



Benutzerhandbuch

# AWS CloudTrail



Version 1.0

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

# AWS CloudTrail: 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 Marken, die nicht im Besitz von Amazon sind, gehören den jeweiligen Besitzern, die möglicherweise mit Amazon verbunden sind oder von Amazon gesponsert werden.

---

# Table of Contents

Was ist AWS CloudTrail? .....	1
Zugreifen CloudTrail .....	3
CloudTrail Konsole .....	3
AWS CLI .....	4
CloudTrail APIs .....	4
AWS SDKs .....	4
Wie CloudTrail funktioniert .....	4
CloudTrail Verlauf der Ereignisse .....	5
CloudTrail Datenspeicher für Seen und Ereignisse .....	5
CloudTrail Wanderwege .....	9
CloudTrail Einblicke und Ereignisse .....	15
CloudTrail Kanäle .....	17
Konzepte .....	17
CloudTrail Ereignisse .....	18
Ereignisverlauf .....	35
Trails .....	36
Organisatorische Pfade .....	38
CloudTrail Datenspeicher für Seen und Ereignisse .....	40
CloudTrail Einblicke .....	41
Tags .....	41
AWS Security Token Service und CloudTrail .....	41
Informationen zu globalen Serviceereignissen .....	42
Unterstützte Regionen .....	44
Unterstützte Services und Integrationen .....	47
AWS Serviceintegrationen mit Protokollen CloudTrail .....	48
CloudTrail Integration mit Amazon EventBridge .....	50
CloudTrail Integration mit AWS Organizations .....	51
AWS Servicethemen für CloudTrail .....	52
Nicht unterstützte Services .....	78
Kontingente in AWS CloudTrail .....	79
CloudTrail Tutorials .....	86
Erteilen Sie Nutzungsberechtigungen CloudTrail .....	86
Event-Historie anzeigen .....	88
Erstellen Sie einen Pfad, um Verwaltungsereignisse zu protokollieren .....	90

Protokolldateien ansehen .....	95
Plan für die nächsten Schritte .....	96
Erstellen Sie einen Ereignisdatenspeicher für S3-Datenereignisse .....	98
Kopieren Sie Trail-Ereignisse in einen CloudTrail Lake-Event-Datenspeicher .....	106
Lake-Dashboards anzeigen CloudTrail .....	116
CloudTrail Lake-Beispielabfragen anzeigen und ausführen .....	121
Speichern Sie die CloudTrail Lake-Abfrageergebnisse in einem S3-Bucket .....	124
CloudTrail Kosten und Nutzung anzeigen .....	128
Weitere Ressourcen .....	132
Mit dem CloudTrail Eventverlauf arbeiten .....	134
Einschränkungen des Ereignisverlaufs .....	135
Aktuelle Verwaltungsereignisse mit der Konsole anzeigen .....	136
Navigieren zwischen den Seiten .....	138
Anpassen der Anzeige .....	138
CloudTrail Ereignisse filtern .....	139
Details zu einem Ereignis ansehen .....	141
Herunterladen von Ereignissen .....	142
Anzeigen von mit AWS Config referenzierten Ressourcen .....	143
Aktuelle Verwaltungsereignisse anzeigen mit dem AWS CLI .....	144
Voraussetzungen .....	146
Erhalten der Befehlszeilenhilfe .....	146
Suchen von Ereignissen .....	146
Angabe der Anzahl der zurückzugebenden Ereignisse .....	148
Suchen von Ereignissen nach Zeitbereich .....	148
Suchen von Ereignissen nach Attribut .....	148
Angabe der nächsten Ergebnisseite .....	150
Abrufen der JSON-Eingabe aus einer Datei .....	151
Ausgabefelder der Suche .....	153
Ich arbeite mit CloudTrail Lake .....	155
CloudTrail Datenspeicher für Ereignisse in Lake .....	155
CloudTrail Lake-Integrationen .....	157
CloudTrail Lake-Abfragen .....	157
Weitere Ressourcen .....	158
CloudTrail Von Seen unterstützte Regionen .....	158
CloudTrail Konzepte und Terminologie von Seen .....	160
Ereignisdatenspeicher .....	161

Integrationen .....	162
Abfragen .....	164
Dashboard .....	164
Ereignisdatenspeicher .....	166
Ereignisdatenspeicher mit der Konsole erstellen, aktualisieren und verwalten .....	168
Erstellen, aktualisieren und verwalten Sie Ereignisdatenspeicher mit dem AWS CLI .....	228
Verwalten der Lebenszyklen von Ereignisdatenspeichern .....	254
Kopieren von Trail-Ereignissen in einen Ereignisdatenspeicher .....	256
Verbund für einen Ereignisdatenspeicher erstellen .....	280
Ereignisdatenspeicher einer Organisation .....	292
Integrationen .....	297
Erstellen Sie mit der Konsole eine Integration mit einem CloudTrail Partner .....	299
Erstellen Sie eine benutzerdefinierte Integration mit der Konsole .....	302
Erstellen, aktualisieren und verwalten Sie CloudTrail Lake-Integrationen mit dem AWS CLI .....	306
Zusätzliche Informationen über Integrationspartner .....	315
CloudTrail Ereignisschema für Lake Integrations .....	317
Lake-Dashboards anzeigen .....	326
Einschränkungen .....	327
Voraussetzungen .....	327
Auswählen eines Dashboards .....	327
Filtern eines Dashboards nach Datum oder Zeitraum .....	329
Anzeigen der Abfrage für ein Dashboard-Widget .....	330
Abfragen .....	157
Tools für Abfrageeditor .....	331
Beispielabfragen anzeigen .....	332
Abfrage erstellen oder bearbeiten .....	334
Ausführen einer Abfrage und Speichern von Abfrageergebnissen .....	337
Abfrageergebnisse anzeigen .....	342
Gespeicherte Abfrageergebnisse herunterladen .....	343
Validierung von gespeicherten Abfrageergebnissen .....	346
Führen Sie CloudTrail Lake-Abfragen aus und verwalten Sie sie mit dem AWS CLI .....	361
CloudTrail Lake-SQL-Einschränkungen .....	366
Unterstützte Funktionen, Bedingungs- und Verknüpfungsoperatoren .....	367
Erweiterte Unterstützung für Abfragen in mehreren Tabellen .....	368
Unterstützte SQL-Schemas für Ereignisdatenspeicher .....	369

Unterstütztes Schema für CloudTrail Ereignisdatensatzfelder .....	369
Unterstütztes Schema für CloudTrail Insights-Ereignisdatensatzfelder .....	373
Unterstütztes Schema für Datensatzfelder für Konfigurationselemente von AWS Config .....	375
Unterstütztes Schema für AWS Audit Manager Nachweisdatensatzfelder .....	376
Unterstütztes Schema für Felder ohne AWS Ereignisse .....	377
Steuern der Benutzerberechtigungen .....	379
Verwaltung der CloudTrail Seekosten .....	379
Preisoptionen für den Ereignisdatenspeicher .....	380
Die Gebühren von CloudTrail Lake verstehen .....	381
Empfehlungen, wie Sie Kosten senken können .....	383
Tools zur Kostenverwaltung .....	385
Weitere Informationen finden Sie auch unter .....	387
Unterstützte CloudWatch Metriken .....	387
Mit CloudTrail Trails arbeiten .....	391
Erstellen Sie einen Trail für Ihren AWS-Konto .....	392
Erstellen und Aktualisieren eines Trails mit der Konsole .....	393
Trails erstellen, aktualisieren und verwalten mit dem AWS CLI .....	442
Erstellen eines Trails für eine Organisation .....	474
Umstellung von Protokollen für Mitgliedskonten auf Organisationstrails .....	479
Vorbereiten der Erstellung eines Trails für Ihre Organisation .....	480
Vorbereiten der Erstellung eines Trails für Ihre Organisation in der Konsole .....	484
Erstellen eines Trails für eine Organisation mit dem AWS Command Line Interface .....	503
Fehlerbehebung .....	510
CloudTrail Insights-Ereignisse für Wanderwege anzeigen .....	513
CloudTrail Insights-Ereignisse für Trails in der CloudTrail Konsole anzeigen .....	514
CloudTrail Insights-Ereignisse für Trails anzeigen mit dem AWS CLI .....	525
Trailereignisse nach CloudTrail Lake kopieren .....	536
Überlegungen zum Kopieren von Trail-Ereignissen .....	538
Erforderliche Berechtigungen zum Kopieren von Trail-Ereignissen .....	540
Kopieren Sie Trail-Ereignisse mithilfe der Konsole in einen vorhandenen Ereignisdatenspeicher CloudTrail .....	545
CloudTrail Logdateien abrufen und einsehen .....	548
Finden Sie Ihre Protokolldateien CloudTrail .....	548
Deine CloudTrail Logdateien herunterladen .....	550
Konfiguration von Amazon SNS SNS-Benachrichtigungen für CloudTrail .....	552
Konfiguration für CloudTrail das Senden von Benachrichtigungen .....	552

Tipps zum Verwalten von Trails .....	554
Verwaltung der CloudTrail Trailkosten .....	555
Benennungsanforderungen .....	558
Erstellen von mehreren Trails .....	560
Steuern der Benutzerberechtigungen .....	562
Unterstützte VPC-Endpunkte .....	563
Verfügbarkeit .....	563
Erstellen Sie einen VPC-Endpunkt für CloudTrail .....	564
Gemeinsam genutzte Subnetze .....	565
AWS-Konto Sperrung und Wege .....	565
CloudTrail Einstellungen konfigurieren .....	567
Delegierte Administratoren einer Organisation .....	567
Erforderliche Berechtigungen zum Zuweisen delegierter Administratoren .....	571
Fügen Sie einen delegierten Administrator hinzu CloudTrail .....	572
Entfernen Sie einen CloudTrail delegierten Administrator .....	573
Serviceverknüpfte Kanäle .....	573
Anzeigen von serviceverknüpften Kanälen mithilfe der Konsole .....	574
Anzeigen von mit Diensten verknüpften Kanälen mithilfe der AWS CLI .....	575
CloudTrail Ereignisse verstehen .....	578
Verwaltungsereignisse .....	578
Datenereignisse .....	581
Einblicke und Ereignisse .....	599
Verwaltungsereignisse .....	602
Verwaltungsereignisse .....	603
Lesen und Schreiben von Ereignissen .....	605
Protokollieren von Ereignissen mit der AWS Command Line Interface .....	606
Protokollieren von Ereignissen mit AWS -SDKs .....	617
Ereignisse an Amazon CloudWatch Logs senden .....	617
Datenereignisse .....	618
Datenereignisse .....	620
Schreibgeschützte Ereignisse und Nur-Schreiben-Ereignisse .....	639
Protokollierung von Datenereignissen mit dem AWS Management Console .....	640
Protokollieren von Datenereignissen mit dem AWS Command Line Interface .....	667
Filtern von Datenereignissen mithilfe erweiterter Ereigniselektoren .....	679
Protokollieren von Datenereignissen für AWS Config -Compliance .....	701
Protokollieren von Datenereignissen mit den SDKs AWS .....	702

Ereignisse an Amazon CloudWatch Logs senden .....	702
Insights-Veranstaltungen .....	703
Grundlegendes zur Insights-Ereignisbereitstellung .....	704
Protokollieren von Insights-Ereignissen mit dem AWS Management Console .....	705
Protokollieren von Insights-Ereignissen mit dem AWS Command Line Interface .....	707
Ereignisse mit den AWS SDKs protokollieren .....	713
Zusätzliche Informationen für Trails .....	713
CloudTrail Inhalt aufzeichnen .....	721
Datensatzfelder von Insights-Ereignissen .....	733
Beispiel für die sharedEventID .....	734
CloudTrail Element „userIdentity“ .....	735
Beispiele .....	736
Felder .....	737
Werte für AWS STS APIs mit SAML und Web-Identitätsverbund .....	745
AWS STS Quellidentität .....	747
Insights-InsightsDetails-Element .....	750
Beispiel-insightDetails-Block .....	757
Nicht-API-Ereignisse, erfasst von CloudTrail .....	759
AWS Serviceereignisse .....	759
AWS Management Console Anmeldeereignisse .....	760
CloudTrail Protokolldateien .....	776
Empfangen von CloudTrail Protokolldateien aus mehreren Regionen .....	778
Verwalten der Datenkonsistenz .....	779
Überwachung von CloudTrail Protokolldateien mit Amazon CloudWatch Logs .....	780
Ereignisse an CloudWatch Logs senden .....	781
CloudWatch Alarme für CloudTrail Ereignisse erstellen: Beispiele .....	790
Das Senden CloudTrail von Ereignissen an CloudWatch Logs beenden .....	798
CloudWatch Benennung von Protokollgruppen und Protokollströmen für CloudTrail ....	799
Rollenrichtlinien-Dokument CloudTrail zur Verwendung von CloudWatch Logs zur Überwachung .....	800
Empfangen von CloudTrail Protokolldateien von mehreren Konten .....	802
Redigieren von Bucket-Eigentümer-Konto-IDs für Datenereignisse, die von anderen Konten aufgerufen werden .....	803
Festlegen der Bucket-Richtlinie für mehrere Konten .....	804
Erstellen von Trails in zusätzlichen Konten .....	806
CloudTrail Protokolldateien zwischen AWS Konten teilen .....	809



Freigeben von Protokolldateien zwischen Konten durch Annehmen einer Rolle .....	809
Überprüfen der Integrität der CloudTrail Protokolldatei .....	820
Warum sollten Sie diese Funktion nutzen? .....	820
Funktionsweise .....	820
Aktivierung der Integritätsprüfung der Protokolldatei für CloudTrail .....	821
Überprüfen der Integrität der CloudTrail Protokolldatei mit dem AWS CLI .....	822
CloudTrail Struktur der Digest-Datei .....	831
Benutzerdefinierte Implementierungen der CloudTrail Integritätsprüfung von Protokolldateien .....	839
CloudTrail Beispiele für Protokolldateien .....	851
CloudTrail Format des Protokolldateinamens .....	852
Beispiele für Protokolldateien .....	852
Verwendung der CloudTrail Processing Library .....	865
Mindestanforderungen .....	866
Protokolle werden verarbeitet CloudTrail .....	866
Erweiterte Themen .....	873
Weitere Ressourcen .....	879
Sicherheit .....	880
Datenschutz .....	881
Identitäts- und Zugriffsverwaltung .....	882
Zielgruppe .....	883
Authentifizierung mit Identitäten .....	884
Verwalten des Zugriffs mit Richtlinien .....	888
Wie AWS CloudTrail funktioniert mit IAM .....	890
Beispiele für identitätsbasierte Richtlinien .....	900
Beispiele für eine ressourcenbasierte Richtlinie .....	917
Amazon S3 S3-Bucket-Richtlinie für CloudTrail .....	920
Amazon S3 S3-Bucket-Richtlinie für CloudTrail Lake-Abfrageergebnisse .....	928
Amazon SNS SNS-Themenrichtlinie für CloudTrail .....	931
Fehlerbehebung .....	939
Verwenden von serviceverknüpften Rollen .....	943
AWS verwaltete Richtlinien .....	946
Compliance-Validierung .....	949
Ausfallsicherheit .....	950
Sicherheit der Infrastruktur .....	951
Serviceübergreifende Confused-Deputy-Prävention .....	952

---

Bewährte Methoden für die Gewährleistung der Sicherheit .....	953
CloudTrail Bewährte Methoden zur Detektivsicherheit .....	953
CloudTrail Bewährte Methoden zur präventiven Sicherheit .....	956
CloudTrail Logdateien mit AWS KMS Schlüsseln verschlüsseln (SSE-KMS) .....	960
Aktivieren der Verschlüsselung von Protokolldateien .....	962
Erteilen der Berechtigung zum Erstellen eines KMS-Schlüssels .....	963
Konfigurieren Sie AWS KMS wichtige Richtlinien für CloudTrail .....	964
Aktualisieren einer Ressource zur Verwendung des KMS-Schlüssels .....	979
Aktivieren und Deaktivieren der CloudTrail Protokolldateiverschlüsselung mit dem AWS CLI .....	984
Dokumentverlauf .....	989
Frühere Aktualisierungen .....	1042
AWS-Glossar .....	1064
.....	mlxv

# Was ist AWS CloudTrail?

AWS CloudTrail ist ein Programm AWS-Service , das Ihnen dabei hilft, die Betriebs- und Risikoprüfung, Unternehmensführung und Einhaltung Ihrer Vorschriften zu ermöglichen AWS-Konto. Von einem Benutzer, einer Rolle oder einem AWS Dienst ausgeführte Aktionen werden als Ereignisse in aufgezeichnet CloudTrail. Zu den Ereignissen gehören Aktionen AWS Management Console AWS Command Line Interface, die in den AWS SDKs und APIs ausgeführt wurden.

