



Benutzerhandbuch

# Amazon Fraud Detector



Version latest

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

# Amazon Fraud Detector: Benutzerhandbuch

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

Die Handelsmarken und Handelsaufmachung von Amazon dürfen nicht in einer Weise in Verbindung mit nicht von Amazon stammenden Produkten oder Services verwendet werden, durch die Kunden irregeführt werden könnten oder Amazon in schlechtem Licht dargestellt oder diskreditiert werden könnte. Alle anderen Handelsmarken, die nicht Eigentum von Amazon sind, gehören den jeweiligen Besitzern, die möglicherweise zu Amazon gehören oder nicht, mit Amazon verbunden sind oder von Amazon gesponsert werden.

---

# Table of Contents

Was ist Amazon Fraud Detector? .....	1
Vorteile .....	1
Kernkonzepte und Begriffe .....	3
So funktioniert Amazon Fraud Detector .....	6
Erkennen von Betrug mit Amazon Fraud Detector .....	8
Zugriff auf Amazon Fraud Detector .....	10
Verfügbarkeit .....	10
Schnittstellen .....	10
Preisgestaltung .....	11
Für Amazon Fraud Detector einrichten .....	12
Registrieren Sie sich für AWS .....	12
So melden Sie sich für ein AWS-Konto an .....	12
Einen Administratorbenutzer erstellen .....	13
Berechtigungen für den Zugriff auf Amazon Fraud Detector Detector-Schnittstellen einrichten ...	14
Richten Sie Schnittstellen für den Zugriff auf Amazon Fraud Detector ein mit .....	16
Rufen Sie die Amazon Fraud Detector Detector-Konsole auf .....	16
Einrichten von AWS CLI .....	16
Richten Sie das AWS SDK ein .....	17
Erste Schritte mit Amazon Fraud Detector .....	18
Beispieldatensatz abrufen und hochladen .....	18
Tutorial: Erste Schritte mit der Amazon Fraud Detector Detector-Konsole .....	20
Teil A: Aufbau, Schulung und Bereitstellung eines Amazon Fraud Detector Detector-	
Modells .....	21
Teil B: Generieren Sie Betrugsvorhersagen .....	25
Tutorial: Erste Schritte mit der Verwendung von AWS SDK for Python (Boto3) .....	31
Voraussetzungen .....	31
Erste Schritte .....	32
(Optional) Erkunden Sie die Amazon Fraud Detector Detector-APIs mit einem Jupyter-	
Notebook (iPython) .....	41
Nächste Schritte .....	42
Ereignis-Dataset .....	43
Struktur von Ereignisdataset .....	44
Rufen Sie die Anforderungen für Ereignisdatensätze mit dem Datenmodell-Explorer ab .....	45
Datenmodell-Explorer .....	45

Ereignisdaten sammeln .....	46
Datensatzvalidierung .....	53
Datensatzspeicher .....	54
Ereignistyp .....	55
Einen Ereignistyp erstellen .....	55
Erstellen Sie den Ereignistyp in der Amazon Fraud Detector-Konsole .....	56
Erstellen Sie einen Ereignistyp mit dem AWS SDK for Python (Boto3) .....	57
Löschen Sie ein Ereignis oder einen Ereignistyp .....	58
Speicherung der Ereignisdaten .....	60
Speichern Sie Ihre Eventdaten extern mit Amazon S3 .....	61
Erstellen einer CSV-Datei .....	61
Laden Sie Ihre Ereignisdaten in einen Amazon S3 Bucket hoch .....	64
Speichern Sie Ihre Eventdaten intern mit Amazon Fraud Detector .....	65
Bereiten Sie die Ereignisdaten für die Speicherung vor .....	66
Speichern von Eventdaten per Batch-Import .....	68
Speichern Sie Ereignisdaten mithilfe der GetEventPredictions API-Operation .....	83
Speichern Sie Ereignisdaten mithilfe der SendEvent API-Operation .....	83
Details zu gespeicherten Ereignisdaten abrufen .....	85
Metriken des gespeicherten Ereignisdatensatzes anzeigen .....	85
Ereignisorchestrierung .....	87
Einrichten der Ereignisorchestrierung .....	88
Aktivieren der Ereignisorchestrierung in Amazon Fraud Detector .....	89
Aktivieren der Ereignisorchestrierung in der Amazon Fraud Detector-Konsole .....	89
Aktivieren der Ereignisorchestrierung mithilfe der AWS SDK for Python (Boto3) .....	90
Deaktivieren der Ereignisorchestrierung in Amazon Fraud Detector .....	90
Deaktivieren der Ereignisorchestrierung in der Amazon Fraud Detector-Konsole .....	90
Deaktivieren der Ereignisorchestrierung mithilfe der AWS SDK for Python (Boto3) .....	91
Modell .....	92
Wählen Sie einen Modelltyp .....	92
Einblicke in Online-Betrug .....	93
Einblicke in Transaktionsbetrug .....	95
Einblicke in die Kontoübernahme .....	97
Ein Modell erstellen .....	104
Trainieren und Bereitstellen eines Modells mithilfe der AWS SDK for Python (Boto3) .....	104
Modellwerte .....	106
Modellleistungsmetriken .....	107

Wichtigkeit von Modellvariablen .....	110
Verwenden von Werten für die Wichtigkeit von Modellvariablen .....	111
Auswerten der Wichtigkeitswerte von Modellvariablen .....	112
Anzeigen der Rangfolge der Wichtigkeit von Modellvariablen .....	113
Verstehen, wie der Wert für die Wichtigkeit der Modellvariablen berechnet wird .....	113
Importieren eines SageMaker Modells .....	114
Importieren eines SageMaker Modells mit der AWS SDK for Python (Boto3) .....	114
Löschen eines Modell .....	115
Detektor .....	118
Erstellen Sie einen Detektor .....	118
Erstellen Sie einen Detektor in der Amazon Fraud Detector-Konsole .....	118
Erstellen Sie einen Detektor mit demAWS SDK for Python (Boto3) .....	122
Erstellen Sie eine Detektorversion .....	122
Modus zur Regelausführung .....	123
Erstellen Sie eine Detektorversion mit demAWS SDK for Python (Boto3) .....	123
Löschen Sie einen Detektor, eine Detektorversion oder eine Regelversion .....	124
Ressourcen .....	127
Variablen .....	127
Datentypen .....	127
Standardwert .....	128
Variablentypen .....	128
Variable Anreicherungen .....	141
Erstellen Sie eine Variable .....	148
Löschen Sie eine Variable .....	150
Bezeichnungen .....	151
Hinzufügen .....	152
Kennzeichnung aktualisieren .....	153
Aktualisierung von Ereignisbezeichnungen in Ereignisdaten, die in Amazon Fraud Detector gespeichert sind .....	153
Kennzeichnung .....	154
Regeln .....	155
Referenz zur Regelsprache .....	156
Regeln erstellen .....	161
Regel aktualisieren .....	163
Listen .....	165
Erstellen einer Liste .....	165

Einträge zu einer Liste hinzufügen .....	167
Weisen Sie einer Liste einen Variablentyp zu .....	168
Löschen einer Liste .....	170
Einträge aus einer Liste löschen .....	170
Alle Einträge aus einer Liste löschen .....	171
Ergebnisse .....	172
Ein Ergebnis erstellen .....	173
Ein Ergebnis löschen .....	174
Entität .....	175
Entitstyp erstellen .....	175
Entitstyp löschen .....	176
Ressourcen verwalten mitAWS CloudFormation .....	177
Amazon Fraud Detector .....	177
Amazon Amazon Fraud Detector .....	178
Amazon Fraud CloudFormation Detector .....	178
AWS CloudFormationBeispielVorlage für Amazon Amazon Amazon Amazon Fraud Detector .....	179
Weitere Informationen zu AWS CloudFormation .....	180
Fraud Preects .....	181
Vorhersage in Echtzeit .....	182
So funktioniert die Betrugsvorhersage in Echtzeit .....	182
Betrugsprognose in Echtzeit abrufen .....	183
Stapelvoraussagen .....	184
So funktionieren Batch-Prognosen .....	184
Eingabe- und Ausgabedateien .....	185
Batch-Prognosen abrufen .....	185
Anleitung zu IAM-Rollen .....	187
Holen Sie sich Betrugsvorhersagen im Batch-Modus mit dem AWS SDK for Python (Boto3) .....	187
Erläuterungen zur Vorhersage .....	188
Anzeigen von Vorhersageerklärungen .....	190
Verstehen, wie Vorhersageerklärungen berechnet werden .....	192
Sicherheit .....	193
Datenschutz .....	194
Verschlüsselung im Ruhezustand .....	195
Verschlüsselung während der Übertragung .....	195

Schlüsselverwaltung .....	195
VPC-Endpunkte (AWS PrivateLink) .....	197
Abmeldung .....	200
Identity and Access Management .....	200
Zielgruppe .....	201
Authentifizierung mit Identitäten .....	201
Verwalten des Zugriffs mit Richtlinien .....	205
Funktionsweise von Amazon Fraud Detector mit IAM .....	208
Beispiele für identitätsbasierte Richtlinien .....	213
Confused-Deputy-Prävention .....	222
Fehlerbehebung .....	224
Überwachen von Amazon Fraud Detector .....	227
Compliance-Validierung .....	227
Ausfallsicherheit .....	229
Sicherheit der Infrastruktur .....	229
Überwachen von Amazon Fraud Detector .....	231
Überwachung mit CloudWatch .....	231
Verwenden von CloudWatch Metriken für Amazon Fraud Detector. ....	232
Metriken für Amazon Fraud Detector .....	234
Protokollieren von API-Aufrufen von Amazon Fraud Detector mit AWS CloudTrail .....	239
Informationen zu Amazon Fraud Detector in CloudTrail .....	239
Grundlegendes zu Protokolldateieinträgen von Amazon Fraud Detector .....	240
Fehlerbehebung .....	242
Beheben von Problemen mit Trainingsdaten .....	242
Instabile Betrugsrate im angegebenen Datensatz .....	243
Unzureichende Daten .....	243
Fehlende oder andere EVENT_LABEL-Werte .....	246
Fehlende oder falsche EVENT_TIMESTAMP-Werte .....	247
Nicht aufgenommene Daten .....	248
Unzureichende Variablen .....	249
Fehlender oder falscher Variablentyp .....	250
Fehlende Variablenwerte .....	250
Unzureichende eindeutige Variablenwerte .....	251
Falscher Variablenausdruck .....	252
Unzureichende eindeutige Entitäten .....	253
Kontingente .....	255

---

Amazon Fraud Detector Modelle .....	255
Amazon Fraud Detector-Detektoren//Variablen/Ergebnisse/Regeln .....	255
Amazon Fraud Detector API .....	256
Dokumentverlauf .....	257
.....	cclxii



# Was ist Amazon Fraud Detector?

Amazon Fraud Detector ist ein vollständig verwalteter Service zur Betrugserkennung, der die Erkennung potenziell betrügerischer Aktivitäten online automatisiert. Zu diesen Aktivitäten gehören unbefugte Transaktionen und die Erstellung gefälschter Konten. Amazon Fraud Detector verwendet Machine Learning, um Ihre Daten zu analysieren. Dies geschieht auf eine Weise, die auf dem Fachwissen von mehr als 20 Jahren Betrugserkennung bei Amazon aufbaut.

Sie können Amazon Fraud Detector verwenden, um maßgeschneiderte Modelle zur Betrugserkennung zu erstellen, eine Entscheidungslogik zur Interpretation der Betrugsbewertungen des Modells hinzuzufügen und Ergebnisse zuzuweisen, z. B. für jede mögliche Betrugsbewertung bestehen oder zur Überprüfung senden. Mit Amazon Fraud Detector benötigen Sie kein Fachwissen für Machine Learning, um betrügerische Aktivitäten zu erkennen.

Sammeln und bereiten Sie zunächst Betrugsdaten vor, die Sie in Ihrer Organisation gesammelt haben. Amazon Fraud Detector verwendet diese Daten dann, um ein benutzerdefiniertes Betrugserkennungsmodell in Ihrem Namen zu trainieren, zu testen und bereitzustellen. Im Rahmen dieses Prozesses verwendet Amazon Fraud Detector Machine-Learning-Modelle, die Betrugsmuster von AWS und Amazons eigenem Betrugswissen gelernt haben, um Ihre Betrugsdaten zu bewerten und Modellbewertungen und ModelleLeistungsdaten zu generieren. Sie konfigurieren die Entscheidungslogik, um die Punktzahl des Modells zu interpretieren und Ergebnisse für den Umgang mit jeder Betrugsbewertung zuzuweisen.

## Vorteile

Amazon Fraud Detector bietet die folgenden Vorteile. Diese Vorteile ermöglichen es Ihnen, Betrug schnell zu erkennen, ohne die Zeit und Ressourcen investieren zu müssen, die traditionell erforderlich sind, um ein Betrugsmanagementsystem aufzubauen und zu unterhalten.

### Automatisierte Erstellung von Betrugsmodellen

Die Betrugserkennungsmodelle von Amazon Fraud Detector sind vollständig automatisierte Machine-Learning-Modelle, die auf Ihre spezifischen Geschäftsanforderungen zugeschnitten sind. Sie können Amazon Fraud Detector-Modelle verwenden, um potenzielle Betrugsfälle bei Online-Transaktionen zu identifizieren, z. B. bei der Erstellung neuer Konten, Online-Zahlungen und beim Checkout für Gäste.

Da Betrugsmodelle durch einen automatisierten Prozess erstellt werden, können Sie viele der Schritte im Zusammenhang mit der Erstellung und dem Training eines Modells weglassen. Zu diesen

Schritten gehören Datenvalidierung und -anreicherung, Feature-Engineering, Algorithmusauswahl, Hyperparameteroptimierung und Modellbereitstellung.

Um ein Betrugserkennungsmodell mit Amazon Fraud Detector zu erstellen, laden Sie nur den historischen Betrugsdatensatz Ihres Unternehmens hoch und wählen den Modelltyp aus. Dann findet Amazon Fraud Detector automatisch den für Ihren Anwendungsfall am besten geeigneten Algorithmus zur Betrugserkennung und erstellt das Modell. Sie müssen weder die Codierung kennen noch über Machine Learning verfügen, um Modelle zur Betrugserkennung zu erstellen.

### Betrügermodelle, die sich weiterentwickeln und lernen

Modelle zur Betrugserkennung müssen sich ständig weiterentwickeln, um mit der sich ändernden Betrugssituation Schritt zu halten. Amazon Fraud Detector tut dies automatisch, indem es Informationen wie das Alter des Kontos, die Zeit seit der letzten Aktivität und die Anzahl der Aktivitäten berechnet. Das Ergebnis ist, dass Ihr Modell den Unterschied zwischen vertrauenswürdigen Kunden lernt, die häufig Transaktionen durchführen, und den kontinuierlichen Versuchen, die für Betrüger typisch sind. Dies trägt dazu bei, die Leistung Ihres Modells zwischen den Neutrainingsitzungen länger aufrechtzuerhalten.

### Leistungsvisualisierung für Betrügermodelle

Nachdem Ihr Modell anhand der von Ihnen bereitgestellten Daten trainiert wurde, überprüft Amazon Fraud Detector die Leistung Ihres Modells. Es bietet auch visuelle Tools, mit denen Sie die Leistung bewerten können. Für jedes Modell, das Sie trainieren, können Sie den Modellleistungswert, das Ergebnisverteilungsdiagramm, die Konfusionsmatrix, die Schwellenwerttabelle und alle von Ihnen bereitgestellten Eingaben nach ihren Auswirkungen auf die Modellleistung geordnet sehen. Mit diesen Leistungstools können Sie erfahren, wie Ihr Modell abschneidet und welche Eingaben die Leistung Ihres Modells beeinflussen. Bei Bedarf können Sie Ihr Modell anpassen, um seine Gesamtleistung zu verbessern.

### Betrugsvorhersage

Amazon Fraud Detector generiert Betrugsvorhersagen für die Geschäftsaktivitäten Ihrer Organisation. Betrugsvorhersage ist eine Bewertung einer Geschäftsaktivität auf Betrugsrisiko. Amazon Fraud Detector generiert Vorhersagen mithilfe der Vorhersagelogik mit den Daten, die der Aktivität zugeordnet sind. Sie haben diese Daten bei der Erstellung Ihres Betrugserkennungsmodells angegeben. Sie können Betrugsprognosen für eine einzelne Aktivität in Echtzeit abrufen oder Betrugsprognosen für eine Reihe von Aktivitäten offline abrufen.

### Erläuterung der Betrugsvorhersage

Amazon Fraud Detector generiert im Rahmen des Betrugsvorhersageprozesses Vorhersageerklärungen. Vorhersageerklärungen geben Aufschluss darüber, wie sich jedes Datenelement, das zum Trainieren Ihres Modells verwendet wurde, auf den Betrugsvorhersagewert Ihres Modells ausgewirkt hat. Vorhersageerklärungen werden mithilfe von visuellen Tools wie Tabellen und Diagrammen bereitgestellt. Sie können diese Tools verwenden, um visuell zu identifizieren, wie stark jedes Datenelement auf die Vorhersagewerte wirkt. Anschließend können Sie diese Informationen verwenden, um die Betrugsmuster in Ihrem Datensatz zu analysieren und gegebenenfalls Verzerrungen zu erkennen. Zuletzt können Sie die Prognoseerklärungen auch verwenden, um die wichtigsten Risikoindikatoren während eines manuellen Betrugsermittlungsprozesses zu identifizieren. Auf diese Weise können Sie die Ursachen eingrenzen, die zu falsch positiven Vorhersagen führen.

## Regelbasierte Aktionen

Nachdem Ihr Betrugserkennungsmodell trainiert wurde, können Sie Regeln hinzufügen, um Maßnahmen für die ausgewerteten Daten zu ergreifen, z. B. die Daten zu akzeptieren, Daten zur Überprüfung zu senden oder weitere Daten zu sammeln. Eine Regel ist eine Bedingung, die Amazon Fraud Detector mitteilt, wie Daten während der Betrugsvorhersage zu interpretieren sind. Sie können beispielsweise eine Regel erstellen, die verdächtige Kundenkonten kennzeichnet, die überprüft werden sollen. Sie können diese Regel so festlegen, dass sie initiiert wird, wenn sowohl der erkannte Modellwert größer als Ihr vordefinierter Schwellenwert ist als auch der Autorisierungscode der Kontozahlung (AUTH\_CODE) ungültig ist.

## Kernkonzepte und Begriffe

Im Folgenden finden Sie eine Liste der wichtigsten Konzepte und Begriffe, die in Amazon Fraud Detector verwendet werden:

### Ereignis

Ein Ereignis ist die Geschäftsaktivität Ihrer Organisation, die auf Betrugsrisiko hin bewertet wird. Amazon Fraud Detector generiert Betrugsvorhersagen für Ereignisse.

### Label (Bezeichnung)

Ein Label klassifiziert ein einzelnes Ereignis als betrügerisches oder legitimes Ereignis. Labels werden verwendet, um Machine-Learning-Modelle in Amazon Fraud Detector zu trainieren.

## Entität

Eine Entität stellt dar, wer das Ereignis ausführt. Sie geben die Entitäts-ID als Teil der Betrugsdaten Ihres Unternehmens an, um die spezifische Entität anzugeben, die das Ereignis durchgeführt hat.

## Ereignistyp

Ein Ereignistyp definiert die Struktur für ein Ereignis, das an Amazon Fraud Detector gesendet wird. Dazu gehören die im Rahmen des Ereignisses gesendeten Daten, die Entität, die das Ereignis ausführt (z. B. ein Kunde), und die Labels, die das Ereignis klassifizieren. Beispiele für Ereignistypen sind Online-Zahlungstransaktionen, Kontoregistrierungen und Authentifizierung.

## Entitätstyp

Ein Entitätstyp klassifiziert die Entität. Zu den Beispielklassifizierungen gehören Kunden, Händler oder Konto.

## Ereignisdatensatz

Der Ereignisdatensatz ist die historischen Daten einer bestimmten Geschäftsaktivität oder eines Ereignisses Ihres Unternehmens. Die Veranstaltung Ihres Unternehmens könnte beispielsweise die Online-Kontoregistrierung sein. Daten aus einem einzelnen Ereignis (Registrierung) können die zugehörige IP-Adresse, E-Mail-Adresse, Rechnungsadresse und den Zeitstempel des Ereignisses enthalten. Sie stellen Amazon Fraud Detector einen Ereignisdatensatz zur Verfügung, um Modelle zur Betrugserkennung zu erstellen und zu trainieren.

## Modell

Ein Modell ist eine Ausgabe von Machine-Learning-Algorithmen. Diese Algorithmen werden im Code implementiert und auf von Ihnen bereitgestellten Ereignisdaten ausgeführt.

## Modelltyp

Der Modelltyp definiert die Algorithmen, Anreicherungen und Feature-Transformationen, die während des Modelltrainings verwendet werden. Außerdem werden die Datenanforderungen für das Training des Modells definiert. Diese Definitionen dienen dazu, Ihr Modell für eine bestimmte Art von Betrug zu optimieren. Sie geben den Modelltyp an, der beim Erstellen Ihres Modells verwendet werden soll.

## Modelltrainings

Modelltraining ist der Prozess der Verwendung eines bereitgestellten Ereignisdatensatzes, um ein Modell zu erstellen, das betrügerische Ereignisse vorhersagen kann. Alle Schritte

des Modelltrainingsprozesses sind vollständig automatisiert. Zu diesen Schritten gehören Datenvalidierung, Datentransformation, Feature-Engineering, Algorithmusauswahl und Modelloptimierung.

## Modellbewertung

Die Modellbewertung ist das Bewertungsergebnis der historischen Betrugsdaten Ihres Unternehmens. Während des Modelltrainingsprozesses bewertet Amazon Fraud Detector den Datensatz auf betrügerische Aktivitäten und generiert eine Punktzahl zwischen 0 und 1000. Für diese Punktzahl steht 0 für ein geringes Betrugsrisiko, während 1 000 für das höchste Betrugsrisiko steht. Der Wert selbst steht in direktem Zusammenhang mit der falsch positiven Rate (FPR).

## Modellversion

Eine Modellversion ist eine Ausgabe des Trainings eines Modells.

## Modellbereitstellung

Die Modellbereitstellung ist ein Prozess, um eine Modellversion zu aktivieren und sie für die Generierung von Betrugsvorhersagen verfügbar zu machen.

## Amazon- SageMaker Modellendpunkt

Zusätzlich zur Erstellung von Modellen mit Amazon Fraud Detector können Sie optional von gehostete Modellendpunkte in Amazon Fraud Detector SageMaker-Bewertungen verwenden.

Weitere Informationen zum Erstellen eines Modells in SageMaker finden Sie unter [Trainieren eines Modells mit Amazon SageMaker](#).

## Detektor

Ein Detektor enthält die Erkennungslogik wie das Modell und die Regeln für ein bestimmtes Ereignis, das Sie auf Betrug prüfen möchten. Sie erstellen einen Detektor mit einer Modellversion.

## Detektor-Version

Ein Detektor kann mehrere Versionen haben, wobei jede Version den Status `Draft`, `Active` oder `Inactive` hat. Es kann jeweils nur eine Detektorversion den `Active` Status haben.

## Variable

Eine Variable stellt ein Datenelement dar, das einem Ereignis zugeordnet ist, das Sie bei einer Betrugsvorhersage verwenden möchten. Variablen können entweder mit einem Ereignis als Teil einer Betrugsvorhersage gesendet oder abgeleitet werden, z. B. durch die Ausgabe eines Amazon Fraud Detector-Modells oder Amazon SageMaker.

## Regel

Eine Regel ist eine Bedingung, die Amazon Fraud Detector mitteilt, wie Variablenwerte während einer Betrugsvorhersage interpretiert werden. Eine Regel besteht aus einer oder mehreren Variablen, einem logischen Ausdruck und einem oder mehreren Ergebnissen. Die in der Regel verwendeten Variablen müssen Teil des Ereignisdatensatzes sein, den der Detektor auswertet. Darüber hinaus muss jedem Detektor mindestens eine Regel zugeordnet sein.

## Ergebnis

Dies ist das Ergebnis oder die Ausgabe einer Betrugsvorhersage. Jede Regel, die in einer Betrugsvorhersage verwendet wird, muss ein oder mehrere Ergebnisse angeben.

## Betrugsvorhersage

Die Betrugsvorhersage ist eine Bewertung des Betrugs entweder für ein einzelnes Ereignis oder eine Reihe von Ereignissen. Amazon Fraud Detector generiert Betrugsvorhersagen für ein einzelnes Online-Ereignis in Echtzeit, indem es synchron eine Modellbewertung und ein Ergebnis auf der Grundlage der Regeln bereitstellt. Amazon Fraud Detector generiert Betrugsvorhersagen für eine Reihe von Ereignissen offline. Sie können die Vorhersagen verwenden proof-of-concept, um einen Offline- durchzuführen oder das Betrugsrisiko stündlich, täglich oder wöchentlich nachträglich zu bewerten.

## Erläuterung der Betrugsvorhersage

Erklärungen zur Betrugsvorhersage geben Aufschluss darüber, wie sich jede Variable auf den Betrugsvorhersagewert Ihres Modells ausgewirkt hat. Es enthält Informationen darüber, wie jede Variable die Risikobewertungen in Bezug auf das Ausmaß (im Bereich von 0 bis 5, wobei 5 am höchsten ist) und die Richtung (das Antreiben der Punktzahl höher oder niedriger) beeinflusst.

# So funktioniert Amazon Fraud Detector

Amazon Fraud Detector erstellt ein maschinelles Lernmodell, das darauf zugeschnitten ist, potenzielle betrügerische Online-Aktivitäten in Ihrem Unternehmen zu erkennen. Bevor Sie beginnen, geben Sie Ihren geschäftlichen Anwendungsfall. Abhängig von Ihrem geschäftlichen Anwendungsfall empfiehlt Amazon Fraud Detector einen Modelltyp, der verwendet wird, um ein Modell zur Betrugserkennung für Sie zu erstellen. Darüber hinaus bietet es auch Einblicke in die Datenelemente, die Sie als Teil der historischen Daten Ihres Unternehmens bereitstellen müssen. Amazon Fraud Detector verwendet den historischen Datensatz, um automatisch ein maßgeschneidertes Modell für Sie zu erstellen und zu trainieren.

Der automatisierte Modelltrainingsprozess umfasst die Auswahl eines Algorithmus für maschinelles Lernen, der Betrug für Ihren spezifischen Geschäftsanwendungsfall erkennt, die Validierung der von Ihnen bereitgestellten Daten und die Durchführung von Datenmanipulationen zur Verbesserung der Modellleistung. Nach dem Training des Modells generiert Amazon Fraud Detector Modellwerte und andere Modellleistungskennzahlen. Sie können den Score und die Leistungskennzahlen verwenden, um die Leistung des Modells zu bewerten. Bei Bedarf können Sie dem Datensatz, den Sie für das Training bereitgestellt haben, Datenelemente hinzufügen oder daraus entfernen und das Modell erneut trainieren, um die Modellbewertung zu verbessern.

Nachdem das Modell erstellt, trainiert und aktiviert wurde, müssen Sie eine Entscheidungslogik, auch Regeln genannt, konfigurieren, die dem Modell vorgibt, wie die von Ihrem Unternehmen generierten Daten zu interpretieren sind, und Ergebnisse für den Umgang mit der Interpretation der einzelnen Aktivitäten zuweisen. Bei den Ergebnissen kann es sich um Maßnahmen wie die Genehmigung oder Überprüfung der Aktivität oder um Risikostufen der Aktivität handeln, z. B. hohes Risiko, mittleres Risiko und niedriges Risiko.

Ein Detektor ist ein Behälter, der Ihr Modell und die zugehörigen Regeln enthält. Sie müssen den Detektor erstellen, testen und in Ihrer Produktionsumgebung einsetzen.

Der Detektor, der in Ihrer Produktionsumgebung eingesetzt wird, bietet Funktionen zur Betrugserkennung für Ihre Geschäftsanwendungen. Bei der Betrugsbeurteilung vergleicht das Modell alle eingehenden Daten aus Ihrer Geschäftstätigkeit mit den historischen Daten Ihres Unternehmens und verwendet die ausgeklügelten Algorithmen für maschinelles Lernen mit den Regeln, die Sie zur Analyse der Ergebnisse und zur Zuordnung der Ergebnisse erstellt haben. Mit Amazon Fraud Detector können Sie entweder Daten aus einer einzelnen Geschäftsaktivität in Echtzeit oder Daten aus mehreren Geschäftsaktivitäten offline auswerten.

Nehmen wir an, Sie haben ein Unternehmen, das Online-Geldtransfers als eine seiner Aktivitäten anbietet. Sie möchten Amazon Fraud Detector verwenden, um betrügerische Anfragen nach Geldtransfers in Echtzeit zu erkennen. Um zu beginnen, müssen Sie Amazon Fraud Detector zunächst Daten aus früheren Überweisungsanfragen zur Verfügung stellen. Amazon Fraud Detector verwendet diese Daten, um ein Modell zu erstellen und zu trainieren, das darauf zugeschnitten ist, betrügerische Anfragen nach Geldtransfers zu erkennen. Anschließend erstellen Sie einen Detektor, indem Sie das Modell hinzufügen und Regeln für Ihr Modell zur Interpretation der Daten konfigurieren. Ein Beispiel für eine Regel für Online-Überweisungsaktivitäten kann sein, wenn die Anfrage für eine Geldüberweisung vonxyz@example.com E-Mail-Adresse, senden Sie die Überprüfungsanfrage. Wenn in der Produktionsumgebung Ihres Unternehmens ein Antrag auf Überweisung eingeht, analysiert das Modell die Daten, die mit der Anfrage geliefert wurden, und

verwendet die Regel, um das Ergebnis zuzuweisen. Sie können dann je nach zugewiesenem Ergebnis eine Aktion auf die Anfrage anwenden.

Amazon Fraud Detector verwendet Komponenten wie Trainingsdatensatz, Modell, Detektor, Regeln und Ergebnisse, um Ihrem Unternehmen eine Logik zur Betrugsbewertung zur Verfügung zu stellen.

Informationen über den Workflow, den Sie zur Betrugserkennung mit Amazon Fraud Detector verwenden, finden Sie unter [Erkennen von Betrug mit Amazon Fraud Detector](#)

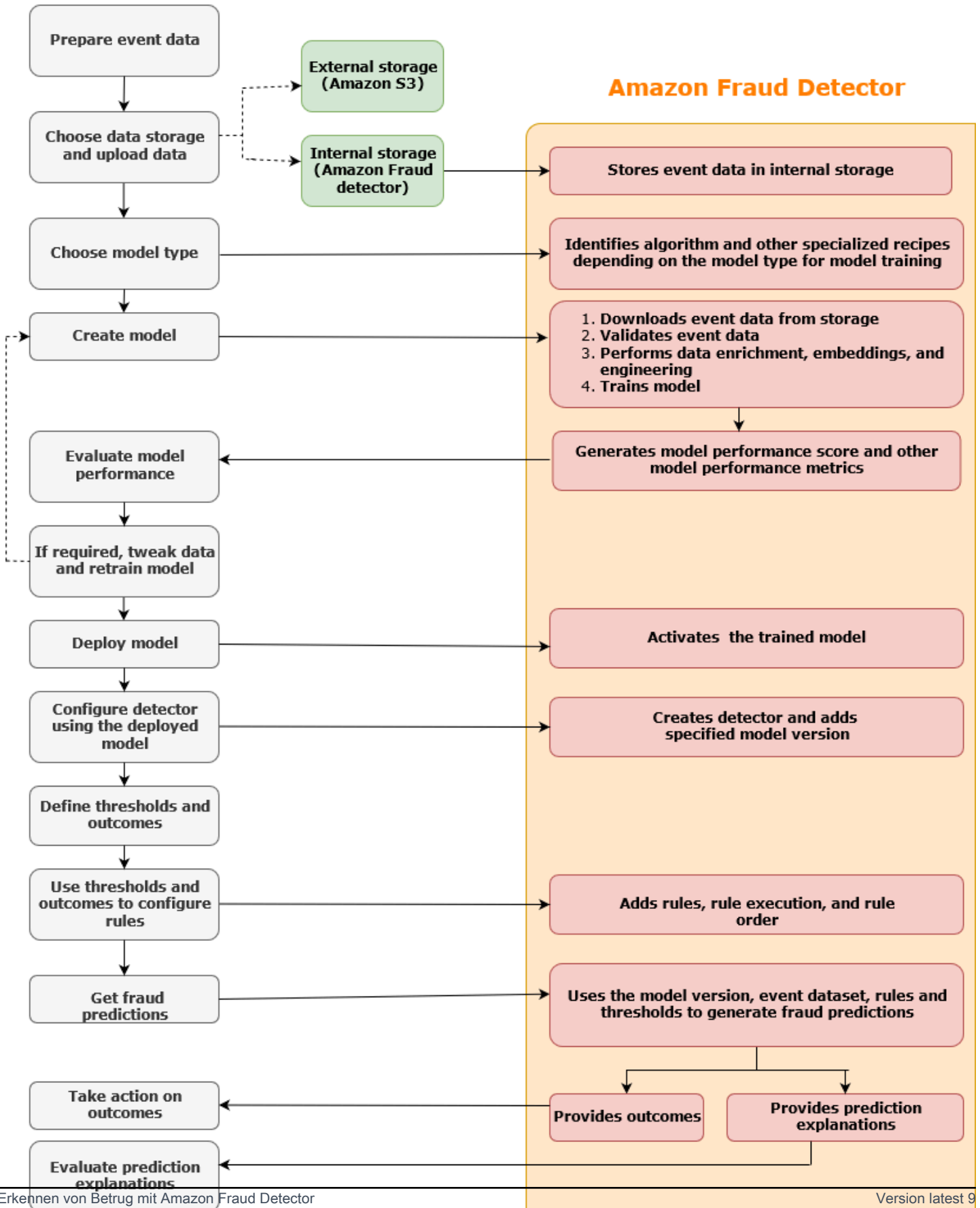
## Erkennen von Betrug mit Amazon Fraud Detector

In diesem Abschnitt wird ein typischer Workflow zur Erkennung von Betrug mit Amazon Fraud Detector beschrieben. Außerdem wird zusammengefasst, wie Sie diese Aufgaben ausführen können. Das folgende Diagramm bietet einen allgemeinen Überblick über den Workflow zur Erkennung von Betrug mit Amazon Fraud Detector.



# You

# Amazon Fraud Detector



Die Betrugserkennung ist ein kontinuierlicher Prozess. Nachdem Sie Ihr Modell bereitgestellt haben, stellen Sie sicher, dass Sie seine Leistungswerte und Metriken auf der Grundlage der Vorhersageerklärungen bewerten. Auf diese Weise können Sie die wichtigsten Risikoindikatoren identifizieren, Ursachen eingrenzen, die zu falsch positiven Ergebnissen führen, Betrugsmuster in Ihrem gesamten Datensatz analysieren und Verzerrungen erkennen, falls vorhanden. Um die Genauigkeit der Vorhersagen zu erhöhen, können Sie Ihren Datensatz so anpassen, dass er neue oder überarbeitete Daten enthält. Anschließend können Sie Ihr Modell mit dem aktualisierten Datensatz neu trainieren. Sobald mehr Daten verfügbar sind, trainieren Sie Ihr Modell weiter, um die Genauigkeit zu erhöhen.

## Zugriff auf Amazon Fraud Detector

Amazon Fraud Detector ist in mehreren verfügbar AWS-Regionen und kann über AWS Schnittstellen aufgerufen werden.

### Verfügbarkeit

Amazon Fraud Detector ist in den USA Ost (Nord-Virginia), USA Ost (Ohio), USA West (Oregon), Europa (Irland), Asien-Pazifik (Singapur) und Asien-Pazifik (Sydney) verfügbar AWS-Regionen.

### Schnittstellen

Sie können mithilfe einer der folgenden Schnittstellen Modelle und Detektoren zur Betrugserkennung erstellen, trainieren, bereitstellen, testen, ausführen und verwalten:

**AWS Management Console** – Amazon Fraud Detector bietet eine webbasierte Benutzeroberfläche, die Amazon Fraud Detector-Konsole. Wenn Sie sich für ein registriert haben AWS-Konto, können Sie auf die Amazon Fraud Detector-Konsole zugreifen. Weitere Informationen finden Sie unter [Einrichten von Amazon Fraud Detector](#).

**AWS Command Line Interface (AWS CLI)** – Bietet eine Schnittstelle, mit der Sie mit einer Vielzahl von interagieren können AWS-Services, einschließlich Amazon Fraud Detector, indem Sie Befehle in Ihrer Befehlszeilen-Shell verwenden. -AWS CLIBefehle für Amazon Fraud Detector implementieren Funktionen, die denen der Amazon Fraud Detector-Konsole entsprechen.

**AWS SDK** – Bietet sprachspezifische APIs und verwaltet viele der Verbindungsdetails, wie Signaturberechnung, Verarbeitung von Wiederholungsversuchen und Fehlerbehandlung. Weitere Informationen finden Sie auf der Seite [Tools to build AWS](#), scrollen Sie nach unten zum Abschnitt SDK und wählen Sie Pluszeichen (+), um den Abschnitt zu erweitern.

AWS CloudFormation – Stellt Vorlagen bereit, mit denen Sie Ihre Ressourcen und Eigenschaften von Amazon Fraud Detector definieren können. Weitere Informationen finden Sie unter [Ressourcentypreferenz für Amazon Fraud Detector](#) im AWS CloudFormation -Benutzerhandbuch.

## Preisgestaltung

Mit Amazon Fraud Detector zahlen Sie nur für das, was Sie tatsächlich nutzen. Es fallen keine Mindestgebühren oder Vorausleistungen an. Ihnen werden die Rechenstunden berechnet, die zum Trainieren und Hosten Ihrer Modelle verwendet werden, die Menge des von Ihnen verwendeten Speichers und die Menge der von Ihnen getroffenen Betrugsprognosen. Weitere Informationen finden Sie unter [Amazon Fraud Detector – Preise](#).

# Für Amazon Fraud Detector einrichten

Um Amazon Fraud Detector verwenden zu können, benötigen Sie zunächst ein Amazon Web Services (AWS) -Konto und anschließend müssen Sie Berechtigungen einrichten, die Ihnen AWS-Konto Zugriff auf alle Schnittstellen gewähren. Später, wenn Sie mit der Erstellung Ihrer Amazon Fraud Detector-Ressourcen beginnen, müssen Sie Berechtigungen erteilen, die es Amazon Fraud Detector ermöglichen, auf Ihr Konto zuzugreifen, um Aufgaben in Ihrem Namen auszuführen und auf Ressourcen zuzugreifen, die Ihnen gehören.

Führen Sie die folgenden Aufgaben in diesem Abschnitt aus, um sich für die Verwendung von Amazon Fraud Detector einzurichten:

- Melden Sie sich an für AWS.
- Richten Sie Berechtigungen ein, die Ihnen AWS-Konto den Zugriff auf die Schnittstellen von Amazon Fraud Detector ermöglichen.
- Richten Sie Schnittstellen ein, die Sie für den Zugriff auf Amazon Fraud Detector verwenden möchten.

Nachdem Sie diese Schritte abgeschlossen haben, finden Sie weitere Informationen [Erste Schritte mit Amazon Fraud Detector](#) zu den ersten Schritten mit Amazon Fraud Detector.

## Registrieren Sie sich für AWS

Wenn Sie sich für Amazon Web Services (AWS) registrieren, ist Ihr AWS-Konto automatisch für alle Dienste angemeldet, einschließlich Amazon Fraud Detector. Berechnet werden Ihnen aber nur die Services, die Sie nutzen. Wenn Sie bereits ein AWS-Konto haben, wechseln Sie zur nächsten Aufgabe.

### So melden Sie sich für ein AWS-Konto an

Wenn Sie kein AWS-Konto haben, führen Sie die folgenden Schritte zum Erstellen durch.

Anmeldung für ein AWS-Konto

1. Öffnen Sie <https://portal.aws.amazon.com/billing/signup>.
2. Folgen Sie den Online-Anweisungen.

Bei der Anmeldung müssen Sie auch einen Telefonanruf entgegennehmen und einen Verifizierungscode über die Telefontasten eingeben.

Wenn Sie sich für ein AWS-Konto anmelden, wird ein Root-Benutzer des AWS-Kontos erstellt. Der Root-Benutzer hat Zugriff auf alle AWS-Services und Ressourcen des Kontos. Als bewährte Sicherheitsmethode weisen Sie einem [Administratorbenutzer Administratorzugriff](#) zu und verwenden Sie nur den Root-Benutzer, um [Aufgaben auszuführen, die Root-Benutzerzugriff](#) erfordern.

AWS sendet Ihnen eine Bestätigungs-E-Mail, sobald die Anmeldung abgeschlossen ist. Sie können jederzeit Ihre aktuelle Kontoaktivität anzeigen und Ihr Konto verwalten. Rufen Sie dazu <https://aws.amazon.com/> auf und klicken Sie auf Mein Konto.

## Einen Administratorbenutzer erstellen

Nachdem Sie sich für einen angemeldet habenAWS-Konto, sichern Sie Ihren Root-Benutzer des AWS-KontosAWS IAM Identity Center, aktivieren und erstellen Sie einen Administratorbenutzer, sodass Sie den Root-Benutzer nicht für alltägliche Aufgaben verwenden.

Schützen Ihres Root-Benutzer des AWS-Kontos

1. Melden Sie sich bei der [AWS Management Console](#) als Kontobesitzer an, indem Sie Root-Benutzer auswählen und Ihre AWS-Konto E-Mail-Adresse eingeben. Geben Sie auf der nächsten Seite Ihr Passwort ein.

Hilfe bei der Anmeldung mit dem Root-Benutzer finden Sie unter [Anmelden als Root-Benutzer](#) im AWS-AnmeldungBenutzerhandbuch zu .

2. Aktivieren Sie die Multi-Faktor-Authentifizierung (MFA) für den Root-Benutzer.

Anweisungen dazu finden Sie unter [Aktivieren eines virtuellen MFA-Geräts für den Root-Benutzer Ihres AWS-Konto \(Konsole\)](#) im IAM-Benutzerhandbuch.

Erstellen eines Administratorbenutzers

1. Aktivieren Sie IAM Identity Center.

Anweisungen finden Sie unter [Aktivieren AWS IAM Identity Center](#) im AWS IAM Identity CenterBenutzerhandbuch.

2. Gewähren Sie in IAM Identity Center einem Administratorbenutzer Administratorzugriff.

Ein Tutorial zur Verwendung von IAM-Identity-Center-Verzeichnis als Identitätsquelle finden [Sie unter Benutzerzugriff mit der Standardeinstellung konfigurieren IAM-Identity-Center-Verzeichnis im AWS IAM Identity Center Benutzerhandbuch](#).

### Als Administratorbenutzer anmelden

- Um sich mit Ihrem IAM-Identity-Center-Benutzer anzumelden, verwenden Sie die Anmelde-URL, die an Ihre E-Mail-Adresse gesendet wurde, als Sie den IAM-Identity-Center-Benutzer erstellt haben.

Hilfe bei der Anmeldung mit einem IAM-Identity-Center-Benutzer finden Sie unter [Anmelden beim AWS-Zugangsportale](#) im AWS-Anmeldung Benutzerhandbuch zu.

## Berechtigungen für den Zugriff auf Amazon Fraud Detector Detector-Schnittstellen einrichten

Um Amazon Fraud Detector zu verwenden, richten Sie Berechtigungen für den Zugriff auf die Amazon Fraud Detector Detector-Konsole und API-Operationen ein.

Erstellen Sie gemäß den bewährten Sicherheitsmethoden einen AWS Identity and Access Management (IAM) -Benutzer mit eingeschränktem Zugriff auf Amazon Fraud Detector Detector-Operationen und mit den erforderlichen Berechtigungen. Sie können bei Bedarf weitere Berechtigungen hinzufügen.

Die folgenden Richtlinien enthalten die erforderliche Genehmigung zur Verwendung von Amazon Fraud Detector:

- `AmazonFraudDetectorFullAccessPolicy`

Hiermit können Sie die folgenden Aktionen ausführen:

- Greifen Sie auf alle Amazon Fraud Detector Detector-Ressourcen zu
- Führen Sie alle Modellendpunkte auf und beschreiben Sie sie in SageMaker
- Listet alle IAM-Rollen im Konto auf
- Alle Amazon S3 S3-Buckets auflisten
- Erlauben Sie der IAM-Pass-Rolle, eine Rolle an Amazon Fraud Detector zu übergeben

- **AmazonS3FullAccess**

Ermöglicht vollen Zugriff auf Amazon Simple Storage Service. Dies ist erforderlich, wenn Sie Trainingsdatensätze auf Amazon S3 hochladen müssen.

Im Folgenden wird beschrieben, wie Sie einen IAM-Benutzer erstellen und die erforderlichen Berechtigungen zuweisen.

So erstellen Sie einen Benutzer und weisen ihm die erforderlichen Berechtigungen zu

1. Melden Sie sich bei der AWS Management Console an und öffnen Sie die IAM-Konsole unter <https://console.aws.amazon.com/iam/>.
2. Wählen Sie im Navigationsbereich Users (Benutzer) und dann Add User (Benutzer hinzufügen) aus.
3. Geben Sie unter User Name (Benutzername) den Text **AmazonFraudDetectorUser** ein.
4. Aktivieren Sie das Kontrollkästchen für den Zugriff auf die AWS Managementkonsole und konfigurieren Sie dann das Benutzerkennwort.
5. (Optional) Standardmäßig AWS muss der neue Benutzer bei der ersten Anmeldung ein neues Passwort erstellen. Sie können das Kontrollkästchen neben User must create a new password at next sign-in (Benutzer muss bei der nächsten Anmeldung ein neues Passwort erstellen) deaktivieren, damit der neue Benutzer sein Kennwort nach der Anmeldung zurücksetzen kann.
6. Wählen Sie Next: Permissions (Weiter: Berechtigungen) aus.
7. Wählen Sie Create group (Gruppe erstellen) aus.
8. Geben Sie als Gruppenname ein. **AmazonFraudDetectorGroup**
9. Aktivieren Sie in der Richtlinienliste das Kontrollkästchen für AmazonFraudDetectorFullAccessPolicy und AmazonS3. FullAccess Wählen Sie Create group (Gruppe erstellen) aus.
10. Aktivieren Sie in der Gruppenliste das Kontrollkästchen der neuen Gruppe. Wählen Sie Aktualisieren, wenn Sie die Gruppe nicht in der Liste sehen.
11. Wählen Sie Next: Tags (Weiter: Tags) aus.
12. (Optional) Fügen Sie dem Benutzer Metadaten hinzu, indem Sie Markierungen als Schlüssel-Wert-Paare anfügen. Anweisungen zur Verwendung von Tags in IAM finden Sie unter [Tagging IAM-Benutzer](#) und -Rollen.

13. Wählen Sie Weiter: Überprüfen, um die Benutzerdetails und die Zusammenfassung der Berechtigungen für den neuen Benutzer anzuzeigen. Wenn Sie bereit sind, fortzufahren, wählen Sie Benutzer erstellen.

## Richten Sie Schnittstellen für den Zugriff auf Amazon Fraud Detector ein mit

Sie können über die Amazon Fraud Detector-Konsole oder das AWS SDK auf Amazon Fraud Detector zugreifen. AWS CLI Bevor Sie sie verwenden können, müssen Sie zunächst das AWS SDK AWS CLI und das SDK einrichten.

### Rufen Sie die Amazon Fraud Detector Detector-Konsole auf

Sie können über die Amazon Fraud Detector Detector-Konsole und andere AWS Dienste auf die Amazon Fraud Detector-Konsole zugreifenAWS Management Console. IhrAWS-Konto, gewährt Ihnen Zugriff auf dieAWS Management Console.

Um auf die Amazon Fraud Detector Detector-Konsole zuzugreifen,

1. Gehen Sie zu <https://console.aws.amazon.com/> und melden Sie sich bei Ihrem anAWS-Konto.
2. Navigieren Sie zu Amazon Fraud Detector.

Mit der Amazon Fraud Detector Detector-Konsole können Sie Ihre Modelle und Ihre Ressourcen zur Betrugserkennung wie Detektoren, Variablen, Ereignisse, Entitäten, Labels und Ergebnisse erstellen und verwalten. Sie können Prognosen erstellen und die Leistung und Prognosen Ihres Modells bewerten.

### Einrichten von AWS CLI

Sie können AWS Command Line Interface (AWS CLI) verwenden, um mit Amazon Fraud Detector zu interagieren, indem Sie Befehle in Ihrer Befehlszeilen-Shell ausführen. Bei minimaler Konfiguration können Sie Befehle für ähnliche Funktionen wie die AWS CLI Amazon Fraud Detector Detector-Konsole über die Befehlszeile in Ihrem Terminal ausführen.

Um das einzurichten AWS CLI

Herunterladen und Konfigurieren von AWS CLI. Anweisungen finden Sie in den folgenden Themen im AWS Command Line Interface Benutzerhandbuch:



- [Einrichten mit der AWS-Befehlszeilenschnittstelle](#)
- [Konfigurieren der AWS-Befehlszeilenschnittstelle](#)

Informationen zu Amazon Fraud Detector Detector-Befehlen finden Sie unter [Verfügbare Befehle](#)

## Richten Sie das AWS SDK ein

Sie können die AWS SDKs verwenden, um Code für die Erstellung und Verwaltung Ihrer Ressourcen zur Betrugserkennung und zum Abrufen von Betrugsprognosen zu schreiben. Die AWS SDKs unterstützen Amazon Fraud Detector in [JavaScript](#) und [Python \(Boto3\)](#).

Zur Einrichtung AWS SDK for Python (Boto3)

Sie können AWS SDK for Python (Boto3) verwenden, um AWS Dienste zu erstellen, zu konfigurieren und zu verwalten. Anweisungen zur Installation von Boto finden Sie unter [AWSSDK for Python \(Boto3\)](#). Stellen Sie sicher, dass Sie das Boto3 SDK Version 1.14.29 oder höher verwenden.

Führen Sie nach der Installation AWS SDK for Python (Boto3) das folgende Python-Beispiel aus, um zu überprüfen, ob Ihre Umgebung korrekt konfiguriert ist. Wenn sie richtig konfiguriert ist, enthält die Antwort eine Liste von Detektoren. Wenn keine Melder erstellt wurden, ist die Liste leer.

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

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

Um AWS SDKs für Java einzurichten

Anweisungen zur Installation und zum Laden von finden Sie unter [Einrichten des SDK für JavaScript](#).  
AWS SDK for JavaScript

# Erste Schritte mit Amazon Fraud Detector

Stellen Sie vor dem Beginn sicher, dass Sie die Schritte unter [gelesen Erkennen von Betrug mit Amazon Fraud Detector](#) und abgeschlossen haben [Für Amazon Fraud Detector einrichten](#).

Die praxisbezogenen Tutorials in diesem Abschnitt erläutern Ihnen, wie Sie Amazon Fraud Detector nutzen können, um ein Modell zur Fraud Detector zu erstellen, zu trainieren und bereitzustellen. In diesem Tutorial übernehmen Sie die Rolle eines Betrugsanalysten, der mithilfe eines maschinellen Lernmodells vorhersagt, ob die Registrierung eines neuen Kontos betrügerisch ist. Das Modell muss anhand von Daten aus Kontoregistrierungen trainiert werden. Amazon Fraud Detector bietet ein Beispiel für einen Datensatz zur Kontoregistrierung für dieses Tutorial. Der Beispieldatensatz muss hochgeladen werden, bevor Sie mit dem Tutorial beginnen.

Sie können Amazon Fraud Detector über eine der folgenden Schnittstellen nutzen. Stellen Sie vor Beginn des Erste-Schritte-Tutorials sicher, dass Sie folgende Anweisungen befolgen: [Beispieldatensatz abrufen und hochladen](#)

- [Tutorial: Erste Schritte mit der Amazon Fraud Detector Detector-Konsole](#)
- [Tutorial: Erste Schritte mit der Verwendung von AWS SDK for Python \(Boto3\)](#)

## Beispieldatensatz abrufen und hochladen

Der Beispieldatensatz, den Sie in diesem Tutorial verwenden, enthält Einzelheiten zu Online-Kontoregistrierungen. Der Datensatz befindet sich in einer Textdatei, die kommagetrennte Werte (CSV) im UTF-8-Format verwendet. Die erste Zeile der CSV-Datensatzdatei enthält die Header. Auf die Kopfzeile folgen mehrere Datenzeilen. Jede dieser Zeilen besteht aus Datenelementen aus einer einzigen Kontoregistrierung. Die Daten sind zu Informationsmöglichkeiten beschriftet. Eine Spalte im Datensatz gibt an, ob die Kontoregistrierung betrügerisch ist.

Um einen Beispieldatensatz abzurufen und hochzuladen

1. Gehe zu [Samples](#).

Es gibt zwei Datendateien mit Daten zur Online-Kontoregistrierung: `registration_data_20K_minimum.csv` und `registration_data_20K_full.csv`. Die Datei `registration_data_20K_minimum` enthält nur zwei Variablen: `ip_address` und `email_address`. Die Datei `registration_data_20K_full` enthält weitere Variablen.

Diese Variablen gelten für jedes Ereignis und umfassen `billing_address`, `phone_number` und `user_agent`. Beide Datendateien enthalten außerdem zwei Pflichtfelder:

- `EVENT_TIMESTAMP` — Definiert, wann das Ereignis aufgetreten ist
- `EVENT_LABEL` — Klassifiziert das Ereignis als betrügerisch oder legitim

Sie können eine der beiden Dateien für dieses Tutorial verwenden. Laden Sie die Datendatei herunter, die Sie verwenden möchten.

## 2. Erstellen Sie einen Amazon Simple Storage Service (Amazon S3) -Bucket.

In diesem Schritt erstellen Sie einen externen Speicher zum Speichern des Datensatzes. Dieser externe Speicher ist Amazon S3 Bucket. Weitere Informationen zu Amazon S3 finden Sie unter [Was ist Amazon S3?](#)

- a. Melden Sie sich bei der AWS Management Console an und öffnen Sie die Amazon-S3-Konsole unter <https://console.aws.amazon.com/s3/>.
  - b. Wählen Sie unter Buckets die Option Create Bucket aus.
  - c. Geben Sie unter Bucket-Name einen Namen für den Bucket ein. Stellen Sie sicher, dass Sie die Regeln für die Benennung von Buckets in der Konsole befolgen und einen global eindeutigen Namen angeben. Wir empfehlen, einen Namen zu verwenden, der den Zweck des Buckets beschreibt.
  - d. Wählen Sie aus AWS-Region, AWS-Region wo Sie Ihren Bucket erstellen möchten. Die von Ihnen gewählte Region muss Amazon Fraud Detector unterstützen. Um die Latenz zu reduzieren, wählen Sie AWS-Region die, die Ihrem geografischen Standort am nächsten liegt. Eine Liste der Regionen, die Amazon Fraud Detector unterstützen, finden Sie in der [Regionstabelle](#) im Global Infrastructure Guide.
  - e. Behalten Sie für dieses Tutorial die Standardeinstellungen für Object Ownership, Bucket-Einstellungen für Block Public Access, Bucket Versioning und Tags bei.
  - f. Wählen Sie für dieses Tutorial unter Standardverschlüsselung die Option Deaktivieren aus.
  - g. Überprüfen Sie Ihre Bucket-Konfiguration und wählen Sie dann Create Bucket.
- ## 3. Laden Sie eine Beispieldatendatei in Amazon S3 Bucket hoch.

Da Sie nun einen Bucket haben, laden Sie eine der Beispieldateien, die Sie zuvor heruntergeladen haben, in den Amazon S3 S3-Bucket hoch, den Sie gerade erstellt haben.

- a. In den Buckets ist Ihr Bucket-Name aufgeführt. Wählen Sie Ihren Bucket aus.

- b. Klicken Sie auf Upload.
- c. Wählen Sie unter Dateien und Ordner die Option Dateien hinzufügen aus.
- d. Wählen Sie eine der Beispieldatendateien aus, die Sie auf Ihren Computer heruntergeladen haben, und wählen Sie dann Öffnen.
- e. Behalten Sie die Standardeinstellungen für Ziel, Berechtigungen und Eigenschaften bei.
- f. Überprüfen Sie die Konfigurationen und wählen Sie dann Hochladen.
- g. Die Beispieldatendatei wird in den Amazon S3 S3-Bucket hochgeladen. Notieren Sie sich den Standort des Buckets. Wählen Sie in den Objekten die Beispieldatendatei aus, die Sie gerade hochgeladen haben.
- h. Kopieren Sie in der Objektübersicht den Standort unter S3 URI. Dies ist der Amazon-S3-Speicherort Ihrer Beispieldatendatei. Sie nutzen sie später. Sie können auch den Amazon-Ressourcennamen (ARN) Ihres S3-Buckets kopieren und speichern.

## Tutorial: Erste Schritte mit der Amazon Fraud Detector Detector-Konsole

Dieses Tutorial besteht aus zwei Teilen. Im ersten Teil wird beschrieben, wie ein Modell zur Betrugserkennung erstellt, trainiert und eingesetzt wird. Der zweite Teil behandelt, wie das Modell verwendet wird, um Betrugsvorhersagen in Echtzeit zu generieren. Das Modell wird anhand der Beispieldatendatei trainiert, die Sie in einen S3-Bucket hochladen. Am Ende dieses Tutorials führen Sie folgende Aktionen aus:

- Erstellen und trainieren Sie ein Amazon Fraud Detector Detector-Modell
- Generieren von Betrugsvorhersagen in Echtzeit

### Important

Stellen Sie vor dem Fortfahren sicher, dass Sie folgende Anweisungen befolgt haben: [Beispieldatensatz abrufen und hochladen](#)

## Teil A: Aufbau, Schulung und Bereitstellung eines Amazon Fraud Detector Detector-Modells

In Teil A definieren Sie Ihren Geschäftsanwendungsfall, definieren Ihr Ereignis, erstellen ein Modell, trainieren das Modell, bewerten die Leistung des Modells und implementieren das Modell.

Schritt 1: Wählen Sie Ihren geschäftlichen Anwendungsfall aus

- In diesem Schritt verwenden Sie den Datenmodels-Explorer, um Ihren Geschäftsanwendungsfall den von Amazon Fraud Detector unterstützten Modelltypen zur Betrugserkennung zuzuordnen. Der Data Models Explorer ist ein in die Amazon Fraud Detector Detector-Konsole integriertes Tool, das einen Modelltyp empfiehlt, der für die Erstellung und Schulung eines Betrugserkennungsmodells für Ihren Geschäftsanwendungsfall verwendet werden kann. Der Datenmodell-Explorer bietet auch Einblicke in die obligatorischen, empfohlenen und optionalen Datenelemente, die Sie in Ihren Datensatz aufnehmen müssen. Der Datensatz wird verwendet, um Ihr Modell zur Betrugserkennung zu erstellen und zu trainieren.

Für die Zwecke dieses Tutorials besteht Ihr geschäftlicher Anwendungsfall in der Registrierung neuer Konten. Nachdem Sie Ihren geschäftlichen Anwendungsfall angegeben haben, empfiehlt der Datenmodell-Explorer einen Modelltyp für die Erstellung eines Betrugserkennungsmodells und stellt Ihnen außerdem eine Liste der Datenelemente zur Verfügung, die Sie für die Erstellung Ihres Datensatzes benötigen. Da Sie bereits einen Beispieldatensatz hochgeladen haben, der Daten aus neuen Kontoregistrierungen enthält, müssen Sie keinen neuen Datensatz erstellen.

- a. Öffnen Sie die [AWSManagement Console](#) und melden Sie sich bei Ihrem Konto an. Navigieren Sie zu Amazon Fraud Detector aus.
- b. Wählen Sie im linken Navigationsbereich Data Models Explorer aus.
- c. Wählen Sie auf der Explorer-Seite für Datenmodelle unter Geschäftsanwendungsfall die Option Betrug mit einem neuen Konto aus.
- d. Amazon Fraud Detector zeigt den empfohlenen Modelltyp an, der verwendet werden soll, um ein Modell zur Betrugserkennung für den ausgewählten Geschäftsanwendungsfall zu erstellen. Der Modelltyp definiert die Algorithmen, Anreicherungen und Transformationen, die Amazon Fraud Detector zum Trainieren Ihres Betrugserkennungsmodells verwendet.

Notieren Sie sich den empfohlenen Modelltyp. Sie benötigen diesen später beim Erstellen Ihres Modells.

- e. Der Bereich Datenmodelleinblicke bietet einen Einblick in die obligatorischen und empfohlenen Datenelemente, die für die Erstellung und das Training eines Betrugserkennungsmodells erforderlich sind.

Schauen Sie sich den Beispieldatensatz an, den Sie heruntergeladen haben, und stellen Sie sicher, dass er alle obligatorischen und einige empfohlene Datenelemente enthält, die in der Tabelle aufgeführt sind.

Wenn Sie später ein Modell für Ihren spezifischen Geschäftsanwendungsfall erstellen, verwenden Sie die bereitgestellten Erkenntnisse, um Ihren Datensatz zu erstellen.

## Schritt 2: Erstellen eines Ereignistyps

- In diesem Schritt definieren Sie die Geschäftsaktivität (Ereignis), die auf Betrug hin untersucht werden soll. Beim Definieren des Ereignisses müssen Sie die Variablen, die das Ereignis ausführt, die das Ereignis ausführt, und die Beschriftungen, die das Ereignis klassifizieren. In diesem Tutorial definieren Sie das Ereignis zur Kontoregistrierung.
  - a. Öffnen Sie die [AWSManagement Console](#) und melden Sie sich bei Ihrem Konto an. Navigieren Sie zu Amazon Fraud Detector aus.
  - b. Wählen Sie im linken Navigationsbereich Ereignisse aus.
  - c. Wählen Sie auf der Seite „Ereignistyp“ die Option Erstellen aus.
  - d. Geben Sie `sample_registration` unter Details zum Veranstaltungstyp den Namen des Veranstaltungstyps und optional eine Beschreibung des Ereignisses ein.
  - e. Wählen Sie für Entität die Option Entität erstellen aus.
  - f. Geben Sie `sample_customer` Sie auf der Seite Entität erstellen den Namen des Entitätstyps ein. Geben Sie optional eine Beschreibung des von, und dem, was Sie möchten, ein.
  - g. Klicken Sie auf Create entity (Entity erstellen).
  - h. Wählen Sie unter Ereignisvariablen für Wählen Sie aus, wie die Variablen dieses Ereignisses definiert werden sollen die Option Variablen aus einem Trainingsdatensatz auswählen aus.
  - i. Wählen Sie für die IAM-Rolle die Option IAM-Rolle erstellen aus.
  - j. Geben Sie auf der Seite „IAM-Rolle erstellen“ den Namen des S3-Buckets ein, in den Sie Ihre Beispieldaten hochgeladen haben, und wählen Sie Rolle erstellen.

- k. Geben Sie im Feld Datenspeicherort den Pfad zu Ihren Beispieldaten ein. Dies ist der S3 URI Pfad, den Sie nach dem Hochladen der Beispieldaten gespeichert haben. Der Pfad ist ähnlich wie dieser: `S3://your-bucket-name/example_dataset_filename.csv`.
- l. Klicken Sie auf Upload.

Amazon Fraud Detector extrahiert die Header aus Ihrer Beispieldatendatei und ordnet sie einem Variablentyp zu. Das Mapping wird in der Konsole angezeigt.

