelo de detección de fraudes. En función de su caso de uso empresarial y del tipo de modelo utilizado para crear y entrenar un modelo de detección de fraudes, Amazon Fraud Detector puede solicitar o recomendar que proporcione variables de eventos específicas. También puede proporcionar opcionalmente otras variables de evento de su evento que desee incluir en el entrenamiento del modelo. Algunos ejemplos de variables de eventos para un evento de registro en línea pueden ser la dirección de correo electrónico, la dirección IP y el número de teléfono. Al especificar el nombre de la variable de evento en el encabezado del archivo CSV, utilice cualquier nombre de variable de su elección y utilice solo letras minúsculas.
- **Datos del evento:** representan los datos recopilados del evento real. En el archivo CSV, cada fila que sigue al encabezado del archivo consta de elementos de datos de un solo evento. Por ejemplo, en un archivo de datos de eventos de registro en línea, cada fila contiene datos de un

solo registro. Cada elemento de datos de la fila debe coincidir con los metadatos de eventos correspondientes o con la variable de evento.

A continuación se muestra un ejemplo de un archivo de un evento de registro de una cuenta. La fila del encabezado contiene los metadatos del evento en mayúsculas y las variables de eventos en minúsculas, seguidas de los datos del evento. Cada fila del conjunto de datos contiene elementos de datos asociados al registro de una sola cuenta y cada elemento de datos se corresponde con el encabezado.

Event metadata			Event variables					
EVENT_TIMESTAMP,	EVENT_ID,	EVENT_LABEL,	email_address,	phone_number,	billing_street,	billing_state,	ip_address	← Header
2020-12-06T03:13:34Z,	R12345,	fraud,	regular1@example.com,	110-345-0990,	mayhem ave,	OH,	112.136.132.151	← Event data
2020-11-13T12:47:00Z,	P56890,	legit,	premium1@example.com,	112-890-4532,	howie lane,	KY,	192.169.234.143	
2021-02-19T22:52:43Z,	R10001,	legit,	regular2@example.net,	078-777-5555,	lankhurst dr,	HI,	185.112.224.79	
2020-11-29T00:16:09Z,	R56099,	fraud,	regular3@example.edu,	777-213-0033,	noland ave,	IL,	68.73.183.186	
2021-01-16T07:30:03Z,	P08954,	legit,	premium2@example.net,	444-040-8344,	oakwood apt,	MA,	117.65.246.206	

## Obtenga los requisitos del conjunto de datos de eventos mediante el explorador de modelos de datos

El tipo de modelo que elija para crear el modelo define los requisitos del conjunto de datos. Amazon Fraud Detector utiliza el conjunto de datos que usted proporciona para crear y entrenar su modelo de detección de fraudes. Antes de que Amazon Fraud Detector comience a crear el modelo, comprueba si el conjunto de datos cumple los requisitos de tamaño, formato y otros requisitos. Si el conjunto de datos no cumple con los requisitos, se produce un error en la creación del modelo y en el entrenamiento. Puede utilizar el explorador de modelos de datos para identificar un tipo de modelo que pueda utilizar en su caso práctico empresarial y obtener información sobre los requisitos del conjunto de datos para el tipo de modelo identificado.

### Explorador de modelos de datos.

El explorador de modelos de datos es una herramienta de la consola de Amazon Fraud Detector que alinea su caso de uso empresarial con el tipo de modelo admitido por Amazon Fraud Detector. El explorador de modelos de datos también proporciona información sobre los elementos de datos que Amazon Fraud Detector necesita para crear su modelo de detección de fraudes. Antes de empezar a preparar el conjunto de datos de eventos, utilice el explorador de modelos de datos para averiguar el tipo de modelo que Amazon Fraud Detector recomienda para su uso empresarial y también para ver una lista de los elementos de datos obligatorios, recomendados y opcionales que necesitará para crear su conjunto de datos.

Para usar el explorador de modelos de datos,

1. Abra la [consolaAWS de administración](#) e inicia sesión en tu cuenta. Navegue hasta Amazon Fraud Detector.
2. En el panel de navegación de la izquierda, elija Explorador de modelos de datos.
3. En la página del explorador de modelos de datos, en Caso de uso empresarial, seleccione el caso de uso empresarial que desee evaluar para determinar el riesgo de fraude.
4. Amazon Fraud Detector muestra el tipo de modelo recomendado que coincide con su caso de uso empresarial. El tipo de modelo define los algoritmos, los enriquecimientos y las transformaciones que Amazon Fraud Detector utilizará para entrenar su modelo de detección de fraudes.

Anote el tipo de modelo recomendado. Lo necesitará más adelante cuando cree su modelo.

#### Note

Si no encuentra su caso de uso empresarial, utilice el enlace [Comuníquese con nosotros](#) que aparece en la descripción para proporcionarnos los detalles de su caso de uso empresarial. Le recomendaremos el tipo de modelo que debe utilizar para crear un modelo de detección de fraudes para su caso de uso empresarial.

5. El panel de información del modelo de datos proporciona información sobre los elementos de datos obligatorios, recomendados y opcionales necesarios para crear y entrenar un modelo de detección de fraudes para su caso de uso empresarial. Utilice la información del panel de información para recopilar los datos de sus eventos y crear su conjunto de datos.

## Recopila datos de eventos

La recopilación de los datos de su evento es un paso importante para crear su modelo. Esto se debe a que el rendimiento de su modelo para predecir el fraude depende de la calidad del conjunto de datos. Cuando comience a recopilar los datos de sus eventos, tenga en cuenta la lista de elementos de datos que el explorador de modelos de datos le proporcionó para crear su conjunto de datos. Deberá recopilar todos los datos obligatorios (metadatos de eventos) y decidir qué elementos de datos recomendados y opcionales (variables de eventos) incluir en función de sus objetivos para crear el modelo. También es importante decidir el formato de cada variable de evento que pretendes incluir y el tamaño total del conjunto de datos.

## Calidad del conjunto de datos de eventos

Para recopilar un conjunto de datos de alta calidad para su modelo, recomendamos lo siguiente:

- **Recopile datos maduros:** el uso de los datos más recientes ayuda a identificar el patrón de fraude más reciente. Sin embargo, para detectar casos de uso fraudulento, deje que los datos maduren. El período de vencimiento depende de su empresa y puede tardar entre dos semanas y tres meses. Por ejemplo, si tu evento incluye una transacción con tarjeta de crédito, el vencimiento de los datos podría determinarse según el período de devolución de la tarjeta de crédito o el tiempo que un investigador haya tardado en tomar una decisión.

Asegúrese de que el conjunto de datos utilizado para entrenar el modelo haya tenido tiempo suficiente para madurar según su empresa.

- **Asegúrese de que la distribución de datos no se desvíe significativamente:** el proceso de entrenamiento del modelo Amazon Fraud Detector muestrea y particiona su conjunto de datos basándose en `EVENT_TIMESTAMP`. Por ejemplo, si su conjunto de datos se compone de eventos de fraude extraídos de los últimos 6 meses, pero solo se incluye el último mes de eventos legítimos, la distribución de datos se considera inestable y a la deriva. Un conjunto de datos inestable puede provocar sesgos en la evaluación del rendimiento del modelo. Si encuentra que la distribución de datos se desvía significativamente, considere equilibrar su conjunto de datos recopilando datos similares a la distribución de datos actual.
- **Asegúrese de que el conjunto de datos sea representativo del caso de uso en el que se implementa/prueba el modelo;** de lo contrario, el rendimiento estimado podría estar sesgado. Supongamos que utilizas un modelo para rechazar automáticamente a todos los candidatos internos, pero tu modelo se entrena con un conjunto de datos que contiene datos y etiquetas históricos que se aprobaron previamente. En ese caso, la evaluación del modelo podría ser inexacta porque se basa en un conjunto de datos que no incluye a los solicitantes rechazados.

## Formato de datos de eventos

Amazon Fraud Detector transforma la mayoría de sus datos al formato requerido como parte de su proceso de formación de modelos. Sin embargo, existen algunos formatos estándar que puede utilizar fácilmente para proporcionar sus datos y que pueden ayudar a evitar problemas más adelante, cuando Amazon Fraud Detector valide su conjunto de datos. La siguiente tabla proporciona orientación sobre los formatos para proporcionar los metadatos de eventos recomendados.

 Note

Al crear el archivo CSV, asegúrese de introducir el nombre de los metadatos del evento tal y como se indica a continuación, en mayúsculas.

Nombre de metadatos	Formato	Obligatorio
ID_DE_EVENTO	<p>Si se proporciona, debe cumplir los siguientes requisitos:</p> <ul style="list-style-type: none"> <li>• Es único para ese evento.</li> <li>• Representa información significativa para su empresa.</li> <li>• Sigue el patrón de expresiones regulares (por ejemplo, <code>^[0-9a-z_-]+\$.)</code></li> <li>• Además de los requisitos anteriores, te recomendamos que no añadas ninguna marca de tiempo al <code>EVENT_ID</code>. Hacerlo podría causar problemas al actualizar el evento. Esto se debe a que debes proporcionar exactamente el mismo <code>EVENT_ID</code> si lo haces.</li> </ul>	Depende del tipo de modelo
EVENT_TIMESTAMP	<ul style="list-style-type: none"> <li>• Debe especificarse en uno de los siguientes formatos: <ul style="list-style-type: none"> <li>• <code>%YYYY-%MM-%DDT</code></li> <li>• <code>%HH: %mm: %sSz</code></li> </ul> </li> </ul>	Sí

Nombre de metadatos	Formato	Obligatorio
	<p>(estándar ISO 8601 solo en UTC sin milisegundos)</p> <p>Ejemplo: 2019-11-30T13:01:01 Z</p> <ul style="list-style-type: none"> <li>• %aaaa/%mm/%dd %hh: %mm: %s (mañana y tarde)</li> </ul> <p>Ejemplos: 30 de noviembre de 2019 a las 13:01:01 p. m., o 30 de noviembre de 2019 a las 13:00:01</p> <ul style="list-style-type: none"> <li>• %mm/%dd/%aaaa %hh: %mm: %ss</li> </ul> <p>Ejemplos: 30/11/2019 1:01:01 p.m., 30/11/2019 13:01:01</p> <ul style="list-style-type: none"> <li>• %mm/%dd/%yy %h: %mm: %s</li> </ul> <p>Ejemplos: 30/11/19 1:01:01 p.m., 11/30/19 13:01:01</p> <ul style="list-style-type: none"> <li>• Amazon Fraud Detector hace las siguientes suposiciones al analizar los formatos de fecha y hora para las marcas de tiempo de los eventos: <ul style="list-style-type: none"> <li>• Si utiliza la norma ISO 8601, debe coincidir</li> </ul> </li> </ul>	



Nombre de metadatos	Formato	Obligatorio
	<p>exactamente con la especificación anterior.</p> <ul style="list-style-type: none"><li>• Si utiliza uno de los otros formatos, hay flexibilidad adicional:<ul style="list-style-type: none"><li>• Para meses y días, puedes proporcionar uno o dos dígitos. Por ejemplo, el 12 de enero de 2019 es una fecha válida.</li><li>• No necesita incluir hh:mm:ss si no los tiene (es decir, simplemente puede proporcionar una fecha). También puede proporcionar un subconjunto de solo la hora y los minutos (por ejemplo, hh:mm). No se admite solo proporcionar la hora. Tampoco se admiten milisegundos.</li><li>• Si proporciona etiquetas de mañana a tarde, se asume que es un reloj de 12 horas. Si no hay información AM/PM, se asume que el reloj es de 24 horas.</li><li>• Puede utilizar «/» o «-» como delimitadores</li></ul></li></ul>	

Nombre de metadatos	Formato	Obligatorio
	para los elementos de fecha. Se asume «:» para los elementos de marca de tiempo.	
IDENTIFICADOR DE ENTIDAD	<ul style="list-style-type: none"> <li>Debe seguir el patrón de expresiones regulares :<code>^[0-9A-Za-z_@+-]+\$</code>.</li> <li>Si el identificador de la entidad no está disponible en el momento de la evaluación, especifique el identificador de la entidad como desconocido.</li> </ul>	Depende del tipo de modelo
TIPO_DE_ENTIDAD	Puede utilizar cualquier cadena.	Depende del tipo de modelo
ETIQUETA_DE_EVENTO	Puede utilizar cualquier etiqueta, como «fraude», «legítimo», «1» o «0».	Necesario si se incluye LABEL_TIMESTAMP
LABEL_TIMESTAMP	Debe seguir el formato de marca de tiempo.	Obligatorio si se incluye EVENT_LABEL

Para obtener información sobre las variables de eventos, consulte [Variables](#).

#### Important

Si está creando el modelo Account Takeover Insights (ATI), consulte [Preparación de datos](#) para obtener más información sobre la preparación y la selección de datos.

## Valores nulos o faltantes

Las variables `EVENT_TIMESTAMP` y `EVENT_LABEL` no deben contener ningún valor nulo o faltante. Puede tener valores nulos o faltantes para otras variables. Sin embargo, recomendamos que solo utilice un número pequeño de nulos para esas variables. Si Amazon Fraud Detector determina que hay demasiados valores nulos o faltantes para las variables de un evento, omitirá automáticamente la variable del modelo.

### Variables mínimas

Al crear el modelo, el conjunto de datos debe incluir al menos dos variables de eventos además de los metadatos de eventos requeridos. Las dos variables de evento deben pasar la comprobación de validación.

### Tamaño del conjunto de datos de eventos

#### Obligatorio

El conjunto de datos debe cumplir los siguientes requisitos básicos para que el entrenamiento del modelo sea exitoso.

- Datos de al menos 100 eventos.
- El conjunto de datos debe incluir al menos 50 eventos (filas) clasificados como fraudulentos.

#### Recomendado

Recomendamos que el conjunto de datos incluya lo siguiente para que el entrenamiento del modelo se realice correctamente y el rendimiento del modelo sea satisfactorio.

- Incluya un mínimo de tres semanas de datos históricos, pero, en el mejor de los casos, seis meses de datos.
- Incluye un mínimo de 10 000 datos de eventos en total.
- Incluye al menos 400 eventos (filas) clasificados como fraudulentos y 400 eventos (filas) clasificados como legítimos.
- Incluye más de 100 entidades únicas, si tu tipo de modelo requiere `ENTITY_ID`.

## Validación de conjunto de datos.

Antes de que Amazon Fraud Detector comience a crear el modelo, comprueba si las variables incluidas en el conjunto de datos para entrenar el modelo cumplen con los requisitos de tamaño,

formato y otros requisitos. Si el conjunto de datos no pasa la validación, no se crea el modelo. Primero debe corregir las variables que no pasaron la validación antes de crear el modelo. Amazon Fraud Detector le proporciona un generador de perfiles de datos que puede utilizar para ayudarlo a identificar y solucionar problemas con su conjunto de datos antes de empezar a entrenar su modelo.

## Generador de perfiles de datos

Amazon Fraud Detector proporciona una herramienta de código abierto para crear perfiles y preparar sus datos para la formación de modelos. Este generador de perfiles de datos automatizado le ayuda a evitar errores comunes de preparación de datos e identificar posibles problemas, como tipos de variables mal mapeados, que podrían afectar negativamente al rendimiento del modelo. El generador de perfiles genera un informe intuitivo y completo de su conjunto de datos, que incluye estadísticas variables, distribución de etiquetas, análisis categóricos y numéricos y correlaciones de variables y etiquetas. Proporciona orientación sobre los tipos de variables, así como una opción para transformar el conjunto de datos en el formato que requiera Amazon Fraud Detector.

## Uso del generador de perfiles de datos

El generador de perfiles de datos automatizado se basa en una AWS CloudFormation pila que puede iniciar fácilmente con unos pocos clics. Todos los códigos están disponibles en [Github](#). Para obtener información sobre cómo utilizar el generador de perfiles de datos, siga las instrucciones de nuestro blog [Entrene modelos más rápido con un generador de perfiles de datos automatizado para Amazon Fraud Detector](#)

## Errores comunes del conjunto de datos de eventos

Los siguientes son algunos de los problemas más comunes con los que se enfrenta Amazon Fraud Detector al validar un conjunto de datos de eventos. Después de ejecutar el generador de perfiles de datos, utilice esta lista para comprobar si hay errores en el conjunto de datos antes de crear el modelo.

- El archivo de CSV no está en formato UTF-8.
- El número de eventos del conjunto de datos es inferior a 100.
- El número de eventos identificados como fraudulentos o legítimos es inferior a 50.
- El número de entidades únicas asociadas a un evento de fraude es inferior a 100.
- Más del 0,1% de los valores de `EVENT_TIMESTAMP` contienen valores nulos o valores distintos de los formatos de fecha y hora admitidos.
- Más del 1% de los valores de `EVENT_LABEL` contienen valores nulos o distintos de los definidos en el tipo de evento.

- Hay menos de dos variables disponibles para el entrenamiento del modelo.

## Almacenamiento de conjuntos de datos.

Después de recopilar el conjunto de datos, los almacena de forma interna Fraud Detector Simple Storage Service (Amazon S3). Le recomendamos que elija dónde almacenar su conjunto de datos en función del modelo que utilice para generar predicciones de fraude. Para obtener más información sobre los tipos de modelos, consulte [Elegir un tipo de modelo](#). Para obtener más información sobre cómo almacenar el conjunto de datos, consulte [Almacenamiento de datos de eventos](#).

# Tipo de evento

Con Amazon Fraud Detector, puede generar predicciones de fraude para eventos. Un tipo de evento define la estructura de un evento individual enviado a Amazon Fraud Detector. Una vez definidos, puede crear modelos y detectores que evalúen el riesgo para tipos de eventos específicos.

La estructura de un evento incluye lo siguiente:

- **Tipo de entidad:** clasifica quién está realizando el evento. Durante la predicción, especifique el tipo de entidad y el identificador de la entidad para definir quién realizó el evento.
- **Variables:** define qué variables se pueden enviar como parte del evento. Los modelos y las reglas utilizan variables para evaluar el riesgo de fraude. Una vez agregadas, las variables no se pueden eliminar de un tipo de evento.
- **Etiquetas:** clasifica un evento como fraudulento o legítimo. Se utiliza durante el entrenamiento de modelos. Una vez añadidas, las etiquetas no se pueden quitar de un tipo de evento.

## Crear un tipo de evento

Antes de crear su modelo de detección de fraudes, primero debe crear un tipo de evento. La creación de un tipo de evento implica definir la actividad empresarial (evento) para evaluar el fraude. Definir el evento implica identificar las variables del evento en el conjunto de datos que se van a incluir para la evaluación del fraude, especificar la entidad que inicia el evento y las etiquetas que clasifican el evento.

### Requisitos previos para crear un tipo de evento

Antes de empezar a crear el tipo de evento, asegúrate de haber completado lo siguiente:

- Utilizó la [Explorador de modelos de datos](#) herramienta para obtener información sobre los elementos de datos que Amazon Fraud Detector necesita para crear su modelo de detección de fraudes.
- Utilizó la información que obtuvo del Explorador de modelos de datos para crear su conjunto de datos de eventos y lo cargó al bucket de Amazon S3.
- Se creó [Variables](#) y [Etiquetas](#) desea que Amazon Fraud Detector lo utilice para crear un modelo de detección de fraudes para este evento. [Entidad](#) Asegúrese de que las variables, el tipo de entidad y las etiquetas que creó estén incluidos en el conjunto de datos de eventos.

Puede crear su tipo de evento en la consola de Amazon Fraud Detector, mediante la APIAWS CLI, el SDK o el AWS SDK.


## Cree un tipo de evento en la consola de Amazon Fraud Detector

Para crear un tipo de evento,

1. Abra la [consola AWS de administración](#) e inicia sesión en tu cuenta. Diríjase a Amazon Fraud Detector.
2. En el panel de navegación izquierdo, elija Events.
3. En la página Tipo de eventos, selecciona Crear.
4. En Detalles del tipo de evento,
  - a. En Nombre, introduce el nombre de tu evento.
  - b. En la Descripción, si lo desea, introduzca una descripción.
  - c. En la Entidad, selecciona el tipo de entidad que creaste para tu evento.
5. En Variables de eventos,
  - En la sección Elija cómo definir las variables de este evento,
    - Si ya ha creado las variables de evento para este evento, seleccione Seleccionar variables de la lista de variables y, en Variables, seleccione las variables que creó para este evento.
    - Si no ha creado variables para este evento, seleccione Seleccionar variables de un conjunto de datos de entrenamiento,
      - En el rol de IAM, seleccione el rol de IAM que desea que Amazon Fraud Detector utilice para acceder al bucket de Amazon S3 que contiene su conjunto de datos.
      - En la ubicación de datos, introduzca la ruta a la ubicación de su conjunto de datos. Utilice la S3 URI ruta similar a esta: `S3://your-bucket-name/example dataset filename.csv`.
      - Seleccione Upload (Cargar).
      - En Variables, se muestran todos los nombres de las variables de eventos que Amazon Fraud Detector ha extraído del archivo del conjunto de datos.

Si desea incluir la variable para detectar el fraude, en el tipo Variable, seleccione el tipo de variable. Elija Eliminar para eliminar las variables que se incluirán para la detección de fraudes. Repita este paso para cada variable de la lista.

6. En Etiquetas (opcional), en Etiquetas, selecciona las etiquetas que creaste para este evento. Asegúrese de seleccionar una etiqueta para cada evento legítimo y fraudulento.
7. Si quieres configurar el procesamiento posterior automático para este evento, en Organización de eventos con Amazon EventBridge (opcional), activa Habilitar la orquestación de eventos con Amazon. EventBridge Para obtener más información sobre la organización de eventos, consulte [Orquestación de eventos](#).


 Note

También puedes habilitar la orquestación de eventos más adelante, después de crear tu tipo de evento.

8. Elige Crear tipo de evento.

## Cree un tipo de evento mediante el AWS SDK for Python (Boto3)

El siguiente ejemplo muestra un ejemplo de solicitud para la PutEventType API. El ejemplo supone que ha creado las variables `ip_address` y `email_address`, las etiquetas `legit` y `fraud`, y el tipo de entidad `sample_customer`. Para obtener información sobre cómo crear estos recursos, consulte [Recursos](#).

 Note

Primero debe crear variables, tipos de entidades y etiquetas antes de agregarlos al tipo de evento.

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

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



```
entityTypes = ['sample_customer'])
```

## Eliminar un evento o un tipo de evento

Al eliminar un evento, Amazon Fraud Detector elimina ese evento de forma permanente y los datos asociados al evento ya no se almacenan en Amazon Fraud Detector.

Para eliminar un evento que Amazon Fraud Detector ha evaluado mediante la **GetEventPrediction** API

1. Inicie sesión en la consola de Amazon Fraud Detector AWS Management Console y ábrala en <https://console.aws.amazon.com/frauddetector>.
2. En el panel de navegación izquierdo de la consola, selecciona Buscar predicciones pasadas.
3. Elige el evento que quieres eliminar.
4. Elija Acciones y, a continuación, elija Eliminar evento.
5. Introduzca **delete**, a continuación, seleccione Eliminar evento.

### Note

Esto elimina todos los registros que están asociados a ese ID de evento, incluidos los datos de eventos enviados a la `SendEvent` operación y los datos de predicción generados a través de la `GetEventPrediction` operación.

Para eliminar un evento que está almacenado en Amazon Fraud Detector pero que no se ha evaluado (es decir, se almacenó mediante la `SendEvent` operación), debe realizar una `DeleteEvent` solicitud y especificar el ID del evento y el ID del tipo de evento. Si desea eliminar tanto el evento como cualquier historial de predicciones asociado al evento, defina el valor del `deleteAuditHistory` parámetro en «true». Con el `deleteAuditHistory` parámetro establecido en «true», los datos del evento estarán disponibles mediante la búsqueda durante un máximo de 30 segundos después de que se complete la operación de eliminación.

Para eliminar todos los eventos asociados a un tipo de evento

1. En el panel de navegación izquierdo de la consola, seleccione Tipos de eventos
2. Elija el tipo de evento para el que desea eliminar todos los eventos.

### 3. Ve a la pestaña Eventos almacenados y selecciona Eliminar eventos almacenados

En función del número de eventos almacenados para el tipo de evento, es posible que se tarde algún tiempo en eliminar todos los eventos almacenados. Por ejemplo, un conjunto de datos de 1 GB (aproximadamente de 1 a 2 millones de eventos para un cliente promedio) tarda unas 2 horas en eliminarse. Durante este tiempo, los nuevos eventos que envíe a Amazon Fraud Detector de este tipo no se almacenarán, pero podrá seguir generando predicciones de fraude mediante la `GetEventPrediction` operación.

#### Para eliminar un tipo de evento

No puede eliminar un tipo de evento que se utilice en un detector o un modelo, ni que tenga eventos almacenados asociados. Antes de eliminar un tipo de evento, debe eliminar todos los eventos asociados a ese tipo de evento.

Al eliminar un tipo de evento, Amazon Fraud Detector elimina permanentemente ese tipo de evento y los datos ya no se almacenan en Amazon Fraud Detector.

1. En el panel de navegación izquierdo de la consola de Amazon Fraud Detector, seleccione Recursos y, a continuación, seleccione Eventos.
2. Elige el tipo de evento que quieres eliminar.
3. Elija Acciones y, a continuación, elija Eliminar tipo de evento.
4. Introduzca el nombre del tipo de evento y, a continuación, seleccione Eliminar tipo de evento.

## Almacenamiento de datos de eventos

Una vez que haya recopilado su conjunto de datos, puede almacenar su conjunto de datos de forma interna utilizando Amazon Fraud Detector o Amazon Simple Storage Service (Amazon S3). Le recomendamos que elija dónde almacenar su conjunto de datos en función del modelo que utilice para generar predicciones de fraude. A continuación se muestra un desglose detallado de estas dos opciones de almacenamiento.

- **Almacenamiento interno:** su conjunto de datos se almacena en Amazon Fraud Detector. Todos los datos de eventos asociados a un evento se almacenan juntos. Puede cargar el conjunto de datos de eventos que está almacenado en Amazon Fraud Detector en cualquier momento. Puede transmitir eventos de uno en uno a una API de Amazon Fraud Detector o importar grandes conjuntos de datos (hasta 1 GB) mediante la función de importación por lotes. Al entrenar un modelo con el conjunto de datos almacenado en Amazon Fraud Detector, puede especificar un intervalo de tiempo para limitar el tamaño del conjunto de datos.
- **Almacenamiento externo:** el conjunto de datos se almacena en una fuente de datos externa que no es Amazon Fraud Detector. Amazon Fraud Detector admite el uso de Amazon Simple Storage Detector (Amazon S3 Simple Storage Detector) para este fin. Si su modelo está en un archivo subido a Amazon S3, ese archivo no puede contener más de 5 GB de datos sin comprimir. Si es más que eso, asegúrate de acortar el intervalo de tiempo de tu conjunto de datos.

La siguiente tabla proporciona detalles sobre el tipo de modelo y la fuente de datos que admite.

Tipo de modelo	Fuente de datos de entrenamiento compatible
Información de Fraud Detector	Almacenamiento externo, almacenamiento interno
Información sobre el Fraud Detector	Almacenamiento interno
Información sobre la adquisición de cuentas	Almacenamiento interno

Para obtener información sobre cómo almacenar el conjunto de datos de forma externa con Amazon Simple Storage Service, consulte [Almacene los datos de sus eventos de forma externa con Amazon S3](#). Para obtener información sobre cómo almacenar su conjunto de datos internamente con

Amazon Fraud Detector, consulte [Almacene los datos de sus eventos internamente con Amazon Fraud Detector](#).

## Almacene los datos de sus eventos de forma externa con Amazon S3

Si está entrenando un modelo de Online Fraud Insights, puede optar por almacenar los datos de sus eventos de forma externa con Amazon S3. Para almacenar los datos de sus eventos en Amazon S3, primero debe crear un archivo de texto en formato CSV, añadir los datos del evento y, a continuación, subir el archivo CSV a un bucket de Amazon S3.

### Note

Los tipos de modelos Transaction Fraud Insights y Account Takeover Insights no admiten conjuntos de datos almacenados externamente en Amazon S3.

## Crear archivo CSV CSV

Amazon Fraud Detector requiere que la primera fila del archivo CSV contenga encabezados de columna. Los encabezados de las columnas del archivo CSV deben corresponder a las variables definidas en el tipo de evento. Para ver un conjunto de datos de ejemplo, consulte [Obtener y cargar un conjunto de datos de ejemplo](#)

El modelo Online Fraud Insights requiere un conjunto de datos de entrenamiento que tenga al menos 2 variables y hasta 100 variables. Además de las variables de eventos, el conjunto de datos de entrenamiento debe contener los siguientes encabezados:

- **EVENT\_TIMESTAMP**: define cuándo se produjo el evento
- **EVENT\_LABEL**: clasifica el evento como fraudulento o legítimo. Los valores de la columna deben corresponder a los valores definidos en el tipo de evento.