CloudTrail ist in deinem aktiv, AWS-Konto wenn du es erstellst. Wenn in Ihrem eine Aktivität stattfindet AWS-Konto, wird diese Aktivität in einem CloudTrail Ereignis aufgezeichnet.

CloudTrail bietet drei Möglichkeiten, Ereignisse aufzuzeichnen:

- Ereignisverlauf – Der Ereignisverlauf stellt eine anzeigbare, durchsuchbare, herunterladbare und unveränderliche Aufzeichnung der Verwaltungsereignisse der letzten 90 Tage in einer AWS-Region bereit. Sie können nach Ereignissen suchen, indem Sie nach einem einzelnen Attribut filtern. Sie haben automatisch Zugriff auf den Eventverlauf, wenn Sie Ihr Konto erstellen. Weitere Informationen finden Sie unter [Mit dem CloudTrail Eventverlauf arbeiten](#).

Für die Anzeige des Eventverlaufs CloudTrail fallen keine Gebühren an.

- CloudTrail Lake — [AWS CloudTrail Lake](#) ist ein verwalteter Data Lake zum Erfassen, Speichern, Zugreifen und Analysieren von Benutzer- und API-Aktivitäten zu AWS Prüf- und Sicherheitszwecken. CloudTrail Lake konvertiert bestehende Ereignisse im zeilenbasierten JSON-Format in das [Apache ORC-Format](#). ORC ist ein spaltenförmiges Speicherformat, das für den schnellen Abruf von Daten optimiert ist. Die Ereignisse werden in Ereignisdatenspeichern zusammengefasst, bei denen es sich um unveränderliche Sammlungen von Ereignissen handelt, die auf Kriterien basieren, die Sie mit Hilfe von erweiterten Ereignisselektoren auswählen. Sie können die Ereignisdaten bis zu 3 653 Tage (etwa 10 Jahre) in einem Ereignisdatenspeicher speichern, wenn Sie sich für die Preisoption mit verlängerbarer Aufbewahrung von einem Jahr entscheiden, oder bis zu 2 557 Tage (etwa 7 Jahre), wenn Sie sich für die Preisoption mit siebenjähriger Aufbewahrung entscheiden. Sie können einen Ereignisdatenspeicher für ein einzelnes AWS-Konto oder für mehrere AWS-Konten Ereignisse erstellen, indem Sie. AWS Organizations Sie können alle vorhandenen CloudTrail Protokolle aus Ihren S3-Buckets in einen vorhandenen oder neuen Ereignisdatenspeicher importieren. Mit [Lake-Dashboards](#) können Sie auch die wichtigsten CloudTrail Veranstaltungstrends visualisieren. Weitere Informationen finden Sie unter [Mit AWS CloudTrail Lake arbeiten](#).

CloudTrail Für die Speicherung und Abfrage von Daten zu Ereignissen in Lake fallen Gebühren an. Beim Erstellen eines Ereignisdatenspeichers wählen Sie die [Preisoption](#) aus, die für den Ereignisdatenspeicher genutzt werden soll. Die Preisoption bestimmt die Kosten für die Erfassung und Speicherung von Ereignissen sowie die standardmäßige und maximale Aufbewahrungsdauer für den Ereignisdatenspeicher. Wenn Sie Abfragen in Lake ausführen, zahlen Sie auf der Grundlage der Menge der gescannten Daten. Informationen zur CloudTrail Preisgestaltung und Verwaltung der Lake-Kosten finden Sie unter [AWS CloudTrail Preise](#) und [Verwaltung der CloudTrail Seekosten](#).

- Trails — Trails zeichnet AWS Aktivitäten auf und übermittelt und speichert diese Ereignisse in einem Amazon S3 S3-Bucket, mit optionaler Übermittlung an [CloudWatch Logs](#) und [Amazon EventBridge](#). Sie können diese Ereignisse in Ihre Sicherheitsüberwachungslösungen eingeben. Sie können auch Ihre eigenen Lösungen von Drittanbietern oder Lösungen wie Amazon Athena verwenden, um Ihre CloudTrail Protokolle zu durchsuchen und zu analysieren. Sie können Trails für einen AWS-Konto oder für mehrere erstellen, AWS-Konten indem Sie AWS Organizations. Sie können [Insights-Ereignisse protokollieren](#), um Ihre Verwaltungsereignisse auf ungewöhnliches Verhalten bei API-Aufrufvolumen und Fehlerraten zu analysieren. Weitere Informationen finden Sie unter [Erstellen Sie einen Trail für Ihren AWS-Konto](#).

Sie können eine Kopie Ihrer laufenden Verwaltungsereignisse kostenlos an Ihren S3-Bucket senden, CloudTrail indem Sie einen Trail erstellen. Es fallen jedoch Amazon S3 S3-Speichergebühren an. Weitere Informationen zur CloudTrail Preisgestaltung finden Sie unter [AWS CloudTrail Preise](#). Informationen zu Amazon-S3-Preisen finden Sie unter [Amazon S3-Preise](#).

Der Einblick in Ihre AWS Kontoaktivitäten ist ein wichtiger Aspekt von Best Practices für Sicherheit und Betrieb. Sie können CloudTrail damit Kontoaktivitäten in Ihrer gesamten AWS Infrastruktur anzeigen, suchen, herunterladen, archivieren, analysieren und darauf reagieren. Sie können ermitteln, wer oder was welche Maßnahme ergriffen hat, auf welche Ressourcen eingewirkt wurde, wann das Ereignis eingetreten ist und weitere Informationen, die Ihnen helfen, Aktivitäten in Ihrem AWS Konto zu analysieren und darauf zu reagieren.

Sie können die API CloudTrail in Anwendungen integrieren, die Erstellung von Trail- oder Event-Datenspeichern für Ihr Unternehmen automatisieren, den Status von Ereignisdatenspeichern und von Ihnen erstellten Pfaden überprüfen und kontrollieren, wie Benutzer CloudTrail Ereignisse betrachten.

# Zugreifen CloudTrail

Sie können auf eine CloudTrail der folgenden Arten damit arbeiten.

Themen

- [CloudTrail Konsole](#)
- [AWS CLI](#)
- [CloudTrail APIs](#)
- [AWS SDKs](#)

## CloudTrail Konsole

Melden Sie sich bei der an AWS Management Console und öffnen Sie die CloudTrail Konsole unter <https://console.aws.amazon.com/cloudtrail/>.

Die CloudTrail Konsole bietet eine Benutzeroberfläche für die Ausführung vieler CloudTrail Aufgaben, wie z. B.:

- Aktuelle Ereignisse und den Ereignisverlauf für Ihr AWS Konto anzeigen.
- Eine gefilterte oder vollständige Datei mit Verwaltungsereignissen der letzten 90 Tage wird aus dem Eventverlauf heruntergeladen.
- CloudTrail Trails erstellen und bearbeiten.
- Datenspeicher für Ereignisse in CloudTrail Lake erstellen und bearbeiten.
- Abfragen auf Ereignisdatenspeichern ausführen.
- Konfiguration von CloudTrail Pfaden, einschließlich:
  - Auswahl eines Amazon-S3-Buckets für Trails.
  - Einrichten eines Präfix.
  - Konfiguration der Übermittlung an CloudWatch Logs.
  - Verwendung von AWS KMS Schlüsseln zur Verschlüsselung von Trail-Daten.
  - Aktivierung von Amazon-SNS-Benachrichtigungen für die Übermittlung von Protokolldateien von Trails.
  - Hinzufügen und Verwalten von Tags für Ihre Trails.
- Konfiguration von CloudTrail Lake-Ereignisdatenspeichern, einschließlich:

- Integration von Ereignisdatenspeichern mit CloudTrail Partnern oder mit Ihren eigenen Anwendungen, um Ereignisse aus Quellen außerhalb von zu protokollieren AWS.
- Zusammenführung von Ereignisdatenspeichern zur Ausführung von Abfragen von Amazon Athena.
- Verwendung von AWS KMS Schlüsseln zur Verschlüsselung von Daten aus dem Ereignisdatenspeicher.
- Hinzufügen und Verwalten von Tags für Ihre Ereignisdatenspeicher.

Weitere Hinweise zu dem finden AWS Management Console Sie unter [AWS Management Console](#).

## AWS CLI

Das AWS Command Line Interface ist ein einheitliches Tool, mit dem Sie CloudTrail von der Befehlszeile aus interagieren können. Weitere Informationen finden Sie im [AWS Command Line Interface -Benutzerhandbuch](#). Eine vollständige Liste der CloudTrail CLI-Befehle finden Sie unter [cloudtrail und cloudtrail-data](#) in der Befehlsreferenz.AWS CLI

## CloudTrail APIs

Neben der Konsole und der CLI können Sie auch die CloudTrail RESTful-APIs verwenden, um CloudTrail direkt zu programmieren. Weitere Informationen finden Sie in der [AWS CloudTrail API-Referenz](#) und der [CloudTrail-Data-API-Referenz](#).

## AWS SDKs

Als Alternative zur Verwendung der CloudTrail API können Sie eines der AWS SDKs verwenden. Jedes SDK enthält Bibliotheken und Beispiel-Code für verschiedene Programmiersprachen und Plattformen. Die SDKs bieten eine bequeme Möglichkeit, programmatischen Zugriff auf zu erstellen. CloudTrail Sie können beispielsweise die SDKs verwenden, um Anforderungen kryptografisch zu signieren, Fehler zu verwalten und Anforderungen automatisch zu wiederholen. Weitere Informationen finden Sie auf der Seite [Tools to Build on AWS](#).

## Wie CloudTrail funktioniert

Sie haben automatisch Zugriff auf den CloudTrail Eventverlauf, wenn Sie Ihren erstellen AWS-Konto. Der Ereignisverlauf stellt eine anzeigbare, durchsuchbare, herunterladbare und unveränderliche Aufzeichnung der Verwaltungsereignisse der letzten 90 Tage in einer AWS-Region bereit.

Für eine fortlaufende Aufzeichnung der Ereignisse in AWS-Konto den letzten 90 Tagen erstellen Sie einen Trail- oder CloudTrail Lake-Event-Datenspeicher.

## Themen

- [CloudTrail Verlauf der Ereignisse](#)
- [CloudTrail Datenspeicher für Seen und Ereignisse](#)
- [CloudTrail Wanderwege](#)
- [CloudTrail Einblicke und Ereignisse](#)
- [CloudTrail Kanäle](#)

## CloudTrail Verlauf der Ereignisse

Sie können die Verwaltungsereignisse der letzten 90 Tage ganz einfach in der CloudTrail Konsole einsehen, indem Sie die Seite mit dem Ereignisverlauf aufrufen. Sie können den Ereignisverlauf auch anzeigen, indem Sie den Befehl [aws cloudtrail lookup-events](#) oder den [LookupEvents](#)-API-Vorgang ausführen. Sie können im Ereignisverlauf nach Ereignissen suchen, indem Sie nach Ereignissen für ein einzelnes Attribut filtern. Weitere Informationen finden Sie unter [Mit dem CloudTrail Eventverlauf arbeiten](#).

Der Ereignisverlauf ist nicht mit irgendwelchen Trails oder Ereignisdatenspeichern verknüpft, die in deinem Konto vorhanden sind, und wird auch nicht von Konfigurationsänderungen beeinflusst, die du an deinen Trails oder Ereignisdatenspeichern vornimmst.

Für das Anzeigen der Seite mit dem Ereignisverlauf oder das Ausführen des `lookup-events` Befehls CloudTrail fallen keine Gebühren an.

## CloudTrail Datenspeicher für Seen und Ereignisse

Sie können einen Ereignisdatenspeicher erstellen, um [CloudTrail Ereignisse](#) (Verwaltungsereignisse, Datenereignisse), [CloudTrailInsights-Ereignisse](#), [AWS Audit Manager Beweise](#), [AWS Config Konfigurationselemente](#) oder [Ereignisse außerhalb von](#) zu protokollieren AWS.

In Ereignisdatenspeichern können Ereignisse aus dem aktuellen AWS-Region Konto oder aus allen Ereignissen AWS-Regionen in Ihrem AWS Konto protokolliert werden. Ereignisdatenspeicher, die Sie verwenden, um Integrationsereignisse von außerhalb zu protokollieren, AWS dürfen nur für eine einzelne Region bestimmt sein. Es kann sich nicht um Ereignisdatenspeicher mit mehreren Regionen handeln.

Wenn Sie eine Organisation in erstellt haben AWS Organizations, können Sie einen Datenspeicher für Organisationsereignisse erstellen, der alle Ereignisse für alle AWS Konten in dieser Organisation protokolliert. Organisations-Ereignisdatspeicher können für alle AWS -Regionen oder die aktuelle Region gelten. Organisations-Ereignisdatspeicher müssen im Verwaltungskonto oder im Konto eines delegierten Administrators erstellt werden. Sobald sie auf eine Organisation angewendet werden, gelten sie automatisch auch für alle Mitgliedskonten in der Organisation. Mitgliedskonten können den Organisations-Ereignisdatspeicher sehen, diesen aber weder ändern noch löschen. Datenspeicher für Organisationsereignisse können nicht zum Sammeln von Ereignissen von außerhalb von verwendet werden AWS. Weitere Informationen finden Sie unter [Ereignisdatspeicher einer Organisation](#).

Standardmäßig werden alle Ereignisse in einem Ereignisdatspeicher von verschlüsselt CloudTrail. Wenn Sie einen Ereignisdatspeicher konfigurieren, können Sie wählen, ob Sie Ihren eigenen verwenden möchten AWS KMS key. Wenn Sie Ihren eigenen KMS-Schlüssel verwenden, fallen AWS KMS Kosten für die Verschlüsselung und Entschlüsselung an. Nachdem Sie einen KMS-Schlüssel einem Ereignisdatspeicher zugeordnet haben, kann der KMS-Schlüssel nicht entfernt oder geändert werden. Weitere Informationen finden Sie unter [CloudTrail Logdateien mit AWS KMS Schlüsseln verschlüsseln \(SSE-KMS\)](#).

Die folgende Tabelle enthält Informationen zu Aufgaben, die Sie mit Ereignisdatspeichern ausführen können.