- m. Wählen Sie unter Labels — optional für Labels die Option Neue Labels erstellen aus.
- n. Geben Sie auf der Seite „Etikett erstellen“ `fraud` als Namen ein. Diese Bezeichnung entspricht dem Wert, der die betrügerische Kontoregistrierung im Beispieldatensatz darstellt.
- o. Wählen Sie Label erstellen.
- p. Erstellen Sie ein zweites Label und geben Sie `legit` es dann als Namen ein. Diese Bezeichnung entspricht dem Wert, der die legitime Kontoregistrierung im Beispieldatensatz darstellt.
- q. Wählen Sie Ereignistyp erstellen.

### Schritt 3: Erstellen eines Modells

1. Wählen Sie auf der Seite Modelle die Option Modell hinzufügen und dann Modell erstellen aus.
2. Geben Sie für Schritt 1 — Modelldetails definierens `sample_fraud_detection_model` als Modellnamen ein. Sie können optional auch eine Beschreibung des Modells hinzufügen.
3. Wählen Sie als Modelltyp das Modell Online Fraud Insights aus.
4. Wählen Sie als Veranstaltungstyp die Option `sample_registration` aus. Dies ist der Ereignistyp, den Sie in Schritt 1 erstellt haben.
5. In Historische Ereignisdaten
  - a. Wählen Sie unter Event-Datenquelle die Option In S3 gespeicherte Event-Daten aus.
  - b. Wählen Sie unter IAM-Rolle die Rolle aus, die Sie in Schritt 1 erstellt haben.
  - c. Geben Sie unter Speicherort der Trainingsdaten den S3-URI-Pfad zu Ihrer Beispieldatendatei ein.
6. Wählen Sie Next (Weiter).

## Schritt 4: Zugmodell

1. Lassen Sie unter Modelleingaben alle Kontrollkästchen aktiviert. Standardmäßig verwendet Amazon Fraud Detector alle Variablen aus Ihrem historischen Ereignisdatensatz als Modelleingaben.
2. Wählen Sie unter Labelklassifizierung für die Labels Betrug die Option Betrug aus, da diese Bezeichnung dem Wert entspricht, der betrügerische Ereignisse im Beispieldatensatz darstellt. Wählen Sie für Legitime Labels die Option legitim aus, da diese Bezeichnung dem Wert entspricht, der legitime Ereignisse im Beispieldatensatz darstellt.
3. Behalten Sie für die Behandlung Unbeschrifteter Ereignisse die Standardauswahl Ignorieren Sie unbeschriftete Ereignisse für diesen Beispieldatensatz bei.
4. Wählen Sie Next (Weiter).
5. Wählen Sie nach der Überprüfung das Modell erstellen und trainieren. Amazon Fraud Detector erstellt ein Modell und beginnt, eine neue Version des Modells zu trainieren.

In Modellversionen gibt die Spalte Status den Status des Modelltrainings an. Das Modelltraining, das den Beispieldatensatz verwendet, dauert ungefähr 45 Minuten. Nach Abschluss des Modelltrainings ändert sich der Status in Bereit für den Einsatz.

## Schritt 5: Überprüfen der Modelleleistung

Ein wichtiger Schritt bei der Verwendung von Amazon Fraud Detector besteht darin, die Genauigkeit Ihres Modells anhand von Modellbewertungen und Leistungskennzahlen zu bewerten. Nach Abschluss des Modelltrainings validiert Amazon Fraud Detector die Modelleleistung anhand der 15% Ihrer Daten, die nicht zum Trainieren des Modells verwendet wurden, und generiert einen Modelleleistungswert und andere Leistungskennzahlen.

1. Um die Leistung des Modells zu sehen,
  - a. Wählen Sie im linken Navigationsbereich der Amazon Fraud Detector Konsole Modelle aus.
  - b. Wählen Sie auf der Seite Modelle das Modell aus, das Sie gerade trainiert haben (`sample_fraud_detection_model`), und wählen Sie dann 1.0. Dies ist die Version, die Amazon Fraud Detector von Ihrem Modell erstellt hat.
2. Sehen Sie sich den Gesamtwert der Modelleleistung und alle anderen Metriken an, die Amazon Fraud Detector für dieses Modell generiert hat.



Weitere Informationen zum Leistungswert und zu den Leistungskennzahlen des Modells finden Sie auf dieser Seite unter [Modellwerte](#) und [Modellleistungsmetriken](#).

Sie können davon ausgehen, dass alle Ihre trainierten Amazon Fraud Detector Modelle über reale Leistungskennzahlen zur Betrugserkennung verfügen, die den Leistungskennzahlen ähneln, die Sie für das Modell in diesem Tutorial sehen.

## Schritt 6: Bereitstellen des Modells

Nachdem Sie die Leistungskennzahlen Ihres trainierten Modells überprüft haben und bereit sind, es zur Generierung von Betrugsvorhersagen zu verwenden, können Sie das Modell bereitstellen.

1. Wählen Sie im linken Navigationsbereich der Amazon Fraud Detector Konsole Modelle aus.
2. Wählen Sie auf der Seite Modelle die Option `sample_fraud_detection_model` und dann die spezifische Modellversion aus, die Sie bereitstellen möchten. Wählen Sie für dieses Tutorial 1.0.
3. Wählen Sie auf der Seite Modellversion die Option Aktionen und dann Modellversion bereitstellen aus.
4. In den Modellversionen zeigt der Status den Status der Bereitstellung an. Nach Abschluss der Bereitstellung ändert sich der Status in Aktiv. Dies bedeutet, dass die Modellversion aktiviert ist und zur Generierung von Betrugsvorhersagen verfügbar ist. Fahren Sie fort [Teil B: Generieren Sie Betrugsvorhersagen](#), um die Schritte zur Generierung von Betrugsvorhersagen abzuschließen.

## Teil B: Generieren Sie Betrugsvorhersagen

Die Betrugsvorhersage ist eine Bewertung von Betrug für eine Geschäftstätigkeit (Ereignis). Amazon Fraud Detector verwendet Detektoren, um Betrugsvorhersagen zu generieren. Ein Detektor enthält Erkennungslogik, z. B. Modelle und Regeln, für ein bestimmtes Ereignis, das Sie auf Betrug hin auswerten möchten. Die Erkennungslogik verwendet Regeln, um Amazon Fraud Detector mitzuteilen, wie die mit dem Modell verknüpften Daten zu interpretieren sind. In diesem Tutorial bewerten Sie das Ereignis der Kontoregistrierung anhand des Beispieldatensatzes für die Kontoregistrierung, den Sie zuvor hochgeladen haben.

In Teil A haben Sie Ihr Modell erstellt, trainiert und eingesetzt. In Teil B erstellen Sie einen Detektor für `sample_registration` Ereignistyp, fügen das bereitgestellte Modell hinzu, erstellen Regeln

und eine Regelausführungsreihenfolge und erstellen und aktivieren dann eine Version des Detektors, die Sie zur Generierung von Betrugsprognosen verwenden.

### Schritt 1: Erstellen eines Detektors

Um einen Detektor zu erstellen

1. Wählen Sie im linken Navigationsbereich der Amazon Fraud Detector Console die Option Detectors aus.
2. Wählen Sie Detektor erstellen.
3. Geben Sie auf der Seite „Melderdetails definieren“ `sample_detector` den Namen des Melders ein. Geben Sie optional eine Beschreibung für den Detektor ein, z.B. `my sample fraud detector B`.
4. Wählen Sie als Ereignistyp die Option `sample_registration` aus. Dies ist das Ereignis, das Sie in Teil A dieses Tutorials erstellt haben.
5. Wählen Sie Next (Weiter).

### Schritt 2: Hinzufügen eines Modells

Wenn Sie Teil A dieses Tutorials abgeschlossen haben, haben Sie wahrscheinlich bereits ein Amazon Fraud Detector Model-Modell, das Sie Ihrem Detektor hinzufügen können. Wenn Sie noch kein Modell erstellt haben, fahren Sie mit Teil A fort und führen Sie die Schritte zum Erstellen, Trainieren und Bereitstellen eines Modells aus. Fahren Sie dann mit Teil B fort.

1. Wählen Sie unter Modell hinzufügen — optional die Option Modell hinzufügen aus.
2. Wählen Sie auf der Seite Modell hinzufügen unter Modell auswählen den Amazon Fraud Detector Model-Modellnamen aus, den Sie zuvor bereitgestellt haben. Wählen Sie unter Version auswählen die Modellversion des bereitgestellten Modells aus.
3. Wählen Sie Add model aus.
4. Wählen Sie Next (Weiter).

### Schritt 3: Hinzufügen von Regeln

Eine Regel ist eine Bedingung, die Amazon Fraud Detector mitteilt, wie der Leistungswert des Modells bei der Bewertung zur Betrugsvorhersage zu interpretieren ist. Für dieses Tutorial erstellen Sie drei Regeln: `high_fraud_risk`, `medium_fraud_risk`, und `low_fraud_risk`.

1. Geben `high_fraud_risk` Sie auf der Seite Regeln hinzufügen unter Regel definieren den Regelnamen und unter Beschreibung — optional eine Beschreibung für die **This rule captures events with a high ML model score** Regel ein.
2. Geben Sie im Feld Ausdruck den folgenden Regelausdruck in der Sprache des vereinfachten Regelausdrucks von Amazon Fraud Detector ein:  

```
$sample_fraud_detection_model_insightscore > 900
```
3. Wählen Sie unter Ergebnisse die Option Neues Ergebnis erstellen aus. Ein Ergebnis ist das Ergebnis einer Betrugsvorhersage und wird zurückgegeben, wenn die Regel während einer Auswertung übereinstimmt.
4. Geben **verify\_customer** Sie im Feld Neues Ergebnis erstellen den Namen des Ergebnisses ein. Geben Sie optional eine Beschreibung ein.
5. Wählen Sie Ergebnis speichern.
6. Wählen Sie Regel hinzufügen, um die Regelüberprüfung auszuführen und die Regel zu speichern. Nach der Erstellung stellt Amazon Fraud Detector die Regel zur Verwendung in Ihrem Detektor zur Verfügung.
7. Wählen Sie Weitere Regel hinzufügen und klicken Sie dann auf die Registerkarte Regel erstellen.
8. Wiederholen Sie diesen Vorgang noch zweimal, um `medium_fraud_risk` `low_fraud_risk` AND-Regeln mit den folgenden Regeldetails zu erstellen:

- mittleres Betrugsrisiko

Name der Regel: `medium_fraud_risk`

Ergebnis: `review`

Ausdruck:

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

```
$sample_fraud_detection_model_insightscore > 700
```

- niedriges Betrugsrisiko

Name der Regel: `low_fraud_risk`

Ergebnis: `approve`

Ausdruck:

```
$sample_fraud_detection_model_insightscore <= 700
```

Diese Werte sind Beispiele für dieses Tutorial. Wenn Sie Regeln für Ihren eigenen Detektor erstellen, verwenden Sie Werte, die für Ihr Modell und Ihren Anwendungsfall geeignet sind.

9. Nachdem Sie alle drei Regeln erstellt haben, wählen Sie Weiter.

Weitere Informationen zum Erstellen und Schreiben von Regeln finden Sie unter [Regeln](#) und [Referenz zur Regelsprache](#).

#### Schritt 4: Konfigurieren der Regelausführung und der Regelreihenfolge

Der Regelausführungsmodus für die Regeln, die im Detektor enthalten sind, bestimmt, ob alle von Ihnen definierten Regeln ausgewertet werden oder ob die Regelauswertung bei der ersten übereinstimmenden Regel beendet wird. Und die Regelreihenfolge bestimmt die Reihenfolge, in der die Regel ausgeführt werden soll.

Der Standardmodus für die Regelausführung ist `FIRST_MATCHED`.

#### Erster Treffer

Der Ausführungsmodus „Erste übereinstimmende Regel“ gibt die Ergebnisse für die erste übereinstimmende Regel auf der Grundlage der definierten Regelreihenfolge zurück. Wenn Sie `FIRST_MATCHED` angeben, bewertet Amazon Fraud Detector die Regeln nacheinander von der ersten bis zur letzten und stoppt dabei bei der ersten übereinstimmenden Regel. Amazon Fraud Detector liefert dann die Ergebnisse für diese einzelne Regel aus.

Die Reihenfolge, in der Sie Regeln ausführen, kann sich auf das Ergebnis der Betrugsprognose auswirken. Nachdem Sie Ihre Regeln erstellt haben, ordnen Sie die Regeln neu an, um sie in der gewünschten Reihenfolge auszuführen, indem Sie die folgenden Schritte ausführen:

Wenn Ihre `high_fraud_risk` Regel nicht bereits oben in Ihrer Regelliste steht, wählen Sie Reihenfolge und dann 1 aus. Dies bewegt sich `high_fraud_risk` zur ersten Position.

Wiederholen Sie diesen Vorgang, sodass sich Ihre `medium_fraud_risk` Regel an der zweiten Position und Ihre `low_fraud_risk` Regel an der dritten Position befindet.

## Alles übereinstimmend

Der Ausführungsmodus „Alle übereinstimmenden Regeln“ gibt unabhängig von der Regelreihenfolge Ergebnisse für alle übereinstimmenden Regeln zurück. Wenn Sie angeben `ALL_MATCHED`, bewertet Amazon Fraud Detector alle Regeln aus und gibt die Ergebnisse für alle übereinstimmenden Regeln zurück.

Wählen Sie `FIRST_MATCHED` für dieses Tutorial aus und wählen Sie dann Weiter.

### Schritt 5: Überprüfen und Erstellen der Detektorversion

Eine Detektorversion definiert die spezifischen Modelle und Regeln, die für die Generierung von Betrugsprognosen verwendet werden.

1. Überprüfen Sie auf der Seite Überprüfen und erstellen die Melderdetails, Modelle und Regeln, die Sie konfiguriert haben. Wenn Sie Änderungen vornehmen müssen, wählen Sie Bearbeiten neben dem entsprechenden Abschnitt Bearbeiten aus.
2. Wählen Sie Detektor erstellen. Nach der Erstellung wird die erste Version Ihres Melders in der Tabelle mit den Detector-Versionen mit dem `Draft` Status angezeigt.

Sie verwenden die Entwurfsversion, um Ihren Detektor zu testen.

### Schritt 6: Testen und Aktivieren der Detektorversion

In der Amazon Fraud Detector Detector-Konsole können Sie die Logik Ihres Detektors mithilfe von Scheindaten mit der Funktion Test ausführen testen. Für dieses Tutorial können Sie Kontoregistrierungsdaten aus dem Beispieldatensatz verwenden.

1. Scrollen Sie unten auf der Seite mit den Detector-Versionsdetails zu Test ausführen.
2. Geben Sie für Ereignismetadaten einen Zeitstempel ein, wann das Ereignis eingetreten ist, und geben Sie eine eindeutige Kennung für die Entität ein, die das Ereignis durchführt. Wählen Sie für dieses Tutorial ein Datum aus der Datumsauswahl für den Zeitstempel aus und geben Sie „1234“ als Entitäts-ID ein.
3. Geben Sie für Eventvariable die Variablenwerte ein, die Sie testen möchten. Für dieses Tutorial benötigen Sie nur die `email_address` Felder `ip_address` und. Dies liegt daran, dass dies die Eingaben sind, die zum Trainieren Ihres Amazon Fraud Detector Detector-Modells verwendet werden. Sie können folgende Beispielwerte verwenden. Dies setzt voraus, dass Sie die vorgeschlagenen Variablennamen verwendet haben:

- `ip_adresse:205.251.233.178`
  - `email_adresse:johndoe@exampledomain.com`
4. Wählen Sie Test ausführen.
  5. Amazon Fraud Detector gibt das Ergebnis der Betrugsvorhersage auf der Grundlage des Regelausführungsmodus zurück. Wenn der Regelausführungsmodus ist `FIRST_MATCHED`, entspricht das zurückgegebene Ergebnis der ersten Regel, die übereinstimmt. Die erste Regel ist die Regel mit der höchsten Priorität. Es ist übereinstimmend, wenn es als wahr bewertet wird. Wenn der Regelausführungsmodus ist `ALL_MATCHED`, entspricht das zurückgegebene Ergebnis allen übereinstimmenden Regeln. Das bedeutet, dass sie alle als wahr bewertet werden. Amazon Fraud Detector gibt auch die Modellbewertung für alle Modelle zurück, die Ihrem Detektor hinzugefügt wurden.

Sie können die Eingaben ändern und einige Tests durchführen, um unterschiedliche Ergebnisse zu sehen. Sie können die Werte `ip_address` und `email_address` aus Ihrem Beispieldatensatz für die Tests verwenden und überprüfen, ob die Ergebnisse den Erwartungen entsprechen.

6. Wenn Sie mit der Funktionsweise des Melders zufrieden sind, bewerben Sie ihn von `Draft` bis `Active`. Dadurch steht der Detektor für die Betrugserkennung in Echtzeit zur Verfügung.

Wählen Sie auf der Seite mit den Versionsdetails von Detector die Optionen `Actions`, `Publish`, `Publish Version` aus. Dadurch wird der Status des Melders von Entwurf auf Aktiv geändert.

Zu diesem Zeitpunkt sind Ihr Modell und die zugehörige Detektorlogik bereit, Online-Aktivitäten mithilfe der `Amazon Fraud DetectorGetEventPrediction` API in Echtzeit auf Betrug hin auszuwerten. Sie können Ereignisse auch offline mithilfe einer CSV-Eingabedatei und der `CreateBatchPredictionJob` API auswerten. Weitere Informationen über die Betrugsvorhersage finden Sie unter [Fraud Preects](#)

Nach Abschluss dieses Tutorials haben Sie Folgendes ausgeführt:

- Hat einen Beispiel-Ereignisdatensatz in Amazon S3 hochgeladen.
- Anhand des Beispieldatensatzes wurde ein Amazon Fraud Detector-Betrugserkennungsmodell erstellt und trainiert.
- Der Leistungswert des Modells und andere Leistungskennzahlen, die Amazon Fraud Detector generiert hat, wurden angezeigt.
- Das Modell zur Betrugserkennung wurde eingesetzt.

- Erstellte einen Detektor und fügte das bereitgestellte Modell hinzu.
- Dem Detektor wurden Regeln, die Reihenfolge der Regelausführung und Ergebnisse hinzugefügt.
- Der Detektor wurde getestet, indem verschiedene Eingaben bereitgestellt und überprüft wurden, ob die Regeln und die Reihenfolge der Regelausführung wie erwartet funktionierten.
- Aktivierte den Detektor, indem du ihn veröffentlicht hast.

## Tutorial: Erste Schritte mit der Verwendung von AWS SDK for Python (Boto3)

In diesem Tutorial wird beschrieben, wie Sie ein Amazon Fraud Detector Detector-Modell erstellen und trainieren und dieses Modell anschließend verwenden, um mithilfe des Betrugsvorhersagen in Echtzeit zu generieren AWS SDK for Python (Boto3). Das Modell wird anhand der Beispieldatendatei für die Kontoregistrierung trainiert, die Sie in den Amazon S3 S3-Bucket hochladen.

Am Ende dieses Tutorials führen Sie die folgenden Aktionen durch:

- Erstellen und trainieren Sie ein Amazon Fraud Detector Detector-Modell
- Generieren von Betrugsprognosen in Echtzeit

## Voraussetzungen

Im Folgenden sind die erforderlichen Schritte für dieses Tutorial aufgeführt.

- Abgeschlossen [Für Amazon Fraud Detector einrichten](#).

Wenn Sie dies bereits getan haben [Richten Sie das AWS SDK ein](#), stellen Sie sicher, dass Sie Boto3 SDK Version 1.14.29 oder höher verwenden.

- Ich habe die für dieses Tutorial erforderlichen [Beispieldatensatz abrufen und hochladen](#) Dateianweisungen befolgt.

# Erste Schritte

## Schritt 1: Einrichten und Überprüfen der Python-Umgebung

Boto ist das Amazon Web Services (AWS) -SDK für Python. Sie können es zum Erstellen, Konfigurieren und Verwalten verwenden AWS-Services. Anweisungen zur Installation von Boto3 finden Sie unter [AWS SDK for Python \(Boto3\)](#).

Führen Sie nach der Installation AWS SDK for Python (Boto3) den folgenden Python-Beispielbefehl aus, um zu überprüfen, ob Ihre Umgebung korrekt konfiguriert ist. Wenn Ihre Umgebung richtig konfiguriert ist, enthält die Antwort eine Liste von Detektoren. Wenn keine Detektoren erstellt wurden, ist die Liste leer.

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

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

## Schritt 2: Variablen, Entitätstyp und Labels erstellen

In diesem Schritt erstellen Sie Ressourcen, die zur Definition von Modell, Ereignis und Regeln verwendet werden.

### Erstellen einer Variablen

Eine Variable ist ein Datenelement aus Ihrem Datensatz, das Sie verwenden möchten, um den Ereignistyp, das Modell und die Regeln zu erstellen.

Im folgenden Beispiel wird die [CreateVariable](#) API verwendet, um zwei Variablen zu erstellen. Die Variablen sind `email_address` und `ip_address`. Weisen Sie sie den entsprechenden Variablentypen zu: `EMAIL_ADDRESS` und `IP_ADDRESS`. Diese Variablen sind Teil des Beispieldatensatzes, den Sie hochgeladen haben. Wenn Sie den Variablentyp angeben, interpretiert Amazon Fraud Detector die Variable während des Modelltrainings und beim Abrufen von Vorhersagen. Nur Variablen mit einem zugehörigen Variablentyp können für das Modelltraining verwendet werden.

```
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>'
)
```

## Entitätstyp erstellen

Eine Entität stellt dar, wer das Ereignis ausführt bewertet die Entität. Zu den Klassifizierungen gehören beispielsweise Kunde, Händler oder Konto.

Im folgenden Beispiel wird [PutEntityType](#) API verwendet, um einensample\_customer Entitätstyp zu erstellen.

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

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

## Erstellen einer Beschriftung

Eine Beschriftung klassifiziert ein Ereignis als betrügerisch oder legitim und dient dazu, das Betrugserkennungsmodell zu trainieren. Das Modell lernt, Ereignisse anhand dieser Labelwerte zu klassifizieren.

Im folgenden Beispiel wird die [PutLabel-API](#) verwendet, um zwei Labels zu erstellen, `fraud` und `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'
)
```

### Schritt 3: Erstellen von Ereignistyp

Mit Amazon Fraud Detector erstellen Sie Modelle zur Bewertung von Risiken und Generierung von Betrugsprognosen für einzelne Ereignisse. Ein Ereignistyp definiert die Struktur eines einzelnen Ereignisses.

Im folgenden Beispiel wird die [PutEventTypeAPI](#) verwendet, um einen Ereignistyp zu erstellen `sample_registration`. Sie definieren den Ereignistyp, indem Sie die Variablen (`email_address`, `ip_address`), den Entitätstyp (`sample_customer`) und die Bezeichnungen (`fraud`, `legit`) angeben, die Sie im vorherigen Schritt erstellt haben.

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

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

### Schritt 4: Modell erstellen, trainieren und bereitstellen

Amazon Fraud Detector trainiert Modelle, um zu lernen, Betrug für einen bestimmten Ereignistyp zu erkennen. Im vorherigen Schritt haben Sie den Ereignistyp erstellt. In diesem Schritt erstellen und

trainieren Sie ein Modell für den Ereignistyp. Das Modell dient als Container für Ihre Modellversionen. Jedes Mal, wenn Sie ein Modell trainieren, wird eine neue Version erstellt.

Verwenden Sie die folgenden Beispielcodes, um ein Online Fraud Insights-Modell zu erstellen und zu trainieren. Dieses Modell heißt `sample_fraud_detection_model`. Es ist für den Ereignistyp `sample_registration` verwendet den Beispieldatensatz für die Kontoregistrierung, den Sie auf Amazon S3 hochgeladen haben.

Weitere Informationen zu den verschiedenen Modelltypen, die Amazon Fraud Detector unterstützt, finden Sie unter [Wählen Sie einen Modelltyp](#).

### Erstellen Sie ein Modell

Im folgenden Beispiel wird die [CreateModel](#)API verwendet, um ein Modell zu erstellen.

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

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

### Trainiere ein Model

Im folgenden Beispiel wird die [CreateModelVersion](#)API verwendet, um das Modell zu trainieren. Geben Sie `'EXTERNAL_EVENTS'` für `trainingDataSource` und den Amazon S3 S3-Standort an, an dem Sie Ihren Beispieldatensatz gespeichert haben, und den RoleArndes Amazon S3 S3-Buckets für `externalEventsDetail`. Geben Sie al `trainingDataSchema` Parameter an, wie Amazon Fraud Detector die Beispieldaten interpretiert. Geben Sie insbesondere an, welche Variablen einbezogen werden sollen und wie die Ereignisbeschriftungen klassifiziert werden sollen.

```
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'
    }
)
```

Sie können Ihr Modell mehrfach trainieren. Jedes Mal, wenn Sie ein Modell trainieren, wird eine neue Version erstellt. Nach Abschluss des Modelltrainings wird der Status der Modellversion auf `aktualisiertTRAINING_COMPLETE`. Sie können den Modelleleistungswert und andere Kennzahlen zur Modelleleistung überprüfen.

### Überprüfen Sie die Leistung des Modells

Ein wichtiger Schritt bei der Verwendung von Amazon Fraud Detector besteht darin, die Genauigkeit Ihres Modells anhand von Modellbewertungen und Leistungskennzahlen zu bewerten. Nach Abschluss des Modelltrainings validiert Amazon Fraud Detector die Modelleleistung anhand der 15% Ihrer Daten, die nicht zum Trainieren des Modells verwendet wurden. Es generiert einen Modelleleistungswert und andere Leistungsmetriken.

Verwenden Sie die [DescribeModelVersions](#) API, um die Modelleleistung zu überprüfen. Sehen Sie sich den Gesamtwert der Modelleleistung und alle anderen von Amazon Fraud Detector für dieses Modell generierten Metriken an.

Weitere Informationen zum Leistungswert und zu den Leistungskennzahlen des Modells finden Sie unter [Modellwerte](#) und [Modelleleistungsmetriken](#).

Sie können davon ausgehen, dass alle Ihre trainierten Amazon Fraud Detector Modelle über reale Leistungskennzahlen zur Betrugserkennung verfügen, die den Kennzahlen in diesem Tutorial ähneln.

### Stellen Sie ein Modell bereit

Nachdem Sie die Leistungskennzahlen Ihres trainierten Modells überprüft haben, stellen Sie das Modell bereit und stellen Sie es Amazon Fraud Detector zur Verfügung, um Betrugsvorhersagen zu

erstellen. Verwenden Sie die [UpdateModelVersionStatus](#)API, um das trainierte Modell bereitzustellen. Im folgenden Beispiel wird es verwendet, um den Status der Modellversion auf ACTIVE zu aktualisieren.

```
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'
)
```

### Schritt 5: Detektor, Ergebnisse, Regeln und Detektorversion erstellen

Ein Detektor enthält die Erkennungslogik, z. B. die Modelle und Regeln. Diese Logik bezieht sich auf ein bestimmtes Ereignis, das Sie auf Betrug hin auswerten möchten. Eine Regel ist eine Bedingung, die Sie angeben, um Amazon Fraud Detector mitzuteilen, wie Variablenwerte während der Vorhersage zu interpretieren sind. Und das Ergebnis ist das Ergebnis einer Betrugsvorhersage. Ein Melder kann mehrere Versionen haben, wobei jede Version den Status ENTWURF, AKTIV oder INAKTIV hat. Einer Detektorversion muss mindestens eine Regel zugeordnet sein.

Verwenden Sie die folgenden Beispielcodes, um den Detektor, die Regeln und das Ergebnis zu erstellen und den Detektor zu veröffentlichen.

#### Erstellen eines Detektors

Im folgenden Beispiel wird die [PutDetector](#)API verwendet, um ein `sample_detector` Detektor für `sample_registration` Ereignistyp zu erstellen.

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

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

## Ergebnisse schaffen

Für jedes mögliche Ergebnis der Betrugsprognose werden Ergebnisse erstellt. Im folgenden Beispiel wird die [PutOutcome](#)API verwendet, um drei Ergebnisse zu erstellen: `verify_customerreview`, `undapprove`. Diese Ergebnisse werden später Regeln zugewiesen.

```
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'
)
```

## Regeln erstellen

Die Regel besteht aus einer oder mehreren Variablen aus Ihrem Datensatz, einem logischen Ausdruck und einem oder mehreren Ergebnissen.

Im folgenden Beispiel wird die [CreateRule](#)API verwendet, um drei verschiedene Regeln zu erstellen: `high_risk`, `medium_risk`, und `low_risk`. Erstellen Sie Regelausdrücke, um den Wert des `sample_fraud_detection_model_insightscore` Modellleistungswerts mit verschiedenen Schwellenwerten zu vergleichen. Dies dient dazu, das Risikoniveau für ein Ereignis zu bestimmen und das im vorherigen Schritt definierte Ergebnis zuzuweisen.

```
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']
)
```

## Erstellen einer Detektorversion

Eine Version des Detektors definiert ein Modell und Regeln, die zur Betrugsvorhersage verwendet werden.

Im folgenden Beispiel wird die [CreateDetectorVersion](#) API verwendet, um eine Detektorversion zu erstellen. Dazu werden Modellversionsdetails, Regeln und ein Regelausführungsmodus FIRST\_MATCHED bereitgestellt. Ein Regelausführungsmodus gibt die Reihenfolge für die Auswertung von Regeln an. Der Regelausführungsmodus FIRST\_MATCHED gibt an, dass die Regeln nacheinander von der ersten bis zur letzten und stoppt dabei bei der ersten übereinstimmenden Regel.

```
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'
)
```

## Schritt 6: Generierung von Betrugsprognosen

Im letzten Schritt dieses Tutorials wird der im vorherigen Schrittsample\_detector erstellte Detektor verwendet, um Betrugsvorhersagen für densample\_registration Ereignistyp in Echtzeit zu generieren. Der Detektor wertet die Beispieldaten aus, die auf Amazon S3 hochgeladen wurden. Die Antwort umfasst die Leistungswerte des Modells sowie alle Ergebnisse, die den abgeglichenen Regeln zugeordnet sind.

Im folgenden Beispiel wird die [GetEventPrediction](#)API verwendet, um bei jeder Anfrage Daten aus einer einzelnen Kontoregistrierung bereitzustellen. Verwenden Sie für dieses Tutorial Daten (email\_address und ip\_address) aus der Beispieldatendatei für die Kontoregistrierung. Jede Zeile (Zeile) nach der oberen Kopfzeile steht für Daten aus einem einzelnen Kontoregistrierungsereignis.

```
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'  
    }  
)
```

Nachdem Sie dieses Tutorial abgeschlossen haben, sind Sie wie folgt vorgegangen:

- Hat einen Beispiel-Ereignisdatensatz in Amazon S3 hochgeladen.
- Variablen, Entitäten und Labels erstellt, die zum Erstellen und Trainieren eines Modells verwendet werden.
- Anhand des Beispieldatensatzes wurde ein Modell erstellt und trainiert.
- Der Leistungswert des Modells und andere von Amazon Fraud Detector generierte Leistungskennzahlen wurden angezeigt.
- Das Modell zur Betrugserkennung wurde eingesetzt.
- Erstellte einen Detektor und fügte das bereitgestellte Modell hinzu.
- Dem Detektor wurden Regeln, die Reihenfolge der Regelausführung und Ergebnisse hinzugefügt.
- Erstellen der Detektorversion.
- Der Detektor wurde getestet, indem verschiedene Eingaben bereitgestellt und überprüft wurden, ob die Regeln und die Reihenfolge der Regelausführung wie erwartet funktionierten.

## (Optional) Erkunden Sie die Amazon Fraud Detector Detector-APIs mit einem Jupyter-Notebook (iPython)

Weitere Beispiele für die Verwendung der Amazon Fraud Detector Detector-APIs finden Sie im [aws-fraud-detector-samples GitHub Repository](#). Zu den Themen, die in den Notizbüchern behandelt werden, gehören sowohl das Erstellen von Modellen als auch Detektoren mithilfe der Amazon Fraud Detector Detector-APIs sowie das Erstellen von Anfragen zur Batch-Betrugsprognose mithilfe der `GetEventPrediction` API.

## Nächste Schritte

Nachdem Sie nun ein Modell und einen Detektor erstellt haben, können Sie sich eingehender damit befassen und mit der Erstellung von Modellen und Detektoren sowie der Generierung von Betrugsvorhersagen beginnen.

In den folgenden Abschnitten des Amazon Fraud Detector-Benutzerhandbuchs wird beschrieben, wie Ihr Unternehmen oder Ihre Organisation Amazon Fraud Detector zur Betrugserkennung verwenden kann.

- Bereiten Sie Ihren Ereignisdatensatz für das Training Ihres Modells vor.
- Ereignistyp erstellen
- Erstellen eines Modells
- Erstellen eines Detektors
- Holen Sie sich Betrugsprognosen
- Verwalten Sie Ihre Amazon Fraud Detector Detector-Ressourcen (insbesondere Variablen, Entitäten, Ergebnisse und Labels)
- Konfigurieren Sie Amazon Fraud Detector entsprechend Ihren Sicherheits- und Compliance-Zielen
- Überwachen Sie Amazon Fraud Detector und protokollieren Sie Amazon Fraud Detector Detector-API-Aufrufe
- Fehlerbehebung für Amazon Fraud Detector

# Ereignis-Dataset

Ein Ereignisdatensatz sind die historischen Betrugsdaten für Ihr Unternehmen. Sie stellen diese Daten Amazon Fraud Detector zur Verfügung, um Modelle zur Betrugserkennung zu erstellen.

Amazon Fraud Detector verwendet Modelle für maschinelles Lernen zur Generierung von Betrugsvorhersagen. Jedes Modell wird mit einem Modelltyp trainiert. Der Modelltyp spezifiziert die Algorithmen und Transformationen, die für das Training des Modells verwendet werden. Beim Modelltraining wird anhand eines von Ihnen bereitgestellten Datensatzes ein Modell erstellt, das betrügerische Ereignisse vorhersagen kann. Weitere Informationen finden Sie unter [Die Funktionsweise von Amazon Fraud Detector](#)

Der für die Erstellung eines Modells zur Betrugserkennung verwendete Datensatz enthält Details zu einem Ereignis. Ein Ereignis ist eine geschäftliche Aktivität, die auf Betrugsrisiken überprüft wird. Beispielsweise kann eine Kontoregistrierung ein Ereignis sein. Bei den mit dem Kontoregistrierungsereignis verknüpften Daten kann es sich um einen Ereignisdatensatz handeln. Amazon Fraud Detector verwendet diesen Datensatz, um Betrug bei der Kontoregistrierung zu bewerten.

Bevor Sie Ihren Datensatz Amazon Fraud Detector zur Erstellung eines Modells zur Verfügung stellen, stellen Sie sicher, dass Sie Ihr Ziel für die Erstellung des Modells definieren. Sie müssen außerdem festlegen, wie Sie das Modell verwenden möchten, und Ihre Kennzahlen definieren, um anhand Ihrer spezifischen Anforderungen zu bewerten, ob das Modell funktioniert.

Ihre Ziele für die Erstellung eines Modells zur Betrugserkennung, das Betrug bei der Kontoregistrierung bewertet, können beispielsweise die folgenden sein:

- Um legitime Registrierungen automatisch zu genehmigen.
- Um betrügerische Anmeldungen für eine spätere Untersuchung zu erfassen.

Nachdem Sie Ihr Ziel festgelegt haben, müssen Sie im nächsten Schritt entscheiden, wie Sie das Modell verwenden möchten. Im Folgenden finden Sie einige Beispiele für die Verwendung des Betrugserkennungsmodells zur Bewertung von Registrierungsbruch:

- Zur Betrugserkennung in Echtzeit für jede Kontoregistrierung.
- Zur stündlichen Offline-Auswertung aller Kontoregistrierungen.

Einige Beispiele für Metriken, mit denen die Leistung des Modells gemessen werden kann, sind die folgenden:

- Die Leistung ist durchweg besser als der aktuelle Ausgangswert in der Produktion.
- Erfasst X% Betrugsregistrierungen mit einer Rate von Y% falsch positiven Ergebnissen.
- Akzeptiert bis zu 5% der automatisch genehmigten betrügerischen Registrierungen.

## Struktur von Ereignisdataset

Amazon Fraud Detector verlangt, dass Sie Ihren Ereignisdatensatz in einer Textdatei mit kommagetrennten Werten (CSV) im UTF-8-Format angeben. Die erste Zeile Ihrer CSV-Datensatzdatei muss Dateiüberschriften enthalten. Der Dateihheader besteht aus Ereignismetadaten und Ereignisvariablen, die jedes Datenelement beschreiben, das mit dem Ereignis verknüpft ist. Auf den Header folgen Ereignisdaten. Jede Zeile besteht aus Datenelementen eines einzelnen Ereignisses.

- Ereignismetadaten — enthält Informationen über das Ereignis. Beispielsweise ist `EVENT_TIMESTAMP` ein Ereignismetadat, der den Zeitpunkt des Auftretens des Ereignisses angibt. Abhängig von Ihrem geschäftlichen Anwendungsfall und dem Modelltyp, der für die Erstellung und Schulung Ihres Betrugserkennungsmodells verwendet wird, verlangt Amazon Fraud Detector, dass Sie bestimmte Ereignismetadaten angeben. Verwenden Sie bei der Angabe von Ereignismetadaten in Ihrem CSV-Datei-Header denselben Event-Metadatenamen wie von Amazon Fraud Detector angegeben und verwenden Sie nur Großbuchstaben.
- Ereignisvariable — stellt die für Ihr Ereignis spezifischen Datenelemente dar, die Sie für die Erstellung und das Training Ihres Betrugserkennungsmodells verwenden möchten. Abhängig von Ihrem geschäftlichen Anwendungsfall und dem Modelltyp, der für die Erstellung und Schulung eines Betrugserkennungsmodells verwendet wird, verlangt oder empfiehlt Amazon Fraud Detector möglicherweise, dass Sie bestimmte Ereignisvariablen angeben. Sie können optional auch andere Ereignisvariablen aus Ihrem Ereignis angeben, die Sie in das Training des Modells einbeziehen möchten. Einige Beispiele für Ereignisvariablen für eine Online-Registrierungsveranstaltung können E-Mail-Adresse, IP-Adresse und Telefonnummer sein. Wenn Sie den Namen der Ereignisvariablen in Ihrem CSV-Datei-Header angeben, verwenden Sie einen beliebigen Variablennamen Ihrer Wahl und verwenden Sie nur Kleinbuchstaben.
- Ereignisdaten — stellen die Daten dar, die während des tatsächlichen Ereignisses gesammelt wurden. In Ihrer CSV-Datei besteht jede Zeile, die auf den Dateihheader folgt, aus Datenelementen eines einzelnen Ereignisses. In einer Eventdatendatei für die Online-Registrierung enthält

beispielsweise jede Zeile Daten aus einer einzelnen Registrierung. Jedes Datenelement in der Zeile muss mit den entsprechenden Ereignismetadaten oder der Ereignisvariablen übereinstimmen.

Nachfolgend finden Sie ein Beispiel für eine CSV-Datei mit Daten aus einem Ereignis zur Kontoregistrierung. Die Kopfzeile enthält sowohl Ereignismetadaten in Großbuchstaben als auch Ereignisvariablen in Kleinbuchstaben, gefolgt von den Ereignisdaten. Jede Zeile im Datensatz enthält Datenelemente, die mit der Registrierung eines einzelnen Kontos verknüpft sind, wobei jedes Datenelement der Kopfzeile entspricht.

Event metadata			Event variables				
EVENT_TIMESTAMP,	EVENT_ID,	EVENT_LABEL,	email_address,	phone_number,	billing_street,	billing_state,	ip_address
2020-12-06T03:13:34Z,	R12345,	fraud,	regular1@example.com,	110-345-0990,	mayhem ave,	OH,	112.136.132.151
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

← Header  
← Event data  
Event dataset

## Rufen Sie die Anforderungen für Ereignisdatensätze mit dem Datenmodell-Explorer ab

Der Modelltyp, den Sie für die Erstellung Ihres Modells wählen, definiert die Anforderungen für Ihren Datensatz. Amazon Fraud Detector verwendet den von Ihnen bereitgestellten Datensatz, um Ihr Modell zur Betrugserkennung zu erstellen und zu trainieren. Bevor Amazon Fraud Detector mit der Erstellung Ihres Modells beginnt, prüft es, ob der Datensatz die Größe, das Format und andere Anforderungen erfüllt. Wenn der Datensatz die Anforderungen nicht erfüllt, schlagen die Modellerstellung und das Training fehl. Sie können den Datenmodell-Explorer verwenden, um einen Modelltyp zu identifizieren, der für Ihren geschäftlichen Anwendungsfall verwendet werden soll, und um Einblicke in die Datensatz-Anforderungen für den identifizierten Modelltyp zu erhalten.

## Datenmodell-Explorer

Der Datenmodell-Explorer ist ein Tool in der Amazon Fraud Detector-Konsole, das Ihren Geschäftsanwendungsfall an den von Amazon Fraud Detector unterstützten Modelltyp anpasst. Der Datenmodell-Explorer bietet auch Einblicke in die Datenelemente, die Amazon Fraud Detector benötigt, um Ihr Modell zur Betrugserkennung zu erstellen. Bevor Sie mit der Vorbereitung Ihres Ereignisdatensatzes beginnen, verwenden Sie den Datenmodell-Explorer, um herauszufinden, welchen Modelltyp Amazon Fraud Detector für Ihre geschäftliche Verwendung empfiehlt. Außerdem erhalten Sie eine Liste der obligatorischen, empfohlenen und optionalen Datenelemente, die Sie für die Erstellung Ihres Datensatzes benötigen.

Um den Datenmodell-Explorer zu verwenden,

1. Öffnen Sie die [AWSManagement Console](#) und melden Sie sich bei Ihrem Konto an. Navigieren Sie zu Amazon Fraud Detector.
2. Wählen Sie im linken Navigationsbereich Data Models Explorer aus.
3. Wählen Sie auf der Explorer-Seite für Datenmodelle unter Geschäftsanwendungsfall den Geschäftsanwendungsfall aus, den Sie im Hinblick auf das Betrugsrisiko bewerten möchten.
4. Amazon Fraud Detector zeigt den empfohlenen Modelltyp an, der Ihrem Geschäftsanwendungsfall entspricht. Der Modelltyp definiert die Algorithmen, Anreicherungen und Transformationen, die Amazon Fraud Detector zum Trainieren Ihres Betrugserkennungsmodells verwendet.

Notieren Sie sich den empfohlenen Modelltyp. Sie benötigen diesen später beim Erstellen Ihres Modells.

#### Note

Wenn Sie Ihren geschäftlichen Anwendungsfall nicht finden, verwenden Sie den Link „Kontaktieren Sie uns“ in der Beschreibung, um uns die Details Ihres geschäftlichen Anwendungsfalls mitzuteilen. Wir empfehlen Ihnen, welchen Modelltyp Sie für die Erstellung eines Betrugserkennungsmodells für Ihren Geschäftsanwendungsfall verwenden möchten.

5. Der Bereich Datenmodellinformationen bietet einen Einblick in die obligatorischen, empfohlenen und optionalen Datenelemente, die erforderlich sind, um ein Betrugserkennungsmodell für Ihren Geschäftsanwendungsfall zu erstellen und zu trainieren. Verwenden Sie die Informationen im Bereich Einblicke, um Ihre Eventdaten zu sammeln und Ihren Datensatz zu erstellen.

## Ereignisdaten sammeln

Das Erfassen Ihrer Eventdaten ist ein wichtiger Schritt bei der Erstellung Ihres Modells. Dies liegt daran, dass die Leistung Ihres Modells bei der Betrugsvorhersage von der Qualität Ihres Datensatzes abhängt. Denken Sie beim Sammeln Ihrer Ereignisdaten an die Liste der Datenelemente, die Ihnen der Datenmodell-Explorer zur Erstellung Ihres Datensatzes zur Verfügung gestellt hat. Sie müssen alle obligatorischen Daten (Ereignismetadaten) sammeln und entscheiden, welche empfohlenen und optionalen Datenelemente (Ereignisvariablen) enthalten sein sollen, basierend auf Ihren Zielen für die

Erstellung des Modells. Es ist auch wichtig, das Format jeder Ereignisvariablen, die Sie einbeziehen möchten, und die Gesamtgröße Ihres Datensatzes festzulegen.

## Qualität des Event-Datensatzes

Es wird Folgendes empfohlen, um qualitativ hochwertige Datensätze für Ihr Modell zu erstellen:

- Erfassung ausgereifter Daten — Die Verwendung der neuesten Daten hilft dabei, das neueste Betrugsmuster zu identifizieren. Lassen Sie die Daten jedoch reifen, um Betrugsfälle zu erkennen. Die Laufzeit hängt von Ihrem Unternehmen ab und kann zwischen zwei Wochen und drei Monaten dauern. Wenn Ihr Ereignis beispielsweise eine Kreditkartentransaktion beinhaltet, kann der Reifegrad der Daten durch die Rückbuchungsfrist der Kreditkarte oder die Zeit bestimmt werden, die ein Prüfer benötigt, um eine Entscheidung zu treffen.


Stellen Sie sicher, dass der Datensatz, der zum Trainieren des Modells verwendet wurde, ausreichend Zeit hatte, um gemäß Ihrem Unternehmen zu reifen.

- Stellen Sie sicher, dass die Datenverteilung nicht signifikant abweicht. Amazon Fraud Detector modelliert Muster für Trainingsprozesse und partitioniert Ihren Datensatz auf der Grundlage von `EVENT_TIMESTAMP`. Wenn Ihr Datensatz beispielsweise aus Betrugsfällen der letzten 6 Monate besteht, aber nur die legitimen Ereignisse des letzten Monats enthalten sind, gilt die Datenverteilung als uneinheitlich und instabil. Ein instabiler Datensatz kann zu Verzerrungen bei der Bewertung der Modellleistung führen. Wenn Sie feststellen, dass die Datenverteilung erheblich abweicht, sollten Sie erwägen, Ihren Datensatz auszugleichen, indem Sie Daten sammeln, die der aktuellen Datenverteilung ähneln.
- Stellen Sie sicher, dass der Datensatz für den Anwendungsfall repräsentativ ist, in dem das Modell implementiert/getestet wird. Andernfalls könnte die geschätzte Leistung verzerrt sein. Nehmen wir an, Sie verwenden ein Modell, mit dem automatisch alle internen Bewerber abgelehnt werden, Ihr Modell wird jedoch mit einem Datensatz trainiert, der historische Daten/Bezeichnungen enthält, die zuvor genehmigt wurden. Dann ist die Bewertung Ihres Modells möglicherweise ungenau, da die Bewertung auf dem Datensatz basiert, der keine Repräsentationen von abgelehnten Bewerbern enthält.

## Format der Veranstaltungsdaten

Amazon Fraud Detector wandelt die meisten Ihrer Daten im Rahmen seines Modelltrainingsprozesses in das erforderliche Format um. Es gibt jedoch einige Standardformate, die Sie problemlos für die Bereitstellung Ihrer Daten verwenden können, um später Probleme zu

vermeiden, wenn Amazon Fraud Detector Ihren Datensatz validiert. Die folgende Tabelle enthält Hinweise zu den Formaten für die Bereitstellung der empfohlenen Ereignismetadaten.

 Note

Achten Sie beim Erstellen Ihrer CSV-Datei darauf, den Namen der Veranstaltungsmetadaten wie unten aufgeführt in Großbuchstaben einzugeben.

Name der Metadaten	Format	Erforderlich
EVENT_ID	<p>Wenn es bereitgestellt wird, muss es die folgenden Anforderungen erfüllen:</p> <ul style="list-style-type: none"> <li>• Es ist einzigartig für diese Veranstaltung.</li> <li>• Es stellt Informationen dar, die für Ihr Unternehmen von Bedeutung sind.</li> <li>• Es folgt dem regulären Ausdrucksmuster (zum Beispiel <code>^[0-9a-z_-]+\$.)</code></li> <li>• Zusätzlich zu den oben genannten Anforderungen empfehlen wir, dass Sie der EVENT_ID keinen Zeitstempel anhängen. Dies kann zu Problemen führen, wenn Sie das Ereignis aktualisieren. Dies liegt daran, dass Sie in diesem Fall genau dieselbe EVENT_ID angeben müssen.</li> </ul>	Hängt vom Modelltyp ab



Name der Metadaten	Format	Erforderlich
ZEITSTEMPEL DES EREIGNISSES	<ul style="list-style-type: none"> <li>• Sie muss in einem der folgenden Formate angegeben werden:               <ul style="list-style-type: none"> <li>• %yyyy-%mm-%ddt%HH: %mm: %ssZ (ISO 8601-Standard in UTC nur ohne Millisekunden)</li> </ul> <p>Beispiel: 2019-11-30T 13:01:01 Z</p> <li>• %yyyy/%mm/%dd %hh: %mm: %ss (vormittag/nachmittags)</li> </li></ul> <p>Beispiele: 30.11.2019 9 13:01:01 Uhr oder 30.11.2019 13:01:01</p> <ul style="list-style-type: none"> <li>• %mm/%dd/%yyyy %hh: %mm: %ss</li> </ul> <p>Beispiele: 30.11.2019 13:01:01 Uhr, 30.11.2019 13:01:01</p> <ul style="list-style-type: none"> <li>• %mm/%dd/%yy %hh: %mm: %ss</li> </ul> <p>Beispiele: 30.11.19 13:01:01 PM, 30.11.19 13:01:01</p> <li>• Amazon Fraud Detector geht beim Analysieren von Datums-/Zeitstempelformaten nach Ereigniszeitstempeln von folgenden Annahmen aus:</li>	Ja

Name der Metadaten	Format	Erforderlich
	<ul style="list-style-type: none"><li>• Wenn Sie den ISO 8601-Standard verwenden, muss dieser exakt mit der vorherigen Spezifikation übereinstimmen</li><li>• Wenn Sie eines der anderen Formate verwenden, gibt es zusätzliche Flexibilität:<ul style="list-style-type: none"><li>• Für Monate und Tage können Sie einstellige oder zweistellige Zahlen angeben. Beispielsweise ist der 12.01.2019 ein gültiges Datum.</li><li>• Sie müssen hh:mm:ss nicht angeben, wenn Sie sie nicht haben (das heißt, Sie können einfach ein Datum angeben). Sie können auch nur eine Teilmenge von Stunde und Minuten angeben (z. B. hh:mm). Die bloße Angabe der Stunde wird nicht unterstützt. Millisekunden werden ebenfalls nicht unterstützt.</li></ul></li><li>• Wenn Sie AM/PM-Etiketten angeben, wird von einer 12-Stunde</li></ul>	

Name der Metadaten	Format	Erforderlich
	<p>n-Uhr ausgegangen. Wenn keine AM/PM-Informationen vorliegen, wird von einer 24-Stunden-Uhr ausgegangen.</p> <ul style="list-style-type: none"> <li>Sie können „/“ oder „-“ als Trennzeichen für die Datumselemente verwenden. „:“ wird für die Zeitstempellemente vorausgesetzt.</li> </ul>	
ENTITY_ID	<ul style="list-style-type: none"> <li>Es muss dem regulären Ausdrucksmuster folgen: <code>^[0-9A-Za-z_@+-]+\$</code>.</li> <li>Wenn die Entitäts-ID zum Zeitpunkt der Auswertung nicht verfügbar ist, geben Sie die Entitäts-ID als unbekannt an.</li> </ul>	Hängt vom Modelltyp ab
ENTITÄTSTYP	Sie können eine beliebige Zeichenfolge verwenden	Hängt vom Modelltyp ab
BEZEICHNUNG DES EREIGNISSES	Sie können beliebige Bezeichnungen verwenden, z. B. „Betrug“, „legitim“, „1“ oder „0“.	Erforderlich, wenn LABEL_TIMESTAMP enthalten ist
LABEL_TIMESTAMP	Es muss dem Zeitstempelformat folgen.	Erforderlich, wenn EVENT_LABEL enthalten ist

Hinweise zu Ereignisvariablen finden Sie unter [Variablen](#).

**⚠ Important**

Wenn Sie ein Account Takeover Insights (ATI) -Modell erstellen, finden Sie weitere Informationen [Vorbereiten von Daten](#) zur Vorbereitung und Auswahl von Daten unter.

## Null oder fehlende Werte

Die Variablen `EVENT_TIMESTAMP` und `EVENT_LABEL` dürfen keine Nullwerte oder fehlende Werte enthalten. Sie können Nullwerte oder fehlende Werte für andere Variablen haben. Wir empfehlen jedoch, nur eine kleine Anzahl von Nullen für diese Variablen für diese Variablen zu verwenden. Wenn Amazon Fraud Detector feststellt, dass zu viele Nullwerte oder fehlende Werte für eine Ereignisvariable vorhanden sind, wird die Variable automatisch aus Ihrem Modell weggelassen.

## Minimale Variablen

Wenn Sie Ihr Modell erstellen, muss der Datensatz zusätzlich zu den erforderlichen Ereignismetadaten mindestens zwei Ereignisvariablen enthalten. Die beiden Ereignisvariablen müssen die Validierungsprüfung bestehen.

## Größe des Event-Datensatzes

### Erforderlich

Ihr Datensatz muss die folgenden grundlegenden Anforderungen für ein erfolgreiches Modelltraining erfüllen.

- Daten von mindestens 100 Ereignissen.
- Der Datensatz muss mindestens 50 Ereignisse (Zeilen) enthalten, die als betrügerisch eingestuft wurden.

### Empfohlen

Für ein erfolgreiches Modelltraining und eine gute Modellleistung empfehlen wir, dass Ihr Datensatz Folgendes enthält.

- Schließen Sie mindestens drei Wochen an historischen Daten ein, bestenfalls jedoch Daten für sechs Monate.
- Schließen Sie insgesamt mindestens 10.000 Ereignisdaten ein.

- Schließen Sie mindestens 400 Ereignisse (Zeilen) ein, die als betrügerisch eingestuft wurden, und 400 Ereignisse (Zeilen), die als legitim eingestuft wurden.
- Schließen Sie mehr als 100 eindeutige Entitäten ein, wenn Ihr Modelltyp ENTITY\_ID erfordert.

## Datensatzvalidierung

Bevor Amazon Fraud Detector mit der Erstellung Ihres Modells beginnt, prüft es, ob die im Datensatz für das Training des Modells enthaltenen Variablen die Größe, das Format und andere Anforderungen erfüllen. Wenn der Datensatz die Validierung nicht besteht, wird kein Modell erstellt. Sie müssen zuerst die Variablen korrigieren, die die Validierung nicht bestanden haben, bevor Sie das Modell erstellen. Amazon Fraud Detector bietet Ihnen einen Datenprofiler, mit dem Sie Probleme mit Ihrem Datensatz identifizieren und beheben können, bevor Sie mit dem Training Ihres Modells beginnen.

### Datenprofiler

Amazon Fraud Detector bietet ein Open-Source-Tool für die Erstellung von Profilen und die Vorbereitung Ihrer Daten für das Modelltraining. Mit diesem automatisierten Datenprofiler können Sie häufige Fehler bei der Datenvorbereitung vermeiden und potenzielle Probleme wie falsch zugeordnete Variablentypen identifizieren, die sich negativ auf die Modellleistung auswirken würden. Der Profiler generiert einen intuitiven und umfassenden Bericht über Ihren Datensatz, einschließlich Variablenstatistiken, Labelverteilung, kategorialer und numerischer Analysen sowie Variablen- und Labelkorrelationen. Es enthält Anleitungen zu Variablentypen sowie eine Option zur Umwandlung des Datensatzes in ein Format, das Amazon Fraud Detector benötigt.

### Datenprofiler verwenden

Der automatisierte Datenprofiler besteht aus einem AWS CloudFormation Stack, den Sie mit wenigen Klicks einfach starten können. Alle Codes sind auf [Github](#) verfügbar. Informationen zur Verwendung von Data Profiler finden Sie in unserem Blog [Train models faster with an automated data profiler for Amazon Fraud Detector](#).

### Häufige Fehler im Ereignisdatsatz

Im Folgenden sind einige der häufigsten Probleme aufgeführt, auf die Amazon Fraud Detector bei der Validierung eines Ereignisdatsatzes stößt. Nachdem Sie den Datenprofiler ausgeführt haben, verwenden Sie diese Liste, um Ihren Datensatz auf Fehler zu überprüfen, bevor Sie Ihr Modell erstellen.

- Die CSV-Datei hat nicht das Format UTF-8.
- Die Anzahl der Ereignisse im Datensatz beträgt weniger als 100.
- Die Anzahl der als betrügerisch oder legitim identifizierten Ereignisse liegt unter 50.
- Die Anzahl der eindeutigen Entitäten, die einem Betrugsereignis zugeordnet sind, beträgt weniger als 100.
- Mehr als 0,1% der Werte in EVENT\_TIMESTAMP enthalten Nullen oder andere Werte als die unterstützten Datums-/Uhrzeitstempelformate.
- Mehr als 1% der Werte in EVENT\_LABEL enthalten Nullen oder Werte, die nicht im Ereignistyp definiert sind.
- Für das Modelltraining stehen weniger als zwei Variablen zur Verfügung.

## Datensatzspeicher

Nachdem Sie Ihren Dataset gesammelt haben, speichern Sie ihn intern mit Amazon Fraud Detector oder extern mit Amazon Simple Storage Service (Amazon S3) -Dataset mit Amazon Fraud Detector oder extern mit Amazon Simple Storage Service (Amazon S3) Wir empfehlen Ihnen, anhand des Modells, das Sie für die Generierung von Betrugsprognosen verwenden, auszuwählen, wo Ihr Datensatz gespeichert werden soll. Weitere Informationen zu Modelltypen finden [Sie unter Wählen eines Modelltyps](#). Weitere Informationen zum Speichern Ihres Datensatzes finden Sie unter [Speicherung der Ereignisdaten](#).

# Ereignistyp

Mit Amazon Fraud Detector erstellen Sie Betrugsprognosen für Ereignisse. Ein Ereignistyp definiert die Struktur für ein einzelnes Ereignis, das an Amazon Fraud Detector gesendet wird. Nach der Definition können Sie Modelle und Detektoren erstellen, die das Risiko für bestimmte Ereignistypen bewerten.

Die Struktur einer Veranstaltung umfasst Folgendes:

- **Entitätstyp:** Klassifiziert, wer die Veranstaltung durchführt. Geben Sie während der Vorhersage den Entitätstyp und die Entitäts-ID an, um zu definieren, wer das Ereignis durchgeführt hat.
- **Variablen:** Definiert, welche Variablen als Teil des Events gesendet werden können. Variablen werden in Modellen und Regeln zur Bewertung des Betrugsrisikos verwendet. Nach dem Hinzufügen können Variablen nicht aus einem Ereignistyp entfernt werden.
- **Labels:** Klassifiziert ein Ereignis als betrügerisch oder legitim. Wird während des Modelltrainings verwendet. Nach dem Hinzufügen können Labels nicht mehr aus einem Ereignistyp entfernt werden.

## Einen Ereignistyp erstellen

Bevor Sie Ihr Betrugserkennungsmodell erstellen, müssen Sie zunächst einen Ereignistyp erstellen. Um einen Ereignistyp zu erstellen, müssen Sie Ihre Geschäftsaktivität (Ereignis) definieren, um sie auf Betrug hin zu untersuchen. Zur Definition des Ereignisses gehören die Identifizierung der Ereignisvariablen in Ihrem Datensatz, die für die Betrugsauswertung berücksichtigt werden sollen, sowie die Angabe der Entität, die das Ereignis auslöst, und der Bezeichnungen, die das Ereignis klassifizieren.

Voraussetzungen für die Erstellung eines Ereignistyps

Bevor Sie mit der Erstellung Ihres Ereignistyps beginnen, stellen Sie sicher, dass Sie die folgenden Schritte ausgeführt haben:

- Haben das [Datenmodell-Explorer](#) Tool verwendet, um Einblicke in die Datenelemente zu gewinnen, die Amazon Fraud Detector zur Erstellung Ihres Betrugserkennungsmodells benötigt.
- Haben Sie die Erkenntnisse aus dem Data Models Explorer verwendet, um Ihren Event-Datensatz zu erstellen und Ihren Datensatz in den Amazon S3-Bucket hochgeladen.

- Erstellt [VariablenEntität](#), und [Bezeichnungen](#) Sie möchten, dass Amazon Fraud Detector für die Erstellung eines Betrugserkennungsmodells für dieses Ereignis verwendet. Stellen Sie sicher, dass die Variablen, der Entitätstyp und die Labels, die Sie erstellt haben, in Ihrem Event-Dataset enthalten sind.

Sie können Ihren Ereignistyp in der Amazon Fraud Detector-Konsole mithilfe der API, mithilfe des AWS CLI oder mithilfe des AWS SDK erstellen.

## Erstellen Sie den Ereignistyp in der Amazon Fraud Detector-Konsole

Um einen Ereignistyp zu erstellen,

1. Öffnen Sie die [AWSManagement Console](#) und melden Sie sich bei Ihrem Konto an. Navigieren Sie zu Amazon Fraud Detector.
2. Wählen Sie im linken Navigationsbereich Ereignisse aus.
3. Wählen Sie auf der Seite „Ereignistyp“ die Option Erstellen aus.
4. Unter Angaben zum Ereignistyp
  - a. Geben Sie im Feld Name den Namen Ihrer Veranstaltung ein.
  - b. Geben Sie in der Beschreibung optional eine Beschreibung ein.
  - c. Wählen Sie in der Entität den Entitätstyp aus, den Sie für Ihr Event erstellt haben.
5. Unter Eventvariablen
  - Im Feld Wählen Sie aus, wie die Variablen dieses Ereignisses definiert werden sollen,
    - Wenn Sie Ihre Eventvariablen für dieses Ereignis bereits erstellt haben, wählen Sie Variablen aus Ihrer Variablenliste auswählen und wählen Sie in den Variablen die Variablen aus, die Sie für dieses Ereignis erstellt haben.
    - Wenn Sie keine Variablen für dieses Ereignis erstellt haben, wählen Sie Variablen aus einem Trainingsdatensatz auswählen aus.
      - Wählen Sie in der IAM-Rolle die IAM-Rolle aus, die Amazon Fraud Detector für den Zugriff auf den Amazon S3-Bucket verwenden soll, der Ihren Datensatz enthält.
      - Geben Sie im Feld Datenposition den Pfad zu Ihrem Datensatzspeicherort ein. Verwenden Sie den S3 URI Pfad, der diesem ähnelt: `S3://your-bucket-name/example dataset filename.csv`.
      - Klicken Sie auf Upload.



- Unter Variablen werden alle Namen der Eventvariablen angezeigt, die Amazon Fraud Detector aus Ihrer Datensatzdatei extrahiert hat.

Wenn Sie möchten, dass die Variable zur Betrugserkennung aufgenommen wird, wählen Sie unter Variablentyp den Variablentyp aus. Wählen Sie Entfernen, um die Variablen aus der Betrugserkennung zu entfernen. Wiederholen Sie diesen Schritt für jede Variable in der Liste.

6. Wählen Sie unter Labels (optional) in den Labels die Labels aus, die Sie für dieses Event erstellt haben. Achten Sie darauf, jeweils ein Etikett für betrügerische und legitime Ereignisse auszuwählen.
7. Wenn Sie die automatische Downstream-Verarbeitung für dieses Ereignis einrichten möchten, aktivieren Sie unter Eventorchestrierung mit Amazon EventBridge — optional die Option Eventorchestrierung mit Amazon aktivieren. EventBridge Weitere Informationen zur Eventorchestrierung finden Sie unter [Ereignisorchestrierung](#).

#### Note

Sie können die Event-Orchestrierung auch später aktivieren, nachdem Sie Ihren Ereignistyp erstellt haben.

8. Wählen Sie Veranstaltungstyp erstellen aus.

## Erstellen Sie einen Ereignistyp mit dem AWS SDK for Python (Boto3)

Das folgende Beispiel zeigt eine Beispielanfrage für die PutEventType API. Im Beispiel wird davon ausgegangen, dass Sie die Variablen `ip_address` und `email_address`, die Labels `legit` und `fraud` den Entitätstyp erstellt `habensample_customer`. Hinweise zum Erstellen dieser Ressourcen finden Sie unter [Ressourcen](#).

#### Note

Sie müssen zuerst Variablen, Entitätstypen und Labels erstellen, bevor Sie sie dem Ereignistyp hinzufügen können.

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

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

## Löschen Sie ein Ereignis oder einen Ereignistyp

Wenn Sie ein Ereignis löschen, löscht Amazon Fraud Detector dieses Ereignis dauerhaft und die mit dem Ereignis verknüpften Daten werden nicht mehr in Amazon Fraud Detector gespeichert.

Um ein Ereignis zu löschen, das Amazon Fraud Detector über die **GetEventPrediction** API ausgewertet hat

1. Melden Sie sich bei der Amazon Fraud Detector-Konsole an AWS Management Console und öffnen Sie die Amazon Fraud Detector-Konsole unter <https://console.aws.amazon.com/frauddetector>.
2. Wählen Sie im linken Navigationsbereich der Konsole die Option Frühere Vorhersagen durchsuchen aus.
3. Wählen Sie das Ereignis aus, das Sie löschen möchten.
4. Wählen Sie Aktionen und dann Ereignis löschen aus.
5. Geben Sie **eindelete**, und wählen Sie dann Ereignis löschen.

### Note

Dadurch werden alle Datensätze gelöscht, die mit dieser Event-ID verknüpft sind, einschließlich aller an den Vorgang gesendeten Ereignisdaten und aller durch den `SendEvent` `GetEventPrediction` Vorgang generierten Prognosedaten.

Um ein Ereignis zu löschen, das in Amazon Fraud Detector gespeichert, aber nicht ausgewertet wurde (d. h., es wurde im Rahmen des `SendEvent` Vorgangs gespeichert), müssen Sie eine `DeleteEvent` Anfrage stellen und die Event-ID und die Ereignistyp-ID angeben. Wenn Sie sowohl das Ereignis als auch den mit dem Ereignis verknüpften Vorhersageverlauf löschen möchten, setzen Sie den Wert des `deleteAuditHistory` Parameters auf „true“. Wenn der `deleteAuditHistory`

Parameter auf „true“ gesetzt ist, sind die Ereignisdaten bis zu 30 Sekunden nach Abschluss des Löschvorgangs über die Suche verfügbar.

Um alle Ereignisse zu löschen, die einem Ereignistyp zugeordnet sind

1. Wählen Sie im linken Navigationsbereich der Konsole Ereignistypen
2. Wählen Sie den Ereignistyp, für den Sie alle Ereignisse löschen möchten.
3. Navigieren Sie zur Registerkarte „Gespeicherte Ereignisse“ und wählen Sie „Gespeicherte Ereignisse löschen“.

Abhängig von der Anzahl der gespeicherten Ereignisse für den Ereignistyp kann es einige Zeit dauern, bis alle gespeicherten Ereignisse gelöscht sind. Zum Beispiel dauert das Löschen eines 1-GB-Datensatzes (etwa 1—2 Millionen Ereignisse für den durchschnittlichen Kunden) etwa 2 Stunden. Während dieser Zeit werden neue Ereignisse dieses Ereignistyps, die Sie an Amazon Fraud Detector senden, nicht gespeichert, aber Sie können mithilfe des `GetEventPrediction` Vorgangs weiterhin Betrugsvorhersagen erstellen.

Um ein Ereignis zu löschen, geben Sie ein

Sie können keinen Ereignistyp löschen, der in einem Detektor oder einem Modell verwendet wird oder dem gespeicherte Ereignisse zugeordnet sind. Bevor Sie einen Ereignistyp löschen, müssen Sie alle Ereignisse löschen, die diesem Ereignistyp zugeordnet sind.

Wenn Sie einen Ereignistyp löschen, löscht Amazon Fraud Detector diesen Ereignistyp dauerhaft und die Daten werden nicht mehr in Amazon Fraud Detector gespeichert.

1. Wählen Sie im linken Navigationsbereich der Amazon Fraud Detector-Konsole Ressourcen und dann Ereignisse aus.
2. Wählen Sie den Ereignistyp aus, den Sie löschen möchten.
3. Wählen Sie Aktionen und dann Ereignistyp löschen aus.
4. Geben Sie den Namen des Ereignistyps ein und wählen Sie dann Ereignistyp löschen.

# Speicherung der Ereignisdaten

Nachdem Sie Ihren Datensatz erfasst haben, speichern Sie ihn intern mit Amazon Fraud Detector oder extern mit Amazon Simple Storage Service (Amazon S3) gespeichert. Wir empfehlen Ihnen, anhand des Modells, das Sie für die Generierung von Betrugsprognosen verwenden, auszuwählen, wo Ihr Datensatz gespeichert werden soll. Im Folgenden finden Sie eine detaillierte Aufschlüsselung dieser beiden Speicheroptionen.

- **Interner Speicher** — Ihr Datensatz wird bei Amazon Fraud Detector gespeichert. Alle mit einem Ereignis verknüpften Ereignisdaten werden zusammen gespeichert. Sie können den Ereignisdatensatz, der bei Amazon Fraud Detector gespeichert ist, jederzeit hochladen. Sie können Ereignisse entweder einzeln an eine Amazon Fraud Detector Detector-API streamen oder mithilfe der Batch-Importfunktion große Datensätze (bis zu 1 GB) importieren. Wenn Sie ein Modell mit dem in Amazon Fraud Detector gespeicherten Datensatz trainieren, können Sie einen Zeitraum angeben, um die Größe Ihres Datensatzes zu begrenzen.
- **Externer Speicher** — Ihr Datensatz wird in einer anderen externen Datenquelle als Amazon Fraud Detector gespeichert. Derzeit unterstützt Amazon Fraud Detector die Verwendung von Amazon Simple Storage Service (Amazon S3) zu diesem Zweck verwendet werden. Wenn sich Ihr Modell in einer Datei befindet, die auf Amazon S3 hochgeladen wurde, darf diese Datei nicht mehr als 5 GB unkomprimierter Daten enthalten. Wenn es mehr als das ist, stellen Sie sicher, dass Sie den Zeitraum Ihres Datensatzes verkürzen.

Die folgende Tabelle enthält Details zum Modelltyp und zur unterstützten Datenquelle.

Modelltyp	Kompatible Trainingsdatenquelle
Einblicke in Online-Betrug	Externer Speicher, Interner Speicher
Einblicke in Transaktionsbetrug	Interner Speicher
Einblicke in die Kontoübernahme	Interner Speicher

Informationen zum externen Speichern Ihres Datensatzes mit Amazon Simple Storage Service finden Sie unter [Speichern Sie Ihre Eventdaten extern mit Amazon S3](#) . Informationen zur internen Speicherung Ihres Datensatzes mit Amazon Fraud Detector finden Sie unter [Speichern Sie Ihre Eventdaten intern mit Amazon Fraud Detector](#) .

# Speichern Sie Ihre Eventdaten extern mit Amazon S3

Wenn Sie ein Online Fraud Insights-Modell trainieren, können Sie sich dafür entscheiden, Ihre Eventdaten extern bei Amazon S3 zu speichern. Um Ihre Eventdaten in Amazon S3 zu speichern, müssen Sie zuerst eine Textdatei im CSV-Format erstellen, Ihre Eventdaten hinzufügen und dann die CSV-Datei in einen Amazon S3 S3-Bucket hochladen.

## Note

Die Modelltypen Transaction Fraud Insights und Account Takeover Insights unterstützen keine extern mit Amazon S3 gespeicherten Datensätze.

## Erstellen einer CSV-Datei

Amazon Fraud Detector verlangt, dass die erste Zeile Ihrer CSV-Datei Spaltenüberschriften enthält. Die Spaltenüberschriften in Ihrer CSV-Datei müssen den Variablen zugeordnet werden, die im Ereignistyp definiert sind. Ein Beispiel für einen Datensatz finden Sie unter [Beispieldatensatz abrufen und hochladen](#)

Das Online Fraud Insights-Modell erfordert einen Trainingsdatensatz, der mindestens 2 Variablen und bis zu 100 Variablen enthält. Zusätzlich zu den Ereignisvariablen muss der Trainingsdatensatz die folgenden Header enthalten:

- EVENT\_TIMESTAMP - Definiert, wann das Ereignis aufgetreten ist
- Das Ereignis wird als betrügerisch oder legitim eingestuft. Die Werte in der Spalte müssen den im Ereignistyp definierten Werten entsprechen.

Die folgenden CSV-Beispieldaten stellen historische Registrierungsereignisse eines Online-Händlers dar:

```
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**

Die CSV-Datendatei kann doppelte Anführungszeichen und Kommas als Teil Ihrer Daten enthalten.