El siguiente ejemplo de datos en CSV representa el historial de eventos de registro de un comerciante en línea:

```
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

El archivo de datos CSV puede contener comillas dobles y comas como parte de los datos.

A continuación se muestra una versión simplificada del tipo de evento correspondiente. Las variables de evento corresponden a los encabezados del archivo CSV y los valores contenidos en `EVENT_LABEL` corresponden a los valores de la lista de etiquetas.

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

## Formatos de marca de tiempo de eventos

Asegúrese de que la marca de tiempo del evento esté en el formato requerido. Como parte del proceso de creación del modelo, el modelo Online Fraud Insights ordena los datos en función de la marca de tiempo del evento y los divide con fines de capacitación y prueba. Para obtener una estimación justa del rendimiento, el modelo primero se entrena en el conjunto de datos de entrenamiento y, a continuación, lo prueba en el conjunto de datos de prueba.

Amazon Fraud Detector admite los siguientes formatos de fecha y hora para los valores que se utilizan `EVENT_TIMESTAMP` durante el entrenamiento del modelo:

- `%YYYY-%MM-%DDT%HH: %mm: %sSz` (estándar ISO 8601 solo en UTC sin milisegundos)

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

- `%aaaa/%mm/%dd %hh: %mm: %s` (mañana y tarde)

Ejemplos: 30 de noviembre de 2019 a las 13:01:01 p. m., o 30 de noviembre de 2019 a las 13:00:01

- `%mm/%dd/%aaaa %hh: %mm: %ss`

Ejemplos: 30/11/2019 1:01:01 p.m., 30/11/2019 13:01:01

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

Ejemplos: 30/11/19 1:01:01 p.m., 11/30/19 13:01:01

Amazon Fraud Detector hace las siguientes suposiciones al analizar los formatos de fecha y hora para las marcas de tiempo de los eventos:

- Si utiliza la norma ISO 8601, debe coincidir exactamente con la especificación anterior
- Si utiliza uno de los otros formatos, hay flexibilidad adicional:
  - Para meses y días, puedes proporcionar uno o dos dígitos. Por ejemplo, el 12 de enero de 2019 es una fecha válida.
  - No necesita incluir hh:mm:ss si no los tiene (es decir, simplemente puede proporcionar una fecha). También puede proporcionar un subconjunto de solo la hora y los minutos (por ejemplo, hh:mm). No se admite solo proporcionar la hora. Tampoco se admiten milisegundos.
  - Si proporciona etiquetas de mañana a tarde, se asume que es un reloj de 12 horas. Si no hay información AM/PM, se asume que el reloj es de 24 horas.
  - Puede utilizar «/» o «-» como delimitadores para los elementos de fecha. Se asume «:» para los elementos de marca de tiempo.

## Muestreo de su conjunto de datos a lo largo del tiempo

Le recomendamos que proporcione ejemplos de fraude y muestras legítimas del mismo intervalo de tiempo. Por ejemplo, si proporciona eventos de fraude de los últimos 6 meses, también debe proporcionar eventos legítimos que abarquen el mismo período de tiempo de manera uniforme. Si tu conjunto de datos contiene una distribución muy desigual del fraude y los eventos legítimos, es posible que recibas el siguiente error: «La distribución del fraude a lo largo del tiempo fluctúa de manera inaceptable. No se puede dividir el conjunto de datos correctamente». Por lo general, la solución más sencilla para este error es garantizar que los eventos de fraude y los eventos legítimos se muestreen de manera uniforme en el mismo período de tiempo. También es posible que tengas que eliminar datos si has experimentado un gran aumento del fraude en poco tiempo.

Si no puedes generar suficientes datos para crear un conjunto de datos distribuido de manera uniforme, un método consiste en aleatorizar el EVENT\_TIMESTAMP de tus eventos de manera que se distribuyan de manera uniforme. Sin embargo, esto suele provocar que las métricas de

rendimiento no sean realistas, ya que Amazon Fraud Detector utiliza `EVENT_TIMESTAMP` para evaluar los modelos del subconjunto de eventos correspondiente del conjunto de datos.

## Valores nulos y faltantes

Amazon Fraud Detector gestiona los valores nulos y faltantes. Sin embargo, el porcentaje de valores nulos para las variables debe ser limitado. Las columnas `EVENT_TIMESTAMP` y `EVENT_LABEL` no deben contener ningún valor faltante.

## Validación de archivos

Amazon Fraud Detector no podrá entrenar un modelo si se activa alguna de las siguientes condiciones:

- Si no se puede analizar el CSV
- Si el tipo de datos de una columna es incorrecto

## Cargue los datos de su evento en un bucket de Amazon S3

Después de crear un archivo CSV con los datos del evento, carga el archivo en su bucket de Amazon S3.

Para cargar en un bucket de Amazon S3

1. Inicie sesión en la AWS Management Console y abra la consola de Amazon S3 en <https://console.aws.amazon.com/s3/>.
2. Elija **Create bucket** (Crear bucket).


Se abrirá el asistente **Crear bucket** (Crear bucket).

3. En **Bucket name** (Nombre del bucket), escriba un nombre compatible con DNS para el bucket.

El nombre del bucket debe:

- Ser único en todo Amazon S3.
- Tener entre 3 y 63 caracteres.
- No contiene caracteres en mayúsculas.
- Comenzar por una letra minúscula o un número.

Una vez que haya creado el bucket, no podrá modificar su nombre. Para obtener información sobre la nomenclatura de buckets, consulte [Reglas de nomenclatura](#) de buckets en la Guía del usuario de Amazon Simple Storage Service.

 Important

Evite incluir información confidencial, como números de cuenta, en el nombre del bucket. El nombre del bucket será visible en las URL que señalan a los objetos almacenados en él.

4. En Region (Región), elija la región de AWS en la que desea que se encuentre el bucket. Debe seleccionar la misma región en la que está utilizando Amazon Fraud Detector (Oregón).
5. En Configuración del bucket para Block Public Access, elija la configuración de Block Public Access que desee aplicar al bucket.

Le recomendamos que deje habilitada toda la configuración. Para obtener más información sobre el bloqueo de acceso [público, consulte Bloquear el acceso público a su almacenamiento](#) de Amazon Simple Storage Service.

6. Elija Crear bucket.
7. Cargue el archivo de datos de entrenamiento en su bucket de Amazon S3. Anote la ruta de ubicación de Amazon S3 para su archivo de entrenamiento (por ejemplo, s3://bucketname/object.csv).

## Almacene los datos de sus eventos internamente con Amazon Fraud Detector

Puede optar por almacenar los datos de los eventos en Amazon Fraud Detector y utilizarlos posteriormente para entrenar sus modelos. Al almacenar los datos de eventos en Amazon Fraud Detector, puede entrenar modelos que utilicen variables calculadas automáticamente para mejorar el rendimiento, simplificar el reentrenamiento de los modelos y actualizar las etiquetas de fraude para cerrar el ciclo de retroalimentación del aprendizaje automático. Los eventos se almacenan en el nivel de recursos del tipo de evento, por lo que todos los eventos del mismo tipo de evento se almacenan juntos en un único conjunto de datos de tipo de evento. Como parte de la definición de un



tipo de evento, puede especificar si desea almacenar eventos para ese tipo de evento activando la configuración de ingesta de eventos en la consola de Amazon Fraud Detector.

Puede almacenar eventos individuales o importar una gran cantidad de conjuntos de datos de eventos en Amazon Fraud Detector. Los eventos individuales se pueden transmitir mediante la [GetEventPrediction](#) API o la [SendEvent](#) API. Los conjuntos de datos grandes se pueden importar rápida y fácilmente a Amazon Fraud Detector mediante la función de importación por lotes de la consola de Amazon Fraud Detector o mediante la [CreateBatchImportJob](#) API.

Puede utilizar la consola de Amazon Fraud Detector en cualquier momento para comprobar el número de eventos ya almacenados para cada tipo de evento.

## Preparar los datos de eventos para su almacenamiento

Los datos de eventos que se almacenan internamente con Amazon Fraud Detector se almacenan a nivel de `Event Type` recursos. Por lo tanto, todos los datos de eventos que provienen del mismo evento se almacenan en uno solo `Event Type`. Los eventos almacenados se pueden usar posteriormente para entrenar un modelo nuevo o volver a entrenar un modelo existente. Al entrenar un modelo con los datos de eventos almacenados, puede especificar opcionalmente un intervalo de tiempo de eventos para limitar el tamaño del conjunto de datos de entrenamiento.

Cada vez que almacena sus datos en Amazon Fraud Detector, mediante la consola de Amazon Fraud Detector, la `SendEvent` API o la `CreateBatchImportJob` API, Amazon Fraud Detector valida los datos antes de almacenarlos. Si los datos no se validan, los datos del evento no se almacenan.

Requisitos previos para almacenar datos internamente con Amazon Fraud Detector

- Para garantizar que los datos del evento pasen la validación y que el conjunto de datos se almacene correctamente, asegúrese de haber utilizado la información proporcionada por el [explorador de modelos de datos](#) para preparar su conjunto de datos.
- Creó un tipo de evento para los datos de eventos que desea almacenar en Amazon Fraud Detector. Si no lo has hecho, sigue las instrucciones para [crear un tipo de evento](#).

## Validación de datos inteligente

Al cargar el conjunto de datos en la consola de Amazon Fraud Detector para importarlo por lotes, Amazon Fraud Detector utiliza la validación inteligente de datos (SDV) para validar el conjunto de datos antes de importarlos. El SDV escanea el archivo de datos cargado e identifica problemas

como la falta de datos y el formato o los tipos de datos incorrectos. Además de validar el conjunto de datos, el SDV también proporciona un informe de validación que enumera todos los problemas que se identificaron y sugiere acciones para solucionar los problemas más impactantes. Algunos de los problemas identificados por el SDV pueden ser críticos y deben solucionarse antes de que Amazon Fraud Detector pueda importar correctamente su conjunto de datos. Para obtener más información, consulte [Informe de validación de datos inteligentes](#).

El SDV valida el conjunto de datos a nivel de archivo y a nivel de datos (fila). A nivel de archivo, el SDV escanea el archivo de datos e identifica problemas como los permisos inadecuados para acceder al archivo, el tamaño del archivo, el formato de archivo y los encabezados (metadatos de eventos y variables de eventos) incorrectos. A nivel de datos, el SDV analiza los datos de cada evento (fila) e identifica problemas como el formato de datos, la longitud de los datos, el formato de marca de tiempo y los valores nulos incorrectos.

Actualmente, la validación inteligente de datos solo está disponible en la consola de Amazon Fraud Detector y la validación está activada de forma predeterminada. Si no desea que Amazon Fraud Detector utilice la validación inteligente de datos antes de importar su conjunto de datos, desactive la validación en la consola de Amazon Fraud Detector cuando cargue su conjunto de datos.

## Validar los datos almacenados al utilizar las API o el AWS SDK

Al cargar eventos mediante la operación `SendEvent`, `GetEventPrediction`, o `CreateBatchImportJob` API, Amazon Fraud Detector valida lo siguiente:

- La configuración de ese tipo de evento está HABILITADA.
- Las marcas de tiempo de los eventos no se pueden actualizar. Un evento con un ID de evento repetido y un `EVENT_TIMESTAMP` diferente se tratará como un error.
- Los nombres y valores de las variables coinciden con el formato esperado. Para obtener más información, consulte [Crear una variable](#)
- Las variables obligatorias se rellenan con un valor.
- Todas las marcas de tiempo de los eventos no tienen más de 18 meses y no están en el future.

## Almacene los datos de eventos mediante la importación por lotes

Con la función de importación por lotes, puede cargar de forma rápida y sencilla grandes conjuntos de datos de eventos históricos en Amazon Fraud Detector mediante la consola, la API o el SDK de AWS. Para utilizar la importación por lotes, cree un archivo de entrada en formato CSV que

contenga todos los datos de sus eventos, cárguelo en el bucket de Amazon S3 e inicie un trabajo de importación. Amazon Fraud Detector primero valida los datos en función del tipo de evento y, a continuación, importa automáticamente todo el conjunto de datos. Una vez importados los datos, están listos para usarse para entrenar modelos nuevos o para volver a entrenar modelos existentes.

## Archivos de entrada y salida

El archivo CSV de entrada debe contener encabezados que coincidan con las variables definidas en el tipo de evento asociado más cuatro variables obligatorias. Para obtener más información, consulte [Preparar los datos de eventos para su almacenamiento](#). El tamaño máximo del archivo de datos de entrada es de 20 Gigabytes (GB), es decir, unos 50 millones de eventos. La cantidad de eventos variará según el tamaño del evento. Si el trabajo de importación se ha realizado correctamente, el archivo de salida está vacío. Si la importación no se realizó correctamente, el archivo de salida contiene los registros de errores.

## Crear un archivo CSV CSV CSV

Amazon Fraud Detector solo importa datos de archivos que están en formato CSV (CSV). La primera fila del archivo CSV debe contener encabezados de columna que coincidan exactamente con las variables definidas en el tipo de evento asociado, además de cuatro variables obligatorias: EVENT\_ID, EVENT\_TIMESTAMP, ENTITY\_ID y ENTITY\_TYPE. También puedes incluir, opcionalmente, EVENT\_LABEL y LABEL\_TIMESTAMP (si se incluye EVENT\_LABEL, se requiere LABEL\_TIMESTAMP).

## Definir variables obligatorias

Las variables obligatorias se consideran metadatos de eventos y deben especificarse en mayúsculas. Los metadatos de los eventos se incluyen automáticamente para el entrenamiento del modelo. En la siguiente tabla se enumeran las variables obligatorias, la descripción de cada variable y el formato requerido para la variable.

Nombre	Descripción	Requisitos
ID_DE_EVENTO	Un identificador del evento. Por ejemplo, si tu evento es una transacción en línea, el EVENT_ID puede ser el número de referencia de	<ul style="list-style-type: none"> <li>El EVENT_ID es obligatorio para los trabajos de importación por lotes.</li> <li>Debe ser único para ese evento.</li> </ul>

Nombre	Descripción	Requisitos
	la transacción que se le proporcionó a tu cliente.	<ul style="list-style-type: none"><li>• Debe representar información que sea significativa para su empresa.</li><li>• Debe satisfacer el patrón de expresiones regulares (por ejemplo, <code>^[0-9a-z_-]+\$.)</code></li><li>• No te recomendamos que añadas una marca de tiempo al <code>EVENT_ID</code>. Hacerlo podría causar problemas al actualizar el evento. Esto se debe a que debes proporcionar exactamente el mismo <code>EVENT_ID</code> si lo haces.</li></ul>

Nombre	Descripción	Requisitos
EVENT_TIMESTAMP	<p>La marca de tiempo de cuando se produjo el evento. La marca de tiempo debe estar en la norma ISO 8601 en UTC.</p>	<ul style="list-style-type: none"> <li>• El EVENT_TIMESTAMP es obligatorio para los trabajos de importación por lotes.</li> <li>• Debe especificarse en uno de los siguientes formatos: <ul style="list-style-type: none"> <li>• %YYYY-%MM-%DDT %HH: %mm: %sSz (estándar ISO 8601 solo en UTC sin milisegundos)</li> </ul> <p>Ejemplo: 2019-11-30T 13:01:01 Z</p> <li>• %aaaa/%mm/%dd %hh: %mm: %s (mañana y tarde)</li> <p>Ejemplos: 30 de noviembre de 2019 a las 13:01:01 p. m., o 30 de noviembre de 2019 a las 13:00:01</p> <li>• %mm/%dd/%aaaa %hh: %mm: %ss</li> <p>Ejemplos: 30/11/2019 1:01:01 p.m., 30/11/2019 13:01:01</p> <li>• %mm/%dd/%yy %h: %mm: %s</li> <p>Ejemplos: 30/11/19 1:01:01 p.m., 11/30/19 13:01:01</p> <li>• Amazon Fraud Detector hace las siguientes</li> </li></ul>

Nombre	Descripción	Requisitos
		<p>suposiciones al analizar los formatos de fecha y hora para las marcas de tiempo de los eventos:</p> <ul style="list-style-type: none"><li>• Si utiliza la norma ISO 8601, debe coincidir exactamente con la especificación anterior</li><li>• Si utiliza uno de los otros formatos, hay flexibilidad adicional:<ul style="list-style-type: none"><li>• Para meses y días, puedes proporcionar uno o dos dígitos. Por ejemplo, el 12 de enero de 2019 es una fecha válida.</li><li>• No necesita incluir hh:mm:ss si no los tiene (es decir, simplemente puede proporcionar una fecha). También puede proporcionar un subconjunto de solo la hora y los minutos (por ejemplo, hh:mm). No se admite solo proporcionar la hora. Tampoco se admiten milisegundos.</li><li>• Si proporciona etiquetas de mañana a tarde, se asume que es</li></ul></li></ul>

Nombre	Descripción	Requisitos
		<p>un reloj de 12 horas. Si no hay información AM/PM, se asume que el reloj es de 24 horas.</p> <ul style="list-style-type: none"> <li>• Puede utilizar «/» o «-» como delimitadores para los elementos de fecha. Se asume «:» para los elementos de marca de tiempo.</li> </ul>
IDENTIDAD_ENTIDAD	Un identificador de la entidad que está realizando el evento.	<ul style="list-style-type: none"> <li>• Se requiere ENTITY_ID para los trabajos de importación por lotes</li> <li>• Debe seguir el patrón de expresiones regulares: <code>^[0-9A-Za-z_@+-]+\$</code></li> <li>• Si el identificador de la entidad no está disponible en el momento de la evaluación, especifique el identificador de la entidad como desconocido.</li> </ul>
TIPO_DE_ENTIDAD	La entidad que realiza el evento, como un comerciante o un cliente	ENTITY_TYPE es obligatorio para los trabajos de importación por lotes
ETIQUETA_DE_EVENTO	Clasifica el evento como <code>fraudulent</code> o <code>legitimate</code>	Se requiere EVENT_LABEL si se incluye LABEL_TIMESTAMP

Nombre	Descripción	Requisitos
LABEL_TIMESTAMP	La marca de tiempo en la que se rellenó o actualizó la etiqueta del evento por última vez	<ul style="list-style-type: none"><li>• LABEL_TIMESTAMP es obligatorio si se incluye EVENT_LABEL.</li><li>• Debe seguir el formato de marca de tiempo.</li></ul>

## Carga de un archivo CSV en Amazon S3 para importarlo de lotes

Después de crear un archivo CSV con sus datos, carga el archivo en su bucket de Amazon Simple Storage Service (Amazon S3).

Para cargar datos de eventos en un bucket de Amazon S3

1. Inicie sesión en la AWS Management Console y abra la consola de Amazon S3 en <https://console.aws.amazon.com/s3/>.
2. Elija Create bucket (Crear bucket).

Se abrirá el asistente Crear bucket (Crear bucket).

3. En Bucket name (Nombre del bucket), escriba un nombre compatible con DNS para el bucket.

El nombre del bucket debe:

- Ser único en todo Amazon S3.
- Tener entre 3 y 63 caracteres.
- No contiene caracteres en mayúsculas.
- Comenzar por una letra minúscula o un número.

Una vez que haya creado el bucket, no podrá modificar su nombre. Para obtener información sobre la nomenclatura de buckets, consulte [Reglas de nomenclatura](#) de buckets en la Guía del usuario de Amazon Simple Storage Service.



**⚠ Important**

Evite incluir información confidencial, como números de cuenta, en el nombre del bucket. El nombre del bucket será visible en las URL que señalan a los objetos almacenados en él.

4. En Region (Región), elija la región de AWS en la que desea que se encuentre el bucket. Debe seleccionar la misma región en la que está utilizando Amazon Fraud Detector (Oregón).
5. En Configuración del bucket para Block Public Access, elija la configuración de Block Public Access que desee aplicar al bucket.

Le recomendamos que deje habilitada toda la configuración. Para obtener más información sobre el bloqueo de acceso [público, consulte Bloquear el acceso público a su almacenamiento de Amazon Simple Storage Service](#).

6. Elija Crear bucket.
7. Cargue el archivo de datos de entrenamiento en su bucket de Amazon S3. Anote la ruta de ubicación de Amazon S3 para su archivo de entrenamiento (por ejemplo, s3://bucketname/object.csv).

## Importación Batch de datos de eventos en la consola de Amazon Fraud Detector


Puede importar fácilmente una gran cantidad de sus conjuntos de datos de eventos en la consola de Amazon Fraud Detector, mediante la `CreateBatchImportJob` API o el SDK de AWS. Antes de continuar, asegúrese de haber seguido las instrucciones para preparar el conjunto de datos como un archivo CSV. Asegúrese de cargar también el archivo CSV en un bucket de Amazon S3.

### Uso de la consola Amazon Fraud Detector

Para importar datos de eventos por lotes en la consola

1. Abra la consola de AWS, inicie sesión en su cuenta y vaya a Amazon Fraud Detector.
2. En el panel de navegación izquierdo, elija Events.
3. Elige el tipo de evento.
4. Selecciona la pestaña Eventos almacenados.
5. En el panel de detalles de los eventos almacenados, asegúrese de que la ingesta de eventos esté activada.

6. En el panel Importar datos de eventos, seleccione Nueva importación.
7. En la página de importación de nuevos eventos, proporcione la siguiente información:
  - [Recomendado] Deje la opción Habilitar la validación inteligente de datos para este conjunto de datos: nueva configuración con la configuración predeterminada.
  - Para la función de IAM para datos, seleccione la función de IAM que creó para el bucket de Amazon S3 que contiene el archivo CSV que tiene previsto importar.
  - En Ubicación de datos de entrada, introduce la ubicación de S3 donde tienes tu archivo CSV.
  - Si desea especificar una ubicación independiente para almacenar los resultados de la importación, haga clic en el botón Separar la ubicación de datos para las entradas y los resultados y proporcione una ubicación de bucket de Amazon S3 válida.

 Important

Asegúrese de que el rol de IAM que ha seleccionado tenga permisos de lectura para su bucket de Amazon S3 de entrada y permisos de escritura para su bucket de Amazon S3 de salida.

8. Elija Start (Inicio).
9. La columna Estado del panel de datos de eventos de importación muestra el estado del trabajo de validación e importación. El banner de la parte superior proporciona una descripción detallada del estado, ya que el conjunto de datos pasa primero por la validación y, luego, por la importación.
10. Siga las instrucciones proporcionadas para [Monitorear el progreso del trabajo de validación e importación de conjuntos de datos](#).

### Monitorear el progreso del trabajo de validación e importación de conjuntos de datos

Si utiliza la consola de Amazon Fraud Detector para realizar un trabajo de importación por lotes, de forma predeterminada, Amazon Fraud Detector valida su conjunto de datos antes de la importación. Puede supervisar el progreso y el estado de los trabajos de validación e importación en la página de importación de nuevos eventos de la consola de Amazon Fraud Detector. En la parte superior de la página se muestra una breve descripción de los resultados de la validación y el estado del trabajo de importación. Según los resultados de la validación y el estado de su trabajo de importación, es posible que deba tomar medidas para garantizar que la validación e importación del conjunto de datos se realicen correctamente.

La siguiente tabla proporciona detalles de las acciones que debe realizar en función del resultado de las operaciones de validación e importación.

Mensaje de pancarta	Estado	Qué significa	Qué debo hacer
Se ha iniciado la validación de datos	Validación en curso	SDV ha empezado a validar su conjunto de datos	Espere a que cambie el estado
La validación de datos no puede continuar debido a errores en el conjunto de datos. Corrija los errores del archivo de datos e inicie un nuevo trabajo de importación. Consulte el informe de validación para obtener más información	Fallo en la validación	El SDV identificó problemas en tu archivo de datos. Estos problemas deben solucionarse para que la importación del conjunto de datos se realice correctamente.	En el panel Importar datos de eventos, seleccione el identificador del Job y consulte el informe de validación. Siga las recomendaciones del informe para corregir todos los errores de la lista. Para obtener más información, consulte <a href="#">Uso del informe de validación</a> .
Se ha iniciado la importación de datos. La validación se ha completado correctamente	Importación en curso	Su conjunto de datos ha superado la validación. AFD ha empezado a importar su	Espere a que cambie el estado

Mensaje de pancarta	Estado	Qué significa	Qué debo hacer
		conjunto de datos	
La validación se completó con advertencias. Se ha iniciado la importación de datos	Importación en curso	Algunos de los datos del conjunto de datos no se validaron. Sin embargo, los datos que superaron la validación cumplen con los requisitos mínimos de tamaño de datos para la importación.	Supervisa el mensaje del banner y espera a que cambie el estado

Mensaje de pancarta	Estado	Qué significa	Qué debo hacer
<p>Sus datos se importaron parcialmente. Algunos de los datos no se validaron y no se importaron. Consulte el informe de validación para obtener más información.</p>	<p>Importado. El estado muestra un icono de advertencia.</p>	<p>Algunos de los datos del archivo de datos que no se pudieron validar no se importaron. Se importó el resto de los datos que superaron la validación.</p>	<p>En el panel Importar datos de eventos, seleccione el identificador del Job y consulte el informe de validación. Siga las recomendaciones de la tabla de advertencias a nivel de datos para abordar las advertencias enumeradas. No es necesario abordar todas las advertencias. Sin embargo, asegúrese de que su conjunto de datos tenga más del 50% de los datos que superen la validación para que la importación se realice correctamente. Después de abordar las advertencias, inicie un nuevo trabajo de importación. Para obtener más información, consulte <a href="#">Uso del informe de validación</a>.</p>
<p>No se pudo importar los datos debido a un error de procesamiento. Iniciar un nuevo trabajo de importación de datos</p>	<p>Importación de errores</p>	<p>La importación falló debido a un error transitorio en tiempo de ejecución</p>	<p>Iniciar un nuevo trabajo de importación</p>

Mensaje de pancarta	Estado	Qué significa	Qué debo hacer
Los datos se importaron correctamente	Importado	Tanto la validación como la importación se completaron correctamente	Seleccione el identificador de Job de su trabajo de importación para ver los detalles y, a continuación, continúe con la formación del modelo.

#### Note

Recomendamos esperar 10 minutos después de que el conjunto de datos se haya importado correctamente a Amazon Fraud Detector para garantizar que el sistema los haya asimilado por completo.

## Informe de validación de datos inteligentes

La validación inteligente de datos crea un informe de validación una vez finalizada la validación. El informe de validación proporciona detalles de todos los problemas que el SDV ha identificado en tu conjunto de datos, con sugerencias de acciones para solucionar los problemas más impactantes. Puede utilizar el informe de validación para determinar cuáles son los problemas, dónde se encuentran en el conjunto de datos, la gravedad de los problemas y cómo solucionarlos. El informe de validación se crea incluso cuando la validación se completa correctamente. En este caso, puede ver el informe para ver si hay algún problema en la lista y, si lo hay, decidir si desea solucionar alguno de ellos.

#### Note

La versión actual del SDV analiza el conjunto de datos en busca de problemas que puedan provocar un error en la importación por lotes. Si la validación y la importación por lotes se realizan correctamente, es posible que el conjunto de datos siga teniendo problemas que puedan provocar un error en el entrenamiento del modelo. Le recomendamos que consulte el informe de validación aunque la validación y la importación se hayan realizado

correctamente, y que aborde todos los problemas que figuran en el informe para que la formación del modelo se realice correctamente. Después de solucionar los problemas, cree un nuevo trabajo de importación por lotes.

## Acceder al informe de validación

Puede acceder al informe de validación en cualquier momento una vez finalizada la validación mediante una de las siguientes opciones:

1. Una vez finalizada la validación y mientras el trabajo de importación esté en curso, en el encabezado superior, seleccione Ver informe de validación.
2. Una vez finalizado el Job de importación, en el panel Importar datos de eventos, elija el ID de trabajo del trabajo de importación que se acaba de completar.

## Uso del informe de validación

La página del informe de validación de su trabajo de importación proporciona los detalles de este trabajo de importación, una lista de los errores críticos, si se encuentran, una lista de advertencias sobre eventos (filas) específicos del conjunto de datos, si se encuentran, y un breve resumen del conjunto de datos que incluye información como los valores que no son válidos y los valores que faltan para cada variable.

- Importar detalles del trabajo

Proporciona detalles del trabajo de importación. Si el trabajo de importación ha fallado o el conjunto de datos se ha importado parcialmente, elija Ir al archivo de resultados para ver los registros de errores de los eventos que no se pudieron importar.

- Errores críticos


Proporciona detalles de los problemas más impactantes del conjunto de datos identificados por el SDV. Todos los problemas que aparecen en este panel son críticos y debe solucionarlos antes de continuar con la importación. Si intenta importar su conjunto de datos sin abordar los problemas críticos, es posible que su tarea de importación falle.

Para abordar los problemas críticos, siga las recomendaciones proporcionadas para cada advertencia. Tras solucionar todos los problemas enumerados en el panel Errores críticos, cree un nuevo trabajo de importación por lotes.

- Advertencias de nivel de datos

Proporciona un resumen de las advertencias para eventos específicos (filas) del conjunto de datos. Si el panel de advertencias a nivel de datos está lleno, algunos de los eventos del conjunto de datos no se validaron y no se importaron.

Para cada advertencia, la columna Descripción muestra el número de eventos que causan el problema. Además, los identificadores de eventos de ejemplo proporcionan una lista parcial de identificadores de eventos de muestra que puede utilizar como punto de partida para localizar el resto de los eventos que tienen el problema. Utilice la recomendación proporcionada como advertencia para solucionar el problema. Utilice también los registros de errores del archivo de salida para obtener información adicional sobre el problema. Los registros de errores se generan para todos los eventos en los que no se pudo importar el lote. Para acceder a los registros de errores, en el panel Importar detalles del trabajo, elija Ir al archivo de resultados.

 Note

Si más del 50% de los eventos (filas) del conjunto de datos no se validaron, también se producirá un error en el trabajo de importación. En este caso, debe corregir los datos antes de iniciar un nuevo trabajo de importación.

- Resumen del conjunto de datos

Proporciona un resumen del informe de validación del conjunto de datos. Si la columna Número de advertencias muestra más de 0 advertencias, decide si necesitas corregir esas advertencias. Si la columna Número de advertencias muestra 0, continúa entrenando tu modelo.

## Importación de datos de eventos de eventos de AWS para Python (Boto3)

En el ejemplo siguiente se muestra una solicitud de ejemplo [CreateBatchImportJob](#) de API. Un trabajo de importación por lotes debe incluir JoBid, InputPath, OutputPath eventTypeName y iamRoleArn. El JoBid no puede contener el mismo ID de un trabajo anterior, a menos que el trabajo exista en el estado CREATE\_FAILED. Las rutas InputPath y OutputPath deben ser rutas S3 válidas. Puede optar por no especificar el nombre del archivo en OutputPath; sin embargo, deberá proporcionar una ubicación de bucket de S3 válida. La eventTypeName tierra iamRoleArn debe existir. El rol de IAM debe conceder permisos de lectura para ingresar el bucket de Amazon S3 y permisos de escritura para generar el bucket de 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-*****'
)
```

## Cancelar trabajo de importación por lotes

Puede cancelar un trabajo de importación por lotes en curso en cualquier momento en la consola de Amazon Fraud Detector, mediante la `CancelBatchImportJob` API o el SDK de AWS.

Para cancelar un trabajo de importación de lotes en la consola,

1. Abra la consola de AWS, inicie sesión en su cuenta y vaya a Amazon Fraud Detector.
2. En el panel de navegación izquierdo, elija Events.
3. Elige el tipo de evento.
4. Selecciona la pestaña Eventos almacenados.
5. En el panel Importar datos de eventos, elija el identificador de trabajo de un trabajo de importación en curso que desee cancelar.
6. En la página del trabajo del evento, haga clic en Acciones y seleccione Cancelar la importación de eventos.
7. Elija Detener la importación de eventos para cancelar el trabajo de importación por lotes.

Cancelación de un trabajo de importación de lotes utilizando el SDK de AWS para Python (Boto3)

En el ejemplo siguiente se muestra una solicitud de ejemplo para la `CancelBatchImportJob` API. El trabajo de importación cancelado debe incluir el identificador de un trabajo de importación por lotes en curso.

```
import boto3
```

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

## Almacene los datos de eventos mediante la operación GetEventPredictions de la API

De forma predeterminada, todos los eventos que se envían a la `GetEventPrediction` API para su evaluación se almacenan en Amazon Fraud Detector. Esto significa que Amazon Fraud Detector almacenará automáticamente los datos de los eventos cuando genere una predicción y los utilizará para actualizar las variables calculadas casi en tiempo real. Puede deshabilitar el almacenamiento de datos accediendo al tipo de evento en la consola de Amazon Fraud Detector y desactivando la ingesta de eventos o actualizando el `EventIngestion` valor a `DISABLED` mediante la operación de la `PutEventType` API. Para obtener más información acerca del funcionamiento `GetEventPrediction` de la API, consulte [Predicciones de fraude](#).

### Important

Recomendamos encarecidamente que, una vez que habilite la ingesta de eventos para un tipo de evento, la mantengas habilitada. Si se desactiva la ingesta de eventos para el mismo tipo de evento y, a continuación, se generan predicciones, se puede producir un comportamiento incoherente.

## Almacene los datos de eventos mediante la operación SendEvent de la API

Puede utilizar la operación de la `SendEvent` API para almacenar eventos en Amazon Fraud Detector sin generar predicciones de fraude para esos eventos. Por ejemplo, puede usar la `SendEvent` operación para cargar un conjunto de datos histórico, que luego podrá usar para entrenar un modelo.

### Formatos de fecha y hora de eventos para SendEvent API

Al almacenar datos de eventos mediante la `SendEvent` API, debes asegurarte de que la marca de tiempo del evento esté en el formato requerido. Amazon Fraud Detector admite los siguientes formatos de fecha y hora:

- %YYYY-%MM-%DDT%HH: %mm: %sSz (estándar ISO 8601 solo en UTC sin milisegundos)

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

- %aaaa/%mm/%dd %hh: %mm: %s (mañana y tarde)

Ejemplos: 30 de noviembre de 2019 a las 13:01:01 p. m., o 30 de noviembre de 2019 a las 13:00:01

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

Ejemplos: 30/11/2019 1:01:01 p.m., 30/11/2019 13:01:01

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

Ejemplos: 30/11/19 1:01:01 p.m., 11/30/19 13:01:01

Amazon Fraud Detector hace las siguientes suposiciones al analizar los formatos de fecha y hora para las marcas de tiempo de los eventos:

- Si utiliza la norma ISO 8601, debe coincidir exactamente con la especificación anterior
- Si utiliza uno de los otros formatos, hay flexibilidad adicional:
  - Para meses y días, puedes proporcionar uno o dos dígitos. Por ejemplo, el 12 de enero de 2019 es una fecha válida.
  - No necesita incluir hh:mm:ss si no los tiene (es decir, simplemente puede proporcionar una fecha). También puede proporcionar un subconjunto de solo la hora y los minutos (por ejemplo, hh:mm). No se admite solo proporcionar la hora. Tampoco se admiten milisegundos.
  - Si proporciona etiquetas de mañana a tarde, se asume que es un reloj de 12 horas. Si no hay información AM/PM, se asume que el reloj es de 24 horas.
  - Puede utilizar «/» o «-» como delimitadores para los elementos de fecha. Se asume «:» para los elementos de marca de tiempo.

El siguiente es un ejemplo de llamada a `SendEvent` la 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@exampldomain.com',
'ip_address' : '1.2.3.4'},
        assignedLabel = 'legit',
        labelTimestamp = '2020-07-13T23:18:21Z',
        entities       = [{'entityType':'sample_customer', 'entityId':'12345'}],
    )
```

## Obtener detalles de los datos de un evento almacenados

Después de almacenar los datos de eventos en Amazon Fraud Detector, puede comprobar los datos más recientes que se almacenaron para un evento mediante la [GetEvent](#) API. El siguiente código de ejemplo comprueba los datos más recientes almacenados para el `sample_registration` evento.

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

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


## Ver las métricas del conjunto de datos de eventos almacenado

Para cada tipo de evento, puede ver métricas como el número de eventos almacenados, el tamaño total de los eventos almacenados y las marcas de tiempo de los eventos almacenados más antiguos y más recientes, en la consola de Amazon Fraud Detector.

Para ver las métricas de eventos almacenadas de un tipo de evento,

1. Abre la AWS consola e inicia sesión en tu cuenta. Navegue hasta Amazon Fraud Detector.
2. En el panel de navegación izquierdo, elija Events.
3. Elige el tipo de evento.
4. Selecciona la pestaña Eventos almacenados.

5. El panel de detalles de los eventos almacenados muestra las métricas. Estas estadísticas se actualizan automáticamente una vez al día.
6. Si lo desea, haga clic en Actualizar métricas de eventos para actualizarlas manualmente.

 Note

Si acabas de importar tus datos, te recomendamos que esperes entre 5 y 10 minutos después de haber terminado de importarlos para actualizar y ver las métricas.

# Orquestación de eventos

[La orquestación de eventos te facilita el envío de eventos Servicios de AWS para su procesamiento posterior mediante Amazon EventBridge](#) Amazon Fraud Detector le proporciona reglas sencillas que puede utilizar para automatizar el procesamiento de los eventos tras la detección del fraude. Con la organización de eventos, puede automatizar los procesos de eventos posteriores, como enviar los eventos a los paneles de control para obtener información a partir de los datos de los eventos, generar notificaciones en función de los resultados de la detección del fraude y actualizar los eventos con una etiqueta en función de lo aprendido de la detección del fraude.

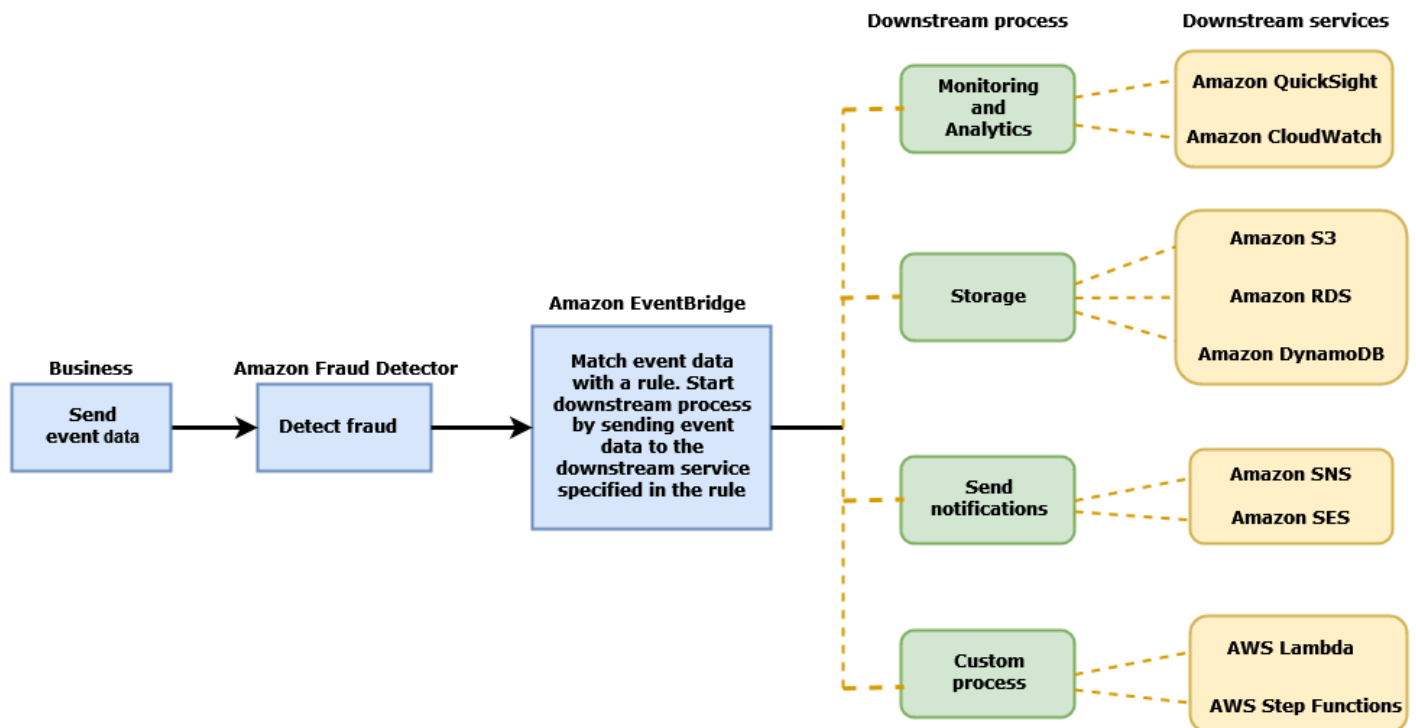
La organización de eventos proporciona un fácil acceso a los servicios del AWS entorno, a través de Amazon EventBridge. Puedes configurar Amazon EventBridge para que envíe eventos directamente Servicios de AWS o indirectamente mediante los [destinos de la API](#). Los Servicios de AWS que utilizas para organizar tus procesos posteriores también se denominan objetivos. Algunos de los objetivos que puede utilizar para organizar el procesamiento posterior son los siguientes:

- Para monitoreo y análisis — [Amazon QuickSight](#), [Amazon CloudWatch](#)
- Para almacenamiento: [Amazon S3](#), [Amazon RDS](#), [Amazon](#) DynamoDB
- [Para enviar notificaciones: Amazon SNS, Amazon SES](#)
- Para procesamiento personalizado: [AWS Lambda](#), [AWS](#) Step Functions

Para obtener más información sobre los objetivos de orquestación compatibles con Amazon EventBridge, consulta [Amazon EventBridge targets](#).

El siguiente diagrama proporciona una vista general de cómo funciona la orquestación de eventos.

## Event Orchestration



## Configuración de la orquestación de eventos

Para configurar la organización de eventos para sus eventos, debe configurar los procesos en el servicio de destino, configurar Amazon EventBridge para recibir y enviar datos de eventos y crear reglas en Amazon EventBridge que especifiquen las condiciones para iniciar los procesos posteriores. Complete los siguientes pasos para configurar la orquestación de eventos:

Para configurar la orquestación de eventos

1. Ve a la [Guía EventBridge del usuario de Amazon](#) y aprende a usar Amazon EventBridge. Asegúrate de aprender a crear [reglas](#) en Amazon EventBridge para tu caso de uso.
2. Sigue las instrucciones para [Habilite la organización de eventos en Amazon Fraud Detector](#).

### Note

La organización de eventos de tu evento está deshabilitada de forma predeterminada.

3. Configura tu servicio de destino para recibir y procesar los datos del evento. Por ejemplo, si su proceso posterior implica el envío de notificaciones y desea utilizar Amazon SNS, vaya a

la consola de Amazon SNS, cree un tema de SNS y, a continuación, suscriba un punto final al tema.

4. Sigue las instrucciones para [crear EventBridge las reglas de Amazon](#).

**⚠ Important**

Al crear el patrón de eventos en Amazon EventBridge, asegúrate de proporcionar el campo `aws.frauddetector` de origen y el campo `Event Prediction Result Returned` de tipo de detalle.

## Habilite la organización de eventos en Amazon Fraud Detector

Puede habilitar la organización de eventos para un evento al crear su tipo de evento o después de haberlo creado. La organización de eventos se puede activar en la consola de Amazon Fraud Detector, mediante el `put-event-type` comando, mediante la `PutEventType` API o mediante el AWS SDK for Python (Boto3).

## Habilite la organización de eventos en la consola de Amazon Fraud Detector

Este ejemplo permite la organización de eventos para un tipo de evento que ya se ha creado. Si va a crear un nuevo tipo de evento y quiere habilitar la orquestación, siga las instrucciones para hacerlo.

[Crear un tipo de evento](#)

Para habilitar la orquestación de eventos

1. Abra la [consola AWS de administración](#) e inicie sesión en su cuenta. Dirígete a Amazon Fraud Detector.
2. En el panel de navegación izquierdo, elija Events.
3. En la página de tipos de eventos, elige tu tipo de evento.
4. Activa Habilitar la organización de eventos con Amazon EventBridge.
5. Continúe con las instrucciones del paso 3 para [Configuración de la orquestación de eventos](#).



## Habilite la orquestación de eventos mediante el AWS SDK for Python (Boto3)

El siguiente ejemplo muestra un ejemplo de solicitud para actualizar un tipo de evento `sample_registration` a fin de habilitar la orquestación de eventos. En el ejemplo se utiliza la `PutEventType` API y se supone que ha creado las variables `ip_address` y `email_address`, las etiquetas `legit` y `fraud` el tipo `sample_customer` de entidad. Para obtener información sobre cómo crear estos recursos, consulta [Recursos](#).

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

## Desactivar la organización de eventos en Amazon Fraud Detector

Puede deshabilitar la organización de eventos para un evento en cualquier momento en la consola de Amazon Fraud Detector, mediante el `put-event-type` comando, la `PutEventType` API o el AWS SDK for Python (Boto3).

### Desactivar la organización de eventos en la consola de Amazon Fraud Detector

Para deshabilitar la organización de eventos

1. Abra la [consola AWS de administración](#) e inicie sesión en su cuenta. Dirígete a Amazon Fraud Detector.
2. En el panel de navegación izquierdo, elija Events.
3. En la página de tipos de eventos, elige tu tipo de evento.
4. Desactiva Habilitar la organización de eventos con Amazon EventBridge.

## Deshabilite la organización de eventos mediante la AWS SDK for Python (Boto3)

En el siguiente ejemplo, se muestra un ejemplo de solicitud para actualizar un tipo de evento `sample_registration` a fin de deshabilitar la organización de eventos mediante la `PutEventType` API.

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

# Modelo

Amazon Fraud Detector utiliza modelos de aprendizaje automático para generar predicciones de fraude. Cada modelo se entrena con un tipo de modelo. El tipo de modelo especifica los algoritmos y las transformaciones que se utilizan para entrenar el modelo. El entrenamiento con modelos es el proceso de usar un conjunto de datos que usted proporciona para crear un modelo que pueda predecir eventos fraudulentos.

Para crear un modelo, primero debe elegir un tipo de modelo y, a continuación, preparar y proporcionar los datos que se utilizarán para entrenar el modelo.

## Elija un tipo de modelo

Los siguientes tipos de modelos están disponibles en Amazon Fraud Detector. Elija un tipo de modelo que se adapte a su caso de uso.

- Información sobre el fraude en línea

El tipo de modelo Online Fraud Insights está optimizado para detectar el fraude cuando hay pocos datos históricos disponibles sobre la entidad que se está evaluando, por ejemplo, cuando un nuevo cliente se registra en línea para abrir una nueva cuenta.

- Información sobre el fraude en las transacciones

El tipo de modelo Transaction Fraud Insights es el más adecuado para detectar casos de fraude en los que la entidad que se está evaluando podría tener un historial de interacciones que el modelo pueda analizar para mejorar la precisión de las predicciones (por ejemplo, un cliente actual con un historial de compras anteriores).

- Información sobre la adquisición de cuentas

El tipo de modelo Account Takeover Insights detecta si una cuenta se ha visto comprometida por una suplantación de identidad u otro tipo de ataque. Los datos de inicio de sesión de una cuenta comprometida, como el navegador y el dispositivo utilizados al iniciar sesión, son diferentes de los datos de inicio de sesión históricos asociados a la cuenta.

## Información sobre el fraude en línea

Online Fraud Insights es un modelo de aprendizaje automático supervisado, lo que significa que utiliza ejemplos históricos de transacciones fraudulentas y legítimas para entrenar el modelo. El modelo Online Fraud Insights puede detectar el fraude basándose en pocos datos históricos. Los datos del modelo son flexibles, por lo que puedes adaptarlo para detectar diversos riesgos de fraude, como las reseñas falsas, el abuso de promociones y el fraude al pagar como huésped.

El modelo Online Fraud Insights utiliza un conjunto de algoritmos de aprendizaje automático para el enriquecimiento de los datos, la transformación y la clasificación del fraude. Como parte del proceso de formación del modelo, Online Fraud Insights enriquece los elementos de datos sin procesar, como la dirección IP y el número BIN, con datos de terceros, como la geolocalización de la dirección IP o el banco emisor de una tarjeta de crédito. Además de los datos de terceros, Online Fraud Insights utiliza algoritmos de aprendizaje profundo que tienen en cuenta los patrones de fraude que se han observado en Amazon y AWS. Estos patrones de fraude se convierten en elementos de entrada para su modelo mediante un algoritmo de aumento del árbol de gradientes.

Para aumentar el rendimiento, Online Fraud Insights optimiza los hiperparámetros del algoritmo de mejora del árbol de gradientes mediante un proceso de optimización bayesiano. Entrena secuencialmente docenas de modelos diferentes con diferentes parámetros del modelo (como el número de árboles, la profundidad de los árboles y el número de muestras por hoja). También utiliza diferentes estrategias de optimización, como aumentar la ponderación de la población minoritaria dedicada al fraude para hacer frente a unas tasas de fraude muy bajas.

### Selección de la fuente de datos

Al entrenar un modelo de Online Fraud Insights, puede elegir entrenar el modelo con datos de eventos que se almacenan externamente (fuera de Amazon Fraud Detector) o almacenados dentro de Amazon Fraud Detector. El almacenamiento externo que Amazon Fraud Detector admite actualmente es Amazon Simple Storage Service (Amazon S3). Si utiliza almacenamiento externo, su conjunto de datos de eventos debe cargarse en formato de valores separados por comas (CSV) en un bucket de Amazon S3. En la configuración de entrenamiento del modelo, estas opciones de almacenamiento de datos se denominan `EXTERNAL_EVENTS` (para almacenamiento externo) e `INGESTED_EVENTS` (para almacenamiento interno). Para obtener más información sobre las fuentes de datos disponibles y cómo almacenar datos en ellas, consulte [Almacenamiento de datos de eventos](#)

## Preparación de datos

Independientemente de dónde elija almacenar los datos de sus eventos (Amazon S3 o Amazon Fraud Detector), los requisitos para el tipo de modelo Online Fraud Insights son los mismos.

Su conjunto de datos debe contener el encabezado de la columna `EVENT_LABEL`. Esta variable clasifica un evento como fraudulento o legítimo. Cuando utilices un archivo CSV (almacenamiento externo), debes incluir `EVENT_LABEL` para cada evento del archivo. Para el almacenamiento interno, el campo `EVENT_LABEL` es opcional, pero todos los eventos deben estar etiquetados para poder incluirlos en un conjunto de datos de entrenamiento. Al configurar tu modelo de entrenamiento, puedes elegir si deseas ignorar los eventos sin etiquetar, usar una etiqueta legítima para los eventos sin etiquetar o asumir una etiqueta fraudulenta para todos los eventos sin etiquetar.

## Selección de datos

Consulte [Recopilar datos de eventos](#) para obtener información sobre cómo seleccionar datos para capacitar su modelo Online Fraud Insights.

El proceso de formación en línea sobre Fraud Insights toma muestras y divide los datos históricos en función de `EVENT_TIMESTAMP`. No es necesario muestrear los datos manualmente y hacerlo podría afectar negativamente a los resultados del modelo.

## Variables de evento

El modelo Online Fraud Insights requiere al menos dos variables, además de los metadatos de eventos necesarios, que hayan pasado la [validación de datos](#) para el entrenamiento del modelo y admite hasta 100 variables por modelo. Por lo general, cuantas más variables proporcione, mejor podrá diferenciar el modelo entre fraude y eventos legítimos. Si bien el modelo Online Fraud Insights admite docenas de variables, incluidas variables personalizadas, recomendamos incluir la dirección IP y la dirección de correo electrónico, ya que estas variables suelen ser más eficaces para identificar a la entidad que se está evaluando.

## Validar los datos

Como parte del proceso de formación, Online Fraud Insights validará el conjunto de datos para detectar problemas de calidad de los datos que puedan afectar a la formación del modelo. Tras validar los datos, Amazon Fraud Detector tomará las medidas adecuadas para crear el mejor modelo posible. Esto incluye emitir advertencias sobre posibles problemas de calidad de los datos, eliminar automáticamente las variables que tengan problemas con la calidad de los datos o emitir un error y

detener el proceso de formación del modelo. Para obtener más información, consulte la [validación del conjunto de datos](#).

## Información sobre el fraude en las transacciones

El tipo de modelo Transaction Fraud Insights está diseñado para detectar el fraude en línea o card-not-present el fraude de transacciones. Transaction Fraud Insights es un modelo de aprendizaje automático supervisado, lo que significa que utiliza ejemplos históricos de transacciones fraudulentas y legítimas para entrenar el modelo.

El modelo Transaction Fraud Insights utiliza un conjunto de algoritmos de aprendizaje automático para el enriquecimiento de los datos, la transformación y la clasificación del fraude. Utiliza un motor de ingeniería de funciones para crear agregados a nivel de entidad y de evento. Como parte del proceso de formación del modelo, Transaction Fraud Insights enriquece los elementos de datos sin procesar, como la dirección IP y el número BIN, con datos de terceros, como la geolocalización de la dirección IP o el banco emisor de una tarjeta de crédito. Además de los datos de terceros, Transaction Fraud Insights utiliza algoritmos de aprendizaje profundo que tienen en cuenta los patrones de fraude observados en Amazon y AWS estos patrones de fraude se convierten en elementos de entrada para su modelo mediante un algoritmo de aumento del árbol de gradientes.

Para aumentar el rendimiento, Transaction Fraud Insights optimiza los hiperparámetros del algoritmo de aumento del árbol de gradientes mediante un proceso de optimización bayesiano, entrenando secuencialmente docenas de modelos diferentes con diferentes parámetros del modelo (como el número de árboles, la profundidad de los árboles, el número de muestras por hoja), así como diferentes estrategias de optimización, como aumentar la ponderación de la población minoritaria de fraude para hacer frente a tasas de fraude muy bajas.

Como parte del proceso de formación del modelo, el motor de ingeniería de funciones del modelo de fraude de transacciones calcula los valores de cada entidad única dentro de su conjunto de datos de formación para ayudar a mejorar las predicciones de fraude. Por ejemplo, durante el proceso de formación, Amazon Fraud Detector calcula y almacena la última vez que una entidad realizó una compra y actualiza este valor de forma dinámica cada vez que llamas a la SendEvent API `GetEventPrediction` o. Durante una predicción de fraude, las variables del evento se combinan con otros metadatos de entidades y eventos para predecir si la transacción es fraudulenta.

## Selección de la fuente de datos

Los modelos de Transaction Fraud Insights se basan únicamente en un conjunto de datos almacenado internamente en Amazon Fraud Detector (`INGESTED_EVENTS`). Esto permite a

Amazon Fraud Detector actualizar continuamente los valores calculados sobre las entidades que está evaluando. Para obtener más información sobre las fuentes de datos disponibles, consulte [Almacenamiento de datos de eventos](#)

## Preparación de datos

Antes de entrenar un modelo de Transaction Fraud Insights, asegúrese de que su archivo de datos contenga todos los encabezados, tal como se menciona en el [conjunto de datos de eventos Prepare](#). El modelo Transaction Fraud Insights compara las nuevas entidades que se reciben con los ejemplos de entidades fraudulentas y legítimas del conjunto de datos, por lo que resulta útil proporcionar muchos ejemplos para cada entidad.

Amazon Fraud Detector transforma automáticamente el conjunto de datos de eventos almacenado en el formato correcto para la formación. Una vez que el modelo haya completado el entrenamiento, puede revisar las métricas de rendimiento y determinar si debe agregar entidades a su conjunto de datos de entrenamiento.

## Selección de datos

De forma predeterminada, Transaction Fraud Insights utiliza todo el conjunto de datos almacenado para el tipo de evento que seleccione. Si lo desea, puede establecer un intervalo de tiempo para reducir los eventos que se utilizan para entrenar su modelo. Al establecer un intervalo de tiempo, asegúrese de que los registros que se utilizan para entrenar el modelo hayan tenido tiempo suficiente para madurar. Es decir, ha transcurrido suficiente tiempo para garantizar que los registros legítimos y de fraude se hayan identificado correctamente. Por ejemplo, en el caso del fraude por contracargos, se suelen tardar 60 días o más en identificar correctamente los eventos fraudulentos. Para obtener el mejor rendimiento del modelo, asegúrate de que todos los registros de tu conjunto de datos de entrenamiento estén actualizados.

No es necesario seleccionar un intervalo de tiempo que represente una tasa de fraude ideal. Amazon Fraud Detector toma muestras automáticamente de sus datos para lograr un equilibrio entre las tasas de fraude, el intervalo de tiempo y el recuento de entidades.

Amazon Fraud Detector devuelve un error de validación durante el entrenamiento del modelo si seleccionas un intervalo de tiempo en el que no hay suficientes eventos para entrenar correctamente un modelo. En el caso de los conjuntos de datos almacenados, el campo `EVENT_LABEL` es opcional, pero los eventos deben estar etiquetados para poder incluirlos en el conjunto de datos de entrenamiento. Al configurar tu modelo de entrenamiento, puedes elegir si deseas ignorar los

eventos sin etiquetar, usar una etiqueta legítima para los eventos sin etiquetar o asumir una etiqueta fraudulenta para los eventos sin etiquetar.

## Variables de eventos

El tipo de evento utilizado para entrenar el modelo debe contener al menos 2 variables, además de los metadatos de eventos necesarios, que hayan pasado la [validación de datos](#) y puedan contener hasta 100 variables. Por lo general, cuantas más variables se proporcionen, mejor podrá diferenciar el modelo entre el fraude y los eventos legítimos. Si bien el modelo Transaction Fraud Insight admite docenas de variables, incluidas las personalizadas, le recomendamos que incluya la dirección IP, la dirección de correo electrónico, el tipo de instrumento de pago, el precio del pedido y el BIN de la tarjeta.

## Validar los datos

Como parte del proceso de formación, Transaction Fraud Insights valida el conjunto de datos de formación para detectar problemas de calidad de los datos que puedan afectar a la formación del modelo. Tras validar los datos, Amazon Fraud Detector toma las medidas adecuadas para crear el mejor modelo posible. Esto incluye emitir advertencias sobre posibles problemas de calidad de los datos, eliminar automáticamente las variables que tengan problemas con la calidad de los datos o emitir un error y detener el proceso de formación del modelo. Para obtener más información, consulte [Validación del conjunto de datos](#).

Amazon Fraud Detector emitirá una advertencia, pero seguirá entrenando un modelo si el número de entidades únicas es inferior a 1500, ya que esto puede afectar a la calidad de los datos de formación. Si recibes una advertencia, revisa la [métrica de rendimiento](#).

## Información sobre la apropiación de cuentas

El tipo de modelo Account Takeover Insights (ATI) identifica la actividad fraudulenta en línea al detectar si las cuentas se vieron comprometidas por apropiaciones malintencionadas, suplantación de identidad o por el robo de credenciales. Account Takeover Insights es un modelo de aprendizaje automático que utiliza los eventos de inicio de sesión de su negocio en línea para entrenar el modelo.

Puedes integrar un modelo especializado de Account Takeover Insights en tu flujo de inicio de sesión en tiempo real para detectar si una cuenta está comprometida. El modelo evalúa una variedad de tipos de autenticación e inicio de sesión. Incluyen los inicios de sesión en aplicaciones web, las autenticaciones basadas en API y single-sign-on (SSO). Para usar el modelo Account Takeover Insights, llama a la [GetEventPrediction](#) API después de presentar unas credenciales de inicio de



sesión válidas. La API genera una puntuación que cuantifica el riesgo de que la cuenta se vea comprometida. Amazon Fraud Detector utiliza la puntuación y las reglas que usted definió para obtener uno o más resultados de los eventos de inicio de sesión. Los resultados son los que usted configuró. En función de los resultados que reciba, podrá tomar las medidas adecuadas para cada inicio de sesión. Es decir, puede aprobar o impugnar las credenciales presentadas para el inicio de sesión. Por ejemplo, puede cuestionar las credenciales solicitando el PIN de la cuenta como verificación adicional.

También puedes usar el modelo Account Takeover Insights para evaluar los inicios de sesión de las cuentas de forma asíncrona y tomar medidas en las cuentas de alto riesgo. Por ejemplo, se puede añadir una cuenta de alto riesgo a la cola de investigación para que un revisor humano determine si es necesario tomar medidas adicionales, como suspender la cuenta.

El modelo Account Takeover Insights se ha diseñado con un conjunto de datos que contiene el historial de inicios de sesión de su empresa. Usted proporciona estos datos. Si lo desea, puede etiquetar las cuentas como legítimas o fraudulentas. Sin embargo, esto no es necesario para entrenar el modelo. El modelo Account Takeover Insights detecta las anomalías en función del historial de inicios de sesión satisfactorios de una cuenta. También aprende a detectar anomalías en el comportamiento de un usuario que sugieran un mayor riesgo de que se produzca un robo malintencionado de una cuenta. Por ejemplo, un usuario que normalmente inicia sesión desde el mismo conjunto de dispositivos y direcciones IP. Por lo general, un defraudador inicia sesión desde un dispositivo y una ubicación geográfica diferentes. Esta técnica genera una puntuación de riesgo de que una actividad sea anómala, lo que suele ser una de las principales características de las apropiaciones malintencionadas de cuentas.

Antes de entrenar un modelo de Account Takeover Insights, Amazon Fraud Detector utiliza una combinación de técnicas de aprendizaje automático para enriquecer, agregar y transformar datos. Luego, durante el proceso de formación, Amazon Fraud Detector enriquece los elementos de datos sin procesar que usted proporciona. Algunos ejemplos de elementos de datos sin procesar incluyen la dirección IP y el agente de usuario. Amazon Fraud Detector utiliza estos elementos para crear entradas adicionales que describen los datos de inicio de sesión. Estas entradas incluyen las entradas del dispositivo, el navegador y la geolocalización. Amazon Fraud Detector también utiliza los datos de inicio de sesión que usted proporciona para calcular continuamente variables agregadas que describen el comportamiento de los usuarios en el pasado. Algunos ejemplos del comportamiento de los usuarios incluyen el número de veces que el usuario ha iniciado sesión desde una dirección IP específica. Con estas mejoras y agregados adicionales, Amazon Fraud Detector puede generar un sólido rendimiento del modelo a partir de un pequeño conjunto de entradas de sus eventos de inicio de sesión.

El modelo Account Takeover Insights detecta los casos en los que un infractor accede a una cuenta legítima, independientemente de si el infractor es humano o un robot. El modelo genera una puntuación única que indica el riesgo relativo de comprometer la cuenta. Las cuentas que podrían haberse visto comprometidas se marcan como cuentas de alto riesgo. Puedes procesar las cuentas de alto riesgo de dos maneras. O bien, puedes exigir una verificación de identidad adicional. O bien, puedes enviar la cuenta a una lista de espera para que la investiguen manualmente.

## Selección de la fuente de datos

Los modelos de Account Takeover Insights se basan en un conjunto de datos que se almacena internamente en Amazon Fraud Detector. Para almacenar los datos de sus eventos de inicio de sesión con Amazon Fraud Detector, cree un archivo CSV con los eventos de inicio de sesión de los usuarios. Para cada evento, incluya los datos de inicio de sesión, como la marca de tiempo del evento, el ID de usuario, la dirección IP, el agente de usuario y si los datos de inicio de sesión son válidos. Tras crear el archivo CSV, súbelo primero a Amazon Fraud Detector y, a continuación, utilice la función de importación para almacenar los datos. A continuación, puede entrenar su modelo con los datos almacenados. Para obtener más información sobre cómo almacenar tu conjunto de datos de eventos con Amazon Fraud Detector, consulta [Almacene los datos de sus eventos internamente con Amazon Fraud Detector](#)

## Preparación de datos

Amazon Fraud Detector requiere que proporciones los datos de inicio de sesión de tu cuenta de usuario en un archivo de valores separados por comas (CSV) codificado en formato UTF-8. La primera línea del archivo CSV debe contener un encabezado de archivo. El encabezado del archivo consta de metadatos de eventos y variables de eventos que describen cada elemento de datos. Los datos del evento siguen al encabezado. Cada línea de los datos del evento consta de datos de un solo evento de inicio de sesión.

Para el modelo Accounts Takeover Insights, debes proporcionar los siguientes metadatos y variables de eventos en la línea de encabezado de tu archivo CSV.

### Metadatos del evento

Te recomendamos que introduzcas los siguientes metadatos en el encabezado del archivo CSV. Los metadatos del evento deben estar en mayúsculas.

- **EVENT\_ID**: identificador único para el evento de inicio de sesión.
- **ENTITY\_TYPE**: la entidad que realiza el evento de inicio de sesión, como un comerciante o un cliente.

- ENTITY\_ID: identificador de la entidad que realiza el evento de inicio de sesión.
- EVENT\_TIMESTAMP: la marca de tiempo en que se produjo el evento de inicio de sesión. La marca de tiempo debe estar en la norma ISO 8601 en UTC.
- EVENT\_LABEL (recomendado): etiqueta que clasifica el evento como fraudulento o legítimo. Puedes usar cualquier etiqueta, como «fraude», «legítimo», «1» o «0».

#### Note

- Los metadatos del evento deben estar en mayúsculas. Distingue entre mayúsculas y minúsculas.
- No se requieren etiquetas para los eventos de inicio de sesión. Sin embargo, te recomendamos que incluyas los metadatos de EVENT\_LABEL y proporciones etiquetas para tus eventos de inicio de sesión. No hay problema si las etiquetas están incompletas o son esporádicas. Si facilitas etiquetas, Amazon Fraud Detector las utilizará para calcular automáticamente la tasa de robo de cuentas descubiertas y la mostrará en el gráfico y la tabla de rendimiento del modelo.

## Variables de eventos

Para el modelo Accounts Takeover Insights, hay variables obligatorias (obligatorias) que debe proporcionar y variables opcionales. Al crear las variables, asegúrese de asignarlas al tipo de variable correcto. Como parte del proceso de formación del modelo, Amazon Fraud Detector utiliza el tipo de variable asociado a la variable para realizar el enriquecimiento de variables y la ingeniería de características.

#### Note

Los nombres de las variables de eventos deben estar en minúsculas. Distinguen mayúsculas de minúsculas.

## Variables obligatorias

Las siguientes variables son necesarias para entrenar un modelo de Accounts Takeover Insights.

Categoría	Tipo de variable	Descripción
Dirección IP	IP_ADDRESS	La dirección IP utilizada en el evento de inicio de sesión
Navegador y dispositivo	AGENTE DE USUARIO	El navegador, el dispositivo y el sistema operativo utilizados en el evento de inicio de sesión
Credenciales válidas	CREDO VÁLIDO	Indica si las credenciales que se utilizaron para iniciar sesión son válidas

### Variables opcionales

Las siguientes variables son opcionales para entrenar un modelo de Accounts Takeover Insights.

Categoría	Tipo	Descripción
Navegador y dispositivo	HUELLA DACTILAR	El identificador único de la huella digital de un navegador o dispositivo
ID de sesión	SESSION_ID	El identificador de una sesión de autenticación
Etiqueta	EVENT_LABEL	Una etiqueta que clasifica el evento como fraudulento o legítimo. Puedes usar cualquier etiqueta, como «fraude», «legítimo», «1» o «0».
Timestamp	LABEL_TIMESTAMP	La marca de tiempo de la última actualización de la etiqueta. Esto es obligatorio si

Categoría	Tipo	Descripción
		se proporciona EVENT_LAB EL.

#### Note

- Puede proporcionar cualquier nombre de variable para ambas variables obligatorias (variables opcionales). Es importante que cada variable obligatoria y opcional se asigne al tipo de variable correcto.
- Puede proporcionar variables adicionales. Sin embargo, Amazon Fraud Detector no incluirá estas variables para entrenar un modelo de Accounts Takeover Insights.

## Selección de datos

La recopilación de datos es un paso importante para crear su modelo Account Takeover Insights. Cuando comience a recopilar sus datos de inicio de sesión, tenga en cuenta los siguientes requisitos y recomendaciones:

### Obligatorio

- Proporcione al menos 1500 ejemplos de cuentas de usuario, cada uno con al menos dos eventos de inicio de sesión asociados.
- Tu conjunto de datos debe cubrir al menos 30 días de eventos de inicio de sesión. Más adelante, podrá especificar el intervalo de tiempo específico de los eventos que se utilizarán para entrenar el modelo.

### Recomendado

- Su conjunto de datos incluye ejemplos de eventos de inicio de sesión fallidos. Si lo desea, puede etiquetar estos inicios de sesión fallidos como «fraudulentos» o «legítimos».
- Prepara datos históricos con eventos de inicio de sesión que abarquen más de seis meses e incluyan 100 000 entidades.

Si aún no tienes un conjunto de datos que cumpla con los requisitos mínimos, considera la posibilidad de transmitir los datos del evento a Amazon Fraud Detector llamando a la operación de [SendEventAPI](#).

## Validar los datos

Antes de crear tu modelo Account Takeover Insights, Amazon Fraud Detector comprueba si los metadatos y las variables que incluiste en tu conjunto de datos para entrenar el modelo cumplen los requisitos de tamaño y formato. Para más información, consulte [Validación de conjunto de datos](#). También comprueba otros requisitos. Si el conjunto de datos no pasa la validación, no se crea el modelo. Para que el modelo se cree correctamente, asegúrate de corregir los datos que no pasaron la validación antes de volver a entrenar.

### Errores comunes en los conjuntos de datos

Al validar un conjunto de datos para entrenar un modelo de Account Takeover Insights, Amazon Fraud Detector analiza estos y otros problemas y arroja un error si encuentra uno o más de ellos.

- El archivo CSV no está en formato UTF-8.
- El encabezado del archivo CSV no contiene al menos uno de los siguientes metadatos: `EVENT_ID`, `ENTITY_ID`, o `EVENT_TIMESTAMP`
- El encabezado del archivo CSV no contiene al menos una variable de los siguientes tipos de variables: `IP_ADDRESS`, `USERAGENT`, o `VALIDCRED`.
- Hay más de una variable asociada al mismo tipo de variable.
- Más del 0,1% de los valores `EVENT_TIMESTAMP` contiene valores nulos o valores distintos de los formatos de fecha y hora admitidos.
- El número de días entre el primer y el último evento es inferior a 30 días.
- Más del 10% de las variables de este tipo no son válidas o son nulas. `IP_ADDRESS`
- Más del 50% de las variables del tipo de `USERAGENT` variable contienen valores nulos.
- Todas las variables del tipo de `VALIDCRED` variable están configuradas en `false`

## Creación de un modelo

Los modelos de Amazon Fraud Detector aprenden a detectar el fraude en un tipo de evento específico. En Amazon Fraud Detector, primero debe crear un modelo, que actúa como contenedor para las versiones de su modelo. Cada vez que entrena un modelo, se crea una nueva versión.

Para obtener más información sobre cómo crear y entrenar un modelo mediante la AWS consola, consulte [Paso 3: Crear un modelo](#).

Cada modelo tiene una variable de puntuación correspondiente. Amazon Fraud Detector crea esta variable en tu nombre cuando creas un modelo. Puede utilizar esta variable en las expresiones de sus reglas para interpretar las puntuaciones del modelo durante una evaluación de fraude.

## Entrene e implemente un modelo utilizando el AWS SDK for Python (Boto3)

Se crea una versión del modelo llamando a las `CreateModelVersion` operaciones `CreateModel` y `CreateModel` inicia el modelo, que actúa como contenedor para las versiones del modelo. `CreateModelVersion` inicia el proceso de formación, que da como resultado una versión específica del modelo. Se crea una nueva versión de la solución cada vez que se llama a `CreateModelVersion`.

En el siguiente ejemplo, se muestra un ejemplo de solicitud para la `CreateModel` API. En este ejemplo, se crea el tipo de modelo `Online Fraud Insights` y se supone que se ha creado un tipo de evento `sample_registration`. Para obtener información adicional sobre la creación de un tipo de evento, consulte [Crear un tipo de evento](#).

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

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

Entrena tu primera versión con la [CreateModelVersion](#) API. Para `TrainingDataSource` y `ExternalEventsDetail` especifique la fuente y la ubicación en Amazon S3 del conjunto de datos de entrenamiento. Para ello, `TrainingDataSchema` especifique cómo Amazon Fraud Detector debe interpretar los datos de formación, específicamente qué variables de eventos incluir y cómo clasificar las etiquetas de los eventos. De forma predeterminada, Amazon Fraud Detector ignora los eventos no etiquetados. Este código de ejemplo se utiliza `AUTO` for `unlabeledEventsTreatment` para especificar que Amazon Fraud Detector decide cómo utilizar los eventos no etiquetados.