Aufgabe	Beschreibung
<a href="#">Lake-Dashboards anzeigen</a>	Sie können CloudTrail Lake-Dashboards verwenden, um die Ereignisse in Ereignisdatspeichern zu visualisieren, in denen Verwaltungsereignisse, S3-Datenereignisse oder Insights-Ereignisse erfasst werden.
<a href="#">Protokollieren Sie Verwaltungseignisse</a>	Konfigurieren Sie Ihren Ereignisdatspeicher so, dass er schreibgeschützte, schreibgeschützte oder alle Verwaltungseignisse protokolliert. Standardmäßig protokollieren Ereignisdaten Verwaltungsereignisse.
<a href="#">Datenereignisse protokollieren</a>	Konfigurieren Sie Ihren Ereignisdatspeicher so, dass Datenereignisse protokolliert werden. Sie können erweiterte Event-Selektoren verwenden, um nach den <code>resources.ARN</code>



Aufgabe	Beschreibung
	<p>Feldern, und zu filtern <code>eventName readOnly</code>, sodass nur die Ereignisse protokolliert werden, die für Sie von Interesse sind.</p>
<a href="#">Loggen Sie Insights-Ereignisse</a>	<p>Konfigurieren Sie Ihre Ereignisdatenspeicher für die Protokollierung von Insights-Ereignissen, damit Sie ungewöhnliche Aktivitäten, die mit Aufrufen der Verwaltungs-API verbunden sind, identifizieren und darauf reagieren können. Weitere Informationen finden Sie unter <a href="#">Protokollieren von Insights-Ereignissen</a>.</p> <p>Für Insights-Ereignisse fallen zusätzliche Gebühren an. Wenn Sie Insights sowohl für Trails als auch für Ereignisdatenspeicher aktivieren, wird Ihnen eine separate Gebühr in Rechnung gestellt. Weitere Informationen finden Sie unter <a href="#">AWS CloudTrail-Preisgestaltung</a>.</p>
<a href="#">Trail-Ereignisse kopieren</a>	<p>Sie können Trail-Ereignisse in einen <a href="#">neuen</a> oder <a href="#">vorhandenen</a> Ereignisdatenspeicher kopieren, um eine point-in-time Momentaufnahme der im Trail protokollierten Ereignisse zu erstellen.</p>
<a href="#">Aktivieren Sie den Verbund für einen Ereignisdatenspeicher</a>	<p>Sie können einen Ereignisdatenspeicher verbinden, um die mit dem Ereignisdatenspeicher verknüpften Metadaten im AWS Glue <a href="#">Datenkatalog</a> zu sehen und mithilfe von Amazon Athena SQL-Abfragen für die Ereignisdaten ausführen. Anhand der im AWS Glue Datenkatalog gespeicherten Tabellenmetadaten weiß die Athena-Abfrage-Engine, wie die Daten, die Sie abfragen möchten, gesucht, gelesen und verarbeitet werden.</p>
<a href="#">Stoppen oder starten Sie die Erfassung von Ereignissen in einem Ereignisdatenspeicher</a>	<p>Sie können die Erfassung von Ereignissen in Ereignisdatenspeichern, in denen CloudTrail Verwaltungs- und Datenereignisse oder Konfigurationselemente erfasst werden, beenden und starten. AWS Config</p>

Aufgabe	Beschreibung
<a href="#">Erstellen Sie eine Integration mit einer Ereignisquelle außerhalb von AWS</a>	<p>Sie können CloudTrail Lake-Integrationen verwenden, um Benutzeraktivitätsdaten von außerhalb zu protokollieren und zu speichern AWS; aus beliebigen Quellen in Ihren Hybridumgebungen, z. B. internen oder SaaS-Anwendungen, die vor Ort oder in der Cloud gehostet werden, virtuellen Maschinen oder Containern. Informationen zu verfügbaren Integrationspartnern finden Sie unter <a href="#">AWS CloudTrail Lake-Integrationen</a>.</p>
<a href="#">Sehen Sie sich die Lake-Beispielabfragen in der Konsole an CloudTrail</a>	<p>Die CloudTrail Konsole bietet eine Reihe von Beispielabfragen, die Ihnen den Einstieg in das Schreiben eigener Abfragen erleichtern können.</p>
<a href="#">Erstellen oder bearbeiten Sie eine Abfrage</a>	<p>Abfragen in CloudTrail werden in SQL verfasst. Sie können eine Abfrage auf der Registerkarte CloudTrail Lake Editor erstellen, indem Sie die Abfrage von Grund auf in SQL schreiben oder indem Sie eine gespeicherte Abfrage oder eine Beispielabfrage öffnen und bearbeiten.</p>
<a href="#">Speichern Sie die Abfrageergebnisse in einem S3-Bucket</a>	<p>Wenn Sie eine Abfrage ausführen, können Sie die Abfrageergebnisse in einem S3-Bucket speichern.</p>
<a href="#">Laden Sie gespeicherte Abfrageergebnisse herunter</a>	<p>Sie können eine CSV-Datei mit Ihren gespeicherten CloudTrail Lake-Abfrageergebnissen herunterladen.</p>
<a href="#">Überprüfen Sie die gespeicherten Abfrageergebnisse</a>	<p>Mithilfe der Integritätsprüfung von CloudTrail Abfrageergebnissen können Sie feststellen, ob die Abfrageergebnisse nach der Übermittlung der Abfrageergebnisse CloudTrail an den S3-Bucket geändert, gelöscht oder unverändert wurden.</p>

Weitere Informationen zu CloudTrail Lake finden Sie unter [Mit AWS CloudTrail Lake arbeiten](#).

CloudTrail Für Datenspeicher und Abfragen von Ereignissen in Lake fallen Gebühren an. Beim Erstellen eines Ereignisdatenspeichers wählen Sie die [Preisoption](#) aus, die für den Ereignisdatenspeicher genutzt werden soll. Die Preisoption bestimmt die Kosten für die Erfassung und Speicherung von Ereignissen sowie die standardmäßige und maximale Aufbewahrungsdauer für den Ereignisdatenspeicher. Wenn Sie Abfragen in Lake ausführen, zahlen Sie auf der Grundlage

der Menge der gescannten Daten. Informationen zur CloudTrail Preisgestaltung und Verwaltung der Lake-Kosten finden Sie unter [AWS CloudTrail Preise](#) und [Verwaltung der CloudTrail Seekosten](#).

## CloudTrail Wanderwege

Ein Trail ist eine Konfiguration, durch die Ereignisse an den von Ihnen angegebenen Amazon-S3-Bucket übermittelt werden. [Mit Amazon CloudWatch Logs und Amazon können Sie Ereignisse auch in einem Trail bereitstellen und analysieren EventBridge](#).

Trails können CloudTrail Verwaltungsereignisse, Datenereignisse und Insights-Ereignisse protokollieren.

Sie können zwei Arten von Wanderwegen für einen erstellen AWS-Konto: Wanderwege mit mehreren Regionen und Wanderwege mit nur einer Region.

### Wanderwege mit mehreren Regionen

Wenn Sie einen Trail mit mehreren Regionen erstellen, CloudTrail zeichnet er alle Ereignisse AWS-Regionen in der [AWS Partition](#) auf, in der Sie arbeiten, und übermittelt die CloudTrail Ereignisprotokolldateien an einen von Ihnen angegebenen S3-Bucket. Wenn nach der Erstellung eines Trails mit mehreren Regionen ein hinzugefügt AWS-Region wird, wird diese neue Region automatisch aufgenommen, und Ereignisse in dieser Region werden protokolliert. Das Erstellen eines Trails mit mehreren Regionen wird als bewährte Methode empfohlen, da Sie Aktivitäten in allen Regionen in Ihrem Konto erfassen. Alle Trails, die Sie mit der CloudTrail Konsole erstellen, sind regionsübergreifend. Sie können einen Pfad mit einer einzelnen Region in einen Pfad mit mehreren Regionen konvertieren, indem Sie den verwenden. AWS CLI Weitere Informationen finden Sie unter [Erstellen eines Trails in der Konsole](#) und [Umwandeln eines Trails, der für eine Region gilt, zu einem Trail für alle Regionen](#).

### Wanderwege für eine einzelne Region

Wenn Sie einen Pfad mit nur einer Region erstellen, werden nur die Ereignisse in dieser Region CloudTrail aufgezeichnet. Anschließend werden die CloudTrail Ereignisprotokolldateien an einen von Ihnen angegebenen Amazon S3 S3-Bucket gesendet. Sie können nur einen einzelnen Regions-Trail erstellen, indem Sie die AWS CLI verwenden. Wenn Sie zusätzliche einzelne Trails erstellen, können Sie festlegen, dass diese Trails CloudTrail Ereignisprotokolldateien an denselben S3-Bucket oder an separate Buckets liefern. Dies ist die Standardoption, wenn Sie einen Trail mithilfe der AWS CLI oder der CloudTrail API erstellen. Weitere Informationen finden Sie unter [Trails erstellen, aktualisieren und verwalten mit dem AWS CLI](#).

**Note**

Für beide Arten von Trails können Sie einen Amazon-S3-Bucket aus einer beliebigen Region angeben.

Wenn Sie in eine Organisation erstellt haben AWS Organizations, können Sie einen Organisationspfad erstellen, der alle Ereignisse für alle AWS Konten in dieser Organisation protokolliert. Organisationspfade können für alle AWS Regionen oder für die aktuelle Region gelten. Organisations-Trails müssen im Verwaltungskonto oder mit dem Konto eines delegierten Administrators erstellt werden. Sobald sie auf eine Organisation angewendet werden, gelten sie automatisch auch für alle Mitgliedskonten in der Organisation. Mitgliedskonten können den Organisationspfad sehen, ihn aber nicht ändern oder löschen. Standardmäßig wird Mitgliedskonten kein Zugriff auf die Protokolldateien für den Organisations-Trail im Amazon-S3-Bucket gewährt.

Wenn Sie in der CloudTrail Konsole einen Trail erstellen, werden Ihre Ereignisprotokolldateien standardmäßig mit einem KMS-Schlüssel verschlüsselt. Wenn Sie die SSE-KMS-Verschlüsselung nicht aktivieren möchten, werden Ihre Ereignisprotokolle mit der serverseitigen Verschlüsselung (SSE) von Amazon S3 verschlüsselt. Sie können Ihre Protokolldateien beliebig lange in Ihrem -Bucket speichern. Außerdem können Sie Amazon-S3-Lebenszyklusregeln definieren, um Protokolldateien automatisch zu archivieren oder zu löschen. Wenn Sie über die Protokolldateilieferung und -validierung informiert werden möchten, können Sie Amazon-SNS-Benachrichtigungen einrichten.

CloudTrail veröffentlicht Protokolldateien mehrmals pro Stunde, etwa alle 5 Minuten. Diese Protokolldateien enthalten API-Aufrufe von Diensten im Konto, die dies unterstützen CloudTrail. Weitere Informationen finden Sie unter [CloudTrail unterstützte Dienste und Integrationen](#).

**Note**

CloudTrail übermittelt Protokolle in der Regel innerhalb von durchschnittlich etwa 5 Minuten nach einem API-Aufruf. Diese Zeit ist nicht garantiert. Weitere Informationen finden Sie unter [AWS CloudTrail Service Level Agreement](#).


Wenn Sie Ihren Trail falsch konfigurieren (z. B. wenn der S3-Bucket nicht erreichbar ist), CloudTrail wird versucht, die Protokolldateien 30 Tage lang erneut in Ihren S3-Bucket zu übertragen. Für diese attempted-to-deliver Ereignisse fallen Standardgebühren an. CloudTrail Um Gebühren für einen falsch konfigurierten Trail zu vermeiden, müssen Sie den Trail löschen.


CloudTrail erfasst Aktionen, die direkt vom Benutzer oder im Namen des Benutzers von einem Dienst ausgeführt werden. AWS Beispielsweise kann ein AWS CloudFormation `CreateStack` Aufruf zu zusätzlichen API-Aufrufen an Amazon EC2, Amazon RDS, Amazon EBS oder andere Dienste führen, wie es die AWS CloudFormation Vorlage erfordert. Dieses Verhalten ist normal und wird erwartet. Anhand des `invokedby` Felds im Ereignis können Sie feststellen, ob die Aktion von einem AWS Service ausgeführt wurde. CloudTrail

Die folgende Tabelle enthält Informationen zu Aufgaben, die Sie auf Trails ausführen können.

Aufgabe	Beschreibung
<a href="#">Protokollierung von Verwaltungsereignissen</a>	Konfigurieren Sie Ihre Trails so, dass sie nur Lese-, Schreib- oder alle Verwaltungsereignisse protokollieren.
<a href="#">Datenereignisse protokollieren</a>	Sie können <a href="#">erweiterte Ereignisselektoren verwenden, um detaillierte Selektoren</a> zu erstellen, um nur die Datenereignisse zu protokollieren, die für Sie von Interesse sind. Wenn Sie erweiterte Event-Selektoren verwenden, können Sie nach dem <code>eventName</code> Feld filtern, um die Protokollierung bestimmter API-Aufrufe ein- oder auszuschließen, was zur Kostenkontrolle beitragen kann.
<a href="#">Insights-Ereignisse protokollieren</a>	<p>Konfigurieren Sie Ihre Trails für die Protokollierung von Insights-Ereignissen, damit Sie ungewöhnliche Aktivitäten, die mit Aufrufen der Verwaltungs-API verbunden sind, identifizieren und darauf reagieren können.</p> <p>Für Insights-Ereignisse fallen zusätzliche Gebühren an. Wenn Sie Insights sowohl für Trails als auch für Ereignisdatenspeicher aktivieren, wird Ihnen eine separate Gebühr in Rechnung gestellt. Weitere Informationen</p>

Aufgabe	Beschreibung
	finden Sie unter <a href="#">AWS CloudTrail -Preisgestaltung</a> .
<a href="#">Insights-Ereignisse anzeigen</a>	Nachdem Sie CloudTrail Insights on a trail aktiviert haben, können Sie sich Insights-Ereignisse von bis zu 90 Tagen über die CloudTrail Konsole oder das ansehen AWS CLI.
<a href="#">Laden Sie Insights-Ereignisse herunter</a>	Nachdem Sie CloudTrail Insights on a Trail aktiviert haben, können Sie eine CSV- oder JSON-Datei herunterladen, die Insights-Ereignisse der letzten 90 Tage für Ihren Trail enthält.
<a href="#">Trail-Ereignisse nach CloudTrail Lake kopieren</a>	Sie können vorhandene Trail-Ereignisse in einen CloudTrail Lake Event Data Store kopieren, um eine point-in-time Momentaufnahme der im Trail protokollierten Ereignisse zu erstellen.

Aufgabe	Beschreibung
<a href="#">Ein Amazon SNS SNS-Thema erstellen und abonnieren</a>	<p>Abonnieren Sie ein Thema, um Benachrichtigungen darüber zu erhalten, dass Protokolldateien in Ihrem Bucket bereitgestellt wurden. Amazon SNS kann Sie auf mehrere Arten benachrichtigen, unter anderem programmgesteuert mit Amazon Simple Queue Service.</p> <div data-bbox="829 541 1507 1094" style="border: 1px solid #add8e6; border-radius: 10px; padding: 10px;"><p> <b>Note</b></p><p>Wenn Sie SNS-Benachrichtigungen über Bereitstellungen von Protokolldateien aus allen Regionen erhalten wollen, geben Sie für den Trail nur ein SNS-Thema an. Informationen zur programmgesteuerten Verarbeitung aller Ereignisse finden Sie unter <a href="#">Verwendung der CloudTrail Processing Library</a>.</p></div>
<a href="#">Sehen Sie sich Ihre Protokolldateien an</a>	Suchen Sie nach Ihren Protokolldateien und laden Sie sie aus dem S3-Bucket herunter.

Aufgabe	Beschreibung
<a href="#">Überwachen Sie Ereignisse mit CloudWatch Logs</a>	<p>Sie können Ihren Trail so konfigurieren, dass Ereignisse an CloudWatch Logs gesendet werden. Anschließend können Sie CloudWatch Logs verwenden, um Ihr Konto auf bestimmte API-Aufrufe und Ereignisse hin zu überwachen.</p> <div data-bbox="829 493 1507 951"><p> <b>Note</b></p><p>Wenn Sie einen Trail konfigurieren, der für alle Regionen gilt, sodass Ereignisse an eine CloudWatch Logs-Protokollgruppe CloudTrail gesendet werden, werden Ereignisse aus allen Regionen an eine einzelne Protokollgruppe gesendet.</p></div>
<a href="#">Aktivieren Sie die Protokollverschlüsselung</a>	<p>Die Verschlüsselung von Protokolldateien bietet eine zusätzliche Sicherheitsebene für Ihre Protokolldateien.</p>
<a href="#">Aktivieren Sie die Integrität der Protokolldatei</a>	<p>Mithilfe der Überprüfung der Integrität von Protokolldateien können Sie überprüfen, ob die Protokolldateien seit ihrer Übermittlung CloudTrail unverändert geblieben sind.</p>
<a href="#">Teilen Sie Protokolldateien mit anderen AWS-Konten</a>	<p>Sie können Protokolldateien zwischen Konten teilen.</p>
<a href="#">Sammeln Sie Logs von mehreren Konten</a>	<p>Sie können Protokolldateien aus mehrere Konten in einem einzelnen Bucket zusammenführen.</p>



Aufgabe	Beschreibung
<a href="#">Arbeiten Sie mit Partnerlösungen</a>	Analysieren Sie CloudTrail Ihre Ergebnisse mit einer Partnerlösung, die sich in integrieren lässt CloudTrail. Partnerlösungen bieten eine breite Palette von Funktionen wie die Änderungsnachverfolgung, Problembehebung und Sicherheitsanalyse.

Sie können eine Kopie Ihrer laufenden Verwaltungsereignisse kostenlos an Ihren S3-Bucket senden, CloudTrail indem Sie einen Trail erstellen. Es fallen jedoch Amazon S3 S3-Speichergebühren an. Weitere Informationen zur CloudTrail Preisgestaltung finden Sie unter [AWS CloudTrail Preise](#). Informationen zu Amazon-S3-Preisen finden Sie unter [Amazon S3-Preise](#).

## CloudTrail Einblicke und Ereignisse

AWS CloudTrail Insights helfen AWS Benutzern, ungewöhnliche Aktivitäten im Zusammenhang mit API-Aufrufen und API-Fehlerraten zu identifizieren und darauf zu reagieren, indem CloudTrail Verwaltungsereignisse kontinuierlich analysiert werden. CloudTrail Insights analysiert Ihre normalen Muster des API-Aufrufvolumens und der API-Fehlerraten, die auch als Baseline bezeichnet werden, und generiert Insights-Ereignisse, wenn das Aufrufvolumen oder die Fehlerraten außerhalb der normalen Muster liegen. Insights-Ereignisse zum API-Aufrufvolumen werden für `write`-Verwaltungs-APIs und Insights-Ereignisse zur API-Fehlerrate für `read`- und `write`-Verwaltungs-APIs generiert.