Eine vereinfachte Version des entsprechenden Ereignistyps ist unten dargestellt. Die Ereignisvariablen entsprechen den Headern in der CSV-Datei und die darin enthaltenen WerteEVENT\_LABEL entsprechen den Werten in der Labelliste.

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

## Formate von Ereigniszeitstempeln

Stellen Sie sicher, dass Ihr Event-Zeitstempel das erforderliche Format hat. Im Rahmen des Modellerstellungsprozesses ordnet der Modelltyp Online Fraud Insights Ihre Daten anhand des Zeitstempels des Ereignisses und teilt Ihre Daten zu Schulungs- und Testzwecken auf. Um eine faire Leistungsschätzung zu erhalten, trainiert das Modell zunächst mit dem Trainingsdatensatz und testet dieses Modell dann am Testdatensatz.

Amazon Fraud Detector unterstützt die folgenden Datums-/Uhrzeitstempelformate für die WerteEVENT\_TIMESTAMP während des Modelltrainings:

- %yyyy-%mm-%dd%HH: %mm: %ssZ (ISO 8601-Standard in UTC nur ohne Millisekunden)

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

- %yyyy/%mm/%dd %hh: %mm: %ss (vormittag/nachmittags)

Beispiele: 30.11.2019 13:01:01 Uhr oder 30.11.2019 13:01:01

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

Beispiele: 30.11.2019 13:01:01 Uhr, 30.11.2019 13:01:01

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

Beispiele: 30.11.19 13:01:01 PM, 30.11.19 13:01:01

Amazon Fraud Detector geht beim Analysieren von Datums-/Zeitstempelformaten nach Ereigniszeitstempeln von folgenden Annahmen aus:

- Wenn Sie den ISO 8601-Standard verwenden, muss dieser exakt mit der vorherigen Spezifikation übereinstimmen.
- Wenn Sie eines der anderen Formate verwenden, gibt es zusätzliche Flexibilität:
  - Für Monate und Tage können Sie einstellige oder zweistellige Zahlen angeben. Beispielsweise ist der 12.01.2019 ein gültiges Datum.
  - Sie müssen hh:mm:ss nicht angeben, wenn Sie sie nicht haben (das heißt, Sie können einfach ein Datum angeben). Sie können auch nur eine Teilmenge von Stunde und Minuten angeben (z. B. hh:mm). Die bloße Angabe der Stunde wird nicht unterstützt. Millisekunden werden ebenfalls nicht unterstützt.
  - Wenn Sie AM/PM-Etiketten angeben, wird von einer 12-Stunden-Uhr ausgegangen. Wenn keine AM/PM-Informationen vorliegen, wird von einer 24-Stunden-Uhr ausgegangen.
  - Sie können „/“ oder „-“ als Trennzeichen für die Datumselemente verwenden. „:“ wird für die Zeitstempелеlemente vorausgesetzt.

## Sampling Ihres Datensatzes im Zeitverlauf

Wir empfehlen Ihnen, Betrugsbeispiele und legitime Beispiele aus demselben Zeitraum anzugeben. Wenn Sie beispielsweise Betrugsfälle aus den letzten 6 Monaten angeben, sollten Sie auch legitime Ereignisse angeben, die sich gleichmäßig über denselben Zeitraum erstrecken. Wenn Ihr Datensatz eine sehr ungleichmäßige Verteilung von Betrug und legitimen Ereignissen enthält, erhalten Sie möglicherweise die folgende Fehlermeldung: „Die Betrugsverteilung über die Zeit ist inakzeptabel schwankend. Datensatz kann nicht richtig aufgeteilt werden.“ In der Regel lässt sich dieser Fehler am einfachsten beheben, indem sichergestellt wird, dass die Betrugsereignisse und die legitimen Ereignisse im gleichen Zeitraum gleichmäßig erfasst werden. Möglicherweise müssen Sie auch Daten entfernen, wenn Sie innerhalb eines kurzen Zeitraums einen starken Anstieg der Betrugsfälle erlebt haben.

Wenn Sie nicht genügend Daten generieren können, um einen gleichmäßig verteilten Datensatz zu erstellen, besteht ein Ansatz darin, den EVENT\_TIMESTAMP Ihrer Ereignisse nach dem Zufallsprinzip zu ordnen, sodass sie gleichmäßig verteilt sind. Dies führt jedoch häufig dazu, dass Leistungskennzahlen unrealistisch sind, da Amazon Fraud Detector EVENT\_TIMESTAMP verwendet, um Modelle für die entsprechende Teilmenge von Ereignissen in Ihrem Datensatz auszuwerten.

## Null und fehlende Werte

Amazon Fraud Detector verarbeitet Nullwerte und fehlende Werte. Der Prozentsatz der Nullen für Variablen sollte jedoch begrenzt sein. Die Spalten `EVENT_TIMESTAMP` und `EVENT_LABEL` sollten keine fehlenden Werte enthalten.

## Dateiüberprüfung

Amazon Fraud Detector kann ein Modell nicht trainieren, wenn eine der folgenden Bedingungen aufgetreten ist:

- Wenn die CSV nicht analysiert werden kann
- Wenn der Datentyp für eine Spalte falsch ist

## Laden Sie Ihre Ereignisdaten in einen Amazon S3 Bucket hoch

Nachdem Sie eine CSV-Datei mit Ihren Ereignisdaten erstellt haben, laden Sie die Datei in Ihren Amazon S3 Bucket hoch, nachdem Sie eine CSV-Datei mit Ihren Ereignisdaten erstellt haben.

Hochladen in einen Amazon S3 Bucket hoch

1. Melden Sie sich bei der AWS Management Console an und öffnen Sie die Amazon S3-Konsole unter <https://console.aws.amazon.com/s3/>.
2. Wählen Sie Create Bucket (Bucket erstellen) aus.

Der Assistent Create Bucket (Bucket erstellen) wird geöffnet.

3. Geben Sie unter Bucket name (Bucket-Name) einen DNS-kompatiblen Namen für Ihren Bucket ein.

Der Bucket-Name muss ...:

- überall in Amazon S3 eindeutig sein.
- zwischen 3 und 63 Zeichen lang sein,
- Enthält keine Großbuchstaben.
- mit einem Kleinbuchstaben oder einer Zahl beginnen.





maschinellen Lernens zu schließen. Ereignisse werden auf der Ressourcenebene des Ereignistyps gespeichert, sodass alle Ereignisse desselben Ereignistyps zusammen in einem einzigen Ereignistypdatensatz gespeichert werden. Im Rahmen der Definition eines Ereignistyps können Sie optional angeben, ob Ereignisse für diesen Ereignistyp gespeichert werden sollen, indem Sie in der Amazon Fraud Detector Detector-Konsole die Einstellung Event Ingestion aktivieren.

Sie können entweder einzelne Ereignisse speichern oder eine große Anzahl von Ereignisdatensätzen in Amazon Fraud Detector importieren. Einzelne Ereignisse können über die [GetEventPredictionAPI](#) oder die [SendEventAPI](#) gestreamt werden. Große Datensätze können mithilfe der Batch-Importfunktion in der Amazon Fraud Detector-Konsole oder mithilfe der [CreateBatchImportJobAPI](#) schnell und einfach in Amazon Fraud Detector importiert werden.

Sie können die Amazon Fraud Detector Detector-Konsole jederzeit verwenden, um die Anzahl der bereits gespeicherten Ereignisse für jeden Ereignistyp zu überprüfen.

## Bereiten Sie die Ereignisdaten für die Speicherung vor

Ereignisdaten, die intern mit Amazon Fraud Detector gespeichert werden, werden auf `Event Type` Ressourcenebene gespeichert. Alle Ereignisdaten, die von demselben Ereignis stammen, werden also in einer einzigen Datei gespeichert `Event Type`. Die gespeicherten Ereignisse können später verwendet werden, um ein neues Modell zu trainieren oder ein vorhandenes Modell erneut zu trainieren. Wenn Sie ein Modell mit den gespeicherten Ereignisdaten trainieren, können Sie optional einen Zeitbereich von Ereignissen angeben, um die Größe Ihres Trainingsdatensatzes zu begrenzen.

Jedes Mal, wenn Sie Ihre Daten in Amazon Fraud Detector speichern, indem Sie die Amazon Fraud Detector-Konsole, die `SendEvent API` oder die `CreateBatchImportJob API` verwenden, validiert Amazon Fraud Detector Ihre Daten vor dem Speichern. Wenn Ihre Daten nicht validiert werden, werden die Ereignisdaten nicht gespeichert.

### Voraussetzungen für die interne Speicherung von Daten mit Amazon Fraud Detector

- Um sicherzustellen, dass Ihre Ereignisdaten die Validierung bestehen und der Datensatz erfolgreich gespeichert wird, stellen Sie sicher, dass Sie die vom [Data Model Explorer](#) bereitgestellten Erkenntnisse zur Vorbereitung Ihres Datensatzes verwendet haben.
- Hat einen Ereignistyp für die Ereignisdaten erstellt, die Sie mit Amazon Fraud Detector speichern möchten. Wenn nicht, folgen Sie den Anweisungen zum [Erstellen eines Ereignistyps](#).

## Intelligente Datenvalidierung

Wenn Sie Ihren Datensatz für den Batch-Import in die Amazon Fraud Detector-Konsole hochladen, verwendet Amazon Fraud Detector Smart Data Validation (SDV), um Ihren Datensatz zu validieren, bevor Sie Ihre Daten importieren. SDV scannt die hochgeladene Datendatei und identifiziert Probleme wie fehlende Daten und falsche Formate oder Datentypen. Neben der Validierung Ihres Datensatzes stellt SDV auch einen Validierungsbericht bereit, der alle identifizierten Probleme auflistet und Maßnahmen zur Behebung der wichtigsten Probleme vorschlägt. Einige der von SDV identifizierten Probleme können kritisch sein und müssen behoben werden, bevor Amazon Fraud Detector Ihren Datensatz erfolgreich importieren kann. Weitere Informationen finden Sie unter [Bericht zur intelligenten Datenvalidierung](#).

Die SDV validiert Ihren Datensatz auf Dateiebene und auf Datenebene (Zeilen). Auf Dateiebene scannt SDV Ihre Datendatei und identifiziert Probleme wie unzureichende Zugriffsrechte auf die Datei, falsche Dateigröße, falsches Dateiformat und Header (Ereignismetadaten und Ereignisvariablen). Auf Datenebene scannt SDV alle Ereignisdaten (Zeile) und identifiziert Probleme wie falsches Datenformat, Datenlänge, Zeitstempelformat und Nullwerte.

Smart Data Validation ist derzeit nur in der Amazon Fraud Detector-Konsole verfügbar und die Validierung ist standardmäßig aktiviert. Wenn Sie nicht möchten, dass Amazon Fraud Detector die Smart Data Validation vor dem Import Ihres Datensatzes verwendet, deaktivieren Sie die Überprüfung in der Amazon Fraud Detector-Konsole, wenn Sie Ihren Datensatz hochladen.

### Validierung gespeicherter Daten bei Verwendung von APIs oder AWS SDK

Beim Hochladen von Ereignissen über den `CreateBatchImportJob` API-Vorgang `SendEvent` `GetEventPrediction`, oder überprüft Amazon Fraud Detector Folgendes:

- Die EventIngestion-Einstellung für diesen Ereignistyp ist `ENABLED`.
- Ereigniszeitstempel können nicht aktualisiert werden. Ein Ereignis mit einer wiederholten Ereignis-ID und einem anderen `EVENT_TIMESTAMP` wird als Fehler behandelt.
- Variablennamen und Werte entsprechen ihrem erwarteten Format. Weitere Informationen finden Sie unter [Erstellen Sie eine Variable](#)
- Erforderliche Variablen werden mit einem Wert gefüllt.
- Alle Zeitstempel für Ereignisse sind nicht älter als 18 Monate und liegen nicht in der future.

## Speichern von Eventdaten per Batch-Import

Mit der Batch-Importfunktion können Sie mithilfe der Konsole, der API oder des AWS-SDK schnell und einfach große historische Ereignisdatensätze in Amazon Fraud Detector hochladen. Um den Batch-Import zu verwenden, erstellen Sie eine Eingabedatei im CSV-Format, die all Ihre Eventdaten enthält, laden Sie die CSV-Datei in den Amazon S3 S3-Bucket hoch und starten Sie einen Importjob. Amazon Fraud Detector validiert die Daten zunächst anhand des Ereignistyps und importiert dann automatisch den gesamten Datensatz. Nachdem die Daten importiert wurden, können sie für das Training neuer Modelle oder für das erneute Training vorhandener Modelle verwendet werden.

### Eingabe- und Ausgabedateien

Die CSV-Eingabedatei muss Header enthalten, die den im zugehörigen Ereignistyp definierten Variablen entsprechen, sowie vier obligatorische Variablen. Weitere Informationen finden Sie unter [Bereiten Sie die Ereignisdaten für die Speicherung vor](#). Die maximale Größe der Eingabedatendatei beträgt 20 Gigabyte (GB) oder etwa 50 Millionen Ereignisse. Die Anzahl der Veranstaltungen hängt von Ihrer Veranstaltungsgröße ab. Wenn der Importjob erfolgreich war, ist die Ausgabedatei leer. Wenn der Import nicht erfolgreich war, enthält die Ausgabedatei die Fehlerprotokolle.

### Erstellen einer CSV-Datei

Amazon Fraud Detector importiert nur Daten aus Dateien im komma-separierten Werte- (CSV) -Format vorliegen. Die erste Zeile Ihrer CSV-Datei muss Spaltenüberschriften enthalten, die exakt den im zugehörigen Ereignistyp definierten Variablen entsprechen, sowie vier obligatorische Variablen: `EVENT_ID`, `EVENT_TIMESTAMP`, `ENTITY_ID` und `ENTITY_TYPE`. Sie können optional auch `EVENT_LABEL` und `LABEL_TIMESTAMP` angeben (`LABEL_TIMESTAMP` ist erforderlich, wenn `EVENT_LABEL` enthalten ist).

### Definieren Sie obligatorische Variablen

Obligatorische Variablen werden als Ereignismetadaten betrachtet und müssen in Großbuchstaben angegeben werden. Ereignismetadaten werden automatisch für das Modelltraining hinzugefügt. In der folgenden Tabelle sind die obligatorischen Variablen, die Beschreibung der einzelnen Variablen und das erforderliche Format für die Variable aufgeführt.

Name	Beschreibung	Voraussetzungen
<code>EVENT_ID</code>	Eine Kennung für das Ereignis. Wenn es sich bei	<ul style="list-style-type: none"> <li>Die <code>EVENT_ID</code> ist für Batch-Importaufträge erforderlich.</li> </ul>

Name	Beschreibung	Voraussetzungen
	<p>Ihrer Veranstaltung beispielsweise um eine Online-Transaktion handelt, kann die EVENT_ID die Transaktionsreferenznummer sein, die Ihrem Kunden zur Verfügung gestellt wurde.</p>	<ul style="list-style-type: none"><li>• Dieser Wert muss für diese Veranstaltung eindeutig sein.</li><li>• Es sollte Informationen enthalten, die für Ihr Unternehmen von Bedeutung sind.</li><li>• Dieser Wert muss das Muster für reguläre Ausdrücke erfüllen (z. B. <code>^[0-9a-z_-]+\$</code>.)</li><li>• Es wird nicht empfohlen, einen Zeitstempel an die EVENT_ID anzuhängen. Dies kann zu Problemen führen, wenn Sie das Ereignis aktualisieren. Dies liegt daran, dass Sie in diesem Fall genau dieselbe EVENT_ID angeben müssen.</li></ul>

Name	Beschreibung	Voraussetzungen
ZEITSTEMPEL DES EREIGNISSES	Der Zeitstempel, zu dem das Ereignis aufgetreten ist. Der Zeitstempel muss im ISO-8601-Standard in UTC angegeben werden.	<ul style="list-style-type: none"> <li>• Der EVENT_TIMESTAMP ist für Batch-Importaufträge erforderlich.</li> <li>• Dieser Wert muss in einem der folgenden Formate angegeben werden: <ul style="list-style-type: none"> <li>• %yyyy-%mm-%ddt%HH: %mm: %ssZ (ISO 8601-Standard in UTC nur ohne Millisekunden)</li> </ul> <p>Beispiel: 2019-11-30T 13:01:01 Z</p> <li>• %yyyy/%mm/%dd %hh: %mm: %ss (vormittag/ nachmittags)</li> <p>Beispiele: 30.11.2019 9 13:01:01 Uhr oder 30.11.2019 13:01:01</p> <li>• %mm/%dd/%yyyy %hh: %mm: %ss</li> <p>Beispiele: 30.11.2019 13:01:01 Uhr, 30.11.2019 13:01:01</p> <li>• %mm/%dd/%yy %hh: %mm: %ss</li> <p>Beispiele: 30.11.19 13:01:01 PM, 30.11.19 13:01:01</p> <li>• Amazon Fraud Detector geht beim Analysieren von Datums-/Zeitstempeln</li> </li></ul>

Name	Beschreibung	Voraussetzungen
		<p>lformaten nach Ereignisz eitstempeln von folgenden Annahmen aus:</p> <ul style="list-style-type: none"><li>• Wenn Sie den ISO 8601- Standard verwenden, muss dieser exakt mit der vorherigen Spezifikation übereinstimmen.</li><li>• Wenn Sie eines der anderen Formate verwenden, gibt es zusätzliche Flexibilität:<ul style="list-style-type: none"><li>• Für Monate und Tage können Sie einstell ige oder zweistellige Zahlen angeben. Beispielsweise ist der 12.01.2019 ein gültiges Datum.</li><li>• Sie müssen hh:mm:ss nicht angeben, wenn Sie sie nicht haben (das heißt, Sie können einfach ein Datum angeben). Sie können auch nur eine Teilmenge von Stunde und Minuten angeben (z. B. hh:mm). Die bloße Angabe der Stunde wird nicht unterstützt. Milliseku nden werden ebenfalls nicht unterstützt.</li></ul></li></ul>

Name	Beschreibung	Voraussetzungen
		<ul style="list-style-type: none"> <li>• Wenn Sie AM/PM-Etiketten angeben, wird von einer 12-Stunden-Uhr ausgegangen. Wenn keine AM/PM-Informationen vorliegen, wird von einer 24-Stunden-Uhr ausgegangen.</li> <li>• Sie können „/“ oder „-“ als Trennzeichen für die Datumselemente verwenden. „:“ wird für die Zeitstempелеlemente vorausgesetzt.</li> </ul>
ENTITY_ID	Eine Kennung für die Entität, das das Ereignis ausführt.	<ul style="list-style-type: none"> <li>• ENTITY_ID ist für Batch-Importaufträge erforderlich</li> <li>• Es muss dem regulären Ausdrucksmuster folgen: <code>^[0-9A-Za-z_@+-]+\$</code>.</li> <li>• Wenn die Entitäts-ID zum Zeitpunkt der Auswertung nicht verfügbar ist, geben Sie die Entitäts-ID als unbekannt an.</li> </ul>
ENTITÄTSTYP	Die Entität, die die Veranstaltung durchführt, z. B. ein Händler oder ein Kunde	ENTITY_TYPE ist für Batch-Importaufträge erforderlich



Name	Beschreibung	Voraussetzungen
BEZEICHNUNG DES EREIGNISSES	Klassifiziert das Ereignis als <code>fraudulent</code> oder <code>legitimate</code>	<code>EVENT_LABEL</code> ist erforderlich, wenn <code>LABEL_TIMESTAMP</code> enthalten ist
LABEL_TIMESTAMP	Der Zeitstempel, zu dem das Event-Label zuletzt gefüllt oder aktualisiert wurde	<ul style="list-style-type: none"><li>• <code>LABEL_TIMESTAMP</code> ist erforderlich, wenn <code>EVENT_LABEL</code> enthalten ist.</li><li>• Dieser Wert muss dem Zeitstempelformat entsprechen.</li></ul>

## Hochladen der CSV-Datei in Amazon S3 hoch, um den Batch-Import hoch

Laden Sie die Datei hoch, nachdem Sie eine CSV-Datei mit Ihren Daten erstellt haben, laden Sie die Datei in Ihren Amazon-S3-Bucket hoch, nachdem Sie eine CSV-Datei mit Ihren Daten erstellt haben.

### Hochladen von Ereignisdaten in einen Amazon S3 Bucket hochgeladen

1. Melden Sie sich bei der AWS Management Console an und öffnen Sie die Amazon S3-Konsole unter <https://console.aws.amazon.com/s3/>.
2. Wählen Sie `Create Bucket` (`Bucket erstellen`) aus.

Der Assistent `Create Bucket` (`Bucket erstellen`) wird geöffnet.

3. Geben Sie unter `Bucket name` (`Bucket-Name`) einen DNS-kompatiblen Namen für Ihren Bucket ein.

Der Bucket-Name muss ...:

- überall in Amazon S3 eindeutig sein.
- zwischen 3 und 63 Zeichen lang sein,
- Enthält keine Großbuchstaben.
- mit einem Kleinbuchstaben oder einer Zahl beginnen.

Der Name eines einmal erstellter Buckets kann nicht nachträglich geändert werden. Weitere Informationen zum Benennen von Buckets finden Sie unter [Bucket-Benennungsregeln](#) im Benutzerhandbuch zu Amazon Simple Storage Service.

**⚠ Important**

Vermeiden Sie, vertrauliche Informationen, wie Kontonummern, in den Bucket-Namen einzubeziehen. Der Bucket-Name wird in der URL angezeigt, die auf die Objekte im Bucket verweist.

4. Unter Region wählen Sie die AWS-Region aus, in der sich der Bucket befinden soll. Sie müssen dieselbe Region, Asien-Pazifik (Singapur) oder Asien-Pazifik (Sydney), USA Ost (Ohio), USA West (Oregon), USA West (Oregon), USA West (Oregon), Europa (Irland), Asien-Pazifik (Singapur) oder Asien-Pazifik (Sydney).
5. Wählen Sie unter Bucket settings for Block Public Access (Bucket-Einstellungen für den öffentlichen Zugriff) die Einstellungen für den öffentlichen Zugriff aus, die Sie auf den Bucket anwenden möchten.

Sie sollten alle Einstellungen aktiviert lassen. Weitere Informationen zum Verwenden des öffentlichen des öffentlichen des öffentlichen des öffentlichen des öffentlichen des öffentlichen des öffentlichen des öffentlichen des [öffentlichen](#) des öffentlichen öffentlichen des öffentlichen des öffentlichen des öffentlichen des öffentlichen des öffentlichen des öffentlichen des öffentlichen des öffentlichen des öffentlichen des öffentlichen des öffentlichen des öffentlichen des öffentlichen des öffentlichen

6. Wählen Sie Create Bucket (Bucket erstellen) aus.
7. Laden Sie die Trainingsdatendatei in Ihren Amazon S3 Bucket hoch. Notieren Sie sich den Amazon S3 S3-Speicherpfad für Ihre Trainingsdatei (z. B. s3://bucketname/object.csv).

## Batch-Import von Ereignisdaten in die Amazon Fraud Detector Detector-Konsole

Sie können ganz einfach eine große Anzahl Ihrer Event-Datensätze in die Amazon Fraud Detector Detector-Konsole importieren, indem Sie die `CreateBatchImportJob` API oder das AWS SDK verwenden. Bevor Sie fortfahren, stellen Sie sicher, dass Sie die Anweisungen zur Vorbereitung Ihres Datensatzes als CSV-Datei befolgt haben. Stellen Sie sicher, dass Sie die CSV-Datei auch in einen Amazon S3 Bucket hochgeladen haben.

## Verwenden der Amazon Fraud Detector Detector-Konsole

So importieren Sie Ereignisdaten stapelweise in die Konsole

1. Öffnen Sie die AWS-Konsole, melden Sie sich bei Ihrem Konto an und navigieren Sie zu Amazon Fraud Detector.
2. Wählen Sie im linken Navigationsbereich Ereignisse die Option Ereignisse aus.
3. Wählen Sie Ihren Ereignistyp aus.
4. Wählen Sie den Tab Gespeicherte Ereignisse aus.
5. Vergewissern Sie sich im Detailbereich Gespeicherte Ereignisse, dass die Ereigniserfassung aktiviert ist.
6. Wählen Sie im Bereich Ereignisdaten importieren die Option Neuer Import aus.
7. Geben Sie auf der Importseite für neue Ereignisse die folgenden Informationen an:
  - [Empfohlen] Belassen Sie die neue Einstellung Enable Smart Data Validation für diesen Datensatz auf die Standardeinstellung.
  - Wählen Sie als IAM-Rolle für Daten die IAM-Rolle aus, die Sie für den Amazon S3 S3-Bucket erstellt haben, der die CSV-Datei enthält, die Sie importieren möchten.
  - Geben Sie unter Speicherort für Eingabedaten den S3-Speicherort ein, an dem Sie Ihre CSV-Datei haben.
  - Wenn Sie einen separaten Speicherort für Ihre Importergebnisse angeben möchten, klicken Sie auf Separater Datenspeicherort für Eingaben und Ergebnisse und geben Sie einen gültigen Amazon S3 S3-Bucket-Standort an.

### Important

Stellen Sie sicher, dass die von Ihnen ausgewählte IAM-Rolle über Leseberechtigungen für Ihren Amazon S3 S3-Eingabe-Bucket und Schreibrechte für Ihren Amazon S3 S3-Ausgabe-Bucket verfügt.

8. Wählen Sie Starten.
9. In der Spalte Status im Datenbereich „Ereignisse importieren“ wird der Status Ihres Validierungs- und Importauftrags angezeigt. Das Banner oben bietet eine allgemeine Beschreibung des Status, während Ihr Datensatz zuerst validiert und dann importiert wird.

## 10. Folgen Sie den Anweisungen unter [Überwachen des Fortschritts der Datensatzvalidierung und des Auftrags](#).

### Überwachen des Fortschritts der Datensatzvalidierung und des Auftrags

Wenn Sie die Amazon Fraud Detector-Konsole verwenden, um einen Batch-Importauftrag auszuführen, validiert Amazon Fraud Detector Ihren Datensatz standardmäßig vor dem Import. Sie können den Fortschritt und den Status von Validierungs- und Importaufträgen auf der Seite „Neue Ereignisse importieren“ der Amazon Fraud Detector-Konsole überwachen. Ein Banner oben auf der Seite enthält eine kurze Beschreibung der Validierungsergebnisse und den Status des Auftrags. Abhängig von den Validierungsergebnissen und dem Status Ihres Importauftrags müssen Sie möglicherweise Maßnahmen ergreifen, um eine erfolgreiche Validierung und einen erfolgreichen Import Ihres Datensatzes sicherzustellen.

Die folgende Tabelle enthält Einzelheiten zu den Aktionen, die Sie je nach Ergebnis der Validierungs- und Importvorgänge ergreifen müssen.

Banner-Nachricht	Status	Bedeutung	Was soll ich tun
Die Datenvalidierung hat begonnen	Validierung in Arbeit	SDV hat mit der Validierung Ihres Datensatzes begonnen	Warten Sie, bis sich der Status ändert
Die Datenüberprüfung kann aufgrund von Fehlern in Ihrem Datensatz nicht fortgesetzt werden. Korrigieren Sie Fehler in Ihrer Datendatei und starten Sie einen neuen Importjob. Weitere Informati	Validierung ist fehlgeschlagen	SDV hat Probleme in Ihrer Datendatei identifiziert. Diese Probleme müssen für einen erfolgreichen Import Ihres Datensatz	Wählen Sie im Bereich Ereignisdaten importieren die Job-ID aus und sehen Sie sich den Validierungsbericht an. Folgen Sie den Empfehlungen im Bericht, um alle aufgelisteten Fehler zu beheben. Weitere Informationen finden Sie unter <a href="#">Verwendung des Validierungsberichts</a> .

Banner-Nachricht	Status	Bedeutung	Was soll ich tun
onen finden Sie im Validierungsbericht		es behoben werden.	
Der Datenimport wurde gestartet . Erfolgreich abgeschlossene Validierung	Import in Arbeit	Ihr Datensatz hat die Validierung bestanden . AFD hat mit dem Import Ihres Datensatzes begonnen	Warten Sie, bis sich der Status ändert
Die Validierung wurde mit Warnungen abgeschlossen. Der Datenimport hat begonnen	Import in Arbeit	Bei einigen Daten in Ihrem Datensatz ist die Überprüfung fehlgeschlagen. Die Daten, die die Validierung bestanden haben, erfüllen jedoch die Mindestanforderungen an die Datengröße für den Import.	Überwachen Sie die Nachricht im Banner und warten Sie, bis sich der Status ändert

Banner-Nachricht	Status	Bedeutung	Was soll ich tun
Ihre Daten wurden teilweise importiert. Einige der Daten konnten nicht überprüft werden und wurden nicht importiert. Weitere Informationen finden Sie im Validierungsbericht.	Importiert. Der Status zeigt ein Warnsymbol.	Einige der Daten in Ihrer Datendatei, deren Überprüfung fehlgeschlagen ist, wurden nicht importiert. Der Rest der Daten, die die Validierung bestanden haben, wurde importiert.	Wählen Sie im Bereich Ereignisdaten importieren die Job-ID aus und sehen Sie sich den Validierungsbericht an. Folgen Sie den Empfehlungen in der Tabelle mit Warnungen auf Datenebene, um die aufgelisteten Warnungen zu beheben. Sie müssen nicht auf alle Warnungen eingehen. Stellen Sie jedoch sicher, dass Ihr Datensatz mehr als 50% der Daten enthält, die die Validierung für einen erfolgreichen Import bestehen. Nachdem Sie die Warnungen behoben haben, starten Sie einen neuen Importjob. Weitere Informationen finden Sie unter <a href="#">Verwendung des Validierungsberichts</a> .
Der Datenimport ist aufgrund eines Verarbeitungsfehlers fehlgeschlagen. Starten Sie einen neuen Datenimportjob	Der Import ist fehlgeschlagen	Der Import ist aufgrund eines vorübergehenden Laufzeitfehlers fehlgeschlagen	Starte einen neuen Importjob

Banner-Nachricht	Status	Bedeutung	Was soll ich tun
Daten wurden erfolgreich importiert	Importiert	Sowohl die Validierung als auch der Import wurden erfolgreich abgeschlossen	Wählen Sie die Job-ID Ihres Importauftrags aus, um Details anzuzeigen, und fahren Sie dann mit dem Modelltraining fort

#### Note

Wir empfehlen, nach dem erfolgreichen Import des Datensatzes in Amazon Fraud Detector 10 Minuten zu warten, um sicherzustellen, dass er vollständig vom System erfasst wurde.

## Bericht zur intelligenten Datenvalidierung

Die Smart Data Validation erstellt nach Abschluss der Validierung einen Validierungsbericht. Der Validierungsbericht enthält Einzelheiten zu allen Problemen, die das SDV in Ihrem Datensatz identifiziert hat, sowie Handlungsempfehlungen zur Behebung der wichtigsten Probleme. Mithilfe des Validierungsberichts können Sie ermitteln, um welche Probleme es sich handelt, wo sich die Probleme im Datensatz befinden, wie schwerwiegend die Probleme sind und wie sie behoben werden können. Der Validierungsbericht wird auch dann erstellt, wenn die Validierung erfolgreich abgeschlossen wurde. In diesem Fall können Sie sich den Bericht ansehen, um zu sehen, ob Probleme aufgeführt sind, und falls ja, entscheiden, ob Sie eines dieser Probleme beheben möchten.

#### Note

Die aktuelle Version von SDV scannt Ihren Datensatz auf Probleme, die dazu führen könnten, dass der Batch-Import fehlschlägt. Wenn die Validierung und der Batch-Import erfolgreich sind, kann Ihr Datensatz immer noch Probleme aufweisen, die dazu führen können, dass das Modelltraining fehlschlägt. Wir empfehlen Ihnen, Ihren Validierungsbericht auch dann anzusehen, wenn die Validierung und der Import erfolgreich waren, und alle im Bericht

aufgeführten Probleme für ein erfolgreiches Modelltraining zu beheben. Nachdem Sie die Probleme behoben haben, erstellen Sie einen neuen Batch-Importjob.

## Zugriff auf den Validierungsbericht

Sie können nach Abschluss der Validierung jederzeit auf den Validierungsbericht zugreifen, indem Sie eine der folgenden Optionen verwenden:

1. Wählen Sie nach Abschluss der Validierung und während der Importaufgabe im oberen Banner die Option Validierungsbericht anzeigen aus.
2. Wählen Sie nach Abschluss des Importauftrags im Bereich Ereignisdaten importieren die Job-ID des gerade abgeschlossenen Importauftrags aus.

## Verwendung des Validierungsberichts

Die Seite mit dem Validierungsbericht Ihres Importauftrags enthält die Details dieses Importauftrags, eine Liste kritischer Fehler, falls welche gefunden wurden, eine Liste mit Warnungen zu bestimmten Ereignissen (Zeilen) in Ihrem Datensatz, falls gefunden, und eine kurze Zusammenfassung Ihres Datensatzes, die Informationen wie ungültige Werte und fehlende Werte für jede Variable enthält.

- Jobdetails importieren

Stellt die Details des Auftrags bereit. Wenn Ihr Importauftrag fehlgeschlagen ist oder Ihr Datensatz teilweise importiert wurde, wählen Sie Gehe zur Ergebnisdatei, um die Fehlerprotokolle der Ereignisse anzuzeigen, die nicht importiert werden konnten.

- Kritische Fehler

Enthält Einzelheiten zu den wichtigsten Problemen in Ihrem Datensatz, die von SDV identifiziert wurden. Alle in diesem Bereich aufgeführten Probleme sind kritisch und müssen behoben werden, bevor Sie mit dem Import fortfahren. Wenn Sie versuchen, Ihren Datensatz zu importieren, ohne die kritischen Probleme zu beheben, schlägt Ihr Importjob möglicherweise fehl.

Um die kritischen Probleme zu lösen, folgen Sie den Empfehlungen für jede Warnung. Nachdem Sie alle im Bereich Kritische Fehler aufgelisteten Probleme behoben haben, erstellen Sie einen neuen Batch-Importauftrag.

- Warnungen auf Datenebene



Stellt eine Zusammenfassung der Warnungen für bestimmte Ereignisse (Zeilen) in Ihrem Datensatz bereit. Wenn der Bereich mit Warnungen auf Datenebene gefüllt ist, sind einige Ereignisse in Ihrem Datensatz nicht validiert worden und wurden nicht importiert.

Für jede Warnung wird in der Spalte Beschreibung die Anzahl der Ereignisse angezeigt, bei denen das Problem aufgetreten ist. Und die Beispielergebnis-IDs enthalten eine unvollständige Liste von Beispielergebnis-IDs, die Sie als Ausgangspunkt verwenden können, um die restlichen Ereignisse zu finden, bei denen das Problem auftritt. Verwenden Sie die Empfehlung für die Warnung, um das Problem zu beheben. Verwenden Sie auch die Fehlerprotokolle aus Ihrer Ausgabedatei für zusätzliche Informationen zu dem Problem. Die Fehlerprotokolle werden für alle Ereignisse generiert, bei denen der Batch-Import fehlgeschlagen ist. Um auf Fehlerprotokolle zuzugreifen, wählen Sie im Bereich Auftragsdetails importieren die Option Gehe zur Ergebnisdatei aus.

#### Note

Wenn mehr als 50% der Ereignisse (Zeilen) in Ihrem Datensatz die Überprüfung nicht bestanden haben, schlägt auch der Importauftrag fehl. In diesem Fall müssen Sie die Daten korrigieren, bevor Sie einen neuen Importjob starten.

- Zusammenfassung des Datensatzes

Bietet eine Zusammenfassung des Validierungsberichts Ihres Datensatzes. Wenn in der Spalte Anzahl der Warnungen mehr als 0 Warnungen angezeigt werden, entscheiden Sie, ob Sie diese Warnungen korrigieren müssen. Wenn in der Spalte Anzahl der Warnungen Nullen angezeigt werden, fahren Sie mit dem Training Ihres Modells fort.

## Batch-Import von Ereignisdaten mit AWS SDK for Python (Boto3)

Das folgende Beispiel zeigt eine Beispielanforderung für eine [CreateBatchImportJob](#) API. Ein Batch-Importauftrag muss eine JobID, InputPath, OutputPath eventTypeName und enthalten iamRoleArn. Die JobID darf nicht dieselbe ID eines vergangenen Jobs enthalten, es sei denn, der Job hat den Status CREATE\_FAILED. Der InputPath und der OutputPath müssen gültige S3-Pfade sein. Sie können die Angabe des Dateinamens im OutputPath deaktivieren, müssen jedoch weiterhin einen gültigen S3-Bucket-Speicherort angeben. Das eventTypeName und iamRoleArn muss existieren. Die IAM-Rolle muss Leseberechtigungen für die Eingabe von Amazon S3 S3-Bucket und Schreibrechte für die Ausgabe von Amazon S3 S3-Bucket gewähren.

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

## Batch-Importauftrag abbrechen

Sie können einen laufenden Batch-Importauftrag jederzeit in der Amazon Fraud Detector Detector-Konsole über die `CancelBatchImportJob` API oder das AWS SDK stornieren.

Um einen Batch-Import-Job in der Konsole abzubrechen,

1. Öffnen Sie die AWS-Konsole, melden Sie sich bei Ihrem Konto an und navigieren Sie zu Amazon Fraud Detector.
2. Wählen Sie im linken Navigationsbereich Ereignisse die Option Ereignisse aus.
3. Wählen Sie Ihren Ereignistyp aus.
4. Wählen Sie den Tab Gespeicherte Ereignisse aus.
5. Wählen Sie im Bereich Ereignisdaten importieren die Auftrags-ID eines laufenden Importauftrags aus, den Sie stornieren möchten.
6. Klicken Sie auf der Event-Job-Seite auf Aktionen und wählen Sie Ereignisimport stornieren aus.
7. Wählen Sie Ereignisimport beenden, um den Batch-Importauftrag abzubrechen.

## Abbrechen des Batch-Auftrags mit AWS SDK for Python (Boto3)

Das folgende Beispiel zeigt eine Beispielanforderung für die `CancelBatchImportJob` API. Der Importauftrag zum Abbrechen muss die Job-ID eines laufenden Batch-Importauftrags enthalten.

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

```
    jobId = 'sample_batch'  
  )
```

## Speichern Sie Ereignisdaten mithilfe der GetEventPredictions API-Operation

Standardmäßig werden alle Ereignisse, die zur Auswertung an die `GetEventPrediction` API gesendet werden, in Amazon Fraud Detector gespeichert. Das bedeutet, dass Amazon Fraud Detector automatisch Ereignisdaten speichert, wenn Sie eine Vorhersage erstellen, und diese Daten verwendet, um berechnete Variablen nahezu in Echtzeit zu aktualisieren. Sie können die Datenspeicherung deaktivieren, indem Sie in der Amazon Fraud Detector Konsole zum Ereignistyp navigieren und die Ereigniserfassung auf OFF setzen oder den `EventIngestion` Wert mithilfe der `PutEventType` API-Operation auf `DISABLED` aktualisieren. Weitere Informationen zum `GetEventPrediction` API-Vorgang finden Sie unter [Fraud Preects](#).

### Important

Es wird dringend empfohlen, die Ereigniserfassung für einen Ereignistyp aktiviert zu lassen, sobald Sie sie aktiviert haben. Das Deaktivieren der Ereigniserfassung für denselben Ereignistyp und das anschließende Generieren von Vorhersagen kann zu inkonsistentem Verhalten führen.

## Speichern Sie Ereignisdaten mithilfe der SendEvent API-Operation

Sie können den `SendEvent` API-Vorgang verwenden, um Ereignisse in Amazon Fraud Detector zu speichern, ohne Betrugsvorhersagen für diese Ereignisse zu generieren. Sie können den `SendEvent` Vorgang beispielsweise verwenden, um einen historischen Datensatz hochzuladen, den Sie später zum Trainieren eines Modells verwenden können.

### Event-Timestamp-Formate für SendEvent API

Wenn Sie Ereignisdaten mithilfe der `SendEvent` API speichern, müssen Sie sicherstellen, dass Ihr Event-Zeitstempel das erforderliche Format hat. Amazon Fraud Detector unterstützt die folgenden Datums-/Uhrzeitstempelformate:

- `%yyyy-%mm-%ddt%HH: %mm: %ssZ` (ISO 8601-Standard in UTC nur ohne Millisekunden)

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

- %yyyy/%mm/%dd %hh: %mm: %ss (vormittag/nachmittags)

Beispiele: 30.11.2019 13:01:01 Uhr oder 30.11.2019 13:01:01

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

Beispiele: 30.11.2019 13:01:01 Uhr, 30.11.2019 13:01:01

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

Beispiele: 30.11.19 13:01:01 PM, 30.11.19 13:01:01

Amazon Fraud Detector geht beim Analysieren von Datums-/Zeitstempelformaten nach Ereigniszeitstempeln von folgenden Annahmen aus:

- Wenn Sie den ISO 8601-Standard verwenden, muss dieser exakt mit der vorherigen Spezifikation übereinstimmen.
- Wenn Sie eines der anderen Formate verwenden, gibt es zusätzliche Flexibilität:
  - Für Monate und Tage können Sie einstellige oder zweistellige Zahlen angeben. Beispielsweise ist der 12.01.2019 ein gültiges Datum.
  - Sie müssen hh:mm:ss nicht angeben, wenn Sie sie nicht haben (das heißt, Sie können einfach ein Datum angeben). Sie können auch nur eine Teilmenge von Stunde und Minuten angeben (z. B. hh:mm). Die bloße Angabe der Stunde wird nicht unterstützt. Millisekunden werden ebenfalls nicht unterstützt.
  - Wenn Sie AM/PM-Etiketten angeben, wird von einer 12-Stunden-Uhr ausgegangen. Wenn keine AM/PM-Informationen vorliegen, wird von einer 24-Stunden-Uhr ausgegangen.
  - Sie können „/“ oder „-“ als Trennzeichen für die Datumselemente verwenden. „:“ wird für die Zeitstempелеlemente vorausgesetzt.

Im Folgenden finden Sie ein Beispiel für einen `SendEvent` API-Aufruf.

```
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'}],
    )
```

## Details zu gespeicherten Ereignisdaten abrufen

Nachdem Sie Ereignisdaten in Amazon Fraud Detector gespeichert haben, können Sie mithilfe der [GetEvent](#)API die neuesten Daten überprüfen, die für ein Ereignis gespeichert wurden. Der folgende Beispielpcode überprüft die neuesten für das `sample_registration` Ereignis gespeicherten Daten.

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

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


## Metriken des gespeicherten Ereignisdatensatzes anzeigen

Für jeden Ereignistyp können Sie in der Amazon Fraud Detector Detector-Konsole Kennzahlen wie die Anzahl der gespeicherten Ereignisse, die Gesamtgröße Ihrer gespeicherten Ereignisse und die Zeitstempel der frühesten und letzten gespeicherten Ereignisse einsehen.

Um gespeicherte Ereignismetriken eines Ereignistyps anzuzeigen,

1. Öffnen Sie die AWS Konsole und melden Sie sich bei Ihrem Konto an. Navigieren Sie zu Amazon Fraud Detector
2. Wählen Sie im linken Navigationsbereich Ereignisse die Option Ereignisse aus.
3. Wählen Sie Ihren Ereignistyp aus.

4. Wählen Sie den Tab Gespeicherte Ereignisse aus.
5. Im Detailbereich „Gespeicherte Ereignisse“ werden die Metriken angezeigt. Diese Metriken werden automatisch einmal pro Tag aktualisiert.
6. Klicken Sie optional auf Event-Metriken aktualisieren, um Ihre Metriken manuell zu aktualisieren.

 Note

Wenn Sie Ihre Daten gerade importiert haben, empfehlen wir, 5 bis 10 Minuten zu warten, nachdem Sie den Datenimport abgeschlossen haben, um die Metriken zu aktualisieren und anzusehen.

# Ereignisorchestrierung

Die Ereignisorchestrierung erleichtert Ihnen das Senden von Ereignissen an AWS-Services für die nachgelagerte Verarbeitung mithilfe von [Amazon EventBridge](#). Amazon Fraud Detector bietet Ihnen einfache Regeln, mit denen Sie die Verarbeitung von Ereignissen nach der Betrugserkennung automatisieren können. Mit der Ereignisorchestrierung können Sie nachgelagerte Ereignisprozesse automatisieren, z. B. das Senden von Ereignissen an Dashboards, um Erkenntnisse aus Ereignisdaten zu erhalten, das Generieren von Benachrichtigungen auf der Grundlage der Ergebnisse der Betrugserkennung und das Aktualisieren von Ereignissen mit einer Bezeichnung, die auf dem Lernen aus der Betrugserkennung basiert.

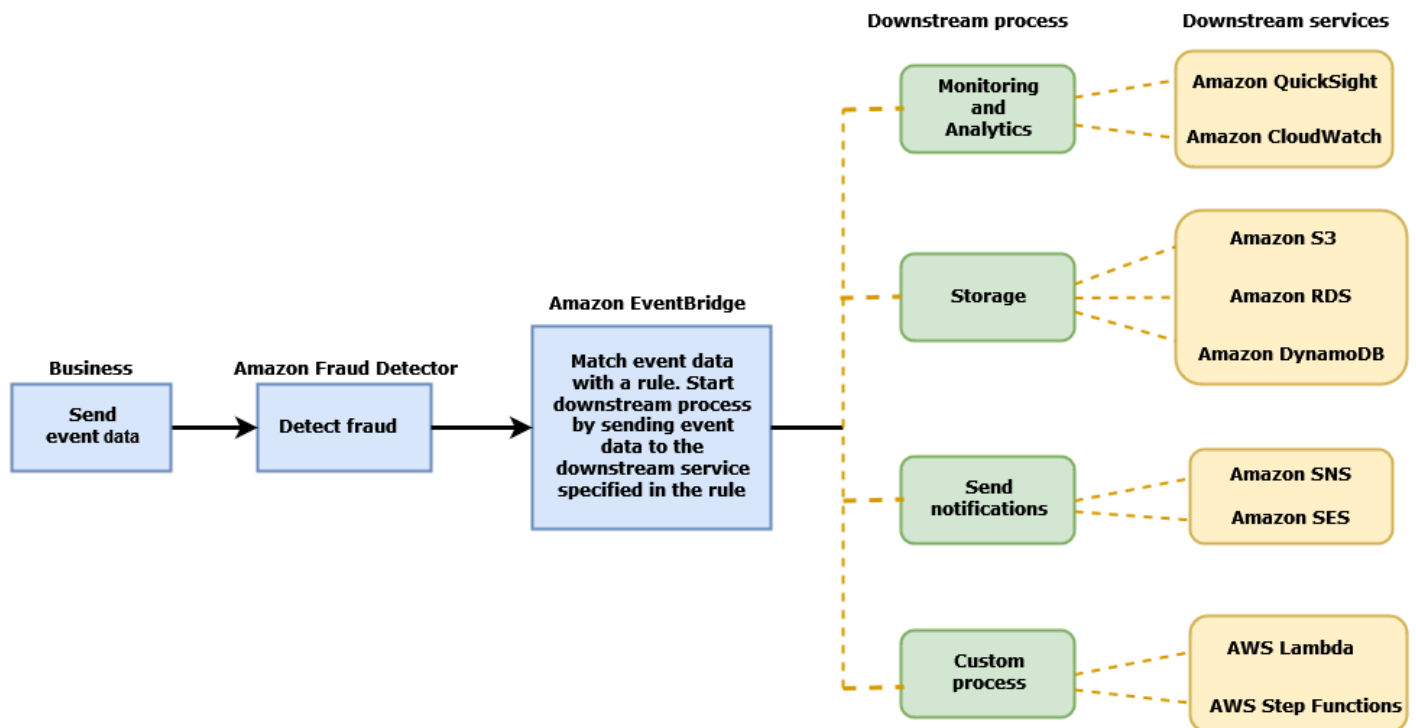
Die Ereignisorchestrierung bietet einfachen Zugriff auf Services in der AWS Umgebung über Amazon EventBridge. Sie können Amazon so konfigurieren EventBridge , dass Ereignisse entweder direkt an AWS-Services oder indirekt über [API-Ziele gesendet werden](#). Die , die AWS-Services Sie zur Orchestrierung Ihrer Downstream-Prozesse verwenden, werden auch als Ziele bezeichnet. Einige der Ziele, die Sie zur Orchestrierung der Downstream-Verarbeitung verwenden können, sind:

- Für Überwachung und Analytik – [Amazon QuickSight](#), [Amazon CloudWatch](#)
- Für die Speicherung – [Amazon S3](#), [Amazon RDS](#) ,[Amazon DynamoDB](#)
- Zum Senden von Benachrichtigungen – [Amazon SNS](#) , [Amazon SES](#)
- Für benutzerdefinierte Verarbeitung – [AWS Lambda](#) , [AWS Step Functions](#)

Weitere Informationen zu den von Amazon unterstützten Orchestrierungsziele finden Sie unter [Amazon- EventBridge Ziele](#) EventBridge.

Das folgende Diagramm bietet einen Überblick über die Funktionsweise der Ereignisorchestrierung.

## Event Orchestration



## Einrichten der Ereignisorchestrierung

Um die Ereignisorchestrierung für Ihre Ereignisse einzurichten, müssen Sie Prozesse in Ihrem Zielservice einrichten, Amazon EventBridge so konfigurieren, dass Ereignisdaten empfangen und gesendet werden, und Regeln in Amazon EventBridge erstellen, die die Bedingungen für den Start der nachgelagerten Prozesse angeben. Führen Sie die folgenden Schritte aus, um die Ereignisorchestrierung einzurichten:

So richten Sie die Ereignisorchestrierung ein

1. Gehen Sie zum [Amazon EventBridge -Benutzerhandbuch](#) und erfahren Sie, wie Sie Amazon EventBridge verwenden. Stellen Sie sicher, dass Sie lernen, wie Sie [Regeln](#) in Amazon EventBridge für Ihren Anwendungsfall erstellen.
2. Folgen Sie den Anweisungen zu [Aktivieren der Ereignisorchestrierung in Amazon Fraud Detector](#).

### Note

Die Ereignisorchestrierung für Ihr Ereignis ist standardmäßig deaktiviert.



3. Richten Sie Ihren Zielservice ein, um die Ereignisdaten zu empfangen und zu verarbeiten. Wenn Ihr Downstream-Prozess beispielsweise das Senden von Benachrichtigungen beinhaltet und Sie Amazon SNS verwenden möchten, gehen Sie zur Amazon SNS-Konsole, erstellen Sie ein SNS-Thema und abonnieren Sie dann einen Endpunkt für das Thema.
4. Folgen Sie den Anweisungen unter [Erstellen von Amazon- EventBridge Regeln](#).

#### Important

Stellen Sie beim Erstellen des Ereignismusters in Amazon sicher EventBridge, dass Sie `aws.frauddetector` für das Quellfeld und `Event Prediction Result Returned` für das Detailtypfeld angeben.

## Aktivieren der Ereignisorchestrierung in Amazon Fraud Detector

Sie können die Ereignisorchestrierung für ein Ereignis aktivieren, entweder beim Erstellen Ihres Ereignistyps oder nachdem Sie Ihren Ereignistyp erstellt haben. Die Ereignisorchestrierung kann in der Amazon-Fraud-Detector-Konsole, mit dem `-put-event-type` Befehl, mit der `PutEventType` API oder mit der `aktiviert werden` AWS SDK for Python (Boto3).

### Aktivieren der Ereignisorchestrierung in der Amazon Fraud Detector-Konsole

Dieses Beispiel ermöglicht die Ereignisorchestrierung für einen Ereignistyp, der bereits erstellt wurde. Wenn Sie einen neuen Ereignistyp erstellen und die Orchestrierung aktivieren möchten, folgen Sie den Anweisungen unter [Einen Ereignistyp erstellen](#).

So aktivieren Sie die Ereignisorchestrierung

1. Öffnen Sie die [AWS Managementkonsole](#) und melden Sie sich bei Ihrem -Konto an. Navigieren Sie zu Amazon Fraud Detector.
2. Wählen Sie im linken Navigationsbereich Ereignisse aus.
3. Wählen Sie auf der Seite Ereignistyp Ihren Ereignistyp aus.
4. Aktivieren Sie Ereignisorchestrierung mit Amazon aktivieren EventBridge.
5. Fahren Sie mit Schritt 3 für fort [Einrichten der Ereignisorchestrierung](#).

## Aktivieren der Ereignisorchestrierung mithilfe der AWS SDK for Python (Boto3)

Das folgende Beispiel zeigt eine Beispielanforderung zum Aktualisieren eines Ereignistypssample\_registration, um die Ereignisorchestrierung zu aktivieren. Das Beispiel verwendet die PutEventType-API und geht davon aus, dass Sie die Variablen ip\_address und email\_address, die Beschriftungen legit und und den Entitätstyp erstellt habensample\_customer. Informationen zum Erstellen dieser Ressourcen finden Sie unter [Ressourcen](#).

```
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'])
```

## Deaktivieren der Ereignisorchestrierung in Amazon Fraud Detector

Sie können die Ereignisorchestrierung für ein Ereignis jederzeit in der Amazon-Fraud-Detector-Konsole, mit dem -put-event-type-Befehl, über die PutEventType-API oder mithilfe der deaktivierenAWS SDK for Python (Boto3).

### Deaktivieren der Ereignisorchestrierung in der Amazon Fraud Detector-Konsole

So deaktivieren Sie die Ereignisorchestrierung

1. Öffnen Sie die [AWSManagementkonsole](#) und melden Sie sich bei Ihrem -Konto an. Navigieren Sie zu Amazon Fraud Detector.
2. Wählen Sie im linken Navigationsbereich Ereignisse aus.
3. Wählen Sie auf der Seite Ereignistyp Ihren Ereignistyp aus.
4. Deaktivieren Sie Ereignisorchestrierung mit Amazon aktivieren EventBridge.