```
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'
}
)
```

Si la solicitud es correcta, aparecerá una nueva versión del modelo con el estado `TRAINING_IN_PROGRESS` correcto. En cualquier momento de la formación, puedes cancelarla llamando `UpdateModelVersionStatus` y actualizando el estado a `TRAINING_CANCELLED`. Una vez finalizada la formación, el estado de la versión del modelo se actualizará a `TRAINING_COMPLETE`. Puedes revisar el rendimiento del modelo en la consola de Amazon Fraud Detector o llamando por teléfono `DescribeModelVersions`. Para obtener más información sobre cómo interpretar las puntuaciones y el rendimiento de los modelos, consulte [Puntuaciones del modelo](#) y [Métricas de rendimiento del modelo](#).

Tras revisar el rendimiento del modelo, actívalo para que los detectores puedan utilizarlo en las predicciones de fraudes en tiempo real. Amazon Fraud Detector desplegará el modelo en varias zonas de disponibilidad para garantizar la redundancia y activará el autoscaling para garantizar que el modelo se adapte al número de predicciones de fraude que realice. Para activar el modelo, llame a la `UpdateModelVersionStatus` API y actualice el estado a `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'  
)
```

## Puntuaciones del modelo

Amazon Fraud Detector genera puntuaciones de modelos diferentes para los distintos tipos de modelos.

Para los modelos Account Takeover Insights (ATI), Amazon Fraud Detector utiliza únicamente un valor agregado (un valor que se calcula mediante la combinación de un conjunto de variables sin procesar) para generar la puntuación del modelo. Se genera una puntuación de -1 para el primer evento de una nueva entidad, lo que indica un riesgo desconocido. Esto se debe a que, en el caso de una entidad nueva, los valores utilizados para calcular el agregado serán cero o nulos. El modelo Account Takeover Insights (ATI) genera puntuaciones de entre 0 y 1000 para todos los eventos posteriores para la misma entidad y para las entidades existentes, donde 0 indica un riesgo de fraude bajo y 1000 indica un riesgo de fraude alto. En el caso de los modelos ATI, las puntuaciones del modelo están directamente relacionadas con la tasa de desafío (CR). Por ejemplo, una puntuación de 500 corresponde a una tasa de desafío estimada del 5%, mientras que una puntuación de 900 corresponde a una tasa de desafío estimada del 0,1%.

Para los modelos Online Fraud Insights (OFI) y Transaction Fraud Insights (TFI), Amazon Fraud Detector utiliza tanto el valor agregado (un valor que se calcula mediante la combinación de un conjunto de variables sin procesar) como el valor sin procesar (el valor proporcionado para la variable) para generar las puntuaciones del modelo. Las puntuaciones del modelo pueden estar entre 0 y 1000, donde 0 indica un riesgo de fraude bajo y 1000 indica un riesgo de fraude alto. En el caso de los modelos OFI y TFI, las puntuaciones del modelo están directamente relacionadas con la tasa de falsos positivos (FPR). Por ejemplo, una puntuación de 600 corresponde a una tasa estimada de falsos positivos del 10%, mientras que una puntuación de 900 corresponde a una tasa estimada de falsos positivos del 2%. La siguiente tabla proporciona detalles sobre cómo se correlacionan las puntuaciones de ciertos modelos con las tasas de falsos positivos estimadas.

Puntuación del modelo	FPR estimado
975	0,50%
950	1%
900	2%

Puntuación del modelo	FPR estimado
860	3%
775	5%
700	7%
600	10%

## Métricas de rendimiento del modelo

Una vez finalizada la formación del modelo, Amazon Fraud Detector valida el rendimiento del modelo utilizando el 15% de los datos que no se utilizaron para entrenar el modelo. Puede esperar que su modelo entrenado de Amazon Fraud Detector tenga un rendimiento de detección de fraudes en el mundo real similar al de las métricas de rendimiento de validación.


Como empresa, debes encontrar un equilibrio entre detectar más fraudes y provocar más problemas con los clientes legítimos. Para ayudarte a elegir el equilibrio adecuado, Amazon Fraud Detector proporciona las siguientes herramientas para evaluar el rendimiento del modelo:

- **Gráfico de distribución de puntuaciones:** un histograma de las distribuciones de puntuaciones de un modelo supone un ejemplo de población de 100 000 eventos. El eje Y izquierdo representa los eventos legítimos y el eje Y derecho representa los eventos de fraude. Puede seleccionar un umbral de modelo específico haciendo clic en el área del gráfico. Esto actualizará las vistas correspondientes en la matriz de confusión y el gráfico ROC.
- **Matriz de confusión:** resume la precisión del modelo para un umbral de puntuación determinado comparando las predicciones del modelo con los resultados reales. Amazon Fraud Detector supone un ejemplo de población de 100 000 eventos. La distribución del fraude y de los eventos legítimos simula la tasa de fraude en sus empresas.
  - **Verdaderos aspectos positivos:** el modelo predice el fraude y, en realidad, el hecho es un fraude.
  - **Falsos positivos:** el modelo predice el fraude, pero en realidad el hecho es legítimo.
  - **Verdaderos negativos:** el modelo predice que el evento es legítimo y, de hecho, lo es.
  - **Falsos negativos:** el modelo predice que el evento es legítimo, pero en realidad es un fraude.
  - **Tasa de resultados positivos verdaderos (TPR):** porcentaje del fraude total que detecta el modelo. También se conoce como tasa de captura.

- Tasa de falsos positivos (FPR): porcentaje del total de eventos legítimos que se predicen incorrectamente como fraude.
- Curva del operador del receptor (ROC): traza la tasa de positivos verdaderos en función de la tasa de falsos positivos en todos los umbrales de puntuación posibles del modelo. Para ver este gráfico, selecciona Métricas avanzadas.
- Área bajo la curva (AUC): resume la TPR y la FPR en todos los umbrales de puntuación posibles del modelo. Un modelo sin poder predictivo tiene un AUC de 0,5, mientras que un modelo perfecto tiene una puntuación de 1,0.
- Rango de incertidumbre: muestra el rango de AUC esperado del modelo. Un rango mayor (diferencia en el límite superior e inferior del AUC  $> 0,1$ ) significa una mayor incertidumbre del modelo. Si el rango de incertidumbre es amplio ( $>0,1$ ), considere la posibilidad de proporcionar más eventos etiquetados y volver a entrenar el modelo.

Para utilizar las métricas de rendimiento del modelo

1. Comience con la tabla de distribución de puntuaciones para revisar la distribución de las puntuaciones modelo en relación con sus casos de fraude y eventos legítimos. Lo ideal es que haya una separación clara entre el fraude y los eventos legítimos. Esto indica que el modelo puede identificar con precisión qué eventos son fraudulentos y cuáles son legítimos. Seleccione un umbral del modelo haciendo clic en el área del gráfico. Puede ver cómo el ajuste del umbral de puntuación del modelo afecta a sus tasas de positivos verdaderos y falsos positivos.

 Note

El gráfico de distribución de puntuaciones muestra el fraude y los eventos legítimos en dos ejes Y diferentes. El eje Y izquierdo representa los eventos legítimos y el eje Y derecho representa los eventos de fraude.

2. Revise la matriz de confusión. Según el umbral de puntuación del modelo seleccionado, puede ver el impacto simulado en función de una muestra de 100 000 eventos. La distribución del fraude y de los eventos legítimos simula la tasa de fraude en sus empresas. Utilice esta información para encontrar el equilibrio adecuado entre la tasa de positivos verdaderos y la tasa de falsos positivos.
3. Para obtener más información, selecciona Métricas avanzadas. Utilice la gráfica ROC para comprender la relación entre la tasa de positivos verdaderos y la tasa de falsos positivos

para cualquier umbral de puntuación del modelo. La curva ROC puede ayudarlo a ajustar la compensación entre la tasa de positivos verdaderos y la tasa de falsos positivos.

#### Note

También puede revisar las métricas en forma de tabla seleccionando Tabla. La vista de tabla también muestra la precisión métrica. La precisión es el porcentaje de eventos de fraude predichos correctamente como fraudulentos en comparación con todos los eventos pronosticados como fraudulentos.

4. Utilice las métricas de rendimiento para determinar los umbrales de modelo óptimos para sus empresas en función de sus objetivos y del caso de uso de la detección del fraude. Por ejemplo, si piensa utilizar el modelo para clasificar los registros de nuevas cuentas como de riesgo alto, medio o bajo, necesitará identificar dos umbrales para poder redactar las tres condiciones reglamentarias siguientes:
  - Las puntuaciones  $> X$  representan un riesgo alto
  - Las puntuaciones  $< X$  but  $> Y$  son de riesgo medio
  - Las puntuaciones  $< Y$  son de bajo riesgo

## Importancia de la variable del modelo

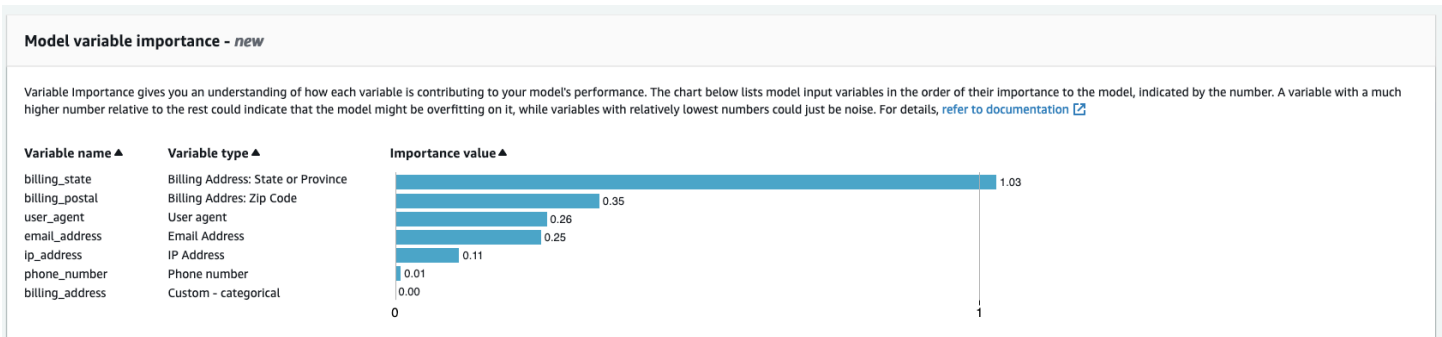
La importancia de las variables del modelo es una función de Amazon Fraud Detector que clasifica las variables del modelo dentro de una versión del modelo. A cada variable del modelo se le proporciona un valor en función de su importancia relativa para el rendimiento general del modelo. La variable de modelo con el valor más alto es más importante para el modelo que las demás variables del conjunto de datos de esa versión del modelo y, de forma predeterminada, aparece en la parte superior. Del mismo modo, la variable de modelo con el valor más bajo aparece en la parte inferior de forma predeterminada y es la menos importante en comparación con las demás variables del modelo. Al utilizar los valores de importancia de las variables del modelo, puede obtener información sobre las entradas que impulsan el rendimiento del modelo.

Puede ver los valores de importancia de las variables del modelo para su versión de modelo entrenada en la consola de Amazon Fraud Detector o mediante la [DescribeModelVersionAPI](#).

La importancia de las variables del modelo proporciona el siguiente conjunto de valores para cada [variable](#) utilizada para entrenar la [versión del modelo](#).

- **Tipo de variable:** tipo de variable (por ejemplo, dirección IP o correo electrónico). Para más información, consulte [Tipos de variables](#). Para los modelos Account Takeover Insights (ATI), Amazon Fraud Detector proporciona un valor de importancia variable tanto para el tipo de variable bruta como para el agregado. Los tipos de variables sin procesar se asignan a las variables que usted proporciona. El tipo de variable agregada se asigna a un conjunto de variables sin procesar que Amazon Fraud Detector ha combinado para calcular un valor de importancia agregado.
- **Nombre de variable:** nombre de la variable de evento que se utilizó para entrenar la versión del modelo (por ejemplo, `ip_address`, `email_address`, `are_credentials_valid`). Para el tipo de variable agregada, se muestran los nombres de todas las variables que se utilizaron para calcular el valor de importancia de la variable agregada.
- **Valor de importancia variable:** número que representa la importancia relativa de la variable bruta o agregada en relación con el rendimiento del modelo. Rango típico: 0—10

En la consola de Amazon Fraud Detector, los valores de importancia de las variables del modelo se muestran de la siguiente manera para un modelo Online Fraud Insights (OFI) o Transaction Fraud Insights (TFI). Un modelo Account Takeover Insight (ATI) proporcionará valores de importancia de variables agregados además de los valores de importancia de la variable bruta. El gráfico visual permite ver fácilmente la importancia relativa entre las variables, ya que la línea punteada vertical hace referencia al valor de importancia de la variable mejor clasificada.



Amazon Fraud Detector genera valores de importancia variables para cada versión del modelo de Fraud Detector sin coste adicional.

### ⚠ Important

Las versiones del modelo que se crearon antes del 9 de julio de 2021 no tienen valores de importancia variables. Debe entrenar una nueva versión del modelo para generar los valores de importancia de las variables del modelo.

## Uso de valores de importancia de las variables del modelo

Puede utilizar los valores de importancia de las variables del modelo para obtener información sobre qué es lo que impulsa o reduce el rendimiento de su modelo y cuáles son las variables que más contribuyen. Y, a continuación, modifique el modelo para mejorar el rendimiento general.

Más específicamente, para mejorar el rendimiento de su modelo, examine los valores de importancia de las variables comparándolos con los conocimientos de su dominio y depure los problemas en los datos de entrenamiento. Por ejemplo, si el identificador de cuenta se utilizó como entrada para el modelo y aparece en la parte superior, observe su valor de importancia variable. Si el valor de importancia de la variable es significativamente más alto que el resto de los valores, es posible que el modelo se ajuste demasiado a un patrón de fraude específico (por ejemplo, todos los casos de fraude se deben al mismo identificador de cuenta). Sin embargo, también puede darse el caso de que se filtre la etiqueta si la variable depende de las etiquetas de fraude. En función del resultado del análisis basado en el conocimiento del dominio, es posible que desee eliminar la variable y entrenarla con un conjunto de datos más diverso, o mantener el modelo tal como está.

Del mismo modo, eche un vistazo a las variables clasificadas en último lugar. Si el valor de importancia de la variable es significativamente inferior al resto de los valores, es posible que esta variable del modelo no tenga ninguna importancia a la hora de entrenar el modelo. Podría considerar la posibilidad de eliminar la variable para entrenar una versión del modelo más sencilla. Si su modelo tiene pocas variables (por ejemplo, solo dos variables), Amazon Fraud Detector seguirá proporcionando los valores de importancia de las variables y clasificándolas. Sin embargo, la información en este caso será limitada.

### Important

1. Si observa que faltan variables en el gráfico de importancia de las variables del modelo, es posible que se deba a una de las siguientes razones. Considere la posibilidad de modificar la variable en su conjunto de datos y volver a entrenar el modelo.
  - El recuento de valores únicos de la variable en el conjunto de datos de entrenamiento es inferior a 100.
  - Faltan más del 0,9 de los valores de la variable en el conjunto de datos de entrenamiento.
2. Debe entrenar una nueva versión del modelo cada vez que desee ajustar las variables de entrada del modelo.

## Evaluar los valores de importancia de las variables del modelo

Se recomienda tener en cuenta lo siguiente al evaluar los valores de importancia de las variables del modelo:

- Los valores de importancia de las variables siempre deben evaluarse en combinación con el conocimiento del dominio.
- Examine el valor de importancia variable de una variable en relación con el valor de importancia variable de las demás variables de la versión del modelo. No considere el valor de importancia de una variable individual de forma independiente.
- Compare los valores de importancia variable de las variables de la misma versión del modelo. No compare los valores de importancia variable de las mismas variables entre las distintas versiones del modelo, ya que el valor de importancia variable de una variable en una versión del modelo puede diferir del valor de la misma variable en una versión de modelo diferente. Si utiliza las mismas variables y el mismo conjunto de datos para entrenar diferentes versiones del modelo, esto no genera necesariamente los mismos valores de importancia de las variables.

## Ver la clasificación de importancia de las variables del modelo

Una vez finalizada la capacitación sobre modelos, puede ver la clasificación de importancia de las variables del modelo de su versión entrenada en la consola de Amazon Fraud Detector o mediante la [DescribeModelVersionAPI](#).

Para ver la clasificación de importancia de las variables del modelo mediante la consola,

1. Abre la AWS consola e inicia sesión en tu cuenta. Dirígete a Amazon Fraud Detector.
2. En el panel de navegación izquierdo, elija Models (Modelos).
3. Elige tu modelo y, a continuación, la versión del modelo.
4. Asegúrese de que la pestaña Descripción general esté seleccionada.
5. Desplácese hacia abajo para ver el panel de importancia de las variables del modelo.

## Comprender cómo se calcula el valor de importancia de la variable del modelo

Al finalizar la formación de cada versión del modelo, Amazon Fraud Detector genera automáticamente valores de importancia de las variables del modelo y métricas de rendimiento

del modelo. Para ello, Amazon Fraud Detector utiliza Shapley Additive Explanations ([SHAP](#)). Básicamente, el SHAP es la contribución media esperada de una variable del modelo una vez consideradas todas las combinaciones posibles de todas las variables del modelo.

En primer lugar, el SHAP asigna la contribución de cada variable del modelo a la predicción de un evento. Luego, agrega estas predicciones para crear una clasificación de las variables a nivel de modelo. Para asignar las contribuciones de cada variable del modelo a una predicción, SHAP considera las diferencias en los resultados del modelo entre todas las combinaciones de variables posibles. Al incluir todas las posibilidades de incluir o eliminar un conjunto específico de variables para generar un resultado del modelo, SHAP puede acceder con precisión a la importancia de cada variable del modelo. Esto es particularmente importante cuando las variables del modelo están altamente correlacionadas entre sí.

Los modelos ML, en la mayoría de los casos, no permiten eliminar variables. En su lugar, puede reemplazar una variable eliminada o faltante en el modelo por los valores de variable correspondientes de una o más líneas base (por ejemplo, eventos no fraudulentos). Elegir las instancias de referencia adecuadas puede resultar difícil, pero Amazon Fraud Detector te lo facilita al establecer esta línea de base como el promedio de la población.

## Importa un SageMaker modelo

Si lo desea, puede importar modelos SageMaker alojados a Amazon Fraud Detector. Al igual que los modelos, SageMaker los modelos se pueden añadir a los detectores y generar predicciones de fraude mediante la `GetEventPrediction` API. Como parte de la `GetEventPrediction` solicitud, Amazon Fraud Detector invocará tu SageMaker punto de conexión y transferirá los resultados a tus reglas.

Puede configurar Amazon Fraud Detector para que utilice las variables de evento enviadas como parte de la `GetEventPrediction` solicitud. Si decide utilizar variables de evento, debe proporcionar una plantilla de entrada. Amazon Fraud Detector utilizará esta plantilla para transformar las variables de tus eventos en la carga útil de entrada necesaria para invocar el SageMaker punto final. Como alternativa, puede configurar su SageMaker modelo para que utilice un `ByteBuffer` que se envía como parte de la solicitud. `GetEventPrediction`

Amazon Fraud Detector admite la importación de SageMaker algoritmos que utilizan formatos de entrada JSON o CSV y formatos de salida JSON o CSV. Algunos ejemplos de SageMaker algoritmos compatibles son XGBoost, Linear Learner y Random Cut Forest.



## Importe un modelo mediante el SageMaker AWS SDK for Python (Boto3)

Para importar un SageMaker modelo, utilice la `PutExternalModel` API. En el siguiente ejemplo, se supone que el SageMaker punto final `sagemaker-transaction-model` ha implementado, se encuentra en `InService` estado y utiliza el algoritmo `XGBoost`.

La configuración de entrada especifica que se utilizarán las variables de evento para construir la entrada del modelo (`useEventVariables` establece en `True`). El formato de entrada es `TEXT_CSV`, dado que `XGBoost` requiere una entrada CSV. `csvInputTemplate` Especifica cómo construir la entrada CSV a partir de las variables enviadas como parte de la solicitud. `GetEventPrediction` En este ejemplo se supone que ha creado las variables `order_amt`, `prev_amt`, `hist_amt` y `payment_type`.

La configuración de salida especifica el formato de respuesta del SageMaker modelo y asigna el índice CSV correspondiente a la variable `Amazon Fraud Detectorsagemaker_output_score`. Una vez configurada, puede utilizar la variable de salida en las reglas.

### Note

La salida de un SageMaker modelo debe asignarse a una variable con origen `EXTERNAL_MODEL_SCORE`. No puede crear estas variables en la consola mediante `Variables`. En su lugar, debe crearlas al configurar la importación del modelo.