Standardmäßig protokollieren CloudTrail Trails und Event-Datenspeicher keine Insights-Ereignisse. Sie müssen Ihren Trail- oder Event-Datenspeicher so konfigurieren, dass Insights-Ereignisse protokolliert werden. Weitere Informationen finden Sie unter [Protokollieren von Insights-Ereignissen mit dem AWS Management Console](#) und [Protokollieren von Insights-Ereignissen mit dem AWS Command Line Interface](#).

Für Insights-Ereignisse fallen zusätzliche Gebühren an. Wenn Sie Insights sowohl für Trails als auch für Ereignisdatenspeicher aktivieren, wird Ihnen eine separate Gebühr in Rechnung gestellt. Weitere Informationen finden Sie unter [AWS CloudTrail -Preisgestaltung](#).

## Insights-Ereignisse für Trails und Event-Datenspeicher anzeigen

CloudTrail unterstützt Insights-Ereignisse sowohl für Trails als auch für Event-Datenspeicher. Es gibt jedoch einige Unterschiede in der Art und Weise, wie du Insights-Ereignisse ansiehst und darauf zugreifst.

### Anzeigen von Insights-Ereignissen für Trails

Wenn du Insights-Ereignisse für einen Trail aktiviert hast und ungewöhnliche Aktivitäten CloudTrail feststellst, werden Insights-Ereignisse in einem anderen Ordner oder Präfix im Ziel-S3-Bucket für deinen Trail protokolliert. Sie können auch die Art der Insights und den Zeitraum des Vorfalls sehen, wenn Sie Insights-Ereignisse auf der CloudTrail Konsole aufrufen. Weitere Informationen finden Sie unter [CloudTrail Insights-Ereignisse für Trails in der CloudTrail Konsole anzeigen](#).

Nachdem Sie CloudTrail Insights zum ersten Mal in einem Trail aktiviert haben, kann es bis zu 36 Stunden dauern, CloudTrail bis das erste Insights-Ereignis angezeigt wird, wenn ungewöhnliche Aktivitäten festgestellt werden.

### Anzeigen von Insights-Ereignissen für Ereignisdatenspeicher

Um Insights-Ereignisse in CloudTrail Lake zu protokollieren, benötigen Sie einen Zielereignisdatenspeicher, der Insights-Ereignisse protokolliert, und einen Quellereignisdatenspeicher, der Insights aktiviert und Verwaltungsereignisse protokolliert. Weitere Informationen finden Sie unter [Erstellen Sie mit der Konsole einen Ereignisdatenspeicher für CloudTrail Insights-Ereignisse](#).

Nachdem Sie CloudTrail Insights zum ersten Mal im Quell-Ereignisdatenspeicher aktiviert haben, kann es bis zu 7 Tage dauern, CloudTrail bis das erste Insights-Ereignis an den Zielereignisdatenspeicher übermittelt wird, falls ungewöhnliche Aktivitäten festgestellt werden.

Wenn Sie CloudTrail Insights in einem Quell-Eventdatenspeicher aktiviert haben und ungewöhnliche Aktivitäten CloudTrail erkannt werden, CloudTrail werden Insights-Ereignisse an Ihren Zielereignisdatenspeicher übermittelt. Anschließend können Sie Ihren Zielereignisdatenspeicher abfragen, um Informationen zu Ihren Insights-Ereignissen zu erhalten, und die Abfrageergebnisse optional in einem S3-Bucket speichern. Weitere Informationen finden Sie unter [Abfrage erstellen oder bearbeiten](#) und [Sehen Sie sich Beispielabfragen in der CloudTrail Konsole an](#).

Sie können das Insights-Events-Dashboard aufrufen, um die Insights-Ereignisse in Ihrem Zielereignisdatenspeicher zu visualisieren. Weitere Informationen zu Lake-Dashboards finden Sie unter [CloudTrail Lake-Dashboards anzeigen](#).

## CloudTrail Kanäle

CloudTrail unterstützt zwei Arten von Kanälen:

### Kanäle für CloudTrail Lake-Integrationen mit Eventquellen außerhalb von AWS

CloudTrail Lake verwendet Kanäle, um Ereignisse von außerhalb von CloudTrail Lake AWS zu übertragen, und zwar von externen Partnern, die mit Ihnen zusammenarbeiten CloudTrail, oder aus Ihren eigenen Quellen. Wenn Sie einen Kanal erstellen, wählen Sie einen oder mehrere Ereignisdatenspeicher aus, um Ereignisse zu speichern, die von der Kanalquelle stammen. Sie können die Zielereignisdatenspeicher für einen Kanal nach Bedarf ändern, sofern die Zielereignisdatenspeicher so eingestellt sind, dass sie Ereignisse protokollieren. Wenn Sie einen Kanal für Ereignisse eines externen Partners erstellen, stellen Sie dem Partner oder der Quellanwendung einen Kanal-ARN zur Verfügung. Die dem Kanal beigefügte Ressourcenrichtlinie ermöglicht es der Quelle, Ereignisse über den Kanal zu übertragen. Weitere Informationen finden Sie unter [Erstellen Sie eine Integration mit einer Ereignisquelle außerhalb von AWS](#) und [CreateChannel](#) in der AWS CloudTrail -API-Referenz.

### Serviceverknüpfte Kanäle

AWS Dienste können einen mit Diensten verknüpften Kanal einrichten, über den CloudTrail Ereignisse in Ihrem Namen empfangen werden. Der AWS Dienst, der den serviceverknüpften Kanal erstellt, konfiguriert erweiterte Ereignisauswahlmöglichkeiten für den Kanal und gibt an, ob der Kanal für alle Regionen oder für die aktuelle Region gilt.

Sie können die [CloudTrail Konsole](#) oder [AWS CLI](#) zum Anzeigen von Informationen über alle CloudTrail dienstverknüpften Kanäle verwenden, die von erstellt wurden. AWS-Services

## CloudTrail Konzepte

In diesem Abschnitt werden grundlegende Konzepte zusammengefasst, die sich auf CloudTrail.

Konzepte:

- [CloudTrail Ereignisse](#)
- [Ereignisverlauf](#)
- [Trails](#)
- [Organisatorische Pfade](#)
- [CloudTrail Datenspeicher für Seen und Ereignisse](#)

- [CloudTrail Einblicke](#)
- [Tags](#)
- [AWS Security Token Service und CloudTrail](#)
- [Informationen zu globalen Serviceereignissen](#)

## CloudTrail Ereignisse

Ein Ereignis in CloudTrail ist die Aufzeichnung einer Aktivität in einem AWS Konto. Bei dieser Aktivität kann es sich um eine Aktion handeln, die von einer IAM-Identität oder einem Dienst ausgeführt wird, der überwacht werden kann. CloudTrail CloudTrailEreignisse bieten einen Verlauf der API- und Nicht-API-Kontoaktivitäten AWS Management Console, die über die AWS SDKs, Befehlszeilentools und andere Dienste durchgeführt wurden. AWS

CloudTrail Protokolldateien sind kein geordneter Stack-Trace der öffentlichen API-Aufrufe, sodass Ereignisse nicht in einer bestimmten Reihenfolge angezeigt werden.

CloudTrail protokolliert drei Arten von Ereignissen:

- [Verwaltungsereignisse](#)
- [Datenereignisse](#)
- [Insights-Ereignisse](#)

Alle Ereignistypen verwenden ein CloudTrail JSON-Protokollformat.

Standardmäßig protokollieren Trails und Ereignisdatenspeicher Verwaltungsereignisse, aber keine Daten- oder Insights-Ereignisse.

Informationen zur AWS-Services Integration mit finden Sie CloudTrail unter [AWS Servicethemen für CloudTrail](#).

### Verwaltungsereignisse

Verwaltungsereignisse enthalten Informationen zu Verwaltungsvorgängen, die mit Ressourcen in Ihrem AWS Konto ausgeführt werden. Sie werden auch als Vorgänge auf Steuerebene bezeichnet.

Beispiele für Verwaltungsereignisse:

- Konfiguration der Sicherheit (z. B. AWS Identity and Access Management AttachRolePolicy API-Operationen).

- Registrieren von Geräten (z. B. `CreateDefaultVpc`-API-Operationen von Amazon EC2).
- Konfigurieren von Regeln für die Datenweiterleitung (z. B. `CreateSubnet`-API-Operationen von Amazon EC2).
- Einrichtung der Protokollierung (z. B. `AWS CloudTrail CreateTrail` API-Operationen).

Verwaltungsereignisse können auch andere als API-Ereignisse einschließen, die in Ihrem Konto auftreten. Wenn sich beispielsweise ein Benutzer bei Ihrem Konto CloudTrail anmeldet, wird das `ConsoleLogin` Ereignis protokolliert. Weitere Informationen finden Sie unter [Nicht-API-Ereignisse, erfasst von CloudTrail](#).

In den Ereignisdaten von CloudTrail Trails und CloudTrail Lake werden standardmäßig Verwaltungsereignisse gespeichert. Weitere Informationen zur Protokollierung von Verwaltungsereignissen finden Sie unter [Protokollieren von Verwaltungsereignissen](#).

## Datenereignisse

Datenereignisse liefern Informationen zu Ressourcenoperationen, die für oder innerhalb einer Ressource ausgeführt wurden. Sie werden auch als Vorgänge auf Datenebene bezeichnet. Datenereignisse sind oft Aktivitäten mit hohem Volume.

Beispiele für Datenereignisse:

- [Amazon S3 S3-API-Aktivität auf Objektebene](#) (z. B., `GetObjectDeleteObject`, und `PutObject` API-Operationen) für Objekte in S3-Buckets.
- AWS Lambda Aktivität zur Ausführung von Funktionen (die `Invoke` API).
- CloudTrail `PutAuditEvents` Aktivität auf einem [CloudTrail Lake-Kanal](#), der verwendet wird, um Ereignisse von außen zu protokollieren AWS.
- [Publish](#)- und [PublishBatch](#)-API-Operationen von Amazon SNS zu Themen.

In der folgenden Tabelle sind die Datenereignistypen aufgeführt, die für Trails und Ereignisdatenspeicher verfügbar sind. In der Spalte Datenereignistyp (Konsole) wird die entsprechende Auswahl in der Konsole angezeigt. In der Wertspalte `resources.type` wird der `resources.type` Wert angezeigt, den Sie angeben würden, um Datenereignisse dieses Typs mithilfe der APIs oder in Ihren Trail- oder Event-Datenspeicher aufzunehmen. AWS CLI CloudTrail

Für Trails können Sie einfache oder erweiterte Event-Selektoren verwenden, um Datenereignisse für Amazon S3 S3-Objekte, Lambda-Funktionen und DynamoDB-Tabellen zu protokollieren (in den

ersten drei Zeilen der Tabelle dargestellt). Sie können nur erweiterte Ereignisselectoren verwenden, um die in den verbleibenden Zeilen angezeigten Datenereignistypen zu protokollieren.

Für Ereignisdatenspeicher können Sie nur erweiterte Ereignisselectoren verwenden, um Datenereignisse einzubeziehen.

AWS-Service	Beschreibung	Typ des Datenereignisses (Konsole)	resources.type-Wert
Amazon-DynamoDB	<p><a href="#">Amazon DynamoDB DynamoDB-API-Aktivität auf Artekelebene</a> für Tabellen (z. B., PutItemDeleteItem, und UpdateItem API-Operationen).</p> <div data-bbox="354 1020 673 1871" style="border: 1px solid #ccc; border-radius: 10px; padding: 10px; background-color: #f0f8ff;"> <p> <b>Note</b></p> <p>Bei Tabellen mit aktivierten Streams enthält das resources-Feld im Datenereignis sowohl AWS::DynamoDB::Stream als auch AWS::DynamoDB::Table. Wenn Sie AWS::Dyna</p> </div>	DynamoDB	AWS::DynamoDB::Table


AWS-Service	Beschreibung	Typ des Datenereignisses (Konsole)	resources.type-Wert
	<p>           moDB::Table als resources.type angeben, werden standardmäßig sowohl DynamoDB-Tabellen als auch DynamoDB-Stream-Ereignisse protokolliert. Um <a href="#">Streams-Ereignisse</a> auszuschließen, fügen Sie dem Feld einen Filter hinzu.         </p> <p>eventName</p>		
AWS Lambda	AWS Lambda Aktivität zur Funktionsausführung (die Invoke API).	Lambda	AWS::Lambda::Function


AWS-Service	Beschreibung	Typ des Datenereignisses (Konsole)	resources.type-Wert
Amazon S3	<a href="#">Amazon S3 S3-API-Aktivität auf Objektebene</a> (z. B., <code>GetObject</code> , <code>DeleteObject</code> , und <code>PutObject</code> API-Operationen) für Objekte in S3-Buckets.	S3	<code>AWS::S3::Object</code>
AWS AppConfig	<a href="#">AWS AppConfig API-Aktivität</a> für Konfigurationsvorgänge wie Aufrufe von <code>StartConfigurationSession</code> und <code>GetLatestConfiguration</code> .	AWS AppConfig	<code>AWS::AppConfig::Configuration</code>
AWS B2B-Datenaustausch	B2B-Datenaustausch-API-Aktivität für Transformer-Operationen wie Aufrufe von <code>GetTransformerJob</code> und <code>StartTransformerJob</code> .	B2B-Datenaustausch	<code>AWS::B2BI::Transformer</code>
Amazon Bedrock	<a href="#">Amazon-Bedrock-API-Aktivität</a> auf einem Agent-Alias.	Bedrock-Agent-Alias	<code>AWS::Bedrock::AgentAlias</code>




AWS-Service	Beschreibung	Typ des Datenereignisses (Konsole)	resources.type-Wert
	<a href="#">Amazon-Bedrock-API-Aktivität</a> auf einer Wissensdatenbank.	Bedrock-Wissensdatenbank	AWS::Bedrock::KnowledgeBase
Amazon CloudFront	CloudFront API-Aktivität auf einem <a href="#">KeyValueStore</a> .	CloudFront KeyValueStore	AWS::CloudFront::KeyValueStore
AWS Cloud Map	<a href="#">AWS Cloud Map API-Aktivität</a> in einem <a href="#">Namespace</a> .	AWS Cloud Map Namespace	AWS::ServiceDiscovery::Namespace
	<a href="#">AWS Cloud Map API-Aktivität</a> für einen <a href="#">Dienst</a> .	AWS Cloud Map Service nicht zulässig	AWS::ServiceDiscovery::Service
AWS CloudTrail	CloudTrail <a href="#">PutAuditEvents</a> Aktivität auf einem <a href="#">CloudTrail Lake-Kanal</a> , der verwendet wird, um Ereignisse von außen zu protokollieren AWS.	CloudTrail Kanal	AWS::CloudTrail::Channel
Amazon CodeWhisperer	CodeWhisperer Amazon-API-Aktivität bei einer Anpassung.	CodeWhisperer Anpassung	AWS::CodeWhisperer::Customization
	CodeWhisperer Amazon-API-Aktivität in einem Profil.	CodeWhisperer	AWS::CodeWhisperer::Profile

AWS-Service	Beschreibung	Typ des Datenereignisses (Konsole)	resources.type-Wert
Amazon Cognito	API-Aktivität von Amazon Cognito in Amazon-Cognito- <a href="#">Identitätspools</a> .	Cognito-Identitätspools	AWS::Cognito::IdentityPool
Amazon-DynamoDB	API-Aktivitäten von <a href="#">Amazon DynamoDB</a> in Streams.	DynamoDB-Streams	AWS::DynamoDB::Stream
Amazon Elastic Block Store	Direkte APIs von <a href="#">Amazon Elastic Block Store (EBS)</a> wie PutSnapshotBlock, GetSnapshotBlock und ListChangedBlocks in Amazon-EBS-Snapshots.	Amazon EBS Direct-APIs	AWS::EC2::Snapshot
Amazon EMR	API-Aktivität von Amazon EMR in einem Write-Ahead-Log-Workspace.	EMR-Write-Ahead-Log-Workspace	AWS::EMRWA::Workspace
Amazon FinSpace	API-Aktivitäten von <a href="#">Amazon FinSpace</a> in Umgebungen.	FinSpace	AWS::FinSpace::Environment