## Deaktivieren der Ereignisorchestrierung mithilfe der AWS SDK for Python (Boto3)

Das folgende Beispiel zeigt eine Beispielanforderung zum Aktualisieren eines Ereignistyps `sample_registration` zum Deaktivieren der Ereignisorchestrierung mithilfe der `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'])
```

# Modell

Amazon Fraud Detector verwendet Machine-Learning-Modelle, um Betrugsprognosen zu erstellen. Jedes Modell wird mit einem Modelltyp trainiert. Der Modelltyp gibt die Algorithmen und Transformationen an, die zum Trainieren des Modells verwendet werden. Modelltraining ist der Prozess der Verwendung eines Datensatzes, den Sie bereitstellen, um ein Modell zu erstellen, das betrügerische Ereignisse vorhersagen kann.

Um ein Modell zu erstellen, müssen Sie zunächst einen Modelltyp auswählen und dann Daten vorbereiten und bereitstellen, die zum Trainieren des Modells verwendet werden.

## Wählen Sie einen Modelltyp

Die folgenden Modelltypen sind in Amazon Fraud Detector verfügbar. Wählen Sie einen Modelltyp aus, der für Ihren Anwendungsfall geeignet ist.

- Online-Betrugseinblicke

Der Modelltyp Online Fraud Insights ist optimiert, um Betrug zu erkennen, wenn nur wenige historische Daten über die ausgewertete Entität verfügbar sind, z. B. ein neuer Kunde, der sich online für ein neues Konto registriert.

- Transaktionsbetrugseinblicke

Der Modelltyp Transaction Fraud Insights eignet sich am besten für die Erkennung von Betrugsanwendungsfällen, in denen die ausgewertete Entität möglicherweise eine Geschichte der Interaktionen hat, die das Modell analysieren kann, um die Vorhersagegenauigkeit zu verbessern (z. B. ein vorhandener Kunde mit der Vergangenheit der Käufe).

- Einblicke in die Kontoübernahme

Der Modelltyp Account Takeover Insights erkennt, ob ein Konto durch Phishing oder eine andere Art von Angriff kompromittiert wurde. Die Anmeldedaten eines kompromittierten Kontos, wie Browser und Gerät, die bei der Anmeldung verwendet werden, unterscheiden sich von den historischen Anmeldedaten, die dem Konto zugeordnet sind.

## Einblicke in Online-Betrug

Online Fraud Insights ist ein überwachtes Machine-Learning-Modell, das bedeutet, dass historische Beispiele für betrügerische und legitime Transaktionen verwendet werden, um das Modell zu trainieren. Das Online Fraud Insights-Modell kann Betrug anhand wenig historischer Daten erkennen. Die Eingaben des Modells sind flexibel, sodass Sie es anpassen können, um eine Vielzahl von Betrugsrisiken zu erkennen, darunter Fake Reviews, Missbrauch von Werbeaktionen und Betrug beim Checkout von Kunden.

Das Online Fraud Insights-Modell verwendet ein Ensemble von Machine Learning-Algorithmen für die Datenanreicherung, -transformation und Betrugsklassifizierung. Im Rahmen des Modelltrainingsprozesses fügt Online Fraud Insights Rohdatenelemente wie IP-Adresse und BIN-Nummer mit Daten von Drittanbietern wie der Geolokalisierung der IP-Adresse oder der ausstellenden Bank für eine Kreditkarte hinzu. Zusätzlich zu Daten von Drittanbietern verwendet Online Fraud Insights Deep-Learning-Algorithmen, die Betrugsmuster berücksichtigen, die bei Amazon und beobachtet wurden AWS. Diese Betrugsmuster werden mithilfe eines Gradient-Baum-Boosting-Algorithmus zu Eingabemerkmale für Ihr Modell.

Um die Leistung zu erhöhen, optimiert Online Fraud Insights die Hyperparameter des Gradient-Tree-Boosting-Algorithmus über einen Bayesschen Optimierungsprozess. Es trainiert nacheinander Dutzende verschiedener Modelle mit unterschiedlichen Modellparametern (z. B. Anzahl der Bäume, Tiefe der Bäume und Anzahl der Stichproben pro Blatt). Es verwendet auch verschiedene Optimierungsstrategien, wie z. B. die Gewichtung der Betrügergruppe für Nebenbetrug, um sich um sehr niedrige Betrugsraten zu kümmern.

### Auswählen der Datenquelle

Beim Training eines Online-Fraud-Insights-Modells können Sie das Modell anhand von Ereignisdaten trainieren, die entweder extern (außerhalb von Amazon Fraud Detector) oder in Amazon Fraud Detector gespeichert werden. Der externe Speicher, den Amazon Fraud Detector derzeit unterstützt, ist Amazon Simple Storage Service (Amazon S3). Wenn Ihr externen Speicher verwendet, muss Ihr Ereignisdatensatz im CSV-Format (durch Kommas getrennte Werte) in einen Amazon S3-Bucket hochgeladen werden. Diese Datenspeicheroptionen werden in der Konfiguration des Modelltrainings als `EXTERNAL_EVENTS` (für externen Speicher) und `INGESTED_EVENTS` (für internen Speicher) bezeichnet. Weitere Informationen zu den verfügbaren Datenquellen und zum Speichern von Daten darin finden Sie unter [Speicherung der Ereignisdaten](#).

## Vorbereiten von Daten

Unabhängig davon, wo Sie Ihre Ereignisdaten speichern möchten (Amazon S3 oder Amazon Fraud Detector), sind die Anforderungen für den Modelltyp Online Fraud Insights dieselben.

Ihr Datensatz muss den Spalten-Header `EVENT_LABEL` enthalten. Diese Variable klassifiziert ein Ereignis als betrügerisches oder legitimes Ereignis. Wenn Sie eine CSV-Datei (externer Speicher) verwenden, müssen Sie `EVENT_LABEL` für jedes Ereignis in die Datei aufnehmen. Für die interne Speicherung ist das Feld `EVENT_LABEL` optional, aber alle Ereignisse müssen beschriftet werden, um in einen Trainingsdatensatz aufgenommen zu werden. Bei der Konfiguration Ihres Modelltrainings können Sie wählen, ob Ereignisse ohne Label ignoriert, ein legitimes Label für Ereignisse ohne Label angenommen oder ein betrügerisches Label für alle Ereignisse ohne Label angenommen werden soll.

## Auswählen von Daten

Informationen zur Auswahl von Daten für das Training Ihres Online Fraud Insights-Modells finden Sie unter [Erfassen von Ereignisdaten](#).

Der Online Fraud Insights-Trainingsprozess nimmt Beispiele für historische Daten auf der Grundlage von `EVENT_TIMESTAMP` und partitioniert sie. Es ist nicht notwendig, die Daten manuell zu erfassen, und dies kann sich negativ auf Ihre Modellergebnisse auswirken.

## Ereignisvariablen

Das Online Fraud Insights-Modell erfordert mindestens zwei Variablen, abgesehen von den erforderlichen Ereignismetadaten, die die [Datenvalidierung](#) für das Modelltraining bestanden haben und bis zu 100 Variablen pro Modell zulassen. Je mehr Variablen Sie angeben, desto besser kann das Modell zwischen Betrug und legitimen Ereignissen unterscheiden. Obwohl das Online Fraud Insights-Modell Dutzende von Variablen unterstützen kann, einschließlich benutzerdefinierter Variablen, empfehlen wir, IP-Adresse und E-Mail-Adresse einzubeziehen, da diese Variablen in der Regel am effektivsten bei der Identifizierung der ausgewerteten Entität sind.

## Validieren von Daten

Im Rahmen des Trainingsprozesses validiert Online Fraud Insights den Datensatz auf Datenqualitätsprobleme, die sich auf das Modelltraining auswirken können. Nach der Validierung der Daten ergreift Amazon Fraud Detector die entsprechenden Maßnahmen, um das bestmögliche Modell zu erstellen. Dazu gehören die Ausgabe von Warnungen für potenzielle Datenqualitätsprobleme, das automatische Entfernen von Variablen, bei

denen Datenqualitätsprobleme auftreten, die Ausgabe eines Fehlers und das Stoppen des Modelltrainingsprozesses. Weitere Informationen finden Sie unter [Datensatzvalidierung](#).

## Einblicke in Transaktionsbetrug

Der Modelltyp Transaction Fraud Insights ist darauf ausgelegt, card-not-present Transaktionsbetrug online oder in zu erkennen. Transaction Fraud Insights ist ein überwachttes Machine-Learning-Modell, was bedeutet, dass historische Beispiele für betrügerische und legitime Transaktionen verwendet werden, um das Modell zu trainieren.

Das Transaction Fraud Insights-Modell verwendet ein Ensemble von Machine Learning-Algorithmen für Datenanreicherung, Transformation und Betrugsklassifizierung. Es nutzt eine Feature-Engine, um Aggregate auf Entitäts- und Ereignisebene zu erstellen. Im Rahmen des Modelltrainingsprozesses fügt Transaction Fraud Insights Rohdatenelemente wie IP-Adresse und BIN-Nummer mit Daten von Drittanbietern wie der Geolokalisierung der IP-Adresse oder der ausstellenden Bank für eine Kreditkarte hinzu. Zusätzlich zu Daten von Drittanbietern verwendet Transaction Fraud Insights Deep-Learning-Algorithmen, die Betrugsmuster berücksichtigen, die bei Amazon beobachtet wurden, und AWS diese Betrugsmuster werden mithilfe eines Gradient-Tree-Boosting-Algorithmus zu Eingabefunktionen für Ihr Modell.

Um die Leistung zu erhöhen, optimiert Transaction Fraud Insights die Hyperparameter des Gradient-Tree-Boosting-Algorithmus über einen Bayesschen Optimierungsprozess, sequenzielles Training von Dutzenden verschiedener Modelle mit unterschiedlichen Modellparametern (z. B. Anzahl der Bäume, Tiefe der Bäume, Anzahl der Stichproben pro Blatt) sowie verschiedene Optimierungsstrategien wie die Gewichtung der Betrügerschaftsgruppen für Nebenbetrug, um sich um sehr niedrige Betrugsraten zu kümmern.

Im Rahmen des Modelltrainingsprozesses berechnet die Feature-Engine des Modells für Transaktionsbetrug Werte für jede eindeutige Entität in Ihrem Trainingsdatensatz, um Betrugsvorhersagen zu verbessern. Während des Trainingsprozesses berechnet und speichert Amazon Fraud Detector beispielsweise das letzte Mal, als eine Entität einen Kauf getätigt hat, und aktualisiert diesen Wert dynamisch bei jedem Aufruf der `GetEventPrediction` oder `SendEvent`-API. Während einer Betrugsvorhersage werden die Ereignisvariablen mit anderen Entitäts- und Ereignismetadaten kombiniert, um vorherzusagen, ob die Transaktion betrügerischer Natur ist.

## Auswählen der Datenquelle

Modelle von Transaction Fraud Insights werden nur für Datensätze trainiert, die intern mit Amazon Fraud Detector (INGESTED\_EVENTS) gespeichert wurden. Auf diese Weise kann Amazon Fraud

Detector die berechneten Werte über die Entitäten, die Sie auswerten, kontinuierlich aktualisieren. Weitere Informationen zu den verfügbaren Datenquellen finden Sie unter [. Speicherung der Ereignisdaten](#)

## Vorbereiten von Daten

Bevor Sie ein Transaction Fraud Insights-Modell trainieren, stellen Sie sicher, dass Ihre Datendatei alle Header enthält, wie unter [Ereignisdatensatz vorbereiten](#) beschrieben. Das Transaction Fraud Insights-Modell vergleicht neue Entitäten, die empfangen werden, mit den Beispielen betrügerischer und legitimer Entitäten im Datensatz. Daher ist es hilfreich, viele Beispiele für jede Entität bereitzustellen.

Amazon Fraud Detector wandelt den gespeicherten Ereignisdatensatz automatisch in das richtige Format für das Training um. Nachdem das Modell das Training abgeschlossen hat, können Sie die Leistungsmetriken überprüfen und bestimmen, ob Sie Ihrem Trainingsdatensatz Entitäten hinzufügen sollten.

## Auswählen von Daten

Standardmäßig trainiert Transaction Fraud Insights anhand Ihres gesamten gespeicherten Datensatzes für den von Ihnen ausgewählten Ereignistyp. Sie können optional einen Zeitraum festlegen, um die Ereignisse zu reduzieren, die zum Trainieren Ihres Modells verwendet werden. Stellen Sie beim Festlegen eines Zeitraums sicher, dass die Datensätze, die zum Trainieren des Modells verwendet werden, ausreichend Zeit hatten, um zu reifen. Das bedeutet, dass genügend Zeit verstrichen ist, um sicherzustellen, dass legitime und Betrugsaufzeichnungen korrekt identifiziert wurden. Bei einem Chargeback-Betrug dauert es beispielsweise oft 60 Tage oder mehr, um betrügerische Ereignisse korrekt zu identifizieren. Um eine optimale Modellleistung zu erzielen, stellen Sie sicher, dass alle Datensätze in Ihrem Trainingsdatensatz ausgereift sind.

Es ist nicht erforderlich, einen Zeitraum auszuwählen, der eine ideale Betrugsrate darstellt. Amazon Fraud Detector nimmt automatisch eine Stichprobe Ihrer Daten vor, um ein Gleichgewicht zwischen Betrugsraten, Zeitbereich und Entitätsanzahl zu erreichen.

Amazon Fraud Detector gibt während des Modelltrainings einen Validierungsfehler zurück, wenn Sie einen Zeitraum auswählen, für den nicht genügend Ereignisse vorhanden sind, um ein Modell erfolgreich zu trainieren. Für gespeicherte Datensätze ist das Feld `EVENT_LABEL` optional, aber Ereignisse müssen beschriftet werden, um in Ihren Trainingsdatensatz aufgenommen zu werden. Bei der Konfiguration Ihres Modelltrainings können Sie wählen, ob Ereignisse ohne Label ignoriert, ein



legitimes Label für Ereignisse ohne Label angenommen oder ein betrügerisches Label für Ereignisse ohne Label angenommen werden soll.

## Ereignisvariablen

Der zum Trainieren des Modells verwendete Ereignistyp muss mindestens 2 Variablen enthalten, abgesehen von den erforderlichen Ereignismetadaten, die die [Datenvalidierung](#) bestanden haben und bis zu 100 Variablen enthalten können. Je mehr Variablen Sie angeben, desto besser kann das Modell zwischen Betrug und legitimen Ereignissen unterscheiden. Obwohl das Transaction Fraud Insight-Modell Dutzende von Variablen unterstützen kann, einschließlich benutzerdefinierter Variablen, empfehlen wir Ihnen, IP-Adresse, E-Mail-Adresse, Zahlungsinstrumenttyp, Bestellpreis und Karten-BIN anzugeben.

## Validieren von Daten

Im Rahmen des Trainingsprozesses validiert Transaction Fraud Insights den Trainingsdatensatz auf Datenqualitätsprobleme, die sich auf das Modelltraining auswirken könnten. Nach der Validierung der Daten ergreift Amazon Fraud Detector geeignete Maßnahmen, um das bestmögliche Modell zu erstellen. Dazu gehören die Ausgabe von Warnungen für potenzielle Datenqualitätsprobleme, das automatische Entfernen von Variablen, bei denen Datenqualitätsprobleme auftreten, die Ausgabe eines Fehlers und das Stoppen des Modelltrainingsprozesses. Weitere Informationen finden Sie unter [Datensatzvalidierung](#).

Amazon Fraud Detector gibt eine Warnung aus, setzt das Training eines Modells jedoch fort, wenn die Anzahl der eindeutigen Entitäten kleiner als 1 500 ist, da dies die Qualität der Trainingsdaten beeinträchtigen kann. Wenn Sie eine Warnung erhalten, überprüfen Sie die [Leistungsmetrik](#).

## Einblicke in die Kontoübernahme

Der Modelltyp Account Takeover Insights (ATI) identifiziert betrügerische Online-Aktivitäten, indem er erkennt, ob Konten durch böswillige Übernahmen, Phishing oder durch gestohlene Anmeldeinformationen kompromittiert wurden. Account Takeover Insights ist ein Machine-Learning-Modell, das Anmeldeereignisse aus Ihrem Online-Unternehmen verwendet, um das Modell zu trainieren.

Sie können ein trainiertes Account Takeover Insights-Modell in Ihren Echtzeit-Anmeldeablauf einbetten, um festzustellen, ob ein Konto kompromittiert wurde. Das Modell bewertet eine Vielzahl von Authentifizierungs- und Anmeldetypen. Dazu gehören Webanwendungsanmeldungen, API-basierte Authentifizierungen und single-sign-on (SSO). Um das Modell Account Takeover Insights

zu verwenden, rufen Sie die [GetEventPrediction](#)-API auf, nachdem gültige Anmeldeinformationen vorgelegt wurden. Die API generiert eine Punktzahl, die das Risiko einer Kompromittierung des Kontos quantifiziert. Amazon Fraud Detector verwendet die Punktzahl und die von Ihnen definierten Regeln, um ein oder mehrere Ergebnisse für die Anmeldeereignisse zurückzugeben. Die Ergebnisse sind diejenigen, die Sie konfiguriert haben. Basierend auf den Ergebnissen, die Sie erhalten, können Sie für jede Anmeldung entsprechende Maßnahmen ergreifen. Das heißt, Sie können die Anmeldeinformationen für die Anmeldung entweder genehmigen oder in Frage stellen. Sie können die Anmeldeinformationen beispielsweise in Frage stellen, indem Sie eine Konto-PIN als zusätzliche Verifizierung anfordern.

Sie können das Account Takeover Insights-Modell auch verwenden, um Kontoanmeldungen asynchron zu bewerten und Aktionen für Konten mit hohem Risiko durchzuführen. Beispielsweise kann ein Konto mit hohem Risiko zur Untersuchungswarteschlange für einen menschlichen Prüfer hinzugefügt werden, um festzustellen, ob weitere Maßnahmen ergriffen werden müssen, z. B. das Konto aussetzen.

Das Modell Account Takeover Insights wird anhand eines Datensatzes trainiert, der die historischen Anmeldeereignisse Ihres Unternehmens enthält. Sie geben diese Daten an. Sie können die Konten optional als legitime oder betrügerische Konten kennzeichnen. Dies ist jedoch nicht erforderlich, um das Modell zu trainieren. Das Modell Account Takeover Insights erkennt Anomalien basierend auf dem Verlauf erfolgreicher Anmeldungen eines Kontos. Außerdem erfahren Sie, wie Sie Anomalien im Verhalten eines Benutzers erkennen, die auf ein erhöhtes Risiko einer schädlichen Kontoübernahme hindeuten. Zum Beispiel ein Benutzer, der sich normalerweise von demselben Satz von Geräten und IP-Adressen aus anmeldet. Ein Betrüger meldet sich in der Regel von einem anderen Gerät und einer anderen Geolokalisierung an. Diese Technik erzeugt eine Risikobewertung für eine Aktivität, die ungewöhnlich ist, was in der Regel ein Hauptmerkmal bössartiger Kontoübernahmen ist.

Vor dem Training eines Account Takeover Insights-Modells verwendet Amazon Fraud Detector eine Kombination von Machine Learning-Techniken, um Datenanreicherung, Datenaggregation und Datentransformation durchzuführen. Anschließend reichert Amazon Fraud Detector während des Trainingsprozesses die von Ihnen bereitgestellten Rohdatenelemente an. Beispiele für Rohdatenelemente sind IP-Adresse und Benutzeragent. Amazon Fraud Detector verwendet diese Elemente, um zusätzliche Eingaben zu erstellen, die die Anmeldeinformationen beschreiben. Zu diesen Eingaben gehören die Eingaben für Gerät, Browser und Geolokalisierung. Amazon Fraud Detector verwendet auch die von Ihnen bereitgestellten Anmeldeinformationen, um kontinuierlich aggregierte Variablen zu berechnen, die das Verhalten früherer Benutzer beschreiben. Beispiele für das Benutzerverhalten sind die Häufigkeit, mit der sich der Benutzer von einer bestimmten IP-Adresse aus angemeldet hat. Mithilfe dieser zusätzlichen Anreicherungen und Aggregate kann Amazon

Fraud Detector aus einer kleinen Menge von Eingaben aus Ihren Anmeldeereignissen eine starke Modellleistung generieren.

Das Account-Capover-Insights-Modell erkennt Instances, auf die ein böswilliger Akteur auf ein legitimes Konto zugreift, unabhängig davon, ob es sich bei dem böswilligen Akteur um einen Menschen oder einen Roboter handelt. Das Modell erzeugt eine einzelne Punktzahl, die das relative Risiko einer Kontokompromittierung angibt. Konten, die möglicherweise kompromittiert wurden, werden als Konten mit hohem Risiko gekennzeichnet. Sie können Konten mit hohem Risiko auf zwei Arten verarbeiten. Entweder können Sie eine zusätzliche Identitätsprüfung erzwingen. Oder Sie können das Konto zur manuellen Untersuchung an eine Warteschlange senden.

## Auswählen der Datenquelle

Modelle von Account Takeover Insights werden anhand eines intern in Amazon Fraud Detector gespeicherten Datensatzes trainiert. Um Ihre Anmeldeereignisdaten mit Amazon Fraud Detector zu speichern, erstellen Sie eine CSV-Datei mit Anmeldeereignissen von Benutzern. Geben Sie für jedes Ereignis Anmeldezeiten wie den Zeitstempel des Ereignisses, die Benutzer-ID, die IP-Adresse, den Benutzeragenten und ob die Anmeldezeiten gültig sind, an. Nachdem Sie die CSV-Datei erstellt haben, laden Sie die Datei zuerst in Amazon Fraud Detector hoch und verwenden Sie dann die Importfunktion, um die Daten zu speichern. Anschließend können Sie Ihr Modell mit den gespeicherten Daten trainieren. Weitere Informationen zum Speichern Ihres Ereignisdatsatzes mit Amazon Fraud Detector finden Sie unter [Speichern Sie Ihre Eventdaten intern mit Amazon Fraud Detector](#)

## Vorbereiten von Daten

Amazon Fraud Detector erfordert, dass Sie Ihre Benutzerkonto-Anmeldezeiten in einer CSV-Datei (durch Kommas getrennte Werte) bereitstellen, die im UTF-8-Format codiert ist. Die erste Zeile Ihrer CSV-Datei muss einen Datei-Header enthalten. Der Datei-Header besteht aus Ereignismetadaten und Ereignisvariablen, die jedes Datenelement beschreiben. Ereignisdaten folgen dem -Header. Jede Zeile in den Ereignisdaten besteht aus Daten aus einem einzigen Anmeldeereignis.

Für das Modell Account Takeover Insights müssen Sie die folgenden Ereignismetadaten und Ereignisvariablen in der Kopfzeile Ihrer CSV-Datei angeben.

### Ereignismetadaten

Wir empfehlen Ihnen, die folgenden Metadaten in Ihrem CSV-Datei-Header anzugeben. Die Ereignismetadaten müssen in Großbuchstaben angegeben werden.

- `EVENT_ID` – Eine eindeutige Kennung für das Anmeldeereignis.
- `ENTITY_TYPE` – Die Entität, die das Anmeldeereignis durchführt, z. B. ein Händler oder ein Kunde.
- `ENTITY_ID` – Eine Kennung für die Entität, die das Anmeldeereignis ausführt.
- `EVENT_TIMESTAMP` – Der Zeitstempel des Anmeldeereignisses. Der Zeitstempel muss im ISO 8601-Standard in UTC vorliegen.
- `EVENT_LABEL` (empfohlen) – Ein Label, das das Ereignis als betrügerisches oder legitimes Ereignis klassifiziert. Sie können alle Bezeichnungen verwenden, z. B. „d“, „legit“, „1“ oder „0“.

#### Note

- Ereignismetadaten müssen in Großbuchstaben angegeben werden. Bei der Groß- und Kleinschreibung wird zwischen Groß- und Kleinschreibung unterschieden.
- Labels sind für Anmeldeereignisse nicht erforderlich. Wir empfehlen jedoch, `EVENT_LABEL`-Metadaten einzuschließen und Labels für Ihre Anmeldeereignisse bereitzustellen. Es ist in Ordnung, wenn die Beschriftungen unvollständig oder sporadisch sind. Wenn Sie Labels angeben, berechnet Amazon Fraud Detector anhand dieser Labels automatisch eine Rate zur Kontoübernahmeerkennung und zeigt sie in der Modellleistungstabelle und -tabelle an.

## Ereignisvariablen

Für das Modell Account Takeover Insights gibt es sowohl erforderliche (Verzeichnis-) Variablen, die Sie angeben müssen, als auch optionale Variablen. Wenn Sie Ihre Variablen erstellen, müssen Sie die Variable dem richtigen Variablentyp zuweisen. Im Rahmen des Modelltrainingsprozesses verwendet Amazon Fraud Detector den Variablentyp, der der Variablen zugeordnet ist, um die Anreicherung von Variablen und das Feature-Engineering durchzuführen.

#### Note

Namen von Ereignisvariablen müssen in Kleinbuchstaben geschrieben werden. Bei ihnen wird zwischen Groß- und Kleinschreibung unterschieden.

## Obligatorische Variablen

Die folgenden Variablen sind erforderlich, um ein Modell von Account Takeover Insights zu trainieren.

Kategorie	Variablentyp	Beschreibung
IP-Adresse	IP_ADDRESS	Die IP-Adresse, die im Anmeldeereignis verwendet wird
Browser und Gerät	BENUTZER	Browser, Gerät und Betriebssystem, die im Anmeldeereignis verwendet werden
Gültige Anmeldeinformationen	GÜLTIG	Gibt an, ob die Anmeldeinformationen, die für die Anmeldung verwendet wurden, gültig sind

### Optionale Variablen

Die folgenden Variablen sind optional, um ein Modell von Account Takeover Insights zu trainieren.

Kategorie	Typ	Beschreibung
Browser und Gerät	FINGER-W dabei	Die eindeutige Kennung für einen Browser oder Geräte-Fingerabdruck
Sitzungs-ID	SESSION_ID	Die Kennung für eine Authentifizierungssitzung
Label (Bezeichnung)	EVENT_LABEL	Ein Label, das das Ereignis als betrügerische oder legitimes Ereignis klassifiziert. Sie können alle Bezeichnungen verwenden, z. B. „d“, „legit“, „1“ oder „0“.

Kategorie	Typ	Beschreibung
Zeitstempel	LABEL_TIMESTAMP	Der Zeitstempel der letzten Aktualisierung des Labels. Dies ist erforderlich, wenn EVENT_LABEL bereitgestellt wird.

#### Note

- Sie können alle Variablennamen für beide obligatorischen Variablen angeben. Es ist wichtig, dass jede obligatorische und optionale Variable dem richtigen Variablentyp zugewiesen ist.
- Sie können zusätzliche Variablen angeben. Amazon Fraud Detector wird diese Variablen jedoch nicht für das Training eines Modells von Account Takeover Insights enthalten.

## Auswählen von Daten

Das Sammeln von Daten ist ein wichtiger Schritt bei der Erstellung Ihres Account-Capover-Insights-Modells. Berücksichtigen Sie beim Sammeln Ihrer Anmeldedaten die folgenden Anforderungen und Empfehlungen:

### Erforderlich

- Geben Sie mindestens 1 500 Beispiele für Benutzerkonten an, die jeweils mindestens zwei zugehörige Anmeldeereignisse aufweisen.
- Ihr Datensatz muss Anmeldeereignisse von mindestens 30 Tagen abdecken. Sie können später den spezifischen Zeitraum der Ereignisse angeben, die zum Trainieren des Modells verwendet werden sollen.

### Empfohlen

- Ihr Datensatz enthält Beispiele für erfolglose Anmeldeereignisse. Sie können diese erfolglosen Anmeldungen optional als „Betrüger“ oder „Legatisch“ kennzeichnen.

- Bereiten Sie historische Daten mit Anmeldeereignissen vor, die sich über mehr als sechs Monate erstrecken und 100K.000 Entitäten enthalten.

Wenn Sie keinen Datensatz haben, der bereits die Mindestanforderungen erfüllt, sollten Sie erwägen, Ereignisdaten an Amazon Fraud Detector zu streamen, indem Sie den [SendEvent](#) -API-Vorgang aufrufen.

## Validieren von Daten

Bevor Sie Ihr Account-Capover-Insights-Modell erstellen, prüft Amazon Fraud Detector, ob die Metadaten und Variablen, die Sie zum Trainieren des Modells in Ihren Datensatz aufgenommen haben, die Größen- und Formatanforderungen erfüllen. Weitere Informationen finden Sie unter [Datensatzvalidierung](#). Es prüft auch auf andere Anforderungen. Wenn der Datensatz nicht validiert wird, wird das Modell nicht erstellt. Damit das Modell erfolgreich erstellt werden kann, stellen Sie sicher, dass Sie die Daten korrigieren, die die Validierung nicht bestanden haben, bevor Sie erneut trainieren.

### Häufige Datensatzfehler

Bei der Validierung eines Datensatzes für das Training eines -Kontoübernahme-Insights-Modells sucht Amazon Fraud Detector nach diesen und anderen Problemen und gibt einen Fehler aus, wenn eines oder mehrere der Probleme auftreten.

- Die CSV-Datei hat nicht das UTF-8-Format.
- Der CSV-Datei-Header enthält nicht mindestens eines der folgenden Metadaten: `EVENT_IDENTITY_ID`, oder `EVENT_TIMESTAMP`.
- Der CSV-Datei-Header enthält nicht mindestens eine Variable der folgenden Variablentypen: `IP_ADDRESSUSERAGENT`, oder `VALIDCRED`.
- Es gibt mehr als eine Variable, die demselben Variablentyp zugeordnet ist.
- Mehr als 0,1 % der Werte in `EVENT_TIMESTAMP` enthalten Null-Werte oder andere Werte als die unterstützten Datums- und Zeitstempelformate.
- Die Anzahl der Tage zwischen dem ersten und dem letzten Ereignis beträgt weniger als 30 Tage.
- Mehr als 10 % der Variablen des `IP_ADDRESS` Variablentyps sind entweder ungültig oder null.
- Mehr als 50 % der Variablen des `USERAGENT` Variablentyps enthalten Null-Werte.
- Alle Variablen des `VALIDCRED` Variablentyps sind auf festgelegt `false`.

## Ein Modell erstellen

Modelle von Amazon Fraud Detector lernen, Betrug für einen bestimmten Ereignistyp zu erkennen. In Amazon Fraud Detector erstellen Sie zunächst ein Modell, das als Container für Ihre Modellversionen fungiert. Jedes Mal, wenn Sie ein Modell trainieren, wird eine neue Version erstellt. Weitere Informationen zum Erstellen und Trainieren eines Modells mit der AWS Konsole finden Sie unter [Schritt 3: Erstellen eines Modells](#).

Jedes Modell hat eine entsprechende Modellbewertungsvariable. Amazon Fraud Detector erstellt diese Variable in Ihrem Namen, wenn Sie ein Modell erstellen. Sie können diese Variable in Ihren Regelausdrücken verwenden, um Ihre Modellwerte während einer Betrugsbewertung zu interpretieren.

## Trainieren und Bereitstellen eines Modells mithilfe der AWS SDK for Python (Boto3)

Eine Modellversion wird durch Aufrufen der `CreateModelVersion` Operationen `CreateModel` und erstellt. `CreateModel` initiiert das Modell, das als Container für Ihre Modellversionen fungiert. `CreateModelVersion` startet den Trainingsprozess, was zu einer bestimmten Version des Modells führt. Eine neue Version der Lösung wird bei jedem Aufruf erstellt `CreateModelVersion`.

Das folgende Beispiel zeigt eine Beispielanforderung für die `CreateModel`-API. In diesem Beispiel wird der Modelltyp `Online Fraud Insights` erstellt und davon ausgegangen, dass Sie einen Ereignistyp erstellt `sample_registration`. Weitere Informationen zum Erstellen eines Ereignistyps finden Sie unter [Einen Ereignistyp erstellen](#).

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

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

Trainieren Sie Ihre erste Version mit der [CreateModelVersion](#)-API. `ExternalEventsDetail` Geben Sie für die `TrainingDataSource` und die Quelle und den Amazon S3-Speicherort des Trainingsdatensatzes an. `TrainingDataSchema` Geben Sie für an, wie Amazon Fraud Detector die Trainingsdaten interpretieren soll, insbesondere welche Ereignisvariablen aufgenommen werden



sollen und wie die Ereignisbezeichnungen klassifiziert werden. Standardmäßig ignoriert Amazon Fraud Detector die nicht gekennzeichneten Ereignisse. Dieser Beispielcode verwendet `AUTO` für `unlabeledEventsTreatment` um anzugeben, dass Amazon Fraud Detector entscheidet, wie die unbeschrifteten Ereignisse verwendet werden sollen.

```
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'
}
)
```

Eine erfolgreiche Anforderung führt zu einer neuen Modellversion mit dem Status `TRAINING_IN_PROGRESS`. Während des Trainings können Sie das Training jederzeit abbrechen, indem Sie aufrufen `updateModelVersionStatus` und den Status auf `aktualisierenTRAINING_CANCELLED`. Sobald das Training abgeschlossen ist, wird der Status der Modellversion auf `aktualisiertTRAINING_COMPLETE`. Sie können die Modellleistung mithilfe der Amazon Fraud Detector-Konsole oder durch Aufrufen von `überprüfenDescribeModelVersions`. Weitere Informationen zur Interpretation von Modellwerten und Leistung finden Sie unter [Modellwerte](#) und [Modellleistungsmetriken](#).

Nachdem Sie die Modellleistung überprüft haben, aktivieren Sie das Modell, um es von Detectors in Betrugsvorhersagen in Echtzeit verwenden zu können. Amazon Fraud Detector stellt das Modell in mehreren Availability Zones bereit, um Redundanz bei aktiviertem Auto Scaling zu gewährleisten, um sicherzustellen, dass das Modell mit der Anzahl der von Ihnen getroffenen Betrugsprognosen

skaliert wird. Um das Modell zu aktivieren, rufen Sie die `UpdateModelVersionStatus` -API auf und aktualisieren Sie den Status auf `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'
)
```

## Modellwerte

Amazon Fraud Detector generiert Modellwerte für verschiedene Modelltypen unterschiedlich.

Für Modelle von Account Takeover Insights (ATI) verwendet Amazon Fraud Detector nur einen aggregierten Wert (einen Wert, der durch die Kombination einer Reihe von Rohvariablen berechnet wird), um den Modellwert zu generieren. Für das erste Ereignis einer neuen Entität wird ein Wert von -1 generiert, was auf ein unbekanntes Risiko hinweist. Dies liegt daran, dass für eine neue Entität die Werte, die für die Berechnung des Aggregats verwendet werden, Null oder Null sind. Das Modell Account Takeover Insights (ATI) generiert Modellbewertungen zwischen 0 und 1 000 für alle nachfolgenden Ereignisse für dieselbe Entität und für bestehende Entitäten, wobei 0 für ein geringes Betrugsrisiko und 1 000 für ein hohes Betrugsrisiko steht. Bei ATI-Modellen stehen die Modellwerte in direktem Zusammenhang mit der Aufforderungsrate (CR). Ein Wert von 500 entspricht beispielsweise einer geschätzten 5-%-Herausforderungsrate, während ein Wert von 900 einer geschätzten 0,1-%-Herausforderungsrate entspricht.

Für Online Fraud Insights (OFI)- und Transaction Fraud Insights (TFI)-Modelle verwendet Amazon Fraud Detector sowohl den aggregierten Wert (ein Wert, der durch die Kombination einer Reihe von Rohvariablen berechnet wird) als auch den Rohwert (der für die Variable bereitgestellte Wert), um die Modellwerte zu generieren. Die Modellwerte können zwischen 0 und 1 000 liegen, wobei 0 für ein geringes Betrugsrisiko und 1 000 für ein hohes Betrugsrisiko steht. Für die OFI- und TFI-Modelle stehen die Modellwerte in direktem Zusammenhang mit der falsch positiven Rate (FPR). Ein Wert von 600 entspricht beispielsweise einer geschätzten Rate falsch positiver Ergebnisse von 10 %, während ein Wert von 900 einer geschätzten Rate falsch positiver Ergebnisse von 2 % entspricht. Die folgende Tabelle enthält Details dazu, wie bestimmte Modellwerte mit geschätzten falsch positiven Raten korrelieren.

Modellbewertung	Geschätzte FPR
975	0,50 %
950	1 %
900	2 %
860	3 %
775	5 %
700	7 %
600	10 %

## Modelleistungsmetriken

Nach Abschluss des Modelltrainings validiert Amazon Fraud Detector die Modelleistung anhand von 15 % Ihrer Daten, die nicht zum Trainieren des Modells verwendet wurden. Sie können davon ausgehen, dass Ihr trainiertes Amazon Fraud Detector-Modell eine reale Leistung zur Betrugserkennung aufweist, die den Validierungsleistungsmetriken ähnelt.


Als Unternehmen müssen Sie zwischen der Erkennung von mehr Betrug und der Erhöhung der Reibung legitimer Kunden abwägen. Zur Unterstützung bei der Auswahl des richtigen Gleichgewichts bietet Amazon Fraud Detector die folgenden Tools zur Bewertung der Modelleistung:

- Ergebnisverteilungsdiagramm – Ein Histogramm der Modellbewertungsverteilungen geht von einer Beispielgruppe von 100.000 Ereignissen aus. Die linke Y-Achse steht für die legitimen Ereignisse und die rechte Y-Achse für die Betrugsereignisse. Sie können einen bestimmten Modellschwellenwert auswählen, indem Sie auf den Diagrammbereich klicken. Dadurch werden die entsprechenden Ansichten in der Konfusionsmatrix und dem ROC-Diagramm aktualisiert.
- Konfusionsmatrix – fasst die Modellgenauigkeit für einen bestimmten Bewertungsschwellenwert zusammen, indem Modellvorhersagen mit tatsächlichen Ergebnissen verglichen werden. Amazon Fraud Detector geht von einer Beispielgruppe von 100.000 Ereignissen aus. Die Verteilung von Betrug und legitimen Ereignissen simuliert die Betrugsrate in Ihren Unternehmen.
  - Wahre positive Ergebnisse – Das Modell prognostiziert Betrug und das Ereignis ist tatsächlich Betrug.

- Falsch positive Ergebnisse – Das Modell sagt Betrug voraus, aber das Ereignis ist tatsächlich legitime.
- Wahre negative Ergebnisse – Das Modell prognostiziert legitime Ereignisse und ist tatsächlich legitime Ereignisse.
- Falsch negative Ergebnisse – Das Modell prognostiziert legitime Ergebnisse, aber das Ereignis ist tatsächlich Betrug.
- True Positive Rate (TPR) – Prozentsatz des Gesamtbetrugs, den das Modell erkennt. Wird auch als Erfassungsrate bezeichnet.
- Falsch positive Rate (FPR) – Prozentsatz der gesamten legitimen Ereignisse, die fälschlicherweise als Betrug vorhergesagt wurden.
- Receiver Operator Curve (ROC) – Plottet die wirklich positive Rate als Funktion der falsch positiven Rate über alle möglichen Schwellenwerte für den Modellwert. Zeigen Sie dieses Diagramm an, indem Sie Erweiterte Metriken auswählen.
- Flächen unter der Kurve (AUC) – fasst TPR und FPR über alle möglichen Schwellenwerte für den Modellwert zusammen. Ein Modell ohne Vorhersagekraft hat eine AUC von 0,5, während ein perfektes Modell einen Wert von 1,0 hat.
- Unsicherer Bereich – Es zeigt den Bereich des vom Modell erwarteten AUC an. Größerer Bereich (Unterschied in der Ober- und Untergrenze von  $AUC > 0,1$ ) bedeutet eine höhere Modellunsicherheit. Wenn der Unsicherheitsbereich groß ist ( $>0,1$ ), sollten Sie erwägen, beschriftete Ereignisse bereitzustellen und das Modell neu zu trainieren.


So verwenden Sie die Modelleleistungsmetriken

1. Beginnen Sie mit dem Ergebnisverteilungsdiagramm, um die Verteilung der Modellwerte für Ihre Betrugs- und legitimen Ereignisse zu überprüfen. Idealerweise besteht eine klare Trennung zwischen Betrug und legitimen Ereignissen. Dies gibt an, dass das Modell genau erkennen kann, welche Ereignisse betrügerische und welche legitime Ereignisse sind. Wählen Sie einen Modellschwellenwert aus, indem Sie auf den Diagrammbereich klicken. Sie können sehen, wie sich die Anpassung des Schwellenwerts für den Modellwert auf Ihre wirklich positiven und falsch positiven Raten auswirkt.

 Note

Das Bewertungsverteilungsdiagramm zeigt die Betrugs- und legitimen Ereignisse auf zwei verschiedenen Y-Achse. Die linke Y-Achse steht für die legitimen Ereignisse und die rechte Y-Achse für die Betrugsereignisse.

- Überprüfen Sie die Konfusionsmatrix . Je nach Schwellenwert für den ausgewählten Modellwert können Sie die simulierten Auswirkungen anhand einer Stichprobe von 100.000 Ereignissen sehen. Die Verteilung von Betrug und legitimen Ereignissen simuliert die Betrugsrate in Ihren Unternehmen. Verwenden Sie diese Informationen, um das richtige Gleichgewicht zwischen der wirklich positiven Rate und der falsch positiven Rate zu finden.
- Weitere Informationen finden Sie unter Erweiterte Metriken. Verwenden Sie das ROC-Diagramm, um die Beziehung zwischen der wirklich positiven Rate und der falsch positiven Rate für jeden Schwellenwert für den Modellwert zu verstehen. Die ROC-Kurve kann Ihnen helfen, den Kompromiss zwischen einer wirklich positiven Rate und einer falsch positiven Rate zu optimieren.

 Note

Sie können Metriken auch in Tabellenform überprüfen, indem Sie Tabelle auswählen. Die Tabellenansicht zeigt auch die Metrik Präzision . Präzision ist der Prozentsatz der Betrugsereignisse, die korrekt als betrügerisch vorhergesagt wurden, im Vergleich zu allen Ereignissen, die als betrügerisch vorhergesagt wurden.

- Verwenden Sie die Leistungsmetriken, um die optimalen Modellschwellenwerte für Ihr Unternehmen auf der Grundlage Ihrer Ziele und Ihres Anwendungsfalls zur Betrugserkennung zu ermitteln. Wenn Sie beispielsweise das Modell verwenden möchten, um neue Kontoregistrierungen entweder als hoch-, mittel- oder niedrigrisikobehaftet zu klassifizieren, müssen Sie zwei Schwellenwertwerte identifizieren, damit Sie drei Regelbedingungen wie folgt entwerfen können:
  - Werte  $> X$  sind ein hohes Risiko
  - Werte  $< X$ , aber  $> Y$  sind ein mittleres Risiko
  - Werte  $< Y$  sind ein geringes Risiko

## Wichtigkeit von Modellvariablen

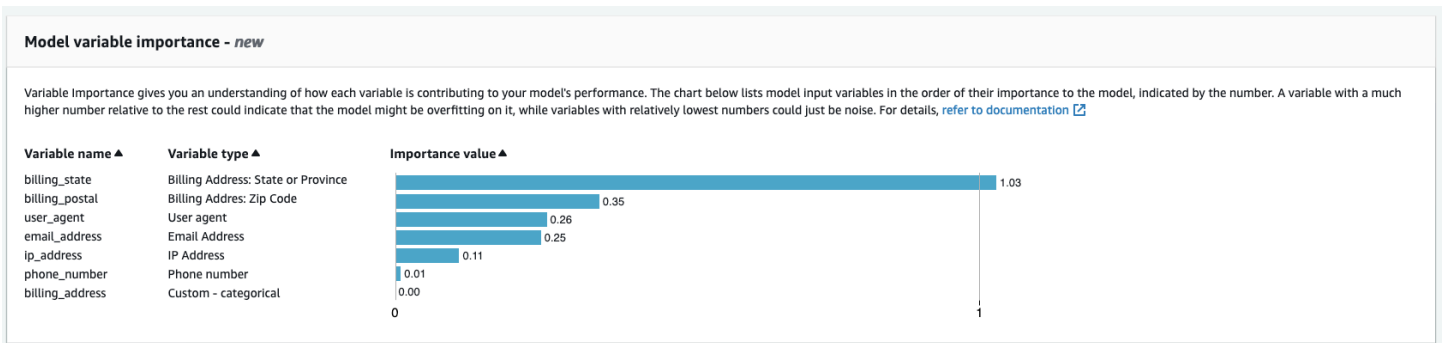
Die Wichtigkeit von Modellvariablen ist ein Feature von Amazon Fraud Detector, das Modellvariablen innerhalb einer Modellversion einstuft. Jede Modellvariable erhält einen Wert, der auf ihrer relativen Bedeutung für die Gesamtleistung Ihres Modells basiert. Die Modellvariable mit dem höchsten Wert ist für das Modell wichtiger als die anderen Modellvariablen im Datensatz für diese Modellversion und wird standardmäßig oben aufgeführt. Ebenso wird die Modellvariable mit dem niedrigsten Wert standardmäßig unten aufgeführt und ist im Vergleich zu den anderen Modellvariablen am wenigsten wichtig. Mithilfe der Werte für die Wichtigkeit von Modellvariablen können Sie einen Einblick in die Eingaben erhalten, die die Leistung Ihres Modells beeinflussen.

Sie können die Werte für die Wichtigkeit von Modellvariablen für Ihre trainierte Modellversion in der Amazon Fraud Detector-Konsole oder mithilfe der [DescribeModelVersion](#) API anzeigen.

Die Wichtigkeit von Modellvariablen bietet die folgenden Werte für jede [Variable](#), die zum Trainieren der [Modellversion](#) verwendet wird.

- **Variablentyp** : Typ der Variablen (z. B. IP-Adresse oder E-Mail). Weitere Informationen finden Sie unter [Variablentypen](#). Für Modelle von Account Takeover Insights (ATI) bietet Amazon Fraud Detector einen Wert mit variabler Bedeutung sowohl für den Roh- als auch für den Aggregatvariablentyp. Rohvariablentypen werden den von Ihnen bereitgestellten Variablen zugewiesen. Der aggregierte Variablentyp wird einer Reihe von Rohvariablen zugewiesen, die Amazon Fraud Detector kombiniert hat, um einen aggregierten Wichtigkeitswert zu berechnen.
- **Variablenname** : Name der Ereignisvariable, die zum Trainieren der Modellversion verwendet wurde (z. B. `ip_address`, `email_address`, `are_credentials_valid`). Für den aggregierten Variablentyp werden die Namen aller Variablen aufgeführt, die zur Berechnung des aggregierten Werts für die Bedeutung der Variablen verwendet wurden.
- **Variable Importance Value**: Eine Zahl, die die relative Bedeutung der Roh- oder Aggregatvariable für die Leistung des Modells darstellt. Typischer Bereich: 0–10

In der Amazon Fraud Detector-Konsole werden die Werte für die Wichtigkeit der Modellvariablen wie folgt für ein Online Fraud Insights (OFI)- oder ein Transaction Fraud Insights (TFI)-Modell angezeigt. Ein ATI-Modell (Account Takeover Insight) stellt zusätzlich zu den Wichtigkeitswerten der Rohvariablen aggregierte Werte für die Bedeutung von Variablen bereit. Das visuelle Diagramm macht es einfach, die relative Bedeutung zwischen Variablen mit der vertikalen gepunkteten Linie zu sehen, die Verweis auf den Wichtigkeitswert der am höchsten eingestuften Variablen bietet.



Amazon Fraud Detector generiert Werte mit variabler Bedeutung für jede Fraud-Detector-Modellversion ohne zusätzliche Kosten.

### ⚠ Important

Modellversionen, die vor dem 9. Juli 2021 erstellt wurden, haben keine Werte mit variabler Bedeutung. Sie müssen eine neue Version Ihres Modells trainieren, um die Wichtigkeitswerte der Modellvariablen zu generieren.

## Verwenden von Werten für die Wichtigkeit von Modellvariablen

Sie können Werte für die Wichtigkeit von Modellvariablen verwenden, um einen Einblick in die Leistung Ihres Modells zu erhalten, die die Leistung Ihres Modells erhöht oder verringert und welche Variablen am meisten beitragen. Passen Sie dann Ihr Modell an, um die Gesamtleistung zu verbessern.

Um die Leistung Ihres Modells zu verbessern, sollten Sie insbesondere die Werte der variablen Wichtigkeit anhand Ihres Domainwissens untersuchen und Probleme in den Trainingsdaten debuggen. Wenn beispielsweise die Konto-ID als Eingabe für das Modell verwendet wurde und sie oben aufgeführt ist, werfen Sie einen Blick auf den Wert der variablen Wichtigkeit. Wenn der Wert der variablen Wichtigkeit deutlich höher ist als die restlichen Werte, könnte Ihr Modell ein bestimmtes Betrugsmuster überschneiden (z. B. stammen alle Betrugsereignisse von derselben Konto-ID). Es könnte jedoch auch der Fall sein, dass es zu einer Kennzeichnungsleckage kommt, wenn die Variable von den Betrugsbezeichnungen abhängt. Abhängig vom Ergebnis Ihrer Analyse auf der Grundlage Ihrer Domainkenntnisse möchten Sie möglicherweise die Variable entfernen und mit einem breiteren Datensatz trainieren oder das Modell unverändert lassen.

Betrachten Sie in ähnlicher Weise die Variablen, die an letzter Stelle stehen. Wenn der Wert für die variable Wichtigkeit deutlich niedriger ist als der Rest der Werte, hat diese Modellvariable

möglicherweise keine Bedeutung für das Training Ihres Modells. Sie könnten erwägen, die Variable zu entfernen, um eine einfachere Modellversion zu trainieren. Wenn Ihr Modell nur wenige Variablen hat, z. B. nur zwei Variablen, stellt Amazon Fraud Detector weiterhin die Werte für die variable Wichtigkeit bereit und ordnet die Variablen zu. Die Erkenntnisse in diesem Fall sind jedoch begrenzt.

### Important

1. Wenn Sie feststellen, dass Variablen im Diagramm zur Wichtigkeit von Modellvariablen fehlen, kann dies einen der folgenden Gründe haben. Erwägen Sie, die Variable in Ihrem Datensatz zu ändern und Ihr Modell neu zu trainieren.
  - Die Anzahl der eindeutigen Werte für die Variable im Trainingsdatensatz ist niedriger als 100.
  - Größer als 0,9 der Werte für die Variable fehlen im Trainingsdatensatz.
2. Sie müssen jedes Mal eine neue Modellversion trainieren, wenn Sie die Eingabevariablen Ihres Modells anpassen möchten.

## Auswerten der Wichtigkeitswerte von Modellvariablen

Wir empfehlen Ihnen, Folgendes zu berücksichtigen, wenn Sie die Wichtigkeitswerte von Modellvariablen bewerten:

- Werte mit variabler Bedeutung müssen immer in Kombination mit dem Domainwissen ausgewertet werden.
- Untersuchen Sie den Wert der Variablenbedeutung einer Variablen relativ zum Wert der Variablenbedeutung der anderen Variablen innerhalb der Modellversion. Berücksichtigen Sie nicht den Wert der variablen Wichtigkeit für eine einzelne Variable unabhängig.
- Vergleichen Sie die Werte der Variablenbedeutung innerhalb derselben Modellversion. Vergleichen Sie nicht die Werte der Variablenbedeutung derselben Variablen über Modellversionen hinweg, da sich der Wert der Variablenbedeutung einer Variablen in einer Modellversion vom Wert derselben Variablen in einer anderen Modellversion unterscheiden kann. Wenn Sie dieselben Variablen und denselben Datensatz verwenden, um verschiedene Modellversionen zu trainieren, generiert dies nicht unbedingt dieselben Werte für die variable Wichtigkeit.



## Anzeigen der Rangfolge der Wichtigkeit von Modellvariablen

Nachdem das Modelltraining abgeschlossen ist, können Sie die Rangfolge der Wichtigkeit von Modellvariablen Ihrer trainierten Modellversion in der Amazon Fraud Detector-Konsole oder mithilfe der [DescribeModelVersion](#) API anzeigen.

Um die Rangfolge der Wichtigkeit von Modellvariablen mithilfe der Konsole anzuzeigen,

1. Öffnen Sie die -AWSKonsole und melden Sie sich bei Ihrem -Konto an. Navigieren Sie zu Amazon Fraud Detector.
2. Wählen Sie im linken Navigationsbereich Models (Modelle) aus.
3. Wählen Sie Ihr Modell und dann Ihre Modellversion aus.
4. Stellen Sie sicher, dass die Registerkarte Übersicht ausgewählt ist.
5. Scrollen Sie nach unten, um den Bereich Wichtigkeit der Modellvariablen anzuzeigen.

## Verstehen, wie der Wert für die Wichtigkeit der Modellvariablen berechnet wird

Nach Abschluss jedes Trainings der Modellversion generiert Amazon Fraud Detector automatisch Werte für die Wichtigkeit von Modellvariablen und die Leistungsmetriken des Modells. Dazu verwendet Amazon Fraud Detector SHapley exPlanations ([SHAP](#)). SHAP ist im Wesentlichen der durchschnittliche erwartete Beitrag einer Modellvariable, nachdem alle möglichen Kombinationen aller Modellvariablen berücksichtigt wurden.

SHAP weist zunächst den Beitrag jeder Modellvariable zur Vorhersage eines Ereignisses zu. Anschließend werden diese Vorhersagen aggregiert, um eine Rangfolge der Variablen auf Modellebene zu erstellen. Um Beiträge jeder Modellvariable für eine Vorhersage zuzuweisen, berücksichtigt SHAP Unterschiede bei den Modellausgaben zwischen allen möglichen Variablenkombinationen. Indem SHAP alle Möglichkeiten zum Einschließen oder Entfernen bestimmter Variablen zur Generierung einer Modellausgabe einschließt, kann es genau auf die Bedeutung jeder Modellvariable zugreifen. Dies ist besonders wichtig, wenn die Modellvariablen stark miteinander korreliert sind.

ML-Modelle erlauben es Ihnen in den meisten Fällen nicht, Variablen zu entfernen. Sie können stattdessen eine entfernte oder fehlende Variable im Modell durch die entsprechenden Variablenwerte aus einer oder mehreren Baselines ersetzen (z. B. Ereignisse, die nicht von

betrügerisch sind). Die Auswahl richtiger Basis-Instances kann schwierig sein, aber Amazon Fraud Detector erleichtert dies, indem diese Basislinie als Populationsdurchschnitt für Sie festgelegt wird.

## Importieren eines SageMaker Modells

Sie können optional SageMaker von gehostete Modelle in Amazon Fraud Detector importieren.

Ähnlich wie Modelle können SageMaker Modelle mithilfe der `GetEventPrediction` API zu Detektoren hinzugefügt und Betrugsprognosen generiert werden. Im Rahmen der `GetEventPrediction` Anforderung ruft Amazon Fraud Detector Ihren SageMaker Endpunkt auf und übergibt die Ergebnisse an Ihre Regeln.

Sie können Amazon Fraud Detector so konfigurieren, dass die als Teil der `GetEventPrediction` Anforderung gesendeten Ereignisvariablen verwendet werden. Wenn Sie Ereignisvariablen verwenden möchten, müssen Sie eine Eingabevorlage angeben. Amazon Fraud Detector verwendet diese Vorlage, um Ihre Ereignisvariablen in die erforderliche Eingabenutzlast umzuwandeln, um den SageMaker Endpunkt aufzurufen. Alternativ können Sie Ihr SageMaker Modell so konfigurieren, dass es einen `byteBuffer` verwendet, der als Teil der `GetEventPrediction` Anforderung gesendet wird.

Amazon Fraud Detector unterstützt den Import von SageMaker Algorithmen, die JSON- oder CSV-Eingabeformate und JSON- oder CSV-Ausgabeformate verwenden. Beispiele für unterstützte SageMaker Algorithmen sind XGBoost, Linear Learner und Random Cut Forest. XGBoost

## Importieren eines SageMaker Modells mit der AWS SDK for Python (Boto3)

Verwenden Sie die `PutExternalModel` API, um ein SageMaker Modell zu importieren. Im folgenden Beispiel wird davon ausgegangen, dass der SageMaker Endpunkt bereitgestellt `sagemaker-transaction-model` wurde, den `InService` Status hat und den XGBoost-Algorithmus verwendet.

Die Eingabekonfiguration gibt an, dass die Ereignisvariablen verwendet, um die Modelleingabe zu erstellen (`useEventVariables` ist auf `gesetztTRUE`). Das Eingabeformat ist `TEXT_CSV`, da XGBoost eine CSV-Eingabe erfordert. Der `csvInputTemplate` gibt an, wie die CSV-Eingabe aus den Variablen erstellt wird, die als Teil der `GetEventPrediction` Anforderung gesendet werden. In diesem Beispiel wird davon ausgegangen, dass Sie die Variablen `prev_amt`, `hist_amt` und erstellt `habenpayment_type`.

Die Ausgabekonfiguration gibt das Antwortformat des SageMaker Modells an und ordnet den entsprechenden CSV-Index der Amazon Fraud Detector-Variablen zu `sagemaker_output_score`. Nach der Konfiguration können Sie die Ausgabevariable in -Regeln verwenden.

**Note**

Die Ausgabe eines SageMaker Modells muss einer Variablen mit der Quelle zugeordnet werden `EXTERNAL_MODEL_SCORE`. Sie können diese Variablen nicht in der Konsole mit Variablen erstellen. Sie müssen sie stattdessen erstellen, wenn Sie Ihren Modellimport konfigurieren.

```
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'
)
```

## Löschen eines Modell

Sie können Modelle und Modellversionen in Amazon Fraud Detector löschen, sofern sie nicht mit einer Detektorversion verknüpft sind. Wenn Sie ein Modell löschen, löscht Amazon Fraud Detector dieses Modell dauerhaft und die Daten werden nicht mehr in Amazon Fraud Detector gespeichert.

Sie können SageMaker Amazon-Modelle auch entfernen, wenn sie nicht mit einer Detektorversion verknüpft sind. Wenn Sie ein SageMaker Modell entfernen, wird es von Amazon Fraud Detector getrennt, aber das Modell ist weiterhin verfügbar in SageMaker.

### So löschen eine Modellversion

Sie können nur Modellversionen löschen, die sich imReady to deploy Status befinden. Um eine Modellversion vom Status inReady to deploy den StatusACTIVE zu ändern, heben Sie die Bereitstellung der Modellversion auf.

1. Melden Sie sich bei der anAWS Management Console und öffnen Sie die Amazon Fraud Detector Konsole unter <https://console.aws.amazon.com/frauddetector>.
2. Wählen Sie im linken Navigationsbereich der Amazon Fraud Detector Konsole die Option Modelle.
3. Wählen Sie das Modell die Modellversion die Sie die Modellversion.
4. Wählen Sie die Modellversion die Sie die Modellversion.
5. Wählen Sie Actions (Aktionen) und anschließend Delete (Löschen).
6. Geben Sie den Namen der Modellversion ein, und wählen Sie dann Modellversion löschen.

### So machen Sie die Bereitstellung einer Modellversion

Sie können die Bereitstellung einer Modellversion, die von einer Detektorversion (ACTIVE,,DRAFT) verwendet wirdINACTIVE, nicht rückgängig machen. Um die Bereitstellung einer Modellversion rückgängig zu machen, die von einer Detektorversion verwendet wird, entfernen Sie daher zuerst die Modellversion aus der Detektorversion.

1. Wählen Sie im linken Navigationsbereich der Amazon Fraud Detector Konsole die Option Modelle.
2. Wählen Sie das Modell aus, das die Modellversion enthält, für die Sie die Bereitstellung rückgängig machen möchten.
3. Wählen Sie die Modellversion die Sie die Modellversion.
4. Wählen Sie Actions und dann Undeploy model version aus.

### Löschen eines Modell

Bevor Sie ein Modell. Sie müssen zuerst alle Modellversionen und die dem Modell zugeordneten Modellversionen.

1. Wählen Sie im linken Navigationsbereich der Amazon Fraud Detector Konsole die Option Modelle.
2. Wählen Sie das Modell das Sie das Sie die Sie löschen möchten.
3. Wählen Sie Actions (Aktionen) und anschließend Delete (Löschen).
4. Geben Sie den Modellnamen ein, und wählen Sie dann Modell löschen.

Um ein SageMaker Amazon-Modell zu entfernen

1. Wählen Sie im linken Navigationsbereich der Amazon Fraud Detector Konsole die Option Modelle.
2. Wählen Sie das SageMaker Modell das Sie das Sie entfernen möchten.
3. Wählen Sie Aktionen und dann Modell entfernen aus.
4. Geben Sie den Modellnamen ein und wählen Sie dann SageMakerModell entfernen.

# Detektor

Ein Detektor ist ein Container, der die Betrugserkennungslogik, wie z. B. die Modelle und Regeln, für ein bestimmtes Geschäftsereignis enthält, das Sie auf Betrug untersuchen möchten. Sie erstellen zunächst einen Detektor, indem Sie das Ereignis angeben, das Sie bereits definiert haben, und fügen optional eine Modellversion hinzu, die bereits von Amazon Fraud Detector für das Ereignis erstellt und trainiert wurde.

Anschließend fügen Sie Regeln und die Reihenfolge der Regelausführung zu einem Detektor hinzu, um eine Version des Detektors zu erstellen. Eine Detektorversion definiert die Regeln und optional ein Modell, das im Rahmen der Anforderung zur Generierung von Betrugsprognosen ausgeführt wird. Sie können jede der in einem Detektor definierten Regeln zur Detektorversion hinzufügen. Sie können der Detektorversion auch jedes Modell hinzufügen, das für den ausgewerteten Ereignistyp trainiert wurde. Ein Detektor kann mehrere Versionen haben, wobei jede Version unterschiedliche Regeln und Regelausführungsreihenfolge hat, um mehrere Anwendungsfälle zu erfüllen.

Jede Detektorversion muss einen Status von `DRAFT`, `ACTIVE`, oder `INACTIVE` haben. Es kann nur eine Detektorversion mit `ACTIVE`-Status nach dem anderen. Amazon Fraud Detector verwendet die Detektorversion mit `ACTIVE`-Status zur Generierung von Betrugsprognosen.

## Erstellen Sie einen Detektor

Sie erstellen einen Detektor, indem Sie den Ereignistyp angeben, den Sie bereits definiert haben. Sie können optional ein Modell hinzufügen, das bereits von Amazon Fraud Detector trainiert und eingesetzt wurde. Wenn Sie ein Modell hinzufügen, können Sie den von Amazon Fraud Detector generierten Modellwert in Ihrem Regelausdruck verwenden, wenn Sie eine Regel erstellen (z. B. `$model score < 90`).

Sie können in der Amazon Fraud Detector-Konsole einen Detektor erstellen, indem Sie den [PutDetector](#) API, unter Verwendung der [Put-Detektor](#) Befehl oder mit dem AWSSDK. Wenn Sie eine API, einen Befehl oder ein SDK verwenden, um einen Detektor zu erstellen, folgen Sie nach der Erstellung des Melders den Anweisungen zu [Erstellen Sie eine Detektorversion](#).

## Erstellen Sie einen Detektor in der Amazon Fraud Detector-Konsole

In diesem Beispiel wird davon ausgegangen, dass Sie einen Ereignistyp erstellt und auch eine Modellversion erstellt und bereitgestellt haben, die Sie für die Betrugsprognose verwenden möchten.

## Schritt 1: Detektor bauen

1. Wählen Sie im linken Navigationsbereich der Amazon Fraud Detector-Konsole Detektoren.
2. Wählen Sie Detektor erstellen.
3. In der Definieren Sie die Detektordetails-Seite, eingeben `sample_detector` für den Namen des Detektors. Geben Sie optional eine Beschreibung für den Detektor ein, z. B. `my sample fraud detector`.
4. Für Art des Ereignisses, wählen Sie den Ereignistyp aus, den Sie für die Betrugsprognose erstellt haben.
5. Wählen Sie Weiter aus.

## Schritt 2: Hinzufügen einer bereitgestellten Modellversion

1. Beachten Sie, dass dies ein optionaler Schritt ist. Sie müssen Ihrem Detektor kein Modell hinzufügen. Um diesen Schritt zu überspringen, wählen Sie Next (Weiter).
2. In der Modell hinzufügen — optional, wählen Sie Modell hinzufügen.
3. In der Modell hinzufügen-Seite, für Modell wählen, wählen Sie den Amazon Fraud Detector-Modellnamen, den Sie zuvor bereitgestellt haben. Für Version wählen, wählen Sie die Modellversion des bereitgestellten Modells.
4. Wählen Sie Add model aus.
5. Wählen Sie Weiter aus.