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

fraudDetector.put_external_model (
    modelSource = 'SAGEMAKER',
    modelEndpoint = 'sagemaker-transaction-model',
    invokeModelEndpointRoleArn = 'your_SagemakerExecutionRole_arn',
    inputConfiguration = {
        'useEventVariables' : True,
        'eventName' : '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'  
)
```

## Eliminar un modelo o versión de modelo

Se pueden eliminar modelos y versiones de modelo en Amazon Fraud Detector siempre que no estén asociados a una versión del detector. Al eliminar un modelo, Amazon Fraud Detector elimina ese modelo de forma permanente y los datos ya no se almacenan en Amazon Fraud Detector.

También puede eliminar SageMaker modelos de Amazon si no están asociados a una versión de detector. Al eliminar un SageMaker modelo, se desconecta de Amazon Fraud Detector, pero el modelo permanece disponible en SageMaker.

Para eliminar una versión de modelo

Solo puede eliminar las versiones del modelo que estén en elReady to deploy estado. Para cambiar elReady to deploy estado de una versión del modelo,ACTIVE anule la implementación de la versión del modelo.

1. Inicie sesión enAWS Management Console y abra la consola de Amazon Fraud Detector en <https://console.aws.amazon.com/frauddetector>.
2. En el panel de navegación izquierdo de la consola de Amazon Fraud Detector, seleccione Modelos.
3. Elija el modelo que contiene la versión del modelo que desea eliminar.
4. Elija la versión del modelo que desea eliminar.
5. Elija Actions (Acciones) y, a continuación, elija Delete (Eliminar).
6. Introduzca el nombre de la versión del modelo y, a continuación, seleccione Eliminar versión del modelo.

Para anular una versión de modelo

No puede anular la implementación de una versión del modelo que esté siendo utilizada por cualquier versión del detector (ACTIVE,INACTIVE,DRAFT). Por lo tanto, para anular la

implementación de una versión de modelo que está siendo utilizada por una versión de detector, primero elimine la versión del modelo de la versión del detector.

1. En el panel de navegación izquierdo de la consola de Amazon Fraud Detector, seleccione Modelos.
2. Elija el modelo que contenga la versión del modelo que desea anular la implementación.
3. Elija la versión del modelo que desea eliminar.
4. Elija Acciones y, a continuación, elija Undeploy model version.

#### Para eliminar un modelo

Antes de eliminar un modelo, primero debe eliminar todas las versiones del modelo y están asociadas al modelo.

1. En el panel de navegación izquierdo de la consola de Amazon Fraud Detector, seleccione Modelos.
2. Elija el modelo que desea eliminar.
3. Elija Actions (Acciones) y, a continuación, elija Delete (Eliminar).
4. Introduzca el nombre del modelo y, a continuación, seleccione Eliminar modelo.

#### Para eliminar un SageMaker modelo de Amazon

1. En el panel de navegación izquierdo de la consola de Amazon Fraud Detector, seleccione Modelos.
2. Elija el SageMaker modelo que desea eliminar.
3. Elija Acciones y, a continuación, elija Eliminar modelo.
4. Introduzca el nombre del modelo y, a continuación, seleccione Eliminar SageMaker modelo.

# Detector

Un detector es un contenedor que contiene la lógica de detección de fraudes, como los modelos y las reglas, para un evento empresarial específico que se desea evaluar para determinar si se trata de un fraude. Primero, cree un detector especificando el evento que ya ha definido y, si lo desea, añada una versión del modelo que Amazon Fraud Detector ya haya creado y entrenado para el evento.

A continuación, agrega reglas y orden de ejecución de reglas a un detector para crear una versión del detector. Una versión del detector define las reglas y, opcionalmente, un modelo que se ejecutará como parte de la solicitud para generar predicciones de fraude. Puede añadir cualquiera de las reglas definidas en un detector a la versión del detector. También puede agregar cualquier modelo entrenado en el tipo de evento evaluado a la versión del detector. Un detector puede tener varias versiones, y cada versión tiene reglas y un orden de ejecución de reglas diferentes para cumplir con varios casos de uso.

Cada versión del detector debe tener un estado de `DRAFT`, `ACTIVE`, o `INACTIVE`. Solo puede haber una versión de detector `ACTIVE` estado a la vez. Amazon Fraud Detector utiliza la versión de detector con `ACTIVE` estado para generar predicciones de fraude.

## Crear un detector

Para crear un detector, especifique el tipo de evento que ya ha definido. Si lo desea, puede añadir un modelo que Amazon Fraud Detector ya haya entrenado e implementado. Si añade un modelo, puede utilizar la puntuación del modelo generada por Amazon Fraud Detector en la expresión de la regla al crear una regla (por ejemplo, `$model score < 90`).

Puede crear un detector en la consola de Amazon Fraud Detector mediante la [PutDetector](#) API, mediante el [detector de entrada](#) comando, o mediante el AWS SDK. Si utiliza la API, el comando o el SDK para crear un detector, una vez creado el detector, siga las instrucciones para [Crear una versión de detector](#).

## Cree un detector en la consola de Amazon Fraud Detector

En este ejemplo se supone que ha creado un tipo de evento y que también ha creado e implementado una versión de modelo que desea utilizar para la predicción del fraude.

### Paso 1: Construir el detector

1. En el panel de navegación izquierdo de la consola de Amazon Fraud Detector, elija `Detectors`.

2. Elige Crear detector.
3. En el Definir los detalles del detector página, introduce `sample_detector` para el nombre del detector. Si lo desea, introduzca una descripción para el detector, como `sample fraud detector`.
4. Para Tipo de evento, seleccione el tipo de evento que ha creado para la predicción de fraudes.
5. Elija Siguiente.

## Paso 2: Agregar una versión del modelo implementado

1. Tenga en cuenta que este es un paso opcional. No necesita añadir un modelo a su detector. Para omitir este paso, elija Next (Siguiente).
2. En el Añadir modelo (opcional), elige Añadir modelo.
3. En el Añadir modelo página, para Selecciona modelo, elija el nombre del modelo de Amazon Fraud Detector que implementó anteriormente. Para Seleccione la versión, elija la versión del modelo implementado.
4. Elija Add model (Añadir modelo).
5. Elija Siguiente.

## Paso 3: Añadir reglas

Una regla es una condición que indica a Amazon Fraud Detector cómo interpretar los valores de las variables al evaluar la predicción del fraude. En este ejemplo se crearán tres reglas utilizando las puntuaciones del modelo como valores variables: `high_fraud_risk`, `medium_fraud_risk`, y `low_fraud_risk`. Para crear sus propias reglas, expresiones de reglas, orden de ejecución de reglas y resultados, utilice valores que sean adecuados para su modelo y su caso de uso.

1. En el Añadir reglas página, en Definir una regla, introduce `high_fraud_risk` para el nombre de la regla y debajo Descripción: opcional, introduce **This rule captures events with a high ML model score** como descripción de la regla.
2. En Expresión, introduzca la siguiente expresión de regla mediante el lenguaje de expresiones de reglas simplificado de Amazon Fraud Detector:  

```
$sample_fraud_detection_model_insightscore > 900
```
3. En Resultados, elige Crea un nuevo resultado. Un resultado es el resultado de una predicción de fraude y se devuelve si la regla coincide durante una evaluación.

4. En Crea un nuevo resultado, introduce `verify_customer` como nombre del resultado. Si lo desea, introduzca una descripción.
5. Elige Guardar resultado.
6. Elige Agregar regla para ejecutar el comprobador de validación de reglas y guardar la regla. Una vez creada, Amazon Fraud Detector hace que la regla esté disponible para su uso en su detector.
7. Elige Añadir otra regla, a continuación, elija la Crear regla pestaña.
8. Repite este proceso dos veces más para crear `medium_fraud_risk` y `low_fraud_risk` reglas utilizando los siguientes detalles de la regla:

- riesgo de fraude medio

Nombre de la regla: `medium_fraud_risk`

Resultado: `review`

Expresión:

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

```
$sample_fraud_detection_model_insightscore > 700
```

- bajo riesgo de fraude

Nombre de la regla: `low_fraud_risk`

Resultado: `approve`

Expresión:

```
$sample_fraud_detection_model_insightscore <= 700
```

9. Una vez que haya creado todas las reglas para su caso de uso, elija Siguiente.

Para obtener más información sobre cómo crear y escribir reglas, consulte [Reglas](#) y [Referencia al lenguaje de las reglas](#).

## Paso 4: Configurar la ejecución y el orden de las reglas

El modo de ejecución de reglas de las reglas que se incluyen en el detector determina si se evalúan todas las reglas que defina o si la evaluación de las reglas se detiene en la primera regla coincidente. Y el orden de las reglas determina el orden en el que desea que se ejecute la regla.

El modo de ejecución de reglas predeterminado es `FIRST_MATCHED`.

### Primer emparejado

El modo de ejecución de la primera regla coincidente devuelve los resultados de la primera regla coincidente en función del orden de reglas definido. Si especifica `FIRST_MATCHED`, Amazon Fraud Detector evalúa las reglas secuencialmente, de la primera a la última, y se detiene en la primera regla que coincida. A continuación, Amazon Fraud Detector proporciona los resultados de esa única regla.

El orden en el que se ejecutan las reglas puede afectar al resultado de la predicción de fraudes resultante. Después de crear las reglas, reordene las reglas para ejecutarlas en el orden deseado siguiendo estos pasos:

Si `tuhigh_fraud_risk` la regla aún no está en la parte superior de tu lista de reglas, elige `Pedidoy`, a continuación, elija `1`. Esto se mueve `tuhigh_fraud_risk` a la primera posición.

Repita este proceso para que `sumedium_fraud_risk` la regla está en la segunda posición y `tu_low_fraud_risk` la regla está en la tercera posición.

### Todos coincidentes

El modo de ejecución de todas las reglas coincidentes devuelve los resultados de todas las reglas coincidentes, independientemente del orden de las reglas. Si especificas `ALL_MATCHED`, Amazon Fraud Detector evalúa todas las reglas y devuelve los resultados de todas las reglas coincidentes.

Seleccione `FIRST_MATCHED` para este tutorial y, a continuación, elija `Siguiente`.

## Paso 5: Revisar y crear la versión del detector

Una versión de detector define los modelos y reglas específicos que se utilizan para generar predicciones de fraude.

1. En `elRevisar y crear` página, revise los detalles del detector, los modelos y las reglas que configuró. Si necesita realizar algún cambio, elija `Editar` junto a la sección correspondiente.

2. Elige `Crear detector`. Una vez creado, la primera versión del detector aparece en la tabla de versiones del detector con `Draft` estado.

Usas el `Borrar versión` para probar su detector.

## Cree un detector mediante el AWS SDK for Python (Boto3)

El siguiente ejemplo muestra un ejemplo de solicitud para `PutDetectorAPI`. Un detector actúa como contenedor para sus versiones de detectores. El `PutDetector` API especifica qué tipo de evento evaluará el detector. En el siguiente ejemplo, se supone que ha creado un tipo de eventos `sample_registration`.

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

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

## Crear una versión de detector

Una versión del detector define las reglas, el orden de ejecución de las reglas y, opcionalmente, una versión del modelo, que se utilizará como parte de la solicitud para generar predicciones de fraude. Puede añadir cualquiera de las reglas definidas en un detector a la versión del detector. También puede añadir cualquier modelo entrenado en el tipo de evento evaluado.

Cada versión del detector tiene un estado de `DRAFT`, `ACTIVE`, o `INACTIVE`. Solo puede haber una versión de detector `ACTIVE` estado a la vez. Durante el `GetEventPredictions` solicitud, Amazon Fraud Detector utilizará el `ACTIVE` detector si no `DetectorVersion` está especificado.

## Modo de ejecución de reglas

Amazon Fraud Detector admite dos modos de ejecución de reglas diferentes: `FIRST_MATCHED` y `ALL_MATCHED`.

- Si el modo de ejecución de la regla es `FIRST_MATCHED`, Amazon Fraud Detector evalúa las reglas de forma secuencial, de la primera a la última, y se detiene en la primera regla coincidente. A



continuación, Amazon Fraud Detector proporciona los resultados de esa única regla. Si una regla da como resultado falsa (no coincide), se evalúa la siguiente regla de la lista.

- Si el modo de ejecución de la regla es `ALL_MATCHED`, entonces todas las reglas de una evaluación se ejecutan en paralelo, independientemente de su orden. Amazon Fraud Detector ejecuta todas las reglas y devuelve los resultados definidos para cada regla coincidente.

## Cree una versión de detector mediante elAWS SDK for Python (Boto3)

El siguiente ejemplo muestra un ejemplo de solicitud para `CreateDetectorVersionAPI`. El modo de ejecución de la regla se establece en `FIRST_MATCHED`, por lo tanto, Amazon Fraud Detector evaluará las reglas de forma secuencial, de la primera a la última, deteniéndose en la primera regla coincidente. A continuación, Amazon Fraud Detector proporciona los resultados de esa única regla durante el `GetEventPrediction` response.

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

fraudDetector.create_detector_version(
    detectorId = 'sample_detector',
    rules = [{
        'detectorId' : 'sample_detector',
        'ruleId' : 'high_fraud_risk',
        'ruleVersion' : '1'
    },
    {
        'detectorId' : 'sample_detector',
        'ruleId' : 'medium_fraud_risk',
        'ruleVersion' : '1'
    },
    {
        'detectorId' : 'sample_detector',
        'ruleId' : 'low_fraud_risk',
        'ruleVersion' : '1'
    }
    ],
    modelVersions = [{
        'modelId' : 'sample_fraud_detection_model',
        'modelType': 'ONLINE_FRAUD_INSIGHTS',
        'modelVersionNumber' : '1.00'
    }],
    ruleExecutionMode = 'FIRST_MATCHED'
```

)

Para actualizar el estado de una versión del detector, utilice la `UpdateDetectorVersionStatusAPI`. El siguiente ejemplo actualiza el estado de la versión del detector desde `DRAFT` a `ACTIVE`. Durante un `GetEventPredictions` solicitud, si no se especifica un identificador de detector, Amazon Fraud Detector utilizará el `ACTIVE` versión del detector.

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

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

## Eliminar un detector, una versión del detector o una versión de regla

Antes de eliminar un detector en Amazon Fraud Detector, primero debe eliminar todas las versiones del detector y las versiones de reglas asociadas al detector.

Al eliminar un detector, una versión del detector o una versión de regla, Amazon Fraud Detector elimina permanentemente ese recurso y los datos ya no se almacenan en Amazon Fraud Detector.

Para eliminar una versión del detector

Solo se pueden eliminar versiones del detector que estén en `DRAFT` o en `INACTIVE` estado.

1. Inicie sesión en `AWS Management Console` y abra la consola de Amazon Fraud Detector en <https://console.aws.amazon.com/frauddetector>.
2. En el panel de navegación izquierdo de la consola de Amazon Fraud Detector, elija `Detectors`.
3. Elija el detector que contenga la versión del detector que desea eliminar.
4. Elija la versión del detector que desea eliminar.
5. Elija `Actions (Acciones)` y, a continuación, elija `Delete (Eliminar)`.
6. Introduzca `ydelete`, a continuación, seleccione `Eliminar detector`.

## Para eliminar una versión de regla

Puede eliminar una versión de regla solo si no la usa ninguna **ACTIVE** de las versiones del **INACTIVE** detector. Si es necesario, antes de eliminar una versión de regla, mueva primero la versión del **ACTIVE** detector a **INACTIVE**, a continuación, elimine la versión del **INACTIVE** detector.

1. En el panel de navegación izquierdo de la consola de Amazon Fraud Detector, elija **Detectors**.
2. Elija el detector que contiene la versión de regla que desea eliminar.
3. Elija la pestaña **Reglas asociadas** y elija la regla que desea eliminar.
4. Elija la versión de regla que desea eliminar.
5. Elija **Acciones** y, a continuación, elija **Eliminar versión de la regla**.
6. Introduzca **delete**, a continuación, seleccione **Eliminar versión**.

## Para eliminar un detector

Antes de eliminar un detector, primero debe eliminar todas las versiones del detector y las versiones de reglas asociadas al detector.

1. En el panel de navegación izquierdo de la consola de Amazon Fraud Detector, elija **Detectors**.
2. Elija el detector que desea eliminar.
3. Elija **Acciones** y, a continuación, elija **Eliminar detector**.
4. Introduzca **delete**, a continuación, seleccione **Eliminar detector**.

# Recursos

Los modelos, las reglas y los detectores utilizan recursos como variables, resultados, etiquetas, listas y entidades para evaluar los eventos y detectar el riesgo de fraude. En esta sección, se proporciona información acerca de cómo crean y se administran las fuentes.

## Temas

- [Variables](#)
- [Etiquetas](#)
- [Reglas](#)
- [Lists](#)
- [Resultados](#)
- [Entidad](#)
- [Gestione los recursos de Amazon Fraud Detector mediante AWS CloudFormation](#)

# Variables

Las variables representan los elementos de datos que desea utilizar en una predicción de fraude. Estas variables se pueden extraer del conjunto de datos de eventos que preparó para entrenar su modelo, de los resultados de la puntuación de riesgo de su modelo de Amazon Fraud Detector o de SageMaker los modelos de Amazon. Para obtener más información sobre las variables tomadas del conjunto de datos de eventos, consulte [Obtenga los requisitos del conjunto de datos de eventos mediante el explorador de modelos de datos](#).

Las variables que desee utilizar en su predicción de fraude deben crearse primero y, a continuación, agregarse al evento al crear su tipo de evento. A cada variable que cree se le debe asignar un tipo de datos, un valor predeterminado y, opcionalmente, un tipo de variable. Amazon Fraud Detector enriquece algunas de las variables que usted proporciona, como las direcciones IP, los números de identificación bancaria (BIN) y los números de teléfono, para crear entradas adicionales y mejorar el rendimiento de los modelos que utilizan estas variables.

## Tipos de datos

Las variables deben tener un tipo de datos para el elemento de datos que representa la variable y, opcionalmente, se les puede asignar uno de los predefinidos [Tipos de variables](#). Para las variables

asignadas a un tipo de variable, el tipo de datos está preseleccionado. Los tipos de datos posibles incluyen los siguientes tipos:

Tipo de datos	Descripción	Valor predeterminado	Valores de ejemplo
Cadena	Cualquier combinación de letras, números enteros o ambos	<empty>	abc, 123, 1D3B
Entero	Números enteros positivos o negativos	0	1, -1
Booleano	Verdadero o falso	False	Verdadero, falso
DateTime	Fecha y hora especificadas únicamente en el formato UTC de la norma ISO 8601	<empty>	2019-11-30T 13:01:01 Z
Float	Números con puntos decimales	0.0	4,01, 0,10

## Valor predeterminado

Las variables deben tener un valor predeterminado. Cuando Amazon Fraud Detector genera predicciones de fraude, este valor predeterminado se utiliza para ejecutar una regla o un modelo si Amazon Fraud Detector no recibe un valor para una variable. Los valores predeterminados que proporcione deben coincidir con el tipo de datos seleccionado. En la consola de AWS, Amazon Fraud Detector asigna el valor predeterminado `0` para números enteros, `false` booleanos, flotantes y (vacío) `0.0` para cadenas. Puede establecer un valor predeterminado personalizado para cualquiera de estos tipos de datos.

## Tipos de variables

Al crear una variable, puede asignarla opcionalmente a un tipo de variable. El tipo de variable representa los elementos de datos comunes que se utilizan para entrenar modelos y generar predicciones de fraude. Solo se pueden usar variables con un tipo de variable asociado para el

entrenamiento del modelo. Como parte del proceso de entrenamiento del modelo, Amazon Fraud Detector utiliza el tipo de variable asociado a la variable para realizar el enriquecimiento de las variables, la ingeniería de funciones y la puntuación del riesgo.

Amazon Fraud Detector ha predefinido los siguientes tipos de variables que se pueden utilizar para asignarlos a sus variables.

Categoría	Tipo de variable	Descripción	Tipo de dato	Ejemplo
Sesión (Sesión)	IP_ADDRESS	La dirección IP que se recopila durante el evento	Cadente	192.0.2.0  Nota: Amazon Fraud Detector enriquece estos datos. Para obtener más información, consulte <a href="#">Enriquecimiento de geolocalización</a>
	AGENTE DE USUARIO	El agente de usuario que se recopila durante el evento	Cadente	Mozilla 5.0 (Windows NT 10.0, Win64,

Categoría	Tipo variable	Descripción	Tipo de dato	Ejemplo
				x64, rv:68.0) Gecko 20100101
	HUELLA DACTILAR	El identificador único del dispositivo utilizado para el evento	Cad	sadfow987 u234
	SESSION_ID	El identificador de sesión de la sesión activa del evento	Cad	sid123456 789
	SON_ACREDITACIONES_VALIDAS	Indica si las credenciales utilizadas para el inicio de sesión en el evento son válidas	Bool	True
Usuarios	DIRECCIÓN_DE_CORREO	La dirección de correo electrónico que se recopila durante el evento	Cad	abc@domai n.com

Categoría	Tipo de variable	Descripción	Tipo de dato	Ejemplo
	PHONE_NUMBER	El número de teléfono obtenido durante el evento	Cadena	+1 555-0100  Nota: Amazon Fraud Detector enriquece estos datos. Para obtener más información, consulte <a href="#">Enriquecimiento de números de teléfono</a>
Facturación	NOMBRE_FACTURACIÓN	El nombre asociado a la dirección de facturación	Cadena	John Doe



Categoría	Tipo variable	Descripción	Tipo de dato	Ejemplo
	TELÉFONO DE_FACTURACIÓN	El número de teléfono asociado a la dirección de facturación	Cad	+1 555-0100  Nota: Amazon Fraud Detector enriquece estos datos. Para obtener más información, consulte <a href="#">Enriquecimiento de números de teléfono</a>
	DIRECCIÓN_DE_FACTURACIÓN_L1	La primera línea de la dirección de facturación	Cad	Cualquier calle
	DIRECCIÓN_DE_FACTURACIÓN_L2	La segunda línea de la dirección de facturación	Cad	Cualquier unidad 123

Categoría	Tipo variable	Descripción	Tipo de dato	Ejemplos
	BILLING_CITY	La ciudad que aparece en la dirección de facturación	Categoría	Cualquier ciudad
	ESTADO_DIRECCIÓN_FACTURACIÓN	El estado o la provincia que aparece en la dirección de facturación	Categoría	Cualquier estado o provincia
	PAÍS DE FACTURACIÓN	El país que aparece en la dirección de facturación	Categoría	Cualquier país  Nota: Amazon Fraud Detector enriquece estos datos. Para obtener más información, consulte <a href="#">Enriquecimiento de geolocalización</a>

Categoría	Tipo de variable	Descripción	Tipo de dato	Ejemplo
	ZIP DE FACTURACIÓN	El código postal que aparece en la dirección de facturación	Cadena	01234  Nota: Amazon Fraud Detector enriquece estos datos. Para obtener más información, consulte <a href="#">Enriquecimiento de geolocalización</a>
Envío	NOMBRE_DEL_ENVÍO	El nombre asociado a la dirección de envío	Cadena	John Doe

Categoría	Tipo variable	Descripción	Tipo de dato	Ejemplo
	TELÉFONO DE_ENVÍO	El número de teléfono asociado a la dirección de envío	Cad	+1 555-0100  Nota: Amazon Fraud Detector enriquece estos datos. Para obtener más información, consulte <a href="#">Enriquecimiento de números de teléfono</a>
	DIRECCIÓN_DE_ENVÍO_L1	La primera línea de la dirección de envío	Cad	Cualquier Calle 123
	DIRECCIÓN_DE_ENVÍO_L2	La segunda línea de la dirección de envío	Cad	Unidad 123

Categoría	Tipo de variable	Descripción	Tipo de dato	Ejemplos
	CIUDAD_DE_ENVÍO	La ciudad que aparece en la dirección de envío	Categoría	Cualquier ciudad
	ESTADO_DE_ENVÍO	El estado o la provincia que aparece en la dirección de envío	Categoría	Cualquier estado
	PAÍS_DE_ENVÍO	El país en el que se encuentra la dirección de envío	Categoría	<p>Cualquier país</p> <p>Nota: Amazon Fraud Detector enriquece estos datos. Para obtener más información, consulte <a href="#">Enriquecimiento de geolocalización</a></p>

Categoría	Tipo variable	Descripción	Tipo de dato	Ejemplo
	SHIPPING_ZIP	El código postal que aparece en la dirección de envío	Cad	01234  Nota: Amazon Fraud Detector enriquece estos datos. Para obtener más información, consulte <a href="#">Enriquecimiento de geolocalización</a>
Pagos	IDENTIFICADOR DEL PEDIDO	El identificador único de la transacción	Cad	LUX60
	PRECIO	El precio total del pedido	Cad	560,00
	CÓDIGO_D VISA	El código de divisa ISO 4217	Cad	USD

Categoría	Tipo variable	Descripción	Tipo de dato	Ejemplo
	TIPO_DE_PAGO	El método de pago que se utiliza para el pago durante el evento	Cad	Tarjeta de crédito
	CÓDIGO DE AUTENTICACIÓN	El código alfanumérico que envía el emisor de la tarjeta de crédito o el banco emisor	Cad	0000
	AVS	El código de respuesta del sistema de verificación de direcciones (AVS) del procesador de la tarjeta	Cad	Y
Producto	CATEGORÍA_DE_PRODUCTO	La categoría de producto del artículo del pedido	Cad	Cocina
Período	NUMERICAL	Cualquier variable que pueda representarse como un número real	Floa	1.224

Categoría	Tipo de variable	Descripción	Tipo de dato	Ejemplo
	CATEGÓRICO	Cualquier variable que describa categorías, segmentos o grupos	Categoría	Grande
	TEXTOS_LIBRES	Cualquier texto en formato libre que se capture como parte del evento (por ejemplo, la opinión o el comentario de un cliente)	Categoría	Ejemplo de entrada de texto en formato libre

## Asignación de una variable a un tipo de variable

Si tiene previsto utilizar una variable para entrenar el modelo, es importante que elija el tipo de variable correcto para asignarlo a la variable. La asignación incorrecta del tipo de variable puede afectar negativamente al rendimiento del modelo. También puede resultar muy difícil cambiar la asignación más adelante, especialmente si varios modelos y eventos han utilizado la variable.


Puede asignar a la variable cualquiera de los tipos de variables predefinidos o uno de los tipos de variables personalizadas: `FREE_FORM_TEXT`, `CATEGORICAL`, o `NUMERIC`.

### Notas importantes para asignar variables a los tipos de variables correctos

1. Si la variable coincide con uno de los tipos de variables predefinidos, úsela. Asegúrese de que el tipo de variable se corresponde con la variable. Por ejemplo, si asigna una variable `ip_address` a un tipo de variable, la `EMAIL_ADDRESS` variable `ip_address` no se enriquecerá con enriquecimientos como ASN, ISP, geolocalización y puntuación de riesgo. Para obtener más información, consulte [Enriquecimientos variables](#).



2. Si la variable no coincide con ninguno de los tipos de variables predefinidos, siga las recomendaciones que se indican a continuación para asignar uno de los tipos de variables personalizados.
3. Asigne el tipo de CATEGORICAL variable a las variables que normalmente no tienen un orden natural y se pueden clasificar en categorías, segmentos o grupos. El conjunto de datos que utiliza para entrenar tu modelo puede tener variables de ID como `merchant_id`, `campaign_id` o `policy_id`. Estas variables representan grupos (por ejemplo, todos los clientes con el mismo `policy_id` representan un grupo). A las variables que tengan los siguientes datos se les debe asignar el tipo de variable CATEGÓRICA -
  - Variables que contienen datos como `Customer_ID`, `Segment_ID`, `Color_ID`, `department_code` o `product_ID`.
  - Variables que contienen datos booleanos con valores verdaderos, falsos o nulos.
  - Variables que se pueden clasificar en grupos o categorías, como el nombre de la empresa, la categoría de producto, el tipo de tarjeta o el medio de referencia.

 Note

ENTITY\_ID es un tipo de variable reservada que Amazon Fraud Detector utiliza para asignar a la variable ENTITY\_ID. La variable ENTITY\_ID es el ID de la entidad que inicia la acción que desea evaluar. Si va a crear un tipo de modelo de Transaction Fraud Insight (TFI), debe proporcionar la variable ENTITY\_ID. Deberá decidir qué variable de sus datos identifica de forma única a la entidad que inicia la acción y pasarla como variable ENTITY\_ID. Asigne el tipo de variable CATEGÓRICA a todos los demás ID de su conjunto de datos, si están presentes y si los está utilizando para el entrenamiento de modelos. Algunos ejemplos de otros identificadores que no son una entidad del conjunto de datos son `Merchant_ID`, `Policy_ID` y `Campaign_ID`.

4. Asigne el tipo de FREE\_FORM\_TEXT variable a las variables que contienen un bloque de texto. Algunos ejemplos de tipos de variables FREE\_FORM\_TEXT son las opiniones de los usuarios, los comentarios, las fechas y los códigos de referencia. Los datos FREE\_FORM\_TEXT contienen varios identificadores separados por un delimitador. Los delimitadores pueden ser cualquier carácter que no sea un símbolo alfanumérico y de subrayado. Por ejemplo, las opiniones y comentarios de los usuarios se pueden separar mediante un delimitador de «espacio», y las fechas y los códigos de referencia pueden utilizar guiones como delimitadores para separar el prefijo, el sufijo y las partes intermedias. Amazon Fraud Detector usa los delimitadores para extraer datos de las variables FREE\_FORM\_TEXT.

5. Asigne el tipo de variable NUMÉRICA a las variables que son números reales y tienen un orden inherente. Algunos ejemplos de variables NUMÉRICAS son `day_of_the_week`, `incident_severity` y `customer_rating`. Si bien puede asignar el tipo de variable CATEGÓRICA a estas variables, se recomienda encarecidamente asignar todas las variables de números reales con un orden inherente al tipo de variable NUMÉRICA.

## Enriquecimientos variables

Amazon Fraud Detector enriquece algunos de los elementos de datos sin procesar que usted proporciona, como las direcciones IP, los números de identificación bancaria (BIN) y los números de teléfono, para crear entradas adicionales y mejorar el rendimiento de los modelos que utilizan estos elementos de datos. El enriquecimiento ayuda a identificar situaciones potencialmente sospechosas y ayuda a los modelos a detectar más casos de fraude.

### Enriquecimiento de números de teléfono

Amazon Fraud Detector enriquece los datos del número de teléfono con información adicional relacionada con la geolocalización, el operador original y la validez del número de teléfono. El enriquecimiento de números de teléfono se habilita automáticamente para todas las modelos que se capaciten el 13 de diciembre de 2021 o después de esa fecha y que tengan un número de teléfono que incluya un código de país (+xxx). Si has incluido la variable de número de teléfono en tu modelo y la has entrenado antes del 13 de diciembre de 2021, vuelve a entrenar tu modelo para que pueda aprovechar este enriquecimiento.

Le recomendamos encarecidamente que utilice el siguiente formato para las variables de número de teléfono a fin de garantizar que los datos se enriquezcan correctamente.

Variable	Formato	Descripción
PHONE_NUMBER	La <a href="#">norma E.164</a>	Asegúrese de incluir el código de país (+xxx) con el número de teléfono.
BILLING_PHONE y SHIPPING_PHONE	La <a href="#">norma E.164</a>	Asegúrese de incluir el código de país (+xxx) con el número de teléfono.

## Enriquecimiento de geolocalización

A partir del 8 de febrero de 2022, Amazon Fraud Detector calculará la distancia física entre los valores IP\_ADDRESS, BILLING\_ZIP y SHIPPING\_ZIP que proporcionas para un evento. Las distancias calculadas se utilizan como entradas para su modelo de detección de fraudes.

Para habilitar el enriquecimiento por geolocalización, los datos del evento deben incluir al menos dos de las tres variables: IP\_ADDRESS, BILLING\_ZIP o SHIPPING\_ZIP. Además, cada valor de BILLING\_ZIP y SHIPPING\_ZIP debe tener un código BILLING\_COUNTRY y un código SHIPPING\_COUNTRY válidos, respectivamente. Si tiene un modelo que se entrenó antes del 8 de febrero de 2022 e incluye estas variables, debe volver a entrenar el modelo para habilitar el enriquecimiento de la geolocalización.

Si Amazon Fraud Detector no puede determinar la ubicación asociada a los valores IP\_ADDRESS, BILLING\_ZIP o SHIPPING\_ZIP de un evento debido a que los datos no son válidos, se utiliza un valor de marcador de posición especial en su lugar. Por ejemplo, supongamos que un evento tiene valores IP\_ADDRESS y BILLING\_ZIP válidos, pero el valor SHIPPING\_ZIP no lo es. En este caso, el enriquecimiento se realiza únicamente para IP\_ADDRESS—> BILLING\_ZIP. El enriquecimiento no está hecho para IP\_ADDRESS—>SHIPPING\_ZIP y BILLING\_ZIP—>SHIPPING\_ZIP. En cambio, los valores de los marcadores de posición se utilizan en su lugar. Independientemente de si el enriquecimiento por geolocalización está habilitado para su modelo o no, el rendimiento de su modelo no cambia.

Para excluirse del enriquecimiento por geolocalización, asigne sus variables BILLING\_ZIP y SHIPPING\_ZIP al tipo de variable CUSTOM\_CATEGORICAL. Cambiar el tipo de variable no afecta al rendimiento del modelo.

### Formato variable de geolocalización

Le recomendamos encarecidamente que utilice el siguiente formato para las variables de geolocalización a fin de garantizar que los datos de ubicación se enriquezcan correctamente.

Variable	Formato	Descripción
IP_ADDRESS	<a href="#">Dirección IPv4</a>	Por ejemplo, 1.1.1.1
BILLING_ZIP y SHIPPING_ZIP	El código postal <a href="#">ISO 3166-1 alpha-2</a> del país especificado	Para obtener más información, consulte la sección Códigos de

Variable	Formato	Descripción
		país y territorio de este tema.
BILLING_COUNTRY y SHIPPING_COUNTRY	El código de <a href="#">país estándar de dos letras ISO 3166-1 alpha-2</a>	Para obtener más información, consulte la sección Códigos de país y territorio de este tema. Amazon Fraud Detector intenta hacer coincidir todas las variaciones comunes del nombre de un país con su código de país estándar ISO 3166-1 de dos letras. Sin embargo, no podemos garantizar que coincidan correctamente.

## Códigos de país y territorio

La siguiente tabla proporciona una lista completa de los países y territorios que Amazon Fraud Detector admite para el enriquecimiento de la geolocalización. Cada país y territorio tiene un código de país asignado (específicamente, el código de país de dos letras ISO 3166-1 alfa-2) y un código postal.

### Formato de código postal

- 9 - número
- a - letra
- [X] - X es opcional. Por ejemplo, «GY9 [9] 9aa» de Guersney significa que tanto «GY9 9aa» como «GY99 9aa» son válidos. Usa un formato.
- [X/XX]: se puede utilizar X o XX. Por ejemplo, «aa [aa/99]» de Bermudas significa que tanto «aa aa» como «aa 99» son válidas. Utilice uno de estos formatos, pero no utilice ambos.

- Algunos países tienen un prefijo fijo. Por ejemplo, el código postal de Andorra es AD999. Esto significa que el código de país debe empezar con las letras AD seguidas de tres números.

Code	Nombre	Código postal
CE	Andorra	ANUNCIO 999
AR	Antillas holandesas	9999
AT	Austria	9999
AU	Australia	9999
AZ	Azerbaiyán	COMO 9999
BD	Bangladesh	9999
BE	Bélgica	9999
BG	Bulgaria	9999
BM	Bermudas	aa [aa/99]
BY	Belarús	999999
CA	Canadá	a9a 9a9
CH	Suiza	9999
CL	Chile	9999999
CO	Colombia	999999
CR	Costa Rica	99999
CY	Chipre	9999
CZ	Chequia	999 99
DE	Alemania	99999

Code	Nombre	Código postal
DK	Dinamarca	9999
DO	República Dominicana	99999
DZ	Argelia	99999
EE	Estonia	99999
ES	España	99999
FI	Finlandia	99999
FM	Estados Federados de Micronesia	99999
FO	Islas Faroe	999
FR	Francia	99999
GB	Reino Unido	[a] 9 [a/9] 9aa
GG	Guernsey	GY9 [9] 9aa
GL	Groenlandia	9999
GP	Guadalupe	99999
GT	Guatemala	99999
GU	Guam	99999
HR	Croacia	99999
HU	Hungría	9999
IE	Irlanda	a99 [a/9] [a/9] [a/9] [a/9]
SOY	Isla de Man	IM9 [9] 9aa
IN	India	999999

Code	Nombre	Código postal
IS	Islandia	999
IT	Italia	99999
JE	Jersey	JE9 [9] 9aa
JP	Japón	999-9999
KR	República de Corea	99999
LI	Liechtenstein	9999
LK	Sri Lanka	99999
LT	Lituania	99999
LU	Luxemburgo	L-9999
LV	Letonia	LV-9999
MC	Mónaco	99999
MD	República de Moldova	9999
MH	Islas Marshall	99999
MK	Macedonia del Norte	9999
MAPA	Islas Marianas del Norte	99999
MQ	Martinica	99999
MT	Malta	aaa 9999
MX	México	99999
MY	Malasia	99999
NL	Países Bajos	999 aa

Code	Nombre	Código postal
NO	Noruega	9999
NZ	Nueva Zelanda	9999
PH	Filipinas	9999
PK	Pakistán	99999
PL	Polonia	99-999
PR	Puerto Rico	99999
PT	Portugal	9999-999
PW	Palaos	99999
RE	Reunión	99999
RO	Rumanía	999999
RU	Federación de Rusia	999999
SE	Suecia	999 99
SG	Singapur	999999
SI	Eslovenia	9999
SK	Eslovaquia	999 99
SM	San Marino	99999
TH	Tailandia	99999
TR	Turquía	99999
UA	Ucrania	99999
EE. UU.	Estados Unidos	99999



Code	Nombre	Código postal
UY	Uruguay	99999
VI	Islas Vírgenes (EE. UU.)	99999
WF	Wallis y Futuna	99999
YET	Mayotte	99999
ZA	Sudáfrica	9999

## Enriquecimiento de agentes de usuario

Si crea el modelo Account Takeover Insights (ATI), debe proporcionar una variable del tipo de `useragent` variable en su conjunto de datos. Esta variable contiene los datos del navegador, el dispositivo y el sistema operativo de un evento de inicio de sesión. Amazon Fraud Detector enriquece los datos del agente de usuario con información adicional `user_agent_familyOS_family`, como, y. `device_family`

## Crear una variable

Puede crear variables en la consola de Amazon Fraud Detector mediante el comando [create-variable](#) `CreateVariable`, o mediante el AWS SDK for Python (Boto3)

### Cree una variable mediante la consola de Amazon Fraud Detector

En este ejemplo se crean dos variables `email_address` y `yip_address`, y se asignan a los tipos de variables correspondientes (`EMAIL_ADDRESS` y `IP_ADDRESS`). Estas variables se utilizan como ejemplos. Si está creando variables para su entrenamiento con modelos, utilice las variables del conjunto de datos que sean apropiadas para su caso de uso. Asegúrese de leer acerca de [Tipos de variables](#) las variables y [Enriquecimientos variables](#) antes de crearlas.

Para crear una variable,

1. Abre la [consola AWS de administración](#) e inicia sesión en tu cuenta.
2. Diríjase a Amazon Fraud Detector, seleccione Variables en el menú de navegación de la izquierda y, a continuación, elija Crear.

3. En la página Nueva variable, introduzca `email_address` el nombre de la variable. Si lo desea, introduzca una descripción de la variable.
4. En el tipo de variable, elija Dirección de correo electrónico.
5. Amazon Fraud Detector selecciona automáticamente el tipo de datos para este tipo de variable porque este tipo de variable está predefinido. Si a la variable no se le asigna automáticamente un tipo de variable, seleccione un tipo de variable de la lista. Para obtener más información, consulte [Tipos de variables](#).
6. Si desea proporcionar un valor predeterminado para la variable, seleccione Definir un valor predeterminado personalizado e introduzca un valor predeterminado para la variable. Omita este paso si sigue este ejemplo.
7. Seleccione Crear.
8. En la página de descripción general de `email_address`, confirma los detalles de la variable que acabas de crear.

Si necesitas actualizar, selecciona Editar y proporciona las actualizaciones. Elija Guardar cambios.

9. Repita el proceso para crear otra variable `ip_address` y elija la dirección IP para el tipo de variable.
10. La página Variables muestra las variables recién creadas.

#### Important

Le recomendamos que cree tantas variables como desee a partir de su conjunto de datos. Más adelante, al crear el tipo de evento, podrá decidir qué variables desea incluir para entrenar su modelo a fin de detectar el fraude y generar detecciones de fraude.

## Cree una variable mediante el AWS SDK for Python (Boto3)

El siguiente ejemplo muestra las solicitudes de la [CreateVariable](#) API. El ejemplo crea dos variables `email_address` y `ip_address`, y las asigna a los tipos de variables correspondientes (`EMAIL_ADDRESS` y `IP_ADDRESS`).

Estas variables se utilizan como ejemplos. Si está creando variables para su entrenamiento con modelos, utilice las variables del conjunto de datos que sean apropiadas para su caso de uso.

Asegúrese de leer acerca de [Tipos de variables](#) las variables y [Enriquecimientos variables](#) antes de crearlas.

Asegúrese de especificar una fuente variable. Ayuda a identificar de dónde se deriva el valor de la variable. Si la fuente de la variable es EVENT, el valor de la variable se envía como parte de la [GetEventPrediction](#) solicitud. Si el valor de la variable es MODEL\_SCORE, lo rellena un detector de fraude de Amazon. Si EXTERNAL\_MODEL\_SCORE, el valor de la variable lo rellena un SageMaker modelo importado.

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

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

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

## Eliminar una variable

Al eliminar una variable, Amazon Fraud Detector la elimina permanentemente y los datos ya no se almacenan en Amazon Fraud Detector.

No puede eliminar las variables que se incluyen en un tipo de evento en Amazon Fraud Detector. Primero tendrá que eliminar el tipo de evento al que está asociada la variable y, a continuación, eliminar la variable.

No puede eliminar manualmente las variables de salida del modelo ni las variables de salida del SageMaker modelo de Amazon Fraud Detector. Amazon Fraud Detector elimina automáticamente las variables de salida del modelo cuando se elimina el modelo.

Puede eliminar una variable en la consola de Amazon Fraud Detector mediante el comando de CLI [delete-variable](#), la [DeleteVariable](#) API o la AWS SDK for Python (Boto3)

## Eliminar la variable mediante la consola

Para eliminar una variable,

1. Inicie sesión en la consola de Amazon Fraud Detector AWS Management Console y ábrala en <https://console.aws.amazon.com/frauddetector>.
2. En el panel de navegación izquierdo de la consola de Amazon Fraud Detector, seleccione Recursos y, a continuación, Variables.
3. Elija la variable que desee eliminar.
4. Elija Actions (Acciones) y, a continuación, elija Delete (Eliminar).
5. Introduzca el nombre de la variable y, a continuación, seleccione Eliminar variable.