AWS-Service	Beschreibung	Typ des Datenereignisses (Konsole)	resources.type-Wert
AWS Glue	<p>AWS Glue API-Aktivität für Tabellen, die von Lake Formation erstellt wurden.</p> <div data-bbox="354 590 673 1780" style="border: 1px solid #add8e6; border-radius: 10px; padding: 10px;"><p> <b>Note</b></p><p>AWS Glue Datenereignisse für Tabellen werden derzeit nur in den folgenden Regionen unterstützt:</p><ul style="list-style-type: none"><li>• USA Ost (Nord-Virginia)</li><li>• USA Ost (Ohio)</li><li>• USA West (Oregon)</li><li>• Europa (Irland)</li><li>• Region Asien-Pazifik (Tokio)</li></ul></div>	Lake Formation	AWS::Glue::Table

AWS-Service	Beschreibung	Typ des Datenereignisses (Konsole)	resources.type-Wert
Amazon GuardDuty	GuardDuty Amazon-API-Aktivität für einen <a href="#">Detektor</a> .	GuardDuty Detektor	AWS::GuardDuty::Detector
AWS HealthImaging	AWS HealthImaging API-Aktivität in Datenspeichern.	Datenspeicher für medizinische Bildgebung	AWS::MedicalImaging::Datastore
AWS IoT	<a href="#">AWS IoT API-Aktivität</a> für <a href="#">Zertifikate</a> .	IoT-Zertifikat	AWS::IoT::Certificate
	<a href="#">AWS IoT API-Aktivität</a> für <a href="#">Dinge</a> .	IoT-Sache	AWS::IoT::Thing
AWS IoT Greengrass Version 2	<a href="#">Greengrass-API-Aktivität</a> von einem Greengrass-Core-Gerät auf einer Komponentenversion.  <div data-bbox="354 1297 672 1801" style="border: 1px solid #00a0e3; border-radius: 10px; padding: 10px; background-color: #e6f2ff;"> <p> <b>Note</b></p> <p>Greengrass protokolliert keine Ereignisse, bei denen der Zugriff verweigert wurde.</p> </div>	IoT Greengrass-Komponentenversion	AWS::GreengrassV2::ComponentVersion

AWS-Service	Beschreibung	Typ des Datenereignisses (Konsole)	resources.type-Wert
	<p><a href="#">Greengrass-API-Aktivität</a> von einem Greengrass-Core-Gerät in einer Bereitstellung.</p> <div style="border: 1px solid #0070C0; border-radius: 10px; padding: 10px; margin-top: 10px;"> <p> <b>Note</b></p> <p>Greengrass protokolliert keine Ereignisse, bei denen der Zugriff verweigert wurde.</p> </div>	Einsatz von IoT Greengrass	AWS::GreengrassV2::Deployment
AWS IoT SiteWise	<a href="#">SiteWise IoT-API-Aktivität</a> für <a href="#">Anlagen</a> .	SiteWise IoT-Anlage	AWS::IoTSiteWise::Asset
	<a href="#">SiteWise IoT-API-Aktivität</a> in <a href="#">Zeitreihen</a> .	SiteWise IoT-Zeitreihen	AWS::IoTSiteWise::TimeSeries
AWS IoT TwinMaker	TwinMaker IoT-API-Aktivität für eine <a href="#">Entität</a> .	TwinMaker IoT-Entität	AWS::IoTTwinMaker::Entity
	TwinMaker IoT-API-Aktivität in einem <a href="#">Workspace</a> .	TwinMaker IoT-Arbeitsplatz	AWS::IoTTwinMaker::Workspace

AWS-Service	Beschreibung	Typ des Datenereignisses (Konsole)	resources.type-Wert
Amazon Kendra Intelligent Ranking	API-Aktivität von Amazon Kendra Intelligent Rankin für <a href="#">Rescore-Ausführung spläne</a> .	Kendra-Rangliste	AWS::KendraRanking::ExecutionPlan
Amazon Keyspaces (für Apache Cassandra)	<a href="#">Amazon Keyspaces-API-Aktivität</a> in einer Tabelle.	Cassandra-Tabelle	AWS::Cassandra::Table
Amazon-Kinesis-Data-Streams	Kinesis Data Streams API-Aktivität in <a href="#">Streams</a> .	Kinesis-Stream	AWS::Kinesis::Stream
	Kinesis Data Streams API-Aktivität auf <a href="#">Stream-Verbrauchern</a> .	Kinesis Stream Consumer	AWS::Kinesis::StreamConsumer
Amazon Kinesis Video Streams	Kinesis Video Streams Streams-API-Aktivitäten in Videostreams, z. B. Aufrufe von GetMedia undPutMedia.	Kinesis-Videostream	AWS::KinesisVideo::Stream
Amazon Managed Blockchain	API-Aktivität von Amazon Managed Blockchain in einem Netzwerk.	Managed-Blockchain-Netzwerk	AWS::ManagedBlockchain::Network

AWS-Service	Beschreibung	Typ des Datenereignisses (Konsole)	resources.type-Wert
	JSON-RPC-Aufrufe von <a href="#">Amazon Managed Blockchain</a> in Ethereum-Knoten, zum Beispiel <code>eth_getBalance</code> oder <code>eth_getBlockByNumber</code> .	Managed Blockchain	<code>AWS::ManagedBlockchain::Node</code>
Amazon-Neptune-Graph	Daten-API-Aktivitäten in einem Neptune-Graph, zum Beispiel Abfragen, Algorithmen oder Vektorsuche.	Neptun-Graph	<code>AWS::NeptuneGraph::Graph</code>
AWS Private CA	AWS Private CA Konnektor für Active Directory-API-Aktivitäten.	AWS Private CA Konnektor für Active Directory	<code>AWS::PCACConnectorAD::Connector</code>
Amazon Q Apps	Daten-API-Aktivität auf <a href="#">Amazon Q Apps</a> .	Amazon Q Apps	<code>AWS::QApps:QApp</code>
Amazon Q Business	<a href="#">Amazon-Q-Business-API-Aktivität</a> auf einer Anwendung.	Amazon-Q-Business-Anwendung	<code>AWS::QBusiness::Application</code>
	<a href="#">Amazon-Q-Business-API-Aktivität</a> auf einer Datenquelle.	Amazon-Q-Business-Datenquelle	<code>AWS::QBusiness::DataSource</code>

AWS-Service	Beschreibung	Typ des Datenereignisses (Konsole)	resources.type-Wert
	<a href="#">Amazon-Q-Business-API-Aktivität</a> auf einem Index.	Amazon-Q-Business-Index	AWS::QBusiness::Index
	<a href="#">Amazon-Q-Business-API-Aktivität</a> auf einem Weberlebnis.	Amazon-Q-Business-Weberlebnis	AWS::QBusiness::WebExperience
Amazon RDS	<a href="#">Amazon RDS-API-Aktivität</a> in einem DB-Cluster.	RDS-Daten-API — DB-Cluster	AWS::RDS::DBCluster
Amazon S3	<a href="#">Amazon S3 S3-API-Aktivität</a> auf Access Points.	S3-Zugangspunkt	AWS::S3::AccessPoint
	<a href="#">API-Aktivitäten für Amazon S3 Object Lambda Access Points</a> , z. B. Aufrufe von CompleteMultipartUpload undGetObject .	S3 Objekt Lambda	AWS::S3ObjectLambda::AccessPoint
Amazon S3 in Outposts	API-Aktivität auf Objektebene auf <a href="#">Amazon S3 on Outposts</a> .	S3-Outposts	AWS::S3Outposts::Object



AWS-Service	Beschreibung	Typ des Datenereignisses (Konsole)	resources.type-Wert
Amazon SageMaker	SageMaker <a href="#">InvokeEndpointWithResponseStream</a> Amazon-Aktivitäten auf Endpunkten.	SageMaker Endpunkt	AWS::SageMaker::Endpoint
	SageMaker Amazon-API-Aktivität in Feature-Stores.	SageMaker feature store	AWS::SageMaker::FeatureGroup
	SageMaker Amazon-API-Aktivität für <a href="#">Versuchskomponente</a> .	SageMaker Metriken, Experiment, Versuchskomponente	AWS::SageMaker::ExperimentTrialComponent
Amazon SNS	<a href="#">Publish</a> -API-Operationen von Amazon SNS auf Plattformendpunkten.	SNS-Plattformendpunkt	AWS::SNS::PlatformEndpoint
	<a href="#">Publish</a> - und <a href="#">PublishBatch</a> - API-Operationen von Amazon SNS zu Themen.	SNS-Thema	AWS::SNS::Topic
Amazon SQS	<a href="#">Amazon-SQS-API-Aktivität</a> auf Nachrichten.	SQS	AWS::SQS::Queue

AWS-Service	Beschreibung	Typ des Datenereignisses (Konsole)	resources.type-Wert
AWS Step Functions	<a href="#">API-Aktivität von Step Functions</a> auf einer Zustandsmaschine.	Step-Functions-Zustandsautomat	AWS::StepFunctions::StateMachine
AWS Supply Chain	AWS Supply Chain API-Aktivität auf einer Instanz.	Lieferkette	AWS::SCN::Instance
Amazon SWF	<a href="#">Amazon SWF SWF-API-Aktivität auf Domains</a> .	SWF-Domäne	AWS::SWF::Domain
AWS Systems Manager	<a href="#">Systems Manager Manager-API-Aktivität</a> auf Kontrollkanälen.	Systems Manager	AWS::SSMMessages::ControlChannel
	<a href="#">Systems Manager Manager-API-Aktivität</a> auf verwalteten Knoten.	Von Systems Manager verwalteter Knoten	AWS::SSM::ManagedNode
Amazon Timestream	<a href="#">Query</a> -API-Aktivität von Amazon Timestream in Datenbanken.	Timestream-Datenbank	AWS::Timestream::Database
	<a href="#">Query</a> -API-Aktivität von Amazon Timestream in Tabellen.	Timestream-Tabelle	AWS::Timestream::Table

AWS-Service	Beschreibung	Typ des Datenereignisses (Konsole)	resources.type-Wert
Amazon Verified Permissions	API-Aktivität von Amazon Verified Permissions in einem Richtlinienpeicher.	Amazon Verified Permissions	AWS::VerifiedPermissions::PolicyStore
Amazon WorkSpaces Thin Client	WorkSpaces Thin Client-API-Aktivität auf einem Gerät.	Thin-Client-Gerät	AWS::ThinClient::Device
	WorkSpaces Thin Client-API-Aktivität in einer Umgebung.	Thin-Client-Umgebung	AWS::ThinClient::Environment
AWS X-Ray	<a href="#">X-Ray-API-Aktivität auf Spuren</a> .	Röntgenspur	AWS::XRay::Trace

Datenereignisse werden standardmäßig nicht protokolliert, wenn Sie einen Trail oder einen Ereignisdatenspeicher erstellen. Um CloudTrail Datenereignisse aufzuzeichnen, müssen Sie explizit die unterstützten Ressourcen oder Ressourcentypen hinzufügen, für die Sie Aktivitäten erfassen möchten. Weitere Informationen zum Protokollieren von Datenereignissen finden Sie unter [Protokollieren von Datenereignissen](#).

Für die Protokollierung von Datenereignissen fallen zusätzliche Gebühren an. CloudTrail Preise finden Sie unter [AWS CloudTrail Preisgestaltung](#).

## Einblicke und Ereignisse

CloudTrail Insights-Ereignisse erfassen ungewöhnliche API-Aufruf- oder Fehlerquoten in Ihrem AWS Konto, indem sie die CloudTrail Verwaltungsaktivitäten analysieren. Insights-Ereignisse stellen relevante Informationen bereit, z. B. die zugehörige API, den Fehlercode, die Vorfallzeit und Statistiken, die Ihnen helfen, ungewöhnliche Aktivitäten zu verstehen und darauf zu reagieren. Im Gegensatz zu anderen Arten von Ereignissen, die in einem CloudTrail Trail- oder Event-Datenspeicher erfasst werden, werden Insights-Ereignisse nur protokolliert, wenn Änderungen in

der API-Nutzung Ihres Kontos oder bei der Protokollierung der Fehlerquote CloudTrail festgestellt werden, die sich erheblich von den typischen Nutzungsmustern des Kontos unterscheiden.

Beispiele für Aktivitäten, bei denen ggf. Insights-Ereignisse generiert werden, sind:

- Für Ihr Konto werden pro Minute normalerweise nicht mehr als 20 DeleteBucket-API-Aufrufe vom Typ Amazon S3 protokolliert, aber unter Ihrem Konto werden nun durchschnittlich 100 DeleteBucket-API-Aufrufe pro Minute protokolliert. Ein Insights-Ereignis wird zu Beginn der ungewöhnlichen Aktivitäten protokolliert und ein anderes Insights-Ereignis wird protokolliert, um das Ende der ungewöhnlichen Aktivitäten zu markieren.
- Für Ihr Konto werden pro Minute normalerweise 20 Aufrufe der Amazon-EC2-AuthorizeSecurityGroupIngress-API protokolliert, aber unter Ihrem Konto werden nun keine Aufrufe von AuthorizeSecurityGroupIngress mehr protokolliert. Ein Insights-Ereignis wird zu Beginn der ungewöhnlichen Aktivitäten protokolliert und zehn Minuten später, nachdem die ungewöhnlichen Aktivitäten nicht mehr auftreten, wird ein anderes Insights-Ereignis protokolliert, um das Ende der ungewöhnlichen Aktivitäten zu markieren.
- Ihr Konto protokolliert normalerweise weniger als einen AccessDeniedException-Fehler in einem Zeitraum von sieben Tagen in der AWS Identity and Access Management -API, DeleteInstanceProfile. Ihr Konto beginnt mit der Protokollierung von durchschnittlich 12 AccessDeniedException-Fehlern pro Minute für den DeleteInstanceProfile-API-Aufruf. Ein Insights-Ereignis wird zu Beginn der ungewöhnlichen Fehlerraten-Aktivitäten protokolliert und ein anderes Insights-Ereignis wird protokolliert, um das Ende der ungewöhnlichen Aktivitäten zu markieren.

Diese Beispiele dienen nur zur Veranschaulichung. Ihre Ergebnisse können je nach Anwendungsfall abweichen.

Um CloudTrail Insights-Ereignisse zu protokollieren, müssen Sie Insights-Ereignisse in einem neuen oder vorhandenen Trail- oder Event-Datenspeicher explizit aktivieren. Weitere Informationen zum Protokollieren von Insights-Ereignissen finden Sie unter [Protokollieren von Insights-Ereignissen](#).

Für Insights-Ereignisse fallen zusätzliche Gebühren an. Wenn Sie Insights sowohl für Trails als auch für Ereignisdatenspeicher aktivieren, wird Ihnen eine separate Gebühr in Rechnung gestellt. Weitere Informationen finden Sie unter [AWS CloudTrail -Preisgestaltung](#).

## Insights-Ereignisse für Trails und Ereignisdatenspeicher anzeigen

CloudTrail unterstützt Insights-Ereignisse sowohl für Trails als auch für Event-Datenspeicher. Es gibt jedoch einige Unterschiede in der Art und Weise, wie du Insights-Ereignisse ansiehst und darauf zugreifst.

### Anzeigen von Insights-Ereignissen für Trails

Wenn du Insights-Ereignisse für einen Trail aktiviert hast und ungewöhnliche Aktivitäten CloudTrail feststellst, werden Insights-Ereignisse in einem anderen Ordner oder Präfix im Ziel-S3-Bucket für deinen Trail protokolliert. Sie können auch die Art der Insights und den Zeitraum des Vorfalls sehen, wenn Sie Insights-Ereignisse auf der CloudTrail Konsole aufrufen. Weitere Informationen finden Sie unter [CloudTrail Insights-Ereignisse für Trails in der CloudTrail Konsole anzeigen](#).

### Anzeigen von Insights-Ereignissen für Ereignisdatenspeicher

Um Insights-Ereignisse in CloudTrail Lake zu protokollieren, benötigen Sie einen Zielereignisdatenspeicher, der Insights-Ereignisse protokolliert, und einen Quellereignisdatenspeicher, der Insights aktiviert und Verwaltungsereignisse protokolliert. Weitere Informationen finden Sie unter [Erstellen Sie mit der Konsole einen Ereignisdatenspeicher für CloudTrail Insights-Ereignisse](#).

Wenn Sie CloudTrail Insights in einem Quell-Eventdatenspeicher aktiviert haben und ungewöhnliche CloudTrail Aktivitäten erkennen, werden Insights-Ereignisse an Ihren Zielereignisdatenspeicher übermittelt. Anschließend können Sie Ihren Zielereignisdatenspeicher abfragen, um Informationen zu Ihren Insights-Ereignissen zu erhalten, und die Abfrageergebnisse optional in einem S3-Bucket speichern. Weitere Informationen finden Sie unter [Abfrage erstellen oder bearbeiten](#) und [Sehen Sie sich Beispielabfragen in der CloudTrail Konsole an](#).