## Schritt 3: Regeln hinzufügen

Eine Regel ist eine Bedingung, die Amazon Fraud Detector mitteilt, wie Variablenwerte bei der Auswertung zur Betrugsprognose zu interpretieren sind. In diesem Beispiel werden drei Regeln erstellt, bei denen die Modellwerte als Variablenwerte verwendet werden: `high_fraud_risk`, `medium_fraud_risk`, und `low_fraud_risk`. Verwenden Sie Werte, die für Ihr Modell und Ihren Anwendungsfall geeignet sind, um Ihre eigenen Regeln, Regelausdrücke, Regelausführungsreihenfolge und Ergebnisse zu erstellen.

1. In der Regeln hinzufügen-Seite, unter Definieren Sie eine Regel, geben Sie ein `high_fraud_risk` für den Regelnamen und unter Beschreibung — optional, geben Sie ein **This rule captures events with a high ML model score** als Beschreibung für die Regel.

- In **Ausdruck**, geben Sie mithilfe der vereinfachten Regelausdruckssprache von Amazon Fraud Detector den folgenden Regelausdruck ein:

```
$sample_fraud_detection_model_insightscore > 900
```

- In **Ergebnisse**, wähle **Erstellen** Sie ein neues Ergebnis. Ein Ergebnis ist das Ergebnis einer Betrugsprognose und wird zurückgegeben, wenn die Regel bei einer Bewertung zutrifft.
- In **Erstellen** Sie ein neues Ergebnis, geben Sie ein **verify\_customers** als Name des Ergebnisses. Geben Sie optional eine Beschreibung ein.
- Wähle **Ergebnis speichern**.
- Wähle **Regel hinzufügen** um den Regelüberprüfungsprogramm auszuführen und die Regel zu speichern. Nach der Erstellung stellt Amazon Fraud Detector die Regel zur Verwendung in Ihrem Detektor zur Verfügung.
- Wähle **Eine weitere Regel hinzufügen**, und wählen Sie dann die **Regel erstellen** Tab.
- Wiederholen Sie diesen Vorgang noch zweimal, um Ihre **medium\_fraud\_risk** und **low\_fraud\_risk** Regeln, die die folgenden Regeldetails verwenden:

- mittleres Betrugsrisiko

Name der Regel: **medium\_fraud\_risk**

Ergebnis: **review**

Ausdruck:

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

```
$sample_fraud_detection_model_insightscore > 700
```

- niedriges Betrugsrisiko

Name der Regel: **low\_fraud\_risk**

Ergebnis: **approve**

Ausdruck:

```
$sample_fraud_detection_model_insightscore <= 700
```

- ~~9. Nachdem Sie alle Regeln für Ihren Anwendungsfall erstellt haben, wählen Sie **Weiter**.~~



Weitere Informationen zum Erstellen und Schreiben von Regeln finden Sie unter [Regeln](#) und [Referenz zur Regelsprache](#).

## Schritt 4: Regelausführung und Regelreihenfolge konfigurieren

Der Regelausführungsmodus für die Regeln, die im Detektor enthalten sind, bestimmt, ob alle von Ihnen definierten Regeln ausgewertet werden oder ob die Regelauswertung bei der ersten übereinstimmenden Regel beendet wird. Und die Reihenfolge der Regeln bestimmt die Reihenfolge, in der die Regel ausgeführt werden soll.

Der Standardausführungsmodus für Regeln ist `FIRST_MATCHED`.

### Erstes Spiel

Der Ausführungsmodus für die erste übereinstimmende Regel gibt die Ergebnisse für die erste übereinstimmende Regel auf der Grundlage der definierten Regelreihenfolge zurück. Wenn Sie `FIRST_MATCHED` angeben bewertet Amazon Fraud Detector die Regeln nacheinander von der ersten bis zur letzten und stoppt dabei bei der ersten übereinstimmenden Regel. Amazon Fraud Detector liefert dann die Ergebnisse für diese einzelne Regel.

Die Reihenfolge, in der Sie Regeln ausführen, kann sich auf das Ergebnis der Betrugsprognose auswirken. Nachdem Sie Ihre Regeln erstellt haben, ordnen Sie die Regeln neu an, um sie in der gewünschten Reihenfolge auszuführen, indem Sie die folgenden Schritte ausführen:

Wenn die Regel `high_fraud_risk` steht noch nicht ganz oben auf Ihrer Regelliste, wählen Sie `Bestellung`, und wählen Sie dann `1`. Das bewegt die Regel `high_fraud_risk` zur ersten Position.

Wiederholen Sie diesen Vorgang, damit die Regel `medium_fraud_risk` an zweiter Stelle und die Regel `low_fraud_risk` an dritter Stelle.

### Alle stimmen überein

Der Ausführungsmodus „Alle übereinstimmenden Regeln“ gibt unabhängig von der Reihenfolge der Regeln Ergebnisse für alle übereinstimmenden Regeln zurück. Wenn Sie `ALL_MATCHED` angeben, bewertet Amazon Fraud Detector alle Regeln und gibt die Ergebnisse für alle übereinstimmenden Regeln zurück.

Auswählen `FIRST_MATCHED` für dieses Tutorial und wähle dann `Weiter`.

## Schritt 5: Überprüfen und erstellen Sie die Detektorversion

Eine Detektorversion definiert die spezifischen Modelle und Regeln, die für die Generierung von Betrugsprognosen verwendet werden.

1. In der Überprüfen und erstellen Seite, überprüfen Sie die Melderdetails, Modelle und Regeln, die Sie konfiguriert haben. Wenn Sie Änderungen vornehmen müssen, wählen Sie Bearbeiten neben dem entsprechenden Abschnitt.
2. Wähle Detektor erstellen. Nach der Erstellung erscheint die erste Version Ihres Melders in der Tabelle mit den Detektorversionen mit Draft Status.

Du benutzt die Entwurf Version, um Ihren Detektor zu testen.

## Erstellen Sie einen Detektor mit dem AWS SDK for Python (Boto3)

Das folgende Beispiel zeigt eine Beispielanfrage für den PutDetector API. Ein Detektor fungiert als Container für Ihre Detektorversionen. Der PutDetector Die API gibt an, welchen Ereignistyp der Detektor auswertet. Im folgenden Beispiel wird davon ausgegangen, dass Sie einen Ereignistyp erstellt haben. `sample_registration`.

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

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

## Erstellen Sie eine Detektorversion

Eine Detektorversion definiert die Regeln, die Reihenfolge der Regelausführung und optional eine Modellversion, die als Teil der Anfrage zur Generierung von Betrugsprognosen verwendet wird. Sie können jede der in einem Detektor definierten Regeln zur Detektorversion hinzufügen. Sie können auch jedes Modell hinzufügen, das für den ausgewerteten Ereignistyp trainiert wurde.

Jede Detektorversion hat einen Status von DRAFT, ACTIVE, oder INACTIVE. Es kann nur eine Detektorversion enthalten sein ACTIVE Status nach dem anderen. Während

der `GetEventPredictionAnfrage`, Amazon Fraud Detector verwendet den `ACTIVE` Detektor falls `DetectorVersion` ist spezifiziert.

## Modus zur Regelausführung

Amazon Fraud Detector unterstützt zwei verschiedene Regelausführungsmodi: `FIRST_MATCHED` und `ALL_MATCHED`.

- Wenn der Regelausführungsmodus lautet `FIRST_MATCHED` bewertet Amazon Fraud Detector die Regeln sequentiell, zuerst nach der letzten, und stoppt bei der ersten übereinstimmenden Regel. Amazon Fraud Detector liefert dann die Ergebnisse für diese einzelne Regel. Wenn eine Regel als falsch (nicht übereinstimmend) ausgewertet wird, wird die nächste Regel in der Liste ausgewertet.
- Wenn der Regelausführungsmodus lautet `ALL_MATCHED`, dann werden alle Regeln in einer Auswertung unabhängig von ihrer Reihenfolge parallel ausgeführt. Amazon Fraud Detector führt alle Regeln aus und gibt die definierten Ergebnisse für jede übereinstimmende Regel zurück.

## Erstellen Sie eine Detektorversion mit dem AWS SDK for Python (Boto3)

Das folgende Beispiel zeigt eine Beispielanfrage für den `CreateDetectorVersionAPI`. Der Regelausführungsmodus ist eingestellt auf `FIRST_MATCHED`, daher bewertet Amazon Fraud Detector die Regeln sequentiell, zuerst nach der letzten, und stoppt bei der ersten übereinstimmenden Regel. Amazon Fraud Detector liefert dann die Ergebnisse für diese einzelne Regel während des `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'
)
```

Um den Status einer Detektorversion zu aktualisieren, verwenden Sie `updateDetectorVersionStatusAPI`. Das folgende Beispiel aktualisiert den Versionsstatus des Detektors von `DRAFT` zu `ACTIVE`. Während einer `GetEventPredictionAnfrage`, wenn keine Melder-ID angegeben ist, verwendet Amazon Fraud Detector die `ACTIVE` Version des Detektors.

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

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

## Löschen Sie einen Detektor, eine Detektorversion oder eine Regelversion

Bevor Sie einen Detektor in Amazon Fraud Detector löschen, müssen Sie zuerst alle Detektorversionen und Regelversionen löschen, die dem Detektor zugeordnet sind.

Wenn Sie einen Detektor, eine Detektorversion oder eine Regelversion löschen, löscht Amazon Fraud Detector diese Ressource dauerhaft und die Daten werden nicht mehr in Amazon Fraud Detector gespeichert.

## So löschen Sie eine Detektorversion

Sie können nur Detektorversionen löschen, die sich im `INACTIVE` Status `DRAFT` oder im Status `INACTIVE` befinden.

1. Melden sich bei der Amazon Fraud Detektorkonsole unter <https://console.aws.amazon.com/frauddetector> an AWS Management Console und öffnen die Amazon Fraud Detector Detektorkonsole unter <https://console.aws.amazon.com/frauddetector>.
2. Wählen im linken Navigationsbereich der Amazon Fraud Detector Detektorkonsole die Option `Detektoren`.
3. Wählen Sie den Melder aus, der die Melderversion enthält, die Sie löschen möchten.
4. Wählen die Detektorversion, die die Sie löschen möchten.
5. Wählen Sie `Actions` (Aktionen) und anschließend `Delete` (Löschen).
6. Geben Sie `delete` ein, und wählen Sie dann `Detektor löschen`.

## So löschen Sie eine Regelversion

Sie können eine Regelversion nur löschen, wenn sie von keiner `ACTIVE` oder `INACTIVE` Detector-Versionen verwendet wird. Falls erforderlich, verschieben Sie vor dem Löschen einer Regelversion zunächst die `ACTIVE` Melderversion auf `INACTIVE` und löschen Sie dann die `INACTIVE` Melderversion.

1. Wählen im linken Navigationsbereich der Amazon Fraud Detector Detektorkonsole die Option `Detektoren`.
2. Wählen den Detektor, der die Regelversion, die Sie löschen möchten.
3. Wählen die Registerkarte `Zugeordnete Regeln` und wählen die Regel, die Sie löschen möchten.
4. Wählen die Regelversion, die Sie löschen möchten.
5. Wählen Sie `Aktionen` und dann `Regelversion löschen` aus.
6. Geben Sie `delete` ein, und wählen Sie dann `Version löschen`.

## Um einen Melder zu löschen

Bevor Sie einen Detektor löschen, müssen Sie zuerst alle Detektorversionen und Regelversionen löschen, die dem Detektor zugeordnet sind.

1. Wählen im linken Navigationsbereich der Amazon Fraud Detector Detektorkonsole die Option **Detektoren**.
2. Wählen den Detektor, den den den den den Sie möchten möchten.
3. Wählen Sie Aktionen und dann Detektor löschen.
4. Geben Sie **eindelete**, und wählen Sie dann Detektor löschen.

# Ressourcen

Modelle, Regeln und Detektoren verwenden Ressourcen wie Variablen, Ergebnisse, Bezeichnungen, Listen und Entitäten, um Ereignisse hinsichtlich des Betrugsrisikos zu bewerten. In diesem Abschnitt finden Sie Informationen zum Erstellen und Verwalten der Ressourcen.

Themen

- [Variablen](#)
- [Bezeichnungen](#)
- [Regeln](#)
- [Listen](#)
- [Ergebnisse](#)
- [Entität](#)
- [Verwalten Sie die Ressourcen von Amazon Fraud Detector mit AWS CloudFormation](#)

## Variablen

Variablen stellen Datenelemente dar, die Sie in einer Betrugsprognose verwenden möchten. Diese Variablen können dem Ereignisdatensatz entnommen werden, den Sie für das Training Ihres Modells vorbereitet haben, aus den Risikobewertungsdaten Ihres Amazon Fraud Detector-Modells oder aus SageMaker Amazon-Modellen. Weitere Hinweise zu Variablen aus dem Event-Dataset finden Sie unter [Rufen Sie die Anforderungen für Ereignisdatensätze mit dem Datenmodell-Explorer ab](#).

Die Variablen, die Sie in Ihrer Betrugsprognose verwenden möchten, müssen zuerst erstellt und dann dem Ereignis hinzugefügt werden, wenn Sie Ihren Ereignistyp erstellen. Jeder Variablen, die Sie erstellen, muss ein Datentyp, ein Standardwert und optional ein Variablentyp zugewiesen werden. Amazon Fraud Detector erweitert einige der von Ihnen bereitgestellten Variablen wie IP-Adressen, Bankidentifikationsnummern (BINs) und Telefonnummern, um zusätzliche Eingaben zu erstellen und die Leistung der Modelle zu steigern, die diese Variablen verwenden.

## Datentypen

Variablen müssen einen Datentyp für das Datenelement haben, das die Variable darstellt, und sie können optional einem der vordefinierten Datentypen zugewiesen werden [Variablentypen](#).

Für Variablen, die einem Variablentyp zugewiesen sind, ist der Datentyp vorausgewählt. Zu den möglichen Datentypen gehören die folgenden Typen:

Datentyp	Beschreibung	Standardwert	Beispielwerte
Zeichenfolge	Beliebige Kombination aus Buchstaben, ganzen Zahlen oder beidem	<empty>	abc, 123, 1D3B
Ganzzahl	Positive oder negative ganze Zahlen	0	1, -1
Boolesch	Wahr oder Falsch	Falsch	Wahr, Falsch
DateTime	Datum und Uhrzeit sind nur im UTC-Format nach ISO 8601 angegeben	<empty>	2019-11-30T 13:01:01 Z
Gleitkommazahl	Zahlen mit Dezimalstellen	0.0	4,01, 0,10

## Standardwert

Variablen müssen einen Standardwert haben. Wenn Amazon Fraud Detector Betrugsprognosen generiert, wird dieser Standardwert verwendet, um eine Regel oder ein Modell auszuführen, falls Amazon Fraud Detector keinen Wert für eine Variable erhält. Die von Ihnen angegebenen Standardwerte müssen dem ausgewählten Datentyp entsprechen. In der AWS-Konsole weist Amazon Fraud Detector den Standardwert von 0 für Ganzzahlen, für Boolesche Werte, false für Fließkommazahlen und (leer) 0.0 für Zeichenketten zu. Sie können für jeden dieser Datentypen einen benutzerdefinierten Standardwert festlegen.

## Variablentypen

Wenn Sie eine Variable erstellen, können Sie die Variable optional einem Variablentyp zuweisen. Der Variablentyp stellt die allgemeinen Datenelemente dar, die zum Trainieren von Modellen und zur Generierung von Betrugsprognosen verwendet werden. Nur Variablen mit einem zugehörigen Variablentyp können für das Modelltraining verwendet werden. Als Teil des Modelltrainingsprozesses



verwendet Amazon Fraud Detector den mit der Variablen verknüpften Variablentyp, um Variablenanreicherungen, Feature-Engineering und Risikobewertungen durchzuführen.

Amazon Fraud Detector hat die folgenden Variablentypen vordefiniert, die verwendet werden können, um sie Ihren Variablen zuzuweisen.

Kategorie	Variablentyp	Beschreibung	Datentyp	Beispiel
Sitzung	IPADDRESS	Die IP-Adresse, die während der Veranstaltung gesammelt wurde	Zeichensymbol	192.168.0.2.0 Hinweis: Amazon Fraud Detector reichert diese Daten an. Weitere Informationen finden Sie unter <a href="#">Anreicherung der Geolokalisierung</a>
BENUTZER	AGENT	Der Benutzeragent, der während der Veranstaltung gesammelt wurde	Zeichensymbol	Mozilla/5.0 (Windows NT 10.0; Win64; x64,

Kategorie	Variablentyp	Beschreibung	Datentyp	Beispiel
				rv: 68.0) Gecko 20100101
	FINGERABIRUCK	Die eindeutige Kennung für ein Gerät, das für die Veranstaltung verwendet wird	Zeichensfolge	sa9fow987u234
	SESSION_ID	Die Sitzungs-ID für die aktive Sitzung des Events	Zeichensfolge	sicfo123456789
	SIND_ANMELDUNGEN_GÜLTIG	Gibt an, ob die für die Event-Anmeldung verwendeten Anmeldeinformationen gültig sind	Boolean	Wahr
Beispiel	EMAIL_ADRESSE	Die E-Mail-Adresse, die während der Veranstaltung gesammelt wurde	Zeichensfolge	abc@domain.com

Kategorie	Variablentyp	Beschreibung	Datentyp	Beispiel
	PHONE_NUMBER	Die während der Veranstaltung gesammelte Telefonnummer	Zeichensymbol	+1555-0100  Hinweis: Amazon Fraud Detector reichert diese Daten an. Weitere Informationen finden Sie unter <a href="#">Anreicherung von Telefonnummern</a>
Funktion	ABRECHNUNGSGSNAME	Der Name, der mit der Rechnungsadresse verknüpft ist	Zeichensymbol	Haar-Muster

Ka	Variablen typ	Beschreibung	Date	Be
	ABRECHNUNGSTELEFONNUMMERN	Die Telefonnummer, die mit der Rechnungsadresse verknüpft ist	Zeichenslange	+1555-0100  Hinweis: Amazon Fraud Detector reichert diese Daten an. Weitere Informationen finden Sie unter <a href="#">Anreicherung von Telefonnummern</a>
	RECHNUNGSADRESSE_1	Die erste Zeile der Rechnungsadresse	Zeichenslange	Jeff Straße
	RECHNUNGSADRESSE_2	Die zweite Zeile der Rechnungsadresse	Zeichenslange	Jeff Einheit 123
	BILLING_CITY	Die Stadt, die in der Rechnungsadresse steht	Zeichenslange	Bellevue Stadt

Ka	Variablen typ	Beschreibung	Date	Be
	ABRECHNUNG STATUS	Der Bundesstaat oder die Provinz, der in der Rechnungsadresse steht	Zeichensymbol	Jeder Bundesstaat oder jede Provinz
	ABRECHNUNG SLAND	Das Land, das in der Rechnungsadresse steht	Zeichensymbol	Irgendein Land  Hinweis: Amazon Fraud Detector reichert diese Daten an. Weitere Informationen finden Sie unter <a href="#">Anreicherung der Geolokalisierung</a>

Kategorie	Variablentyp	Beschreibung	Datentyp	Beispiel
	ABRECHNUNG_ZIP	Die Postleitzahl, die in der Rechnungsadresse steht	Zeichensymbol	01234 Hinweis: Amazon Fraud Detector reichert diese Daten an. Weitere Informationen finden Sie unter <a href="#">Anreicherung der Geolokalisierung</a>
Verpackung	VERSANDNAME	Der Name, der mit der Lieferadresse verknüpft ist	Zeichensymbol	Häufiges Muster

Kategorie	Variablentyp	Beschreibung	Datentyp	Beispiel
	VERSANDNUMMER	Die Telefonnummer, die mit der Lieferadresse verknüpft ist	Zeichensymbol	+1555-0100  Hinweis: Amazon Fraud Detector reichert diese Daten an. Weitere Informationen finden Sie unter <a href="#">Anreicherung von Telefonnummern</a>
	LIEFERADRESSE_L1	Die erste Zeile der Lieferadresse	Zeichensymbol	123 Any Street
	LIEFERADRESSE_L2	Die zweite Zeile der Lieferadresse	Zeichensymbol	Einheit 123
	VERSANDSTADT	Die Stadt, die in der Lieferadresse steht	Zeichensymbol	Beliebige Stadt

Kategorie	Variablentyp	Beschreibung	Datentyp	Beispiel
	VERSANDSTATUS	Der Bundesstaat oder die Provinz, der in der Lieferadresse steht	Zeichensymbol	Irgendein Bundesstaat
	LIEFERLANDID	Das Land, in dem sich das befindet, steht in der Lieferadresse	Zeichensymbol	Irgendein Land  Hinweis: Amazon Fraud Detector reichert diese Daten an. Weitere Informationen finden Sie unter <a href="#">Anreicherung der Geolokalisierung</a>



Kategorie	Variablentyp	Beschreibung	Datentyp	Beispiel
	VERSAND_IP	Die Postleitzahl, die in der Lieferadresse steht	Zeichengebiet	01234 Hinweis: Amazon Fraud Detector reichert diese Daten an. Weitere Informationen finden Sie unter <a href="#">Anreicherung der Geolokalisierung</a>
Payment	ORDER_ID (Zahlung)	Die eindeutige Kennung für die Transaktion	Zeichengebiet	LUX60
	PREIS	Der Gesamtbestellpreis	Zeichengebiet	560,00
	WÄHRUNG_CODE	Der ISO-4217-Währungscode	Zeichengebiet	USD

Kategorie	Variablentyp	Beschreibung	Datentyp	Beispiel
Kreditkarte	ZAHLUNGSMETHODE	Die Zahlungsmethode, die für die Zahlung während der Veranstaltung verwendet wird	Zeichensymbol	Kreditkarte
	AUTH_CODE	Der alphanumerische Code, der von einem Kreditkartenaussteller oder einer ausstellenden Bank gesendet wird	Zeichensymbol	0000
	AVS	Der Antwortcode des Adressverifikationssystems (AVS) vom Kartenprozessor	Zeichensymbol	Yfolge
Produkt	PRODUKT_KATEGORIE	Die Produktkategorie des Bestellartikels	Zeichensymbol	Küchengerät
Benutzerdefiniert	NUMERISCH	Jede Variable, die als reelle Zahl dargestellt werden kann	Gleichwertig	1.234
	KATEGORIAL	Jede Variable, die Kategorie, Segmente oder Gruppen beschreibt	Zeichensymbol	Large (Groß)

Kategorie	Variablentyp	Beschreibung	Datentyp	Beispiel
	FREIE_FOF	Jeder Freiformtext, der im Rahmen der Veranstaltung erfasst wurde (z. B. eine Kundenbewertung oder ein Kommentar)	Zeichensfolge	Beispiel für eine Texteingabe in freier Form

## Variablen einem Variablentyp zuweisen

Wenn Sie planen, eine Variable für das Training Ihres Modells zu verwenden, ist es wichtig, dass Sie den richtigen Variablentyp auswählen, der der Variablen zugewiesen wird. Eine falsche Zuweisung von Variablentypen kann sich negativ auf Ihre Modellleistung auswirken. Es kann für Sie auch sehr schwierig werden, die Zuweisung später zu ändern, insbesondere wenn mehrere Modelle und Ereignisse die Variable verwendet haben.


Sie können Ihrer Variablen einen der vordefinierten Variablentypen oder einen der benutzerdefinierten Variablentypen zuweisen —`FREE_FORM_TEXT`, `CATEGORICAL`, oder `NUMERIC`.

### Wichtige Hinweise zur Zuordnung von Variablen zu den richtigen Variablentypen

1. Wenn die Variable einem der vordefinierten Variablentypen entspricht, verwenden Sie sie. Stellen Sie sicher, dass der Variablentyp der Variablen entspricht. Wenn Sie beispielsweise eine `ip_address`-Variable einem Variablentyp zuweisen, wird die `EMAIL_ADDRESS` Variable `ip_address` nicht mit Anreicherungen wie ASN, ISP, Geolokalisierung und Risikobewertung angereichert. Weitere Informationen finden Sie unter [Variable Anreicherungen](#).
2. Wenn die Variable keinem der vordefinierten Variablentypen entspricht, folgen Sie den unten aufgeführten Empfehlungen, um einen der benutzerdefinierten Variablentypen zuzuweisen.
3. Weisen Sie `CATEGORICAL` Variablen, die normalerweise keine natürliche Reihenfolge haben und in Kategorien, Segmente oder Gruppen unterteilt werden können, einen Variablentyp zu. Der Datensatz, den Sie zum Trainieren Ihres Modells verwenden, kann ID-Variablen wie `merchant_id`, `campaign_id` oder `policy_id` enthalten. Diese Variablen stellen Gruppen dar (zum Beispiel stehen

alle Kunden mit derselben Policy\_ID für eine Gruppe). Variablen mit den folgenden Daten muss der Variablentyp CATEGORICAL zugewiesen werden -

- Variablen, die Daten wie Customer\_ID, Segment\_ID, Color\_ID, Department\_Code oder Product\_ID enthalten.
- Variablen, die boolesche Daten mit den Werten „Wahr“, „Falsch“ oder „Null“ enthalten.
- Variablen, die in Gruppen oder Kategorien wie Firmenname, Produktkategorie, Kartentyp oder Empfehlungsmedium eingeteilt werden können.

 Note

ENTITY\_ID ist ein reservierter Variablentyp, der von Amazon Fraud Detector verwendet wird, um einer ENTITY\_ID-Variablen zuzuweisen. Die Variable ENTITY\_ID ist die ID der Entität, die die Aktion initiiert, die Sie auswerten möchten. Wenn Sie einen Transaction Fraud Insight (TFI) -Modelltyp erstellen, müssen Sie die Variable ENTITY\_ID angeben. Sie müssen entscheiden, welche Variable in Ihren Daten die Entität, die die Aktion initiiert, eindeutig identifiziert und sie als ENTITY\_ID-Variable weiterleiten. Weisen Sie allen anderen IDs in Ihrem Datensatz den Variablentyp CATEGORICAL zu, sofern sie vorhanden sind und Sie sie für das Modelltraining verwenden. Beispiele für andere IDs, die keine Entität in Ihrem Datensatz sind, können Merchant\_ID, Policy\_ID und Campaign\_ID sein.

4. Weisen Sie FREE\_FORM\_TEXT Variablen, die einen Textblock enthalten, einen Variablentyp zu. Beispiele für FREE\_FORM\_TEXT-Variablentypen sind — Benutzerrezensionen, Kommentare, Daten und EmpfehlungsCodes. Die FREE\_FORM\_TEXT-Daten enthalten mehrere Token, die durch ein Trennzeichen getrennt sind. Bei den Trennzeichen kann es sich um ein beliebiges Zeichen mit Ausnahme von alphanumerischen Zeichen und Unterstrichen handeln. Beispielsweise können Benutzerrezensionen und Kommentare durch ein Leerzeichen getrennt werden, Daten und EmpfehlungsCodes können Bindestriche als Trennzeichen verwenden, um Präfix, Suffix und dazwischen liegende Teile voneinander zu trennen. Amazon Fraud Detector verwendet die Trennzeichen, um Daten aus FREE\_FORM\_TEXT-Variablen zu extrahieren.
5. Weisen Sie Variablen, die reelle Zahlen sind und eine inhärente Reihenfolge haben, den Variablentyp NUMERIC zu. Beispiele für NUMERISCHE Variablen sind day\_of\_the\_week, incident\_severity, customer\_rating. Sie können diesen Variablen zwar den Variablentyp CATEGORICAL zuweisen, es wird jedoch dringend empfohlen, alle reellen Zahlen mit inhärenter Reihenfolge dem Variablentyp NUMERIC zuzuweisen.

## Variable Anreicherungen

Amazon Fraud Detector erweitert einige der von Ihnen bereitgestellten Rohdatenelemente wie IP-Adressen, Bank-Identifikationsnummern (BINs) und Telefonnummern, um zusätzliche Eingaben zu erstellen und die Leistung der Modelle zu steigern, die diese Datenelemente verwenden. Die Anreicherung hilft dabei, potenziell verdächtige Situationen zu identifizieren und den Modellen zu helfen, mehr Betrugsfälle zu erkennen.

### Anreicherung von Telefonnummern

Amazon Fraud Detector reichert die Telefonnummerndaten mit zusätzlichen Informationen an, die sich auf den Standort, den ursprünglichen Mobilfunkanbieter und die Gültigkeit der Telefonnummer beziehen. Die Anreicherung von Telefonnummern wird automatisch für alle Models aktiviert, die am oder nach dem 13. Dezember 2021 trainiert wurden und deren Telefonnummer eine Landesvorwahl (+xxx) enthält. Wenn Sie eine Rufnummernvariable in Ihr Modell aufgenommen und es vor dem 13. Dezember 2021 trainiert haben, schulen Sie Ihr Modell neu, damit es diese Erweiterung nutzen kann.

Wir empfehlen Ihnen dringend, das folgende Format für Telefonnummernvariablen zu verwenden, um sicherzustellen, dass Ihre Daten erfolgreich angereichert werden.

Variable	Format	Beschreibung
PHONE_NUMBER	Der <a href="#">E.164-Standard</a>	Achten Sie darauf, die Landesvorwahl (+xxx) bei der Telefonnummer anzugeben.
BILLING_PHONE und SHIPPING_PHONE	Der <a href="#">E.164-Standard</a>	Achten Sie darauf, die Landesvorwahl (+xxx) bei der Telefonnummer anzugeben.

### Anreicherung der Geolokalisierung

Ab dem 8. Februar 2022 berechnet Amazon Fraud Detector die physische Entfernung zwischen den Werten IP\_ADDRESS, BILLING\_ZIP und SHIPPING\_ZIP, die Sie für ein Ereignis angeben. Die berechneten Entfernungen werden als Eingaben für Ihr Betrugserkennungsmodell verwendet.

Um die Geolocation Enrichment zu aktivieren, müssen Ihre Eventdaten mindestens zwei der drei Variablen enthalten: IP\_ADDRESS, BILLING\_ZIP oder SHIPPING\_ZIP. Darüber hinaus muss jeder BILLING\_ZIP- und SHIPPING\_ZIP-Wert jeweils einen gültigen BILLING\_COUNTRY-Code bzw. SHIPPING\_COUNTRY-Code haben. Wenn Sie ein Modell haben, das vor dem 8. Februar 2022 trainiert wurde und es diese Variablen enthält, müssen Sie das Modell neu trainieren, um die Geolokationsanreicherung zu ermöglichen.

Wenn Amazon Fraud Detector den Standort, der mit den IP\_ADDRESS-, BILLING\_ZIP- oder SHIPPING\_ZIP-Werten für ein Ereignis verknüpft ist, nicht ermitteln kann, weil die Daten ungültig sind, wird stattdessen ein spezieller Platzhalterwert verwendet. Nehmen wir beispielsweise an, dass ein Ereignis gültige IP\_ADDRESS- und BILLING\_ZIP-Werte hat, der Wert SHIPPING\_ZIP jedoch nicht gültig ist. In diesem Fall erfolgt die Anreicherung nur für IP\_ADDRESS—> BILLING\_ZIP. Die Anreicherung erfolgt nicht für IP\_ADDRESS—>SHIPPING\_ZIP und BILLING\_ZIP—>SHIPPING\_ZIP. Stattdessen werden die Platzhalterwerte an ihrer Stelle verwendet. Unabhängig davon, ob die Geolocation Enrichment für Ihr Modell aktiviert ist oder nicht, die Leistung Ihres Modells ändert sich nicht.

Sie können die Geolokationsanreicherung deaktivieren, indem Sie Ihre Variablen BILLING\_ZIP und SHIPPING\_ZIP dem Variablentyp CUSTOM\_CATEGORICAL zuordnen. Eine Änderung des Variablentyps wirkt sich nicht auf die Leistung Ihres Modells aus.

### Variablenformat für Geolokalisierung

Wir empfehlen Ihnen dringend, das folgende Format für Geolokalisierungsvariablen zu verwenden, um sicherzustellen, dass Ihre Standortdaten erfolgreich angereichert werden.

Variable	Format	Beschreibung
IP_ADDRESS	<a href="#">IPv4-Adresse</a>	Zum Beispiel - 1.1.1.1
BILLING_ZIP und SHIPPING_ZIP	Die <a href="#">ISO 3166-1 Alpha-2-Postleitzahl</a> für das angegebene Land	Weitere Informationen finden Sie im Abschnitt Länder- und Gebietsverwaltung in diesem Thema.
BILLING_COUNTRY und SHIPPING_COUNTRY	Der zweibuchstabile Standard-Ländercode <a href="#">nach ISO 3166-1 Alpha-2</a>	Weitere Informationen finden Sie im Abschnitt Länder- und Gebietsverwaltung in diesem Thema.

Variable	Format	Beschreibung
SHIPPING_COUNTRY		rwahlen in diesem Thema. Amazon Fraud Detector versucht, alle gängigen Varianten des Namens eines Landes dem aus zwei Buchstaben bestehenden ISO-3166-1-Standard-Ländercode zuzuordnen. Wir können jedoch nicht garantieren, dass sie korrekt zugeordnet werden.

## Länder- und Gebietsvorwahlen

Die folgende Tabelle enthält eine vollständige Liste der Länder und Gebiete, die von Amazon Fraud Detector für die Anreicherung von Geolokationen unterstützt werden. Jedem Land und Gebiet ist ein Ländercode (insbesondere der zweibuchstabile Ländercode nach ISO 3166-1 Alpha-2) und eine Postleitzahl zugewiesen.

## Format der Postleitzahl

- 9 - Zahl
- a - Buchstabe
- [X] - X ist optional. Guernsey „GY9 [9] 9aa“ bedeutet beispielsweise, dass sowohl „GY9 9aa“ als auch „GY99 9aa“ gültig sind. Verwenden Sie ein Format.
- [X/XX] — entweder X oder XX können verwendet werden. Zum Beispiel bedeutet Bermuda „aa [aa/99]“, dass sowohl „aa aa“ als auch „aa 99“ gültig sind. Verwenden Sie eines dieser Formate, aber nicht beide.
- Einige Länder haben ein festes Präfix. Die Postleitzahl für Andorra ist beispielsweise AD999. Das bedeutet, dass die Landesvorwahl mit den Buchstaben AD beginnen muss, gefolgt von drei Zahlen.

Code	Name	PLZ
AD	Andorra	AD999
AR	Niederländische Antillen	9999
AT	Österreich	9999
AU	Australien	9999
AZ	Aserbaidshan	AB 999
BD	Bangladesch	9999
BE	Belgien	9999
BG	Bulgarien	9999
BM	Bermuda	aa [aa/99]
BY	Belarus	999999
CA	Kanada	a9a 9a9
CH	Schweiz	9999
CL	Chile	9999999
CO	Kolumbien	999999
CR	Costa Rica	99999
CY	Zypern	9999
CZ	Tschechien	99 99
DE	Deutschland	99999
DK	Dänemark	9999
DO	Dominikanische Republik	99999



Code	Name	PLZ
DZ	Algerien	99999
EE	Estland	99999
ES	Spanien	99999
FI	Finnland	99999
FM	Föderierte Staaten von Mikronesien	99999
FO	Färöer-Inseln	999
FR	Frankreich	99999
GB	Großbritannien und Nordirland	[a] 9 [a/9] 9aa
GG	Guernsey	GY9 [9] 9aa
GL	Grönland	9999
GP	Guadeloupe	99999
GT	Guatemala	99999
GU	Guam	99999
HR	Kroatien	99999
HU	Ungarn	9999
IE	Irland	a99 [a/9] [a/9] [a/9] [a/9]
IM	Isle of Man	IM9 [9] 9aa
IN	Indien	999999
IS	Island	999
IT	Italien	99999

Code	Name	PLZ
JE	Jersey	JE9 [9] 9aa
JP	Japan	999-9999
KR	Republik Korea	99999
LI	Liechtenstein	9999
LK	Sri Lanka	99999
LT	Litauen	99999
LU	Luxemburg	L-999
LV	Lettland	LV-9999
MC	Monaco	99999
MD	Republik Moldawien	9999
MH	Marshallinseln	99999
MK	Nordmazedonien	9999
MP	Nördliche Marianen	99999
MQ	Matinique	99999
MT	Malta	aaa 999
MX	Mexiko	99999
MY	Malaysia	99999
NL	Niederlande	999 aa
NO	Norwegen	9999
NZ	Neuseeland	9999

Code	Name	PLZ
PH	Philippinen	9999
PK	Pakistan	99999
PL	Polen	99-999
PR	Puerto Rico	99999
PT	Portugal	9999-999
PW	Palau	99999
RE	Wiedersehen	99999
RO	Rumänien	999999
RU	Russische Föderation	999999
SE	Schweden	99 99
SG	Singapur	999999
SI	Slowenien	9999
SK	Slowakei	99 99
SM	San Marino	99999
TH	Thailand	99999
TR	Türkei	99999
UA	Ukraine	99999
USA	Vereinigte Staaten	99999
UY	Uruguay	99999
VI	Amerikanische Jungferninseln	99999

Code	Name	PLZ
WF	Wallis und Futuna	99999
YT	Mayotte	99999
ZA	Südafrika	9999

## Anreicherung durch Useragent

Wenn Sie das Account Takeover Insights (ATI) -Modell erstellen, müssen Sie eine `useragent` Variable des Variablentyps in Ihrem Datensatz angeben. Diese Variable enthält die Browser-, Geräte- und Betriebssystemdaten eines Anmeldeereignisses. Amazon Fraud Detector reichert die Useragent-Daten mit zusätzlichen Informationen wie `user_agent_family`, `device_family` und `an.`

## Erstellen Sie eine Variable

Sie können Variablen in der Amazon Fraud Detector-Konsole erstellen, indem Sie den Befehl [create-variable](#) verwenden [CreateVariable](#), den oder AWS SDK for Python (Boto3)

## Erstellen Sie eine Variable mithilfe der Amazon Fraud Detector-Konsole

In diesem Beispiel werden zwei Variablen `email_address` und `ip_address`, erstellt und sie den entsprechenden Variablentypen (`EMAIL_ADDRESS` und `IP_ADDRESS`) zugewiesen. Diese Variablen werden als Beispiele verwendet. Wenn Sie Variablen für Ihr Modelltraining erstellen, verwenden Sie die Variablen aus Ihrem Datensatz, die für Ihren Anwendungsfall geeignet sind. Lesen Sie unbedingt über [Variablentypen](#) und [Variable Anreicherungen](#) bevor Sie Ihre Variablen erstellen.

Um eine Variable zu erstellen,

1. Öffnen Sie die [AWS Management Console](#) und melden Sie sich bei Ihrem Konto an.
2. Navigieren Sie zu Amazon Fraud Detector, wählen Sie in der linken Navigationsleiste Variablen und dann Erstellen.
3. Geben Sie auf der Seite Neue Variable `email_address` als Variablennamen ein. Geben Sie optional eine Beschreibung der Variablen ein.
4. Wählen Sie im Variablentyp die Option E-Mail-Adresse aus.

5. Amazon Fraud Detector wählt automatisch den Datentyp für diesen Variablentyp aus, da dieser Variablentyp vordefiniert ist. Wenn Ihrer Variablen nicht automatisch ein Variablentyp zugewiesen wird, wählen Sie einen Variablentyp aus der Liste aus. Weitere Informationen finden Sie unter [Variablentypen](#).
6. Wenn Sie einen Standardwert für Ihre Variable angeben möchten, wählen Sie Benutzerdefinierten Standardwert definieren aus und geben Sie einen Standardwert für Ihre Variable ein. Überspringen Sie diesen Schritt, wenn Sie diesem Beispiel folgen.
7. Wählen Sie Erstellen aus.
8. Bestätigen Sie auf der Übersichtsseite `email_address` die Details der Variablen, die Sie gerade erstellt haben.

Wenn Sie ein Update benötigen, wählen Sie Bearbeiten und geben Sie die Updates ein. Wählen Sie Änderungen speichern aus.

9. Wiederholen Sie den Vorgang, um eine weitere Variable zu erstellen, `ip_address` und wählen Sie IP-Adresse für den Variablentyp.
10. Auf der Variablen-Seite werden die neu erstellten Variablen angezeigt.

#### Important

Wir empfehlen, dass Sie aus Ihrem Datensatz so viele Variablen erstellen, wie Sie möchten. Sie können später bei der Erstellung Ihres Ereignistyps entscheiden, welche Variablen Sie einbeziehen möchten, um Ihr Modell zur Betrugserkennung und zur Generierung von Betrugserkennungen zu trainieren.

## Erstellen Sie eine Variable mit dem AWS SDK for Python (Boto3)

Das folgende Beispiel zeigt Anfragen für die [CreateVariable](#) API. Das Beispiel erstellt zwei Variablen `email_address` und `ip_address`, und weist sie den entsprechenden Variablentypen zu (`EMAIL_ADDRESS` und `IP_ADDRESS`).

Diese Variablen werden als Beispiele verwendet. Wenn Sie Variablen für Ihr Modelltraining erstellen, verwenden Sie die Variablen aus Ihrem Datensatz, die für Ihren Anwendungsfall geeignet sind. Lesen Sie unbedingt über [Variablentypen](#) und [Variable Anreicherungen](#) bevor Sie Ihre Variablen erstellen.

Stellen Sie sicher, dass Sie eine variable Quelle angeben. Es hilft zu erkennen, woher der Variablenwert abgeleitet wird. Wenn die Variablenquelle `EVENT` ist, wird der Variablenwert als Teil

der [GetEventPrediction](#)Anfrage gesendet. Wenn der Variablenwert lautet `MODEL_SCORE`, wird er von einem Amazon Fraud Detector aufgefüllt. Wenn `EXTERNAL_MODEL_SCORE`, wird der Variablenwert von einem importierten SageMaker Modell aufgefüllt.

```
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>'
)
```

## Löschen Sie eine Variable

Wenn Sie eine Variable löschen, löscht Amazon Fraud Detector diese Variable dauerhaft und die Daten werden nicht mehr in Amazon Fraud Detector gespeichert.

Sie können keine Variablen löschen, die in einem Ereignistyp in Amazon Fraud Detector enthalten sind. Sie müssen zuerst den Ereignistyp löschen, mit dem die Variable verknüpft ist, und dann die Variable löschen.

Sie können Amazon Fraud Detector-Modellausgabevariablen und SageMaker Modellausgabevariablen nicht manuell löschen. Amazon Fraud Detector löscht automatisch die Modellausgabevariablen, wenn Sie das Modell löschen.

Sie können Variablen in der Amazon Fraud Detector-Konsole löschen, indem Sie den CLI-Befehl [delete-variable](#) verwenden, die [DeleteVariable](#)API verwenden oder AWS SDK for Python (Boto3)

## Löschen Sie die Variable mit der Konsole

Um eine Variable zu löschen,

1. Melden Sie sich bei der Amazon Fraud Detector-Konsole an AWS Management Console und öffnen Sie die Amazon Fraud Detector-Konsole unter <https://console.aws.amazon.com/frauddetector>.
2. Wählen Sie im linken Navigationsbereich der Amazon Fraud Detector-Konsole Ressourcen und dann Variablen aus.
3. Wählen Sie die Variable aus, die Sie löschen möchten.
4. Wählen Sie Actions (Aktionen) und anschließend Delete (Löschen).
5. Geben Sie den Variablennamen ein und wählen Sie dann Variable löschen.

## Löschen Sie die Variable mit dem AWS SDK for Python (Boto3)

Im folgenden Codebeispiel wird eine Variable `customer_name` mithilfe der API gelöscht.

### [DeleteVariable](#)

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

fraudDetector.delete_variable (

name = 'customer_name'

)
```

## Bezeichnungen

Eine Beschriftung klassifiziert ein Ereignis als betrügerisch oder legitim. Beschriftungen werden Ereignistypen zugeordnet und verwendet, um Machine Learning-Modelle in Amazon Fraud Detector zu trainieren. Wenn Sie planen, entweder ein Online Fraud Insights (OFI) oder ein Transaction Fraud Insights (TFI) -Modell zu trainieren, müssen mindestens 400 Ereignisse in Ihrem Trainingsdatensatz als betrügerisch oder legitim eingestuft werden. Sie können beliebige Bezeichnungen wie Fraud, Legit, 1 oder 0 verwenden, um Ereignisse in Ihrem Trainingsdatensatz zu klassifizieren. Nach

Abschluss der Schulung bewertet das trainierte Modell Ereignisse auf Betrug und verwendet diese Werte, um Ereignisse als betrügerisch oder legitim zu klassifizieren.

Sie müssen zuerst die Labels mit den in Ihrem Trainingsdatensatz verwendeten Werten erstellen und dann die Labels dem Ereignistyp zuordnen, der zum Erstellen und Trainieren Ihres Betrugserkennungsmodells verwendet wird.

## Hinzufügen

Sie können Labels in der Amazon Fraud Detector-Konsole erstellen, indem Sie den Befehl [put-label](#), die [PutLabel](#)API oder den verwendenAWS SDK for Python (Boto3).

### Erstellen Sie ein Etikett mit der Amazon Fraud Detector-Konsole

Um Labels zu erstellen,

1. Öffnen Sie die [AWSManagement Console](#) und melden Sie sich bei Ihrem Konto an.
2. Navigieren Sie zu Amazon Fraud Detector, wählen Sie in der linken Navigationsleiste Labels und dann Create.
3. Geben Sie auf der Seite Etikett erstellen Ihren Labelnamen für ein betrügerisches Ereignis als Labelnamen ein. Der Labelname muss der Bezeichnung entsprechen, die betrügerische Aktivitäten in Ihrem Trainingsdatensatz darstellt. Geben Sie optional eine Beschreibung der Bezeichnung ein.
4. Wählen Sie Label erstellen.
5. Erstellen Sie ein zweites Label und geben Sie einen Labelnamen für ein legitimes Ereignis ein. Stellen Sie sicher, dass der Labelname dem Wert entspricht, der die legitime Aktivität in Ihrem Trainingsdatensatz darstellt.

### Erstellen Sie ein Etikett mit demAWS SDK for Python (Boto3)

Der folgendeAWS SDK for Python (Boto3) Beispielcode erstellt mithilfe der [PutLabel](#)API zwei Labels (Fraud, Legit). Nachdem Sie die Labels erstellt haben, können Sie sie einem Ereignistyp hinzufügen, um bestimmte Ereignisse zu klassifizieren.

```
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'
)
```

## Kennzeichnung aktualisieren

Wenn Ihr Ereignisdatensatz mit Amazon Fraud Detector gespeichert ist, müssen Sie möglicherweise Labels für die gespeicherten Ereignisse hinzufügen oder aktualisieren, z. B. wenn Sie eine Offline-Betrugsuntersuchung für ein Ereignis durchführen und die Feedback-Schleife für maschinelles Lernen schließen möchten.

Sie können Labels für gespeicherte Ereignisse hinzufügen oder aktualisieren, indem Sie den [update-event-label](#) Befehl, die [UpdateEventLabel](#) API oder den AWS SDK for Python (Boto3)

Im folgenden AWS SDK for Python (Boto3) Beispielcode wird ein Labelbetrug hinzugefügt, der mit der Registrierung des Ereignistyps über die `UpdateEventLabel` API verknüpft ist.

```
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'
)
```

## Aktualisierung von Ereignisbezeichnungen in Ereignisdaten, die in Amazon Fraud Detector gespeichert sind

Möglicherweise müssen Sie Betrugsbezeichnungen für Ereignisse hinzufügen oder aktualisieren, die bereits in Amazon Fraud Detector gespeichert sind, z. B. wenn Sie eine Offline-

Betrugsuntersuchung für ein Ereignis durchführen und die Feedback-Schleife für maschinelles Lernen schließen möchten. Verwenden Sie den `updateEventLabel` API-Vorgang, um die Bezeichnung für ein Ereignis zu aktualisieren, das bereits in Amazon Fraud Detector gespeichert ist. Im Folgenden wird ein Beispiel für einen `updateEventLabel` API-Aufruf gezeigt.

```
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'
)
```

## Kennzeichnung

Wenn Sie ein Etikett löschen, löscht Amazon Fraud Detector dieses Etikett dauerhaft und die Daten werden nicht mehr in Amazon Fraud Detector gespeichert.

Sie können keine Bezeichnung löschen, die in einem Ereignistyp in Amazon Fraud Detector enthalten ist. Sie können auch kein Label löschen, das einer Ereignis-ID zugewiesen ist. Sie müssen zuerst die entsprechende Ereignis-ID löschen.

Sie können Labels in der Amazon Fraud Detector-Konsole löschen, indem Sie den Befehl [delete-label](#) verwenden, die [DeleteLabel](#) API verwenden oder AWS SDK for Python (Boto3)

### Löschen Sie das Label über die Konsole

So löschen Sie eine Bezeichnung

1. Melden Sie sich bei der an AWS Management Console und öffnen Fraud Detector Konsole unter <https://console.aws.amazon.com/frauddetector>.
2. Wählen Sie im linken Navigationsbereich Fraud Detector Konsole Ressourcen und dann Beschriftungen.
3. Wählen Sie das Label aus, das Sie löschen möchten.
4. Wählen Sie Actions (Aktionen) und anschließend Delete (Löschen).

5. Geben Sie den Labelnamen ein und wählen Sie dann Bezeichnung löschen.

## Löschen Sie ein Label mit dem AWS SDK for Python (Boto3)

Der folgende AWS SDK for Python (Boto3) Beispielcode löscht ein Label legitim mithilfe der [DeleteLabelAPI](#).

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

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

## Regeln

Eine Regel ist eine Bedingung, die Amazon Fraud Detector mitteilt, wie Variablenwerte während einer Betrugsprognose zu interpretieren sind. Eine Regel ist Teil einer Detektorlogik und besteht aus den folgenden Elementen:

- Variable oder Liste — Variable steht für ein Datenelement in Ihrem Event-Dataset, das Sie für eine Betrugsprognose verwenden möchten. Eine Liste ist ein Satz von Eingabedatenelementen für eine Variable in Ihrem Event-Dataset. In einer Regel verwendete Variablen müssen im ausgewerteten Ereignistyp vordefiniert sein, und die in einer Regel verwendeten Listen müssen einem Variablentyp zugeordnet sein. Weitere Informationen erhalten Sie unter [Variablen](#) und [Listen](#).
- Ausdruck — Ein Ausdruck in einer Regel erfasst Ihre Geschäftslogik. Wenn Sie in Ihrer Regel eine Variable verwenden, wird ein einfacher Regelausdruck mit einer Variablen, einem Vergleichsoperator wie >, <, <=, >=, == und einem Wert erstellt. Wenn Sie eine Liste verwenden, wird der Regelausdruck als Listeneintrag und Listenname erstellt. In Weitere Informationen finden Sie unter [Referenz zur Regelsprache](#). Sie können mehrere Ausdrücke mit and und kombinieren. Alle Ausdrücke müssen einen booleschen Wert (wahr oder falsch) ergeben und weniger als 4.000 Zeichen lang sein. Bedingungen vom Typ If-else werden nicht unterstützt.
- Ergebnis — Ein Ergebnis ist eine Antwort, die Amazon Fraud Detector zurückgibt, wenn eine Regel erfüllt wird. Das Ergebnis weist auf das Ergebnis einer Betrugsvorhersage hin. Sie können Ergebnisse für jede mögliche Betrugsprognose erstellen und diese zu einer Regel hinzufügen. Weitere Informationen finden Sie unter [Ergebnisse](#).

Einem Detektor muss mindestens eine Regel zugeordnet sein. Eine Regel kann bis zu 3 Listen enthalten, und ein Detektor kann bis zu 30 Listen haben. Sie erstellen eine Regel als Teil des Erstellungsprozesses des Detektors. Sie können auch neue Regeln erstellen und mit einem vorhandenen Detektor verknüpfen.

## Referenz zur Regelsprache

Im folgenden Abschnitt werden die Funktionen von Amazon Fraud Detector für Ausdrücke (d. h. das Schreiben von Regeln) beschrieben.

### Variablen verwenden

Sie können jede Variable, die im ausgewerteten Ereignistyp definiert ist, als Teil Ihres Ausdrucks verwenden. Verwenden Sie das Dollarzeichen, um eine Variable anzugeben:

```
$example_variable < 100
```

### Listen verwenden

Sie können jede Liste verwenden, die einem Variablentyp zugeordnet ist und als Teil Ihres Regelausdrucks mit Einträgen gefüllt ist. Verwenden Sie das Dollarzeichen, um einen Wert für einen Listeneintrag anzugeben:

```
$example_list_variable in @list_name
```

### Vergleichs-, Mitgliedschafts- und Identitätsoperatoren

Amazon Fraud Detector enthält die folgenden Vergleichsoperatoren: >, >=, <, <=, !=, ==, in, nicht in

Im Folgenden sind einige Beispiele aufgeführt:

Beispiel: <

```
$variable < 100
```

Beispiel: in, nicht in

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

Beispiel: !=

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

Beispiel: ==

```
$variable == 1000
```

## Operatortabellen

Operator	Betreiber von Amazon Fraud Detector
gleich	==
nicht gleich	!=
größer als	>
kleiner als	<
Großartig oder gleich	>=
kleiner als oder gleich	<=
In	in
And	und
Or	oder
NOT	!

## Grundlegende Mathematik

Sie können grundlegende mathematische Operatoren in Ihrem Ausdruck verwenden (z. B. +, -, \*, /). Ein typischer Anwendungsfall ist, wenn Sie während Ihrer Bewertung Variablen kombinieren müssen.

In der folgenden Regel fügen wir die Variable `$variable_1` mit hinzu und prüfen `$variable_2`, ob die Summe kleiner als 10 ist.

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

## Grundlegende mathematische Tabellendaten

Operator	Betreiber von Amazon Fraud Detector
Plus	+
Minus	-
Multipliy (Multiplikation)	*
Division	/
Modulo	%

## Regulärer Ausdruck (Regex)

Sie können Regex verwenden, um nach bestimmten Mustern als Teil Ihres Ausdrucks zu suchen. Dies ist besonders nützlich, wenn Sie nach einer bestimmten Zeichenfolge oder einem bestimmten numerischen Wert für eine Ihrer Variablen suchen. Amazon Fraud Detector unterstützt Matches nur, wenn mit regulären Ausdrücken gearbeitet wird (z. B. gibt es Wahr/Falsch zurück, je nachdem, ob die angegebene Zeichenfolge mit dem regulären Ausdruck übereinstimmt). Die Unterstützung regulärer Ausdrücke von Amazon Fraud Detector basiert auf `.matches()` in Java (unter Verwendung der RE2J-Bibliothek für reguläre Ausdrücke). Es gibt mehrere hilfreiche Websites im Internet, die zum Testen verschiedener regulärer Ausdrucksmuster nützlich sind.

Im ersten Beispiel unten transformieren wir die Variable zunächst `email` in Kleinbuchstaben. Anschließend prüfen wir, ob das Muster in der `email` Variablen enthalten `@gmail.com` ist. Beachten Sie, dass der zweite Punkt maskiert wird, damit wir explizit nach der Zeichenfolge suchen können `.com`.

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

Im zweiten Beispiel prüfen wir, ob die Variable die Landesvorwahl `phone_number` enthält, `+1` um festzustellen, ob die Telefonnummer aus den USA stammt. Das Plus-Symbol wird maskiert, sodass wir explizit nach der Zeichenfolge suchen können `+1`.

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

## Regex-Tabelle

Operator	Beispiel für Amazon Fraud Detector
Entspricht jeder Zeichenfolge, die mit beginnt	<code>regex_match („^mystring“, \$variable)</code>
Entspricht der gesamten Zeichenfolge exakt	<code>regex_match („meine Zeichenfolge“, \$variable)</code>
Entspricht einem beliebigen Zeichen außer einer neuen Zeile	<code>regex_match („ . „, \$variabel)</code>
Entspricht einer beliebigen Anzahl von Zeichen außer der neuen Zeile vor 'mystring'	<code>regex_match („ *mystring“, \$ variabel)</code>
Entkomme Sonderzeichen	<code>\</code>

## Auf fehlende Werte überprüfen

Manchmal ist es von Vorteil zu überprüfen, ob der Wert fehlt. In Amazon Fraud Detector wird dies durch Null dargestellt. Sie können dies tun, indem Sie die folgende Syntax verwenden:

```
$variable != null
```

In ähnlicher Weise können Sie Folgendes tun, wenn Sie überprüfen möchten, ob ein Wert nicht vorhanden ist:

```
$variable == null
```

## Mehrere Bedingungen

Sie können mehrere Ausdrücke mit `and` und `combineor` kombinieren. Amazon Fraud Detector stoppt in einem OR Ausdruck, wenn ein einziger wahrer Wert gefunden wird, und er stoppt in einem, AND wenn ein einziger falscher Wert gefunden wird.

Im folgenden Beispiel suchen wir anhand der `and` Bedingung nach zwei Bedingungen. In der ersten Anweisung prüfen wir, ob Variable 1 kleiner als 100 ist. In der zweiten prüfen wir, ob Variable 2 nicht die USA sind.

Da die Regel ein verwendetand, müssen beide wahr sein, damit die gesamte Bedingung als WAHR ausgewertet wird.

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

Sie können Klammern verwenden, um boolesche Operationen zu gruppieren, wie im Folgenden gezeigt:

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

## Andere Ausdruckstypen

### DateTimeFunktionen

Funktion	Beschreibung	Beispiel
<code>getcurrentdatetime ()</code>	Gibt die aktuelle Uhrzeit der Regelausführung im ISO8601 UTC-Format an. Sie können <code>getepochmillisecons (getcurrentdatetime ())</code> verwenden, um zusätzliche Operationen auszuführen	<code>getcurrentdatetime () == „2023-03-28T 18:34:02 Z“</code>
<code>ist vor (DateTime 1, DateTime 2)</code>	Gibt einen booleschen Wert (Wahr/Falsch) zurück, wenn der Aufrufer 1 vor 2 steht <code>DateTime DateTime</code>	<code>isbefore (getcurrentdatetime (), „2019-11-30T 01:01:01 Z“) == „Falsch“</code>  <code>isbefore (getcurrentdatetime (), „2050-11-30T 01:05:01 Z“) == „Wahr“</code>
<code>danach (DateTime1, DateTime 2)</code>	Gibt einen booleschen Wert (Wahr/Falsch) zurück, wenn der Aufrufer 1 hinter 2 steht <code>DateTime DateTime</code>	<code>isafter (getcurrentdatetime (), „2019-11-30T 01:01:01 Z“) == „Wahr“</code>  <code>isafter (getcurrentdatetime (), „2050-11-30T 01:05:01 Z“) == „Falsch“</code>



Funktion	Beschreibung	Beispiel
getepochmillisekunden (DateTime)	Nimmt a DateTime und gibt das DateTime in Epochen-Millisekunden zurück. Nützlich für die Durchführung mathematischer Operationen am Datum	getepochmillisekunden („2019-11-30T 01:01:01 Z“) = 1575032461

## Zeichenfolgen-Operatoren

Operator	Beispiel
Zeichenfolge in Großbuchstaben umwandeln	Großbuchstaben (\$variable)
Zeichenfolge in Kleinbuchstaben umwandeln	Kleinbuchstaben (\$variable)

## Sonstige

Operator	Kommentar
Füge einen Kommentar hinzu	# mein Kommentar

## Regeln erstellen

Sie können Regeln in der Amazon Fraud Detector-Konsole erstellen, indem Sie den Befehl [create-rule](#) verwenden, die [CreateRule](#)API verwenden oder die AWS SDK for Python (Boto3)

Jede Regel muss einen einzigen Ausdruck enthalten, der Ihre Geschäftslogik erfasst. Alle Ausdrücke müssen einen booleschen Wert (wahr oder falsch) ergeben und weniger als 4.000 Zeichen lang sein. Bedingungen vom Typ If-else werden nicht unterstützt. Alle im Ausdruck verwendeten Variablen müssen im ausgewerteten Ereignistyp vordefiniert sein. Ebenso müssen alle in dem Ausdruck verwendeten Listen vordefiniert, einem Variablentyp zugeordnet und mit Einträgen gefüllt sein.

Im folgenden Beispiel wird eine Regel `high_risk` für einen vorhandenen Detektor `erstellungpayments_detector`. Die Regel verknüpft der Regel einen Ausdruck und ein Ergebnis `verify_customer`.

## Voraussetzungen

Um die unten genannten Schritte auszuführen, stellen Sie sicher, dass Sie die folgenden Schritte ausführen, bevor Sie mit der Erstellung von Regeln fortfahren:

- [Erstellen Sie einen Detektor](#)
- [Ein Ergebnis erstellen](#)

Wenn Sie einen Detektor, eine Regel und ein Ergebnis für Ihren Anwendungsfall erstellen, ersetzen Sie den Beispieldetektornamen, den Regelnamen, den Regelausdruck und den Ergebnisnamen durch die Namen und Ausdrücke, die für Ihren Anwendungsfall relevant sind.

## Erstellen Sie eine neue Regel in der Amazon Fraud Detector-Konsole

1. Öffnen Sie die [AWSManagement Console](#) und melden Sie sich bei Ihrem Konto an. Navigieren Sie zu Amazon Fraud Detector.
2. Wählen Sie im linken Navigationsbereich Detectors und wählen Sie den Detektor aus, den Sie für Ihren Anwendungsfall erstellt haben, z. B. `payments_detector`.
3. Wählen Sie auf der Seite `payments_detector` die Registerkarte Verknüpfte Regeln und dann Regel erstellen aus.
4. Geben Sie auf der Seite Neue Regel Folgendes ein:
  - a. Geben Sie im Feld Name einen Namen für die Regel ein, Beispiel **high\_risk**
  - b. Geben Sie im Feld Beschreibung — optional eine Regelbeschreibung ein, z. B. **This rule captures events with a high ML model score**
  - c. Geben Sie im Feld Ausdruck mithilfe der Kurzanleitung zu Ausdrücken einen Regelausdruck für Ihren Anwendungsfall ein.  
Beispiel-`$sample_fraud_detection_model_insight_score >900`
  - d. Wählen Sie unter Ergebnisse das Ergebnis aus, das Sie für Ihren Anwendungsfall erstellt haben, z. B. `verify_customer`. Ein Ergebnis ist das Ergebnis einer Betrugsprognose und wird zurückgegeben, wenn die Regel bei einer Bewertung zutrifft.
5. Wählen Sie Regel speichern

Sie haben eine neue Regel für Ihren Detektor erstellt. Dies ist die Version 1 der Regel, die Amazon Fraud Detector dem Detektor automatisch zur Verwendung zur Verfügung stellt.

## Erstellen Sie eine Regel mit dem AWS SDK for Python (Boto3)

Der folgende Beispielcode verwendet die [CreateRule](#)API, um eine Regel `high_risk` für einen vorhandenen Detektor zu erstellen `payments_detector`. Der Beispielcode fügt der Regel auch einen Regelausdruck und ein Ergebnis `verify_customer` hinzu.

### Voraussetzungen

Um den Beispielcode zu verwenden, stellen Sie sicher, dass Sie die folgenden Schritte ausgeführt haben, bevor Sie mit der Erstellung von Regeln fortfahren:

- [Erstellen Sie einen Detektor](#)
- [Ein Ergebnis erstellen](#)

Wenn Sie einen Detektor, eine Regel und ein Ergebnis für Ihren Anwendungsfall erstellen, ersetzen Sie den Beispieldetektornamen, den Regelnamen, den Regelausdruck und den Ergebnisnamen durch Namen und Ausdrücke, die für Ihren Anwendungsfall relevant sind.

```
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']
)
```

Sie haben die Version 1 der Regel erstellt, die Amazon Fraud Detector dem Detektor automatisch zur Verwendung zur Verfügung stellt.

## Regel aktualisieren

Sie können eine Regel jederzeit aktualisieren, indem Sie die Regelbeschreibung hinzufügen oder aktualisieren, den Regelausdruck aktualisieren oder das Ergebnis für die Regel hinzufügen oder entfernen. Wenn Sie eine Regel aktualisieren, wird eine neue Regelversion erstellt.