## Elimine la variable mediante el AWS SDK for Python (Boto3)

El siguiente ejemplo de código elimina una variable `customer_name` mediante la API. [DeleteVariable](#)

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

fraudDetector.delete_variable (

name = 'customer_name'

)
```

## Etiquetas

Una etiqueta clasifica un evento como fraudulento o legítimo. Las etiquetas se asocian a tipos de eventos y se utilizan para entrenar modelos de Machine Learning en Amazon Fraud Detector. Si tiene previsto entrenar un modelo de información sobre el fraude en línea (OFI) o un modelo de

información sobre el fraude de las transacciones (TFI), un mínimo de 400 eventos de su conjunto de datos de capacitación deben clasificarse como fraudulentos o legítimos. Puedes usar cualquier etiqueta, como fraude, legítimo, 1 o 0, para clasificar los eventos de tu conjunto de datos de entrenamiento. Una vez finalizada la capacitación, el modelo capacitado evalúa los eventos para determinar si son fraudulentos y usa estos valores para clasificar los eventos como fraudulentos o legítimos.

Primero tendrá que crear las etiquetas con los valores utilizados en su conjunto de datos de entrenamiento y, a continuación, asociarlas al tipo de evento que se utiliza para crear y entrenar su modelo de detección de fraudes.

## Crear etiqueta

Puede crear etiquetas en la consola de Amazon Fraud Detector, mediante el comando [put-label](#), la [PutLabelAPI](#) o la AWS SDK for Python (Boto3).

### Cree una etiqueta con la consola de Amazon Fraud Detector

Para crear etiquetas,

1. Abre la [consola AWS de administración](#) e inicia sesión en tu cuenta.
2. Diríjase a Amazon Fraud Detector, seleccione Etiquetas en el menú de navegación de la izquierda y, a continuación, elija Crear.
3. En la página Crear etiqueta, introduce el nombre de la etiqueta para un evento fraudulento como nombre de etiqueta. El nombre de la etiqueta debe coincidir con la etiqueta que representa la actividad fraudulenta en tu conjunto de datos de entrenamiento. De manera opcional, ingrese una descripción de la etiqueta.
4. Selecciona Crear etiqueta.
5. Cree una segunda etiqueta e introduzca un nombre de etiqueta para el evento legítimo. Asegúrese de que el nombre de la etiqueta corresponda al valor que representa la actividad legítima en su conjunto de datos de entrenamiento.

### Cree una etiqueta con el AWS SDK for Python (Boto3)

El siguiente código de AWS SDK for Python (Boto3) ejemplo crea dos etiquetas (fraudulentas, legítimas) mediante la [PutLabelAPI](#). Después de crear las etiquetas, puede agregarlas a un tipo de evento para clasificar eventos específicos.

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

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

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

## Actualizar etiqueta

Si su conjunto de datos de eventos está almacenado en Amazon Fraud Detector, es posible que tenga que añadir o actualizar las etiquetas de los eventos almacenados, por ejemplo, cuando realiza una investigación de fraude fuera de línea para un evento y desea cerrar el ciclo de retroalimentación del aprendizaje automático.

Puede añadir o actualizar las etiquetas de los eventos almacenados mediante el [update-event-label](#) comando, la [UpdateEventLabel](#) API o la AWS SDK for Python (Boto3)

El siguiente código de AWS SDK for Python (Boto3) ejemplo agrega un fraude de etiquetas asociado al registro del tipo de evento mediante la `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'
)
```

## Actualización de las etiquetas de eventos en los datos de eventos almacenados en Amazon Fraud Detector

Es posible que tenga que añadir o actualizar etiquetas de fraude para los eventos que ya están almacenados en Amazon Fraud Detector, por ejemplo, cuando realiza una investigación de fraude fuera de línea para un evento y desea cerrar el ciclo de retroalimentación del aprendizaje automático. Para actualizar la etiqueta de un evento que ya está almacenado en Amazon Fraud Detector, utilice la operación `UpdateEventLabel` de API. A continuación se muestra un ejemplo de llamada a `UpdateEventLabel` la 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'
)
```

## Eliminar etiqueta

Al eliminar una etiqueta, Amazon Fraud Detector la elimina permanentemente y los datos ya no se almacenan en Amazon Fraud Detector.

No puede eliminar una etiqueta incluida en un tipo de evento en Amazon Fraud Detector. Tampoco se puede eliminar una etiqueta asignada a un ID de evento. Primero debe eliminar el ID de evento pertinente.

Puede eliminar etiquetas en la consola de Amazon Fraud Detector mediante el comando [delete-label](#), la [DeleteLabel](#) API o la AWS SDK for Python (Boto3)

### Eliminación de etiqueta mediante la consola

Para eliminar una etiqueta

1. Inicie sesión en AWS Management Console y abra la consola de Amazon Fraud Detector en <https://console.aws.amazon.com/frauddetector>.

2. En el panel de navegación izquierdo de la consola de Amazon Fraud Detector, seleccione Recursos y, a continuación, Etiquetas.
3. Elija la etiqueta que desea eliminar.
4. Elija Actions (Acciones) y, a continuación, elija Delete (Eliminar).
5. Introduzca el nombre de la etiqueta y, a continuación, seleccione Eliminar etiqueta.

## Elimine una etiqueta mediante elAWS SDK for Python (Boto3)

El siguiente código deAWS SDK for Python (Boto3) ejemplo elimina una etiqueta legítima mediante la [DeleteLabelAPI](#).

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

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

## Reglas

Una regla es una condición que indica a Amazon Fraud Detector cómo interpretar los valores de las variables durante una predicción de fraude. Una regla forma parte de la lógica de un detector y consta de los siguientes elementos:

- Variable o lista: la variable representa un elemento de datos de su conjunto de datos de eventos que desea utilizar en una predicción de fraude. Una lista es un conjunto de elementos de datos de entrada para una variable del conjunto de datos de eventos. Las variables utilizadas en una regla deben estar predefinidas en el tipo de evento evaluado y las listas utilizadas en una regla deben estar asociadas a un tipo de variable. Para obtener más información, consulte [Variables](#) y [Lists](#).
- Expresión: una expresión de una regla captura la lógica empresarial. Si utiliza una variable en la regla, se construye una expresión de regla simple mediante una variable, un operador de comparación como >, <, <=, >=, == y un valor. Si utiliza una lista, la expresión de la regla se construye como entrada de lista y el nombre de la lista. Para obtener más información, consulte [Referencia al lenguaje de las reglas](#). Puede combinar varias expresiones usando and y or. Todas las expresiones deben dar como resultado un valor booleano (verdadero o falso) y tener una longitud inferior a 4000 caracteres. No se admiten las condiciones de tipo If-Else.



- **Resultado:** un resultado es una respuesta que Amazon Fraud Detector devuelve cuando se cumple una regla. El resultado indica el resultado de una predicción de fraude. Puede crear resultados para cada posible predicción de fraude y añadirlos a una regla. Para obtener más información, consulte [Resultados](#).

Un detector debe tener al menos una regla asociada. Una regla puede tener hasta 3 listas y un detector puede tener hasta 30 listas. La regla se crea como parte del proceso de creación del detector. También puede crear reglas nuevas y asociarlas a un detector existente.

## Referencia al lenguaje de las reglas

En la siguiente sección se describen las capacidades de expresión (es decir, redacción de reglas) de Amazon Fraud Detector.

### Uso de variables

Puede utilizar cualquier variable definida en el tipo de evento evaluado como parte de la expresión. Usa el signo de dólar para indicar una variable:

```
$example_variable < 100
```

### Uso de listas

Puede utilizar cualquier lista que esté asociada a un tipo de variable y que se rellene con entradas como parte de la expresión de la regla. Utilice el signo de dólar para indicar un valor de entrada en la lista:

```
$example_list_variable in @list_name
```

### Operadores de comparación, membresía e identidad

Amazon Fraud Detector incluye los siguientes operadores de comparación: >, >=, <, <=, !=, ==, en, no en

A continuación se muestran algunos ejemplos:

Ejemplo: <

```
$variable < 100
```

### Ejemplo: en, no en

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

### Ejemplo:!=

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

### Ejemplo: ==

```
$variable == 1000
```

### Tablas de operadores

":"	Operador de detectores de fraude de Amazon
Igual que	==
No igual a	!=
Mayor que	>
Menor que	<
Mayor o igual a	>=
Menor o igual que	<=
En	in
And	Protección de los datos
O bien	o bien
No	!

### Matemáticas básicas

Puede utilizar operadores matemáticos básicos en la expresión (por ejemplo, +, -, \*, /). Un caso de uso típico es cuando necesita combinar variables durante la evaluación.

En la siguiente regla, sumamos la variable `$variable_1` con `$variable_2` y comprobamos si el total es inferior a 10.

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

## Datos básicos de tablas matemáticas

"."	Operador de detectores de fraude de Amazon
Más	+
Menos	-
Multipliy (Multiplicación)	*
Divide (División)	/
Módulo	%

## Expresión regular (regex)

Puede utilizar expresiones regulares para buscar patrones específicos como parte de la expresión. Esto es especialmente útil si busca hacer coincidir una cadena específica o un valor numérico para una de sus variables. Amazon Fraud Detector solo admite la coincidencia cuando se trabaja con expresiones regulares (por ejemplo, devuelve Verdadero/Falso en función de si la cadena proporcionada coincide con la expresión regular). El soporte de expresiones regulares de Amazon Fraud Detector se basa en `.matches()` en java (mediante la biblioteca de expresiones regulares RE2J). Hay varios sitios web útiles en Internet que son útiles para probar diferentes patrones de expresiones regulares.

En el primer ejemplo siguiente, primero transformamos la variable `email` a minúsculas. Luego comprobamos si el patrón `@gmail.com` está en la `email` variable. Observe que el segundo punto tiene un escape para que podamos comprobar explícitamente la cadena `.com`.

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

En el segundo ejemplo, comprobamos si la variable `phone_number` contiene el código de país `+1` para determinar si el número de teléfono es de EE. UU. El símbolo `+` se usa como escape para que podamos comprobar explícitamente la cadena `+1`.

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

## Tabla Regex

."	Ejemplo de detector de fraude de Amazon
Coincide con cualquier cadena que comience por	<code>regex_match («^mystring», \$variable)</code>
Coincide exactamente con toda la cadena	<code>regex_match («micadena», \$variable)</code>
Coincide con cualquier carácter excepto con la nueva línea	<code>regex_match («.», \$ (variable))</code>
Haga coincidir cualquier número de caracteres excepto la nueva línea antes de 'mystring'	<code>regex_match («. *mystring», \$variable)</code>
Personajes especiales de escape	<code>\</code>

## Comprobar si faltan valores

A veces es beneficioso comprobar si falta el valor. En Amazon Fraud Detector, esto se representa con un valor nulo. Para ello, utilice la siguiente sintaxis:

```
$variable != null
```

Del mismo modo, si desea comprobar si un valor no está presente, puede hacer lo siguiente:

```
$variable == null
```

## Múltiples condiciones

Puede combinar varias expresiones usando `and` y `or`. Amazon Fraud Detector se detiene en una OR expresión cuando se encuentra un único valor verdadero y se detiene en una AND cuando se encuentra un único valor falso.

En el ejemplo siguiente, estamos comprobando dos condiciones mediante la `and` condición. En la primera declaración, estamos comprobando si la variable 1 es inferior a 100. En la segunda comprobamos si la variable 2 no es EE. UU.

Dado que la regla usa un `and`, ambos deben ser VERDADEROS para que toda la condición se evalúe como VERDADERA.

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

Puede utilizar paréntesis para agrupar operaciones booleanas, como se muestra a continuación:

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

## Otros tipos de expresiones

### DateTimefunciones

Función	Descripción	Ejemplo
<code>getcurrentdatetime ()</code>	Indica la hora actual de ejecución de la regla en formato ISO8601 UTC. Puede usar <code>getepochmilliseconds (getcurrentdatetime ())</code> para realizar operaciones adicionales	<code>getcurrentdatetime () == «2023-03-28T 18:34:02 Z»</code>
<code>es anterior (DateTime1, DateTime 2)</code>	Devuelve un booleano (Verdadero/Falso) si la persona que llama 1 está antes de 2 DateTime DateTime	<code>isbefore (getcurrentdatetime (), «2019-11-30T 01:01:01 Z») == «Falso»</code>  <code>isbefore (getcurrentdatetime (), «2050-11-30T 01:05:01 Z») == «Verdadero»</code>

Función	Descripción	Ejemplo
después (DateTime1, DateTime 2)	Devuelve un booleano (Verdadero/ Falso) si la persona que llama 1 está después de 2 DateTime DateTime	isafter (getcurrentdatetime ()), «2019-11-30T 01:01:01 Z») == «Verdadero»  isafter (getcurrentdatetime ()), «2050-11-30T 01:05:01 Z») == «Falso»
getepochmilisegundos (DateTime)	Toma un DateTime y lo devuelve DateTime en milisegundos de época. Útil para realizar operaciones matemáticas en la fecha	getepochmilisegundos («2019-11-30T 01:01:01 Z») = 1575032461

## Operadores de cadena

Función	Ejemplo
Transformar cadena en mayúsculas	mayúsculas (\$variable)
Transforma cadena en minúsculas	minúsculas (\$variable)

## Otros

Función	Comentario
Añadir un comentario	# mi comentario

## Crear reglas

Puede crear reglas en la consola de Amazon Fraud Detector mediante el comando [create-rule](#), la [CreateRule](#)API o la AWS SDK for Python (Boto3)

Cada regla debe contener una sola expresión que refleje su lógica empresarial. Todas las expresiones deben dar como resultado un valor booleano (verdadero o falso) y tener una longitud inferior a 4000 caracteres. No se admiten las condiciones de tipo If-Else. Todas las variables utilizadas en la expresión deben estar predefinidas en el tipo de evento evaluado. Del mismo modo, todas las listas utilizadas en la expresión deben estar predefinidas, asociadas a un tipo de variable y rellenarse con entradas.

El siguiente ejemplo crea una regla `high_risk` para un detector `existingpayments_detector`. La regla asocia una expresión y un resultado `verify_customer` a la regla.

### Requisitos previos

Para seguir los pasos que se mencionan a continuación, asegúrese de completar lo siguiente antes de continuar con la creación de reglas:

- [Crear un detector](#)
- [Crea un resultado](#)

Si está creando un detector, una regla y un resultado para su caso de uso, sustituya el nombre del detector, el nombre de la regla, la expresión de la regla y el nombre del resultado del ejemplo por los nombres y expresiones relevantes para su caso de uso.

## Cree una nueva regla en la consola de Amazon Fraud Detector

1. Abra la [consola AWS de administración](#) e inicia sesión en tu cuenta. Diríjase a Amazon Fraud Detector.
2. En el panel de navegación de la izquierda, elija Detectores y seleccione el detector que creó para su caso de uso, por ejemplo, `payments_detector`.
3. En la página `payments_detector`, elija la pestaña Reglas asociadas y, a continuación, elija Crear regla.
4. En la página Nueva regla, introduzca lo siguiente:
  - a. En Nombre, introduzca un nombre para la regla, por ejemplo **high\_risk**
  - b. En la descripción (opcional), introduzca opcionalmente una descripción de la regla, por ejemplo, **This rule captures events with a high ML model score**
  - c. En la Expresión, introduzca una expresión de regla para su caso de uso mediante la guía de referencia rápida de expresiones. Ejemplo `$sample_fraud_detection_model_insightscore >900`

- d. En los Resultados, elige el resultado que creaste para tu caso de uso, por ejemplo `verify_customer`. Un resultado es el resultado de una predicción de fraude y se devuelve si la regla coincide durante una evaluación.

## 5. Elija Guardar regla

Ha creado una nueva regla para su detector. Esta es la versión 1 de la regla que Amazon Fraud Detector pone automáticamente a disposición del detector para que la utilice.

## Cree una regla mediante el AWS SDK for Python (Boto3)

El siguiente código de ejemplo usa la [CreateRule](#) API para crear una regla `high_risk` para un detector existente `payments_detector`. El código de ejemplo también agrega una expresión de regla y un resultado `verify_customer` a la regla.

### Requisitos previos

Para usar el código de ejemplo, asegúrese de completar lo siguiente antes de continuar con la creación de reglas:

- [Crear un detector](#)
- [Crea un resultado](#)

Si está creando un detector, una regla y un resultado para su caso de uso, sustituya el nombre del detector, el nombre de la regla, la expresión de la regla y el nombre del resultado del ejemplo por nombres y expresiones relevantes para su caso de uso.

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

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

Ha creado la versión 1 de la regla y Amazon Fraud Detector la pone automáticamente a disposición del detector para que la utilice.



## Actualizar regla

Puede actualizar una regla en cualquier momento añadiendo o actualizando la descripción de la regla, actualizando la expresión de la regla o añadiendo o quitando el resultado de la regla. Al actualizar una regla, se crea una nueva versión de la regla.

Puede actualizar una regla en la consola de Amazon Fraud Detector mediante el [update-rule-version](#) comando, la [UpdateRuleVersion](#) API o el AWS SDK.

Después de actualizar la regla, asegúrese de actualizar la versión del detector para usar la nueva versión de la regla.

### Actualizar la regla en la consola de Amazon Fraud Detector

Para actualizar una regla,

1. Abra la [consola AWS de administración](#) e inicia sesión en tu cuenta. Diríjase a Amazon Fraud Detector.
2. En el panel de navegación de la izquierda, seleccione Detectores.
3. En el panel Detectores, seleccione el detector asociado a la regla que desea actualizar.
4. En la página del detector, elija la pestaña Reglas asociadas y seleccione la regla que desee actualizar.
5. En la página de reglas, selecciona Acciones y selecciona Crear versión.
6. Tenga en cuenta que la versión ha cambiado. Introduzca la descripción, la expresión o el resultado actualizados.
7. Elija Guardar nueva versión

### Actualice la regla mediante el AWS SDK for Python (Boto3)

El siguiente código de ejemplo usa la [UpdateRuleVersion](#) API para actualizar el umbral de la regla `high_risk` de 900 a 950. Esta regla está asociada al detector `payments_detector`.

```
fraudDetector.update_rule_version(  
rule = {  
    'detectorId' : 'payments_detector',  
    'ruleId' : 'high_risk',  
    'ruleVersion' : '1'  
})
```

```
},  
expression = '$sample_fraud_detection_model_insightscore > 950',  
language = 'DETECTORPL',  
outcomes = ['verify_customer']  
)
```

## Lists

Una lista es un conjunto de datos de entrada para una variable del conjunto de datos de eventos. Los datos de entrada se utilizan en una regla que está asociada al detector. Una regla es una condición que indica a Amazon Fraud Detector cómo interpretar los datos de entrada durante una predicción de fraude. Por ejemplo, puede crear una lista de direcciones IP y, a continuación, crear una regla para denegar el acceso si hay una dirección IP específica en la lista. Las reglas que utilizan listas se expresan en `@list_name formato$ip_address_value in`.

Con Amazon Fraud Detector, puede administrar una lista añadiendo o eliminando datos sin necesidad de actualizar una regla asociada. Una regla asociada a la lista incorpora automáticamente los datos que se hayan añadido o eliminado recientemente.

Una lista puede contener hasta 100 000 entradas únicas y cada entrada puede tener hasta 320 caracteres. Todas las listas que utilice en una regla están asociadas de forma predeterminada a [Tipos de variables](#) `FREE_FORM_TEXT` de Amazon Fraud Detector. Puede asignar un tipo de variable a la lista en cualquier momento. Puede utilizar hasta 3 listas en una regla.

Puede crear una lista, añadir entradas a la lista, eliminar una lista o eliminar una o más entradas de la lista, o asignar un tipo de variable a la lista en la consola de Amazon Fraud Detector, mediante la `APIAWS CLI`, el `SDK` o el `AWS SDK`.

## Crear una lista

Puede crear una lista que contenga los datos de entrada (entradas) de una variable en su conjunto de datos de eventos y utilizar la lista en la expresión de reglas. Las entradas de la lista se pueden administrar de forma dinámica sin actualizar la regla que usa la lista.

Para crear una lista, primero debe especificar un nombre y, si lo desea, asociarla a un detector de fraude [Tipos de variables](#) compatible con Amazon Fraud Detector. De forma predeterminada, Amazon Fraud Detector asume que la lista es del tipo de variable `FREE_FORM_TEXT`.

Puede crear una lista en la consola de Amazon Fraud Detector, mediante la APIAWS CLI, el SDK o elAWS SDK.

## Cree una lista con la consola de Amazon Fraud Detector

Para crear una lista

1. Abra la [consolaAWS de administración](#) e inicia sesión en tu cuenta. Navegue hasta Amazon Fraud Detector Detector Detector.
2. En el panel de navegación izquierdo, elija Listas.
3. En Detalles de las listas
  - a. En el nombre de la lista, introduzca un nombre para la lista.
  - b. En la descripción, introduzca una descripción.
  - c. (Opcional) En Tipo de variable, seleccione un tipo de variable para la lista.

### Important

Si la lista contiene direcciones IP, asegúrese de seleccionar IP\_ADDRESS como tipo de variable. Si no selecciona un tipo de variable, Amazon Fraud Detector asume que la lista es del tipo de variable FREE\_FORM\_TEXT.

4. En Agregar datos de lista, añada entradas a la lista, una entrada en cada línea. También puedes copiar y pegar entradas de una hoja de cálculo.

### Note

Asegúrese de que las entradas no estén separadas por comas y que sean únicas en la lista. Si se introducen dos entradas idénticas, solo se añadirá una.

5. Seleccione Create (Crear).

## Cree una lista mediante elAWS SDK for Python (Boto3)

Para crear una lista, especifique un nombre de lista. Si lo desea, puede proporcionar una descripción, asociar un tipo de variable o añadir entradas a la lista al crear una lista. O bien, puede actualizar la lista más adelante añadiendo entradas o una descripción. Puede asignar un tipo de

variable a la lista más adelante si no lo ha asignado en el momento de la creación de la lista. El tipo de variable de una lista no se puede cambiar después de asignarla.

### Important

Si la lista contiene direcciones IP, asegúrese de asignar IP\_ADDRESS como tipo de variable. Si no asigna ningún tipo de variable, Amazon Fraud Detector asume que la lista es del tipo de variable FREE\_FORM\_TEXT.

El siguiente ejemplo usa la operación de la [CreateList](#) API para crear una `allow_email_ids` lista proporcionando una descripción, un tipo de variable y agregando cuatro entradas de lista.

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

fraudDetector.create_list (
    name = 'allow_email_ids',
    description = 'legitimate email_ids'
    variableType = 'EMAIL_ADDRESS',
    elements = ['emailId_1', 'emailId_2', 'emailId_3', 'emailId_4']
)
```

## Añadir entradas a una lista

Después de crear la lista, puede añadir o anexar entradas a la lista en cualquier momento. Al agregar o anexar entradas a la lista, no es necesario la actualización de la regla a la que está asociada. La regla incorpora automáticamente las entradas recién agregadas.

La lista puede contener hasta 100 000 entradas únicas y cada entrada puede tener hasta 320 caracteres.

Puede añadir entradas en la consola de Amazon Fraud Detector, mediante la APIAWS CLI, el SDK o elAWS SDK.

## Añada entradas a una lista mediante la consola de Amazon Fraud Detector

Para agregar una o varias entradas a una lista

1. Abre la [consolaAWS de administración](#) e inicia sesión en tu cuenta. Navegue hasta Amazon Fraud Detector Detector Detector.
2. En el panel de navegación izquierdo, elija Listas.
3. En la página Listas, seleccione la lista a la que desee añadir entradas.
4. En la página de detalles de la lista, selecciona la pestaña Datos de lista y elige Agregar datos.
5. En el cuadro Agregar datos de lista, añada una entrada en cada línea o copie y pegue las entradas de una hoja de cálculo. Asegúrese de no utilizar comas para separar las entradas.
6. Elija Add (Agregar).

## Añada entradas a una lista mediante elAWS SDK for Python (Boto3)

En el siguiente ejemplo, se utiliza la operación de [UpdateListAPI](#) para añadir dos entradas nuevas a la `allow_email_ids` lista. Asegúrese de que las entradas que añada sean únicas en la lista.

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

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

## Asignar un tipo de variable a una lista

Cada lista que utilice en una regla debe estar asociada al tipo de [Tipos de variables](#) variable de Amazon Fraud Detector. De forma predeterminada, Amazon Fraud Detector asume que la lista es del tipo de variable `FREE_FORM_TEXT`. Es importante tener en cuenta que una lista que contenga direcciones IP debe estar asociada al tipo de variable `IP_ADDRESS`.

Puede asociar la lista a un tipo de variable en el momento de la creación de la lista o en cualquier momento posterior. Si ya ha asociado la lista a un tipo de variable y desea cambiarla más adelante, debe crear una lista nueva. No se puede cambiar el tipo de variable de una lista.

Puede asignar un tipo de variable en la consola de Amazon Fraud Detector, mediante la APIAWS CLI, el SDK o elAWS SDK.

## Asigne un tipo de variable a una lista mediante la consola de Amazon Fraud Detector

Para asignar un tipo de variable a una lista

1. Abra la [consolaAWS de administración](#) e inicia sesión en tu cuenta. Navegue hasta Amazon Fraud Detector Detector Detector.
2. En el panel de navegación izquierdo, elija Listas.
3. En la página Listas, seleccione la lista a la que desee asignar un tipo de variable.
4. En la página de detalles de la lista, selecciona Acciones y selecciona Editar lista.
5. En el cuadro Editar lista, seleccione el tipo de variable de la lista.
6. Seleccione Guardar.

## Asigne un tipo de variable a una lista medianteAWS SDK for Python (Boto3)

El siguiente ejemplo usa la operación [UpdateList](#)de API para asignar un tipo de variable a laallow\_ip\_address lista.

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

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

## Eliminar una lista

Puede eliminar una lista que no se utilice en ninguna regla. Al eliminar una lista, Amazon Fraud Detector elimina permanentemente esa lista y todas las entradas de la lista.

Puede eliminar una lista en la consola de Amazon Fraud Detector, mediante la API, el SDKAWS CLI o elAWS SDK.

## Eliminar la lista mediante la consola de Amazon Fraud Detector

### Eliminación de una lista

1. Abre la [consolaAWS de administración](#) e inicia sesión en tu cuenta. Navegue hasta Amazon Fraud Detector Detector Detector.
2. En el panel de navegación izquierdo, elija Listas
3. En la página Listas, seleccione la lista que desee eliminar.
4. En la página de detalles de la lista, selecciona Acciones y selecciona Eliminar lista.
5. Selecciona Eliminar lista.

### Elimine la lista mediante elAWS SDK for Python (Boto3)

En el siguiente ejemplo, se utiliza la operación de [DeleteList](#)API para eliminar `allow_email_ids`.

```
import boto3

fraudDetector = boto3.client('frauddetector')

fraudDetector.delete_list(
    name = 'allow_email_ids'
)
```

## Eliminar entradas de una lista

Puede eliminar una o varias entradas de sus listas en cualquier momento. Al eliminar entradas de la lista, no es necesario actualizar la regla a la que está asociada la lista. La regla incorpora automáticamente la lista actualizada.

Puede eliminar las entradas de una lista en la consola de Amazon Fraud Detector, mediante la API, el SDKAWS CLI o elAWS SDK.

## Eliminar entradas de una lista mediante la consola de Amazon Fraud Detector

### Eliminación de una o varias entradas de una lista

1. Abre la [consolaAWS de administración](#) e inicia sesión en tu cuenta. Navegue hasta Amazon Fraud Detector Detector Detector.
2. En el panel de navegación izquierdo, elija Listas

3. En la página Listas, seleccione la lista que contiene las entradas que desea eliminar.
4. En la página de detalles de la lista, selecciona la pestaña Datos de lista y selecciona las entradas que deseas eliminar.
5. Selecciona Eliminar y elige Eliminar de nuevo para confirmar.

## Elimine entradas de una lista mediante elAWS SDK for Python (Boto3)

En el siguiente ejemplo, la operación [UpdateList](#) de API elimina las entradas de la `allow_email_ids` lista.

```
import boto3

fraudDetector = boto3.client('frauddetector')

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

## Eliminar todas las entradas de una lista

Puede eliminar todas las entradas de la lista si la lista no se usa en una regla. Puede eliminar todas las entradas de la lista y, posteriormente, añadir entradas a la misma lista.

Puede eliminar las entradas de una lista en la consola de Amazon Fraud Detector, mediante la API, el SDKAWS CLI o elAWS SDK.

## Elimine todas las entradas de una lista mediante la consola de Amazon Fraud Detector

Para eliminar todas las entradas de una lista

1. Abre la [consolaAWS de administración](#) e inicia sesión en tu cuenta. Navegue hasta Amazon Fraud Detector.
2. En el panel de navegación izquierdo, elija Listas
3. En la página Listas, seleccione la lista que contiene las entradas que desea eliminar.
4. En la página de detalles de la lista, selecciona la pestaña Datos de la lista y elige Eliminar todo.
5. En el cuadro Eliminar todo, escriba `delete all` para confirmar y, a continuación, elija Eliminar todos los datos de la lista.



## Elimine todas las entradas de una lista mediante elAWS SDK for Python (Boto3)

En el siguiente ejemplo, la operación de [UpdateList](#)API elimina todas las entradas de la `allow_email_ids` lista.

```
import boto3

fraudDetector = boto3.client('frauddetector')

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

## Resultados

Un resultado es el resultado de una predicción de fraude. Puede crear un resultado para cada posible resultado de predicción de fraude. Por ejemplo, puede que los resultados representen niveles de riesgo (riesgo alto, riesgo medio y riesgo bajo) o acciones (aprobación, revisión). Después de crear un resultado, puede añadir uno o varios resultados. Como parte de la [GetEventPrediction](#) respuesta, Amazon Fraud Detector devuelve los resultados definidos para cualquier regla coincidente.

### Creación de un resultado

Puede crear resultados en la consola de Amazon Fraud Detector, mediante el comando [put-result](#), la [PutOutcome](#)API o laAWS SDK for Python (Boto3).

### Creación de un resultado mediante la consola de Amazon Fraud Detector

Para crear uno o varios resultados,

1. Abra la [consolaAWS de administración](#) e inicia sesión en tu cuenta. Navegue hasta Amazon Fraud Detector.
2. En el panel de navegación izquierdo, elija Resultados.
3. En la página Resultados, selecciona Crear.
4. En la página de nuevos resultados, introduce lo siguiente:
  - a. En el nombre del resultado, introduzca un nombre para el resultado.

- b. En la descripción del resultado, puede introducir una descripción.
5. Selecciona Guardar resultado.
6. Repita los pasos 2 a 5 para crear resultados adicionales.

## Cree un resultado mediante elAWS SDK for Python (Boto3)

En el siguiente ejemplo, se utiliza laPutOutcome API para crear tres resultados.

Sonverify\_customerreview, yapprove. Una vez creados los resultados, puede asignarlos a las reglas.

```
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'
)
```

## Eliminar un resultado

No se puede eliminar un resultado que se utiliza en una versión de regla.

Al eliminar un resultado, Amazon Fraud Detector elimina ese resultado de forma permanente y los datos ya no se almacenan en Amazon Fraud Detector.

Puede eliminar un resultado en la consola de Amazon Fraud Detector mediante el comando [delete-result](#), la [DeleteOutcome](#)API o laAWS SDK for Python (Boto3)

## Eliminar un resultado en la consola de Amazon Fraud Detector

Para eliminar un resultado

1. Inicie sesión en AWS Management Console y abra la consola de Amazon Fraud Detector en <https://console.aws.amazon.com/frauddetector>.
2. En el panel de navegación izquierdo de la consola de Amazon Fraud Detector, seleccione Recursos y, a continuación, elija Resultados.
3. Elija el resultado que desee eliminar.
4. Elija Actions (Acciones) y, a continuación, elija Delete (Eliminar).
5. Introduzca el nombre del resultado y, a continuación, seleccione Eliminar resultado.

## Elimine un resultado mediante el AWS SDK for Python (Boto3)

En el siguiente ejemplo, se utiliza la [DeleteOutcome](#) API para eliminar el `verify_customer` resultado. Una vez eliminado el resultado, ya no podrá asignarlo a una regla.

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

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

## Entidad

Una entidad representa a una persona o cosa que realiza el evento. Un tipo de entidad clasifica la entidad. Entre las clasificaciones de ejemplo se incluyen cliente, comerciante, usuario o cuenta. Debe proporcionar el tipo de entidad (ENTITY\_TYPE) y un identificador de entidad (ENTITY\_ID) como parte del conjunto de datos de eventos para indicar la entidad específica que realizó el evento.

Amazon Fraud Detector utiliza el tipo de entidad al generar una predicción de fraude para un evento para indicar quién lo realizó. El tipo de entidad que desee utilizar en sus predicciones de fraude debe crearse primero en Amazon Fraud Detector y, a continuación, agregarse al evento al crear su tipo de evento.

## Crear un tipo de entidad

Puede crear un tipo de entidad en la consola de Amazon Fraud Detector mediante el [put-entity-type](#) comando, la [PutEntityType](#) API o la AWS SDK for Python (Boto3). Los siguientes ejemplos crean un tipo de entidad `customer` en la consola de Amazon Fraud Detector y mediante el SDK for Python (Boto3). Si va a crear un tipo de entidad para asociarlo a un tipo de evento para entrenar un modelo de detección de fraudes, utilice el tipo de entidad del conjunto de datos de eventos que sea adecuado para su caso de uso.

### Cree un tipo de entidad mediante la consola de Amazon Fraud Detector

Para crear un tipo de entidad,

1. Abra la [consola AWS de administración](#) e inicia sesión en tu cuenta.
2. Diríjase a Amazon Fraud Detector, elija Entidades en el menú de navegación de la izquierda y, a continuación, elija Crear.
3. En la página Crear entidad, introduzca cliente como nombre del tipo de entidad. De manera opcional, ingrese una descripción de la entidad.
4. Seleccione Create entity (Crear entidad).

### Cree un tipo de entidad mediante el AWS SDK for Python (Boto3)

El siguiente ejemplo AWS SDK for Python (Boto3) de código usa la `PutEntityType` API para crear un tipo de entidad `customer`. Si va a crear un tipo de entidad para asociarlo a un tipo de evento a fin de entrenar un modelo de detección de fraudes, utilice la entidad del conjunto de datos de eventos que sea adecuada para su caso de uso.

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

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

## Eliminar un tipo de entidad

Los tipos de entidad incluidos en un tipo de evento no se pueden eliminar en Amazon Fraud Detector. Primero tendrá que eliminar el tipo de evento al que está asociada la entidad y, a continuación, eliminar el tipo de entidad.

Al eliminar un tipo de entidad, Amazon Fraud Detector elimina permanentemente ese tipo de entidad y los datos ya no se almacenan en Amazon Fraud Detector.

Se puede eliminar un tipo de entidad en la consola de Amazon Fraud Detector mediante el [delete-entity-type](#) comando, la [DeleteEntityType](#) API o la AWS SDK for Python (Boto3)

### Eliminar un tipo de entidad en la consola de Amazon Fraud Detector

Para eliminar un tipo de entidad,

1. Inicie sesión en AWS Management Console y abra la consola de Amazon Fraud Detector en <https://console.aws.amazon.com/frauddetector>.
2. En el panel de navegación izquierdo de la consola de Amazon Fraud Detector, seleccione Recursos y, a continuación, Entidades.
3. Elija el tipo de entidad que desea eliminar.
4. Elija Actions (Acciones) y, a continuación, elija Delete (Eliminar).
5. Introduzca el nombre del tipo de entidad y, a continuación, seleccione Eliminar tipo de entidad.

### Elimine el tipo de entidad mediante el AWS SDK for Python (Boto3)

El siguiente código de AWS SDK for Python (Boto3) ejemplo elimina el tipo de entidad client mediante la [DeleteEntityType](#) API.

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

fraudDetector.delete_entity_type (

name = 'customer'

)
```

# Gestione los recursos de Amazon Fraud Detector mediante AWS CloudFormation

## Amazon

CloudFormation Puede crear una plantilla que describa los recursos de Amazon Fraud Detector que desea aprovisionar y configurar en varias cuentas y regiones de AWS. Puede reutilizar la plantilla para aprovisionar y configurar los recursos de manera coherente y repetida en varias cuentas y regiones de AWS.

El uso de AWS no supone ningún cargo adicional de CloudFormation.

## Amazon CloudFormation

[Para aprovisionar y configurar los recursos de Amazon Fraud Detector con AWS CloudFormation](#) Las plantillas son archivos de texto con formato de tipo JSON o YAML. Estas plantillas describen los recursos que desea aprovisionar en sus pilas de AWS CloudFormation. Si no está familiarizado con JSON o YAML, puede utilizar Designer de AWS CloudFormation para comenzar a utilizar las plantillas de AWS CloudFormation. Para obtener más información, consulte [¿Qué es Designer de AWS CloudFormation?](#) en la Guía del usuario de AWS CloudFormation.

También puede crear, actualizar y eliminar los recursos de Amazon Fraud Detector con AWS CloudFormation. Para obtener más información, incluidos ejemplos de plantillas JSON y YAML para sus recursos, consulte la [referencia de AWS CloudFormation tipo de recurso de Amazon Fraud Detector](#)

Si ya lo está utilizando con CloudFormation, no es necesario administrar políticas o registros de CloudTrail adicionales.

## Amazon CloudFormation

Puede crear, actualizar y eliminar sus pilas de Amazon Fraud Detector a través de la consola de CloudFormation o de la CLI de AWS.

Para crear una pila, debe disponer de una plantilla que describa qué recursos de CloudFormation incluirá en la pila. También puede incorporar a la administración de CloudFormation los recursos de Amazon Fraud Detector que ya haya creado [importándolos](#) a una pila nueva o existente.

Para obtener instrucciones detalladas sobre cómo administrar las pilas, consulta la Guía del AWS CloudFormation usuario para aprender a [crear](#), [actualizar](#) y [eliminar](#) pilas.

## Amazon Fraud Detector

La forma en que AWS CloudFormation organices tus pilas depende totalmente de ti. Por lo general, se recomienda organizar las pilas por ciclo de vida y propiedad. Esto significa agrupar los recursos según la frecuencia con la que cambian o por equipos que son responsables de actualizarlos.

Puede optar por organizar sus pilas creando una pila para cada detector y su lógica de detección (por ejemplo, reglas, variables, etc.). Si utiliza otros servicios, debería plantearse si desea combinar los recursos de Amazon Fraud Detector con los recursos de otros servicios. Por ejemplo, podría crear una pila que incluya los recursos de Kinesis que ayudan a recopilar datos y los recursos de Amazon Fraud Detector que procesan los datos. Esta puede ser una forma eficaz de garantizar que todos los productos de su equipo de fraude funcionen en conjunto.

## Amazon CloudFormation DetDetDetDetDetDetDetDetDet

Además de los parámetros estándar que están disponibles en todas las CloudFormation plantillas, Amazon Fraud Detector presenta dos parámetros adicionales que le ayudarán a gestionar el comportamiento de la implementación. Si no incluye uno o ambos parámetros, CloudFormation utilizará el valor predeterminado que se muestra a continuación.

Parámetro	Valores	Valor predeterminado
DetectorVersionStatus	<p>ACTIVO: Establece la versión nueva o actualizada del detector en estado Activo</p> <p>BORRADOR: Establece la versión nueva o actualizada del detector en estado Borrador</p>	BORRADOR
Inline	<p>VERDADERO: permite CloudFormation crear, actualizar o eliminar el recurso al crear, actualizar o eliminar la pila.</p> <p>FALSO: CloudFormation permite validar que el objeto existe, pero no realizar ningún cambio en él.</p>	TRUE

## Amazon Fraud DetectorAWS CloudFormation

El siguiente es un ejemplo de plantillaAWS CloudFormation YAML para administrar un aud y las versiones del detector asociadas.

```
# 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'
```

## Obtener más información sobre AWS CloudFormation

Para obtener más información acerca de AWS CloudFormation, consulte los siguientes recursos:

- [AWS CloudFormation](#)
- [Guía del usuario de AWS CloudFormation](#)
- [Referencia de la API de AWS CloudFormation](#)
- [Guía del usuario de la interfaz de la línea de comandos de AWS CloudFormation](#)

# Predicciones de fraude

Puede utilizar Amazon Fraud Detector para obtener predicciones de fraude para un solo evento en tiempo real o para obtener predicciones de fraude sin conexión para un conjunto de eventos. Para generar predicciones de fraude para un solo evento o para un conjunto de eventos, deberá proporcionar a Amazon Fraud Detector la siguiente información:

- Lógica de predicción de fraude
- Metadatos del evento

## Lógica de detección de fraudes

La lógica de predicción de fraudes utiliza una o más reglas para evaluar los datos asociados a un evento y, a continuación, proporciona el resultado y una puntuación de predicción de fraude. La lógica de predicción del fraude se crea mediante los siguientes componentes:

- Tipos de eventos: define la estructura del evento
- Modelos: define los requisitos de algoritmos y datos para predecir el fraude
- Variables: representan un elemento de datos asociado al evento
- Reglas: indica a Amazon Fraud Detector cómo interpretar los valores de las variables durante la predicción de fraude
- Resultados: resultados generados a partir de una predicción de fraude
- Versión de detector: contiene la lógica de predicción de fraudes para un evento en particular

Para obtener más información sobre los componentes utilizados para crear la lógica de detección de fraudes, consulte los [conceptos de Amazon Fraud Detector](#). Antes de empezar a generar predicciones de fraude, asegúrese de haber creado y publicado la versión del detector que contiene su lógica de predicción de fraude. Puede crear y publicar la versión del detector mediante la API o la consola Fraud Detector. Para obtener instrucciones sobre cómo utilizar la consola, consulte [Hora de inicio \(consola\)](#). Para obtener instrucciones sobre el uso de la API, consulte [Crear una versión de detector](#).

## Metadatos de eventos

Los metadatos del evento proporcionan detalles del evento que se está evaluando. Cada evento que desee evaluar debe incluir el valor de cada variable en el tipo de evento asociado a la versión del detector. Además, los metadatos del evento deben incluir lo siguiente:

- **EVENT\_ID**: identificador del evento. Por ejemplo, si tu evento es una transacción en línea, el **EVENT\_ID** puede ser el número de referencia de la transacción proporcionado a tu cliente.

#### Notas importantes sobre **EVENT\_ID**

- Debe ser único para ese evento
- Debe representar información que sea significativa para su empresa
- Debe cumplir con el patrón de expresiones regulares: `^[0-9a-z_-]+$`.
- Debe salvarse. **EVENT\_ID** es la referencia del evento y se usa para realizar operaciones sobre el evento, como eliminarlo.
- No se recomienda añadir una marca de tiempo al **EVENT\_ID**, ya que podría causar problemas cuando desees actualizar el evento más adelante, ya que tendrás que proporcionar exactamente el mismo **EVENT\_ID**.
- **ENTITY\_TYPE**: la entidad que realiza el evento, como un comerciante o un cliente.
- **ENTITY\_ID**: identificador de la entidad que realiza el evento. El **ENTITY\_ID** debe cumplir con el siguiente patrón de expresiones regulares: `^[0-9a-z_-]+$`. Si el **ENTITY\_ID** no está disponible en el momento de la evaluación, introduzca la cadena `unknown`.
- **EVENT\_TIMESTAMP**: la marca de tiempo en la que se produjo el evento. La marca de tiempo debe estar en la norma ISO 8601 en UTC.

## Predicción en tiempo real

Puede evaluar las actividades en línea para detectar fraude en tiempo real llamando a `GetEventPrediction` la API. Usted proporciona información sobre un solo evento en cada solicitud y recibe de forma sincrónica una puntuación del modelo y un resultado en función de la lógica de predicción de fraudes asociada al detector especificado.

## Cómo funciona la predicción de fraudes en tiempo real

La `GetEventPrediction` API usa una versión de detector especificada para evaluar los metadatos del evento proporcionados para el evento. Durante la evaluación, Amazon Fraud Detector primero genera las puntuaciones de los modelos para los modelos que se añaden a la versión del detector y, a continuación, pasa los resultados a las reglas para su evaluación. Las reglas se ejecutan según lo

especificado en el modo de ejecución de reglas (consulte [Crear una versión de detector](#)). Como parte de la respuesta, Amazon Fraud Detector proporciona las puntuaciones de los modelos, así como cualquier resultado asociado a las reglas coincidentes.

## Obtener una predicción de fraude en tiempo real

Para obtener predicciones de fraude en tiempo real, asegúrese de haber creado y publicado un detector que contenga su modelo y reglas de predicción de fraudes, o simplemente un conjunto de reglas.

Puede obtener una predicción de fraude para un evento en tiempo real llamando a la operación de la [GetEventPrediction](#) API mediante la interfaz de línea de AWS comandos (AWSCLI) o uno de los SDK de Amazon Fraud Detector.

Para usar la API, proporciona información de un solo evento con cada solicitud. Como parte de la solicitud, debe especificar qué `detectorId` utilizará Amazon Fraud Detector para evaluar el evento. Puede especificar un `detectorVersionId`. Si no `detectorVersionId` se especifica un, Amazon Fraud Detector utilizará la `ACTIVE` versión del detector.

Si lo desea, puede enviar datos para invocar un SageMaker modelo pasando los datos del campo `externalModelEndpointBlobs`.

## Obtenga una predicción de fraude mediante el AWS SDK for Python (Boto3)

Para generar una predicción de fraude, llama a la `GetEventPrediction` API. En el ejemplo siguiente se asume que ha completado [Parte B: Generar predicciones de fraude](#). Como parte de la respuesta, recibirás una puntuación modelo, así como las reglas coincidentes y los resultados correspondientes. Puedes encontrar ejemplos adicionales de `GetEventPrediction` solicitudes en el [aws-fraud-detector-samples GitHub repositorio](#).

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

fraudDetector.get_event_prediction(
    detectorId = 'sample_detector',
    eventId = '802454d3-f7d8-482d-97e8-c4b6db9a0428',
    eventName = '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'  
}  
)
```

## Predicciones por lotes

Puede utilizar un trabajo de predicción por lotes en Amazon Fraud Detector para obtener predicciones de un conjunto de eventos que no requieren una puntuación en tiempo real. Por ejemplo, puede crear un trabajo de predicciones por lotes para realizar un trabajo sin conexión proof-of-concept o para evaluar retrospectivamente el riesgo de eventos por hora, día o semana.