Sie können das Insights-Events-Dashboard aufrufen, um die Insights-Ereignisse in Ihrem Zielereignisdatenspeicher zu visualisieren. Weitere Informationen finden Sie unter [CloudTrail Lake-Dashboards anzeigen](#).

## Ereignisverlauf

CloudTrail Der Ereignisverlauf bietet eine einsehbare, durchsuchbare, herunterladbare und unveränderliche Aufzeichnung der CloudTrail Verwaltungsereignisse der letzten 90 Tage in einem AWS-Region. Sie können diesen Verlauf verwenden, um sich einen Überblick über die Aktionen zu verschaffen, die in Ihrem AWS Konto in den AWS SDKs, AWS Management Console, Befehlszeilentools und anderen Diensten durchgeführt wurden. AWS Sie können Ihre Ansicht

des Ereignisverlaufs in der CloudTrail Konsole anpassen, indem Sie auswählen, welche Spalten angezeigt werden. Weitere Informationen finden Sie unter [Mit dem CloudTrail Eventverlauf arbeiten](#).

## Trails

Ein Trail ist eine Konfiguration, die die Übertragung von CloudTrail Ereignissen an einen S3-Bucket mit optionaler Lieferung an [CloudWatch Logs](#) und [Amazon](#) ermöglicht EventBridge. Sie können einen Trail verwenden, um die CloudTrail Ereignisse auszuwählen, die Sie übertragen möchten, Ihre CloudTrail Ereignisprotokolldateien mit einem AWS KMS Schlüssel verschlüsseln und Amazon SNS SNS-Benachrichtigungen für die Übermittlung von Protokolldateien einrichten. Weitere Informationen zum Erstellen und Verwalten eines Trails finden Sie unter [Erstellen Sie einen Trail für Ihren AWS-Konto](#).

### Wanderwege mit mehreren Regionen und nur einer Region

Sie können zwei Arten von Wegen für einen erstellen AWS-Konto: Wanderwege mit mehreren Regionen und Wanderwege mit nur einer Region.


#### Wanderwege mit mehreren Regionen

Wenn Sie einen Trail mit mehreren Regionen erstellen, CloudTrail zeichnet er alle Ereignisse AWS-Regionen in der [AWS Partition](#) auf, in der Sie arbeiten, und übermittelt die CloudTrail Ereignisprotokolldateien an einen von Ihnen angegebenen S3-Bucket. Wenn ein Trail hinzugefügt AWS-Region wird, nachdem Sie einen Trail mit mehreren Regionen erstellt haben, wird diese neue Region automatisch hinzugefügt, und Ereignisse in dieser Region werden protokolliert. Das Erstellen eines Trails mit mehreren Regionen wird als bewährte Methode empfohlen, da Sie Aktivitäten in allen Regionen in Ihrem Konto erfassen. Alle Trails, die Sie mit der CloudTrail Konsole erstellen, sind regionsübergreifend. Sie können einen Pfad mit einer einzelnen Region in einen Pfad mit mehreren Regionen konvertieren, indem Sie den verwenden. AWS CLI Weitere Informationen finden Sie unter [Erstellen eines Trails in der Konsole](#) und [Umwandeln eines Trails, der für eine Region gilt, zu einem Trail für alle Regionen](#).

#### Wanderwege für eine einzelne Region

Wenn Sie einen Pfad mit nur einer Region erstellen, werden nur die Ereignisse in dieser Region CloudTrail aufgezeichnet. Anschließend werden die CloudTrail Ereignisprotokolldateien an einen von Ihnen angegebenen Amazon S3 S3-Bucket gesendet. Sie können nur einen einzelnen Regions-Trail erstellen, indem Sie die AWS CLI verwenden. Wenn Sie zusätzliche einzelne Trails erstellen, können Sie festlegen, dass diese Trails CloudTrail Ereignisprotokolldateien an denselben S3-Bucket oder an separate Buckets liefern. Dies ist die Standardoption, wenn Sie

einen Trail mithilfe der AWS CLI oder der CloudTrail API erstellen. Weitere Informationen finden Sie unter [Trails erstellen, aktualisieren und verwalten mit dem AWS CLI](#).

 Note

Für beide Arten von Trails können Sie einen Amazon-S3-Bucket aus einer beliebigen Region angeben.

Ein Trail mit mehreren Regionen bietet die folgenden Vorteile:

- Die Konfigurationseinstellungen für den Trail gelten einheitlich für alle AWS-Regionen.
- Sie erhalten CloudTrail Ereignisse von allen AWS-Regionen in einem einzigen Amazon S3 S3-Bucket und optional in einer CloudWatch Logs-Protokollgruppe.
- Sie verwalten die Trail-Konfiguration für alle AWS-Regionen von einem Standort aus.

Wenn Sie einen Trail auf alle AWS Regionen anwenden, verwendet er den Pfad, den Sie in einer bestimmten Region erstellen, um Trails mit identischer Konfiguration in allen anderen Regionen der [AWS Partition](#) zu erstellen, in der Sie arbeiten.

Dies hat folgende Auswirkungen:

- CloudTrail liefert Protokolldateien für Kontoaktivitäten aus allen AWS Regionen an den einzelnen Amazon S3 S3-Bucket, den Sie angeben, und optional an eine CloudWatch Logs-Protokollgruppe.
- Wenn Sie ein Amazon SNS SNS-Thema für den Trail konfiguriert haben, werden SNS-Benachrichtigungen über Protokolldateizustellungen in allen AWS Regionen an dieses einzelne SNS-Thema gesendet.

Unabhängig davon, ob es sich um einen Trail mit mehreren Regionen oder einer einzelnen Region handelt, EventBridge werden Ereignisse, die an Amazon gesendet werden, im [Eventbus](#) jeder Region empfangen und nicht in einem einzigen Eventbus.

### Mehrere Trails pro Region

Wenn Sie zwar mehrere, aber ähnliche Benutzergruppen (wie Developer, Sicherheitspersonal und IT-Auditoren) haben, können Sie mehrere Trails pro Region erstellen. Auf diese Weise erhält jede Gruppe eine eigene Kopie der Protokolldateien.

CloudTrail unterstützt fünf Trails pro Region. Ein Pfad mit mehreren Regionen zählt als ein Weg pro Region.

Das Folgende ist ein Beispiel für eine Region mit fünf Wanderwegen:

- Sie erstellen zwei Trails in der USA West (Nordkalifornien), die nur für diese Region gelten.
- Sie erstellen zwei weitere Trails mit mehreren Regionen in der Region USA West (Nordkalifornien).
- Sie erstellen einen weiteren Wanderweg mit mehreren Regionen in der Region Asien-Pazifik (Sydney). Dieser Trail ist auch in der Region USA West (Nordkalifornien) vorhanden.

Sie können sich eine Liste der Wanderwege auf AWS-Region der Seite Trails der CloudTrail Konsole ansehen. Weitere Informationen finden Sie unter [Aktualisieren eines Trails](#). CloudTrail Preise finden Sie unter [AWS CloudTrail Preise](#).

## Organisatorische Pfade

Ein Organisationspfad ist eine Konfiguration, die die Übertragung von CloudTrail Ereignissen im Verwaltungskonto und allen Mitgliedskonten einer AWS Organizations Organisation an denselben Amazon S3 S3-Bucket, dieselben CloudWatch Logs und Amazon ermöglicht EventBridge. Das Erstellen eines Organisations-Trails hilft Ihnen dabei, für Ihre Organisation eine einheitliche Ereignisprotokollierungsstrategie zu definieren.

Bei allen über die Konsole erstellten Organisationspfade handelt es sich um regionsübergreifende Organisationspfade, in denen Ereignisse von den AWS-Regionen in jedem Mitgliedskonto der Organisation [aktivierten](#) Konten protokolliert werden. Um Ereignisse in allen AWS Partitionen Ihrer Organisation zu protokollieren, erstellen Sie in jeder Partition einen regionsübergreifenden Organisationspfad. Sie können entweder einen Organisationspfad mit einer Region oder mit mehreren Regionen erstellen, indem Sie den verwenden. AWS CLI Wenn Sie einen Pfad mit nur einer Region erstellen, protokollieren Sie nur Aktivitäten in den Pfaden AWS-Region (auch als Heimatregion bezeichnet).

Obwohl die meisten Regionen standardmäßig für dich aktiviert AWS-Regionen sind AWS-Konto, musst du bestimmte Regionen (auch als Opt-in-Regionen bezeichnet) manuell aktivieren. Informationen darüber, welche Regionen standardmäßig aktiviert sind, finden Sie im AWS Account Management Referenzhandbuch unter [Überlegungen vor dem Aktivieren und Deaktivieren von Regionen](#). Eine Liste der CloudTrail unterstützten Regionen finden Sie unter [CloudTrail unterstützte Regionen](#).



Wenn Sie einen Organisationspfad erstellen, wird in den Mitgliedskonten, die zu Ihrer Organisation gehören, eine Kopie des Trails mit dem Namen erstellt, den Sie ihm geben.

- Wenn sich der Organisationspfad auf eine einzelne Region bezieht und die Heimatregion des Trails keine OPT-Region ist, wird in jedem Mitgliedskonto eine Kopie des Trails in der Heimatregion des Organisationstrails erstellt.
- Wenn sich der Organisationspfad auf eine einzelne Region bezieht und die Heimatregion des Trails eine OPT-Region ist, wird eine Kopie des Trails in der Heimatregion des Organisationstrails in den Mitgliedskonten erstellt, die diese Region aktiviert haben.
- Wenn es sich bei dem Organisationspfad um mehrere Regionen handelt und die Heimatregion des Trails keine Region ist, in der sich der Weg angemeldet hat, wird in jedem Mitgliedskonto, das aktiviert AWS-Region ist, eine Kopie des Trails erstellt. Wenn ein Mitgliedskonto eine Opt-in-Region aktiviert, wird nach Abschluss der Aktivierung dieser Region eine Kopie des Multi-Region-Trails in der neu angemeldeten Region für das Mitgliedskonto erstellt.
- Wenn es sich bei dem Organisationspfad um einen Multi-Region-Trail handelt und die Heimatregion eine optionale Region ist, senden Mitgliedskonten keine Aktivitäten an den Organisationspfad, es sei denn, sie entscheiden sich für den Ort, an AWS-Region dem der Multi-Region-Trail erstellt wurde. Wenn du beispielsweise einen Trail mit mehreren Regionen erstellst und die Region Europa (Spanien) als Heimatregion für den Trail auswählst, senden nur Mitgliedskonten, die die Region Europa (Spanien) für ihr Konto aktiviert haben, ihre Kontoaktivitäten an den Organisationspfad.

#### Note

CloudTrail erstellt Organisationspfade in Mitgliedskonten, auch wenn eine Ressourcenvalidierung fehlschlägt. Zu den Beispielen für fehlgeschlagene Überprüfungen gehören:

- eine falsche Amazon S3 S3-Bucket-Richtlinie
- eine falsche Amazon SNS SNS-Themenrichtlinie
- Unfähigkeit, an eine CloudWatch Logs-Protokollgruppe zu liefern
- unzureichende Rechte zur Verschlüsselung mit einem KMS-Schlüssel

Ein Mitgliedskonto mit CloudTrail Berechtigungen kann alle Validierungsfehler für einen Organisationspfad anzeigen, indem es die Detailseite des Trails in der CloudTrail Konsole aufruft oder den AWS CLI [get-trail-status](#) Befehl ausführt.

Benutzer mit CloudTrail Berechtigungen für Mitgliedskonten können Organisationspfade (einschließlich des Trail-ARN) sehen, wenn sie sich von ihren AWS Konten aus bei der AWS CloudTrail Konsole anmelden oder wenn sie AWS CLI Befehle wie ausführen `describe-trails` (allerdings müssen Mitgliedskonten den ARN für den Organisationspfad verwenden und nicht den Namen, wenn sie den verwenden AWS CLI). Benutzer mit Mitgliedskonten verfügen jedoch nicht über ausreichende Berechtigungen, um Organisationspfade zu löschen, die Anmeldung ein- oder auszuschalten, zu ändern, welche Arten von Ereignissen protokolliert werden, oder Organisationspfade auf andere Weise zu ändern. Weitere Informationen zu AWS Organizations finden Sie unter [Terminologie und Konzepte von Organizations](#). Weitere Informationen zum Erstellen von und zum Arbeiten mit Organisations-Trails finden Sie unter [Erstellen eines Trails für eine Organisation](#).

## CloudTrail Datenspeicher für Seen und Ereignisse

CloudTrail Mit Lake können Sie feinkörnige SQL-basierte Abfragen zu Ihren Ereignissen ausführen und Ereignisse aus externen Quellen protokollieren AWS, z. B. aus Ihren eigenen Anwendungen und von Partnern, die integriert sind. CloudTrail Sie müssen in Ihrem Konto keinen Trail konfiguriert haben, um Lake verwenden zu können. CloudTrail

Die Ereignisse werden in Ereignisdatenspeichern zusammengefasst, bei denen es sich um unveränderliche Sammlungen von Ereignissen handelt, die auf Kriterien basieren, die Sie mit Hilfe von [erweiterten Ereignisselektoren](#) auswählen. Sie können die Ereignisdaten bis zu 3 653 Tage (etwa 10 Jahre) in einem Ereignisdatenspeicher speichern, wenn Sie sich für die Preisoption mit verlängerbarer Aufbewahrung von einem Jahr entscheiden, oder bis zu 2 557 Tage (etwa 7 Jahre), wenn Sie sich für die Preisoption mit siebenjähriger Aufbewahrung entscheiden. Sie können Lake-Abfragen für die zukünftige Verwendung speichern und die Ergebnisse von Abfragen bis zu sieben Tage lang anzeigen. Sie können Abfrageergebnisse auch in einem S3-Bucket speichern. CloudTrail Lake kann auch Ereignisse einer Organisation AWS Organizations in einem Ereignisdatenspeicher oder Ereignisse aus mehreren Regionen und Konten speichern. CloudTrail Lake ist Teil einer Auditing-Lösung, die Sie bei der Durchführung von Sicherheitsuntersuchungen und

Problembhebungen unterstützt. Weitere Informationen finden Sie unter [Mit AWS CloudTrail Lake arbeiten](#) und [CloudTrail Konzepte und Terminologie von Seen](#).

## CloudTrail Einblicke

CloudTrail Mithilfe von Erkenntnissen AWS können Benutzer ungewöhnliche Mengen an API-Aufrufen oder bei API-Aufrufen protokollierte Fehler erkennen und darauf reagieren, indem CloudTrail Verwaltungsereignisse kontinuierlich analysiert werden. Ein Insights-Ereignis ist eine Aufzeichnung ungewöhnlicher `write`-Verwaltungs-API-Aktivitäten oder ungewöhnlicher Fehlermengen, die für Verwaltungs-API-Aktivitäten zurückgegeben werden. Standardmäßig protokollieren Trails und Event-Datenspeicher keine CloudTrail Insights-Ereignisse. In der Konsole können Sie auswählen, ob beim Erstellen oder Aktualisieren eines Trails oder Ereignisdatenspeichers Insights-Ereignisse protokolliert werden sollen. Wenn Sie die CloudTrail API verwenden, können Sie Insights-Ereignisse protokollieren, indem Sie die Einstellungen eines vorhandenen Trail- oder Event-Datenspeichers mit der [PutInsightSelectors](#)API bearbeiten. Für die Protokollierung von CloudTrail Insights-Ereignissen fallen zusätzliche Gebühren an. Wenn Sie Insights sowohl für Trails als auch für Ereignisdatenspeicher aktivieren, wird Ihnen eine separate Gebühr in Rechnung gestellt. Weitere Informationen finden Sie unter [Protokollieren von Insights-Ereignissen](#) und [Preise zu AWS CloudTrail](#).

## Tags

Ein Tag ist ein vom Kunden definierter Schlüssel und ein optionaler Wert, der AWS Ressourcen wie CloudTrail Pfade, Ereignisdatenspeichern und Kanälen, S3-Buckets zum Speichern von CloudTrail Protokolldateien, AWS Organizations Organisationen und Organisationseinheiten und vielem mehr zugewiesen werden kann. Indem Sie den Trails und den S3-Buckets, die Sie zum Speichern von Protokolldateien für Trails verwenden, dieselben Tags hinzufügen, können Sie die Verwaltung, Suche und Filterung dieser Ressourcen vereinfachen. [AWS Resource Groups](#) Sie können Tagging-Strategien implementieren, mit deren Hilfe Sie Ihre Ressourcen konsistent, effektiv und leicht finden und verwalten können. Weitere Informationen finden Sie unter [Bewährte Methoden für das Taggen von Ressourcen AWS](#).