Sie können eine Regel in der Amazon Fraud Detector-Konsole mithilfe des [update-rule-version](#)Befehls, mithilfe der [UpdateRuleVersion](#)API oder mithilfe des AWS SDK aktualisieren.

Nachdem Sie die Regel aktualisiert haben, stellen Sie sicher, dass Sie Ihre Detektorversion aktualisieren, um die neue Regelversion zu verwenden.

## Regel in der Amazon Fraud Detector-Konsole aktualisieren

Um eine Regel zu aktualisieren,

1. Öffnen Sie die [AWS Management Console](#) und melden Sie sich bei Ihrem Konto an. Navigieren Sie zu Amazon Fraud Detector.
2. Wählen Sie im linken Navigationsbereich Detectors aus.
3. Wählen Sie im Bereich Detektoren den Melder aus, der der Regel zugeordnet ist, die Sie aktualisieren möchten.
4. Wählen Sie auf Ihrer Melderseite die Registerkarte Zugeordnete Regeln und wählen Sie die Regel aus, die Sie aktualisieren möchten.
5. Wählen Sie auf Ihrer Regelseite Aktionen und dann Version erstellen aus.
6. Beachten Sie, dass sich die Version geändert hat. Geben Sie eine aktualisierte Beschreibung, einen Ausdruck oder ein Ergebnis ein.
7. Wählen Sie Neue Version speichern

## Regel aktualisieren mit dem AWS SDK for Python (Boto3)

Der folgende Beispielcode verwendet die [UpdateRuleVersion](#)API, um den Schwellenwert für die Regel `high_risk` von 900 auf 950 zu aktualisieren. Diese Regel ist mit dem Detektor `verknüpftpayments_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']  
)
```

## Listen

Eine Liste ist ein Satz von Eingabedaten für eine Variable in Ihrem Ereignisdatensatz. Sie verwenden die Eingabedaten in einer Regel, die Ihrem Detektor zugeordnet ist. Eine Regel ist eine Bedingung, die Amazon Fraud Detector mitteilt, wie Eingabedaten während einer Betrugsvorhersage zu interpretieren sind. Sie können beispielsweise eine Liste von IP-Adressen erstellen und dann eine Regel erstellen, um den Zugriff zu verweigern, wenn eine bestimmte IP-Adresse in der Liste enthalten ist. Regeln, die Listen verwenden, werden im `@list_name Format$ip_address_value` in ausgedrückt.

Mit Amazon Fraud Detector können Sie eine Liste verwalten, indem Sie Daten hinzufügen oder entfernen, ohne eine zugehörige Regel aktualisieren zu müssen. Eine Ihrer Liste zugeordnete Regel beinhaltet automatisch neu hinzugefügte oder entfernte Daten.

Eine Liste kann bis zu 100.000 eindeutige Einträge enthalten und jeder Eintrag kann bis zu 320 Zeichen lang sein. Jede Liste, die Sie in einer Regel verwenden, ist standardmäßig mit [Variablentypen](#) `FREE_FORM_TEXT` von Amazon Fraud Detector verknüpft. Sie können Ihrer Liste jederzeit einen Variablentyp zuweisen. Sie können bis zu 3 Listen in einer Regel verwenden.

Sie können eine Liste erstellen, Einträge zur Liste hinzufügen, eine Liste löschen oder einen oder mehrere Einträge in der Liste löschen oder Ihrer Liste in der Amazon Fraud Detector Detector-Konsole einen Variablentyp zuweisen, indem Sie die APIAWS CLI, das oder dasAWS SDK verwenden.

## Erstellen einer Liste

Sie können eine Liste mit Eingabedaten (Einträgen) einer Variablen in Ihrem Event-Dataset erstellen und die Liste in einem Regelausdruck verwenden. Die Einträge in der Liste können dynamisch verwaltet werden, ohne dass die Regel aktualisiert wird, die die Liste verwendet.

Um eine Liste zu erstellen, müssen Sie zuerst einen Namen angeben und die Liste dann optional einem von Amazon [Variablentypen](#) unterstützten Fraud Detector zuordnen. Standardmäßig geht Amazon Fraud Detector davon aus, dass die Liste vom Variablentyp `FREE_FORM_TEXT` ist.

Sie können eine Liste in der Amazon Fraud Detector Detector-Konsole erstellen, indem Sie die APIAWS CLI, das oder dasAWS SDK verwenden.

## Erstellen Sie eine Liste mit der Amazon Fraud Detector Detector-Konsole

So erstellen Sie eine Liste

1. Öffnen Sie die [AWSManagement Console](#) und melden Sie sich bei Ihrem Konto an. Navigieren Sie zu Amazon Fraud Detector.
2. Wählen Sie im linken Navigationsbereich Listen aus.
3. Unter Listendetails
  - a. Geben Sie im Feld Listenname einen Namen für Ihre Liste ein.
  - b. Geben Sie in der Beschreibung optional eine Beschreibung ein.
  - c. (Optional) Wählen Sie unter Variablentyp einen Variablentyp für Ihre Liste aus.

### Important

Wenn Ihre Liste IP-Adressen enthält, stellen Sie sicher, dass Sie `IP_ADDRESS` als Variablentyp auswählen. Wenn Sie keinen Variablentyp auswählen, geht Amazon Fraud Detector davon aus, dass es sich bei der Liste um den Variablentyp `FREE_FORM_TEXT` handelt.

4. Fügen Sie im Feld Listendaten hinzufügen Listeneinträge hinzu, einen Eintrag in jeder Zeile. Sie können auch Einträge aus einer Tabelle kopieren und einfügen.

### Note

Stellen Sie sicher, dass die Einträge nicht durch ein Komma getrennt sind und in der Liste eindeutig sind. Wenn zwei identische Einträge eingegeben werden, wird nur einer hinzugefügt.

5. Wählen Sie Create (Erstellen) aus.

## Erstellen Sie eine Liste mit demAWS SDK for Python (Boto3)

Sie erstellen eine Liste, indem Sie einen Listennamen angeben. Sie können optional eine Beschreibung angeben, einen Variablentyp zuordnen oder Einträge zu Ihrer Liste hinzufügen, wenn Sie eine Liste erstellen. Sie können die Liste auch später aktualisieren, indem Sie Einträge oder eine Beschreibung hinzufügen. Sie können der Liste später einen Variablentyp zuweisen, falls Sie ihn bei

der Erstellung der Liste noch nicht zugewiesen haben. Der Variablentyp einer Liste kann nach der Zuweisung nicht geändert werden.

### Important

Wenn Ihre Liste IP-Adressen enthält, stellen Sie sicher, dass Sie `IP_ADDRESS` als Variablentyp zuweisen. Wenn Sie keinen Variablentyp zuweisen, geht Amazon Fraud Detector davon aus, dass die Liste vom Variablentyp `FREE_FORM_TEXT` ist.

Im folgenden Beispiel wird eine [CreateList](#) API-Operation verwendet, um eine `allow_email_ids` Liste zu erstellen, indem eine Beschreibung und ein Variablentyp bereitgestellt und vier Listeneinträge hinzugefügt werden.

```
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']
)
```

## Einträge zu einer Liste hinzufügen

Nachdem Sie Ihre Liste erstellt haben, können Sie jederzeit Einträge zu Ihrer Liste hinzufügen oder anhängen. Wenn Sie Einträge zu Ihrer Liste hinzufügen oder anhängen, müssen Sie die Regel, der die Liste zugeordnet ist, nicht aktualisieren. Die Regel berücksichtigt automatisch die neu hinzugefügten Einträge.

Ihre Liste kann bis zu 100.000 eindeutige Einträge enthalten und jeder Eintrag kann bis zu 320 Zeichen lang sein.

Sie können Einträge in der Amazon Fraud Detector Detector-Konsole hinzufügen, indem Sie die `APIAWS CLI`, das oder das `AWS SDK` verwenden.

## Hinzufügen von Einträgen zu einer Liste mithilfe der Amazon Fraud Detector Detector-Konsole

So fügen Sie mindestens einen Eintrag zu einer Liste hinzu:

1. Öffnen Sie die [AWSManagement Console](#) und melden Sie sich bei Ihrem Konto an. Navigieren Sie zu Amazon Fraud Detector.
2. Wählen Sie im linken Navigationsbereich Listen aus.
3. Wählen Sie auf der Seite Listen die Liste aus, zu der Sie Einträge hinzufügen möchten.
4. Wählen Sie auf der Seite mit den Listendetails die Registerkarte Daten auflisten und dann Daten hinzufügen aus.
5. Fügen Sie im Feld Listendaten hinzufügen in jeder Zeile einen Eintrag hinzu, oder kopieren Sie Einträge aus einer Tabelle und fügen Sie sie ein. Achten Sie darauf, dass Sie kein Komma verwenden, um die Einträge zu trennen.
6. Wählen Sie Add (Hinzufügen) aus.

## Fügen Sie Einträge zu einer Liste hinzu, indem Sie AWS SDK for Python (Boto3)

Im folgenden Beispiel wird der [UpdateList](#) API-Vorgang verwendet, um der `allow_email_ids` Liste zwei neue Einträge hinzuzufügen. Stellen Sie sicher, dass die Einträge, die Sie hinzufügen, in der Liste eindeutig sind.

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

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

## Weisen Sie einer Liste einen Variablentyp zu

Jede Liste, die Sie in einer Regel verwenden, muss dem [Variablentypen](#) Variablentyp eines Amazon Fraud Detector zugeordnet sein. Standardmäßig geht Amazon Fraud Detector davon aus, dass die Liste vom Variablentyp `FREE_FORM_TEXT` ist. Es ist wichtig zu beachten, dass eine Liste, die aus IP-Adressen besteht, dem Variablentyp `IP_ADDRESS` zugeordnet werden muss.



Sie können Ihre Liste entweder bei der Erstellung der Liste oder jederzeit später einem Variablentyp zuordnen. Wenn Sie Ihre Liste bereits mit einem Variablentyp verknüpft haben und ihn später ändern möchten, müssen Sie eine neue Liste erstellen. Sie können den Variablentyp einer Liste nicht ändern.

Sie können in der Amazon Fraud Detector Detector-Konsole mithilfe der API, mithilfe des oder mithilfe des AWS CLI/AWS SDK einen Variablentyp zuweisen.

## Weisen Sie einer Liste mithilfe der Amazon Fraud Detector Detector-Konsole einen Variablentyp zu

Um einer Liste einen Variablentyp zuzuweisen

1. Öffnen Sie die [AWS Management Console](#) und melden Sie sich bei Ihrem Konto an. Navigieren Sie zu Amazon Fraud Detector.
2. Wählen Sie im linken Navigationsbereich Listen aus.
3. Wählen Sie auf der Seite Listen die Liste aus, der Sie einen Variablentyp zuweisen möchten.
4. Wählen Sie auf der Seite mit den Listendetails die Option Aktionen und anschließend Liste bearbeiten aus.
5. Wählen Sie im Listenfeld Bearbeiten den Variablentyp für Ihre Liste aus.
6. Wählen Sie Speichern.

## Weisen Sie einer Liste den Variablentyp zu, indem Sie AWS SDK for Python (Boto3)

Im folgenden Beispiel wird der [UpdateList](#) API-Vorgang verwendet, um einer `allow_ip_address` Liste einen Variablentyp zuzuweisen.

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

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

## Löschen einer Liste

Sie können eine Liste löschen, die in keiner Regel verwendet wird. Wenn Sie eine Liste löschen, löscht Amazon Fraud Detector diese Liste und alle Einträge in der Liste dauerhaft.

Sie können eine Liste in der Amazon Fraud Detector Detector-Konsole löschen, indem Sie die API, dasAWS CLI oder dasAWS SDK verwenden.

### Liste mit der Amazon Fraud Detector Detector-Konsole löschen

So löschen Sie eine Liste

1. Öffnen Sie die [AWSManagement Console](#) und melden Sie sich bei Ihrem Konto an. Navigieren Sie zu Amazon Fraud Detector.
2. Wählen Sie im linken Navigationsbereich Listen aus.
3. Wählen Sie auf der Listenseite die Liste aus, die Sie löschen möchten.
4. Wählen Sie auf der Seite mit den Listendetails die Option Aktionen und anschließend Liste löschen aus.
5. Wählen Sie Liste löschen.

### Löschen Sie die Liste mit demAWS SDK for Python (Boto3)

Im folgenden Beispiel wird der [DeleteList](#)API-Vorgang zum Löschen verwendetallow\_email\_ids.

```
import boto3
        fraudDetector = boto3.client('frauddetector')
    fraudDetector.delete_list(
        name = 'allow_email_ids'
    )
```

### Einträge aus einer Liste löschen

Sie können jederzeit einen oder mehrere Einträge aus Ihren Listen löschen. Wenn Sie Einträge in Ihrer Liste löschen, müssen Sie die Regel, der die Liste zugeordnet ist, nicht aktualisieren. Die Regel enthält automatisch die aktualisierte Liste.

Sie können Einträge aus einer Liste in der Amazon Fraud Detector Detector-Konsole löschen, indem Sie die API, dasAWS CLI oder dasAWS SDK verwenden.

## Löschen Sie Einträge aus einer Liste mithilfe der Amazon Fraud Detector Detector-Konsole

So löschen Sie einen oder mehrere Einträge aus einer Liste

1. Öffnen Sie die [AWSManagement Console](#) und melden Sie sich bei Ihrem Konto an. Navigieren Sie zu Amazon Fraud Detector.
2. Wählen Sie im linken Navigationsbereich Listen aus.
3. Wählen Sie auf der Listenseite die Liste der Einträge aus, die Sie löschen möchten.
4. Wählen Sie auf Ihrer Listendetailseite die Registerkarte Listendaten und wählen Sie die Einträge aus, die Sie löschen möchten.
5. Wählen Sie Löschen und klicken Sie zur Bestätigung erneut auf Löschen.

## Löschen Sie Einträge aus einer Liste mit demAWS SDK for Python (Boto3)

Im folgenden Beispiel löscht die [UpdateList](#)API-Operation Einträge aus `allow_email_ids` der Liste.

```
import boto3

fraudDetector = boto3.client('frauddetector')

fraudDetector.update_list(
    name = 'allow_email_ids',
    updateMode = 'REMOVE',
    elements = ['emailId_4', 'emailId_12']
)
```

## Alle Einträge aus einer Liste löschen

Sie können alle Einträge in Ihrer Liste löschen, wenn die Liste nicht in einer Regel verwendet wird. Sie können alle Einträge in der Liste löschen und später Einträge in derselben Liste hinzufügen.

Sie können Einträge aus einer Liste in der Amazon Fraud Detector Detector-Konsole löschen, indem Sie die API, dasAWS CLI oder dasAWS SDK verwenden.

## Löschen Sie alle Einträge aus einer Liste mithilfe der Amazon Fraud Detector Detector-Konsole

Um alle Einträge aus einer Liste zu löschen

1. Öffnen Sie die [AWSManagement Console](#) und melden Sie sich bei Ihrem Konto an. Navigieren Sie zu Amazon Fraud Detector.
2. Wählen Sie im linken Navigationsbereich Listen aus.
3. Wählen Sie auf der Listenseite die Liste der Einträge aus, die Sie löschen möchten.
4. Wählen Sie auf der Seite mit den Listendetails die Registerkarte Daten auflisten und dann Alle löschen aus.
5. Geben Sie in das Feld Alle löschen den Textdelete all zur Bestätigung ein und wählen Sie dann Alle Listendaten löschen.

## Löschen Sie alle Einträge aus einer Liste mit demAWS SDK for Python (Boto3)

Im folgenden Beispiel löscht die [UpdateList](#)API-Operation alle Einträge ausallow\_email\_ids der Liste.

```
import boto3

fraudDetector = boto3.client('frauddetector')

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

## Ergebnisse

Ein Ergebnis ist das Ergebnis einer Betrugsvorhersage. Sie können für jedes mögliche Ergebnis der Betrugsvorhersage ein Ergebnis erstellen. Beispielsweise möchten Sie, dass die Ergebnisse Risikostufen (hohes Risiko, mittleres Risiko und niedriges Risiko) oder Maßnahmen (genehmigen, überprüfen) darstellen. Nach dem Erstellen eines Ergebnisses können Sie einer Regel ein oder mehrere Ergebnisse hinzufügen. Als Teil der [GetEventPrediction](#)Antwort gibt Amazon Fraud Detector die definierten Ergebnisse für jede übereinstimmende Regel zurück.

## Ein Ergebnis erstellen

Sie können Ergebnisse in der Amazon Fraud Detector-Konsole erstellen, indem Sie den Befehl [put-outcome](#), die [PutOutcome](#)API oder den verwendenAWS SDK for Python (Boto3).

### Erstellen Sie ein Ergebnis mit der Amazon Fraud Detector-Konsole

Um ein oder mehrere Ergebnisse zu erzielen

1. Öffnen Sie die [AWSManagement Console](#) und melden Sie sich bei Ihrem Konto an. Navigieren Sie Fraud Detector.
2. Wählen Sie im linken Navigationsbereich Ergebnisse aus.
3. Wählen Sie auf der Seite Ergebnisse die Option Erstellen aus.
4. Geben Sie auf Ihrer Seite mit dem neuen Ergebnis Folgendes ein:
  - a. Geben Sie im Feld Ergebnisname einen Namen für Ihr Ergebnis ein.
  - b. In der Ergebnisbeschreibung geben Sie optional eine Beschreibung ein.
5. Wählen Sie Ergebnis speichern.
6. Wiederholen Sie die Schritte 2 bis 5, um weitere Ergebnisse zu erzielen.

### Erstellen Sie ein Ergebnis mit demAWS SDK for Python (Boto3)

Das folgende Beispiel verwendet diePutOutcome API, um drei Ergebnisse zu erstellen. Sie sindverify\_customerreview, undapprove. Nachdem die Ergebnisse erstellt wurden, können Sie sie Regeln zuweisen.

```
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'  
)
```

## Ein Ergebnis löschen

Sie können kein Ergebnis löschen, das in einer Regelversion verwendet wird.

Wenn Sie ein Ergebnis löschen, löscht Amazon Fraud Detector dieses Ergebnis dauerhaft und die Daten werden nicht mehr in Amazon Fraud Detector gespeichert.

Sie können ein Ergebnis in der Amazon Fraud Detector-Konsole löschen, indem Sie den Befehl [delete-outcome](#) verwenden, die [DeleteOutcome](#)API verwenden oder AWS SDK for Python (Boto3)

### Löschen Sie ein Ergebnis in der Amazon Fraud Detector-Konsole

So löschen Sie ein Ergebnis

1. [Melden Sie sich bei der anAWS Management Console und öffnen Sie die Amazon Fraud Detector](https://console.aws.amazon.com/frauddetector) <https://console.aws.amazon.com/frauddetector>
2. Wählen Sie im linken Navigationsbereich der Amazon Fraud Detector-Konsole Ressourcen und dann Outcomes aus.
3. Wählen Sie das Ergebnis aus, das Sie löschen möchten.
4. Wählen Sie Actions (Aktionen) und anschließend Delete (Löschen).
5. Geben Sie den Namen des Ergebnisses ein und wählen Sie dann Ergebnis löschen.

### Löschen Sie ein Ergebnis mit demAWS SDK for Python (Boto3)

Im folgenden Beispiel wird die [DeleteOutcome](#)API verwendet, um das `verify_customer` Ergebnis zu löschen. Nachdem das Ergebnis gelöscht wurde, können Sie es keiner Regel mehr zuweisen.

```
import boto3  
fraudDetector = boto3.client('frauddetector')  
  
fraudDetector.delete_outcome(  
name = 'verify_customer'  
)
```

# Entität

Eine Entität steht für eine Person oder Sache, die das Ereignis durchführt. Ein Entitätstyp klassifiziert die Entität. Zu den Beispielklassifizierungen gehören Kunden, Händler, Benutzer oder Konto. Sie geben den Entitätstyp (ENTITY\_TYPE) und eine Entitätskennung (ENTITY\_ID) als Teil Ihres Ereignisdatensatzes an, um die spezifische Entität anzugeben, die das Ereignis durchgeführt hat.

Amazon Fraud Detector verwendet den Entitätstyp bei der Generierung einer Betrugsprognose für ein Ereignis, um anzugeben, wer das Ereignis durchgeführt hat. Der Entitätstyp, den Sie für Ihre Betrugsprognosen verwenden möchten, muss zuerst in Amazon Fraud Detector erstellt und dann dem Ereignis hinzugefügt werden, wenn Sie Ihren Ereignistyp erstellen.

## Entitstyp erstellen

Sie können einen Entitätstyp in der Amazon Fraud Detector-Konsole erstellen, indem Sie den [put-entity-type](#)Befehl, die [PutEntityType](#)API oder den verwendenAWS SDK for Python (Boto3). Die folgenden Beispiele erstellen einen Entitstypcustomer in der Amazon Fraud Detector-Konsole mit Hilfe des SDK for Python (Boto3). Wenn Sie einen Entitätstyp erstellen, der einem Ereignistyp zugeordnet werden soll, um ein Betrugserkennungsmodell zu trainieren, verwenden Sie den Entitätstyp aus Ihrem Ereignisdatensatz, der für Ihren Anwendungsfall geeignet ist.

### Erstellen Sie einen Entitätstyp mithilfe der Amazon Fraud Detector-Konsole

Um einen Entitstyp zu erstellen,

1. Öffnen Sie die [AWSManagement Console](#) und melden Sie sich bei Ihrem Konto an.
2. Navigieren Sie zu Amazon Fraud Detector, wählen Sie in der linken Navigationsleiste Entitäten und anschließend Erstellen aus.
3. Geben Sie auf der Seite Entität erstellen den Namen des Entitätstyps customer ein. Geben Sie optional eine Entität ein.
4. Klicken Sie auf Create entity (Entity erstellen).

### Erstellen Sie einen Entitätstyp mit demAWS SDK for Python (Boto3)

Das folgendeAWS SDK for Python (Boto3) Codebeispiel verwendet diePutEntityType API, um einen Entitätstyp zu erstellencustomer. Wenn Sie einen Entitätstyp erstellen, der einem Ereignistyp zugeordnet werden soll, um ein Modell zur Betrugserkennung zu trainieren, verwenden Sie die Entität aus Ihrem Ereignisdatensatz, die für Ihren Anwendungsfall geeignet ist.

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

fraudDetector.put_entity_type(
    name = 'customer',
    description = 'customer'
)
```

## Entitätstyp löschen

In Amazon Fraud Detector können Sie keinen Entitätstyp löschen, der in einem Ereignistyp enthalten ist. Sie müssen zuerst den Ereignistyp löschen, mit dem die Entität verknüpft ist, und dann den Entitätstyp löschen.

Wenn Sie einen Entitätstyp löschen, löscht Amazon Fraud Detector diesen Entitätstyp dauerhaft und die Daten werden nicht mehr in Amazon Fraud Detector gespeichert.

Ein Entitätstyp kann in der Amazon Fraud Detector-Konsole gelöscht werden, indem Sie den [delete-entity-type](#)Befehl, die [DeleteEntityType](#)API oder denAWS SDK for Python (Boto3)

### Löschen Sie einen Entitätstyp in der Amazon Fraud Detector-Konsole

Um einen Entitätstyp zu löschen,

1. Melden Sie sich bei der anAWS Management Console und öffnen Sie die Amazon Fraud Detector-Konsole unter <https://console.aws.amazon.com/frauddetector>.
2. Wählen Sie im linken Navigationsbereich der Amazon Fraud Detector-Konsole Resources und dann Entität aus.
3. Wählen Sie den Entitätstyp aus, den Sie löschen möchten.
4. Wählen Sie Actions (Aktionen) und anschließend Delete (Löschen).
5. Geben Sie den Namen des Entitätstyps ein und wählen Sie dann Entitätstyp löschen.

### Löschen Sie den Entitätstyp mit demAWS SDK for Python (Boto3)

Der folgendeAWS SDK for Python (Boto3) Beispielcode löscht den Entitätstyp Kunde mithilfe der [DeleteEntityType](#)API.

```
import boto3
```



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

fraudDetector.delete_entity_type (

name = 'customer'

)
```

## Verwalten Sie die Ressourcen von Amazon Fraud Detector mit AWS CloudFormation

Amazon Fraud Detector AWS CloudFormation, Amazon Fraud Detector, Sie erstellen eine Vorlage, in der alle gewünschten Amazon Fraud Detector Ressourcen definiert sind. Sie können die Vorlage wiederverwenden, können Sie zur konsistenten Bereitstellung und Konfiguration der Ressourcen in mehreren AWS Konten und Regionen.

Für die Nutzung von AWS fallen keine zusätzlichen Gebühren an CloudFormation.

### Amazon Fraud Detector

Um Ressourcen für Amazon Fraud Detector zu erstellen, müssen Sie Amazon [AWS CloudFormation](#) Vorlagen sind formatierte Textdateien in JSON oder YAML. Diese Vorlagen beschreiben die Ressourcen, die Sie in Ihren AWS CloudFormation-Stacks bereitstellen möchten. Wenn Sie noch keine Erfahrungen mit JSON oder YAML haben, können Sie [AWS CloudFormation Designer](#) verwenden, der den Einstieg in die Arbeit mit AWS CloudFormation-Vorlagen erleichtert. Weitere Informationen finden Sie unter [Was ist AWS CloudFormation-Designer?](#) im AWS CloudFormation-Benutzerhandbuch.

Sie können auch Ihre Amazon Fraud Detector Ressourcen mit AWS CloudFormation erstellen. Weitere Informationen, einschließlich Beispiele für JSON- und YAML-Vorlagen für Ihre Ressourcen, finden Sie in der [AWS CloudFormation Amazon Fraud Detector](#)

Wenn Sie es bereits verwenden CloudFormation, müssen Sie keine zusätzlichen IAM-Richtlinien oder die CloudTrail Protokollierung verwalten.

## Amazon Amazon Fraud Detector

Sie können Ihre Amazon Fraud Detector Detector-Stacks über die CloudFormation Konsole oder über die AWS-CLI erstellen, aktualisieren und löschen.

Um einen Stack zu erstellen, müssen Sie über eine Vorlage verfügen, die beschreibt, welche Ressourcen AWS CloudFormation in Ihren Stack einschließt. Sie können auch Amazon Fraud Detector Detector-Ressourcen, die Sie bereits erstellt haben, in die CloudFormation Verwaltung übernehmen, indem Sie [sie in einen neuen oder vorhandenen Stack importieren](#).

Detaillierte Anweisungen zur Verwaltung Ihrer Stacks finden Sie im AWS CloudFormationBenutzerhandbuch, um zu erfahren, wie Sie Stacks [erstellen](#), [aktualisieren](#) und [löschen](#).

### Amazon Fraud Detector

Die Art und Weise, wie Sie IhreAWS CloudFormation Stacks organisieren, liegt ganz bei Ihnen. Im Allgemeinen ist es eine bewährte Methode, Stacks nach Lebenszyklus und Eigentumsverhältnissen zu organisieren. Das bedeutet, Ressourcen danach zu gruppieren, wie oft sie sich ändern, oder nach Teams, die für ihre Aktualisierung verantwortlich sind.

Sie können wählen, ob Sie Ihre Stacks organisieren möchten, indem Sie für jeden Detektor und seine Erkennungslogik (z. B. Regeln, Variablen usw.) einen Stapel erstellen. Wenn Sie andere Dienste verwenden, sollten Sie überlegen, ob Sie die Ressourcen von Amazon Fraud Detector mit Ressourcen anderer Dienste kombinieren möchten. Sie könnten beispielsweise einen Stack erstellen, der Kinesis-Ressourcen, die beim Sammeln von Daten helfen, und Amazon Fraud Detector Detector-Ressourcen, die die Daten verarbeiten, enthält. Dies kann ein effektiver Weg sein, um sicherzustellen, dass alle Produkte Ihres Betrugsteams zusammenarbeiten.

### Amazon Fraud CloudFormation Detector

Zusätzlich zu den Standardparametern, die in allen CloudFormation Vorlagen verfügbar sind, führt Amazon Fraud Detector zwei zusätzliche Parameter ein, die Ihnen bei der Verwaltung des Bereitstellungsverhaltens helfen. Wenn Sie einen oder beide dieser Parameter nicht angeben, CloudFormation wird der unten angegebene Standardwert verwendet.

Parameter	Werte	Standardwert
DetectorVersionStatus	AKTIV: Setzen Sie die neue/aktualisierte Melderversion auf den Status Aktiv	EINZIEHUNG

Parameter	Werte	Standardwert
	ENTWURF: Setzen Sie die neue/aktualisierte Melderversion auf den Status Entwurf	
Eingebunden	<p>TRUE: CloudFormation Erlaubt, die Ressource beim Erstellen/Löschen des Stacks.</p> <p>FALSCH: Erlauben Sie CloudFormation zu überprüfen, ob das Objekt existiert, nehmen Sie jedoch keine Änderungen am Objekt vor.</p>	TRUE

## AWS CloudFormationBeispielVorlage für Amazon Amazon Amazon Amazon Fraud Detector

Im Folgenden finden Sie eineAWS CloudFormation YAML-Vorlage für die Verwaltung eines Dettor und zugehörige Dettor

```
# 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'
```

## Weitere Informationen zu AWS CloudFormation

Weitere Informationen zu AWS CloudFormation finden Sie in den folgenden Ressourcen.

- [AWS CloudFormation](#)
- [AWS CloudFormation-Benutzerhandbuch](#)
- [AWS CloudFormation API Referenz](#)
- [AWS CloudFormation-Benutzerhandbuch für die Befehlszeilenschnittstelle](#)

# Fraud Preects

Sie können Amazon Fraud Detector verwenden, um Betrugsvorhersagen für ein einzelnes Ereignis in Echtzeit zu erhalten, oder um Betrugsvorhersagen für eine Reihe von Ereignissen offline abzurufen. Um Betrugsvorhersagen für ein einzelnes Ereignis oder eine Reihe von Ereignissen zu erstellen, müssen Sie Amazon Fraud Detector die folgenden Informationen zur Verfügung stellen:

- Weitere Informationen zur Betrugsvorhersage
- Ereignismetadaten

## Logik zur Betrugserkennung

Die Logik zur Betrugsvorhersage verwendet eine oder mehrere Regeln, um Daten im Zusammenhang mit einem Ereignis auszuwerten, und liefert dann ein Ergebnis und einen Wert für die Betrugsprognose. Sie erstellen Ihre Betrugsvorhersagelogik mit den folgenden Komponenten:

- Ereignistypen — Definiert die Struktur des Ereignisses
- Modelle — Definiert Algorithmus- und Datenanforderungen für die Betrugsvorhersage
- Variablen — Stellt ein dem Ereignis zugeordnetes Datenelement dar
- Regeln — Teilt Amazon Fraud Detector mit, wie die Variablenwerte bei der Betrugsprognose zu interpretieren sind
- Ergebnisse — Ergebnisse, die auf der Grundlage einer Betrugsprognose generiert wurden
- Version des Detektors — Enthält eine Logik zur Betrugsvorhersage für ein bestimmtes Ereignis

Weitere Informationen zu den Komponenten, die zur Erstellung der Betrugserkennungslogik verwendet werden, finden Sie unter [Amazon Fraud Detector Detector-Konzepte](#). Bevor Sie mit der Generierung von Betrugsvorhersagen beginnen, stellen Sie sicher, dass Sie die Erkennungsversion erstellt und veröffentlicht haben, die Ihre Betrugsvorhersagelogik enthält. Sie können die Detektorversion mithilfe der Fraud Detector Console oder der API erstellen und veröffentlichen. Weitere Informationen zur Verwendung der Konsole finden [Sie unter Weitere Informationen zur Verwendung der Konsole](#). Anweisungen zur Verwendung der API finden Sie unter [Erstellen einer Detektorversion](#).

## Metadaten des Ereignisses

Die Ereignismetadaten enthalten Details des ausgewerteten Ereignisses. Jedes Ereignis, das Sie auswerten möchten, muss einen Wert für jede Variable im Ereignistyp enthalten, der Ihrer Detektorversion zugeordnet ist. Darüber hinaus müssen Ihre Ereignismetadaten folgende Elemente enthalten:

- **EVENT\_ID** — Eine Kennung für das Ereignis. Wenn es sich bei Ihrer Veranstaltung beispielsweise um eine Online-Transaktion handelt, kann die **EVENT\_ID** die Transaktionsreferenznummer sein, die Ihrem Kunden zur Verfügung gestellt wurde.

#### Wichtige Hinweise zu **EVENT\_ID**

- Muss für diese Veranstaltung einzigartig sein
- Sollte Informationen darstellen, die für Ihr Unternehmen von Bedeutung sind
- Muss dem regulären Ausdrucksmuster entsprechen: `^[0-9a-z_-]+$`.
- Muss gespeichert werden. **EVENT\_ID** ist die Referenz für das Ereignis und wird verwendet, um Operationen für das Ereignis auszuführen, z. B. das Ereignis zu löschen.
- Das Anhängen eines Zeitstempels an die **EVENT\_ID** wird nicht empfohlen, da dies zu Problemen führen kann, wenn Sie das Ereignis später aktualisieren möchten, da Sie genau dieselbe **EVENT\_ID** angeben müssen.
- **ENTITY\_TYPE** — Die Entität, die das Ereignis durchführt, z. B. ein Händler oder ein Kunde.
- **ENTITY\_ID** — Eine Kennung für die Entität, die das Ereignis durchführt. Die **ENTITY\_ID** muss das folgende reguläre Ausdrucksmuster erfüllen: `^[0-9a-z_-]+$`. Wenn die **ENTITY\_ID** zum Zeitpunkt der Auswertung nicht verfügbar ist, geben Sie die Zeichenfolge `unknown` weiter.
- **EVENT\_TIMESTAMP** — Der Zeitstempel, zu dem das Ereignis aufgetreten ist. Der Zeitstempel muss dem ISO 8601-Standard in UTC entsprechen.

## Vorhersage in Echtzeit

Sie können Online-Aktivitäten in Echtzeit auf Betrug hin auswerten, indem Sie die `GetEventPrediction` API aufrufen. Sie geben in jeder Anfrage Informationen zu einem einzelnen Ereignis an und erhalten synchron eine Modellbewertung und ein Ergebnis, das auf der mit dem angegebenen Detektor verknüpften Betrugsvorhersage basiert.

## So funktioniert die Betrugsvorhersage in Echtzeit

Die `GetEventPrediction` API verwendet eine angegebene Detektorversion, um die für das Ereignis bereitgestellten Ereignismetadaten auszuwerten. Während der Bewertung generiert Amazon

Fraud Detector zunächst Modellwerte für Modelle, die der Detektorversion hinzugefügt wurden, und leitet die Ergebnisse dann an die Regeln zur Bewertung weiter. Die Regeln werden gemäß dem Regelausführungsmodus ausgeführt (siehe [Erstellen einer Detektorversion](#)). Als Teil der Antwort liefert Amazon Fraud Detector Modellbewertungen sowie alle Ergebnisse, die mit den abgeglichenen Regeln verknüpft sind.

## Betrugsprognose in Echtzeit abrufen

Um Betrugsvorhersagen in Echtzeit zu erhalten, stellen Sie sicher, dass Sie einen Detektor erstellt und veröffentlicht haben, der Ihr Betrugsvorhersagemodell und Ihre Regeln oder einfach einen Regelsatz enthält.

Sie können Betrugsvorhersagen für ein Ereignis in Echtzeit abrufen, indem Sie den [GetEventPrediction](#) API-Vorgang über die AWS Befehlszeilenschnittstelle (AWSCLI) oder eines der Amazon Fraud Detector-SDKs aufrufen.

Um die API zu verwenden, geben Sie bei jeder Anfrage Informationen zu einem einzelnen Ereignis an. Im Rahmen der Anfrage müssen Sie angeben `detectorId`, dass Amazon Fraud Detector das Ereignis auswerten soll. Optional können Sie eine `detectorVersionId` angeben. Wenn ein nicht angegebener `detectorVersionId` ist, verwendet Amazon Fraud Detector die `ACTIVE` Version des Detektors.

Sie können optional Daten senden, um ein SageMaker Modell aufzurufen, indem Sie die Daten in das Feld `externalModelEndpointBlobs` übergeben.

Holen Sie sich eine Betrugsvorhersage mit dem AWS SDK for Python (Boto3)

Rufen Sie die `GetEventPrediction` API auf, um eine Betrugsvorhersage zu generieren. Im folgenden Beispiel wird davon ausgegangen, dass Sie den Vorgang abgeschlossen haben [Teil B: Generieren Sie Betrugsvorhersagen](#). Als Teil der Antwort erhalten Sie eine Modellbewertung sowie alle übereinstimmenden Regeln und die entsprechenden Ergebnisse. Weitere Beispiele für `GetEventPrediction` Anfragen finden Sie im [aws-fraud-detector-samples GitHub Repository](#).

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

fraudDetector.get_event_prediction(
    detectorId = 'sample_detector',
    eventId = '802454d3-f7d8-482d-97e8-c4b6db9a0428',
    eventName = 'sample_registration',
    eventTimestamp = '2020-07-13T23:18:21Z',
```

```
entities = [{'entityType':'sample_customer', 'entityId':'12345'}],
eventVariables = {
  'email_address' : 'johndoe@example.com',
  'ip_address' : '1.2.3.4'
}
)
```

## Stapelvoraussagen

Sie können einen Batch-Prognose-Job in Amazon Fraud Detector verwenden, um Vorhersagen für eine Reihe von Ereignissen zu erhalten, für die keine Bewertung in Echtzeit erforderlich ist. Sie könnten beispielsweise einen Auftrag zur Batch-Vorhersage erstellen, um einen Offline-Auftrag auszuführen, um das Risiko von Ereignissen auf stündlicher, täglicher oder wöchentlicher Basis rückwirkend zu bewerten.

Sie können einen Auftrag zur Batch-Vorhersage mithilfe der [Amazon Fraud Detector-Konsole](#) erstellen oder indem Sie den [CreateBatchPredictionJob](#) API-Vorgang über die AWS Befehlszeilenschnittstelle (AWSCLI) oder eines der Amazon Fraud Detector SDKs aufrufen.

### Themen

- [So funktionieren Batch-Prognosen](#)
- [Eingabe- und Ausgabedateien](#)
- [Batch-Prognosen abrufen](#)
- [Anleitung zu IAM-Rollen](#)
- [Holen Sie sich Betrugsvorhersagen im Batch-Modus mit dem AWS SDK for Python \(Boto3\)](#)

## So funktionieren Batch-Prognosen

Der `CreateBatchPredictionJob` API-Vorgang verwendet eine angegebene Detektorversion, um Vorhersagen auf der Grundlage von Daten zu treffen, die in einer CSV-Eingabedatei bereitgestellt werden, die sich in einem Amazon S3 S3-Bucket befindet. Die API gibt dann die resultierende CSV-Datei an einen S3-Bucket zurück.

Bei Batch-Prognoseaufträgen werden Modellwerte und Prognoseergebnisse auf dieselbe Weise wie bei der `GetEventPrediction` Operation berechnet. Ähnlich `GetEventPrediction` wie beim Erstellen eines Batch-Prognose-Jobs erstellen Sie zunächst einen Ereignistyp, trainieren optional ein Modell und erstellen dann eine Detektorversion, die die Ereignisse in Ihrem Batch-Job auswertet.



Die Preise für Risikobewertungen von Ereignissen, die anhand von Batch-Prognoseaufträgen bewertet werden, entsprechen den Preisen für die von der `GetEventPrediction` API erstellten Scores. Einzelheiten finden Sie unter [Amazon Fraud Detector — Preise](#).

Sie können jeweils nur einen Batch-Vorhersage-Job ausführen.

## Eingabe- und Ausgabedateien

Die CSV-Eingabedatei sollte Header enthalten, die dem Ereignistyp entsprechen, der der ausgewählten Detektorversion zugeordnet ist. Die maximale Größe der Eingabedatendatei beträgt 1 GB. Die Anzahl der Veranstaltungen hängt von der Größe Ihrer Veranstaltung ab.

Amazon Fraud Detector erstellt die Ausgabedatei im gleichen Bucket wie die Eingabedatei, sofern Sie keinen separaten Speicherort für die Ausgabedaten angeben. Die Ausgabedatei enthält die Originaldaten aus der Eingabedatei und den folgenden angefügten Spalten:

- **MODEL\_SCORES**— Gibt die Modellwerte für das Ereignis aus jedem Modell an, das der ausgewählten Detektorversion zugeordnet ist.
- **OUTCOMES**— Gibt die Ergebnisse des Ereignisses an, wie sie anhand der ausgewählten Detektorversion und ihrer Regeln bewertet wurden.
- **STATUS**— Gibt an, ob das Ereignis erfolgreich ausgewertet wurde. Wenn das Ereignis nicht erfolgreich ausgewertet wurde, wird in dieser Spalte ein Ursachencode für den Fehler angezeigt.
- **RULE\_RESULTS**— Eine Liste aller Regeln, die übereinstimmten, basierend auf dem Regelausführungsmodus.

## Batch-Prognosen abrufen

Bei den folgenden Schritten wird davon ausgegangen, dass Sie bereits einen Ereignistyp erstellt, ein Modell mit diesem Ereignistyp trainiert haben (optional) und eine Detektorversion für diesen Ereignistyp erstellt haben.

Um eine Batch-Vorhersage zu erhalten

1. Melden Sie bei der an AWS Management Console und öffnen Sie Fraud Detector Amazon-Konsole unter <https://console.aws.amazon.com/frauddetector>
2. Wählen Sie im linken Navigationsbereich der Amazon Fraud Detector Detector-Konsole Batch Predictions und dann New Batch Prediction aus.

3. Geben Sie unter Auftragsname einen Namen für Ihren Batch-Prognose-Job an. Wenn Sie keinen Namen angeben, generiert Amazon Fraud Detector nach dem Zufallsprinzip einen Jobnamen.
4. Wählen Sie unter Detektor den Detektor für diese Chargenvorhersage aus.
5. Wählen Sie unter Detektorversion die Detektorversion für diese Chargenvorhersage aus. Sie können in jedem Status eine Detektorversion auswählen. Wenn Ihr Melder eine Melderversion im Active Status hat, wird diese Version automatisch ausgewählt. Sie können diese Auswahl jedoch bei Bedarf auch ändern.
6. Wählen oder erstellen Sie unter IAM-Rolle eine Rolle, die Lese- und Schreibzugriff auf Ihre Amazon S3 S3-Buckets für Eingabe und Ausgabe hat. Weitere Informationen finden Sie unter [Anleitung zu IAM-Rollen](#).

Um Batch-Vorhersagen zu erhalten, muss die IAM-Rolle, die den `CreateBatchPredictionJob` Vorgang aufruft, über Leseberechtigungen für Ihren S3-Eingabe-Bucket und über Schreibberechtigungen für Ihren S3-Ausgabe-Bucket verfügen. Weitere Informationen zu Bucket-Berechtigungen finden Sie unter [Beispiele für Benutzerrichtlinien](#) im Amazon S3 S3-Benutzerhandbuch.

7. Geben Sie unter Speicherort der Eingabedaten den Amazon S3 S3-Speicherort Ihrer Eingabedaten an. Wenn Sie die Ausgabedatei in einem anderen S3-Bucket haben möchten, wählen Sie Separater Datenspeicherort für die Ausgabe aus und geben Sie den Amazon S3 S3-Speicherort für Ihre Ausgabedaten an.
8. (Optional) Erstellen Sie Tags für Ihren Auftrag zur Batch-Vorhersage.
9. Wählen Sie Starten.

Amazon Fraud Detector erstellt den Auftrag zur Batch-Vorhersage, und der Status des Jobs lautet `In progress`. Die Verarbeitungszeiten für Batch-Prediction-Jobs hängen von der Anzahl der Ereignisse und der Konfiguration Ihrer Detektorversion ab.

Um einen laufenden Batch-Prognoseauftrag zu beenden, rufen Sie die Detailseite des Batch-Prognoseauftrags auf, wählen Sie Aktionen und dann Batch-Vorhersage beenden aus. Wenn Sie einen Batch-Vorhersage-Job beenden, erhalten Sie keine Ergebnisse für den Job.

Wenn sich der Status des Batch-Prognoseauftrags in `ändertComplete`, können Sie die Ausgabe des Jobs aus dem angegebenen Amazon S3 S3-Ausgabebucket abrufen. Der Name der Ausgabedatei entspricht dem Format `batch prediction job name_file creation timestamp_output.csv`. Die Ausgabedatei eines Jobs mit dem Namen `mybatchjob` lautet beispielsweise `mybatchjob_1611170650_output.csv`.

Um nach bestimmten Ereignissen zu suchen, die im Rahmen eines Batch-Prognoseauftrags ausgewertet wurden, wählen Sie im linken Navigationsbereich der Amazon Fraud Detector Detector-Konsole die Option Frühere Prognosen durchsuchen aus.

Um einen abgeschlossenen Batch-Prognoseauftrag zu löschen, rufen Sie die Detailseite des Batch-Prognoseauftrags auf, wählen Sie Aktionen und dann Batch-Vorhersage löschen.

## Anleitung zu IAM-Rollen

Um Batch-Vorhersagen zu erhalten, muss die IAM-Rolle, die den [CreateBatchPredictionJob](#) Vorgang aufruft, über Leseberechtigungen für Ihren S3-Eingabe-Bucket und über Schreibberechtigungen für Ihren S3-Ausgabe-Bucket verfügen. Weitere Informationen zu Bucket-Berechtigungen finden Sie unter Beispiele für Benutzerrichtlinien im Amazon S3 S3-Benutzerhandbuch. In der Amazon Fraud Detector Detector-Konsole haben Sie drei Optionen, um eine IAM-Rolle für Batch Predictions auszuwählen:

1. Erstellen Sie eine Rolle, wenn Sie einen neuen Batch Prediction-Job erstellen.
2. Wählen Sie eine bestehende IAM-Rolle aus, die Sie zuvor in der Amazon Fraud Detector Detector-Konsole erstellt haben. Stellen Sie sicher, dass Sie der Rolle die `s3:PutObject` Berechtigung hinzufügen, bevor Sie diesen Schritt ausführen.
3. Geben Sie einen benutzerdefinierten ARN für eine zuvor erstellte IAM-Rolle ein.

Wenn Ihnen ein Fehler im Zusammenhang mit Ihrer IAM-Rolle angezeigt wird, gehen Sie folgendermaßen vor:

1. Ihre Amazon S3 S3-Eingabe- und Ausgabe-Bucket befinden sich in derselben Region wie Ihr Melder.
2. Die von Ihnen verwendete IAM-Rolle hat die `s3:GetObject` Berechtigung für Ihren S3-Eingabe-Bucket und die `s3:PutObject` Berechtigung für Ihren S3-Ausgabe-Bucket.
3. Die von Ihnen verwendete IAM-Rolle hat eine Vertrauensrichtlinie für Service `Principalfrauddetector.amazonaws.com`.

## Holen Sie sich Betrugsvorhersagen im Batch-Modus mit dem AWS SDK for Python (Boto3)

Das folgende Beispiel zeigt eine Beispielanforderung für die [CreateBatchPredictionJob](#) API. Ein Auftrag zur Batch-Vorhersage muss die folgenden vorhandenen Ressourcen enthalten: Detektor,

Detektorversion und Name des Ereignistyps. Im folgenden Beispiel wird davon ausgegangen, dass Sie einen Ereignistyp `sample_registration`, einen Detektor `sample_detector` und eine Detektorversion erstellt haben<sup>1</sup>.

```
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-
**'
)
```

## Erläuterungen zur Vorhersage

Vorhersageerklärungen geben Aufschluss darüber, wie sich jede Ereignisvariable auf den Betrugsvorhersagewert Ihres Modells ausgewirkt hat, und werden im Rahmen der Betrugsvorhersage automatisch generiert. Jede Betrugsvorhersage hat eine Risikobewertung zwischen 1 und 1 000. Vorhersageerklärungen geben Ihnen Details zum Einfluss jeder Ereignisvariable auf die Risikobewertungen in Bezug auf das Ausmaß (0–5, wobei 5 am höchsten ist) und die Richtung (Schleifenwert höher oder niedriger). Sie können Prognoseerklärungen auch für die folgenden Aufgaben verwenden:

- Um die wichtigsten Risikoindikatoren bei manuellen Inversitierungen zu identifizieren, wenn ein Ereignis zur Überprüfung markiert wird.
- Um Ursachen einzugrenzen, die zu falsch positiven Vorhersagen führen (z. B. hohe Risikowerte für legitime Ereignisse).
- Um Betrugsmuster über Ereignisdaten hinweg zu analysieren und Verzerrungen, falls vorhanden, in Ihrem Datensatz zu erkennen.

### Important

Vorhersageerklärungen werden automatisch generiert und sind nur für Modelle verfügbar, die am oder nach dem 30. Juni 2021 trainiert wurden. Um Vorhersageerklärungen für Modelle zu erhalten, die vor dem 30. Juni 2021 trainiert wurden, trainieren Sie diese Modelle erneut.

Vorhersageerklärungen enthalten die folgenden Werte für jede Ereignisvariable, die zum Trainieren des Modells verwendet wurde.

### Relative Auswirkungen

Bietet einen visuellen Verweis auf die Auswirkungen der Variablen in Bezug auf das Ausmaß auf die Betrugsvorhersagewerte. Die relativen Auswirkungswerte bestehen aus einer Sternbewertung (0–5, 5 ist die höchste) und der Richtung (erhöht/verringert) des Betrugsrisikos.

- Variablen, die das Betrugsrisiko erhöhen, werden durch rot farbige Sterne angezeigt. Je höher die Anzahl der rot farbigen Sterne ist, desto höher war der Betrugswert und die Wahrscheinlichkeit von Betrug stieg.
- Variablen, die das Betrugsrisiko verringert haben, werden durch grüne Sterne angezeigt. Je höher die Anzahl der grünen Farbstars, desto stärker stieg die Variable die Betrugsrisikobewertung herunter und die Wahrscheinlichkeit von Betrug nahm ab.
- Null Sternchen für alle Variablen deuten darauf hin, dass keine der Variablen allein das Betrugsrisiko erheblich verändert hat.

### Roherklärungswert

Stellt einen unformatierten, nicht interpretierten Wert bereit, der als Log-Odds des Betrugs dargestellt wird. Diese Werte liegen in der Regel zwischen -10 und +10, liegen aber im Bereich von – unendlich bis + unendlich.

- Ein positiver Wert gibt an, dass die Variable die Risikobewertung nach oben gestuft hat.
- Ein negativer Wert gibt an, dass die Variable die Risikobewertung nach unten gestuft hat.

In der Amazon Fraud Detector-Konsole werden die Werte der Prognoseerklärung wie folgt angezeigt. Die farbigen Sternbewertungen und die entsprechenden numerischen Rohwerte erleichtern das Erkennen des relativen Einflusses zwischen Variablen.

**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

## Anzeigen von Vorhersageerklärungen

Nachdem Sie Betrugsvorhersagen generiert haben, können Sie sich die Vorhersageerklärungen in der Amazon Fraud Detector-Konsole ansehen. Um die Prognoseerklärungen mithilfe von APIs aus dem AWS SDK anzuzeigen, müssen Sie zuerst die `ListEventPrediction` API aufrufen, um den Prognosezeitstempel für das Ereignis abzurufen, und dann die `GetEventPredictionMetadata` API aufrufen, um die Prognoseerklärungen abzurufen.

### Anzeigen von Vorhersageerklärungen mithilfe der Amazon Fraud Detector-Konsole

Um die Vorhersageerklärungen mit der Konsole anzuzeigen,

1. Öffnen Sie die -AWS-Konsole und melden Sie sich bei Ihrem -Konto an. Navigieren Sie zu Amazon Fraud Detector.
2. Wählen Sie im linken Navigationsbereich Nach Vorhersagen suchen aus.

3. Verwenden Sie die Filter Eigenschaft , Operator und Wert, um die Vorhersage auszuwählen, die Sie überprüfen möchten.
4. Stellen Sie im oberen Filter bereichsicher, dass Sie den Zeitraum auswählen, in dem die Vorhersage generiert wurde, die Sie überprüfen möchten.
5. Im Bereich Ergebnisse wird eine Liste aller im angegebenen Zeitraum generierten Vorhersagen angezeigt. Klicken Sie auf die Ereignis-ID der Vorhersage, um die Vorhersageerklärungen anzuzeigen.
6. Scrollen Sie nach unten zum Bereich Vorhersageerklärungen.
7. Legen Sie die Schaltfläche Erläuterungswert der Rohvorhersage anzeigen auf fest, um den Wert der Erläuterung der Rohvorhersage aller Variablen anzuzeigen.

## Anzeigen von Vorhersageerklärungen mit dem AWS SDK for Python (Boto3)

Die folgenden Beispiele zeigen Beispielanforderungen zum Anzeigen von Vorhersageerklärungen mithilfe von `ListEventPredictions` und `GetEventPredictionMetadata` APIs aus dem `AWSSDK`.

Beispiel 1: Abrufen einer Liste der neuesten Vorhersagen mithilfe der **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'
    }
)
```

Beispiel 2; Abrufen einer Liste früherer Vorhersagen für den Ereignistyp „Registrierung“ mithilfe der **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'  
}  
)
```

Beispiel 3: Abrufen von Details zu einer früheren Vorhersage für eine angegebene Ereignis-ID, einen Ereignistyp, eine Detektor-ID und eine Detektorversions-ID, die im angegebenen Zeitraum mithilfe der **-GetEventPredictionMetadataAPI** generiert wurde.

Das für diese Anforderung `predictionTimestamp` angegebene wird abgerufen, indem zuerst die `ListEventPredictions-API` aufgerufen wird.

```
import boto3  
fraudDetector = boto3.client('frauddetector')  
fraudDetector.get_event_prediction_metadata (  
    detectorId = 'sample_detector',  
    detectorVersionId = '1',  
    eventId = '802454d3-f7d8-482d-97e8-c4b6db9a0428',  
    eventName = 'sample_registration',  
    predictionTimestamp = '2021-07-13T21:18:21Z'  
)
```

## Verstehen, wie Vorhersageerklärungen berechnet werden

Amazon Fraud Detector verwendet [SHAP \(SHapeleye exPlanations\)](#), um einzelne Ereignisvorhersagen zu erklären, indem es die Roherklärungswerte jeder Ereignisvariable berechnet, die für das Modelltraining verwendet wird. Die Roherklärungswerte werden vom Modell als Teil des Klassifizierungsalgorithmus berechnet, wenn Vorhersagen generiert werden. Diese Roherklärungswerte stellen den Beitrag jeder Eingabe zum Logarithmus der Betrugswahrscheinlichkeiten dar. Die Roherklärungswerte (von -unendlich bis +unendlich) werden mithilfe einer Zuordnung in einen relativen Auswirkungswert (-5 bis +5) konvertiert. Der Wert für die relative Auswirkung, der aus dem Roherklärungswert abgeleitet wird, stellt die Häufigkeit dar, mit der die Wahrscheinlichkeit zunimmt, dass der Betrug (positive) oder der Legit-Wert (negative) zunimmt, wodurch die Vorhersageerklärungen leichter verständlich sind.



# Sicherheit in Amazon Fraud Detector

Die Sicherheit in der Cloud hat für AWS höchste Priorität. Als AWS-Kunde profitieren Sie von Rechenzentren und Netzwerkarchitekturen, die eingerichtet wurden, um die Anforderungen der anspruchsvollsten Organisationen in puncto Sicherheit zu erfüllen.

Sicherheit ist eine übergreifende Verantwortlichkeit zwischen AWS und Ihnen. Das [Modell der geteilten Verantwortung](#) beschreibt dies als Sicherheit der Cloud selbst und Sicherheit in der Cloud:

- Sicherheit der Cloud selbst – AWS ist dafür verantwortlich, die Infrastruktur zu schützen, mit der AWS-Services in der AWS Cloud ausgeführt werden. AWS stellt Ihnen außerdem Services bereit, die Sie sicher nutzen können. Auditoren von Drittanbietern testen und überprüfen die Effektivität unserer Sicherheitsmaßnahmen im Rahmen der [AWS-Compliance-Programme](#) regelmäßig. Weitere Informationen zu den Compliance-Programmen, die für Amazon Fraud Detector gelten, finden Sie unter [Im Rahmen des Compliance-Programms zugelassene AWS-Services](#).
- Sicherheit in der Cloud – Ihr Verantwortungsumfang wird durch den AWS-Dienst bestimmt, den Sie verwenden. Sie sind auch für andere Faktoren verantwortlich, etwa für die Vertraulichkeit Ihrer Daten, für die Anforderungen Ihres Unternehmens und für die geltenden Gesetze und Vorschriften.

Diese Dokumentation hilft Ihnen zu verstehen, wie Sie das Modell der geteilten Verantwortung bei der Verwendung von Amazon Fraud Detector einsetzen können. Die folgenden Themen zeigen Ihnen, wie Sie Amazon Fraud Detector so konfigurieren, dass Ihre Sicherheits- und Compliance-Ziele erreicht werden. Sie erfahren auch, wie Sie andere -AWSServices verwenden, die Sie bei der Überwachung und Sicherung Ihrer Amazon Fraud Detector-Ressourcen unterstützen.

## Themen

- [Datenschutz in Amazon Fraud Detector](#)
- [Identity and Access Management für Amazon Fraud Detector](#)
- [Protokollierung und Überwachung in Amazon Fraud Detector](#)
- [Compliance-Validierung für Amazon Fraud Detector](#)
- [Ausfallsicherheit in Amazon Fraud Detector](#)
- [Infrastruktursicherheit in Amazon Fraud Detector](#)

# Datenschutz in Amazon Fraud Detector

Das Modell der AWS geteilten gilt für den Datenschutz in Amazon Fraud Detector. <https://aws.amazon.com/compliance/shared-responsibility-model/> Wie in diesem Modell beschrieben, ist AWS für den Schutz der globalen Infrastruktur verantwortlich, in der die gesamte AWS Cloud ausgeführt wird. Sie sind dafür verantwortlich, die Kontrolle über Ihre in dieser Infrastruktur gehosteten Inhalte zu behalten. Sie sind auch für die Sicherheitskonfiguration und die Verwaltungsaufgaben für die von Ihnen verwendeten AWS-Services verantwortlich. Weitere Informationen zum Datenschutz finden Sie unter [Häufig gestellte Fragen zum Datenschutz](#). Informationen zum Datenschutz in Europa finden Sie im Blog-Beitrag [AWS-Modell der geteilten Verantwortung und in der DSGVO](#) im AWS-Sicherheitsblog.

Aus Datenschutzgründen empfehlen wir, AWS-Konto-Anmeldeinformationen zu schützen und einzelne Benutzer mit AWS IAM Identity Center oder AWS Identity and Access Management (IAM) einzurichten. So erhält jeder Benutzer nur die Berechtigungen, die zum Durchführen seiner Aufgaben erforderlich sind. Außerdem empfehlen wir, die Daten mit folgenden Methoden zu schützen:

- Verwenden Sie für jedes Konto die Multi-Faktor Authentifizierung (MFA).
- Verwenden Sie SSL/TLS für die Kommunikation mit AWS-Ressourcen. Wir benötigen TLS 1.2 und empfehlen TLS 1.3.
- Richten Sie die API und die Protokollierung von Benutzeraktivitäten mit AWS CloudTrail ein.
- Verwenden Sie AWS-Verschlüsselungslösungen zusammen mit allen Standardsicherheitskontrollen in AWS-Services.
- Verwenden Sie erweiterte verwaltete Sicherheitsservices wie Amazon Macie, die dabei helfen, in Amazon S3 gespeicherte persönliche Daten zu erkennen und zu schützen.
- Wenn Sie für den Zugriff auf AWS über eine Befehlszeilenschnittstelle oder über eine API FIPS 140-2-validierte kryptografische Module benötigen, verwenden Sie einen FIPS-Endpunkt. Weitere Informationen über verfügbare FIPS-Endpunkte finden Sie unter [Federal Information Processing Standard \(FIPS\) 140-2](#).

Wir empfehlen dringend, in Freitextfeldern, z. B. im Feld Name, keine vertraulichen oder sensiblen Informationen wie die E-Mail-Adressen Ihrer Kunden einzugeben. Dies gilt auch, wenn Sie mit Amazon Fraud Detector oder anderen AWS-Services über die Konsole, API/AWS CLI, oder AWS SDKs arbeiten. Alle Daten, die Sie in Tags oder Freitextfelder eingeben, die für Namen verwendet werden, können für Abrechnungs- oder Diagnoseprotokolle verwendet werden. Wenn Sie eine URL

für einen externen Server bereitstellen, empfehlen wir dringend, keine Anmeldeinformationen zur Validierung Ihrer Anforderung an den betreffenden Server in die URL einzuschließen.

## Verschlüsseln von Daten im Ruhezustand

Amazon Fraud Detector verschlüsselt Ihre Daten im Ruhezustand mit einem Verschlüsselungsschlüssel Ihrer Wahl. Sie können eine der folgenden Optionen auswählen:

- Ein AWS-eigener [KMS-Schlüssel](#) . Wenn Sie keinen Verschlüsselungsschlüssel angeben, werden Ihre Daten standardmäßig mit diesem Schlüssel verschlüsselt.
- Ein vom Kunden [verwalteter KMS-Schlüssel](#) . Sie können den Zugriff auf Ihren vom Kunden verwalteten KMS-Schlüssel mithilfe von [Schlüsselrichtlinien](#) steuern. Informationen zum Erstellen und Verwalten von kundenverwalteten KMS-Schlüsseln finden Sie unter [Schlüsselverwaltung](#).

## Verschlüsseln von Daten während der Übertragung

Amazon Fraud Detector kopiert Daten aus Ihrem Konto und verarbeitet sie in einem internen AWS System. Standardmäßig verwendet Amazon Fraud Detector TLS 1.2 mit AWS Zertifikaten, um Daten während der Übertragung zu verschlüsseln.

## Schlüsselverwaltung

Amazon Fraud Detector verschlüsselt Ihre Daten mit einem von zwei Schlüsseltypen:

- Ein AWS-eigener [KMS-Schlüssel](#) . Dies ist die Standardeinstellung.
- Ein vom Kunden [verwalteter KMS-Schlüssel](#) .

## Erstellen eines vom Kunden verwalteten KMS-Schlüssels

Sie können vom Kunden verwaltete KMS-Schlüssel entweder über die AWS KMS-Konsole oder die [CreateKey](#) API erstellen. Stellen Sie beim Erstellen des Schlüssels sicher, dass Sie

- Wählen Sie einen vom Kunden verwalteten KMS-Schlüssel mit symmetrischer Verschlüsselung aus. Amazon Fraud Detector unterstützt keine asymmetrischen KMS-Schlüssel. Weitere Informationen finden Sie unter [Asymmetrische Schlüssel in AWS KMS](#) im Entwicklerhandbuch für AWS Key Management Service.

- Erstellen Sie einen KMS-Schlüssel für eine einzelne Region. Amazon Fraud Detector unterstützt keine multiregionalen KMS-Schlüssel. Weitere Informationen finden Sie unter [Multiregionale Schlüssel in AWS KMS](#) im Entwicklerhandbuch für AWS Key Management Service.
- Geben Sie die folgende [Schlüsselrichtlinie](#) an, um Amazon Fraud Detector Berechtigungen zur Verwendung des Schlüssels zu erteilen.