Puede crear un trabajo de predicción por lotes mediante la [consola de Amazon Fraud Detector](#) o llamando a la operación de [CreateBatchPredictionJob](#) API mediante la interfaz de línea de AWS comandos (AWSCLI) o uno de los SDK de Amazon Fraud Detector.

### Temas

- [Cómo funcionan las predicciones por lotes](#)
- [archivos de entrada y salida](#)
- [Obtener predicciones de lotes](#)
- [Guía sobre las funciones de IAM](#)
- [Obtenga predicciones de fraude por lotes mediante el AWS SDK for Python \(Boto3\)](#)

## Cómo funcionan las predicciones por lotes

La operación de la `CreateBatchPredictionJob` API utiliza una versión de detector especificada para realizar predicciones basadas en los datos proporcionados en un archivo CSV de entrada que se encuentra en un bucket de Amazon S3. La API luego devuelve el archivo CSV resultante a un Amazon S3.

Los trabajos de predicción Batch calculan las puntuaciones del modelo y los resultados de la predicción de la misma manera que la `GetEventPrediction` operación. De manera similar `GetEventPrediction`, para crear un trabajo de predicciones por lotes, primero se crea un tipo de evento, se entrena opcionalmente un modelo y, a continuación, se crea una versión de detector que evalúe los eventos del trabajo por lotes.

El precio de las puntuaciones de riesgo de eventos evaluadas mediante los trabajos de predicción por lotes es el mismo que el precio de las puntuaciones creadas por la `GetEventPrediction` API. Para obtener más información, consulte los [precios de Amazon Fraud Detector](#).

Solo puede ejecutar un trabajo de predicción por lotes a la vez.

## archivos de entrada y salida

El archivo CSV de entrada debe contener encabezados que coincidan con el tipo de evento asociado a la versión del detector seleccionada. El tamaño máximo del archivo de datos de entrada es de 1 GB. La cantidad de eventos variará según el tamaño del evento.

Amazon Fraud Detector crea el archivo de salida en el mismo depósito que el archivo de entrada, a menos que especifique una ubicación diferente para los datos de salida. El archivo de salida contiene los datos originales del archivo de entrada y las siguientes columnas anexadas:

- `MODEL_SCORES`— Detalla las puntuaciones del modelo para el evento de cada modelo asociado a la versión del detector seleccionada.
- `OUTCOMES`— Detalla los resultados del evento evaluados por la versión del detector seleccionada y sus reglas.
- `STATUS`— Indica si el evento se evaluó correctamente. Si el evento no se evaluó correctamente, en esta columna se muestra un código de motivo del error.
- `RULE_RESULTS`— Una lista de todas las reglas que coincidieron, según el modo de ejecución de las reglas.

## Obtener predicciones de lotes

En los siguientes pasos se supone que ya ha creado un tipo de evento, ha entrenado un modelo con ese tipo de evento (opcional) y ha creado una versión de detector para ese tipo de evento.

Para obtener una predicción de lotes

1. Inicie sesión en `AWS Management Console` y abra la consola de Amazon Fraud Detector en <https://console.aws.amazon.com/frauddetector>.
2. En el panel de navegación izquierdo de la consola de Amazon Fraud Detector, elija `Predicciones de Batch` y, a continuación, elija `Nueva predicción de lotes`.
3. En `Nombre del Job`, especifique un nombre para el trabajo de predicción por lotes. Si no especifica un nombre, Amazon Fraud Detector genera aleatoriamente un nombre de trabajo.

4. En Detector, elija el detector para esta predicción de lotes.
5. En la versión Detector, elija la versión del detector para esta predicción de lotes. Puede elegir una versión del detector en cualquier estado. Si su detector tiene una versión de detector en Active estado, esa versión se selecciona automáticamente, pero también puede cambiar esta selección si es necesario.
6. En el rol de IAM, elija o cree un rol que tenga acceso de lectura y escritura a sus buckets de Amazon S3 de entrada y salida. Para obtener más información, consulte [Guía sobre las funciones de IAM](#).

Para obtener predicciones por lotes, la función de IAM que llama a la `CreateBatchPredictionJob` operación debe tener permisos de lectura en el bucket de S3 de entrada y permisos de escritura en el bucket de S3 de salida. Para obtener más información sobre los permisos de bucket, consulte los [ejemplos de políticas de usuario](#) en la Guía del usuario de Amazon S3.

7. En Ubicación de datos de entrada, especifique la ubicación de Amazon S3 de los datos de entrada. Si desea que el archivo de salida esté en un bucket de S3 diferente, seleccione Separar ubicación de datos para la salida y proporcione la ubicación de Amazon S3 para los datos de salida.
8. (Opcional) Cree etiquetas para su trabajo de predicción de lotes.
9. Elija Start (Inicio).

Amazon Fraud Detector crea el trabajo de predicción por lotes y el estado del trabajo es `In progress`. Los tiempos de procesamiento de los trabajos de predicción Batch varían según la cantidad de eventos y la configuración de la versión del detector.

Para detener un trabajo de predicción por lotes que esté en curso, vaya a la página de detalles del trabajo de predicción por lotes, elija Acciones y, a continuación, elija Detener la predicción por lotes. Si detiene un trabajo de predicción por lotes, no recibirá ningún resultado del trabajo.

Cuando el estado del trabajo de predicción por lotes cambie a `Complete`, puede recuperar el resultado del trabajo del bucket de salida designado de Amazon S3. El nombre del archivo de salida está en el formato `batch_prediction_job_name_file_creation_timestamp_output.csv`. Por ejemplo, el archivo de salida de un trabajo denominado `mybatchjob` es `mybatchjob_1611170650_output.csv`.

Para buscar eventos específicos evaluados mediante un trabajo de predicción por lotes, en el panel de navegación izquierdo de la consola de Amazon Fraud Detector, seleccione Buscar predicciones pasadas.

Para eliminar un trabajo de predicción por lotes que se haya completado, vaya a la página de detalles del trabajo de predicción por lotes, elija Acciones y, a continuación, elija Eliminar predicción por lotes.

## Guía sobre las funciones de IAM

Para obtener predicciones por lotes, la función de IAM que llama a la [CreateBatchPredictionJob](#) operación debe tener permisos de lectura en el bucket de S3 de entrada y permisos de escritura en el bucket de S3 de salida. Para obtener más información sobre los permisos de Amazon S3, consulte ejemplos de políticas de usuario en la Guía del usuario de Amazon S3. En la consola de Amazon Fraud Detector, tiene tres opciones para seleccionar una función de IAM para las predicciones de Batch:

1. Cree un rol al crear un nuevo trabajo de predicción de Batch.
2. Seleccione un rol de IAM existente que haya creado anteriormente en la consola de Amazon Fraud Detector. Asegúrese de añadir el `s3:PutObject` permiso al rol antes de realizar este paso.
3. Introduzca un ARN personalizado para un rol de IAM creado anteriormente.

Si aparece un error relacionado con su rol de IAM, verifique lo siguiente:

1. Los Amazon S3 están en la misma región que su detector.
2. El rol de IAM que está utilizando tiene el `s3:GetObject` permiso para su bucket de S3 de entrada y el `s3:PutObject` permiso para su bucket de S3 de salida.
3. El rol de IAM que está utilizando tiene una política de confianza para el director del `frauddetector.amazonaws.com` servicio.

## Obtenga predicciones de fraude por lotes mediante el AWS SDK for Python (Boto3)

El ejemplo siguiente es una respuesta de ejemplo para la [CreateBatchPredictionJob](#) API. Un trabajo de predicción por lotes debe incluir los siguientes recursos existentes: detector, versión del



detector y nombre del tipo de evento. En el ejemplo siguiente se supone que ha creado un tipo de eventos `sample_registration`, un detector `sample_detector` y una versión del detector `1`.

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

fraudDetector.create_batch_prediction_job (
    jobId = 'sample_batch',
    inputPath = 's3://bucket_name/input_file_name.csv',
    outputPath = 's3://bucket_name/',
    eventName = 'sample_registration',
    detectorName = 'sample_detector',
    detectorVersion = '1',
    iamRoleArn = 'arn:aws:iam::*:role/service-role/AmazonFraudDetector-DataAccessRole-
**'
)
```

## Explicaciones de predicción

Las explicaciones de las predicciones proporcionan información sobre cómo cada variable de evento afectó a la puntuación de predicción del fraude de su modelo y se generan automáticamente como parte de la predicción del fraude. Cada predicción de fraude incluye una puntuación de riesgo entre 1 y 1000. Las explicaciones de las predicciones proporcionan detalles sobre la influencia de cada variable del evento en las puntuaciones de riesgo en términos de magnitud (0-5, siendo 5 la máxima) y dirección (puntuación de impulsión más alta o más baja). También puede utilizar las explicaciones de predicción para las siguientes tareas:

- Identificar los principales indicadores de riesgo durante las investigaciones manuales cuando se marca un evento para su revisión.
- Para reducir las causas fundamentales que conducen a predicciones de falsos positivos (por ejemplo, puntuaciones de riesgo altas para eventos legítimos).
- Para analizar los patrones de fraude en los datos de los eventos y detectar sesgos, si los hubiera, en su conjunto de datos.

**⚠ Important**

Las explicaciones de las predicciones se generan automáticamente y están disponibles solo para los modelos entrenados a partir del 30 de junio de 2021. Para recibir explicaciones de predicción para los modelos entrenados antes del 30 de junio de 2021, vuelva a entrenarlos.

Las explicaciones de predicción proporcionan el siguiente conjunto de valores para cada variable de evento que se utilizó para entrenar el modelo.

**Impacto relativo**

Proporciona una referencia visual del impacto de la variable en términos de magnitud en las puntuaciones de predicción del fraude. Los valores de impacto relativo consisten en una calificación por estrellas (0-5, siendo 5 la más alta) y el impacto direccional (aumento/disminuido) del riesgo de fraude.

- Las variables que aumentan el riesgo de fraude se indican con estrellas rojas. Cuanto mayor sea el número de estrellas de color rojo, más aumentará la variable la puntuación de fraude y aumentará la probabilidad de fraude.
- Las variables que reducen el riesgo de fraude se indican con estrellas de color verde. Cuanto mayor sea el número de inicios de color verde, más baja será la variable en la puntuación de riesgo de fraude y disminuirá la probabilidad de fraude.
- El número cero de estrellas para todas las variables indica que ninguna de las variables por sí sola modificó significativamente el riesgo de fraude.

**Valor explicativo bruto**

Proporciona un valor bruto y no interpretado representado como probabilidades logarítmicas del fraude. Estos valores suelen estar entre -10 y +10, pero oscilan entre - infinito y + infinito.

- Un valor positivo indica que la variable hizo subir la puntuación de riesgo.
- Un valor negativo indica que la variable hizo bajar la puntuación de riesgo.

En la consola de Amazon Fraud Detector, los valores explicativos de la predicción se muestran a continuación. Las clasificaciones por estrellas coloreadas y los valores numéricos brutos correspondientes permiten ver fácilmente la influencia relativa entre las 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

## Ver las explicaciones de las predicciones

Tras generar las predicciones de fraude, podrá ver las explicaciones de las predicciones en la consola de Amazon Fraud Detector. Para ver las explicaciones de las predicciones mediante las API del AWS SDK, primero debe llamar a la `ListEventPrediction` API para obtener la marca temporal de la predicción del evento y, a continuación, llamar a la `GetEventPredictionMetadata` API para obtener las explicaciones de las predicciones.

## Consulta las explicaciones de las predicciones con la consola Amazon Fraud Detector

Para ver las explicaciones de las predicciones mediante la consola,

1. Abre la AWS consola e inicia sesión en tu cuenta. Navega hasta Amazon Fraud Detector.
2. En el panel de navegación izquierdo, selecciona `Buscar predicciones anteriores`.
3. Utilice los filtros de propiedad, operador y valor para seleccionar la predicción que desee revisar.

4. En el panel de filtros superior, asegúrese de seleccionar el período de tiempo en el que se generó la predicción que desea revisar.
5. El panel de resultados muestra una lista de todas las predicciones generadas durante el período de tiempo especificado. Haga clic en el ID de evento de la predicción para ver las explicaciones de la predicción.
6. Desplácese hacia abajo hasta el panel de explicaciones de la predicción.
7. Active el botón Mostrar el valor de la explicación de la predicción sin procesar para ver el valor de la explicación de la predicción sin procesar de todas las variables.

## Vea las explicaciones de las predicciones con el AWS SDK para Python (Boto3)

Los siguientes ejemplos muestran ejemplos de solicitudes para ver las explicaciones de las predicciones utilizando `ListEventPredictions` las `GetEventPredictionMetadata` API del AWS SDK.

Ejemplo 1: Obtenga una lista de las predicciones más recientes mediante la **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'
    }
)
```

Ejemplo 2: obtenga una lista de predicciones anteriores para el tipo de evento «registro» mediante la **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'
}
)
```

Ejemplo 3: Obtenga detalles de una predicción anterior para un ID de evento específico, un tipo de evento, un ID de detector y un ID de versión del detector que se generó en el período de tiempo especificado mediante la **GetEventPredictionMetadata** API.

Lo `predictionTimestamp` especificado para esta solicitud se obtiene llamando primero a la `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'
)
```

## Comprender cómo se calculan las explicaciones de las predicciones

Amazon Fraud Detector utiliza [SHAP \(ShapeLey Additive Explanations\)](#) para explicar las predicciones de eventos individuales mediante el cálculo de los valores explicativos sin procesar de cada variable de evento utilizada para el entrenamiento del modelo. El modelo calcula los valores explicativos sin procesar como parte del algoritmo de clasificación al generar las predicciones. Estos valores explicativos sin procesar representan la contribución de cada entrada al logaritmo de las probabilidades de fraude. Los valores explicativos sin procesar (de  $-\infty$  a  $+\infty$ ) se convierten en un valor de impacto relativo (de -5 a +5) mediante un mapeo. El valor de impacto relativo derivado del valor explicativo bruto representa el número de veces que aumentan las probabilidades de fraude (positivo) o legítimo (negativo), lo que facilita la comprensión de las explicaciones de las predicciones.

# Seguridad en Amazon Fraud Detector

En AWS, la seguridad en la nube es la máxima prioridad. Como cliente de AWS, se beneficiará de una arquitectura de red y de centros de datos diseñados para satisfacer los requisitos de seguridad de las organizaciones más exigentes.

La seguridad es una responsabilidad compartida entre AWS y usted. El [modelo de responsabilidad compartida](#) la describe como seguridad de la nube y seguridad en la nube:

- Seguridad de la nube: AWS es responsable de proteger la infraestructura que ejecuta los servicios de AWS en la nube de AWS. AWS también proporciona servicios que puede utilizar de forma segura. Los auditores externos prueban y verifican periódicamente la eficacia de nuestra seguridad como parte de los [Programas de conformidad de AWS](#) . Para obtener más información sobre los programas de conformidad que se aplican a Amazon Fraud Detector, consulte [AWS Services in](#) .
- Seguridad en la nube: su responsabilidad se determina según el servicio de AWS que utilice. También es responsable de otros factores, incluida la confidencialidad de los datos, los requisitos de la empresa y la legislación y la normativa aplicables.

Esta documentación le ayuda a entender cómo aplicar el modelo de responsabilidad compartida al utilizar Amazon Fraud Detector. En los temas siguientes se muestra cómo configurar Amazon Fraud Detector para que cumpla sus objetivos de seguridad y conformidad. También aprenderá a utilizar otros AWS servicios que le ayudan a supervisar y proteger sus recursos de Amazon Fraud Detector.

## Temas

- [Protección de datos en Amazon Fraud Detector](#)
- [Gestión de identidad y acceso para Amazon Fraud Detector](#)
- [Registro y supervisión en Amazon Fraud Detector](#)
- [Validación de conformidad para Amazon Fraud Detector](#)
- [Resiliencia en Amazon Fraud Detector](#)
- [Seguridad de infraestructura en Amazon Fraud Detector](#)

## Protección de datos en Amazon Fraud Detector

El [modelo de](#) se aplica a protección de datos en Amazon Fraud Detector. Como se describe en este modelo, AWS es responsable de proteger la infraestructura global que ejecuta la totalidad de

Nube de AWS. Usted es responsable de mantener el control sobre el contenido alojado en esta infraestructura. Usted también es responsable de las tareas de administración y configuración de seguridad para los Servicios de AWS que utiliza. Para obtener más información sobre la privacidad de los datos, consulte las [Preguntas frecuentes sobre la privacidad de datos](#). Para obtener información sobre la protección de datos en Europa, consulte la publicación de blog [Modelo de responsabilidad compartida y GDPR de AWS](#) en el Blog de seguridad de AWS.

Con fines de protección de datos, recomendamos proteger las credenciales de la cuenta de Cuenta de AWS y configurar cuentas de usuario individuales con AWS IAM Identity Center o AWS Identity and Access Management (IAM). De esta manera, solo se otorgan a cada usuario los permisos necesarios para cumplir sus obligaciones laborales. También recomendamos proteger sus datos de la siguiente manera:

- Utilice autenticación multifactor (MFA) en cada cuenta.
- Utilice SSL/TLS para comunicarse con los recursos de AWS. Se recomienda el uso de TLS 1.2 y recomendamos TLS 1.3.
- Configure la API y el registro de actividad del usuario con AWS CloudTrail.
- Utilice las soluciones de cifrado de AWS, junto con todos los controles de seguridad predeterminados dentro de los Servicios de AWS.
- Utilice servicios de seguridad gestionados avanzados, como Amazon Macie, que lo ayuden a detectar y proteger los datos confidenciales almacenados en Amazon S3.
- Si necesita módulos criptográficos validados FIPS 140-2 al acceder a AWS a través de una interfaz de la línea de comandos o una API, utilice un punto de conexión de FIPS. Para obtener más información sobre los puntos de conexión de FIPS disponibles, consulte [Estándar de procesamiento de la información federal \(FIPS\) 140-2](#).

Se recomienda encarecidamente no introducir nunca información confidencial o sensible, como, por ejemplo, direcciones de correo electrónico de clientes, en etiquetas o campos de formato libre, tales como el campo Nombre. Esto incluye cuando trabajas con Amazon Fraud Detector u otro Servicios de AWS dispositivo mediante la consola, la API o AWS los SDK. AWS CLI Cualquier dato que ingrese en etiquetas o campos de formato libre utilizados para nombres se puede emplear para los registros de facturación o diagnóstico. Si proporciona una URL a un servidor externo, recomendamos encarecidamente que no incluya información de credenciales en la URL a fin de validar la solicitud para ese servidor.

## Cifrado de datos en reposo

Amazon Fraud Detector cifra tus datos en reposo con la clave de cifrado que elijas. Puede elegir una de las siguientes opciones:

- Una [clave AWS KMS propia](#). Si no especifica una clave de cifrado, los datos se cifran con esta clave de forma predeterminada.
- Una [clave KMS](#) gestionada por el cliente. Puede controlar el acceso a la clave KMS administrada por el cliente mediante [políticas clave](#). Para obtener información sobre cómo crear y administrar la clave KMS administrada por el cliente, consulte [Administración de claves](#).

## Cifrado de datos en tránsito

Amazon Fraud Detector copia los datos de tu cuenta y los procesa en un AWS sistema interno. De forma predeterminada, Amazon Fraud Detector utiliza TLS 1.2 con AWS certificados para cifrar los datos en tránsito.

## Administración de claves

Amazon Fraud Detector cifra los datos mediante uno de los dos tipos de claves siguientes:

- Una [clave AWS KMS propia](#). Esta es la opción predeterminada.
- Una [clave KMS](#) gestionada por el cliente.

## Crear una clave KMS gestionada por el cliente

Puede crear una clave de KMS administrada por el cliente mediante la consola AWS KMS o la [CreateKey](#) API. Al crear la clave, asegúrese de:

- Seleccione una clave de KMS de cifrado simétrico gestionada por el cliente, Amazon Fraud Detector no admite claves de KMS asimétricas. Para obtener más información, consulte [Asymmetric Keys AWS KMS en](#) la Guía para desarrolladores del servicio de administración de AWS claves.
- Cree una clave KMS de una sola región. Amazon Fraud Detector no admite claves KMS multirregionales. Para obtener más información, consulte [las claves multirregionales AWS KMS en](#) la Guía para desarrolladores del servicio de administración de AWS claves.



- Proporciona la siguiente [política clave](#) para conceder permisos a Amazon Fraud Detector para usar la clave.

```
{
  "Effect": "Allow",
  "Principal": {
    "Service": "frauddetector.amazonaws.com"
  },
  "Action": [
    "kms:Encrypt",
    "kms:Decrypt",
    "kms:ReEncrypt*",
    "kms:GenerateDataKey*",
    "kms:DescribeKey",
    "kms:CreateGrant",
    "kms:RetireGrant"
  ],
  "Resource": "*"
}
```

Para obtener información sobre las políticas clave, consulte [Uso de políticas clave en AWS KMS](#) en la Guía AWS para desarrolladores del servicio de administración de claves.

## Cifrar datos mediante una clave KMS administrada por el cliente

Utilice la EncryptionKey API [PutKMS](#) de Amazon Fraud Detector para cifrar los datos en reposo de Amazon Fraud Detector mediante la clave de KMS gestionada por el cliente. Puede cambiar la configuración de cifrado en cualquier momento mediante la API. `PutKMSEncryptionKey`

### Notas importantes sobre los datos cifrados

- Los datos generados después de configurar la clave KMS administrada por el cliente están cifrados. Los datos generados antes de configurar la clave KMS administrada por el cliente permanecerán sin cifrar.
- Si se cambia la clave KMS administrada por el cliente, los datos que se cifraron con la configuración de cifrado anterior no se volverán a cifrar.

## Ver datos

Cuando utilizas una clave KMS gestionada por el cliente para cifrar los datos de Amazon Fraud Detector, los datos cifrados con este método no se pueden buscar mediante los filtros del área Buscar predicciones pasadas de la consola de Amazon Fraud Detector. Para garantizar que los resultados de búsqueda sean completos, utilice una o más de las siguientes propiedades para filtrar los resultados:

- ID de evento
- Fecha y hora de la evaluación
- Estado del detector
- Versión de detector
- Versión del modelo
- Tipo de modelo
- Estado de evaluación de la regla
- Modo de ejecución de reglas
- Estado de coincidencia de reglas
- Versión de la regla
- Fuente de datos variable

Si la clave de KMS gestionada por el cliente se ha eliminado o está programada para su eliminación, es posible que sus datos no estén disponibles. Para obtener más información, consulte [Eliminar la clave KMS](#).

## Amazon Fraud Detector y puntos finales de VPC de interfaz () AWS PrivateLink

Puede establecer una conexión privada entre su VPC y Amazon Fraud Detector creando un punto final de interfaz de VPC. Los puntos de enlace de la interfaz funcionan con una tecnología que le permite acceder de forma privada a las API de Amazon Fraud Detector sin una puerta de enlace a Internet, un dispositivo NAT, una conexión VPN o una conexión AWS Direct Connect. [AWS PrivateLink](#) Las instancias de su VPC no necesitan direcciones IP públicas para comunicarse con las API de Amazon Fraud Detector. El tráfico entre tu VPC y Amazon Fraud Detector no sale de la red de Amazon.

Cada punto de conexión de la interfaz está representado por una o más [interfases de red elásticas](#) en las subredes.

Para obtener más información, consulte [Interface VPC Endpoints \(AWS PrivateLink\)](#) en la Guía del usuario de Amazon VPC.

## Consideraciones sobre los puntos de conexión VPC de Amazon Fraud Detector

Antes de configurar un punto de enlace de VPC de interfaz para Amazon Fraud Detector, asegúrese de revisar las [propiedades y limitaciones del punto de enlace de interfaz](#) en la Guía del usuario de Amazon VPC.

Amazon Fraud Detector permite realizar llamadas a todas sus acciones de API desde su VPC.

Amazon Fraud Detector admite las políticas de puntos finales de VPC. De forma predeterminada, se permite el acceso total a Amazon Fraud Detector a través del punto de conexión. Para obtener más información, consulte [Control del acceso a los servicios con puntos de conexión de VPC](#) en la Guía del usuario de Amazon VPC.

## Creación de un punto final de VPC de interfaz para Amazon Fraud Detector

Puede crear un punto de conexión de VPC para el servicio Amazon Fraud Detector mediante la consola Amazon VPC o el `awscli`. Para obtener más información, consulte [Creación de un punto de conexión de interfaz](#) en la Guía del usuario de Amazon VPC.

Cree un punto de conexión de VPC para Amazon Fraud Detector con el siguiente nombre de servicio:

- `com.amazonaws.region.frauddetector`

Si habilitas el DNS privado para el punto de conexión, puedes realizar solicitudes de API a Amazon Fraud Detector utilizando su nombre de DNS predeterminado para la región, por ejemplo `frauddetector.us-east-1.amazonaws.com`.

Para obtener más información, consulte [Acceso a un servicio a través de un punto de conexión de interfaz](#) en la Guía del usuario de Amazon VPC.

## Creación de una política de puntos finales de VPC para Amazon Fraud Detector

Puede crear una política para los puntos de enlace de la VPC de interfaz para Amazon Fraud Detector para especificar lo siguiente:

- La entidad principal que puede realizar acciones
- Las acciones que se pueden realizar
- Los recursos en los que se pueden llevar a cabo las acciones

Para obtener más información, consulte [Controlar el acceso a servicios con puntos de conexión de VPC](#) en la Guía del usuario de Amazon VPC.

El siguiente ejemplo de política de punto final de VPC especifica que todos los usuarios que tienen acceso al punto final de la interfaz de VPC pueden acceder al detector de Amazon Fraud Detector denominado `my_detector`

```
{
  "Statement": [
    {
      "Action": "frauddetector:*Detector",
      "Effect": "Allow",
      "Resource": "arn:aws:frauddetector:us-east-1:123456789012:detector/
my_detector",
      "Principal": "*"
    }
  ]
}
```

En este ejemplo, los siguientes se deniegan:

- Otras acciones de la API Amazon Fraud Detector
- Invocar la API de Amazon Fraud Detector `GetEventPrediction`

#### Note

En este ejemplo, los usuarios aún pueden realizar otras acciones de la API de Amazon Fraud Detector desde fuera de la VPC. Para obtener información acerca de cómo restringir las llamadas a la API a estos desde la VPC, consulte [Políticas basadas en la identidad de Amazon Fraud Detector](#).

## Optar por no utilizar sus datos para mejorar el servicio

Los datos históricos de eventos que proporciona para entrenar modelos y generar predicciones se utilizan únicamente para proporcionar y mantener su servicio. Estos datos también se pueden utilizar para mejorar la calidad de Amazon Fraud Detector. Su confianza, privacidad y seguridad de su contenido son nuestra máxima prioridad y garantizan que nuestro uso cumpla con nuestros compromisos con usted. Consulte las [preguntas frecuentes sobre privacidad de datos](#) para obtener más información.

Puede optar por no utilizar los datos de sus eventos para desarrollar o mejorar la calidad de Amazon Fraud Detector visitando la página de [políticas de exclusión de los servicios de IA](#) en la Guía del usuario de AWS Organizations y siguiendo el proceso que se explica allí.

### Note

AWS Organizations deberá gestionar sus cuentas de AWS de forma centralizada para que pueda utilizar la política de exclusión voluntaria. Si aún no ha creado una organización para sus cuentas de AWS, visite la página [Creación y administración de una organización](#) y siga el proceso que se explica allí.

## Gestión de identidad y acceso para Amazon Fraud Detector

AWS Identity and Access Management (IAM) es un Servicio de AWS que ayuda a los administradores a controlar de forma segura el acceso a los recursos de AWS. Los administradores de IAM controlan quién puede autenticarse (iniciar sesión) y quién puede autorizarse (tener permisos) para usar los recursos de Amazon Fraud Detector. IAM es un servicio de Servicio de AWS que se puede utilizar sin cargo adicional.

### Temas

- [Público](#)
- [Autenticación con identidades](#)
- [Administración de acceso mediante políticas](#)
- [Cómo funciona Amazon Fraud Detector con IAM](#)
- [Ejemplos de políticas basadas en la identidad de Amazon Fraud Detector](#)
- [Prevención del suplente confuso](#)

- [Solución de problemas de identidad y acceso a Amazon Fraud Detector](#)

## Público

La forma de usar AWS Identity and Access Management (IAM) varía según el trabajo que realices en Amazon Fraud Detector.

**Usuario del servicio:** si utilizas el servicio Amazon Fraud Detector para realizar tu trabajo, el administrador te proporcionará las credenciales y los permisos que necesitas. A medida que utilices más funciones de Amazon Fraud Detector para realizar tu trabajo, es posible que necesites permisos adicionales. Entender cómo se administra el acceso puede ayudarte a solicitar los permisos correctos al administrador. Si no puede acceder a una función de Amazon Fraud Detector, consulte [Solución de problemas de identidad y acceso a Amazon Fraud Detector](#).

**Administrador de servicios:** si está a cargo de los recursos de Amazon Fraud Detector en su empresa, probablemente tenga acceso completo a Amazon Fraud Detector. Es tu trabajo determinar a qué funciones y recursos de Amazon Fraud Detector deben acceder los usuarios del servicio. Luego, debe enviar solicitudes a su administrador de IAM para cambiar los permisos de los usuarios de su servicio. Revise la información de esta página para conocer los conceptos básicos de IAM. Para obtener más información sobre cómo su empresa puede utilizar IAM con Amazon Fraud Detector, consulte [Cómo funciona Amazon Fraud Detector con IAM](#).

**Administrador de IAM:** si es administrador de IAM, puede que le interese obtener más información sobre cómo redactar políticas para gestionar el acceso a Amazon Fraud Detector. Para ver ejemplos de políticas basadas en la identidad de Amazon Fraud Detector que puedes usar en IAM, consulta [Ejemplos de políticas basadas en la identidad de Amazon Fraud Detector](#)

## Autenticación con identidades

La autenticación es la manera de iniciar sesión en AWS mediante credenciales de identidad. Debe estar autenticado (haber iniciado sesión en AWS) como Usuario raíz de la cuenta de AWS, como un usuario de IAM o asumiendo un rol de IAM.

Puede iniciar sesión en AWS como una identidad federada mediante las credenciales proporcionadas a través de una fuente de identidad de AWS IAM Identity Center. Los usuarios (de IAM Identity Center), la autenticación de inicio de sesión único de su empresa y sus credenciales de Google o Facebook son ejemplos de identidades federadas. Al iniciar sesión como una identidad federada, su administrador habrá configurado previamente la federación de identidades mediante

roles de IAM. Cuando accede a AWS mediante la federación, está asumiendo un rol de forma indirecta.

Según el tipo de usuario que sea, puede iniciar sesión en la AWS Management Console o en el portal de acceso a AWS. Para obtener más información sobre el inicio de sesión en AWS, consulte [Cómo iniciar sesión en su Cuenta de AWS](#) en la Guía del usuario de AWS Sign-In.

Si accede a AWS mediante programación, AWS proporciona un kit de desarrollo de software (SDK) y una interfaz de la línea de comandos (CLI) para firmar criptográficamente las solicitudes mediante el uso de las credenciales. Si no usa las herramientas de AWS, debe firmar usted mismo las solicitudes. Para obtener más información sobre el método recomendado para la firma de solicitudes, consulte [Firma de solicitudes API de AWS](#) en la Guía del usuario de IAM.

Independientemente del método de autenticación que use, es posible que deba proporcionar información de seguridad adicional. Por ejemplo, AWS le recomienda el uso de la autenticación multifactor (MFA) para aumentar la seguridad de su cuenta. Para obtener más información, consulte [Autenticación multifactor](#) en la Guía del usuario de AWS Single Sign-On y [Uso de la autenticación multifactor \(MFA\) en AWS](#) en la Guía del usuario de IAM.

## Usuario raíz de cuenta de Cuenta de AWS

Cuando se crea una cuenta de Cuenta de AWS, se comienza con una identidad de inicio de sesión que tiene acceso completo a todos los servicios y recursos de Servicios de AWS de la cuenta. Esta identidad recibe el nombre de usuario raíz de la Cuenta de AWS y se accede a ella iniciando sesión con el email y la contraseña que utilizó para crear la cuenta. Recomendamos encarecidamente que no utilice el usuario raíz para sus tareas diarias. Proteja las credenciales del usuario raíz y utilícelas solo para las tareas que solo el usuario raíz pueda realizar. Para ver la lista completa de las tareas que requieren que inicie sesión como usuario raíz, consulte [Tareas que requieren credenciales de usuario raíz](#) en la Guía del usuario de IAM.

## Usuarios y grupos

Un [usuario de IAM](#) es una identidad en su Cuenta de AWS que dispone de permisos específicos para una sola persona o aplicación. Siempre que sea posible, recomendamos emplear credenciales temporales, en lugar de crear usuarios de IAM que tengan credenciales de larga duración como contraseñas y claves de acceso. No obstante, si tiene casos de uso específicos que requieran credenciales de larga duración con usuarios de IAM, recomendamos rotar las claves de acceso. Para más información, consulte [Rotar las claves de acceso periódicamente para casos de uso que requieran credenciales de larga duración](#) en la Guía del Usuario de IAM.

Un [grupo de IAM](#) es una identidad que especifica un conjunto de usuarios de IAM. No puede iniciar sesión como grupo. Puede usar los grupos para especificar permisos para varios usuarios a la vez. Los grupos facilitan la administración de los permisos de grandes conjuntos de usuarios. Por ejemplo, podría tener un grupo cuyo nombre fuese IAMAdmins y conceder permisos a dicho grupo para administrar los recursos de IAM.

Los usuarios son diferentes de los roles. Un usuario se asocia exclusivamente a una persona o aplicación, pero la intención es que cualquier usuario pueda asumir un rol que necesite. Los usuarios tienen credenciales permanentes a largo plazo y los roles proporcionan credenciales temporales. Para más información, consulte [Cuándo crear un usuario de IAM \(en lugar de un rol\)](#) en la Guía del Usuario de IAM.

## Roles de IAM

Un [rol de IAM](#) es una identidad de tu cuenta de Cuenta de AWS que dispone de permisos específicos. Es similar a un usuario de IAM, pero no está asociado a una determinada persona. Puede asumir temporalmente un rol de IAM en la AWS Management Console [cambiando de roles](#). Puede asumir un rol llamando a una operación de AWS CLI o de la API de AWS, o utilizando una URL personalizada. Para más información sobre los métodos para el uso de roles, consulte [Uso de roles de IAM](#) en la Guía del Usuario de IAM.

Los roles de IAM con credenciales temporales son útiles en las siguientes situaciones:

- **Acceso de usuario federado:** para asignar permisos a una identidad federada, puede crear un rol y definir sus permisos. Cuando se autentica una identidad federada, se asocia la identidad al rol y se le conceden los permisos define el rol. Para obtener información acerca de roles para federación, consulte [Creación de un rol para un proveedor de identidades de terceros](#) en la Guía del Usuario de IAM. Si utiliza el IAM Identity Center, debe configurar un conjunto de permisos. El IAM Identity Center correlaciona el conjunto de permisos con un rol en IAM para controlar a qué pueden acceder las identidades después de autenticarse. Para obtener información acerca de los conjuntos de permisos, consulte [Conjuntos de permisos](#) en la Guía del usuario de AWS IAM Identity Center.
- **Permisos de usuario de IAM temporales:** un usuario de IAM puede asumir un rol de IAM para recibir temporalmente permisos distintos que le permitan realizar una tarea concreta.
- **Acceso entre cuentas:** puede utilizar un rol de IAM para permitir que alguien (una entidad principal de confianza) de otra cuenta acceda a los recursos de la cuenta. Los roles son la forma principal de conceder acceso entre cuentas. No obstante, con algunos Servicios de AWS se puede asociar una política directamente a un recurso (en lugar de utilizar un rol como representante). Para



obtener información sobre la diferencia entre los roles y las políticas basadas en recursos para el acceso entre cuentas, consulte [Cómo los roles de IAM difieren de las políticas basadas en recursos](#) en la Guía del usuario de IAM.

- **Acceso entre servicios:** algunos servicios de Servicios de AWS utilizan características de otros Servicios de AWS. Por ejemplo, cuando realiza una llamada en un servicio, es común que ese servicio ejecute aplicaciones en Amazon EC2 o almacene objetos en Amazon S3. Es posible que un servicio haga esto usando los permisos de la entidad principal, usando un rol de servicio o usando un rol vinculado a servicios.
- **Reenviar sesiones de acceso (FAS):** cuando utiliza un rol o un usuario de IAM para llevar a cabo acciones en AWS, se le considera una entidad principal. Cuando utiliza algunos servicios, es posible que realice una acción que desencadene otra acción en un servicio diferente. FAS utiliza los permisos de la entidad principal para llamar a un Servicio de AWS, combinados con el Servicio de AWS solicitante para realizar solicitudes a servicios posteriores. Las solicitudes de FAS solo se realizan cuando un servicio recibe una solicitud que requiere interacciones con otros Servicios de AWS o recursos para completarse. En este caso, debe tener permisos para realizar ambas acciones. Para obtener información sobre las políticas a la hora de realizar solicitudes de FAS, consulte [Reenviar sesiones de acceso](#).
- **Rol de servicio:** un rol de servicio es un [rol de IAM](#) que adopta un servicio para realizar acciones en su nombre. Un administrador de IAM puede crear, modificar y eliminar un rol de servicio desde IAM. Para obtener más información, consulte [Creación de un rol para delegar permisos a un Servicio de AWS](#) en la Guía del usuario de IAM.
- **Rol vinculado a servicios:** un rol vinculado a servicios es un tipo de rol de servicio que está vinculado a un Servicio de AWS. El servicio puede asumir el rol para realizar una acción en su nombre. Los roles vinculados a servicios aparecen en la Cuenta de AWS y son propiedad del servicio. Un administrador de IAM puede ver, pero no editar, los permisos de los roles vinculados a servicios.
- **Aplicaciones que se ejecutan en Amazon EC2:** puede utilizar un rol de IAM que le permita administrar credenciales temporales para las aplicaciones que se ejecutan en una instancia de EC2 y realizan solicitudes a la AWS CLI o a la API de AWS. Es preferible hacerlo de este modo a almacenar claves de acceso en la instancia EC2. Para asignar un rol de AWS a una instancia de EC2 y ponerla a disposición de todas las aplicaciones, cree un perfil de instancia asociado a la instancia. Un perfil de instancia contiene el rol y permite a los programas que se ejecutan en la instancia EC2 obtener credenciales temporales. Para obtener más información, consulte [Uso de un rol de IAM para conceder permisos a aplicaciones que se ejecutan en instancias de Amazon EC2](#) en la Guía del usuario de IAM.

Para obtener información sobre el uso de los roles de IAM, consulte [Cuándo crear un rol de IAM \(en lugar de un usuario\)](#) en la Guía del Usuario de IAM.

## Administración de acceso mediante políticas

Para controlar el acceso en AWS, se crean políticas y se adjuntan a identidades o recursos de AWS. Una política es un objeto de AWS que, cuando se asocia a una identidad o un recurso, define sus permisos. AWS evalúa estas políticas cuando una entidad principal (sesión de rol, usuario o usuario raíz) realiza una solicitud. Los permisos en las políticas determinan si la solicitud se permite o se deniega. La mayoría de las políticas se almacenan en AWS como documentos JSON. Para obtener más información sobre la estructura y el contenido de los documentos de política JSON, consulte [Información general de las políticas JSON](#) en la Guía del Usuario de IAM.

Los administradores pueden utilizar las políticas JSON de AWS para especificar quién tiene acceso a qué. Es decir, qué entidad principal puede realizar acciones en qué recursos y en qué condiciones.

De forma predeterminada, los usuarios y los roles no tienen permisos. Para conceder permiso a los usuarios para realizar acciones en los recursos que necesiten, un administrador de IAM puede crear políticas de IAM. A continuación, el administrador puede añadir las políticas de IAM a roles y los usuarios pueden asumirlos.