## AWS Security Token Service und CloudTrail

AWS Security Token Service (AWS STS) ist ein Dienst, der über einen globalen Endpunkt verfügt und auch regionsspezifische Endpunkte unterstützt. Ein Endpunkt ist eine URL, die als Eintrittspunkt für Webserviceanforderungen fungiert. <https://cloudtrail.us-west-2.amazonaws.com> ist beispielsweise der regionale Zugangspunkt USA West (Oregon) für den Service. AWS CloudTrail Regionale Endpunkte reduzieren die Latenzzeiten der Anwendungen.

Wenn Sie einen AWS STS regionsspezifischen Endpunkt verwenden, übermittelt der Trail in dieser Region nur die AWS STS Ereignisse, die in dieser Region auftreten. Wenn Sie beispielsweise den Endpunkt `sts.us-west-2.amazonaws.com` nutzen, übermittelt der Trail in „us-west-2“ nur solche AWS STS -Ereignisse, die aus der Region „us-west-2“ stammen. Weitere Informationen zu AWS STS regionalen Endpunkten finden Sie unter [Aktivierung und Deaktivierung AWS STS in einer AWS Region im IAM-Benutzerhandbuch](#).

Eine vollständige Liste der AWS regionalen Endpunkte finden Sie unter [AWS Regionen und Endpunkte](#) in der [Allgemeine AWS-Referenz](#). Weitere Informationen zu Ereignissen des globalen AWS STS -Endpunkts finden Sie unter [Informationen zu globalen Serviceereignissen](#).

## Informationen zu globalen Serviceereignissen

### Important

Am 22. November 2021 wurde die Art und Weise AWS CloudTrail geändert, wie Trails globale Serviceereignisse erfassen. Jetzt AWS STS werden Ereignisse, die von Amazon CloudFront, AWS Identity and Access Management, erstellt und in der Region aufgezeichnet wurden, in der sie erstellt wurden, der Region USA Ost (Nord-Virginia), us-east-1. Dadurch wird die Art und Weise, wie diese Dienste CloudTrail behandelt werden, mit der anderer AWS globaler Dienste konsistent. Um weiterhin globale Service-Events außerhalb von USA Ost (Nord-Virginia) zu erhalten, sollten Sie einzelregionale Trails unter Verwendung globaler Serviceereignisse außerhalb von USA Ost (Nord-Virginia) in multiregionale Trails konvertieren. Weitere Informationen zum Erfassen von globalen Serviceereignissen finden Sie [Aktivieren und Deaktivieren der Protokollierung von globalen Serviceereignissen](#) später in diesem Abschnitt.

Im Gegensatz dazu zeigen der Ereignisverlauf in der CloudTrail Konsole und der `aws cloudtrail lookup-events` Befehl diese Ereignisse dort an, AWS-Region wo sie aufgetreten sind.

Für die meisten Services werden Ereignisse in der Region aufgezeichnet, in der die Aktion aufgetreten ist. Bei globalen Diensten wie AWS Identity and Access Management (IAM) und Amazon werden Ereignisse an jeden beliebigen Trail übertragen CloudFront, der globale Dienste beinhaltet.  
AWS STS

Bei den meisten globalen Serviceereignissen werden Ereignisse als in der Region USA Ost (Nord-Virginia) auftretend protokolliert, aber einige globale Serviceereignisse werden als in anderen Regionen auftretend protokolliert, z. B. in der Region USA Ost (Ohio) oder USA West (Oregon).

Damit die globalen Serviceereignisse nicht mehrfach übermittelt werden, beachten Sie Folgendes:

- Globale Serviceereignisse werden standardmäßig an Trails übermittelt, die mit der CloudTrail Konsole erstellt wurden. Ereignisse werden an den Bucket für den Trail gesendet.
- Wenn Sie über mehrere Einzelregion-Trails verfügen, sollten Sie Ihre Trails so konfigurieren, dass globale Serviceereignisse nur an einen der Trails gesendet werden. Weitere Informationen finden Sie unter [Aktivieren und Deaktivieren der Protokollierung von globalen Serviceereignissen](#).
- Wenn Sie die Konfiguration eines Trails ändern, sodass nicht alle Regionen protokolliert werden, sondern nur eine einzelne Region, wird die globale Serviceereignisprotokollierung für diesen Trail automatisch deaktiviert. Wenn Sie analog dazu die Konfiguration eines Trails ändern, sodass nicht mehr nur eine einzige Region, sondern alle Regionen protokolliert werden, wird die globale Serviceereignisprotokollierung für diesen Trail automatisch aktiviert.

Weitere Informationen zum Ändern der globalen Service-Ereignisprotokollierung für einen Trail finden Sie unter [Aktivieren und Deaktivieren der Protokollierung von globalen Serviceereignissen](#).

Beispiel:

1. Sie erstellen einen Trail in der CloudTrail Konsole. Standardmäßig werden globale Serviceereignisse von diesem Trail protokolliert.
2. Sie haben mehrere Trails für eine einzelne Region.
3. Es ist nicht erforderlich, die globalen Services für die Trails der einzelnen Region zu aktivieren. Globale Serviceereignisse werden an den ersten Trail übermittelt. Weitere Informationen finden Sie unter [Trails erstellen, aktualisieren und verwalten mit dem AWS CLI](#).

#### Note

Wenn Sie einen Trail mit den AWS SDKs oder der AWS CLI CloudTrail API erstellen oder aktualisieren, können Sie angeben, ob globale Serviceereignisse für Trails ein- oder ausgeschlossen werden sollen. Sie können die globale Protokollierung von Serviceereignissen nicht von der CloudTrail Konsole aus konfigurieren.

## CloudTrail unterstützte Regionen

### Note

Informationen zu Regionen, die von CloudTrail Lake unterstützt werden, finden Sie unter [CloudTrail Von Seen unterstützte Regionen](#).

Informationen zu Endpunkten der Datenebene finden Sie unter Endpunkte der [Datenebene](#) in der. Allgemeine AWS-Referenz

Name der Region	Region	Endpunkt der Steuerungsebene	Protokoll	Datum der Unterstützung
USA Ost (Nord-Virginia)	us-east-1	cloudtrail.us-east-1.amazonaws.com	HTTPS	13.11.2013
USA Ost (Ohio)	us-east-2	cloudtrail.us-east-2.amazonaws.com	HTTPS	17.10.2016
USA West (Nordkalifornien)	us-west-1	cloudtrail.us-west-1.amazonaws.com	HTTPS	13.05.2014
USA West (Oregon)	us-west-2	cloudtrail.us-west-2.amazonaws.com	HTTPS	13.11.2013
Afrika (Kapstadt)	af-south-1	cloudtrail.af-south-1.amazonaws.com	HTTPS	22.04.2020
Asien-Pazifik (Hongkong)	ap-east-1	cloudtrail.ap-east-1.amazonaws.com	HTTPS	24.04.2019
Asien-Pazifik (Hyderabad)	ap-south-2	cloudtrail.ap-south-2.amazonaws.com	HTTPS	22.11.2022

Name der Region	Region	Endpunkt der Steuerungsebene	Protokoll	Datum der Unterstützung
Asien-Pazifik (Jakarta)	ap-southeast-3	cloudtrail.ap-southeast-3.amazonaws.com	HTTPS	13.12.2021
Asien-Pazifik (Melbourne)	ap-southeast-4	cloudtrail.ap-southeast-4.amazonaws.com	HTTPS	23.01.2023
Asien-Pazifik (Mumbai)	ap-south-1	cloudtrail.ap-south-1.amazonaws.com	HTTPS	27.06.2016
Asien-Pazifik (Osaka)	ap-northeast-3	cloudtrail.ap-northeast-3.amazonaws.com	HTTPS	12.02.2018
Asien-Pazifik (Seoul)	ap-northeast-2	cloudtrail.ap-northeast-2.amazonaws.com	HTTPS	06.01.2016
Asien-Pazifik (Singapur)	ap-southeast-1	cloudtrail.ap-southeast-1.amazonaws.com	HTTPS	30.06.2014
Asien-Pazifik (Sydney)	ap-southeast-2	cloudtrail.ap-southeast-2.amazonaws.com	HTTPS	13.05.2014
Asien-Pazifik (Tokio)	ap-northeast-1	cloudtrail.ap-northeast-1.amazonaws.com	HTTPS	30.06.2014
Kanada (Zentral)	ca-central-1	cloudtrail.ca-central-1.amazonaws.com	HTTPS	08.12.2016
Kanada West (Calgary)	ca-west-1	cloudtrail.ca-west-1.amazonaws.com	HTTPS	20.12.2023

Name der Region	Region	Endpunkt der Steuerungsebene	Protokoll	Datum der Unterstützung
China (Beijing)	cn-north-1	cloudtrail.cn-north-1.amazonaws.com.cn	HTTPS	01.03.2014
China (Ningxia)	cn-northwest-1	cloudtrail.cn-northwest-1.amazonaws.com.cn	HTTPS	11.12.2017
Europa (Frankfurt)	eu-central-1	cloudtrail.eu-central-1.amazonaws.com	HTTPS	23.10.2014
Europa (Irland)	eu-west-1	cloudtrail.eu-west-1.amazonaws.com	HTTPS	13.05.2014
Europa (London)	eu-west-2	cloudtrail.eu-west-2.amazonaws.com	HTTPS	13.12.2016
Europa (Mailand)	eu-south-1	cloudtrail.eu-south-1.amazonaws.com	HTTPS	27.04.2020
Europa (Paris)	eu-west-3	cloudtrail.eu-west-3.amazonaws.com	HTTPS	18.12.2017
Europa (Spanien)	eu-south-2	cloudtrail.eu-south-2.amazonaws.com	HTTPS	16.11.2022
Europa (Stockholm)	eu-north-1	cloudtrail.eu-north-1.amazonaws.com	HTTPS	11.12.2018
Europa (Zürich)	eu-central-2	cloudtrail.eu-central-2.amazonaws.com	HTTPS	09.11.2022
Israel (Tel Aviv)	il-central-1	cloudtrail.il-central-1.amazonaws.com	HTTPS	31.07.2023



Name der Region	Region	Endpunkt der Steuerungsebene	Protokoll	Datum der Unterstützung
Naher Osten (Bahrain)	me-south-1	cloudtrail.me-south-1.amazonaws.com	HTTPS	29.07.2019
Naher Osten (VAE)	me-central-1	cloudtrail.me-central-1.amazonaws.com	HTTPS	30.08.2022
Südamerika (São Paulo)	sa-east-1	cloudtrail.sa-east-1.amazonaws.com	HTTPS	30.06.2014
AWS GovCloud (US-Ost)	us-gov-east-1	cloudtrail.us-gov-east-1.amazonaws.com	HTTPS	12.11.2018
AWS GovCloud (US-West)	us-gov-west-1	cloudtrail.us-gov-west-1.amazonaws.com	HTTPS	16.08.2011

Weitere Informationen zur Verwendung von CloudTrail finden Sie unter [Service Endpoints](#) im AWS GovCloud (US) Benutzerhandbuch. AWS GovCloud (US) Regions

Weitere Informationen zur Verwendung CloudTrail in der Region China (Peking) finden Sie unter [Endpunkte und ARNs für AWS in China im](#). Allgemeine Amazon Web Services-Referenz

## CloudTrail unterstützte Dienste und Integrationen

CloudTrail unterstützt die Protokollierung von Ereignissen für viele AWS-Services. Nähere Angaben zu den unterstützten Services finden Sie im Handbuch für den entsprechenden Service. Eine Liste der dienstspezifischen Themen finden Sie unter [AWS Servicethemen für CloudTrail](#). Darüber hinaus AWS-Services können einige davon verwendet werden, um in CloudTrail Protokollen gesammelte Daten zu analysieren und darauf zu reagieren.

**Note**

Die Liste der unterstützten Regionen für jeden Service finden Sie unter [Service-Endpunkte und Kontingente](#) in Allgemeine Amazon Web Services-Referenz.

## Themen

- [AWS Serviceintegrationen mit Protokollen CloudTrail](#)
- [CloudTrail Integration mit Amazon EventBridge](#)
- [CloudTrail Integration mit AWS Organizations](#)
- [AWS Servicethemen für CloudTrail](#)
- [CloudTrail nicht unterstützte Dienste](#)


## AWS Serviceintegrationen mit Protokollen CloudTrail


**Note**

Sie können CloudTrail Lake auch verwenden, um Ihre Ereignisse abzufragen und zu analysieren. CloudTrail Lake-Abfragen bieten eine umfassendere und besser anpassbare Ansicht von Ereignissen als einfache Schlüssel- und Werte-Suchen im Event-Verlauf oder in der Event-Historie. LookupEvents CloudTrail Lake-Benutzer können komplexe SQL-Abfragen (Standard Query Language) für mehrere Felder in einem CloudTrail Ereignis ausführen. Weitere Informationen finden Sie unter [Mit AWS CloudTrail Lake arbeiten](#) und [Trailereignisse nach CloudTrail Lake kopieren](#).

CloudTrail Für Datenspeicher und Abfragen von Lake-Ereignissen CloudTrail fallen Gebühren an. Weitere Informationen zu den Preisen von CloudTrail Lake finden Sie unter [AWS CloudTrail Preise](#).

Sie können andere AWS Dienste konfigurieren, um die in den CloudTrail Protokollen gesammelten Ereignisdaten weiter zu analysieren und darauf zu reagieren. Weitere Informationen finden Sie unter den folgenden Themen.

AWS Dienst	Thema	Beschreibung
Amazon Athena	<a href="#">Protokolle abfragen AWS CloudTrail</a>	<p>Die Verwendung von Athena mit CloudTrail Protokollen ist eine leistungsstarke Methode, um Ihre Analyse der AWS Serviceaktivitäten zu verbessern. Beispielsweise können Sie mithilfe von Abfragen Trends ermitteln und Vorgänge nach Attributen (z. B. Quell-IP-Adresse oder Benutzer) trennen.</p> <p>Sie können automatisch Tabellen für die Abfrage von Protokollen direkt von der CloudTrail Konsole erstellen und diese Tabellen verwenden, um Abfragen in Athena auszuführen. Weitere Informationen finden Sie unter <a href="#">Erstellen einer Tabelle für CloudTrail Protokolle in der CloudTrail Konsole im Amazon Athena Athena-Benutzerhandbuch</a>.</p> <div data-bbox="1068 1457 1507 1829"><p> <b>Note</b></p><p>Das Ausführen von Abfragen in Amazon Athena verursacht zusätzliche Kosten. Weitere Informationen hierzu finden Sie unter</p></div>

AWS Dienst	Thema	Beschreibung
		<p><a href="#">Preise zu Amazon Athena.</a></p>
CloudWatch Amazon-Protokolle	<p><a href="#">Überwachung von CloudTrail Protokolldateien mit Amazon CloudWatch Logs</a></p>	<p>Sie können CloudWatch Logs so konfigurieren CloudTrail , dass Ihre Trail-Logs überwacht werden und Sie benachrichtigt werden, wenn bestimmte Aktivitäten auftreten. Sie können beispielsweise Metrikenfilter für CloudWatch Logs definieren, die CloudWatch Alarme auslösen und Ihnen Benachrichtigungen senden, wenn diese Alarme ausgelöst werden.</p> <div data-bbox="1068 1024 1507 1577" style="border: 1px solid #ccc; border-radius: 10px; padding: 10px; margin-top: 10px;"> <p> <b>Note</b></p> <p>Es gelten die Standardpreise für Amazon CloudWatch und Amazon CloudWatch Logs. Weitere Informationen finden Sie unter <a href="#">Amazon CloudWatch – Preise</a>.</p> </div>

## CloudTrail Integration mit Amazon EventBridge

Amazon EventBridge ist ein AWS Service, der einen Stream von Systemereignissen nahezu in Echtzeit bereitstellt, die Änderungen an AWS Ressourcen beschreiben. In können Sie Regeln

erstellen EventBridge, die auf Ereignisse reagieren, die von aufgezeichnet wurden CloudTrail. Weitere Informationen finden Sie unter [Eine Regel in Amazon erstellen EventBridge](#).

Sie können Ereignisse, die Sie abonniert haben, auf eigene Fahnen übertragen, EventBridge indem Sie mit der EventBridge Konsole eine Regel erstellen.