```
{
  "Effect": "Allow",
  "Principal": {
    "Service": "frauddetector.amazonaws.com"
  },
  "Action": [
    "kms:Encrypt",
    "kms:Decrypt",
    "kms:ReEncrypt*",
    "kms:GenerateDataKey*",
    "kms:DescribeKey",
    "kms:CreateGrant",
    "kms:RetireGrant"
  ],
  "Resource": "*"
}
```

Informationen zu Schlüsselrichtlinien finden Sie unter [Verwenden von Schlüsselrichtlinien in AWS KMS](#) im Entwicklerhandbuch für AWS Key Management Service.

## Verschlüsseln von Daten mit vom Kunden verwaltetem KMS-Schlüssel

Verwenden Sie die [PutKMSEncryptionKey](#)-API von Amazon Fraud Detector, um Ihre Amazon Fraud Detector-Daten im Ruhezustand mit dem vom Kunden verwalteten KMS-Schlüssel zu verschlüsseln. Sie können die Verschlüsselungskonfiguration jederzeit über die [PutKMSEncryptionKey](#)-API ändern.

### Wichtige Hinweise zu verschlüsselten Daten

- Daten, die nach der Einrichtung des vom Kunden verwalteten KMS-Schlüssels generiert wurden, werden verschlüsselt. Daten, die vor der Einrichtung des vom Kunden verwalteten KMS-Schlüssels generiert wurden, bleiben unverschlüsselt.

- Wenn der vom Kunden verwaltete KMS-Schlüssel geändert wird, werden die Daten, die mit der vorherigen Verschlüsselungskonfiguration verschlüsselt wurden, nicht erneut verschlüsselt.

## Daten anzeigen

Wenn Sie den vom Kunden verwalteten KMS-Schlüssel verwenden, um Ihre Amazon Fraud Detector-Daten zu verschlüsseln, können die mit dieser Methode verschlüsselten Daten nicht mithilfe von Filtern im Bereich Frühere Suchvorhersagen der Amazon Fraud Detector-Konsole durchsucht werden. Um vollständige Suchergebnisse sicherzustellen, verwenden Sie eine oder mehrere der folgenden Eigenschaften, um Ergebnisse zu filtern:

- Ereignis-ID
- Bewertungszeitstempel
- Detektorstatus
- Detektor-Version
- Modellversion
- Modelltyp
- Status der Regelbewertung
- Regelausführungsmodus
- Status der Regelübereinstimmung
- Regelversion
- Variable Datenquelle

Wenn der vom Kunden verwaltete KMS-Schlüssel entweder gelöscht wurde oder gelöscht werden soll, sind Ihre Daten möglicherweise nicht verfügbar. Weitere Informationen finden Sie unter [Löschen von KMS-Schlüsseln](#).

## Amazon Fraud Detector und Schnittstellen-VPC-Endpunkte (AWS PrivateLink)

Sie können eine private Verbindung zwischen Ihrer VPC und Amazon Fraud Detector herstellen, indem Sie einen Schnittstellen-VPC-Endpunkt erstellen. Schnittstellenendpunkte werden von [unterstützt AWS PrivateLink](#), einer Technologie, mit der Sie ohne Internet-Gateway, NAT-Gerät, VPN-Verbindung oder AWS Direct Connect-Verbindung privat auf Amazon Fraud Detector-APIs zugreifen

können. Instances in Ihrer VPC benötigen für die Kommunikation mit Amazon Fraud Detector APIs keine öffentlichen IP-Adressen. Der Datenverkehr zwischen Ihrer VPC und Amazon Fraud Detector verlässt das Amazon-Netzwerk nicht.

Jeder Schnittstellenendpunkt wird durch eine oder mehrere [Elastic-Netzwerk-Schnittstellen](#) in Ihren Subnetzen dargestellt.

Weitere Informationen finden Sie unter [Schnittstellen-VPC-Endpunkte \(AWS PrivateLink\)](#) im Amazon-VPC-Benutzerhandbuch.

## Überlegungen zu Amazon Fraud Detector VPC-Endpunkten

Bevor Sie einen Schnittstellen-VPC-Endpunkt für Amazon Fraud Detector einrichten, lesen Sie die [Eigenschaften und Einschränkungen von Schnittstellenendpunkten](#) im Amazon-VPC-Benutzerhandbuch.

Amazon Fraud Detector unterstützt Aufrufe aller API-Aktionen aus Ihrer VPC.

VPC-Endpunktrichtlinien werden für Amazon Fraud Detector unterstützt. Standardmäßig ist der vollständige Zugriff auf Amazon Fraud Detector über den Endpunkt erlaubt. Weitere Informationen finden Sie unter [Steuerung des Zugriffs auf Services mit VPC-Endpunkten](#) im Amazon-VPC-Benutzerhandbuch.

## Erstellen eines Schnittstellen-VPC-Endpunkts für Amazon Fraud Detector

Sie können einen VPC-Endpunkt für den Amazon Fraud Detector-Service entweder über die Amazon VPC-Konsole oder die AWS Command Line Interface (AWS CLI) erstellen. Weitere Informationen finden Sie unter [Erstellung eines Schnittstellenendpunkts](#) im Benutzerhandbuch für Amazon VPC.

Erstellen Sie einen VPC-Endpunkt für Amazon Fraud Detector mit dem folgenden Servicenamen:

- `com.amazonaws.region.frauddetector`

Wenn Sie ein privates DNS für den Endpunkt aktivieren, können Sie API-Anforderungen an Amazon Fraud Detector unter Verwendung seines standardmäßigen DNS-Namens für die Region senden, z. B. `frauddetector.us-east-1.amazonaws.com`.

Weitere Informationen finden Sie unter [Zugriff auf einen Service über einen Schnittstellenendpunkt](#) im Benutzerhandbuch für Amazon VPC.

## Erstellen einer VPC-Endpunktrichtlinie für Amazon Fraud Detector

Sie können eine Richtlinie für Schnittstellen-VPC-Endpunkte für Amazon Fraud Detector erstellen, um Folgendes anzugeben:

- Der Prinzipal, der die Aktionen ausführen kann
- Aktionen, die ausgeführt werden können
- Ressourcen, für die Aktionen ausgeführt werden können

Weitere Informationen finden Sie unter [Steuerung des Zugriffs auf Services mit VPC-Endpunkten](#) im Amazon VPC User Guide.

Die folgende Beispiel-VPC-Endpunktrichtlinie gibt an, dass alle Benutzer, die Zugriff auf den VPC-Schnittstellenendpunkt haben, auf den Amazon Fraud Detector-Detektor mit dem Namen zugreifen dürfen `my_detector`.

```
{
  "Statement": [
    {
      "Action": "frauddetector:*Detector",
      "Effect": "Allow",
      "Resource": "arn:aws:frauddetector:us-east-1:123456789012:detector/
my_detector",
      "Principal": "*"
    }
  ]
}
```

In diesem Beispiel wird Folgendes verweigert:

- Andere API-Aktionen von Amazon Fraud Detector
- Aufrufen der API von Amazon Fraud Detector `GetEventPrediction`

### Note

In diesem Beispiel können Benutzer weiterhin andere API-Aktionen von Amazon Fraud Detector außerhalb der VPC ausführen. Weitere Informationen zum Einschränken von API-

Aufrufen von innerhalb der VPC finden Sie unter [Identitätsbasierte Amazon Fraud Detector-Richtlinien](#).

## Abmeldung von der Verwendung Ihrer Daten zur Serviceverbesserung

Historische Ereignisdaten, die Sie zum Trainieren von Modellen und Generieren von Vorhersagen bereitstellen, werden ausschließlich verwendet, um Ihren Service bereitzustellen und zu verwalten. Diese Daten können auch verwendet werden, um die Qualität von Amazon Fraud Detector zu verbessern. Ihr Vertrauen, Ihr Datenschutz und die Sicherheit Ihrer Inhalte haben höchste Priorität und stellen sicher, dass unsere Nutzung unseren Verpflichtungen Ihnen gegenüber entspricht. Weitere Informationen finden Sie unter [Häufig gestellte Fragen zum Datenschutz](#)

Sie können sich dafür entscheiden, dass Ihre Ereignisdaten zur Entwicklung oder Verbesserung der Qualität von Amazon Fraud Detector verwendet werden, indem Sie die Seite [KI-Services-Opt-Out-Richtlinien](#) im AWS Organizations-Benutzerhandbuch besuchen und den dort erläuterten Prozess befolgen.

### Note

Ihre AWS-Konten müssen zentral von AWS Organizations verwaltet werden, damit Sie die Opt-Out-Richtlinie verwenden können. Wenn Sie noch keine Organisation für Ihre AWS-Konten erstellt haben, besuchen [Sie Erstellen und Verwalten einer Organisationsseite](#) und folgen Sie dem dort beschriebenen Prozess.

## Identity and Access Management für Amazon Fraud Detector

AWS Identity and Access Management (IAM) ist ein AWS-Service, mit dem Administratoren den Zugriff auf AWS-Ressourcen sicher steuern können. IAM-Administratoren steuern, wer authentifiziert (angemeldet) und autorisiert (im Besitz von Berechtigungen) ist, Amazon Fraud Detector-Ressourcen zu nutzen. IAM ist ein AWS-Service, den Sie ohne zusätzliche Kosten verwenden können.

### Themen

- [Zielgruppe](#)
- [Authentifizierung mit Identitäten](#)
- [Verwalten des Zugriffs mit Richtlinien](#)



- [Funktionsweise von Amazon Fraud Detector mit IAM](#)
- [Beispiele für identitätsbasierte Amazon Fraud Detector-Richtlinien](#)
- [Confused-Deputy-Prävention](#)
- [Fehlerbehebung für Identität und Zugriff auf Amazon Fraud Detector](#)

## Zielgruppe

Wie Sie AWS Identity and Access Management (IAM) verwenden, unterscheidet sich je nach Ihrer Arbeit in Amazon Fraud Detector.

**Service-Benutzer** – Wenn Sie den Amazon Fraud Detector-Service zur Ausführung von Aufgaben verwenden, stellt Ihnen Ihr Administrator die Anmeldeinformationen und Berechtigungen bereit, die Sie benötigen. Wenn Sie zur Ausführung von Aufgaben weitere Funktionen von Amazon Fraud Detector verwenden, benötigen Sie möglicherweise zusätzliche Berechtigungen. Wenn Sie die Featuresweise der Zugriffskontrolle nachvollziehen, wissen Sie bereits, welche Berechtigungen Sie von Ihrem Administrator anfordern müssen. Wenn Sie nicht auf ein Feature in Amazon Fraud Detector zugreifen können, finden Sie weitere Informationen unter [Fehlerbehebung für Identität und Zugriff auf Amazon Fraud Detector](#).

**Service-Administrator** – Wenn Sie in Ihrem Unternehmen für die Ressourcen von Amazon Fraud Detector verantwortlich sind, haben Sie wahrscheinlich vollständigen Zugriff auf Amazon Fraud Detector. Ihre Aufgabe besteht darin, zu bestimmen, auf welche Funktionen und Ressourcen von Amazon Fraud Detector Ihre Service-Benutzer zugreifen sollen. Sie müssen dann Anträge an Ihren IAM-Administrator stellen, um die Berechtigungen Ihrer Servicenutzer zu ändern. Lesen Sie die Informationen auf dieser Seite, um die Grundkonzepte von IAM nachzuvollziehen. Weitere Informationen dazu, wie Ihr Unternehmen IAM mit Amazon Fraud Detector verwenden kann, finden Sie unter [Funktionsweise von Amazon Fraud Detector mit IAM](#).

**IAM-Administrator** – Wenn Sie als IAM-Administrator fungieren, sollten Sie Einzelheiten dazu kennen, wie Sie Richtlinien zur Verwaltung des Zugriffs auf Amazon Fraud Detector verfassen können. Beispiele für identitätsbasierte Amazon Fraud Detector-Richtlinien, die Sie in IAM verwenden können, finden Sie unter [Beispiele für identitätsbasierte Amazon Fraud Detector-Richtlinien](#).

## Authentifizierung mit Identitäten

Authentifizierung ist die Art, wie Sie sich mit Ihren Anmeldeinformationen bei AWS anmelden. Die Authentifizierung (Anmeldung bei AWS) muss als Root-Benutzer des AWS-Kontos, als IAM-Benutzer oder durch Übernahme einer IAM-Rolle erfolgen.

Sie können sich bei AWS als Verbundidentität mit Anmeldeinformationen anmelden, die über eine Identitätsquelle bereitgestellt werden. Benutzer von AWS IAM Identity Center (IAM Identity Center), die Single-Sign-on-Authentifizierung Ihres Unternehmens und Anmeldeinformationen für Google oder Facebook sind Beispiele für Verbundidentitäten. Wenn Sie sich als Verbundidentität anmelden, hat der Administrator vorher mithilfe von IAM-Rollen einen Identitätsverbund eingerichtet. Wenn Sie auf AWS mithilfe des Verbunds zugreifen, übernehmen Sie indirekt eine Rolle.

Je nachdem, welcher Benutzertyp Sie sind, können Sie sich bei der AWS Management Console oder beim AWS-Zugriffsportal anmelden. Weitere Informationen zum Anmelden bei AWS finden Sie unter [So melden Sie sich bei Ihrem AWS-Konto an](#) im Benutzerhandbuch von AWS-Anmeldung.

Bei programmgesteuertem Zugriff auf AWS bietet AWS ein Software Development Kit (SDK) und eine Command Line Interface (CLI, Befehlszeilenschnittstelle) zum kryptographischen Signieren Ihrer Anfragen mit Ihren Anmeldeinformationen. Wenn Sie keine AWS-Tools verwenden, müssen Sie Anforderungen selbst signieren. Weitere Informationen zur Verwendung der empfohlenen Methode zum eigenen Signieren von Anforderungen finden Sie unter [Signieren von AWS-API-Anforderungen](#) im IAM-Benutzerhandbuch.

Unabhängig von der verwendeten Authentifizierungsmethode müssen Sie möglicherweise zusätzliche Sicherheitsinformationen angeben. AWS empfiehlt beispielsweise die Verwendung von Multi-Faktor Authentifizierung (MFA), um die Sicherheit Ihres Kontos zu verbessern. Weitere Informationen finden Sie unter [Multi-Faktor-Authentifizierung](#) im AWS IAM Identity Center-Benutzerhandbuch und [Verwenden der Multi-Faktor-Authentifizierung \(MFA\) in AWS](#) im IAM-Benutzerhandbuch.

## AWS-Konto-Root-Benutzer

Wenn Sie ein AWS-Konto neu erstellen, beginnen Sie mit einer Anmeldeidentität, die vollständigen Zugriff auf alle AWS-Services und Ressourcen des Kontos hat. Diese Identität wird als AWS-Konto-Root-Benutzer bezeichnet. Für den Zugriff auf den Root-Benutzer müssen Sie sich mit der E-Mail-Adresse und dem Passwort anmelden, die zur Erstellung des Kontos verwendet wurden. Wir raten ausdrücklich davon ab, den Root-Benutzer für Alltagsaufgaben zu verwenden. Schützen Sie Ihre Root-Benutzer-Anmeldeinformationen und verwenden Sie diese, um die Aufgaben auszuführen, die nur der Root-Benutzer ausführen kann. Eine vollständige Liste der Aufgaben, für die Sie sich als Root-Benutzer anmelden müssen, finden Sie unter [Aufgaben, die Root-Benutzer-Anmeldeinformationen erfordern](#) im IAM-Benutzerhandbuch.

## Benutzer und Gruppen

Ein [IAM-Benutzer](#) ist eine Identität in Ihrem AWS-Konto mit bestimmten Berechtigungen für eine einzelne Person oder eine einzelne Anwendung. Wenn möglich, empfehlen wir, temporäre Anmeldeinformationen zu verwenden, anstatt IAM-Benutzer zu erstellen, die langfristige Anmeldeinformationen wie Passwörter und Zugriffsschlüssel haben. Bei speziellen Anwendungsfällen, die langfristige Anmeldeinformationen mit IAM-Benutzern erfordern, empfehlen wir jedoch, die Zugriffsschlüssel zu rotieren. Weitere Informationen finden Sie unter [Regelmäßiges Rotieren von Zugriffsschlüsseln für Anwendungsfälle, die langfristige Anmeldeinformationen erfordern](#) im IAM-Benutzerhandbuch.

Eine [IAM-Gruppe](#) ist eine Identität, die eine Sammlung von IAM-Benutzern angibt. Sie können sich nicht als Gruppe anmelden. Mithilfe von Gruppen können Sie Berechtigungen für mehrere Benutzer gleichzeitig angeben. Gruppen vereinfachen die Verwaltung von Berechtigungen, wenn es zahlreiche Benutzer gibt. Sie könnten beispielsweise einer Gruppe mit dem Namen IAMAdmins Berechtigungen zum Verwalten von IAM-Ressourcen erteilen.

Benutzer unterscheiden sich von Rollen. Ein Benutzer ist einer einzigen Person oder Anwendung eindeutig zugeordnet. Eine Rolle kann von allen Personen angenommen werden, die sie benötigen. Benutzer besitzen dauerhafte Anmeldeinformationen. Rollen stellen temporäre Anmeldeinformationen bereit. Weitere Informationen finden Sie unter [Erstellen eines IAM-Benutzers \(anstatt einer Rolle\)](#) im IAM-Benutzerhandbuch.

## IAM-Rollen

Eine [IAM-Rolle](#) ist eine Identität in Ihrem AWS-Konto mit spezifischen Berechtigungen. Sie ist einem IAM-Benutzer vergleichbar, ist aber nicht mit einer bestimmten Person verknüpft. Sie können vorübergehend eine IAM-Rolle in der AWS Management Console übernehmen, indem Sie [Rollen wechseln](#). Sie können eine Rolle annehmen, indem Sie eine AWS CLI oder AWS-API-Operation aufrufen oder eine benutzerdefinierte URL verwenden. Weitere Informationen zu Methoden für die Verwendung von Rollen finden Sie unter [Verwenden von IAM-Rollen](#) im IAM-Benutzerhandbuch.

IAM-Rollen mit temporären Anmeldeinformationen sind in folgenden Situationen hilfreich:

- **Verbundbenutzerzugriff:** Um einer Verbundidentität Berechtigungen zuzuweisen, erstellen Sie eine Rolle und definieren Berechtigungen für die Rolle. Wird eine Verbundidentität authentifiziert, so wird die Identität der Rolle zugeordnet und erhält die von der Rolle definierten Berechtigungen. Informationen zu Rollen für den Verbund finden Sie unter [Erstellen von Rollen für externe Identitätsanbieter](#) im IAM-Benutzerhandbuch. Wenn Sie IAM Identity Center verwenden,

konfigurieren Sie einen Berechtigungssatz. Wenn Sie steuern möchten, worauf Ihre Identitäten nach der Authentifizierung zugreifen können, korreliert IAM Identity Center den Berechtigungssatz mit einer Rolle in IAM. Informationen zu Berechtigungssätzen finden Sie unter [Berechtigungssätze](#) im AWS IAM Identity Center-Benutzerhandbuch.

- Temporäre IAM-Benutzerberechtigungen: Ein IAM-Benutzer oder eine -Rolle kann eine IAM-Rolle übernehmen, um vorübergehend andere Berechtigungen für eine bestimmte Aufgabe zu erhalten.
- Kontoübergreifender Zugriff – Sie können eine IAM-Rolle verwenden, um einem vertrauenswürdigen Prinzipal in einem anderen Konto den Zugriff auf Ressourcen in Ihrem Konto zu ermöglichen. Rollen stellen die primäre Möglichkeit dar, um kontoübergreifendem Zugriff zu gewähren. In einigen AWS-Services können Sie jedoch eine Richtlinie direkt an eine Ressource anfügen (anstatt eine Rolle als Proxy zu verwenden). Informationen zu den Unterschieden zwischen Rollen und ressourcenbasierten Richtlinien für den kontoübergreifenden Zugriff finden Sie unter [So unterscheiden sich IAM-Rollen von ressourcenbasierten Richtlinien](#) im IAM-Benutzerhandbuch.
- Serviceübergreifender Zugriff: Einige AWS-Services verwenden Features in anderen AWS-Services. Wenn Sie beispielsweise einen Aufruf in einem Service tätigen, führt dieser Service häufig Anwendungen in Amazon EC2 aus oder speichert Objekte in Amazon S3. Ein Dienst kann dies mit den Berechtigungen des aufrufenden Prinzipals mit einer Servicerolle oder mit einer serviceverknüpften Rolle tun.
- Forward access sessions (FAS) – Wenn Sie einen IAM-Benutzer oder eine IAM-Rolle zum Ausführen von Aktionen in AWS verwenden, gelten Sie als Prinzipal. Bei einigen Services könnte es Aktionen geben, die dann eine andere Aktion in einem anderen Service auslösen. FAS verwendet die Berechtigungen des Prinzipals, der einen AWS-Service aufruft, in Kombination mit der Anforderung an den AWS-Service, Anforderungen an nachgelagerte Services zu stellen. FAS-Anfragen werden nur dann gestellt, wenn ein Service eine Anfrage erhält, die eine Interaktion mit anderen AWS-Services oder -Ressourcen erfordert. In diesem Fall müssen Sie über Berechtigungen zum Ausführen beider Aktionen verfügen. Einzelheiten zu den Richtlinien für FAS-Anfragen finden Sie unter [Zugriffssitzungen weiterleiten](#).
- Servicerolle: Eine Servicerolle ist eine [IAM-Rolle](#), die ein Service übernimmt, um Aktionen in Ihrem Namen auszuführen. Ein IAM-Administrator kann eine Servicerolle innerhalb von IAM erstellen, ändern und löschen. Weitere Informationen finden Sie unter [Erstellen einer Rolle zum Delegieren von Berechtigungen an einen AWS-Service](#) im IAM-Benutzerhandbuch.
- Serviceverknüpfte Rolle: Eine serviceverknüpfte Rolle ist ein Typ von Servicerolle, die mit einem AWS-Service verknüpft ist. Der Service kann die Rolle übernehmen, um eine Aktion in Ihrem Namen auszuführen. Serviceverknüpfte Rollen werden in Ihrem AWS-Konto angezeigt und

gehören zum Service. Ein IAM-Administrator kann die Berechtigungen für serviceverbundene Rollen anzeigen, aber nicht bearbeiten.

- Anwendungen in Amazon EC2: Sie können eine IAM-Rolle verwenden, um temporäre Anmeldeinformationen für Anwendungen zu verwalten, die auf einer EC2-Instance ausgeführt werden und AWS CLI- oder AWS-API-Anforderungen durchführen. Das ist eher zu empfehlen, als Zugriffsschlüssel innerhalb der EC2-Instance zu speichern. Erstellen Sie ein Instance-Profil, das an die Instance angefügt ist, um eine AWS-Rolle einer EC2-Instance zuzuweisen und die Rolle für sämtliche Anwendungen der Instance bereitzustellen. Ein Instance-Profil enthält die Rolle und ermöglicht, dass Programme, die in der EC2-Instance ausgeführt werden, temporäre Anmeldeinformationen erhalten. Weitere Informationen finden Sie unter [Verwenden einer IAM-Rolle zum Erteilen von Berechtigungen für Anwendungen, die auf Amazon EC2-Instances ausgeführt werden](#) im IAM-Benutzerhandbuch.

Informationen dazu, wann Sie IAM-Rollen oder IAM-Benutzer verwenden sollten, finden Sie unter [Erstellen einer IAM-Rolle \(anstatt eines Benutzers\)](#) im IAM-Benutzerhandbuch.

## Verwalten des Zugriffs mit Richtlinien

Für die Zugriffssteuerung in AWS erstellen Sie Richtlinien und weisen diese den AWS-Identitäten oder -Ressourcen zu. Eine Richtlinie ist ein Objekt in AWS, das, wenn es einer Identität oder Ressource zugeordnet wird, deren Berechtigungen definiert. AWS wertet diese Richtlinien aus, wenn ein Prinzipal (Benutzer, Root-Benutzer oder Rollensitzung) eine Anforderung stellt. Berechtigungen in den Richtlinien bestimmen, ob die Anforderung zugelassen oder abgelehnt wird. Die meisten Richtlinien werden in AWS als JSON-Dokumente gespeichert. Weitere Informationen zu Struktur und Inhalten von JSON-Richtliniendokumenten finden Sie unter [Übersicht über JSON-Richtlinien](#) im IAM-Benutzerhandbuch.

Administratoren können mithilfe von AWS-JSON-Richtlinien festlegen, wer zum Zugriff auf was berechtigt ist. Das bedeutet, welcher Prinzipal kann Aktionen für welche Ressourcen und unter welchen Bedingungen ausführen.

Standardmäßig haben Benutzer, Gruppen und Rollen keine Berechtigungen. Ein IAM-Administrator muss IAM-Richtlinien erstellen, die Benutzern die Berechtigung erteilen, Aktionen für die Ressourcen auszuführen, die sie benötigen. Der Administrator kann dann die IAM-Richtlinien zu Rollen hinzufügen, und Benutzer können die Rollen annehmen.

IAM-Richtlinien definieren Berechtigungen für eine Aktion unabhängig von der Methode, die Sie zur Ausführung der Aktion verwenden. Angenommen, es gibt eine Richtlinie, die Berechtigungen für die

`iam:GetRole`-Aktion erteilt. Ein Benutzer mit dieser Richtlinie kann Benutzerinformationen über die AWS Management Console, die AWS CLI oder die AWS -API abrufen.

## Identitätsbasierte Richtlinien

Identitätsbasierte Richtlinien sind JSON-Berechtigungsrichtliniendokumente, die Sie einer Identität anfügen können, wie z. B. IAM-Benutzern, -Benutzergruppen oder -Rollen. Diese Richtlinien steuern, welche Aktionen die Benutzer und Rollen für welche Ressourcen und unter welchen Bedingungen ausführen können. Informationen zum Erstellen identitätsbasierter Richtlinien finden Sie unter [Erstellen von IAM-Richtlinien](#) im IAM-Benutzerhandbuch.

Identitätsbasierte Richtlinien können weiter als Inline-Richtlinien oder verwaltete Richtlinien kategorisiert werden. Inline-Richtlinien sind direkt in einen einzelnen Benutzer, eine einzelne Gruppe oder eine einzelne Rolle eingebettet. Verwaltete Richtlinien sind eigenständige Richtlinien, die Sie mehreren Benutzern, Gruppen und Rollen in Ihrem AWS-Konto anfügen können. Verwaltete Richtlinien umfassen von AWS verwaltete und von Kunden verwaltete Richtlinien. Informationen dazu, wie Sie zwischen einer verwalteten Richtlinie und einer eingebundenen Richtlinie wählen, finden Sie unter [Auswahl zwischen verwalteten und eingebundenen Richtlinien](#) im IAM-Benutzerhandbuch.

## Ressourcenbasierte Richtlinien

Ressourcenbasierte Richtlinien sind JSON-Richtliniendokumente, die Sie an eine Ressource anfügen. Beispiele für ressourcenbasierte Richtlinien sind IAM-Rollen-Vertrauensrichtlinien und Amazon-S3-Bucket-Richtlinien. In Services, die ressourcenbasierte Richtlinien unterstützen, können Service-Administratoren sie verwenden, um den Zugriff auf eine bestimmte Ressource zu steuern. Für die Ressource, an welche die Richtlinie angehängt ist, legt die Richtlinie fest, welche Aktionen ein bestimmter Prinzipal unter welchen Bedingungen für diese Ressource ausführen kann. Sie müssen in einer ressourcenbasierten Richtlinie [einen Prinzipal angeben](#). Prinzipale können Konten, Benutzer, Rollen, Verbundbenutzer oder AWS-Services umfassen.

Ressourcenbasierte Richtlinien sind Richtlinien innerhalb dieses Diensts. Sie können verwaltete AWS-Richtlinien von IAM nicht in einer ressourcenbasierten Richtlinie verwenden.

## Zugriffssteuerungslisten (ACLs)

Zugriffssteuerungslisten (ACLs) steuern, welche Prinzipale (Kontomitglieder, Benutzer oder Rollen) auf eine Ressource zugreifen können. ACLs sind ähnlich wie ressourcenbasierte Richtlinien, verwenden jedoch nicht das JSON-Richtliniendokumentformat.

Amazon S3, AWS WAF und Amazon VPC sind Beispiele für Dienste, die ACLs unterstützen. Weitere Informationen zu ACLs finden Sie unter [Zugriffskontrollliste \(ACL\) – Übersicht](#) (Access Control List) im Amazon-Simple-Storage-Service-Entwicklerhandbuch.

## Weitere Richtlinientypen

AWS unterstützt zusätzliche, weniger häufig verwendete Richtlinientypen. Diese Richtlinientypen können die maximalen Berechtigungen festlegen, die Ihnen von den häufiger verwendeten Richtlinientypen erteilt werden können.

- **Berechtigungsgrenzen:** Eine Berechtigungsgrenze ist ein erweitertes Feature, mit der Sie die maximalen Berechtigungen festlegen können, die eine identitätsbasierte Richtlinie einer IAM-Entität (IAM-Benutzer oder -Rolle) erteilen kann. Sie können eine Berechtigungsgrenze für eine Entität festlegen. Die daraus resultierenden Berechtigungen sind der Schnittpunkt der identitätsbasierten Richtlinien einer Entität und ihrer Berechtigungsgrenzen. Ressourcenbasierte Richtlinien, die den Benutzer oder die Rolle im Feld `Principal` angeben, werden nicht durch Berechtigungsgrenzen eingeschränkt. Eine explizite Zugriffsverweigerung in einer dieser Richtlinien setzt eine Zugriffserlaubnis außer Kraft. Weitere Informationen über Berechtigungsgrenzen finden Sie unter [Berechtigungsgrenzen für IAM-Entitäten](#) im IAM-Benutzerhandbuch.
- **Service-Kontrollrichtlinien (SCPs)** – SCPs sind JSON-Richtlinien, die die maximalen Berechtigungen für eine Organisation oder Organisationseinheit (OE) in AWS Organizations angeben. AWS Organizations ist ein Dienst für die Gruppierung und zentrale Verwaltung mehrerer AWS-Konten Ihres Unternehmens. Wenn Sie innerhalb einer Organisation alle Features aktivieren, können Sie Service-Kontrollrichtlinien (SCPs) auf alle oder einzelne Ihrer Konten anwenden. SCPs schränken Berechtigungen für Entitäten in Mitgliedskonten einschließlich des jeweiligen Root-Benutzer des AWS-Kontos ein. Weitere Informationen zu Organizations und SCPs finden Sie unter [Funktionsweise von SCPs](#) im AWS Organizations-Benutzerhandbuch.
- **Sitzungsrichtlinien:** Sitzungsrichtlinien sind erweiterte Richtlinien, die Sie als Parameter übergeben, wenn Sie eine temporäre Sitzung für eine Rolle oder einen verbundenen Benutzer programmgesteuert erstellen. Die resultierenden Sitzungsberechtigungen sind eine Schnittmenge der auf der Identität des Benutzers oder der Rolle basierenden Richtlinien und der Sitzungsrichtlinien. Berechtigungen können auch aus einer ressourcenbasierten Richtlinie stammen. Eine explizite Zugriffsverweigerung in einer dieser Richtlinien setzt eine Zugriffserlaubnis außer Kraft. Weitere Informationen finden Sie unter [Sitzungsrichtlinien](#) im IAM-Benutzerhandbuch.



## Mehrere Richtlinientypen

Wenn mehrere auf eine Anforderung mehrere Richtlinientypen angewendet werden können, sind die entsprechenden Berechtigungen komplizierter. Informationen dazu, wie AWS die Zulässigkeit einer Anforderung ermittelt, wenn mehrere Richtlinientypen beteiligt sind, finden Sie unter [Logik für die Richtlinienauswertung](#) im IAM-Benutzerhandbuch.

## Funktionsweise von Amazon Fraud Detector mit IAM

Bevor Sie IAM verwenden, um den Zugriff auf Amazon Fraud Detector zu verwalten, sollten Sie verstehen, welche IAM-Funktionen Sie mit Amazon Fraud Detector verwenden können. Einen Überblick über das Zusammenwirken von Amazon Fraud Detector und anderen -AWSServices mit IAM finden Sie unter [-AWSServices, die mit IAM funktionieren](#) im IAM-Benutzerhandbuch.

### Themen

- [Identitätsbasierte Amazon Fraud Detector-Richtlinien](#)
- [Ressourcenbasierte Richtlinien für Amazon Fraud Detector](#)
- [Autorisierung basierend auf Amazon Fraud Detector Tags](#)
- [IAM-Rollen von Amazon Fraud Detector](#)

## Identitätsbasierte Amazon Fraud Detector-Richtlinien

Mit identitätsbasierten IAM-Richtlinien können Sie angeben, welche Aktionen und Ressourcen zugelassen oder abgelehnt werden. Darüber hinaus können Sie die Bedingungen festlegen, unter denen Aktionen zugelassen oder abgelehnt werden. Amazon Fraud Detector unterstützt bestimmte Aktionen, Ressourcen und Bedingungsschlüssel. Informationen zu sämtlichen Elementen, die Sie in einer JSON-Richtlinie verwenden, finden Sie in der [IAM-Referenz für JSON-Richtlinienelemente](#) im IAM-Benutzerhandbuch.

Für die ersten Schritte mit Amazon Fraud Detector empfehlen wir, einen -Benutzer mit Zugriff zu erstellen, der auf Amazon Fraud Detector-Operationen und erforderliche Berechtigungen beschränkt ist. Sie können bei Bedarf weitere Berechtigungen hinzufügen. Die folgenden Richtlinien gewähren die erforderliche Berechtigung zur Verwendung von Amazon Fraud Detector: `AmazonFraudDetectorFullAccessPolicy` und `AmazonS3FullAccess`. Weitere Informationen zum Einrichten von Amazon Fraud Detector mit diesen Richtlinien finden Sie unter [Für Amazon Fraud Detector einrichten](#).



## Aktionen

Administratoren können mit AWS-JSON-Richtlinien festlegen, welche Personen zum Zugriff auf welche Ressourcen berechtigt sind. Das heißt, welcher Prinzipal kann Aktionen für welche Ressourcen und unter welchen Bedingungen ausführen.

Das Element `Action` einer JSON-Richtlinie beschreibt die Aktionen, mit denen Sie den Zugriff in einer Richtlinie zulassen oder verweigern können. Richtlinienaktionen haben normalerweise denselben Namen wie die zugehörige AWS-API-Operation. Es gibt einige Ausnahmen, z. B. Aktionen, die nur mit Genehmigung durchgeführt werden können und für die es keine passende API-Operation gibt. Es gibt auch einige Operationen, die mehrere Aktionen in einer Richtlinie erfordern. Diese zusätzlichen Aktionen werden als abhängige Aktionen bezeichnet.

Schließen Sie Aktionen in eine Richtlinie ein, um Berechtigungen zur Durchführung der zugeordneten Operation zu erteilen.

Richtlinienaktionen in Amazon Fraud Detector verwenden das folgende Präfix vor der Aktion: `frauddetector:`. Um beispielsweise eine Regel mit der `APICreateRule`-Operation von Amazon Fraud Detector zu erstellen, fügen Sie die `frauddetector:CreateRule` Aktion in die Richtlinie ein. Richtlinienanweisungen müssen entweder ein `Action`- oder ein `NotAction`-Element enthalten. Amazon Fraud Detector definiert eine eigene Gruppe von Aktionen, die Aufgaben beschreiben, die Sie mit diesem Service durchführen können.

Um mehrere Aktionen in einer einzigen Anweisung anzugeben, trennen Sie sie wie folgt durch Kommata:

```
"Action": [  
  "frauddetector:action1",  
  "frauddetector:action2"
```

Sie können auch Platzhalter verwenden, um mehrere Aktionen anzugeben. Beispielsweise können Sie alle Aktionen festlegen, die mit dem Wort `Describe` beginnen, einschließlich der folgenden Aktion:

```
"Action": "frauddetector:Describe*"
```

Eine Liste der Aktionen von Amazon Fraud Detector finden Sie unter [Von Amazon Fraud Detector definierte Aktionen](#) im IAM-Benutzerhandbuch.

## Ressourcen

Administratoren können mit AWS-JSON-Richtlinien festlegen, welche Personen zum Zugriff auf welche Ressourcen berechtigt sind. Das bedeutet die Festlegung, welcher Prinzipal Aktionen für welche Ressourcen unter welchen Bedingungen ausführen kann.

Das JSON-Richtlinienelement `Resource` gibt die Objekte an, auf welche die Aktion angewendet wird. Anweisungen müssen entweder ein `Resource` oder ein `NotResource`-Element enthalten. Als bewährte Methode geben Sie eine Ressource mit dem zugehörigen [Amazon-Ressourcennamen \(ARN\)](#) an. Sie können dies für Aktionen tun, die einen bestimmten Ressourcentyp unterstützen, der als Berechtigungen auf Ressourcenebene bezeichnet wird.

Verwenden Sie für Aktionen, die keine Berechtigungen auf Ressourcenebene unterstützen, z. B. Auflistungsoperationen, einen Platzhalter (\*), um anzugeben, dass die Anweisung für alle Ressourcen gilt.

```
"Resource": "*" 
```

Von [Amazon Fraud Detector definierte Ressourcentypen](#) listen alle Ressourcen-ARNs von Amazon Fraud Detector auf.

Um beispielsweise den `my_detector`-Detektor in Ihrer Anweisung anzugeben, verwenden Sie den folgenden ARN:

```
"Resource": "arn:aws:frauddetector:us-east-1:123456789012:detector/my_detector" 
```

Weitere Informationen zum Format von ARNs finden Sie unter [Amazon-Ressourcennamen \(ARNs\) und AWS-Service-Namespaces](#).

Um alle Detektoren anzugeben, die zu einem bestimmten Konto gehören, verwenden Sie den Platzhalter (\*):

```
"Resource": "arn:aws:frauddetector:us-east-1:123456789012:detector/*" 
```

Einige Amazon Fraud Detector-Aktionen, z. B. das Erstellen von Ressourcen, können nicht für eine bestimmte Ressource ausgeführt werden. In diesen Fällen müssen Sie den Platzhalter (\*) verwenden.

```
"Resource": "*" 
```

Eine Liste der Ressourcentypen von Amazon Fraud Detector und ihrer ARNs finden Sie unter [Von Amazon Fraud Detector definierte Ressourcen](#) im IAM-Benutzerhandbuch. Informationen zu den Aktionen, mit denen Sie den ARN einzelner Ressourcen angeben können, finden Sie unter [Von Amazon Fraud Detector definierte Aktionen](#).

## Bedingungsschlüssel

Administratoren können mithilfe von AWS-JSON-Richtlinien festlegen, wer zum Zugriff auf was berechtigt ist. Das heißt, welcher Prinzipal kann Aktionen für welche Ressourcen und unter welchen Bedingungen ausführen.

Das Element `Condition` (oder `Condition block`) ermöglicht Ihnen die Angabe der Bedingungen, unter denen eine Anweisung wirksam ist. Das Element `Condition` ist optional. Sie können bedingte Ausdrücke erstellen, die [Bedingungsoperatoren](#) verwenden, z. B. `ist gleich` oder `kleiner als`, damit die Bedingung in der Richtlinie mit Werten in der Anforderung übereinstimmt.

Wenn Sie mehrere `Condition`-Elemente in einer Anweisung oder mehrere Schlüssel in einem einzelnen `Condition`-Element angeben, wertet AWS diese mittels einer logischen AND-Operation aus. Wenn Sie mehrere Werte für einen einzelnen Bedingungsschlüssel angeben, wertet AWS die Bedingung mittels einer logischen OR-Operation aus. Alle Bedingungen müssen erfüllt werden, bevor die Berechtigungen der Anweisung gewährt werden.

Sie können auch Platzhaltervariablen verwenden, wenn Sie Bedingungen angeben. Beispielsweise können Sie einem IAM-Benutzer die Berechtigung für den Zugriff auf eine Ressource nur dann gewähren, wenn sie mit dessen IAM-Benutzernamen gekennzeichnet ist. Weitere Informationen finden Sie unter [IAM-Richtlinienelemente: Variablen und Tags](#) im IAM-Benutzerhandbuch.

AWS unterstützt globale Bedingungsschlüssel und servicespezifische Bedingungsschlüssel. Eine Liste aller globalen AWS-Bedingungsschlüssel finden Sie unter [Globale AWS-Bedingungskontextschlüssel](#) im IAM-Benutzerhandbuch.

Amazon Fraud Detector definiert einen eigenen Satz von Bedingungsschlüsseln und unterstützt auch einige globale Bedingungsschlüssel. Eine Liste aller globalen AWS-Bedingungsschlüssel finden Sie unter [Globale AWS-Bedingungskontextschlüssel](#) im IAM-Benutzerhandbuch.

Eine Liste der Bedingungsschlüssel von Amazon Fraud Detector finden Sie unter [Bedingungsschlüssel für Amazon Fraud Detector](#) im IAM-Benutzerhandbuch. Informationen dazu, welche Aktionen und Ressourcen Sie einen Bedingungsschlüssel verwenden können, finden Sie unter [Von Amazon Fraud Detector definierte Aktionen](#).

## Beispiele

Beispiele für identitätsbasierte Richtlinien von Amazon Fraud Detector finden Sie unter [Beispiele für identitätsbasierte Amazon Fraud Detector-Richtlinien](#).

## Ressourcenbasierte Richtlinien für Amazon Fraud Detector

Amazon Fraud Detector unterstützt keine ressourcenbasierten Richtlinien.

## Autorisierung basierend auf Amazon Fraud Detector Tags

Sie können Tags an Amazon Fraud Detector-Ressourcen anfügen oder Tags in einer Anforderung an Amazon Fraud Detector übergeben. Um den Zugriff auf der Grundlage von Tags zu steuern, geben Sie im Bedingungelement einer [Richtlinie Tag-Informationen](#) an, indem Sie die Schlüssel `aws:ResourceTag/key-name`, `aws:RequestTag/key-name`, oder Bedingung `aws:TagKeys` verwenden.

## IAM-Rollen von Amazon Fraud Detector

Eine [IAM-Rolle](#) ist eine Entität in Ihrem AWS-Konto mit spezifischen Berechtigungen.

## Verwenden temporärer Anmeldeinformationen mit Amazon Fraud Detector

Sie können temporäre Anmeldeinformationen verwenden, um sich über einen Verbund anzumelden, eine IAM-Rolle anzunehmen oder eine kontenübergreifende Rolle anzunehmen. Sie erhalten temporäre Sicherheitsanmeldeinformationen, indem Sie AWS STS -API-Operationen wie [AssumeRole](#) oder aufrufen [GetFederationToken](#).

Amazon Fraud Detector unterstützt die Verwendung temporärer Anmeldeinformationen.

## Serviceverknüpfte Rollen

[Serviceverknüpfte Rollen](#) erlauben AWS-Services den Zugriff auf Ressourcen in anderen Services, um eine Aktion in Ihrem Auftrag auszuführen. Serviceverknüpfte Rollen werden in Ihrem IAM-Konto angezeigt und gehören zum Service. Ein IAM-Administrator kann die Berechtigungen für serviceverknüpfte Rollen anzeigen, aber nicht bearbeiten.

Amazon Fraud Detector unterstützt keine serviceverknüpften Rollen.

## Servicerollen

Dieses Feature ermöglicht einem Service das Annehmen einer [Servicerolle](#) in Ihrem Namen. Diese Rolle gewährt dem Service Zugriff auf Ressourcen in anderen Diensten, um eine Aktion in Ihrem Namen auszuführen. Servicerollen werden in Ihrem -Konto angezeigt und gehören zum Konto. Dies bedeutet, dass ein -Administrator die Berechtigungen für diese Rolle ändern kann. Dies kann jedoch die Funktionalität des Dienstes beeinträchtigen.

Amazon Fraud Detector unterstützt Servicerollen.

## Beispiele für identitätsbasierte Amazon Fraud Detector-Richtlinien

Benutzer und IAM-Rollen besitzen standardmäßig keine Berechtigungen zum Erstellen oder Ändern von Amazon Fraud Detector-Ressourcen. Sie können auch keine Aufgaben ausführen, die die AWS Management Console-, – AWS CLI oder AWS-API benutzen. Ein Administrator muss IAM-Richtlinien erstellen, die Benutzern und Rollen die Berechtigung zum Ausführen bestimmter API-Operationen für die angegebenen Ressourcen gewähren, die diese benötigen. Der Administrator muss diese Richtlinien anschließend den -Benutzern oder -Gruppen anfügen, die diese Berechtigungen benötigen.

Informationen dazu, wie Sie unter Verwendung dieser beispielhaften JSON-Richtliniendokumente eine identitätsbasierte IAM-Richtlinie erstellen, finden Sie unter [Erstellen von Richtlinien auf der JSON-Registerkarte](#) im IAM-Benutzerhandbuch.

### Themen

- [Bewährte Methoden für Richtlinien](#)
- [Von AWS verwaltete \(vordefinierte\) Richtlinie für Amazon Fraud Detector](#)
- [Gewähren der Berechtigung zur Anzeige der eigenen Berechtigungen für Benutzer](#)
- [Vollzugriff auf Amazon Fraud Detector-Ressourcen gewähren](#)
- [Lesezugriff auf Amazon Fraud Detector-Ressourcen zulassen](#)
- [Zugriff auf eine bestimmte Ressource zulassen](#)
- [Erlauben des Zugriffs auf bestimmte Ressourcen bei Verwendung der Dual-Modus-API](#)
- [Beschränken des Zugriffs basierend auf Tags](#)

## Bewährte Methoden für Richtlinien

Identitätsbasierte Richtlinien legen fest, ob jemand Amazon Fraud Detector-Ressourcen in Ihrem Konto erstellen, darauf zugreifen oder sie löschen kann. Dies kann zusätzliche Kosten für Ihr verursachen AWS-Konto. Befolgen Sie beim Erstellen oder Bearbeiten identitätsbasierter Richtlinien die folgenden Anleitungen und Empfehlungen:

- **Erste Schritte mit AWS-verwaltete Richtlinien und Umstellung auf Berechtigungen mit den geringsten Berechtigungen:**Um Ihren Benutzern und Workloads Berechtigungen zu gewähren, verwenden Sie die AWS-verwaltete Richtlinien die Berechtigungen für viele allgemeine Anwendungsfälle gewähren. Sie sind in Ihrem AWS-Konto verfügbar. Wir empfehlen Ihnen, die Berechtigungen weiter zu reduzieren, indem Sie vom Kunden verwaltete AWS-Richtlinien definieren, die speziell auf Ihre Anwendungsfälle zugeschnitten sind. Weitere Informationen finden Sie unter [AWS-verwaltete Richtlinien](#) oder [AWS-verwaltete Richtlinien für Auftragsfunktionen](#) im IAM-Benutzerhandbuch.
- **Anwendung von Berechtigungen mit den geringsten Rechten:**Wenn Sie mit IAM-Richtlinien Berechtigungen festlegen, gewähren Sie nur die Berechtigungen, die für die Durchführung einer Aufgabe erforderlich sind. Sie tun dies, indem Sie die Aktionen definieren, die für bestimmte Ressourcen unter bestimmten Bedingungen durchgeführt werden können, auch bekannt als die geringsten Berechtigungen. Weitere Informationen zur Verwendung von IAM zum Anwenden von Berechtigungen finden Sie unter [Richtlinien und Berechtigungen in IAM](#) im IAM-Benutzerhandbuch.
- **Verwenden von Bedingungen in IAM-Richtlinien zur weiteren Einschränkung des Zugriffs:**Sie können Ihren Richtlinien eine Bedingung hinzufügen, um den Zugriff auf Aktionen und Ressourcen zu beschränken. Sie können beispielsweise eine Richtlinienbedingung schreiben, um festzulegen, dass alle Anforderungen mithilfe von SSL gesendet werden müssen. Sie können auch Bedingungen verwenden, um Zugriff auf Service-Aktionen zu gewähren, wenn diese durch ein bestimmtes AWS-Service, wie beispielsweise AWS CloudFormation, verwendet werden. Weitere Informationen finden Sie unter [IAM-JSON-Richtlinienelemente: Bedingung](#) im IAM-Benutzerhandbuch.
- **Verwenden von IAM Access Analyzer zur Validierung Ihrer IAM-Richtlinien, um sichere und funktionale Berechtigungen zu gewährleisten:**IAM Access Analyzer validiert neue und vorhandene Richtlinien, damit die Richtlinien der IAM-Richtliniensprache (JSON) und den bewährten IAM-Methoden entsprechen. IAM Access Analyzer stellt mehr als 100 Richtlinienprüfungen und umsetzbare Empfehlungen zur Verfügung, damit Sie sichere und funktionale Richtlinien erstellen können. Weitere Informationen finden Sie unter [Richtlinienvvalidierung zum IAM Access Analyzer](#) im IAM-Benutzerhandbuch.

- Bedarf einer Multi-Faktor-Authentifizierung (MFA): Wenn Sie ein Szenario haben, das IAM-Benutzer oder Root-Benutzer in Ihrem AWS-Konto erfordert, aktivieren Sie MFA für zusätzliche Sicherheit. Um MFA beim Aufrufen von API-Vorgängen anzufordern, fügen Sie Ihren Richtlinien MFA-Bedingungen hinzu. Weitere Informationen finden Sie unter [Konfigurieren eines MFA-geschützten API-Zugriffs](#) im IAM-Benutzerhandbuch.

Weitere Informationen zu bewährten Methoden in IAM finden Sie unter [Bewährte Methoden für die Sicherheit in IAM](#) im IAM-Benutzerhandbuch.

## Von AWS verwaltete (vordefinierte) Richtlinie für Amazon Fraud Detector

AWS Durch die Bereitstellung von eigenständigen IAM-Richtlinien, die von erstellt und verwaltet werden, deckt viele häufige Anwendungsfälle ab AWS. Diese AWS verwalteten Richtlinien erteilen die erforderlichen Berechtigungen für viele häufige Anwendungsfälle, sodass Sie nicht mühsam ermitteln müssen, welche Berechtigungen erforderlich sind. Weitere Informationen finden Sie unter Von [AWS verwaltete Richtlinien](#) im AWS Identity and Access Management-Management-Benutzerhandbuch.

Die folgende AWS verwaltete Richtlinie, die Sie Benutzern in Ihrem Konto anfügen können, ist spezifisch für Amazon Fraud Detector:

`AmazonFraudDetectorFullAccess`: Gewährt vollen Zugriff auf Amazon Fraud Detector-Ressourcen, -Aktionen und die unterstützten Operationen, einschließlich:

- Auflisten und Beschreiben aller Modellendpunkte in Amazon SageMaker
- Auflisten aller IAM-Rollen im Konto
- Auflisten aller Amazon S3-Buckets
- IAM-Passrolle erlauben, eine Rolle an Amazon Fraud Detector zu übergeben

Diese Richtlinie gewährt keinen uneingeschränkten S3-Zugriff. Wenn Sie Modelltrainingsdatensätze in S3 hochladen müssen, ist auch die `AmazonS3FullAccess` -verwaltete Richtlinie (oder eine begrenzte benutzerdefinierte Amazon S3-Zugriffsrichtlinie) erforderlich.

Sie können die Berechtigungen der Richtlinie überprüfen, indem Sie sich bei der IAM-Konsole anmelden und nach dem Richtlinienamen suchen. Sie können auch Ihre eigenen benutzerdefinierten IAM-Richtlinien erstellen, um Berechtigungen für Amazon Fraud Detector-Aktionen und -Ressourcen nach Bedarf zu gewähren. Die benutzerdefinierten Richtlinien können Sie dann den -Benutzern oder -Gruppen zuweisen, die diese Berechtigungen benötigen.

## Gewähren der Berechtigung zur Anzeige der eigenen Berechtigungen für Benutzer

In diesem Beispiel wird gezeigt, wie Sie eine Richtlinie erstellen, die IAM-Benutzern die Berechtigung zum Anzeigen der eingebundenen Richtlinien und verwalteten Richtlinien gewährt, die ihrer Benutzeridentität angefügt sind. Diese Richtlinie enthält Berechtigungen für die Ausführung dieser Aktion auf der Konsole oder für die programmgesteuerte Ausführung über die AWS CLI oder die AWS-API.

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



## Vollzugriff auf Amazon Fraud Detector-Ressourcen gewähren

Im folgenden Beispiel erhält ein -Benutzer in Ihrem AWS-Konto vollständigen Zugriff auf alle Ressourcen und Aktionen von Amazon Fraud Detector.

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Action": [
        "frauddetector:*"
      ],
      "Resource": "*"
    }
  ]
}
```

## Lesezugriff auf Amazon Fraud Detector-Ressourcen zulassen

In diesem Beispiel gewähren Sie einem -Benutzer in Ihrem AWS-Kontoschreibgeschützten Zugriff auf Ihre Amazon Fraud Detector-Ressourcen.

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

```

## Zugriff auf eine bestimmte Ressource zulassen

In diesem Beispiel einer Richtlinie auf Ressourcenebene gewähren Sie einem -Benutzer in Ihrem AWS-Konto Zugriff auf alle Aktionen und Ressourcen mit Ausnahme einer bestimmten Detector-Ressource.

```

{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Action": [
        "frauddetector:*"
      ],
      "Resource": "*"
    },
    {
      "Effect": "Deny",
      "Action": [
        "frauddetector:*Detector"
      ],
      "Resource": "arn:${Partition}:frauddetector:${Region}:${Account}:detector/
${detector-name}"
    }
  ]
}

```

## Erlauben des Zugriffs auf bestimmte Ressourcen bei Verwendung der Dual-Modus-API

Amazon Fraud Detector bietet Dual-Modus-Get-APIs, die sowohl als List- als auch als Describe-Vorgang funktionieren. Eine Dual-Modus-API, wenn sie ohne Parameter aufgerufen wird, gibt eine

Liste der angegebenen Ressource zurück, die Ihrem zugeordnet istAWS-Konto. Eine Dual-Modus-API, wenn sie mit dem Parameter aufgerufen wird, gibt die Details der angegebenen Ressource zurück. Die Ressource kann Modelle, Variablen, Ereignistypen oder Entitätstypen sein.

Die Dual-Modus-APIs unterstützen Berechtigungen auf Ressourcenebene in IAM-Richtlinien. Die Berechtigungen auf Ressourcenebene werden jedoch nur angewendet, wenn ein oder mehrere Parameter als Teil der Anforderung bereitgestellt werden. Wenn der Benutzer beispielsweise die [GetVariables](#) -API aufruft und einen Variablennamen angibt und eine IAM-Verweigerungsrichtlinie an die Variablenressource oder den Variablennamen angehängt ist, erhält der Benutzer den `AccessDeniedException` Fehler . Wenn ein Benutzer die `GetVariables` API aufruft und keinen Variablennamen angibt, werden alle Variablen zurückgegeben, was zu einem Informationsleck führen kann.

Um Benutzern nur das Anzeigen von Details zu bestimmten Ressourcen zu ermöglichen, verwenden Sie ein `IAM-NotResource` Richtlinienelement in einer IAM-Verweigerungsrichtlinie. Nachdem Sie dieses Richtlinienelement zu einer IAM-Verweigerungsrichtlinie hinzugefügt haben, können Benutzer nur die Details der Ressourcen anzeigen, die im `-NotResource`Block angegeben sind. Weitere Informationen finden Sie unter [IAM-JSON-Richtlinienelemente: NotResource](#) im IAM-Benutzerhandbuch.

Die folgende Beispielrichtlinie ermöglicht Benutzern den Zugriff auf alle Ressourcen von Amazon Fraud Detector. Das `NotResource` Richtlinienelement wird jedoch verwendet, um [GetVariables](#) API-Aufrufe auf die Variablennamen mit den Präfixen `user*`, `job_*`und zu beschränken`var*`.

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Action": "frauddetector:*",
      "Resource": "*"
    },
    {
      "Effect": "Deny",
      "Action": "frauddetector:GetVariables",
      "NotResource": [
        "arn:aws:frauddetector:*:*:variable/user*",
        "arn:aws:frauddetector:*:*:variable/job_*",
        "arn:aws:frauddetector:*:*:variable/var*"
      ]
    }
  ]
}
```

```
]
}
```

## Antwort

Für diese Beispielrichtlinie weist die Antwort das folgende Verhalten auf:

- Ein `GetVariables` Aufruf, der keine Variablennamen enthält, führt zu einem `AccessDeniedException` Fehler, da die Anforderung der `Deny`-Anweisung zugeordnet ist.
- Ein `GetVariables` Aufruf, der einen Variablennamen enthält, der nicht zulässig ist, führt zu einem `AccessDeniedException` Fehler, da der Variablenname nicht dem Variablennamen im `NotResource` Block zugeordnet ist. Beispielsweise `email_address` führt ein `GetVariables` Aufruf mit einem Variablennamen zu einem `AccessDeniedException` Fehler.
- Ein `GetVariables` Aufruf, der einen Variablennamen enthält, der einem Variablennamen im `NotResource` Block entspricht, wird wie erwartet zurückgegeben. Ein `GetVariables` Aufruf mit Variablenname gibt beispielsweise die Details der `job_cpa` Variablen `job_cpa` zurück.

## Beschränken des Zugriffs basierend auf Tags

Diese Beispielrichtlinie zeigt, wie Sie den Zugriff auf Amazon Fraud Detector basierend auf Ressourcen-Tags einschränken. In diesem Beispiel wird davon ausgegangen, dass:

- In Ihrem haben AWS-Konto Sie zwei verschiedene Gruppen mit den Namen `Team1` und `Team2` definiert
- Sie haben vier Detektoren erstellt
- Sie möchten Mitgliedern von `Team1` erlauben, API-Aufrufe auf zwei Detektoren durchzuführen
- Sie möchten Mitgliedern von `Team2` erlauben, API-Aufrufe auf den anderen 2 Detektoren durchzuführen

So steuern Sie den Zugriff auf API-Aufrufe (Beispiel)

1. Fügen Sie den von `Team1` verwendeten Detektoren ein Tag mit dem Schlüssel `Project` und dem Wert `A` hinzu.
2. Fügen Sie den von `Team2` verwendeten Detektoren ein Tag mit dem Schlüssel `Project` und dem Wert `B` hinzu.

- Erstellen Sie eine IAM-Richtlinie mit einer ResourceTag Bedingung, die den Zugriff auf Detektoren mit Tags mit Schlüssel Project und Wert verweigertB, und fügen Sie diese Richtlinie an Team1 an.
- Erstellen Sie eine IAM-Richtlinie mit einer ResourceTag Bedingung, die den Zugriff auf Detektoren verweigert, die Tags mit Schlüssel Project und Wert habenA, und fügen Sie diese Richtlinie an Team2 an.

Im Folgenden finden Sie ein Beispiel für eine Richtlinie, die bestimmte Aktionen für jede Amazon Fraud Detector-Ressource verweigert, die ein Tag mit dem Schlüssel Project und dem Wert hatB:

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

## Confused-Deputy-Prävention

Das Problem des verwirrten Stellvertreters tritt auf, wenn eine Entität, die nicht über die Berechtigung zum Ausführen einer Aktion verfügt, eine privilegiere Entität zwingen kann, die Aktion auszuführen. AWS bietet Tools, mit denen Sie Ihr Konto schützen können, wenn Sie Dritten (sogenannte kontoübergreifende ) oder anderen -AWS Services (sogenannte serviceübergreifende ) Zugriff auf Ressourcen in Ihrem Konto gewähren.

Das Problem des dienstübergreifenden verwirrten Stellvertreters kann auftreten, wenn ein Service (der aufrufende Service ) einen anderen Service aufruft (der aufgerufene Service ). Der Anruf-Dienst kann so manipuliert werden, dass er seine Berechtigungen verwendet, um auf die Ressourcen eines anderen Kunden zu reagieren, auf die er sonst nicht zugreifen dürfte. Um dies zu verhindern, können Sie Richtlinien erstellen, die Ihnen helfen, Ihre Daten für alle Services mit Service-Prinzipalen zu schützen, denen Zugriff auf die Ressourcen Ihres Services gewährt wurde.

Amazon Fraud Detector unterstützt die Verwendung von [Servicerollen](#) in Ihren Berechtigungsrichtlinien, damit ein Service in Ihrem Namen auf die Ressourcen eines anderen Services zugreifen kann. Eine Rolle erfordert zwei Richtlinien: eine Rollenvertrauensrichtlinie, die den Prinzipal angibt, der die Rolle übernehmen darf, und eine Berechtigungsrichtlinie, die angibt, was mit der Rolle gemacht werden kann. Wenn ein Dienst eine Rolle in Ihrem Namen übernimmt, muss der Service-Prinzipal die `sts:AssumeRole`-Aktion in der Rollenvertrauensrichtlinie ausführen dürfen. Wenn ein Service `sts:AssumeRole` aufruft, gibt AWS STS eine Reihe temporärer Sicherheitsanmeldeinformationen zurück, die der Service-Prinzipal für den Zugriff auf die Ressourcen verwendet, die laut Berechtigungsrichtlinie der Rolle zulässig sind.

Um ein serviceübergreifendes Confused-Deputy-Problem zu vermeiden, empfiehlt Amazon Fraud Detector, die [aws:SourceAccount](#) globalen Bedingungskontextschlüssel [aws:SourceArn](#) und in Ihrer Rollenvertrauensrichtlinie zu verwenden, um den Zugriff auf die Rolle auf die Anforderungen zu beschränken, die von erwarteten Ressourcen generiert werden.

Die `aws:SourceAccount` gibt die Konto-ID und die den ARN der Ressource `aws:SourceArn` an, die dem serviceübergreifenden Zugriff zugeordnet ist. Der `aws:SourceArn` muss im [ARN-Format](#) angegeben werden. Stellen Sie sicher, dass `aws:SourceAccount` sowohl als auch dieselbe Konto-ID verwenden, wenn sie in derselben Richtlinienanweisung verwendet `aws:SourceArn` werden.

Der effektivste Weg, um sich vor dem Confused-Deputy-Problem zu schützen, ist die Verwendung des globalen Bedingungskontext-Schlüssels `aws:SourceArn` mit dem vollständigen ARN der Ressource. Wenn Sie den vollständigen ARN der Ressource nicht kennen oder

wenn Sie mehrere Ressourcen angeben, verwenden Sie den `aws:SourceArn` globalen Kontextbedingungsschlüssel mit einem Platzhalter (\*) für die unbekannt Teile des ARN. Beispiel: `arn:aws:servicename:*:123456789012:*` Informationen zu Ressourcen und Aktionen von Amazon Fraud Detector, die Sie in Ihren Berechtigungsrichtlinien verwenden können, finden Sie unter [Aktionen, Ressourcen und Bedingungsschlüssel für Amazon Fraud Detector](#).

Im folgenden Beispiel für eine Rollenvertrauensrichtlinie wird Platzhalter (\*) im `aws:SourceArn` Bedingungsschlüssel verwendet, um Amazon Fraud Detector den Zugriff auf mehrere Ressourcen zu ermöglichen, die der Konto-ID zugeordnet sind.

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

Die folgende Rollenvertrauensrichtlinie gewährt Amazon Fraud Detector nur Zugriff auf `Ressourcenexternal-model`. Beachten Sie den `aws:SourceArn` Parameter im Bedingungsblock. Der Ressourcenqualifizierer wird mit dem Modellendpunkt erstellt, der für den `PutExternalModel` API-Aufruf bereitgestellt wird.

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

## Fehlerbehebung für Identität und Zugriff auf Amazon Fraud Detector

Verwenden Sie die folgenden Informationen, um häufige Probleme zu diagnostizieren und zu beheben, die bei der Arbeit mit Amazon Fraud Detector und IAM auftreten können.

### Themen

- [Ich bin nicht autorisiert, eine Aktion in Amazon Fraud Detector auszuführen](#)
- [Ich bin nicht autorisiert, iam durchzuführen:PassRole](#)
- [Ich möchte Personen außerhalb meines -AWSKontos Zugriff auf meine Amazon Fraud Detector-Ressourcen gewähren](#)
- [Amazon Fraud Detector konnte die angegebene Rolle nicht übernehmen](#)

### Ich bin nicht autorisiert, eine Aktion in Amazon Fraud Detector auszuführen

Wenn die AWS Management Console Ihnen mitteilt, dass Sie nicht zur Ausführung einer Aktion autorisiert sind, müssen Sie sich an Ihren Administrator wenden, um Unterstützung zu erhalten. Ihr Administrator hat Ihnen Ihre Anmeldeinformationen zur Verfügung gestellt.