Las políticas de IAM definen permisos para una acción independientemente del método que se utilice para realizar la operación. Por ejemplo, suponga que dispone de una política que permite la acción `iam:GetRole`. Un usuario con dicha política puede obtener información del usuario de la AWS Management Console, AWS CLI o la API de AWS.

### Políticas basadas en identidades

Las políticas basadas en identidades son documentos de políticas de permisos JSON que puede adjuntar a una identidad, como un usuario, un grupo de usuarios o un rol de IAM. Estas políticas controlan qué acciones pueden realizar los usuarios y los roles, en qué recursos y en qué condiciones. Para obtener más información sobre cómo crear una política basada en identidad, consulte [Creación de políticas de IAM](#) en la Guía del usuario de IAM.

Las políticas basadas en identidades pueden clasificarse además como políticas insertadas o políticas administradas. Las políticas insertadas se integran directamente en un único usuario, grupo o rol. Las políticas administradas son políticas independientes que puede asociar a varios usuarios, grupos y roles de su Cuenta de AWS. Las políticas administradas incluyen las políticas administradas de AWS y las políticas administradas por el cliente. Para obtener más información sobre cómo elegir

una política administrada o una política insertada, consulte [Elegir entre políticas administradas y políticas insertadas](#) en la Guía del usuario de IAM.

## Políticas basadas en recursos

Las políticas basadas en recursos son documentos de política JSON que se asocian a un recurso. Ejemplos de políticas basadas en recursos son las políticas de confianza de roles de IAM y las políticas de bucket de Amazon S3. En los servicios que admiten políticas basadas en recursos, los administradores de servicios pueden utilizarlos para controlar el acceso a un recurso específico. Para el recurso al que se asocia la política, la política define qué acciones puede realizar una entidad principal especificada en ese recurso y en qué condiciones. Debe [especificar una entidad principal](#) en una política en función de recursos. Las entidades principales pueden incluir cuentas, usuarios, roles, usuarios federados o servicios de Servicios de AWS.

Las políticas basadas en recursos son políticas insertadas que se encuentran en ese servicio. No se puede utilizar políticas de IAM administradas por AWS en una política basada en recursos.

## Listas de control de acceso (ACL)

Las listas de control de acceso (ACL) controlan qué entidades principales (miembros de cuentas, usuarios o roles) tienen permisos para acceder a un recurso. Las ACL son similares a las políticas basadas en recursos, aunque no utilizan el formato de documento de políticas JSON.

Amazon S3, AWS WAF y Amazon VPC son ejemplos de servicios que admiten las ACL. Para obtener más información sobre las ACL, consulte [Información general de Lista de control de acceso \(ACL\)](#) en la Guía para Desarrolladores de Amazon Simple Storage Service.

## Otros tipos de políticas

AWS admite otros tipos de políticas adicionales menos frecuentes. Estos tipos de políticas pueden establecer el máximo de permisos que los tipos de políticas más frecuentes le conceden.

- **Límites de permisos:** un límite de permisos es una característica avanzada que le permite establecer los permisos máximos que una política basada en identidad puede conceder a una entidad de IAM (usuario o rol de IAM). Puede establecer un límite de permisos para una entidad. Los permisos resultantes son la intersección de las políticas basadas en la identidad de la entidad y los límites de permisos. Las políticas basadas en recursos que especifiquen el usuario o rol en el campo `Principal` no estarán restringidas por el límite de permisos. Una denegación explícita en cualquiera de estas políticas anulará el permiso. Para obtener más información sobre los límites

de los permisos, consulte [Límites de permisos para las entidades de IAM](#) en la Guía del Usuario de IAM.

- Políticas de control de servicio (SCP): las SCP son políticas de JSON que especifican los permisos máximos de una organización o una unidad organizativa en AWS Organizations. AWS Organizations es un servicio que le permite agrupar y administrar de manera centralizada varias cuentas de Cuentas de AWS que posea su empresa. Si habilita todas las características en una empresa, entonces podrá aplicar políticas de control de servicio (SCP) a una o todas sus cuentas. Una SCP limita los permisos para las entidades de las cuentas de miembros, incluido cada Usuario raíz de la cuenta de AWS. Para obtener más información acerca de Organizations y las SCP, consulte [Funcionamiento de las SCP](#) en la Guía del usuario de AWS Organizations.
- Políticas de sesión: las políticas de sesión son políticas avanzadas que se pasan como parámetro cuando se crea una sesión temporal mediante programación para un rol o un usuario federado. Los permisos de la sesión resultantes son la intersección de las políticas basadas en identidades del rol y las políticas de la sesión. Los permisos también pueden proceder de una política en función de recursos. Una denegación explícita en cualquiera de estas políticas anulará el permiso. Para más información, consulte [Políticas de sesión](#) en la Guía del Usuario de IAM.

## Varios tipos de políticas

Cuando se aplican varios tipos de políticas a una solicitud, los permisos resultantes son más complicados de entender. Para obtener información sobre cómo AWS decide si permite o no una solicitud cuando hay varios tipos de políticas implicados, consulte [Lógica de evaluación de políticas](#) en la Guía del usuario de IAM.

## Cómo funciona Amazon Fraud Detector con IAM

Antes de utilizar IAM para gestionar el acceso a Amazon Fraud Detector, debe saber qué funciones de IAM están disponibles para su uso con Amazon Fraud Detector. Para obtener una visión general de cómo Amazon Fraud Detector y otros AWS servicios funcionan con IAM, consulte [AWS Servicios que funcionan con IAM](#) en la Guía del usuario de IAM.

### Temas

- [Políticas basadas en la identidad de Amazon Fraud Detector](#)
- [Políticas basadas en recursos de Amazon Fraud Detector](#)
- [Autorización basada en las etiquetas de Amazon Fraud Detector](#)
- [Funciones de IAM de Amazon Fraud Detector](#)

## Políticas basadas en la identidad de Amazon Fraud Detector

Con las políticas basadas en identidades de IAM, puede especificar las acciones y los recursos permitidos o denegados, así como las condiciones en las que se permiten o deniegan las acciones. Amazon Fraud Detector admite acciones, recursos y claves de condición específicos. Para obtener información sobre todos los elementos que utiliza en una política JSON, consulte [Referencia de los elementos de las políticas JSON de IAM](#) en la Guía del usuario de IAM.

Para empezar a utilizar Amazon Fraud Detector, te recomendamos crear un usuario con acceso restringido a las operaciones de Amazon Fraud Detector y con los permisos necesarios. Puede añadir otros permisos según sea necesario. Las siguientes políticas proporcionan el permiso necesario para utilizar Amazon Fraud Detector: `AmazonFraudDetectorFullAccessPolicy` y `AmazonS3FullAccess`. Para obtener más información sobre cómo configurar Amazon Fraud Detector mediante estas políticas, consulte [Configurar Amazon Fraud Detector](#).

### Acciones

Los administradores pueden utilizar las políticas JSON de AWS para especificar quién tiene acceso a qué. Es decir, qué entidad principal puede realizar acciones en qué recursos y en qué condiciones.

El elemento `Action` de una política JSON describe las acciones que puede utilizar para permitir o denegar el acceso en una política. Las acciones de la política generalmente tienen el mismo nombre que la operación de API de AWS asociada. Hay algunas excepciones, como acciones de solo permiso que no tienen una operación de API coincidente. También hay algunas operaciones que requieren varias acciones en una política. Estas acciones adicionales se denominan acciones dependientes.

Incluya acciones en una política para conceder permisos y así llevar a cabo la operación asociada.

Las acciones políticas en Amazon Fraud Detector utilizan el siguiente prefijo antes de la acción: `frauddetector:`. Por ejemplo, para crear una regla con la operación de la `CreateRule` API de Amazon Fraud Detector, debes incluir la `frauddetector:CreateRule` acción en la política. Las instrucciones de la política deben incluir un elemento `Action` o un elemento `NotAction`. Amazon Fraud Detector define su propio conjunto de acciones que describen las tareas que puede realizar con este servicio.

Para especificar varias acciones en una única instrucción, sepárelas con comas del siguiente modo:

```
"Action": [
```

```
"frauddetector:action1",  
"frauddetector:action2"
```

Puede utilizar caracteres comodín para especificar varias acciones (\*). Por ejemplo, para especificar todas las acciones que comiencen con la palabra `Describe`, incluya la siguiente acción:

```
"Action": "frauddetector:Describe*"
```

Para ver una lista de las acciones de Amazon Fraud Detector, consulte [Acciones definidas por Amazon Fraud Detector](#) en la Guía del usuario de IAM.

## Recursos

Los administradores pueden utilizar las políticas JSON de AWS para especificar quién tiene acceso a qué. Es decir, qué entidad principal puede realizar acciones en qué recursos y en qué condiciones.

El elemento `Resource` de la política JSON especifica el objeto u objetos a los que se aplica la acción. Las instrucciones deben contener un elemento `Resource` o `NotResource`. Como práctica recomendada, especifique un recurso utilizando el [Nombre de recurso de Amazon \(ARN\)](#). Puede hacerlo para acciones que admitan un tipo de recurso específico, conocido como permisos de nivel de recurso.

Para las acciones que no admiten permisos de nivel de recurso, como las operaciones de descripción, utilice un carácter comodín (\*) para indicar que la instrucción se aplica a todos los recursos.

```
"Resource": "*"
```

[Los tipos de recursos definidos por Amazon Fraud Detector](#) muestran todos los ARN de recursos de Amazon Fraud Detector.

Por ejemplo, para especificar el `my_detector` detector en la sentencia, utilice el siguiente ARN:

```
"Resource": "arn:aws:frauddetector:us-east-1:123456789012:detector/my_detector"
```

Para obtener más información acerca del formato de los ARN, consulte [Nombres de recursos de Amazon \(ARN\) y espacios de nombres de servicios de AWS](#).

Para especificar todos los detectores que pertenecen a una cuenta específica, utilice el comodín (\*):

```
"Resource": "arn:aws:frauddetector:us-east-1:123456789012:detector/*"
```

Algunas acciones de Amazon Fraud Detector, como las de creación de recursos, no se pueden realizar en un recurso específico. En dichos casos, debe utilizar el carácter comodín (\*).

```
"Resource": "*"
```

Para ver una lista de los tipos de recursos de Amazon Fraud Detector y sus ARN, consulte [Recursos definidos por Amazon Fraud Detector](#) en la Guía del usuario de IAM. Para saber qué acciones puede especificar el ARN de cada recurso, consulte [Acciones definidas por Amazon Fraud Detector](#).

### Claves de condición

Los administradores pueden utilizar las políticas JSON de AWS para especificar quién tiene acceso a qué. Es decir, qué entidad principal puede realizar acciones en qué recursos y en qué condiciones.

El elemento `Condition` (o bloque de `Condition`) permite especificar condiciones en las que entra en vigor una instrucción. El elemento `Condition` es opcional. Puede crear expresiones condicionales que utilicen [operadores de condición](#), tales como igual o menor que, para que la condición de la política coincida con los valores de la solicitud.

Si especifica varios elementos de `Condition` en una instrucción o varias claves en un único elemento de `Condition`, AWS las evalúa mediante una operación lógica AND. Si especifica varios valores para una única clave de condición, AWS evalúa la condición con una operación OR lógica. Se deben cumplir todas las condiciones antes de que se concedan los permisos de la instrucción.

También puede utilizar variables de marcador de posición al especificar condiciones. Por ejemplo, puede conceder un permiso de usuario de IAM para acceder a un recurso solo si está etiquetado con su nombre de usuario de IAM. Para más información, consulte [Elementos de la política de IAM: variables y etiquetas](#) en la Guía del usuario de IAM.

AWS admite claves de condición globales y claves de condición específicas del servicio. Para ver todas las claves de condición globales de AWS, consulte [Claves de contexto de condición globales de AWS](#) en la Guía del Usuario de IAM.

Amazon Fraud Detector define su propio conjunto de claves de condición y también admite el uso de algunas claves de condición globales. Para ver todas las claves de condición globales de AWS, consulte [Claves de contexto de condición globales de AWS](#) en la Guía del usuario de IAM.



Para ver una lista de claves de condición de Amazon Fraud Detector, consulta [Claves de condición de Amazon Fraud Detector](#) en la Guía del usuario de IAM. Para saber qué acciones y recursos puede utilizar una clave de condición, consulte [Acciones definidas por Amazon Fraud Detector](#).

## Ejemplos

Para ver ejemplos de políticas basadas en la identidad de Amazon Fraud Detector, consulte [Ejemplos de políticas basadas en la identidad de Amazon Fraud Detector](#)

## Políticas basadas en recursos de Amazon Fraud Detector

Amazon Fraud Detector no admite políticas basadas en recursos.

## Autorización basada en las etiquetas de Amazon Fraud Detector

Puedes adjuntar etiquetas a los recursos de Amazon Fraud Detector o pasar las etiquetas en una solicitud a Amazon Fraud Detector. Para controlar el acceso en función de etiquetas, debe proporcionar información de las etiquetas en el [elemento de condición](#) de una política utilizando las claves de condición `aws:ResourceTag/key-name`, `aws:RequestTag/key-name` o `aws:TagKeys`.

## Funciones de IAM de Amazon Fraud Detector

Un [rol de IAM](#) es una entidad de la cuenta de AWS que dispone de permisos específicos.

## Uso de credenciales temporales con Amazon Fraud Detector

Puede utilizar credenciales temporales para iniciar sesión con federación, asumir un rol de IAM o asumir un rol de acceso entre cuentas. Las credenciales de seguridad temporales se obtienen mediante una llamada a operaciones de la API de AWS STS, como [AssumeRole](#) o [GetFederationToken](#).

Amazon Fraud Detector admite el uso de credenciales temporales.

## Roles vinculados al servicio

Los [roles vinculados a servicios](#) permiten a los servicios de AWS obtener acceso a los recursos de otros servicios para completar una acción en su nombre. Los roles vinculados a servicios aparecen en la cuenta de IAM y son propiedad del servicio. Un administrador de IAM puede ver, pero no editar, los permisos de los roles vinculados a servicios.

Amazon Fraud Detector no admite funciones vinculadas a servicios.



## Roles de servicio

Esta característica permite que un servicio asuma un [rol de servicio](#) en su nombre. Este rol permite que el servicio obtenga acceso a los recursos de otros servicios para completar una acción en su nombre. Los roles de servicio aparecen en su cuenta de y son propiedad de la cuenta. Esto significa que un administrador puede cambiar los permisos de este rol. Sin embargo, hacerlo podría deteriorar la funcionalidad del servicio.

Amazon Fraud Detector apoya las funciones de servicio.

## Ejemplos de políticas basadas en la identidad de Amazon Fraud Detector

De forma predeterminada, los usuarios y los roles de IAM no tienen permiso para crear o modificar los recursos de Amazon Fraud Detector. Tampoco pueden realizar tareas mediante la AWS Management Console, la AWS CLI o la API de AWS. Un administrador debe crear políticas de IAM que concedan permisos a los usuarios y a los roles para realizar operaciones de la API concretas en los recursos especificados que necesiten. El administrador debe adjuntar esas políticas a los usuarios o grupos que necesiten esos permisos.

Para obtener información acerca de cómo crear una política basada en identidad de IAM con estos documentos de políticas JSON de ejemplo, consulte [Creación de políticas en la pestaña JSON](#) en la Guía del usuario de IAM.

### Temas

- [Prácticas recomendadas relativas a políticas](#)
- [Política gestionada por AWS \(predefinida\) para Amazon Fraud Detector](#)
- [Cómo permitir a los usuarios consultar sus propios permisos](#)
- [Permita el acceso total a los recursos de Amazon Fraud Detector](#)
- [Permitir el acceso de solo lectura a los recursos de Amazon Fraud Detector](#)
- [Permitir el acceso a un recurso específico](#)
- [Permita el acceso a recursos específicos cuando utilice la API de modo dual](#)
- [Limitar el acceso en función de las etiquetas](#)

## Prácticas recomendadas relativas a políticas

Las políticas basadas en la identidad determinan si alguien puede crear recursos de Amazon Fraud Detector de su cuenta, acceder a ellos o eliminarlos. Estas acciones pueden generar costes

adicionales para su Cuenta de AWS. Siga estas directrices y recomendaciones al crear o editar políticas basadas en identidades:

- Comience con las políticas administradas de AWS y continúe con los permisos de privilegio mínimo: a fin de comenzar a conceder permisos a los usuarios y las cargas de trabajo, utilice las políticas administradas de AWS, que conceden permisos para muchos casos de uso comunes. Están disponibles en su Cuenta de AWS. Se recomienda definir políticas administradas por el cliente de AWS específicas para los casos de uso a fin de reducir aún más los permisos. Con el fin de obtener más información, consulte las [políticas administradas por AWS](#) o las [políticas administradas por AWS para funciones de trabajo](#) en la Guía del usuario de IAM.
- Aplique permisos de privilegio mínimo: cuando establezca permisos con políticas de IAM, conceda solo los permisos necesarios para realizar una tarea. Para ello, debe definir las acciones que se pueden llevar a cabo en determinados recursos en condiciones específicas, también conocidos como permisos de privilegios mínimos. Con el fin de obtener más información sobre el uso de IAM para aplicar permisos, consulte [Políticas y permisos en IAM](#) en la Guía de usuario de IAM.
- Utilice condiciones en las políticas de IAM para restringir aún más el acceso: puede agregar una condición a sus políticas para limitar el acceso a las acciones y los recursos. Por ejemplo, puede escribir una condición de políticas para especificar que todas las solicitudes deben enviarse utilizando SSL. También puede usar condiciones para conceder acceso a acciones de servicios si se emplean a través de un Servicio de AWS determinado, como por ejemplo AWS CloudFormation. Para obtener más información, consulte [Elementos de la política de JSON de IAM: Condición](#) en la Guía del usuario de IAM.
- Utilice el analizador de acceso de IAM para validar las políticas de IAM con el fin de garantizar la seguridad y funcionalidad de los permisos: el analizador de acceso de IAM valida políticas nuevas y existentes para que respeten el lenguaje (JSON) de las políticas de IAM y las prácticas recomendadas de IAM. El analizador de acceso de IAM proporciona más de 100 verificaciones de políticas y recomendaciones procesables para ayudar a crear políticas seguras y funcionales. xPara más información, consulte la [política de validación del Analizador de acceso de IAM](#) en la Guía de usuario de IAM.
- Solicite la autenticación multifactor (MFA): si se encuentra en una situación en la que necesita usuarios raíz o de IAM en su Cuenta de AWS, active la MFA para mayor seguridad. Para solicitar la MFA cuando se invocan las operaciones de la API, agregue las condiciones de la MFA a sus políticas. Para obtener más información, consulte [Configuración de acceso a una API protegida por MFA](#) en la Guía del usuario de IAM.

Para obtener más información sobre las prácticas recomendadas de IAM, consulte las [Prácticas recomendadas de seguridad en IAM](#) en la Guía del usuario de IAM.

## Política gestionada por AWS (predefinida) para Amazon Fraud Detector

AWS aborda muchos casos de uso comunes dando políticas de IAM independientes creadas y administradas por AWS. Estas políticas administradas por AWS conceden los permisos necesarios para casos de uso comunes, lo que le evita tener que investigar los permisos que se necesitan. Para obtener más información, consulte [Políticas administradas de AWS](#) en la Guía del usuario de AWS Identity and Access Management administración.

La siguiente política AWS gestionada, que puedes adjuntar a los usuarios de tu cuenta, es específica de Amazon Fraud Detector:

`AmazonFraudDetectorFullAccess`: Otorga acceso completo a los recursos, las acciones y las operaciones compatibles de Amazon Fraud Detector, que incluyen:

- Enumere y describa todos los puntos finales del modelo en Amazon SageMaker
- Enumere todas las funciones de IAM de la cuenta
- Listar todos los buckets de Amazon S3
- Permita que IAM Pass Role pase una función a Amazon Fraud Detector

Esta política no proporciona acceso ilimitado a S3. Si necesita cargar conjuntos de datos de entrenamiento de modelos en S3, también es necesaria la política `AmazonS3FullAccess` gestionada (o la política de acceso a Amazon S3 personalizada y con alcance limitado).

Para revisar los permisos de la política, inicia sesión en la consola de IAM y busca por el nombre de la política. También puedes crear tus propias políticas de IAM personalizadas para permitir permisos para las acciones y los recursos de Amazon Fraud Detector cuando los necesites. Puede asociar estas políticas personalizadas a los usuarios o grupos de que las requieran.

## Cómo permitir a los usuarios consultar sus propios permisos

En este ejemplo, se muestra cómo podría crear una política que permita a los usuarios de IAM ver las políticas administradas e insertadas que se asocian a la identidad de sus usuarios. Esta política incluye permisos para realizar esta acción en la consola o mediante programación con la AWS CLI o la API de AWS.

```
{
```

```

"Version": "2012-10-17",
"Statement": [
  {
    "Sid": "ViewOwnUserInfo",
    "Effect": "Allow",
    "Action": [
      "iam:GetUserPolicy",
      "iam:ListGroupsWithUser",
      "iam:ListAttachedUserPolicies",
      "iam:ListUserPolicies",
      "iam:GetUser"
    ],
    "Resource": ["arn:aws:iam::*:user/${aws:username}"]
  },
  {
    "Sid": "NavigateInConsole",
    "Effect": "Allow",
    "Action": [
      "iam:GetGroupPolicy",
      "iam:GetPolicyVersion",
      "iam:GetPolicy",
      "iam:ListAttachedGroupPolicies",
      "iam:ListGroupPolicies",
      "iam:ListPolicyVersions",
      "iam:ListPolicies",
      "iam:ListUsers"
    ],
    "Resource": "*"
  }
]
}

```

## Permita el acceso total a los recursos de Amazon Fraud Detector

El siguiente ejemplo proporciona a un usuario acceso Cuenta de AWS completo a todos los recursos y acciones de Amazon Fraud Detector.

```

{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Action": [

```

```

        "frauddetector:*"
    ],
    "Resource": "*"
}
]
}

```

## Permitir el acceso de solo lectura a los recursos de Amazon Fraud Detector

En este ejemplo, concedes a un usuario acceso de Cuenta de AWS solo lectura a tus recursos de Amazon Fraud Detector.

```

{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Action": [
        "frauddetector:GetEventTypes",
        "frauddetector:BatchGetVariable",
        "frauddetector:DescribeDetector",
        "frauddetector:GetModelVersion",
        "frauddetector:GetEventPrediction",
        "frauddetector:GetExternalModels",
        "frauddetector:GetLabels",
        "frauddetector:GetVariables",
        "frauddetector:GetDetectors",
        "frauddetector:GetRules",
        "frauddetector:ListTagsForResource",
        "frauddetector:GetKMSEncryptionKey",
        "frauddetector:DescribeModelVersions",
        "frauddetector:GetDetectorVersion",
        "frauddetector:GetPrediction",
        "frauddetector:GetOutcomes",
        "frauddetector:GetEntityTypes",
        "frauddetector:GetModels"
      ],
      "Resource": "*"
    }
  ]
}

```

## Permitir el acceso a un recurso específico

En este ejemplo de política a nivel de recursos, concedes a un usuario el Cuenta de AWS acceso a todas las acciones y recursos, excepto a un recurso de Detector concreto.

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Action": [
        "frauddetector:*"
      ],
      "Resource": "*"
    },
    {
      "Effect": "Deny",
      "Action": [
        "frauddetector:*Detector"
      ],
      "Resource": "arn:${Partition}:frauddetector:${Region}:${Account}:detector/
${detector-name}"
    }
  ]
}
```

## Permita el acceso a recursos específicos cuando utilice la API de modo dual

Amazon Fraud Detector proporciona API de obtención en modo dual que funcionan como operaciones de lista y descripción. Una API de modo dual, cuando se llama sin ningún parámetro, devuelve una lista del recurso especificado asociado a su Cuenta de AWS. Cuando se llama a una API de modo dual con un parámetro, se muestran los detalles del recurso especificado. El recurso puede ser de modelos, variables, tipos de eventos o tipos de entidades.

Las API de modo dual admiten permisos a nivel de recursos en las políticas de IAM. Sin embargo, los permisos a nivel de recursos solo se aplican cuando se proporcionan uno o más parámetros como parte de la solicitud. Por ejemplo, si el usuario llama a la [GetVariables](#) API y proporciona un nombre de variable y si hay una política de denegación de IAM asociada al recurso variable o al nombre de la variable, el usuario recibirá `AccessDeniedException` un error. Si el usuario llama a la `GetVariables` API y no especifica un nombre de variable, se devuelven todas las variables, lo que puede provocar una pérdida de información.

Para permitir a los usuarios ver únicamente los detalles de recursos específicos, utilice un elemento de política de IAM en una NotResource política de denegación de IAM. Tras añadir este elemento de política a una política de denegación de IAM, los usuarios solo pueden ver los detalles de los recursos que se especifican en el bloque. NotResource Para obtener más información, consulte los [elementos de la política JSON de IAM: NotResource](#) en la Guía del usuario de IAM.

El siguiente ejemplo de política permite a los usuarios acceder a todos los recursos de Amazon Fraud Detector. Sin embargo, el elemento NotResource de política se utiliza para limitar las llamadas a la [GetVariables](#)API únicamente a los nombres de las variables con los prefijos `user*job_*`, `yvar*`.

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

## Respuesta

En este ejemplo de política, la respuesta presenta el siguiente comportamiento:

- Una `GetVariables` llamada que no incluye nombres de variables genera un `AccessDeniedException` error porque la solicitud se asigna a la sentencia `Deny`.
- Una `GetVariables` llamada que incluye un nombre de variable no permitido genera un `AccessDeniedException` error porque el nombre de la variable no se corresponde con el

nombre de la variable del NotResource bloque. Por ejemplo, una GetVariables llamada con un nombre de variable email\_address produce un AccessDeniedException error.

- Una GetVariables llamada que incluye un nombre de variable que coincide con un nombre de variable del NotResource bloque se devuelve como se esperaba. Por ejemplo, una GetVariables llamada que incluye el nombre de la variable job\_cpa devuelve los detalles de la job\_cpa variable.

## Limitar el acceso en función de las etiquetas

En este ejemplo de política se muestra cómo limitar el acceso a Amazon Fraud Detector en función de las etiquetas de recursos. En este ejemplo se supone que:

- En su casoCuenta de AWS, ha definido dos grupos diferentes, denominados Team1 y Team2
- Ha creado cuatro detectores
- Desea permitir a los miembros del Team1 realizar llamadas a la API en 2 detectores
- Desea permitir a los miembros del Team2 realizar llamadas a la API en los otros 2 detectores

Para controlar el acceso a llamadas a la API (ejemplo)

1. Añada una etiqueta con la clave Project y el valor A a los detectores utilizados por Team1.
2. Añada una etiqueta con la clave Project y el valor B a los detectores utilizados por Team2.
3. Cree una política de IAM con una ResourceTag condición que deniegue el acceso a los detectores que tengan etiquetas con una clave Project y un valorB, y adjunte esa política a Team1.
4. Cree una política de IAM con una ResourceTag condición que deniegue el acceso a los detectores que tengan etiquetas con una clave Project y un valorA, y adjunte esa política a Team2.

El siguiente es un ejemplo de una política que deniega acciones específicas en cualquier recurso de Amazon Fraud Detector que tenga una etiqueta con una clave Project y un valor deB:

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

## Prevención del suplente confuso

El confuso problema del diputado se produce cuando una entidad que no tiene permiso para realizar una acción puede coaccionar a una entidad con más privilegios para que la lleve a cabo. AWS proporciona herramientas que te ayudan a proteger tu cuenta si permites a terceros (lo que se denomina multicuenta) o a otros AWS servicios (denominados servicios cruzados) acceder a los recursos de tu cuenta.

Cuando un servicio (el servicio de llamadas) llama a otro servicio (el servicio al que se llama) se produce un problema de confusión entre servicios (el servicio al que se llama). El servicio que lleva a cabo las llamadas se puede manipular para utilizar sus permisos a fin de actuar en función de los recursos de otro cliente de una manera en la que no debe tener permiso para acceder. Para evitarlo, puedes crear políticas que te ayuden a proteger los datos de todos los servicios con los directores de servicio que tengan acceso a los recursos de tu servicio.

Amazon Fraud Detector admite el uso de [funciones de servicio](#) en sus políticas de permisos para permitir que un servicio acceda a los recursos de otro servicio en su nombre. Un rol requiere dos políticas: una política de confianza de rol que especifica la entidad principal que puede asumir el rol y una política de permisos que especifica qué se puede hacer con el rol. Cuando un servicio asume un rol en su nombre, se debe permitir que la entidad principal del servicio realice la acción `sts:AssumeRole` en la política de confianza de rol. Cuando un servicio llama a `sts:AssumeRole`, AWS STS devuelve un conjunto de credenciales de seguridad temporales que la entidad principal del servicio utiliza para obtener acceso a los recursos permitidos por la política de permisos del rol.

Para evitar el problema de los adjuntos confusos entre servicios, Amazon Fraud Detector recomienda utilizar las claves de contexto de condición [aws:SourceAccount](#) global [aws:SourceArn](#) las claves de contexto de condición global en su política de confianza de roles para limitar el acceso al rol solo a las solicitudes generadas por los recursos esperados.

`aws:SourceAccount` Especifica el ID de cuenta y `aws:SourceArn` especifica el ARN del recurso asociado al acceso entre servicios. `aws:SourceArn` debe especificarse mediante el [formato ARN](#). Asegúrese de que ambos `aws:SourceAccount` `aws:SourceArn` utilizan el mismo identificador de cuenta cuando se utilizan en la misma declaración de política.

La forma más eficaz de protegerse contra el problema de la sustitución confusa es utilizar la clave de contexto de condición global de `aws:SourceArn` con el ARN completo del recurso. Si no conoce el ARN completo del recurso o si está especificando varios recursos, utilice la clave de condición de contexto `aws:SourceArn` global con un comodín (\*) para las partes desconocidas del ARN. Por ejemplo, `arn:aws:servicename:*:123456789012:*`. Para obtener información sobre los recursos y las acciones de Amazon Fraud Detector que puede utilizar en sus políticas de permisos, consulte [Acciones, recursos y claves de condición de Amazon Fraud Detector](#).

El siguiente ejemplo de política de confianza de roles utiliza un comodín (\*) en la clave de `aws:SourceArn` condición para permitir que Amazon Fraud Detector acceda a varios recursos asociados al ID de cuenta.

```
{
  "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 siguiente política de confianza de roles permite a Amazon Fraud Detector acceder únicamente a `external-model` los recursos. Observe el `aws:SourceArn` parámetro en el bloque de condiciones. El calificador de recursos se crea utilizando el punto final del modelo que se proporciona para realizar la llamada a la `PutExternalModel` API.

```

{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Principal": {
        "Service": [
          "frauddetector.amazonaws.com"
        ]
      },
      "Action": "sts:AssumeRole",
      "Condition": {
        "StringEquals": {
          "aws:SourceAccount": "123456789012"
        },
        "StringLike": {
          "aws:SourceArn": "arn:aws:frauddetector:us-west-2:123456789012:external-
model/MyExternalModeldoNotDelete-ReadOnly"
        }
      }
    }
  ]
}

```

}

## Solución de problemas de identidad y acceso a Amazon Fraud Detector

Utiliza la siguiente información para ayudarte a diagnosticar y solucionar los problemas habituales que te pueden surgir al trabajar con Amazon Fraud Detector e IAM.

### Temas

- [No estoy autorizado a realizar ninguna acción en Amazon Fraud Detector](#)
- [No estoy autorizado a realizar el iam: PassRole](#)
- [Quiero permitir que personas ajenas a mi AWS cuenta accedan a mis recursos de Amazon Fraud Detector](#)
- [Amazon Fraud Detector no pudo asumir el rol asignado](#)

### No estoy autorizado a realizar ninguna acción en Amazon Fraud Detector

Si la AWS Management Console le indica que no tiene autorización para llevar a cabo una acción, debe ponerse en contacto con su administrador para recibir ayuda. El administrador es la persona que le proporcionó las credenciales de inicio de sesión.

El siguiente ejemplo de error se produce cuando el mateojackson usuario intenta utilizar la consola para ver los detalles de un *detector* pero no tiene `frauddetector:GetDetectors` permisos.

```
User: arn:aws:iam::123456789012:user/mateojackson is not authorized to perform:
frauddetector:GetDetectors on resource: my-example-detector
```

En este caso, Mateo pide a su administrador que actualice sus políticas de forma que pueda obtener acceso al recurso *my-example-detector* mediante la acción `frauddetector:GetDetectors`.

### No estoy autorizado a realizar el iam: PassRole

Si recibes un error que indica que no estás autorizado a realizar la `iam:PassRole` acción, debes actualizar tus políticas para que puedas transferir una función a Amazon Fraud Detector.

Algunos Servicios de AWS le permiten transferir un rol existente a dicho servicio en lugar de crear un nuevo rol de servicio o uno vinculado al servicio. Para ello, debe tener permisos para transferir el rol al servicio.

El siguiente ejemplo de error se produce cuando un usuario de IAM denominado `marymajor` intenta utilizar la consola para realizar una acción en Amazon Fraud Detector. Sin embargo, la acción requiere que el servicio cuente con permisos que concede un rol de servicio. Mary no tiene permisos para transferir el rol al servicio.

```
User: arn:aws:iam::123456789012:user/marymajor is not authorized to perform:
iam:PassRole
```

En este caso, las políticas de Mary se deben actualizar para permitirle realizar la acción `iam:PassRole`.

Si necesita ayuda, póngase en contacto con su administrador de AWS. El administrador es la persona que le proporcionó las credenciales de inicio de sesión.

## Quiero permitir que personas ajenas a mi AWS cuenta accedan a mis recursos de Amazon Fraud Detector

Puede crear un rol que los usuarios de otras cuentas o las personas externas a la organización puedan utilizar para acceder a sus recursos. Puede especificar una persona de confianza para que asuma el rol. En el caso de los servicios que admitan las políticas basadas en recursos o las listas de control de acceso (ACL), puede utilizar dichas políticas para conceder a las personas acceso a sus recursos.

Para más información, consulte lo siguiente:

- Para saber si Amazon Fraud Detector admite estas funciones, consulta [Cómo funciona Amazon Fraud Detector con IAM](#).
- Para obtener información acerca de cómo proporcionar acceso a los recursos de las Cuentas de AWS de su propiedad, consulte [Proporcionar acceso a un usuario de IAM a otra Cuenta de AWS de la que es propietario](#) en la Guía del usuario de IAM.
- Para obtener información acerca de cómo proporcionar acceso a tus recursos a Cuentas de AWS de terceros, consulte [Proporcionar acceso a Cuentas de AWS que son propiedad de terceros](#) en la Guía del usuario de IAM.
- Para obtener información sobre cómo proporcionar acceso mediante federación de identidades, consulte [Proporcionar acceso a usuarios autenticados externamente \(federación de identidades\)](#) en la Guía del usuario de IAM.

- Para obtener información sobre la diferencia entre los roles y las políticas basadas en recursos para el acceso entre cuentas, consulte [Cómo los roles de IAM difieren de las políticas basadas en recursos](#) en la Guía del Usuario de IAM.

## Amazon Fraud Detector no pudo asumir el rol asignado

Si recibes un error que indica que Amazon Fraud Detector no ha podido asumir el rol asignado, debes actualizar la relación de confianza para el rol especificado. Al especificar Amazon Fraud Detector como entidad de confianza, el servicio puede asumir esa función. Cuando utilizas Amazon Fraud Detector para crear un rol, esta relación de confianza se establece automáticamente. Solo necesita establecer esta relación de confianza para las funciones de IAM que no haya creado Amazon Fraud Detector.

Establecer una relación de confianza para un puesto existente con Amazon Fraud Detector

1. Abra la consola de IAM en <https://console.aws.amazon.com/iam/>.
2. En el panel de navegación, elija Roles.
3. Elija el nombre del rol que desee modificar y seleccione la pestaña Relaciones de confianza.
4. Elija Editar relación de confianza.
5. En Policy Document, pegue lo siguiente y, a continuación, seleccione Update Trust Policy.

```
{
  "Version": "2012-10-17",
  "Statement": [ {
    "Effect": "Allow",
    "Principal": {
      "Service": "frauddetector.amazonaws.com"
    },
    "Action": "sts:AssumeRole"
  } ]
}
```

# Registro y supervisión en Amazon Fraud Detector

AWS proporciona las siguientes herramientas de supervisión para vigilar Amazon Fraud Detector, informar cuando algo va mal y tomar medidas automáticas cuando sea necesario:

- Amazon CloudWatch monitorea tus AWS recursos y las aplicaciones en las que AWS ejecutas en tiempo real. Para obtener más información CloudWatch, consulta la [Guía del CloudWatch usuario de Amazon](#).
- AWS CloudTrail captura llamadas a la API y eventos relacionados efectuados por su cuenta de AWS o en su nombre, y entrega los archivos de registro al bucket de Amazon S3 que se haya especificado. Para obtener más información CloudTrail, consulte la [Guía AWS CloudTrail del usuario](#).

Para obtener más información sobre la supervisión de Amazon Fraud Detector, consulte [Supervise Amazon Fraud Detector](#).

## Validación de conformidad para Amazon Fraud Detector

Audidores externos evalúan la seguridad y la conformidad de los servicios de AWS como parte de varios programas de conformidad de AWS, como SOC, PCI, FedRAMP e HIPAA.


Para saber si un Servicio de AWS está incluido en el ámbito de programas de conformidad específicos, consulte [Servicios de AWS en el ámbito del programa de conformidad](#) y escoja el programa de conformidad que le interese. Para obtener información general, consulte [Programas de conformidad de AWS](#).

Puede descargar los informes de auditoría de terceros utilizando AWS Artifact. Para obtener más información, consulte [Descarga de informes en AWS Artifact](#).

Su responsabilidad de conformidad al utilizar Servicios de AWS se determina en función de la sensibilidad de los datos, los objetivos de cumplimiento de su empresa y la legislación y los reglamentos correspondientes. AWS proporciona los siguientes recursos para ayudar con la conformidad:

- [Guías de inicio rápido de seguridad y conformidad](#): estas guías de implementación tratan consideraciones sobre arquitectura y ofrecen pasos para implementar los entornos de referencia centrados en la seguridad y la conformidad en AWS.

- [Arquitectura para la seguridad y el cumplimiento de la HIPAA en Amazon Web Services](#): en este documento técnico, se describe cómo las empresas pueden utilizar AWS para crear aplicaciones aptas para HIPAA.

 Note

No todos los Servicios de AWS son aptos para HIPAA. Para obtener más información, consulte la [Referencia de servicios aptos para HIPAA](#).

- [Recursos de conformidad de AWS](#): este conjunto de manuales y guías podría aplicarse a su sector y ubicación.
- [Guías de cumplimiento para clientes de AWS](#): comprenda el modelo de responsabilidad compartida desde el punto de vista del cumplimiento. Las guías resumen las mejores prácticas para garantizar la seguridad de los Servicios de AWS y orientan los controles de seguridad en varios marcos (incluidos el Instituto Nacional de Estándares y Tecnología (NIST, por sus siglas en inglés), el Consejo de Estándares de Seguridad de la Industria de Tarjetas de Pago (PCI, por sus siglas en inglés) y la Organización Internacional de Normalización (ISO, por sus siglas en inglés)).
- [Evaluación de recursos con reglas](#) en la Guía para desarrolladores de AWS Config: el servicio AWS Config evalúa en qué medida las configuraciones de sus recursos cumplen las prácticas internas, las directrices del sector y las normativas.
- [AWS Security Hub](#): este Servicio de AWS proporciona una visión completa de su estado de seguridad en AWS. Security Hub utiliza controles de seguridad para evaluar sus recursos de AWS y comprobar su cumplimiento con los estándares y las prácticas recomendadas del sector de la seguridad. Para obtener una lista de los servicios y controles compatibles, consulte la [Referencia de controles de Security Hub](#).
- [AWS Audit Manager](#): este servicio de Servicio de AWS le ayuda a auditar continuamente el uso de AWS con el fin de simplificar la forma en que administra el riesgo y la conformidad con las normativas y los estándares del sector.

## Resiliencia en Amazon Fraud Detector

La infraestructura global de AWS está conformada por regiones y zonas de disponibilidad de AWS. Las regiones de AWS proporcionan varias zonas de disponibilidad físicamente independientes y aisladas que se encuentran conectadas mediante redes con un alto nivel de rendimiento y redundancia, además de baja latencia. Mediante las zonas de disponibilidad, puede diseñar y utilizar aplicaciones y bases de datos que realizan una conmutación por error automática entre las zonas sin



interrupciones. Las zonas de disponibilidad tienen una mayor disponibilidad, tolerancia a errores y escalabilidad que las infraestructuras tradicionales de uno o varios centros de datos.

Para obtener más información sobre las zonas de disponibilidad y las regiones de AWS, consulte [Infraestructura global de AWS](#).

## Seguridad de infraestructura en Amazon Fraud Detector

Como servicio gestionado, Amazon Fraud Detector está protegido por la seguridad de la red AWS global. Para obtener información sobre los servicios de seguridad de AWS y cómo AWS protege la infraestructura, consulte [Seguridad en la nube de AWS](#). Para diseñar su entorno de AWS conforme a las prácticas recomendadas de seguridad de la infraestructura, consulte [Protección de la infraestructura](#) en Pilar de seguridad del Marco de AWS Well-Architected.

Utiliza las llamadas a la API AWS publicadas para acceder a Amazon Fraud Detector a través de la red. Los clientes deben admitir lo siguiente:

- Seguridad de la capa de transporte (TLS). Exigimos TLS 1.2 y recomendamos TLS 1.3.
- Conjuntos de cifrado con confidencialidad directa total (PFS) como DHE (Ephemeral Diffie-Hellman) o ECDHE (Elliptic Curve Ephemeral Diffie-Hellman). La mayoría de los sistemas modernos como Java 7 y posteriores son compatibles con estos modos.