Der folgende Beispielfehler tritt auf, wenn der `mateojackson` Benutzer versucht, die Konsole zu verwenden, um Details zu einem *Detektor* anzuzeigen, jedoch nicht über `frauddetector:GetDetectors` Berechtigungen verfügt.

```
User: arn:aws:iam::123456789012:user/mateojackson is not authorized to perform:
frauddetector:GetDetectors on resource: my-example-detector
```

In diesem Fall bittet Mateo seinen Administrator um die Aktualisierung seiner Richtlinien, um unter Verwendung der Aktion *my-example-detector* auf die Ressource `frauddetector:GetDetectors` zugreifen zu können.

## Ich bin nicht autorisiert, iam durchzuführen:PassRole

Wenn Sie die Fehlermeldung erhalten, dass Sie nicht zur Ausführung der `iam:PassRole` Aktion autorisiert sind, müssen Ihre Richtlinien aktualisiert werden, um eine Rolle an Amazon Fraud Detector übergeben zu können.

Einige AWS-Services erlauben die Übergabe einer vorhandenen Rolle an diesen Dienst, sodass keine neue Servicerolle oder serviceverknüpfte Rolle erstellt werden muss. Hierzu benötigen Sie Berechtigungen für die Übergabe der Rolle an den Dienst.

Der folgende Beispielfehler tritt auf, wenn ein IAM-Benutzer mit dem Namen `marymajor` versucht, die Konsole zu verwenden, um eine Aktion in Amazon Fraud Detector auszuführen. Die Aktion erfordert jedoch, dass der Service über Berechtigungen verfügt, die durch eine Servicerolle gewährt werden. Mary besitzt keine Berechtigungen für die Übergabe der Rolle an den Dienst.

```
User: arn:aws:iam::123456789012:user/marymajor is not authorized to perform:
iam:PassRole
```

In diesem Fall müssen die Richtlinien von Mary aktualisiert werden, um die Aktion `iam:PassRole` ausführen zu können.

Wenden Sie sich an Ihren AWS-Administrator, falls Sie weitere Unterstützung benötigen. Ihr Administrator hat Ihnen Ihre Anmeldeinformationen zur Verfügung gestellt.

## Ich möchte Personen außerhalb meines -AWSKontos Zugriff auf meine Amazon Fraud Detector-Ressourcen gewähren

Sie können eine Rolle erstellen, die Benutzer in anderen Konten oder Personen außerhalb Ihrer Organisation für den Zugriff auf Ihre Ressourcen verwenden können. Sie können festlegen, wem

die Übernahme der Rolle anvertraut wird. Im Fall von Diensten, die ressourcenbasierte Richtlinien oder Zugriffskontrolllisten (Access Control Lists, ACLs) verwenden, können Sie diese Richtlinien verwenden, um Personen Zugriff auf Ihre Ressourcen zu gewähren.

Weitere Informationen dazu finden Sie hier:

- Informationen dazu, ob Amazon Fraud Detector diese Funktionen unterstützt, finden Sie unter [Funktionsweise von Amazon Fraud Detector mit IAM](#).
- Informationen zum Gewähren des Zugriffs auf Ihre Ressourcen für alle Ihre AWS-Konten finden Sie unter [Gewähren des Zugriffs für einen IAM-Benutzer in einem anderen Ihrer AWS-Konto](#) im IAM-Benutzerhandbuch.
- Informationen dazu, wie Sie AWS-Konten-Drittanbieter Zugriff auf Ihre Ressourcen bereitstellen, finden Sie unter [Gewähren des Zugriffs auf AWS-Konten von externen Benutzern](#) im IAM-Benutzerhandbuch.
- Informationen dazu, wie Sie über einen Identitätsverbund Zugriff gewähren, finden Sie unter [Gewähren von Zugriff für extern authentifizierte Benutzer \(Identitätsverbund\)](#) im IAM-Benutzerhandbuch.
- Informationen zum Unterschied zwischen der Verwendung von Rollen und ressourcenbasierten Richtlinien für den kontoübergreifenden Zugriff finden Sie unter [So unterscheiden sich IAM-Rollen von ressourcenbasierten Richtlinien](#) im IAM-Benutzerhandbuch.

## Amazon Fraud Detector konnte die angegebene Rolle nicht übernehmen

Wenn Sie die Fehlermeldung erhalten, dass Amazon Fraud Detector die angegebene Rolle nicht übernehmen konnte, müssen Sie die Vertrauensstellung für die angegebene Rolle aktualisieren. Durch die Angabe von Amazon Fraud Detector als vertrauenswürdige Entität kann der Service die Rolle übernehmen. Wenn Sie mit Amazon Fraud Detector eine Rolle erstellen, wird diese Vertrauensstellung automatisch festgelegt. Sie müssen diese Vertrauensstellung nur für IAM-Rollen einrichten, die nicht von Amazon Fraud Detector erstellt wurden.

So richten Sie eine Vertrauensstellung für eine vorhandene Rolle für Amazon Fraud Detector ein

1. Öffnen Sie die IAM-Konsole unter <https://console.aws.amazon.com/iam/>
2. Wählen Sie im Navigationsbereich Rollen aus.
3. Wählen Sie den Namen der Rolle aus, die Sie ändern möchten, und wählen Sie die Registerkarte Vertrauensstellungen.

4. Wählen Sie Vertrauensstellung bearbeiten aus.
5. Fügen Sie unter Policy Document Folgendes ein und wählen Sie dann Update Trust Policy.

```
{
  "Version": "2012-10-17",
  "Statement": [ {
    "Effect": "Allow",
    "Principal": {
      "Service": "frauddetector.amazonaws.com"
    },
    "Action": "sts:AssumeRole"
  } ]
}
```

## Protokollierung und Überwachung in Amazon Fraud Detector

AWS bietet die folgenden Überwachungstools, um Amazon Fraud Detector zu überwachen, Missstände zu melden und gegebenenfalls automatische Maßnahmen zu ergreifen:

- Amazon CloudWatch überwacht Ihre AWS Ressourcen und die Anwendungen, auf denen Sie ausgeführt werden, AWS in Echtzeit. Weitere Informationen zu CloudWatch finden Sie im [Amazon CloudWatch -Benutzerhandbuch](#).
- AWS CloudTrail erfasst API-Aufrufe und zugehörige Ereignisse, die von oder im Namen Ihres AWS-Kontos erfolgten, und übermittelt die Protokolldateien an einen von Ihnen angegebenen Amazon-S3-Bucket. Weitere Informationen zu finden CloudTrail Sie im [AWS CloudTrail-Benutzerhandbuch](#).

Weitere Informationen zur Überwachung von Amazon Fraud Detector finden Sie unter [Überwachen von Amazon Fraud Detector](#).

## Compliance-Validierung für Amazon Fraud Detector


Die Auditoren Dritter bewerten die Sicherheit und die Compliance von AWS-Services im Rahmen mehrerer AWS-Compliance-Programme, z. B. SOC, PCI, FedRAMP und HIPAA.

Informationen darüber, ob ein AWS-Service in den Geltungsbereich bestimmter Compliance-Programme fällt, finden Sie unter [AWS-Services in Geltungsbereich nach Compliance-Programm](#). Wählen Sie das Compliance-Programm, das Sie interessiert. Allgemeine Informationen finden Sie unter [AWS-Compliance-Programme](#).

Sie können Auditberichte von Drittanbietern unter AWS Artifact herunterladen. Weitere Informationen finden Sie unter [Berichte herunterladen in AWS Artifact](#).

Ihre Compliance-Verantwortung bei der Verwendung von AWS-Services ist von der Sensibilität Ihrer Daten, den Compliance-Zielen Ihres Unternehmens und den geltenden Gesetzen und Vorschriften abhängig. AWS stellt die folgenden Ressourcen zur Unterstützung der Compliance bereit:

- [Kurzanleitungen für Sicherheit und Compliance](#): In diesen Bereitstellungsleitfäden werden Überlegungen zur Architektur erörtert und Schritte zum Bereitstellen von Basisumgebungen auf AWS zur Verfügung gestellt, die auf Sicherheit und Compliance ausgerichtet sind.
- [Erstellung einer Architektur mit HIPAA-konformer Sicherheit und Compliance in Amazon Web Services](#) – In diesem Whitepaper wird beschrieben, wie Unternehmen mithilfe von AWS HIPAA-berechtigte Anwendungen erstellen können.

 Note

Nicht alle AWS-Services sind HIPAA-berechtigt. Weitere Informationen finden Sie in der [Referenz für HIPAA-berechtigte Services](#).

- [AWS-Compliance-Ressourcen](#) – Diese Arbeitsbücher und Leitfäden könnten für Ihre Branche und Ihren Standort relevant sein.
- [AWS-Compliance-Leitfäden für Kunden](#): Verstehen Sie das Modell der geteilten Verantwortung aus dem Blickwinkel der Einhaltung von Vorschriften. In den Leitfäden werden die bewährten Methoden zum Schutz von AWS-Services zusammengefasst und die Leitlinien den Sicherheitskontrollen in verschiedenen Frameworks (einschließlich des National Institute of Standards and Technology (NIST), des Payment Card Industry Security Standards Council (PCI) und der International Organization for Standardization (ISO)) zugeordnet.
- [Auswertung von Ressourcen mit Regeln](#) im AWS Config-Entwicklerhandbuch – Der AWS Config-Service bewertet, wie gut Ihre Ressourcenkonfigurationen mit internen Praktiken, Branchenrichtlinien und Vorschriften übereinstimmen.
- [AWS Security Hub](#): Dieser AWS-Service bietet einen umfassenden Überblick über Ihren Sicherheitsstatus innerhalb von AWS. Security Hub verwendet Sicherheitskontrollen, um Ihre AWS-

Ressourcen zu bewerten und Ihre Einhaltung von Sicherheitsstandards und bewährten Methoden zu überprüfen. Eine Liste der unterstützten Services und Kontrollen finden Sie in der [Security-Hub-Steuerungsreferenz](#).

- [AWS Audit Manager](#): Dieser AWS-Service hilft Ihnen, Ihre AWS-Nutzung kontinuierlich zu überprüfen, um den Umgang mit Risiken und die Compliance von Branchenstandards zu vereinfachen.

## Ausfallsicherheit in Amazon Fraud Detector

Im Zentrum der globalen AWS-Infrastruktur stehen die AWS-Regionen und Availability Zones. AWS-Regionen stellen mehrere physisch getrennte und isolierte Availability Zones bereit, die über hoch redundante Netzwerke mit niedriger Latenz und hohen Durchsätzen verbunden sind. Mithilfe von Availability Zones können Sie Anwendungen und Datenbanken erstellen und ausführen, die automatisch Failover zwischen Zonen ausführen, ohne dass es zu Unterbrechungen kommt. Availability Zones sind besser verfügbar, fehlertoleranter und skalierbarer als herkömmliche Infrastrukturen mit einem oder mehreren Rechenzentren.

Weitere Informationen zu AWS-Regionen und Availability Zones finden Sie unter [Weltweite AWS-Infrastruktur](#).

## Infrastruktursicherheit in Amazon Fraud Detector

Als verwalteter Service ist Amazon Fraud Detector durch die AWS globale Netzwerksicherheit von geschützt. Informationen zu AWS-Sicherheitsservices und wie AWS die Infrastruktur schützt, finden Sie unter [AWS-Cloud-Sicherheit](#). Informationen zum Entwerfen Ihrer AWS-Umgebung anhand der bewährten Methoden für die Infrastruktursicherheit finden Sie unter [Infrastrukturschutz](#) im Security Pillar AWS Well-Architected Framework.

Sie verwenden durch AWS veröffentlichte API-Aufrufe, um über das Netzwerk auf Amazon Fraud Detector zuzugreifen. Kunden müssen Folgendes unterstützen:

- Transport Layer Security (TLS). Wir benötigen TLS 1.2 und empfehlen TLS 1.3.
- Verschlüsselungs-Suiten mit Perfect Forward Secrecy (PFS) wie DHE (Ephemeral Diffie-Hellman) oder ECDHE (Elliptic Curve Ephemeral Diffie-Hellman). Die meisten modernen Systeme wie Java 7 und höher unterstützen diese Modi.

Außerdem müssen Anforderungen mit einer Zugriffsschlüssel-ID und einem geheimen Zugriffsschlüssel signiert sein, der einem IAM-Prinzipal zugeordnet ist. Alternativ können Sie mit [AWS Security Token Service](#) (AWS STS) temporäre Sicherheitsanmeldeinformationen erstellen, um die Anforderungen zu signieren.

# Überwachen von Amazon Fraud Detector

Die Überwachung ist wichtig, um die Zuverlässigkeit, Verfügbarkeit und Leistung von Amazon Fraud Detector und Ihren anderen AWS-Lösungen aufrechtzuerhalten. AWS bietet die folgenden Überwachungstools, um Amazon Fraud Detector zu überwachen, Missstände zu melden und gegebenenfalls automatische Maßnahmen zu ergreifen:

- Amazon CloudWatch überwacht Ihre AWS Ressourcen und die Anwendungen, auf denen Sie ausgeführt werden, AWS in Echtzeit. Sie können Kennzahlen erfassen und verfolgen, benutzerdefinierte Dashboards erstellen und Alarme festlegen, die Sie benachrichtigen oder Maßnahmen ergreifen, wenn eine bestimmte Metrik einen von Ihnen festgelegten Schwellenwert erreicht. Weitere Informationen finden Sie im [Amazon- CloudWatch Benutzerhandbuch](#).
- AWS CloudTrail erfasst API-Aufrufe und zugehörige Ereignisse, die von oder im Namen Ihres AWS-Kontos erfolgten, und übermittelt die Protokolldateien an einen von Ihnen angegebenen Amazon-S3-Bucket. Sie können die Benutzer und Konten, die AWS aufgerufen haben, identifizieren, sowie die Quell-IP-Adresse, von der diese Aufrufe stammen, und den Zeitpunkt der Aufrufe ermitteln. Weitere Informationen finden Sie im [AWS CloudTrail-Benutzerhandbuch](#).

## Themen

- [Überwachen von Amazon Fraud Detector mit Amazon CloudWatch](#)
- [Protokollieren von API-Aufrufen von Amazon Fraud Detector mit AWS CloudTrail](#)

# Überwachen von Amazon Fraud Detector mit Amazon CloudWatch

Sie können Amazon Fraud Detector mit überwachen CloudWatch, das Rohdaten sammelt und sie in lesbare Metriken verarbeitet, die nahezu in Echtzeit vorliegen. Diese Statistiken werden 15 Monate gespeichert, damit Sie auf Verlaufsdaten zugreifen können und einen besseren Überblick darüber erhalten, wie Ihre Webanwendung oder der Service ausgeführt werden. Sie können auch Alarme einrichten, die auf bestimmte Grenzwerte achten und Benachrichtigungen senden oder Aktivitäten auslösen, wenn diese Grenzwerte erreicht werden. Weitere Informationen finden Sie im [Amazon- CloudWatch Benutzerhandbuch](#).

## Themen

- [Verwenden von CloudWatch Metriken für Amazon Fraud Detector.](#)
- [Metriken für Amazon Fraud Detector](#)

## Verwenden von CloudWatch Metriken für Amazon Fraud Detector.

Um Metriken zu verwenden, müssen Sie die folgenden Informationen angeben:

- Der Metrik-Namespace. Ein Namespace ist ein CloudWatch Container, den Amazon Fraud Detector verwendet, um seine Metriken zu veröffentlichen. Wenn Sie die CloudWatch [ListMetrics](#) API oder den Befehl [list-metrics](#) verwenden, um die Metriken für Amazon Fraud Detector anzuzeigen, geben Sie `AWS/FraudDetector` für den Namespace an.
- Die Metrikdimension. Eine Dimension ist ein Name-Wert-Paar, mit dem Sie eine Metrik eindeutig identifizieren. `DetectorId` können, z. B. kann ein Dimensionsname sein. Die Angabe einer Metrikdimension ist optional.
- Der Metrikname, beispielsweise `GetEventPrediction`.

Sie können Überwachungsdaten für Amazon Fraud Detector mithilfe der AWS Management Console, der AWS CLI oder der API abrufen. Sie können die CloudWatch API auch über eines der Amazon AWS Software Development Kits (SDKs) oder die CloudWatch API-Tools verwenden. Die Konsole zeigt eine Reihe von Diagrammen an, die auf den Rohdaten der CloudWatch API basieren. Je nach Anforderungen können Sie entweder die in der Konsole angezeigten oder die mit der API aufgerufenen Graphen verwenden.

In der folgenden Liste finden Sie einige häufige Verwendungszwecke für die Metriken. Es handelt sich dabei um Vorschläge für den Einstieg und nicht um eine umfassende Liste.

Wie gehe ich vor?	Relevante Metriken
Wie verfolge ich die Anzahl der durchgeführten Vorhersagen?	Überwachen Sie die <code>GetEventPrediction</code> -Metrik.
Wie kann ich <code>GetEventPrediction</code> Fehler überwachen?	Verwenden Sie die <code>GetEventPrediction4xxError</code> Metriken <code>GetEventPrediction5xxError</code> und <code>.</code>
Wie überwache ich die Latenz der <code>GetEventPrediction</code> -Aufrufe?	Verwenden Sie die <code>GetEventPredictionLatency</code> -Metrik.



Sie müssen über die entsprechenden CloudWatch Berechtigungen verfügen, um Amazon Fraud Detector mit zu überwachen CloudWatch. Weitere Informationen finden Sie unter [Identity and Access Management for Amazon CloudWatch](#).

## Zugriff auf Metriken von Amazon Fraud Detector

Die folgenden Schritte zeigen, wie Sie über die CloudWatch Konsole auf Amazon Fraud Detector-Metriken zugreifen.

So zeigen Sie Metriken an (Konsole)

1. Öffnen Sie die - CloudWatch Konsole unter <https://console.aws.amazon.com/cloudwatch/>.
2. Wählen Sie Metriken, dann die Registerkarte Alle Metriken und dann Fraud Detector aus.
3. Wählen Sie die Metrikdimension.
4. Wählen Sie die gewünschte Metrik aus der Liste und einen Zeitraum für das Diagramm aus.

## Einrichten eines Alarms

Sie können einen CloudWatch Alarm erstellen, der eine Amazon Simple Notification Service (Amazon SNS)-Nachricht sendet, wenn sich der Status des Alarms ändert. Ein Alarm überwacht eine Metrik über einen bestimmten, von Ihnen definierten Zeitraum. Der Alarm führt eine oder mehrere Aktionen durch, basierend auf dem Wert der Metrik im Vergleich zu einem bestimmten Schwellenwert in einer Reihe von Zeiträumen. Die Aktion ist eine Benachrichtigung, die an ein Amazon-SNS-Thema oder eine Auto-Scaling-Richtlinie gesendet wird.

Alarme rufen nur Aktionen für anhaltende Statusänderungen auf. CloudWatch Alarme rufen keine Aktionen auf, nur weil sie sich in einem bestimmten Status befinden. Der Status muss sich geändert haben und für eine festgelegte Anzahl an Zeiträumen aufrechterhalten worden sein.

So richten Sie einen Alarm ein (Konsole)

1. Melden Sie sich bei der an AWS Management Console und öffnen Sie die - CloudWatch Konsole unter <https://console.aws.amazon.com/cloudwatch/>.
2. Wählen Sie im Navigationsbereich Alarme und dann Alarm erstellen aus. Dadurch wird der Assistent zum Erstellen von Alarmen geöffnet.
3. Wählen Sie Select metric (Metrik auswählen) aus.
4. Wählen Sie auf der Registerkarte Alle Metriken die Option Fraud Detector aus.

5. Wählen Sie Nach Detektor-ID und dann die GetEventPrediction Metrik aus.
6. Wählen Sie die Registerkarte Graphed metrics (Grafisch dargestellte Metriken) aus.
7. Wählen Sie für Statistic (Statistik) Sum (Summe) aus.
8. Wählen Sie Select metric (Metrik auswählen) aus.
9. Wählen Sie für Bedingungen die Option Statisch für Schwellenwerttyp und Größer für Wann immer... aus und geben Sie dann einen Höchstwert Ihrer Wahl ein. Wählen Sie Weiter aus.
10. Um Alarme für ein bestehendes Amazon-S3-Thema zu senden, wählen Sie für Benachrichtigung senden an: ein bestehendes SNS-Thema aus. Um den Namen und die E-Mail-Adressen für eine neue E-Mail-Abonnementliste festzulegen, wählen Sie Neue Liste . CloudWatch speichert die Liste und zeigt sie im Feld an, damit Sie sie verwenden können, um zukünftige Alarme einzurichten.

#### Note

Wenn Sie die neue Liste verwenden, um ein neues Amazon SNS-Thema zu erstellen, müssen die E-Mail-Adressen verifiziert werden, bevor die gewünschten Empfänger Benachrichtigungen erhalten. Amazon SNS sendet nur dann eine E-Mail, wenn der Alarm einen Alarmzustand auslöst. Wenn sich dieser Alarmstatus ändert, bevor die E-Mail-Adressen verifiziert werden, erhalten die vorgesehenen Empfänger keine Benachrichtigung.

11. Wählen Sie Weiter aus. Fügen Sie einen Namen und eine optionale Beschreibung für Ihren Alarm hinzu. Wählen Sie Weiter aus.
12. Wählen Sie Alarm erstellen aus.

## Metriken für Amazon Fraud Detector

Amazon Fraud Detector sendet die folgenden Metriken an CloudWatch. Alle Metriken unterstützen diese Statistiken: Average, Minimum, Maximum, Sum.

Kennzahl	Beschreibung
GetEventPrediction	Die Anzahl der GetEventPrediction API-Anforderungen.  Gültige Dimensionen: DetectorID

Kennzahl	Beschreibung
GetEventPredictionLatency	<p>Das Zeitintervall, das benötigt wird, um auf eine Client-Anfrage aus der GetEventPrediction Anfrage zu antworten.</p> <p>Gültige Dimensionen: DetectorID</p> <p>Einheit: Millisekunden</p>
GetEventPrediction4XXError	<p>Die Anzahl der GetEventPrediction Anfragen, bei denen Amazon Fraud Detector einen 4xx-HTTP-Antwortcode zurückgegeben hat. Für jede 4xx-Antwort wird 1 gesendet.</p> <p>Gültige Dimensionen: DetectorID</p>
GetEventPrediction5XXError	<p>Die Anzahl der GetEventPrediction Anfragen, bei denen Amazon Fraud Detector einen 5xx-HTTP-Antwortcode zurückgegeben hat. Für jede 5xx-Antwort wird 1 gesendet.</p> <p>Gültige Dimensionen: DetectorID</p>
Prediction	<p>Die Anzahl der Vorhersagen. 1 wird gesendet, wenn erfolgreich.</p> <p>Gültige Dimensionen: DetectorID , DetectorVersionID</p>
PredictionLatency	<p>Das Zeitintervall für eine Vorhersageoperation.</p> <p>Gültige Dimensionen: DetectorID , DetectorVersionID</p> <p>Einheit: Millisekunden</p>

Kennzahl	Beschreibung
PredictionError	<p>Die Anzahl der Vorhersagen, bei denen Amazon Fraud Detector auf einen Fehler gestoßen ist. 1 wird gesendet, wenn ein Fehler auftritt.</p> <p>Gültige Dimensionen: DetectorID , DetectorVersionID</p>
VariableUsed	<p>Die Anzahl der GetEventPrediction Anforderungen, bei denen die Variable im Rahmen der Auswertung verwendet wurde.</p> <p>Gültige Dimensionen: DetectorID , DetectorVersionID , VariableName</p>
VariableDefaultReturned	<p>Die Anzahl der GetEventPrediction Anforderungen, bei denen die Variable nicht als Teil der Ereignisattribute vorhanden war und daher der Standardwert für die Variable während der Auswertung verwendet wurde.</p> <p>Gültige Dimensionen: DetectorID , DetectorVersionID , VariableName</p>
RuleNotEvaluated	<p>Die Anzahl der GetEventPrediction Anforderungen, bei denen die Regel nicht ausgewertet wurde, weil eine vorherige Regel übereinstimmte.</p> <p>Gültige Dimensionen: DetectorID , DetectorVersionID , RuleID</p>
RuleEvaluateTrue	<p>Die Anzahl der GetEventPrediction Anforderungen, bei denen die Regel als wahr ausgelöst wurde und das Regelergebnis zurückgegeben wurde.</p> <p>Gültige Dimensionen: DetectorID , DetectorVersionID , RuleID</p>

Kennzahl	Beschreibung
<code>RuleEvaluateFalse</code>	<p>Die Anzahl der <code>GetEventPrediction</code> Anforderungen, bei denen die Regel auf „Falsch“ ausgewertet wurde.</p> <p>Gültige Dimensionen: <code>DetectorID</code> , <code>DetectorVersionID</code> , <code>RuleID</code></p>
<code>RuleEvaluateError</code>	<p>Die Anzahl der <code>GetEventPrediction</code> Anforderungen, bei denen die Regel fehlerhaft ausgewertet wird</p> <p>Gültige Dimensionen: <code>DetectorID</code> , <code>DetectorVersionID</code> , <code>RuleID</code></p>
<code>OutcomeReturned</code>	<p>Die Anzahl der <code>GetEventPrediction</code> Anrufe, bei denen das angegebene Ergebnis zurückgegeben wurde.</p> <p>Gültige Dimensionen: <code>DetectorID</code> , <code>DetectorVersionID</code> , <code>OutcomeName</code></p>
<code>ModelInvocation</code> (Amazon SageMaker model endpoint)	<p>Die Anzahl der <code>GetEventPrediction</code> Anforderungen, bei denen der SageMaker Modellendpunkt im Rahmen der Auswertung aufgerufen wurde.</p> <p>Gültige Dimensionen: <code>DetectorID</code> , <code>DetectorVersionID</code> , <code>ModelEndpoint</code></p>
<code>ModelInvocationError</code> (Amazon SageMaker model endpoint)	<p>Die Anzahl der <code>GetEventPrediction</code> Anforderungen, bei denen der aufgerufene SageMaker Modellendpunkt während der Auswertung einen Fehler zurückgegeben hat.</p> <p>Gültige Dimensionen: <code>DetectorID</code> , <code>DetectorVersionID</code> , <code>ModelEndpoint</code></p>

Kennzahl	Beschreibung
ModelInvocationLatency (Amazon SageMaker model endpoint)	<p>Das Zeitintervall, das das importierte Modell benötigt, um wie von Amazon Fraud Detector angesehen zu reagieren. Dieses Intervall umfasst nur den Modellaufruf.</p> <p>Gültige Dimensionen: DetectorID , DetectorVersionID , ModelEndpoint</p> <p>Einheit: Millisekunden</p>
ModelInvocation	<p>Die Anzahl der GetEventPrediction Anfragen, bei denen das Modell im Rahmen der Auswertung aufgerufen wurde.</p> <p>Gültige Dimensionen: DetectorID , DetectorVersionID , ModelType , ModelID</p>
ModelInvocationError	<p>Die Anzahl der GetEventPrediction Anfragen, bei denen das Amazon Fraud Detector-Modell während der Auswertung einen Fehler zurückgegeben hat.</p> <p>Gültige Dimensionen: DetectorID , DetectorVersionID , ModelType , ModelID</p>
ModelInvocationLatency	<p>Das Zeitintervall, das das Amazon Fraud Detector Model benötigt, um wie von Amazon Fraud Detector angesehen zu reagieren. Dieses Intervall umfasst nur den Modellaufruf.</p> <p>Gültige Dimensionen: DetectorID , DetectorVersionID , ModelType , ModelID</p> <p>Einheit: Millisekunden</p>

# Protokollieren von API-Aufrufen von Amazon Fraud Detector mit AWS CloudTrail

Amazon Fraud Detector ist integriert, einem ServiceAWS CloudTrail, der die Aktionen eines Benutzers, einer Rolle oder eines -AWSServices in Amazon Fraud Detector aufzeichnet. CloudTrail erfasst alle API-Aufrufe für Amazon Fraud Detector als Ereignisse, einschließlich Aufrufen von der Amazon Fraud Detector-Konsole und Aufrufen von Code an die Amazon Fraud Detector APIs.

Wenn Sie einen Trail erstellen, können Sie die kontinuierliche Bereitstellung von CloudTrail Ereignissen an einen Amazon S3-Bucket aktivieren, einschließlich Ereignissen für Amazon Fraud Detector. Wenn Sie keinen Trail konfigurieren, können Sie trotzdem die neuesten Ereignisse in der CloudTrail Konsole unter Ereignisverlauf anzeigen. Anhand der von CloudTrail gesammelten Informationen können Sie die an Amazon Fraud Detector gestellte Anfrage, die IP-Adresse, von der die Anfrage gestellt wurde, den Initiator der Anfrage, den Zeitpunkt der Anfrage und zusätzliche Details bestimmen.

Weitere Informationen zu CloudTrail finden Sie im [AWS CloudTrail -Benutzerhandbuch](#).

## Informationen zu Amazon Fraud Detector in CloudTrail

CloudTrail wird beim Erstellen des AWS Kontos in Ihrem Konto aktiviert. Wenn eine Aktivität in Amazon Fraud Detector auftritt, wird diese Aktivität in einem - CloudTrail Ereignis zusammen mit anderen -AWSServiceereignissen im Ereignisverlauf aufgezeichnet. Sie können die neuesten Ereignisse in Ihr AWS-Konto herunterladen und dort suchen und anzeigen. Weitere Informationen finden Sie unter [Anzeigen von Ereignissen mit dem CloudTrail Ereignisverlauf](#).

Erstellen Sie für eine fortlaufende Aufzeichnung der Ereignisse in Ihrem AWS Konto, einschließlich Ereignissen für Amazon Fraud Detector, einen Trail. Ein Trail ermöglicht CloudTrail die Bereitstellung von Protokolldateien an einen Amazon S3-Bucket. Wenn Sie einen Pfad in der Konsole anlegen, gilt dieser für alle AWS-Regionen. Der Trail protokolliert Ereignisse aus allen Regionen in der AWS-Partition und stellt die Protokolldateien in dem von Ihnen angegebenen Amazon-S3-Bucket bereit. Darüber hinaus können Sie andere -AWSServices konfigurieren, um die in den CloudTrail Protokollen erfassten Ereignisdaten weiter zu analysieren und entsprechend zu agieren. Weitere Informationen finden Sie hier:

- [Übersicht zum Erstellen eines Trails](#)
- [CloudTrail Unterstützte Services und Integrationen](#)
- [Konfigurieren von Amazon SNS-Benachrichtigungen für CloudTrail](#)

- [Empfangen von CloudTrail Protokolldateien aus mehreren Regionen](#) und [Empfangen CloudTrail von Protokolldateien aus mehreren Konten](#)

Amazon Fraud Detector unterstützt die Protokollierung jeder Aktion (API-Operation) als Ereignis in CloudTrail Protokolldateien. Weitere Informationen finden Sie unter [Aktionen](#).

Jeder Ereignis- oder Protokolleintrag enthält Informationen zu dem Benutzer, der die Anforderung generiert hat. Die Identitätsinformationen unterstützen Sie bei der Ermittlung der folgenden Punkte:

- Ob die Anforderung mit Root- oder -Benutzeranmeldeinformationen ausgeführt wurde.
- Gibt an, ob die Anforderung mit temporären Sicherheitsanmeldeinformationen für eine Rolle oder einen Verbundbenutzer gesendet wurde.
- Ob die Anforderung aus einem anderen AWS-Service gesendet wurde

Weitere Informationen finden Sie unter [CloudTrail userIdentity-Element](#).

## Grundlegendes zu Protokolldateieinträgen von Amazon Fraud Detector

Ein Trail ist eine Konfiguration, die die Bereitstellung von Ereignissen als Protokolldateien an einen von Ihnen angegebenen Amazon S3-Bucket ermöglicht. CloudTrail Protokolldateien enthalten einen oder mehrere Protokolleinträge. Ein Ereignis stellt eine einzelne Anforderung aus einer beliebigen Quelle dar und enthält Informationen über die angeforderte Operation, das Datum und die Uhrzeit der Operation, die Anforderungsparameter usw. CloudTrail Protokolldateien sind kein geordnetes Stacktrace der öffentlichen API-Aufrufe und erscheinen daher nicht in einer bestimmten Reihenfolge.

Das folgende Beispiel zeigt einen - CloudTrail Protokolleintrag, der die -GetDetectorsOperation demonstriert.

```
{
  "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"
}
```




# Fehlerbehebung

Die folgenden Abschnitte helfen Ihnen bei der Behebung von Problemen, die bei der Arbeit mit Amazon Fraud Detector auftreten können.

## Beheben von Problemen mit Trainingsdaten

Verwenden Sie die Informationen in diesem Abschnitt, um Probleme zu diagnostizieren und zu beheben, die im Diagnosebereich Modelltraining in der Amazon Fraud Detector-Konsole auftreten können, wenn Sie Ihr Modell trainieren.

Die im Diagnosebereich Modelltraining angezeigten Probleme sind wie folgt kategorisiert. Die Anforderung zur Behebung des Problems hängt von der Kategorie des Problems ab.

-  Fehler – führt dazu, dass das Modelltraining fehlschlägt. Diese Probleme müssen behoben werden, damit das Modell erfolgreich trainiert werden kann.
-  Warnung – bewirkt, dass das Modelltraining fortgesetzt wird. Einige der Variablen werden jedoch möglicherweise im Trainingsprozess ausgeschlossen. Suchen Sie nach den entsprechenden Anleitungen in diesem Abschnitt, um die Qualität Ihres Datensatzes zu verbessern.
-  Informationen (Informationen) – hat keine Auswirkungen auf das Modelltraining und alle Variablen werden für das Training verwendet. Wir empfehlen Ihnen, die entsprechenden Anleitungen in diesem Abschnitt zu lesen, um die Qualität Ihres Datensatzes und Ihrer Modellleistung weiter zu verbessern.

### Themen

- [Instabile Betrugsrate im angegebenen Datensatz](#)
- [Unzureichende Daten](#)
- [Fehlende oder andere EVENT\\_LABEL-Werte](#)
- [Fehlende oder falsche EVENT\\_TIMESTAMP-Werte](#)
- [Nicht aufgenommene Daten](#)
- [Unzureichende Variablen](#)

- [Fehlender oder falscher Variablentyp](#)
- [Fehlende Variablenwerte](#)
- [Unzureichende eindeutige Variablenwerte](#)
- [Falscher Variablenausdruck](#)
- [Unzureichende eindeutige Entitäten](#)

## Instabile Betrugsrate im angegebenen Datensatz

Problemtyp : Fehler

Beschreibung

Die Betrugsrate in den angegebenen Daten ist im Laufe der Zeit zu instabil. Bitte stellen Sie sicher, dass Ihre Betrugs- und legitimen Ereignisse im Laufe der Zeit einheitlich erfasst werden.

Ursache

Dieser Fehler tritt auf, wenn die Betrugs- und legitimen Ereignisse in Ihrem Datensatz ungleichmäßig verteilt sind und aus verschiedenen Zeitfenstern stammen. Der Modelltrainingsprozess von Amazon Fraud Detector nimmt Stichproben und partitioniert Ihren Datensatz basierend auf `EVENT_TIMESTAMP`. Wenn Ihr Datensatz beispielsweise aus Betrugsereignissen der letzten 6 Monate besteht, aber nur der letzte Monat legitimer Ereignisse enthalten ist, wird der Datensatz als instabil betrachtet. Ein instabiler Datensatz kann zu Verzerrungen bei der Bewertung der Modellleistung führen.

Lösung

Stellen Sie sicher, dass Sie die Daten zu betrügerischen und legitimen Ereignissen aus demselben Zeitfenster bereitstellen, und die Betrugsrate ändert sich im Laufe der Zeit nicht drastisch.

## Unzureichende Daten

1. Problemtyp : Fehler

Beschreibung

Weniger als 50 Zeilen werden als betrügerische Ereignisse gekennzeichnet. Stellen Sie sicher, dass sowohl betrügerische als auch legitime Ereignisse die Mindestanzahl von 50 überschreiten, und trainieren Sie das Modell erneut.

## Ursache

Dieser Fehler tritt auf, wenn Ihr Datensatz weniger Ereignisse enthält, die als betrügerisch gekennzeichnet sind als für das Modelltraining erforderlich. Amazon Fraud Detector erfordert mindestens 50 betrügerische Ereignisse, um Ihr Modell zu trainieren.

## Lösung

Stellen Sie sicher, dass Ihr Datensatz mindestens 50 betrügerische Ereignisse enthält. Sie können dies sicherstellen, indem Sie bei Bedarf einen längeren Zeitraum abdecken.

## 2. Problemtyp : Fehler

### Beschreibung

Weniger als 50 Zeilen werden als legitime Ereignisse bezeichnet. Stellen Sie sicher, dass sowohl betrügerische als auch legitime Ereignisse die Mindestanzahl von `$threshold` überschreiten, und trainieren Sie das Modell erneut.

### Ursache

Dieser Fehler tritt auf, wenn Ihr Datensatz weniger Ereignisse enthält, die als legitime Ereignisse gekennzeichnet sind, als für das Modelltraining erforderlich. Amazon Fraud Detector erfordert mindestens 50 legitime Ereignisse, um Ihr Modell zu trainieren.

### Lösung

Stellen Sie sicher, dass Ihr Datensatz mindestens 50 legitime Ereignisse enthält. Sie können dies sicherstellen, indem Sie bei Bedarf einen längeren Zeitraum abdecken.

## 3. Problemtyp : Fehler

### Beschreibung

Die Anzahl der eindeutigen Entitäten im Zusammenhang mit Betrug beträgt weniger als 100. Erwägen Sie, weitere Beispiele für betrügerische Entitäten einzubeziehen, um die Leistung zu verbessern.

### Ursache

Dieser Fehler tritt auf, wenn Ihr Datensatz weniger Entitäten mit betrügerischen Ereignissen enthält, als für das Modelltraining erforderlich. Das Transaction Fraud Insights (TFI)-Modell

erfordert mindestens 100 Entitäten mit Betrugseignissen, um eine maximale Abdeckung des Betrugsbereichs sicherzustellen. Das Modell kann möglicherweise nicht gut verallgemeinert werden, wenn alle Betrugseignisse von einer kleinen Gruppe von Entitäten ausgeführt werden.

### Lösung

Stellen Sie sicher, dass Ihr Datensatz mindestens 100 Entitäten mit betrügerischen Ereignissen enthält. Sie können sicherstellen, dass dies bei Bedarf einen längeren Zeitraum abdeckt.

## 4. Problemtyp : Fehler

### Beschreibung

Die Anzahl der eindeutigen Entitäten, die mit legitimen Entitäten verknüpft sind, beträgt weniger als 100. Erwägen Sie, weitere Beispiele für legitime Entitäten einzubeziehen, um die Leistung zu verbessern.

### Ursache

Dieser Fehler tritt auf, wenn Ihr Datensatz weniger Entitäten mit legitimen Ereignissen hat, als für das Modelltraining erforderlich. Das Transaction Fraud Insights (TFI)-Modell erfordert mindestens 100 Entitäten mit legitimen Ereignissen, um eine maximale Abdeckung des Betrugsbereichs sicherzustellen. Das Modell kann möglicherweise nicht gut verallgemeinert werden, wenn alle legitimen Ereignisse von einer kleinen Gruppe von Entitäten ausgeführt werden.

### Lösung

Stellen Sie sicher, dass Ihr Datensatz mindestens 100 Entitäten mit legitimen Ereignissen enthält. Sie können sicherstellen, dass dies bei Bedarf einen längeren Zeitraum abdeckt.

## 5. Problemtyp : Fehler

### Beschreibung

Im Datensatz befinden sich weniger als 100 Zeilen. Stellen Sie sicher, dass mehr als 100 Zeilen im gesamten Datensatz vorhanden sind und mindestens 50 Zeilen als betrügerisch gekennzeichnet sind.

### Ursache

Dieser Fehler tritt auf, wenn Ihr Datensatz weniger als 100 Datensätze enthält. Amazon Fraud Detector benötigt Daten aus mindestens 100 Ereignissen (Datensätzen) in Ihrem Datensatz für das Modelltraining.

### Lösung

Stellen Sie sicher, dass Sie Daten aus mehr als 100 Ereignissen in Ihrem Datensatz haben.

## Fehlende oder andere EVENT\_LABEL-Werte

### 1. Problemtyp : Fehler

#### Beschreibung

Größer als 1 % Ihrer Spalte EVENT\_LABEL sind null oder andere Werte als die, die in der Modellkonfiguration definiert sind **\$label\_values**. Stellen Sie sicher, dass in Ihrer Spalte EVENT\_LABEL weniger als 1 % der fehlenden Werte vorhanden sind und die Werte in der Modellkonfiguration definiert sind **\$label\_values**.

#### Ursache

Dieser Fehler tritt aus einem der folgenden Gründe auf:

- Bei mehr als 1 % der Datensätze in der CSV-Datei, die Ihre Trainingsdaten enthalten, fehlen Werte in der Spalte EVENT\_LABEL.
- Mehr als 1 % der Datensätze in der CSV-Datei, die Ihre Trainingsdaten enthalten, haben Werte in der Spalte EVENT\_LABEL, die sich von denen unterscheiden, die mit Ihrem Ereignistyp verknüpft sind.

Das OFI-Modell (Online Fraud Insights) erfordert, dass die Spalte EVENT\_LABEL in jedem Datensatz mit einer der Bezeichnungen gefüllt wird, die Ihrem Ereignistyp zugeordnet sind (oder in zugeordnet sind `CreateModelVersion`).

#### Lösung

Wenn dieser Fehler auf die fehlenden Werte von EVENT\_LABEL zurückzuführen ist, sollten Sie diesen Datensätzen die richtigen Bezeichnungen zuweisen oder diese Datensätze aus Ihrem Datensatz entfernen. Wenn dieser Fehler darauf zurückzuführen ist, dass Beschriftungen einiger Datensätze nicht zu den gehören **label\_values**, stellen Sie sicher, dass Sie alle

Werte in der Spalte `EVENT_LABEL` zu Beschriftungen des Ereignistyps hinzufügen und bei der Modellerstellung entweder betrügerischen oder legitimen (betrügerischen, Legit-) zugeordnet sind.

## 2. Problemtyp : Informationen

### Beschreibung

Ihre Spalte `EVENT_LABEL` enthält andere Null- oder Labelwerte als die, die in der Modellkonfiguration definiert sind `$label_values`. Diese inkonsistenten Werte wurden vor dem Training in „nicht in Betrug“ umgewandelt.

### Ursache

Sie erhalten diese Informationen aus einem der folgenden Gründe:

- Weniger als 1 % der Datensätze in der CSV-Datei, die Ihre Trainingsdaten enthalten, haben fehlende Werte in der Spalte `EVENT_LABEL`
- Weniger als 1 % der Datensätze in der CSV-Datei, die Ihre Trainingsdaten enthalten, haben Werte in der Spalte `EVENT_LABEL`, die sich von denen unterscheiden, die mit Ihrem Ereignistyp verknüpft sind.

Das Modelltraining wird in beiden Fällen erfolgreich sein. Die Beschriftungswerte dieser Ereignisse, die fehlende oder nicht zugeordnete Beschriftungswerte aufweisen, werden jedoch in legitime Werte umgewandelt. Wenn Sie dies als Problem betrachten, folgen Sie der unten aufgeführten Lösung.

### Lösung

Wenn in Ihrem Datensatz `EVENT_LABEL`-Werte fehlen, sollten Sie diese Datensätze aus Ihrem Datensatz entfernen. Wenn die für diese `EVENT_LABELS` bereitgestellten Werte nicht zugeordnet sind, stellen Sie sicher, dass alle diese Werte für jedes Ereignis entweder betrügerischen oder legitimen (betrügerischen, suffizienten) Werten zugeordnet sind.

## Fehlende oder falsche `EVENT_TIMESTAMP`-Werte

### 1. Problemtyp : Fehler

#### Beschreibung

Ihr Trainingsdatensatz enthält EVENT\_TIMESTAMP mit Zeitstempeln, die nicht den akzeptierten Formaten entsprechen. Stellen Sie sicher, dass das Format eines der akzeptierten Datums-/Zeitstempelformate ist.

### Ursache

Dieser Fehler tritt auf, wenn die Spalte EVENT\_TIMESTAMP einen Wert enthält, der nicht den von Amazon Fraud Detector unterstützten [Zeitstempelformaten](#) entspricht.

### Lösung

Stellen Sie sicher, dass die für die Spalte EVENT\_TIMESTAMP bereitgestellten Werte den unterstützten [Zeitstempelformaten](#) entsprechen. Wenn in der Spalte EVENT\_TIMESTAMP Werte fehlen, können Sie diese entweder mit Werten im unterstützten Zeitstempelformat auffüllen oder erwägen, das Ereignis vollständig zu löschen mit null, anstatt Zeichenfolgen wie none, oder einzugeben missing.

## 2. Problemtyp : Fehler

Ihr Trainingsdatensatz enthält EVENT\_TIMESTAMP mit fehlenden Werten. Stellen Sie sicher, dass keine Werte fehlen.

### Ursache

Dieser Fehler tritt auf, wenn in der Spalte EVENT\_TIMESTAMP in Ihrem Datensatz Werte fehlen. Amazon Fraud Detector erfordert, dass die Spalte EVENT\_TIMESTAMP in Ihrem Datensatz Werte enthält.

### Lösung

Stellen Sie sicher, dass die Spalte EVENT\_TIMESTAMP in Ihrem Datensatz Werte enthält und diese Werte den unterstützten [Zeitstempelformaten](#) entsprechen. Wenn in der Spalte EVENT\_TIMESTAMP Werte fehlen, können Sie diese entweder mit Werten im unterstützten Zeitstempelformat auffüllen oder erwägen, das Ereignis vollständig zu löschen mit null, anstatt Zeichenfolgen wie none, oder einzugeben missing.

## Nicht aufgenommene Daten

### Problemtyp : Fehler



## Beschreibung

Für das Training wurden keine aufgenommenen Ereignisse gefunden. Bitte überprüfen Sie Ihre Trainingskonfiguration.

## Ursache

Dieser Fehler tritt auf, wenn Sie ein Modell mit Ereignisdaten erstellen, die in Amazon Fraud Detector gespeichert sind, Ihren Datensatz jedoch nicht in Amazon Fraud Detector importiert haben, bevor Sie mit dem Trainieren Ihres Modells begonnen haben.

## Lösung

Verwenden Sie die `SendEvent` API-Operation, die `CreateBatchImportJob` API-Operation oder die Batch-Importfunktion in der Amazon Fraud Detector-Konsole, um zuerst Ihre Ereignisdaten zu importieren und dann Ihr Modell zu trainieren. Weitere Informationen finden Sie unter [Gespeicherte Ereignisdatensätze](#).

### Note

Wir empfehlen, 10 Minuten zu warten, nachdem Sie den Import Ihrer Daten abgeschlossen haben, bevor Sie sie zum Trainieren Ihres Modells verwenden.

Sie können die Amazon Fraud Detector-Konsole verwenden, um die Anzahl der Ereignisse zu überprüfen, die bereits für jeden Ereignistyp gespeichert sind. Weitere Informationen finden Sie unter [Anzeigen von Metriken Ihrer gespeicherten Ereignisse](#).

## Unzureichende Variablen

Problemtyp : Fehler

## Beschreibung

Der Datensatz muss mindestens 2 Variablen enthalten, die für das Training geeignet sind.

## Ursache

Dieser Fehler tritt auf, wenn Ihr Datensatz weniger als 2 Variablen enthält, die für das Modelltraining geeignet sind. Amazon Fraud Detector betrachtet eine Variable, die nur für das Modelltraining geeignet ist, wenn sie alle Validierungen besteht. Wenn eine Variable nicht validiert werden kann,

wird sie im Modelltraining ausgeschlossen und Sie erhalten eine Meldung unter Diagnose des Modelltrainings.

## Lösung

Stellen Sie sicher, dass Ihr Datensatz über mindestens zwei Variablen verfügt, die mit Werten gefüllt sind und alle Datenvalidierungen bestanden haben. Beachten Sie, dass die Zeile mit den Ereignismetadaten, in der Sie Ihre Spaltenüberschriften angegeben haben (EVENT\_TIMESTAMP, EVENT\_ID, ENTITY\_ID, EVENT\_LABEL usw.), nicht als Variable betrachtet wird.

## Fehlender oder falscher Variablentyp

Problemtyp : Warnung

### Beschreibung

Der erwartete Datentyp für **\$variable\_name** ist NUMERIC. Überprüfen und aktualisieren Sie **\$variable\_name** in Ihrem Datensatz und trainieren Sie das Modell erneut.

### Ursache

Sie erhalten diese Warnung, wenn eine Variable als NUMERIC-Variable definiert ist, aber im Datensatz Werte enthält, die nicht in NUMERIC konvertiert werden können. Daher wird diese Variable beim Modelltraining ausgeschlossen.

## Lösung

Wenn Sie sie als NUMERIC-Variable beibehalten möchten, stellen Sie sicher, dass die von Ihnen angegebenen Werte in eine Gleitkommazahl konvertiert werden können. Beachten Sie, dass die Variable keine Zeichenfolgen wie , oder enthältnonenenu11, wenn sie fehlende Werte enthältmissing. Wenn die Variable nicht numerische Werte enthält, erstellen Sie sie als CATEGORICAL- oder microSD\_FORM\_TEXT-Variablentyp neu.

## Fehlende Variablenwerte

Problemtyp : Warnung

### Beschreibung

Größer als **\$threshold** Werte für **\$variable\_name** fehlen in Ihrem Trainingsdatensatz. Erwägen Sie, **\$variable\_name** Ihren Datensatz zu ändern und das Training erneut durchzuführen, um die Leistung zu verbessern.

## Ursache

Sie erhalten diese Warnung, wenn die angegebene Variable aufgrund zu vieler fehlender Werte gelöscht wird. Amazon Fraud Detector lässt fehlende Werte für eine Variable zu. Wenn jedoch eine Variable zu viele fehlende Werte enthält, trägt sie nicht viel zum Modell bei und diese Variable wird beim Modelltraining gelöscht.

## Lösung

Stellen Sie zunächst sicher, dass diese fehlenden Werte nicht auf Fehler bei der Datenerfassung und -vorbereitung zurückzuführen sind. Wenn es sich um Fehler handelt, können Sie sie aus Ihrem Modelltraining entfernen. Wenn Sie jedoch der Meinung sind, dass diese fehlenden Werte nützlich sind und diese Variable trotzdem beibehalten möchten, können Sie fehlende Werte sowohl beim Modelltraining als auch bei der Echtzeitinferenz manuell mit einer Konstante füllen.

## Unzureichende eindeutige Variablenwerte

Problemtyp : Warnung

### Beschreibung

Die Anzahl der eindeutigen Werte von **\$variable\_name** ist niedriger als 100. Überprüfen und aktualisieren Sie **\$variable\_name** in Ihrem Datensatz und trainieren Sie das Modell erneut.

### Ursache

Sie erhalten diese Warnung, wenn die Anzahl der eindeutigen Werte der angegebenen Variablen kleiner als 100 ist. Die Schwellenwerte unterscheiden sich je nach Variablentyp. Bei sehr wenigen eindeutigen Werten besteht das Risiko, dass der Datensatz nicht allgemein genug ist, um den Feature-Bereich dieser Variablen abzudecken. Daher kann es sein, dass das Modell bei Echtzeitvorhersagen nicht gut verallgemeinert wird.

### Lösung

Stellen Sie zunächst sicher, dass die Variablenverteilung repräsentativ für den echten Geschäftsverkehr ist. Anschließend können Sie entweder fein trainierte Variablen mit höherer Kardinalität übernehmen, z. B. `full_customer_name` anstelle von `first_name` und `last_name` separat verwenden, oder den Variablentyp in CATEGORICAL ändern, was eine geringere Kardinalität ermöglicht.

# Falscher Variablenausdruck

## 1. Problemtyp : Informationen

### Beschreibung

Größer als 50 % der **\$email\_variable\_name** Werte entsprechen nicht dem erwarteten regulären Ausdruck `http://emailregex.com`. Erwägen Sie, **\$email\_variable\_name** Ihren Datensatz zu ändern und das Training erneut durchzuführen, um die Leistung zu verbessern.

### Ursache

Diese Informationen werden angezeigt, wenn mehr als 50 % Datensätze in Ihrem Datensatz E-Mail-Werte haben, die nicht einem regulären E-Mail-Ausdruck entsprechen und daher nicht validiert werden können.

### Lösung

Formatieren Sie die E-Mail-Variablenwerte so, dass sie dem regulären Ausdruck entsprechen. Wenn E-Mail-Werte fehlen, empfehlen wir, sie leer zu lassen `null`, anstatt sie mit Zeichenfolgen wie `none`, oder zu füllen `missing`.

## 2. Problemtyp : Informationen

### Beschreibung

Größer als 50 % der **\$IP\_variable\_name** Werte stimmen nicht mit dem regulären Ausdruck für IPv4- oder IPv6-Adressen `https://digitalfortress.tech/tricks/top-15-commonly-used-regex/` überein. Erwägen Sie, **\$IP\_variable\_name** Ihren Datensatz zu ändern und das Training erneut durchzuführen, um die Leistung zu verbessern.

### Ursache

Diese Informationen werden angezeigt, wenn mehr als 50 % Datensätze in Ihrem Datensatz IP-Werte haben, die nicht einem regulären IP-Ausdruck entsprechen und daher nicht validiert werden können.

### Lösung

Formatieren Sie die IP-Werte so, dass sie dem regulären Ausdruck entsprechen. Wenn IP-Werte fehlen, empfehlen wir, sie leer zu lassen `null`, anstatt sie mit Zeichenfolgen wie `none`, oder zu füllen `missing`.

### 3. Problemtyp : Informationen

#### Beschreibung

Größer als 50 % der **\$phone\_variable\_name** Werte stimmen nicht mit dem regulären Standardausdruck des Telefons überein `/ $pattern/`. Erwägen Sie, **\$phone\_variable\_name** in Ihrem Datensatz zu ändern und erneut zu trainieren, um die Leistung zu verbessern.

#### Ursache

Diese Informationen werden angezeigt, wenn mehr als 50 % Datensätze in Ihrem Datensatz Telefonnummern haben, die nicht einem regulären Telefonnummernausdruck entsprechen und daher nicht validiert werden können.

#### Lösung

Formatieren Sie die Telefonnummern so, dass sie dem regulären Ausdruck entsprechen. Wenn Telefonnummern fehlen, empfehlen wir, sie leer zu lassen `null`, anstatt sie mit Zeichenfolgen wie `none`, oder zu füllen `missing`.

## Unzureichende eindeutige Entitäten

### Problemtyp : Informationen

#### Beschreibung

Die Anzahl der eindeutigen Entitäten beträgt weniger als 1 500. Erwägen Sie, mehr Daten einzubeziehen, um die Leistung zu verbessern.

#### Ursache

Diese Informationen werden angezeigt, wenn Ihr Datensatz eine geringere Anzahl eindeutiger Entitäten als die empfohlene Anzahl hat. Das Transaction Fraud Insights (TFI)-Modell verwendet sowohl Zeitreihenaggregate als auch generische Transaktionsfunktionen, um die beste Leistung zu erzielen. Wenn Ihr Datensatz zu wenige eindeutige Entitäten hat, haben die meisten Ihrer generischen Daten wie `IP_ADDRESS`, `EMAIL_ADDRESS` möglicherweise keine eindeutigen Werte.

Dann besteht auch das Risiko, dass dieser Datensatz nicht allgemein genug ist, um den Feature-Bereich dieser Variablen abzudecken. Daher kann es sein, dass das Modell bei Transaktionen von neuen Entitäten nicht gut generalisiert wird.

### Lösung

Fügen Sie weitere Entitäten hinzu. Verlängern Sie Ihren Zeitbereich für Trainingsdaten bei Bedarf.

# Kontingente

Ihr AWS-Konto verfügt über Standardkontingente, die früher als Limits bezeichnet wurden, für jeden Amazon Web Service. Wenn nicht anders angegeben, gilt jedes Kontingent spezifisch für eine Region. Sie können eine Kontingenterhöhung für alle in den folgenden Tabellen genannten anpassbaren Kontingenterhöhungen anfordern. Weitere Informationen finden Sie unter [Beantragen einer Kontingenterhöhung](#)

In den folgenden Tabellen sind die Amazon Fraud Detector Detector-Kontingente nach Komponenten aufgeführt.

## Amazon Fraud Detector Modelle

Kontingentname	Standardkontingent	Anpassbar
Größe der Trainingsdaten	5 GB	Nein
Modelle pro Konto	50	Nein
Versionen pro Modell	200	Nein
Bereitgestellte Modellversionen pro Konto	5	Nein
Gleichzeitige Trainingsaufträge pro Konto	3	Nein
Gleichzeitige Trainingsaufträge pro Modell	1	Nein

## Amazon Fraud Detector-Detektoren//Variablen/Ergebnisse/Regeln

Kontingentname	Standardkontingent	Anpassbar
Variablen pro Konto	5000	Nein

Kontingentsname	Standardkontingent	Anpassbar
Regeln pro -Konto	5000	Nein
Listen pro Regel	3	Nein
Ergebnisse pro Konto	5000	Nein
Detektoren pro Konto	100	Nein
Listen pro Detektor	30	Nein
Entwurfsversionen pro Detektor	100	Nein
Modelle pro Detektorversion	10	Nein
Labels pro Konto	100	Nein
Ereignistypen pro Konto	100	Nein
Objekttypen pro Konto	100	Nein

## Amazon Fraud Detector API

Kontingentsname	Standardkontingent	Anpassbar
GetEventPrediction API-Aufrufe pro Sekunde	200 TPS	Ja
Größe der Nutzlast pro GetEventPrediction API-Aufruf	256 KB	Nein
Anzahl der Eingänge pro GetEventPrediction API-Aufruf	5000	Nein



# Dokumentverlauf

In der folgenden Tabelle werden wichtige Änderungen im Amazon Fraud Detector-Benutzerhandbuch beschrieben. Wir aktualisieren auch das Amazon Fraud Detector-Benutzerhandbuch regelmäßig, um auf das Feedback einzugehen, das Sie uns senden.

Änderung	Beschreibung	Datum
<a href="#">Neue Variablen- und Datentypen</a>	Amazon Fraud Detector führt neue Variablentypen und einen Datentyp ein, mit dem Sie nützliche Informationen extrahieren können.	5. Juni 2023
<a href="#">Orchestrierung von Veranstaltungen</a>	Die Event-Orchestrierung macht es Ihnen einfach, Ereignisse mithilfe von Amazon AWS-Services EventBridge zur Weiterverarbeitung an die Weiterverarbeitung zu senden.	30. Mai 2023
<a href="#">Listen</a>	Mit der Ressource Listen können Sie als Teil einer Regel auf eine Reihe von Werten wie IP-Adressen oder E-Mail-Adressen verweisen. Verwenden Sie Listen in einer Regel, um den Zugriff oder eine Transaktion zuzulassen oder zu verweigern.	14. Februar 2023
<a href="#">Datenmodelle Explorer</a>	Der Data Models Explorer bietet Einblicke in die Datenelemente, die Amazon Fraud Detector zur Erstellung Ihres Betrugserkennungsm	15. Dezember 2022

odells benötigt. Verwenden Sie den Datenmodell-Explorer, bevor Sie Ihren Event-Datensatz vorbereiten.

### [Modell „Account Takeover Insights“](#)

Verwenden Sie das ATI (Account Takeover Insights) -Modell, um Konten zu erkennen, die durch böswillige Übernahmen, Phishing oder den Diebstahl von Anmeldeinformationen kompromittiert wurden.

21. Juli 2022

### [Aktualisierung des Kapitels](#)

Das Einführungskapitel wurde mit zusätzlichen Informationen zu Amazon Fraud Detector aktualisiert

11. April 2022

### [Variable Anreicherung](#)

Aktivieren Sie die Anreicherung einiger der von Ihnen bereitgestellten Rohdaten, um die Leistung der Modelle zu steigern, die diese Datenelemente verwenden und die vor dem 8. Februar 2022 trainiert wurden.

8. Februar 2022

### [Opt-Out-Richtlinien](#)

Verwenden Sie Opt-Out-Richtlinien, um die Verwendung Ihrer Eventdaten zur Entwicklung oder Verbesserung der Qualität von Amazon Fraud Detector abzulehnen.

6. Januar 2022

<a href="#">Verwirrter Abgeordneter: Prävention</a>	Erstellen Sie Richtlinien, um zu verhindern, dass ein Dritter oder eine dienstübergreifende Organisation eine Entität manipuliert, die berechtigt ist, in ihrem Namen zu handeln, um Zugriff auf Ressourcen in Ihrem Konto zu erhalten.	6. Dezember 2021
<a href="#">Event-Datensatz erstellen</a>	Verwenden Sie die Anleitung unter Event-Dataset erstellen , um Daten für das Training Ihres Modells vorzubereiten und zu sammeln.	22. November 2021
<a href="#">Erklärungen zur Vorhersage</a>	Verwenden Sie die Erläuterungen zu Prognosen, um zu erfahren, wie sich jede Ereignisvariable auf die Betrugsprognosewerte Ihres Modells ausgewirkt hat.	10. November 2021
<a href="#">Problembehandlung</a>	Verwenden Sie die Informationen unter Problembehandlung bei Trainingsdaten, um Probleme zu diagnostizieren und zu lösen, die möglicherweise in der Amazon Fraud Detector-Konsole auftreten, wenn Sie Ihr Modell trainieren.	11. Oktober 2021
<a href="#">Modell zur Erfassung von Erkenntnissen über Transaktionsbetrug</a>	Verwenden Sie das Modell Transaction Fraud Insights (TFI), um Online- oder card-not-present Transaktionsbetrug zu erkennen.	11. Oktober 2021

## [Gespeicherte Ereignisse](#)

Speichern Sie Ihre Eventdaten in Amazon Fraud Detector und verwenden Sie die gespeicherten Daten, um Ihre Modelle später zu trainieren. Durch das Speichern von Ereignisdaten in Amazon Fraud Detector können Sie Modelle trainieren, die automatisch berechnete Variablen verwenden, um die Leistung zu verbessern, die Modellumschulung zu vereinfachen und Betrugszeichnungen zu aktualisieren, um die Feedbackschleife des maschinellen Lernens zu schließen.

11. Oktober 2021

## [Wichtigkeit der Modellvariablen](#)

Verwenden Sie die Wichtigkeit von Modellvariablen, um zu erfahren, was die Leistung Ihres Modells nach oben oder unten treibt und welche Ihrer Modellvariablen am meisten dazu beitragen. Und dann optimieren Sie Ihr Modell, um die Gesamtleistung zu verbessern.

09. Juli 2021

## [Integration in AWS CloudFormation](#)

Verwenden Sie esAWS CloudFormation, um Ihre Amazon Fraud Detector-Ressourcen zu verwalten.

10. Mai 2021

---

<a href="#">Batch-Prognosen</a>	Verwenden Sie Batch-Vorhersagen, um Vorhersagen für eine Reihe von Ereignissen zu erhalten, für die keine Bewertung in Echtzeit erforderlich ist.	31. März 2021
<a href="#">Überarbeitung des Kapitels</a>	Überarbeitung von Ersten Schritten und anderen Abschnitten	17. Juli 2020
<a href="#">Erstversion</a>	Erstversion	02. Dezember 2019

Die vorliegende Übersetzung wurde maschinell erstellt. Im Falle eines Konflikts oder eines Widerspruchs zwischen dieser übersetzten Fassung und der englischen Fassung (einschließlich infolge von Verzögerungen bei der Übersetzung) ist die englische Fassung maßgeblich.