Además, las solicitudes deben estar firmadas mediante un ID de clave de acceso y una clave de acceso secreta que esté asociada a una entidad principal de IAM. También puede utilizar [AWS Security Token Service](#) (AWS STS) para generar credenciales de seguridad temporales para firmar solicitudes.

# Supervise Amazon Fraud Detector

La supervisión es una parte importante del mantenimiento de la fiabilidad, la disponibilidad y el rendimiento de Amazon Fraud Detector y las demás soluciones de AWS. AWS proporciona las siguientes herramientas de supervisión para vigilar Amazon Fraud Detector, informar cuando algo va mal y tomar medidas automáticas cuando sea necesario:

- Amazon CloudWatch monitorea tus AWS recursos y las aplicaciones en las que AWS ejecutas en tiempo real. Puede recopilar métricas y realizar un seguimiento de las métricas, crear paneles personalizados y definir alarmas que le advierten o que toman medidas cuando una métrica determinada alcanza el umbral que se especifique. Para obtener más información, consulta la [Guía del CloudWatch usuario de Amazon](#).
- AWS CloudTrail captura llamadas a la API y eventos relacionados efectuados por su cuenta de AWS o en su nombre, y entrega los archivos de registro al bucket de Amazon S3 que se haya especificado. También puede identificar qué usuarios y cuentas llamaron a AWS, la dirección IP de origen de las llamadas y el momento en que se hicieron. Para más información, consulte la [Guía del usuario de AWS CloudTrail](#).

## Temas

- [Supervisión de Amazon Fraud Detector con Amazon CloudWatch](#)
- [Registro de llamadas a la API de Amazon Fraud Detector con AWS CloudTrail](#)

## Supervisión de Amazon Fraud Detector con Amazon CloudWatch

Puedes monitorizar Amazon Fraud Detector con Amazon CloudWatch, que recopila datos sin procesar y los procesa para convertirlos en métricas legibles prácticamente en tiempo real. Estas estadísticas se mantienen durante 15 meses, de forma que pueda obtener acceso a información histórica y disponer de una mejor perspectiva sobre el desempeño de su aplicación web o servicio. También puede establecer alarmas que vigilen determinados umbrales y enviar notificaciones o realizar acciones cuando se cumplan dichos umbrales. Para obtener más información, consulta la [Guía del CloudWatch usuario de Amazon](#).

## Temas

- [Uso de CloudWatch métricas para Amazon Fraud Detector](#).
- [Métricas de Amazon Fraud Detector](#)

## Uso de CloudWatch métricas para Amazon Fraud Detector.

Para utilizar métricas, debe especificar la siguiente información:

- El espacio de nombres de las métricas. Un espacio de nombres es un contenedor que CloudWatch Amazon Fraud Detector utiliza para publicar sus métricas. Si utilizas la CloudWatch [ListMetrics](#) API o el comando [list-metrics para ver las métricas](#) de Amazon Fraud Detector, especifica el espacio de `AWS/FraudDetector` nombres.
- La dimensión de la métrica. Una dimensión es un par nombre-valor que le ayuda a identificar de forma única una métrica; por ejemplo, `DetectorId` puede ser el nombre de una dimensión. La especificación de una dimensión métrica es opcional.
- El nombre de la métrica, como `GetEventPrediction`.

Puedes obtener datos de supervisión de Amazon Fraud Detector mediante la AWS Management Console, la AWS CLI, o la CloudWatch API. También puede usar la CloudWatch API a través de uno de los kits de desarrollo de software (SDK) de Amazon AWS o las herramientas de CloudWatch API. La consola muestra una serie de gráficos basados en los datos sin procesar de la CloudWatch API. En función de sus necesidades, es posible que prefiera utilizar los gráficos que se muestran en la consola o que se recuperan de la API.

En la siguiente lista se indican algunos usos frecuentes de las métricas. Se trata de sugerencias que puede usar como punto de partida y no de una lista completa.

¿Cómo?	Métricas relevantes
¿Cómo hago un seguimiento del número de predicciones que se han realizado?	Monitoree la métrica <code>GetEventPrediction</code> .
¿Cómo puedo supervisar <code>GetEventPrediction</code> los errores?	Usa las métricas <code>GetEventPrediction 5xxError</code> y las <code>GetEventPrediction 4xxError</code> métricas.
¿Cómo puedo monitorizar la latencia de las llamadas <code>GetEventPrediction</code> ?	Utilice la métrica <code>GetEventPrediction Latency</code> .

Debes tener los CloudWatch permisos adecuados para monitorear Amazon Fraud Detector con CloudWatch. Para obtener más información, consulte [Autenticación y control de acceso de Amazon CloudWatch](#).

## Acceda a las métricas de Amazon Fraud Detector

Los siguientes pasos muestran cómo acceder a las métricas de Amazon Fraud Detector mediante la CloudWatch consola.

Para ver las métricas (consola)

1. Abra la CloudWatch consola en <https://console.aws.amazon.com/cloudwatch/>.
2. Elija Métricas, elija la pestaña Todas las métricas y, a continuación, elija Fraud Detector.
3. Elija la dimensión de la métrica.
4. Elija en la lista la métrica que desea usar y elija un periodo de tiempo para el gráfico.

## Crear una alarma

Puede crear una CloudWatch alarma que envíe un mensaje de Amazon Simple Notification Service (Amazon SNS) cuando la alarma cambie de estado. Una alarma vigila una métrica determinada durante el periodo especificado. Realiza una o varias acciones según el valor de la métrica con respecto a un umbral dado durante varios periodos de tiempo. La acción es una notificación que se envía a un tema de Amazon SNS o a una política de Auto Scaling.

Las alarmas invocan acciones únicamente en caso de cambios de estado sostenidos. CloudWatch las alarmas no invocan acciones simplemente porque se encuentran en un estado determinado. El estado debe haber cambiado y debe haberse mantenido durante el número de periodos de tiempo especificado.

Para configurar una alarma (consola)

1. Inicie sesión AWS Management Console y abra la CloudWatch consola en <https://console.aws.amazon.com/cloudwatch/>.
2. En el panel de navegación, selecciona Alarmas y selecciona Crear alarma. Se abrirá el asistente de creación de alarmas.
3. Elija Seleccionar métrica.
4. En la pestaña Todas las métricas, selecciona Fraud Detector.

5. Elija Por ID de detector y, a continuación, elija la GetEventPrediction métrica.
6. Elija la pestaña Métricas diagramadas.
7. En Statistic (Estadística), elija Sum (Suma).
8. Elija Seleccionar métrica.
9. En Condiciones, elija Estático para el tipo de umbral y Mayor para Siempre que... y, a continuación, introduzca el valor máximo que desee. Elija Siguiente.
10. Para enviar alarmas a un tema de Amazon SNS existente, en Enviar notificación a:, elija un tema de SNS existente. Para configurar el nombre y las direcciones de correo electrónico de una nueva lista de suscripciones de correo electrónico, seleccione Nueva lista. CloudWatch guarda la lista y la muestra en el campo para que pueda utilizarla para configurar futuras alarmas.

#### Note

Si utiliza Nueva lista para crear un nuevo tema de Amazon SNS, deben verificarse las direcciones de correo electrónico para que los destinatarios previstos puedan recibir las notificaciones. Amazon SNS envía solo mensajes de correo electrónico cuando la alarma entra en un estado de alarma. Si este cambio de estado de alarma se produce antes de que se verifiquen las direcciones de correo electrónico, los destinatarios previstos no recibirán ninguna notificación.

11. Elija Siguiente. Agrega un nombre y una descripción opcional para la alarma. Elija Siguiente.
12. Seleccione Crear alarma.

## Métricas de Amazon Fraud Detector

Amazon Fraud Detector envía las siguientes métricas a CloudWatch. Todas las métricas respaldan estas estadísticas: Average, Minimum, Maximum, Sum.

Métrica	Descripción
GetEventPrediction	El número de solicitudes de GetEventPrediction API.  Dimensiones válidas: DetectorID

Métrica	Descripción
GetEventPredictionLatency	<p>El intervalo de tiempo necesario para responder a una solicitud del cliente desde la GetEventPrediction solicitud.</p> <p>Dimensiones válidas: <code>DetectorID</code></p> <p>Unidad: milisegundos</p>
GetEventPrediction4XXError	<p>El número de GetEventPrediction solicitudes en las que Amazon Fraud Detector devolvió un código de respuesta HTTP 4xx. Por cada 4xx respuestas, se envía 1.</p> <p>Dimensiones válidas: <code>DetectorID</code></p>
GetEventPrediction5XXError	<p>El número de GetEventPrediction solicitudes en las que Amazon Fraud Detector devolvió un código de respuesta HTTP de 5xx. Por cada 5xx respuestas, se envía 1.</p> <p>Dimensiones válidas: <code>DetectorID</code></p>
Prediction	<p>El número de predicciones. Si se realiza correctamente, se envía 1.</p> <p>Dimensiones válidas: <code>DetectorID</code> , <code>DetectorVersionID</code></p>
PredictionLatency	<p>El intervalo de tiempo que tarda una operación de predicción.</p> <p>Dimensiones válidas: <code>DetectorID</code> , <code>DetectorVersionID</code></p> <p>Unidad: milisegundos</p>

Métrica	Descripción
PredictionError	<p>Número de predicciones en las que Amazon Fraud Detector detectó un error. Si se detecta un error, se envía 1.</p> <p>Dimensiones válidas:DetectorID , DetectorVersionID</p>
VariableUsed	<p>El número de GetEventPrediction solicitudes en las que se utilizó la variable como parte de la evaluación.</p> <p>Dimensiones válidas:DetectorID ,DetectorVersionID , VariableName</p>
VariableDefaultReturned	<p>El número de GetEventPrediction solicitudes en las que la variable no estaba presente como parte de los atributos del evento y, por lo tanto, se utilizó el valor predeterminado de la variable durante la evaluación.</p> <p>Dimensiones válidas:DetectorID ,DetectorVersionID , VariableName</p>
RuleNotEvaluated	<p>El número de GetEventPrediction solicitudes en las que la regla no se evaluó porque coincidió con una regla anterior.</p> <p>Dimensiones válidas:DetectorID ,DetectorVersionID , RuleID</p>
RuleEvaluateTrue	<p>El número de GetEventPrediction solicitudes en las que la regla se activó como True y se devolvió el resultado de la regla.</p> <p>Dimensiones válidas:DetectorID ,DetectorVersionID , RuleID</p>

Métrica	Descripción
RuleEvaluateFalse	<p>El número de GetEventPrediction solicitudes en las que la regla se evaluó como False.</p> <p>Dimensiones válidas:DetectorID ,DetectorVersionID ,RuleID</p>
RuleEvaluateError	<p>El número de GetEventPrediction solicitudes en las que la regla se evalúa por error</p> <p>Dimensiones válidas:DetectorID ,, DetectorVersionID RuleID</p>
OutcomeReturned	<p>El número de GetEventPrediction llamadas en las que se devolvió el resultado especificado.</p> <p>Dimensiones válidas:DetectorID ,DetectorVersionID ,OutcomeName</p>
ModelInvocation (Amazon SageMaker model endpoint)	<p>El número de GetEventPrediction solicitudes en las que se invocó el punto final del SageMaker modelo como parte de la evaluación.</p> <p>Dimensiones válidas:DetectorID ,DetectorVersionID ,ModelEndpoint</p>
ModelInvocationError (Amazon SageMaker model endpoint)	<p>El número de GetEventPrediction solicitudes en las que el punto final del SageMaker modelo invocado arrojó un error durante la evaluación.</p> <p>Dimensiones válidas:DetectorID ,DetectorVersionID ,ModelEndpoint</p>



Métrica	Descripción
ModelInvocationLatency (Amazon SageMaker model endpoint)	<p>El intervalo de tiempo que tarda el modelo importado en responder visto desde Amazon Fraud Detector. Este intervalo incluye solo la invocación del modelo.</p> <p>Dimensiones válidas:DetectorID , DetectorVersionID ModelEndpoint</p> <p>Unidad: milisegundos</p>
ModelInvocation	<p>El número de GetEventPrediction solicitudes en las que se invocó el modelo como parte de la evaluación.</p> <p>Dimensiones válidas:DetectorID ,DetectorVersionID ,ModelType , ModelID</p>
ModelInvocationError	<p>El número de GetEventPrediction solicitudes en las que el modelo Amazon Fraud Detector arrojó un error durante la evaluación.</p> <p>Dimensiones válidas:DetectorID ,DetectorVersionID ,ModelType , ModelID</p>
ModelInvocationLatency	<p>El intervalo de tiempo que tarda el modelo Amazon Fraud Detector en responder visto desde Amazon Fraud Detector. Este intervalo incluye solo la invocación del modelo.</p> <p>Dimensiones válidas:DetectorID ,DetectorVersionID , ModelType ModelID</p> <p>Unidad: milisegundos</p>

# Registro de llamadas a la API de Amazon Fraud Detector con AWS CloudTrail

Amazon Fraud Detector está integrado con AWS CloudTrail un servicio que proporciona un registro de las acciones realizadas por un usuario, un rol o un AWS servicio en Amazon Fraud Detector. CloudTrail captura todas las llamadas a las API de Amazon Fraud Detector como eventos, incluidas las llamadas desde la consola de Amazon Fraud Detector y las llamadas desde código a las API de Amazon Fraud Detector.

Si crea una ruta, puede habilitar la entrega continua de CloudTrail eventos a un bucket de Amazon S3, incluidos los eventos de Amazon Fraud Detector. Si no configura una ruta, podrá ver los eventos más recientes en la CloudTrail consola, en el historial de eventos. Con la información recopilada por CloudTrail, puedes determinar la solicitud que se realizó a Amazon Fraud Detector, la dirección IP desde la que se realizó la solicitud, quién la hizo, cuándo se realizó y detalles adicionales.

Para obtener más información CloudTrail, consulte la [Guía AWS CloudTrail del usuario](#).

## Información sobre Amazon Fraud Detector en CloudTrail

CloudTrail está activado en tu AWS cuenta al crearla. Cuando se produce una actividad en Amazon Fraud Detector, esa actividad se registra en un CloudTrail evento junto con otros eventos de AWS servicio en el historial de eventos. Puede ver, buscar y descargar los últimos eventos de la cuenta de AWS. Para obtener más información, consulte [Visualización de eventos con el historial de CloudTrail eventos](#).

Para tener un registro continuo de los eventos de tu AWS cuenta, incluidos los relacionados con Amazon Fraud Detector, crea un registro. Un rastro permite CloudTrail entregar archivos de registro a un bucket de Amazon S3. De forma predeterminada, cuando se crea un registro de seguimiento en la consola, el registro de seguimiento se aplica a todas las regiones de AWS. El registro de seguimiento registra los eventos de todas las regiones de la partición de AWS y envía los archivos de registro al bucket de Amazon S3 especificado. Además, puede configurar otros AWS servicios para analizar más a fondo los datos de eventos que se recopilan en los CloudTrail registros y tomar medidas en función de ellos. Para más información, consulte los siguientes temas:

- [Introducción a la creación de registros de seguimiento](#)
- [CloudTrail Integraciones y servicios compatibles](#)
- [Configuración de las notificaciones de Amazon SNS para CloudTrail](#)

- [Recibir archivos de CloudTrail registro de varias regiones](#) y [recibir archivos de CloudTrail registro de varias cuentas](#)

Amazon Fraud Detector permite registrar cada acción (operación de API) como un evento en los archivos de CloudTrail registro. Para obtener más información, consulte [Acciones](#).

Cada entrada de registro o evento contiene información sobre quién generó la solicitud. La información de identidad del usuario lo ayuda a determinar lo siguiente:

- Si la solicitud se realizó con las credenciales raíz o del usuario.
- Si la solicitud se realizó con credenciales de seguridad temporales de un rol o fue un usuario federado.
- Si la solicitud la realizó otro servicio de AWS.

Para obtener más información, consulte el [Elemento userIdentity de CloudTrail](#).

## Descripción de las entradas de los archivos de registro de Amazon Fraud Detector

Un rastro es una configuración que permite la entrega de eventos como archivos de registro a un bucket de Amazon S3 que usted especifique. CloudTrail Los archivos de registro contienen una o más entradas de registro. Un evento representa una solicitud única de cualquier fuente e incluye información sobre la operación solicitada, la fecha y la hora de la operación, los parámetros de la solicitud, etc. CloudTrail Los archivos de registro no son un seguimiento ordenado de las llamadas a la API pública, por lo que no aparecen en ningún orden específico.

En el siguiente ejemplo, se muestra una entrada de CloudTrail registro que demuestra la GetDetectors operación.

```
{
  "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"  
}
```




# Solucionar problemas

Las siguientes secciones le ayudan a solucionar problemas que puedan surgir al trabajar con Amazon Fraud Detector.

## Solucione problemas con los datos de formación

Utilice la información de esta sección para diagnosticar y resolver los problemas que puedan aparecer en el panel de diagnóstico de formación de modelos de la consola de Amazon Fraud Detector cuando entrene a su modelo.

Los problemas que se muestran en el panel de diagnóstico del entrenamiento de modelos se clasifican de la siguiente manera. El requisito de abordar el problema depende de la categoría del problema.

-  **Error:**  
hace que el entrenamiento del modelo falle. Estos problemas deben abordarse para que el modelo se entrene correctamente.
-  **Advertencia:**  
hace que el entrenamiento del modelo continúe; sin embargo, es posible que algunas de las variables se estén excluyendo del proceso de capacitación. Consulta las directrices pertinentes en esta sección para mejorar la calidad de tu conjunto de datos.
-  **Información:**  
(información): no afecta al entrenamiento del modelo y todas las variables se utilizan para el entrenamiento. Le recomendamos que consulte las directrices pertinentes de esta sección para mejorar aún más la calidad del conjunto de datos y el rendimiento del modelo.

### Temas

- [Tasa de fraude inestable en el conjunto de datos dado](#)
- [Datos insuficientes](#)
- [Faltan valores de EVENT\\_LABEL o son diferentes](#)
- [Faltan valores de EVENT\\_TIMESTAMP o son incorrectos](#)
- [Datos no ingeridos](#)
- [Variables insuficientes](#)

- [Falta el tipo de variable o es incorrecto](#)
- [Faltan valores de variables](#)
- [Valores de variables únicas insuficientes](#)
- [Expresión de variable incorrecta](#)
- [Entidades únicas insuficientes](#)

## Tasa de fraude inestable en el conjunto de datos dado

Tipo de problema: error

### Descripción

La tasa de fraude en los datos proporcionados es demasiado inestable a lo largo del tiempo. Asegúrese de que su fraude y sus eventos legítimos se muestreen de manera uniforme a lo largo del tiempo.

### Causa

Este error se produce si los eventos fraudulentos y legítimos de tu conjunto de datos se distribuyen de forma desigual y se toman en diferentes franjas horarias. El proceso de entrenamiento de Amazon Fraud Detector modela y divide su conjunto de datos en función de `EVENT_TIMESTAMP`. Por ejemplo, si su conjunto de datos consta de eventos de fraude extraídos de los últimos 6 meses, pero solo se incluye el último mes de eventos legítimos, el conjunto de datos se considera inestable. Un conjunto de datos inestable puede provocar sesgos en la evaluación del rendimiento del modelo.

### Solución

Asegúrese de proporcionar los datos de los eventos fraudulentos y legítimos de la misma franja horaria para que la tasa de fraude no cambie drásticamente con el tiempo.

## Datos insuficientes

### 1. Tipo de problema: error

#### Descripción

Menos de 50 filas están etiquetadas como eventos fraudulentos. Asegúrese de que tanto los eventos fraudulentos como los legítimos superen el recuento mínimo de 50 y vuelva a entrenar el modelo.

## Causa

Este error se produce si el conjunto de datos tiene menos eventos etiquetados como fraudulentos de los necesarios para el entrenamiento del modelo. Amazon Fraud Detector requiere al menos 50 eventos fraudulentos para entrenar a tu modelo.

## Solución

Asegúrese de que su conjunto de datos incluya un mínimo de 50 eventos fraudulentos. Puedes garantizar esto cubriendo un período de tiempo más largo, si es necesario.

### 2. Tipo de problema: error

#### Descripción

Menos de 50 filas están etiquetadas como eventos legítimos. Asegúrese de que tanto los eventos fraudulentos como los legítimos superen el recuento mínimo de `$threshold` y vuelva a entrenar el modelo.

#### Causa

Este error se produce si el conjunto de datos tiene menos eventos etiquetados como legítimos que los necesarios para el entrenamiento del modelo. Amazon Fraud Detector requiere al menos 50 eventos legítimos para entrenar a tu modelo.

#### Solución

Asegúrese de que su conjunto de datos incluya un mínimo de 50 eventos legítimos. Puedes garantizar esto cubriendo un período de tiempo más largo, si es necesario.

### 3. Tipo de problema: error

#### Descripción

El número de entidades únicas asociadas al fraude es inferior a 100. Considere incluir más ejemplos de entidades fraudulentas para mejorar el rendimiento.

#### Causa

Este error se produce si el conjunto de datos tiene menos entidades con eventos fraudulentos de las necesarias para el entrenamiento del modelo. El modelo Transaction Fraud Insights (TFI) requiere al menos 100 entidades con casos de fraude para garantizar la máxima cobertura del

ámbito del fraude. Es posible que el modelo no se generalice bien si todos los actos de fraude los lleva a cabo un pequeño grupo de entidades.

### Solución

Asegúrese de que su conjunto de datos incluya al menos 100 entidades con eventos fraudulentos. Puedes asegurarte de que abarque un período de tiempo más largo, si es necesario.

## 4. Tipo de problema: error

### Descripción

El número de entidades únicas asociadas a lo legítimo es inferior a 100. Considere incluir más ejemplos de entidades legítimas para mejorar el rendimiento.

### Causa

Este error se produce si el conjunto de datos tiene menos entidades con eventos legítimos que las necesarias para el entrenamiento del modelo. El modelo Transaction Fraud Insights (TFI) requiere al menos 100 entidades con eventos legítimos para garantizar la máxima cobertura del ámbito del fraude. Es posible que el modelo no se generalice bien si todos los eventos legítimos los lleva a cabo un pequeño grupo de entidades.

### Solución

Asegúrese de que su conjunto de datos incluya al menos 100 entidades con eventos legítimos. Si es necesario, puedes asegurarte de que abarque un período de tiempo más largo.

## 5. Tipo de problema: error

### Descripción

Hay menos de 100 filas en el conjunto de datos. Asegúrese de que haya más de 100 filas en el conjunto de datos total y de que al menos 50 filas estén etiquetadas como fraudulentas.

### Causa

Este error se produce si el conjunto de datos contiene menos de 100 registros. Amazon Fraud Detector requiere datos de al menos 100 eventos (registros) de su conjunto de datos para el entrenamiento de modelos.

### Solución



Asegúrese de tener datos de más de 100 eventos en su conjunto de datos.

## Faltan valores de EVENT\_LABEL o son diferentes

### 1. Tipo de problema: error

#### Descripción

Más del 1% de la columna EVENT\_LABEL es nula o son valores distintos de los definidos en la configuración del modelo. **\$label\_values** Asegúrese de que falte menos del 1% de los valores en la columna EVENT\_LABEL y que los valores sean los definidos en la configuración del modelo. **\$label\_values**

#### Causa

Este error se produce por uno de los siguientes motivos:

- A más del 1% de los registros del archivo CSV que contiene tus datos de entrenamiento les faltan valores en la columna EVENT\_LABEL.
- Más del 1% de los registros del archivo CSV que contiene tus datos de entrenamiento tienen valores en la columna EVENT\_LABEL que son diferentes de los asociados a tu tipo de evento.

El modelo Online Fraud Insights (OFI) requiere que la columna EVENT\_LABEL de cada registro se rellene con una de las etiquetas asociadas al tipo de evento (o mapeadas).

CreateModelVersion

#### Solución

Si este error se debe a que faltan los valores de EVENT\_LABEL, considere la posibilidad de asignar las etiquetas adecuadas a esos registros o eliminarlos del conjunto de datos. Si este error se debe a que las etiquetas de algunos registros no están entre ellas **label\_values**, asegúrese de añadir todos los valores de la columna EVENT\_LABEL a las etiquetas del tipo de evento y asignarlas como fraudulentas o legítimas (fraudulentas, legítimas) en la creación del modelo.

### 2. Tipo de problema: información

#### Descripción

La columna `EVENT_LABEL` contiene valores nulos o valores de etiqueta distintos de los definidos en la configuración del modelo. **\$label\_values** Estos valores incoherentes se convirtieron en valores «no fraudulentos» antes del entrenamiento.

## Causa

Esta información se obtiene por uno de los siguientes motivos:

- Faltan valores en la columna `EVENT_LABEL` en menos del 1% de los registros del archivo CSV que contiene tus datos de entrenamiento
- Menos del 1% de los registros del archivo CSV que contiene tus datos de entrenamiento tienen valores en la columna `EVENT_LABEL` diferentes a los asociados a tu tipo de evento.

El modelo de entrenamiento en ambos casos tendrá éxito. Sin embargo, los valores de etiqueta de los eventos a los que les faltan valores de etiqueta o no están mapeados se convierten en legítimos. Si considera que se trata de un problema, siga la solución que se proporciona a continuación.

## Solución

Si faltan valores de `EVENT_LABEL` en su conjunto de datos, considere eliminar esos registros de su conjunto de datos. Si los valores proporcionados para esos `EVENT_LABELS` no están mapeados, asegúrate de que todos esos valores estén mapeados como fraudulentos o legítimos (fraudulentos, legítimos) para cada evento.

# Faltan valores de `EVENT_TIMESTAMP` o son incorrectos

## 1. Tipo de problema: error

### Descripción

Tu conjunto de datos de entrenamiento contiene `EVENT_TIMESTAMP` con marcas de tiempo que no se ajustan a los formatos aceptados. Asegúrese de que el formato sea uno de los formatos de fecha y hora aceptados.

### Causa

Este error se produce si la columna `EVENT_TIMESTAMP` contiene un valor que no cumple con los formatos de [marca de tiempo admitidos por Amazon Fraud Detector](#).

## Solución

[Asegúrese de que los valores proporcionados para la columna EVENT\\_TIMESTAMP cumplan con los formatos de marca de tiempo admitidos.](#) Si faltan valores en la columna EVENT\_TIMESTAMP, puede rellenarlos con valores utilizando el formato de marca de tiempo compatible o considerar la posibilidad de eliminar el evento por completo en lugar de introducir cadenas como, o. none null missing

### 2. Tipo de problema: error

Tu conjunto de datos de entrenamiento contiene EVENT\_TIMESTAMP y faltan valores. Asegúrate de que no falte ningún valor.

#### Causa

Este error se produce si faltan valores en la columna EVENT\_TIMESTAMP del conjunto de datos. Amazon Fraud Detector requiere que la columna EVENT\_TIMESTAMP del conjunto de datos tenga valores.

#### Solución

[Asegúrese de que la columna EVENT\\_TIMESTAMP de su conjunto de datos tenga valores y que dichos valores cumplan con los formatos de marca de tiempo admitidos.](#) Si faltan valores en la columna EVENT\_TIMESTAMP, puede rellenarlos con valores utilizando el formato de marca de tiempo compatible o considerar la posibilidad de eliminar el evento por completo en lugar de introducir cadenas como, o. none null missing

## Datos no ingeridos

### Tipo de problema: error

#### Descripción

No se han encontrado eventos ingeridos para la formación. Compruebe la configuración de la formación.

#### Causa

Este error se produce si estás creando un modelo con datos de eventos almacenados en Amazon Fraud Detector pero no has importado tu conjunto de datos a Amazon Fraud Detector antes de empezar a entrenar tu modelo.

### Solución

Utilice la operación de `SendEvent` API, la operación de `CreateBatchImportJob` API o la función de importación por lotes de la consola de Amazon Fraud Detector para importar primero los datos de sus eventos y, a continuación, entrenar su modelo. Consulte Conjuntos de [datos de eventos almacenados](#) para obtener más información.

#### Note

Se recomienda esperar 10 minutos después de haber terminado de importar los datos antes de usarlos para entrenar el modelo.

Puedes usar la consola Amazon Fraud Detector para comprobar el número de eventos ya almacenados para cada tipo de evento. Consulte [Visualización de las métricas de los eventos almacenados](#) para obtener más información.

## Variables insuficientes

Tipo de problema: Error

### Descripción

El conjunto de datos debe contener al menos 2 variables adecuadas para el entrenamiento.

### Causa

Este error se produce si el conjunto de datos contiene menos de 2 variables adecuadas para el entrenamiento del modelo. Amazon Fraud Detector considera que una variable es adecuada para el entrenamiento de modelos solo si supera todas las validaciones. Si una variable no pasa la validación, se excluye del entrenamiento del modelo y verá un mensaje en el diagnóstico del entrenamiento del modelo.

### Solución

Asegúrese de que su conjunto de datos tenga al menos dos variables rellenas con valores y de que haya superado todas las validaciones de datos. Ten en cuenta que la fila de metadatos

del evento en la que has proporcionado los encabezados de las columnas (EVENT\_TIMESTAMP, EVENT\_ID, ENTITY\_ID, EVENT\_LABEL, etc.) no se considera variable.

## Falta el tipo de variable o es incorrecto

Tipo de problema: Advertencia

### Descripción

El tipo de datos esperado **\$variable\_name** es NUMÉRICO. Revise y actualice **\$variable\_name** su conjunto de datos y vuelva a entrenar el modelo.

### Causa

Recibirás esta advertencia si una variable está definida como una variable NUMÉRICA, pero en el conjunto de datos tiene valores que no se pueden convertir a NUMÉRICOS. Como resultado, esa variable se excluye del entrenamiento del modelo.

### Solución

Si desea mantenerla como una variable NUMÉRICA, asegúrese de que los valores que proporcione se puedan convertir en números flotantes. Tenga en cuenta que si la variable contiene valores faltantes, no los llene con cadenas como nonenull, omissing. Si la variable contiene valores no numéricos, vuelva a crearla como una variable del tipo CATEGORICAL o FREE\_FORM\_TEXT.

## Faltan valores de variables

Tipo de problema: Advertencia

### Descripción

Faltan **\$threshold** valores superiores a los **\$variable\_name** de en tu conjunto de datos de entrenamiento. Considera la posibilidad de modificar **\$variable\_name** tu conjunto de datos y volver a entrenarlo para mejorar el rendimiento.

### Causa

Recibirás esta advertencia si la variable especificada se descarta porque faltan demasiados valores. Amazon Fraud Detector permite que falten valores en una variable. Sin embargo, si una variable tiene demasiados valores faltantes, no contribuye mucho al modelo y esa variable se descarta durante el entrenamiento del modelo.

## Solución

En primer lugar, compruebe que esos valores faltantes no se deban a errores en la recopilación y preparación de los datos. Si se trata de errores, puedes considerar eliminarlos de tu entrenamiento de modelo. Sin embargo, si cree que esos valores faltantes son valiosos y aun así quiere conservar esa variable, puede rellenar manualmente los valores faltantes con una constante tanto en el entrenamiento del modelo como en la inferencia en tiempo real.

## Valores de variables únicas insuficientes

Tipo de problema: Advertencia

### Descripción

El recuento de valores únicos de **\$variable\_name** es inferior a 100. Revise y actualice **\$variable\_name** su conjunto de datos y vuelva a entrenar el modelo.

### Causa

Recibirá esta advertencia si el número de valores únicos de la variable especificada es inferior a 100. Los umbrales varían según el tipo de variable. Con muy pocos valores únicos, existe el riesgo de que el conjunto de datos no sea lo suficientemente general como para cubrir el espacio de entidades de esa variable. Como resultado, es posible que el modelo no generalice bien las predicciones en tiempo real.

### Solución

En primer lugar, asegúrese de que la distribución variable sea representativa del tráfico empresarial real. Luego, puede adoptar variables más precisas con mayor cardinalidad, por ejemplo, utilizándolas en `full_customer_name` lugar de `first_name` y `last_name` por separado, o cambiar el tipo de variable a CATEGÓRICO, lo que permite una cardinalidad más baja.

## Expresión de variable incorrecta

1. Tipo de problema: Información

### Descripción

Más del 50% de **\$email\_variable\_name** los valores no coinciden con la expresión regular esperada `http://emailregex.com`. Considere la posibilidad de modificar **\$email\_variable\_name** su conjunto de datos y volver a entrenarlo para mejorar el rendimiento.

## Causa

Esta información se muestra si más del 50% de los registros de su conjunto de datos tienen valores de correo electrónico que no cumplen con una expresión de correo electrónico normal y, por lo tanto, no se validan.

## Solución

Formatee los valores de las variables de correo electrónico para que se ajusten a la expresión regular. Si faltan valores de correo electrónico, se recomienda dejarlos vacíos en lugar de rellenarlos con cadenas como `nonnull`, `omissing`.

### 2. Tipo de problema: Información

#### Descripción

Más del 50% de **\$IP\_variable\_name** los valores no coinciden con la expresión regular de las direcciones IPv4 o IPv6 `https://digitalfortress.tech/tricks/top-15 - /. commonly-used-regex`. Considere la posibilidad de modificar su conjunto **\$IP\_variable\_name** de datos y volver a entrenarlo para mejorar el rendimiento.

## Causa

Esta información se muestra si más del 50% de los registros de su conjunto de datos tienen valores de IP que no cumplen con una expresión de IP normal y, por lo tanto, no se validan.

## Solución

Formatee los valores de IP para que se ajusten a la expresión regular. Si faltan valores de IP, se recomienda dejarlos vacíos en lugar de rellenarlos con cadenas como `nonnull`, `omissing`.

### 3. Tipo de problema: Información

#### Descripción

Más del 50% de **\$phone\_variable\_name** los valores no coinciden con la expresión regular básica del teléfono `/ $pattern/`. Considere la posibilidad de modificar su conjunto **\$phone\_variable\_name** de datos y volver a entrenarlo para mejorar el rendimiento.

## Causa

Esta información se muestra si más del 50% de los registros de su conjunto de datos contienen números de teléfono que no cumplen con una expresión de número de teléfono normal y, por lo tanto, no se validan.

### Solución

Formatee los números de teléfono para que se ajusten a la expresión regular. Si faltan números de teléfono, se recomienda dejarlos vacíos en lugar de rellenarlos con cadenas como `nonenu11`, `omissing`.

## Entidades únicas insuficientes

Tipo de problema: Información

### Descripción

El número de entidades únicas es inferior a 1500. Considere incluir más datos para mejorar el rendimiento.

### Causa

Esta información se muestra si el conjunto de datos tiene un número menor de entidades únicas que el número recomendado. El modelo Transaction Fraud Insights (TFI) utiliza conjuntos de series temporales y funciones de transacciones genéricas para ofrecer el mejor rendimiento. Si su conjunto de datos tiene muy pocas entidades únicas, es posible que la mayoría de los datos genéricos, como `IP_ADDRESS` o `EMAIL_ADDRESS`, no tengan valores únicos. Por lo tanto, también existe el riesgo de que este conjunto de datos no sea lo suficientemente general como para cubrir el espacio de entidades de esa variable. Como resultado, es posible que el modelo no se generalice bien en las transacciones de entidades nuevas y nuevas.

### Solución

Incluya más entidades. Amplía el rango de tiempo de tus datos de entrenamiento, si es necesario.



## Cuotas

Su Cuenta de AWS tiene cuotas predeterminadas, anteriormente conocidas como «límites», para cada servicio de. A menos que se indique otra cosa, cada cuota es específica de la región. Puede solicitar un aumento de todas las cuotas web por cuenta de. Para obtener más información, consulte este tema acerca de cómo [solicitar un aumento de cuota](#).

En las siguientes tablas se describen las cuotas de Amazon Fraud Detector por componente.

### Modelos Fraud Detector de

Nombre de la cuota	Cuota predeterminada	Ajustable
Tamaño de los datos de entrenamiento	5 GB	No
Modelos por cuenta	50	No
Verweb por cuenta de	200	No
Versiones de modelos implementados por cuenta	5	No
Trabajos de formación simultáneos por cuenta	3	No
Trabajos de formación simultáneos por modelo	1	No

### Detectores de fraudes de Amazon, variables, resultados, reglas

Nombre de la cuota	Cuota predeterminada	Ajustable
Varipor cuenta por cuenta por cuenta	5000	No
Reglas por cuenta de	5000	No

Nombre de la cuota	Cuota predeterminada	Ajustable
Listas por regla	3	No
Resultados por cuenta por cuenta por cuenta	5000	No
cuenta por cuenta por cuenta por cuenta	100	No
Listas por detector	30	No
Borrador de versiones por detector	100	No
Modelos por versión de detector	10	No
Etiquetas por cuenta por cuenta por cuenta	100	No
Tipos por cuenta por cuenta por cuenta por cuenta	100	No
Tipos por cuenta por cuenta por cuenta por cuenta	100	No

## API Fraud Detector de

Nombre de la cuota	Cuota predeterminada	Ajustable
GetEventPrediction Llamweb por cuenta por cuenta por cuenta de	200 TPS	Sí
Tamaño de la carga útil por llamada a GetEventPrediction la API	256 KB	No

Nombre de la cuota	Cuota predeterminada	Ajustable
Número de entradas por llamada a GetEventPrediction la API	5000	No

## Historial de documentos

La siguiente tabla describe los cambios importantes en la Guía del usuario de Amazon Fraud Detector. También actualizamos la Guía del usuario de Amazon Fraud Detector con frecuencia para abordar los comentarios que nos envía.

Cambio	Descripción	Fecha
<a href="#">Nuevos tipos de variables y datos</a>	Amazon Fraud Detector presenta nuevos tipos de variables y un tipo de datos que puede utilizar para extraer información útil.	5 de junio de 2023
<a href="#">Organización de eventos</a>	La organización de eventos facilita el envío de eventos Servicios de AWS para su procesamiento posterior mediante Amazon. EventBridge	30 de mayo de 2023
<a href="#">Listas</a>	El recurso Listas permite hacer referencia a un conjunto de valores, como direcciones IP o direcciones de correo electrónico, como parte de una regla. Use listas en una regla para permitir o denegar el acceso o una transacción.	14 de febrero de 2023
<a href="#">Explorador de modelos de datos</a>	El explorador de modelos de datos proporciona información sobre los elementos de datos que Amazon Fraud Detector necesita para crear su modelo de detección de fraudes. Utilice el explorador	15 de diciembre de 2022

de modelos de datos antes de preparar su conjunto de datos de eventos.

### [Modelo Account Takeover Insights](#)

Utilice el modelo Account Takeover Insights (ATI) para detectar las cuentas que se ven comprometidas debido a la apropiación malintencionada, la suplantación de identidad o el robo de credenciales.

21 de julio de 2022

### [Actualización del capítulo](#)

Se actualizó el capítulo introductorio con información adicional sobre Amazon Fraud Detector

11 de abril de 2022

### [Enriquecimiento variable](#)

Habilite el enriquecimiento de algunos de los datos sin procesar que proporciona para mejorar el rendimiento de los modelos que utilizan estos elementos de datos y que se entrenaron antes del 8 de febrero de 2022.

8 de febrero de 2022

### [Políticas de exclusión](#)

Utilice políticas de exclusión voluntaria para impedir que los datos de sus eventos se utilicen para desarrollar o mejorar la calidad de Amazon Fraud Detector.

6 de enero de 2022

<a href="#">Prevención adjunta confusa</a>	Crea políticas para evitar que un tercero o una entidad multiservicio manipule a una entidad con permisos para actuar en su nombre y obtener acceso a los recursos de tu cuenta.	6 de diciembre de 2021
<a href="#">Crear conjunto de datos de eventos</a>	Utilice las instrucciones proporcionadas en Crear conjunto de datos de eventos para preparar y recopilar datos para entrenar su modelo.	22 de noviembre de 2021
<a href="#">Explicaciones de predicción</a>	Utilice las explicaciones de predicción para obtener información sobre el impacto de cada variable del evento en las puntuaciones de predicción de fraudes de su modelo.	10 de noviembre de 2021
<a href="#">Solucionar problemas</a>	Utilice la información de Solucionar problemas con los datos de entrenamiento para ayudar a diagnosticar y resolver los problemas que pueda ver en la consola de Amazon Fraud Detector al entrenar su modelo.	11 de octubre de 2021
<a href="#">Modelo de información sobre el fraude en las transacciones</a>	Utilice el modelo Transaction Fraud Insights (TFI) para detectar el fraude en línea o en las card-not-present transacciones.	11 de octubre de 2021

[Eventos almacenados](#)

Almacene los datos de sus eventos en Amazon Fraud Detector y utilícelos para entrenar posteriormente sus modelos. Al almacenar los datos de eventos en Amazon Fraud Detector, puede entrenar modelos que utilicen variables calculadas automáticamente para mejorar el rendimiento, simplificar el reentrenamiento de los modelos y actualizar las etiquetas de fraude para cerrar el ciclo de retroalimentación del aprendizaje automático.

11 de octubre de 2021

[Importancia de la variable modelo](#)

Utilice la importancia de las variables del modelo para obtener información sobre qué es lo que hace que el rendimiento de su modelo aumente o disminuya y cuáles de las variables del modelo son las que más contribuyen. Y, a continuación, modifique su modelo para mejorar el rendimiento general.

9 de julio de 2021

[Integración con el AWS CloudFormation](#)

Úselo AWS CloudFormation para administrar sus recursos de Amazon Fraud Detector.

10 de mayo de 2021

---

<a href="#">Predicciones de lotes</a>	Utilice las predicciones por lotes para obtener predicciones para un conjunto de eventos que no requieren puntuación en tiempo real.	31 de marzo de 2021
<a href="#">Reelaboración del capítulo</a>	Reelaboración de las secciones Cómo empezar y otras	17 de julio de 2020
<a href="#">Versión inicial</a>	Versión inicial	2 de diciembre de 2019



Las traducciones son generadas a través de traducción automática. En caso de conflicto entre la traducción y la versión original de inglés, prevalecerá la versión en inglés.