Von der EventBridge Konsole aus:

- Wählen Sie den `AWS API Call via CloudTrail` Detailtyp für die Bereitstellung von CloudTrail Daten und Verwaltungsereignissen mit einem `eventType` von `AwsApiCall` Um Ereignisse mit einem Detailtypwert von aufzuzeichnen, benötigen Sie einen `TrailAWS API Call via CloudTrail`, der aktuell Verwaltungs- oder Datenereignisse protokolliert.
- [Wählen Sie den AWS Console Sign In via CloudTrail Detailtyp für die Übermittlung von Anmeldeereignissen.AWS Management Console](#) Um Ereignisse mit dem Detailtyp von aufzuzeichnen, benötigen Sie einen `TrailAWS Console Sign In via CloudTrail`, der derzeit Verwaltungsereignisse protokolliert.
- Wählen Sie den `AWS Insight via CloudTrail` Detailtyp für die Übermittlung von Insights-Ereignissen. Um Ereignisse mit einem Detailtypwert von aufzuzeichnen, benötigen Sie einen `TrailAWS Insight via CloudTrail`, der derzeit Insights-Ereignisse protokolliert. Weitere Informationen zum Protokollieren von Insights-Ereignissen finden Sie unter [Protokollieren von Insights-Ereignissen](#).

Informationen zum Erstellen eines Trails finden Sie unter [Erstellen eines Trails](#).

## CloudTrail Integration mit AWS Organizations

Das Verwaltungskonto für eine AWS Organizations Organisation kann einen [delegierten Administrator](#) hinzufügen, der die CloudTrail Ressourcen der Organisation verwaltet. Sie können einen Organisations-Trail oder einen Organisations-Ereignisdatspeicher im Verwaltungskonto oder im Konto eines delegierten Administrators für eine Organisation erstellen, der alle Ereignisdaten für alle AWS -Konten einer Organisation in AWS Organizations protokolliert. Das Erstellen eines Organisations-Trails hilft Ihnen dabei, für Ihre Organisation eine einheitliche Ereignisprotokollierungsstrategie zu definieren.

Ein Organisationspfad wird automatisch auf jedes AWS Konto in Ihrer Organisation angewendet. Benutzer in Mitgliedskonten können diese Trails sehen, aber nicht ändern. Für die Organisation erstellte Protokolldateien werden diesen Benutzern ebenfalls nicht angezeigt. Weitere Informationen finden Sie unter [Erstellen eines Trails für eine Organisation](#).

## AWS Servicethemen für CloudTrail

Sie können mehr darüber erfahren, wie die Ereignisse für einzelne AWS Dienste in CloudTrail Protokollen aufgezeichnet werden, einschließlich Beispielergebnissen für diesen Dienst in Protokolldateien. Weitere Informationen zur Integration bestimmter AWS Dienste finden Sie im Thema Integration im jeweiligen Leitfaden für diesen Dienst. CloudTrail

Dienste, die sich noch in der Vorschauversion befinden oder noch nicht für die allgemeine Verfügbarkeit (GA) freigegeben sind oder die keine öffentlichen APIs haben, gelten als nicht unterstützt. CloudTrail protokolliert derzeit keine richtlinienspezifischen Ereignisse für Amazon VPC-Endpunkte.

### Note

Die Liste der unterstützten Regionen für jeden Service finden Sie unter [Service-Endpunkte und Kontingente](#) in Allgemeine Amazon Web Services-Referenz. Weitere Informationen zu den Services, die Datenereignisse protokollieren, finden Sie unter [Datenereignisse](#).

AWS Service	CloudTrail Themen	Support seit
Amazon API Gateway	<a href="#">API-Management-Aufrufe an Amazon API Gateway protokollieren mit AWS CloudTrail</a>	09.07.2015
Amazon AppFlow	<a href="#">Protokollierung Amazon AppFlow Amazon-API-Aufrufen mit AWS CloudTrail</a>	22.04.2020
Amazon AppStream 2.0	<a href="#">Protokollieren von Amazon AppStream 2.0-API-Aufrufen mit AWS CloudTrail</a>	25.04.2019
Amazon Athena	<a href="#">Protokollieren Amazon Athena Athena-API-Aufrufen mit AWS CloudTrail</a>	19.05.2017

AWS Service	CloudTrail Themen	Support seit
Amazon Aurora	<a href="#">Überwachung von Amazon Aurora Aurora-API-Aufrufen</a> <a href="#">AWS CloudTrail</a>	31.08.2018
Amazon Bedrock	<a href="#">Protokollieren Sie Amazon Bedrock API-Aufrufe mit AWS CloudTrail</a>	23.10.2023
Amazon Braket	<a href="#">Amazon Braket-API-Protokollierung mit CloudTrail</a>	12.08.2020
Amazon Chime	<a href="#">Amazon Chime-Administrationsanrufe protokollieren mit AWS CloudTrail</a>	27.09.2017
Amazon Cloud Directory	<a href="#">Cloud Directory Directory-API-Aufrufe protokollieren mit AWS CloudTrail</a>	26.01.2017
Amazon CloudFront	<a href="#">Wird AWS CloudTrail zur Erfassung von Anfragen verwendet, die an die CloudFront API gesendet wurden</a>	28.05.2014
Amazon CloudSearch	<a href="#">Protokollieren von Amazon CloudSearch Configuration Service-Aufrufen mit AWS CloudTrail</a>	16.10.2014
Amazon CloudWatch	<a href="#">CloudWatchAmazon-API-Aufrufe protokollieren AWS CloudTrail</a>	30.04.2014
CloudWatch Amazon-Protokolle	<a href="#">Protokollierung von Amazon CloudWatch protokolliert API-Aufrufe AWS CloudTrail</a>	10.03.2016

AWS Service	CloudTrail Themen	Support seit
Amazon CodeCatalyst	<a href="#">Protokollierung von CodeCatalyst API-Aufrufen im verbundenen Modus AWS-Konten mit AWS CloudTrail</a>	12/01/2022
CodeGuru Amazon-Rezensent	<a href="#">Protokollieren von Amazon CodeGuru Reviewer-API-Aufrufen mit AWS CloudTrail</a>	02.12.2019
Amazon CodeWhisperer	<a href="#">AWS CloudTrail und CodeWhisperer APIs</a>	13.04.2023
Amazon Cognito	<a href="#">Protokollieren Amazon Cognito Cognito-API-Aufrufen mit AWS CloudTrail</a>	18.02.2016
Amazon Comprehend	<a href="#">Protokollieren von Amazon Comprehend API-Aufrufen mit AWS CloudTrail</a>	17.01.2018
Amazon Comprehend Medical	<a href="#">Protokollieren von Amazon-Comprehend-Medical-API-Aufrufen mithilfe von AWS CloudTrail</a>	27.11.2018
Amazon Connect	<a href="#">Protokollieren von Amazon-Connect-API-Aufrufen mit AWS CloudTrail</a>	11.12.2019
Amazon Data Firehose	<a href="#">Überwachung von Amazon Data Firehose API-Aufrufen mit AWS CloudTrail</a>	17.03.2016
Amazon Data Lifecycle Manager	<a href="#">Protokollieren von Amazon Data Lifecycle Manager-API-Aufrufen mithilfe AWS CloudTrail</a>	24.07.2018



AWS Service	CloudTrail Themen	Support seit
Amazon Detective	<a href="#">Protokollieren von Amazon-Detective-API-Aufrufen mit AWS CloudTrail</a>	31.03.2020
DevOpsAmazon-Guru	<a href="#">Protokollieren von Amazon DevOps Guru-API-Aufrufen mit AWS CloudTrail</a>	04.05.2021
Amazon DocumentDB (mit MongoDB-Kompatibilität)	<a href="#">Protokollieren von Amazon-DocumentDB-API-Aufrufen mit AWS CloudTrail</a>	09.01.2019
Amazon-DynamoDB	<a href="#">Protokollieren von DynamoDB-Vorgängen mithilfe von AWS CloudTrail</a>	28.05.2015
Amazon EC2	<a href="#">Amazon EC2 EC2-API-Aufrufe protokollieren mit AWS CloudTrail</a>	13.11.2013
Amazon EC2 Auto Scaling	<a href="#">Protokollieren von Auto Scaling Scaling-API-Aufrufen mithilfe von CloudTrail</a>	16.07.2014
EC2-Kapazitätsblöcke von Amazon	<a href="#">Kapazität protokollieren Blockiert API-Aufrufe mit AWS CloudTrail</a>	31.10.2023
Amazon EC2 Image Builder	<a href="#">Protokollieren EC2 Image Builder Builder-API-Aufrufen mit CloudTrail</a>	02.12.2019

AWS Service	CloudTrail Themen	Support seit
Amazon Elastic Block Store (Amazon EBS)	<a href="#">Protokollieren von API-Aufrufen mit AWS CloudTrail</a>	Amazon EBS: 13.11.2013
EBS-Direct-APIs	<a href="#">Protokollieren von API-Aufrufen für die EBS-Direct-APIs mit AWS CloudTrail</a>	Direkte EBS-APIs: 30.06.2020
Amazon Elastic Container Registry (Amazon ECR)	<a href="#">Protokollieren von Amazon ECR-API-Aufrufen mithilfe von AWS CloudTrail</a>	21.12.2015
Amazon Elastic Container Service (Amazon ECS)	<a href="#">Protokollieren von Amazon ECS-API-Aufrufen mithilfe von AWS CloudTrail</a>	09.04.2015
Amazon Elastic File System (Amazon EFS)	<a href="#">Protokollieren von Amazon EFS-API-Aufrufen mit AWS CloudTrail</a>	28.06.2016
Amazon Elastic Kubernetes Service (Amazon EKS)	<a href="#">Protokollieren von Amazon EKS-API-Aufrufen mit AWS CloudTrail</a>	05.06.2018
Amazon Elastic Transcoder	<a href="#">Protokollieren Amazon Elastic Transcoder Transcoder-API-Aufrufen mit AWS CloudTrail</a>	27.10.2014
Amazon ElastiCache	<a href="#">Protokollieren Amazon ElastiCache Amazon-API-Aufrufen mit AWS CloudTrail</a>	15.09.2014
Amazon EMR	<a href="#">Amazon EMR-API-Aufrufe protokollieren AWS CloudTrail</a>	04.04.2014
Amazon EMR auf EKS	<a href="#">Protokollieren von Amazon EMR auf EKS-API-Aufrufen mit AWS CloudTrail</a>	12.09.2020

AWS Service	CloudTrail Themen	Support seit
Amazon EventBridge	<a href="#">Protokollieren Amazon EventBridge Amazon-API-Aufrufen mit AWS CloudTrail</a>	11.07.2019
Amazon FinSpace	<a href="#">Logs abfragen AWS CloudTrail</a>	18.10.2022
Amazon Forecast	<a href="#">Protokollieren von Amazon Forecast-API-Aufrufen mit AWS CloudTrail</a>	28.11.2018
Amazon Fraud Detector	<a href="#">Protokollieren von Amazon-Fraud-Detector-API-Aufrufen mit AWS CloudTrail</a>	01.09.2020
Amazon FSx for Lustre	<a href="#">Protokollieren von Amazon FSx for Lustre-API-Aufrufen mit AWS CloudTrail</a>	11.01.2019
Amazon FSx for Windows File Server	<a href="#">Überwachung mit AWS CloudTrail</a>	28.11.2018
Amazon GameLift	<a href="#">GameLift Amazon-API-Aufrufe protokollieren mit AWS CloudTrail</a>	27.01.2016
Amazon GuardDuty	<a href="#">GuardDuty Amazon-API-Aufrufe protokollieren mit AWS CloudTrail</a>	12.02.2018
Amazon Inspector	<a href="#">Protokollieren Amazon Inspector Inspector-API-Aufrufen mit AWS CloudTrail</a>	29.11.2021
Amazon Inspector Classic	<a href="#">Protokollieren von Amazon Inspector Classic API-Aufrufen mit AWS CloudTrail</a>	20.04.2016

AWS Service	CloudTrail Themen	Support seit
Amazon-Inspector-Scan	<a href="#">Amazon Inspector Scaninformationen in CloudTrail</a>	27.11.2023
Amazon Interactive Video Service	<a href="#">Protokollieren von Amazon-IVS-API-Aufrufen mit AWS CloudTrail</a>	15.07.2020
Amazon Kendra	<a href="#">Protokollieren von Amazon Kendra API-Aufrufen mit AWS CloudTrail</a> und <a href="#">Protokollieren von Amazon Kendra Intelligent Ranking API-Aufrufen</a> mit Protokollen AWS CloudTrail	05/11/2020
Amazon Keyspaces (für Apache Cassandra)	<a href="#">Protokollieren von Amazon-Keyspaces-API-Aufrufen mit AWS CloudTrail</a>	13.01.2020
Amazon Managed Service für Apache Flink	<a href="#">Protokollierung von Managed Service für Apache Flink API-Aufrufe mit AWS CloudTrail</a>	22.03.2019
Amazon-Kinesis-Data-Streams	<a href="#">Protokollieren Amazon Kinesis Data Streams Streams-API-Aufrufen mithilfe AWS CloudTrail</a>	25.04.2014
Amazon Kinesis Video Streams	<a href="#">Protokollieren von Kinesis Video Streams Streams-API-Aufrufen mit AWS CloudTrail</a>	24.05.2018
Amazon Lex	<a href="#">Protokollieren von Amazon Lex API-Aufrufen mit CloudTrail</a>	15.08.2017
Amazon Lightsail	<a href="#">Lightsail-API-Aufrufe protokollieren mit AWS CloudTrail</a>	23.12.2016

AWS Service	CloudTrail Themen	Support seit
Amazon Location Service	<a href="#">Protokollierung und Überwachung mit AWS CloudTrail</a>	15.12.2020
Amazon Lookout für Equipment	<a href="#">Überwachung von Amazon Lookout for Equipment</a>	12/01/2020
Amazon Lookout für Metrics	<a href="#">API-Aktivität von Amazon Lookout for Metrics anzeigen in AWS CloudTrail</a>	12/08/2020
Amazon Lookout für Vision	<a href="#">Protokollieren von Amazon-Lookout-for-Vision-Aufrufen mit AWS CloudTrail</a>	12.01.2020
Amazon Machine Learning	<a href="#">Protokollieren von Amazon ML-API-Aufrufen mithilfe von AWS CloudTrail</a>	10.12.2015
Amazon Macie	<a href="#">Protokollieren von Amazon-Macie-API-Aufrufen mithilfe von AWS CloudTrail</a>	05/13/2020
Amazon Managed Blockchain	<a href="#">Protokollieren von Amazon-Managed-Blockchain-API-Aufrufen mit AWS CloudTrail</a>  <a href="#">Protokollierung von Ethereum für Managed-Blockchain-API-Aufrufe mit AWS CloudTrail (Vorschau)</a>	04/01/2019
Amazon Managed Grafana	<a href="#">Protokollieren von Amazon-Managed-Grafana-API-Aufrufen mit AWS CloudTrail</a>	15.12.2020

AWS Service	CloudTrail Themen	Support seit
Amazon Managed Service für Prometheus	<a href="#">Protokollieren von Amazon Managed Service für Prometheus-API-Aufrufe mithilfe von AWS CloudTrail</a>	15.12.2020
Amazon Managed Streaming für Apache Kafka	<a href="#">API-Aufrufe protokollieren mit AWS CloudTrail</a>	11.12.2018
Amazon Managed Workflows für Apache Airflow	<a href="#">Audit-Logs anzeigen in AWS CloudTrail</a>	24.11.2020
Amazon MemoryDB für Redis	<a href="#">Protokollieren von Amazon MemoryDB for Redis-API-Aufrufen mit AWS CloudTrail</a>	19.08.2021
Amazon MQ	<a href="#">Protokollieren Amazon MQ MQ-API-Aufrufen mithilfe von AWS CloudTrail</a>	19.07.2018
Amazon Neptune	<a href="#">Protokollieren Amazon Neptune Neptune-API-Aufrufen mit AWS CloudTrail</a>	30.05.2018
Amazon Nimble Studio	<a href="#">Protokollieren von Nimble Studio-Aufrufen mit AWS CloudTrail</a>	19.06.2023
Amazon One Enterprise	<a href="#">Protokollieren von Amazon One Enterprise API-Aufrufen mit AWS CloudTrail</a>	27.11.2023
OpenSearch Amazon-Dienst	<a href="#">Überwachung von Amazon OpenSearch Service API-Aufrufen mit AWS CloudTrail</a>	01.10.2015

AWS Service	CloudTrail Themen	Support seit
Amazon Personalize	<a href="#">Protokollieren Amazon Personalize Personalize-API-Aufrufen mit AWS CloudTrail</a>	28.11.2018
Amazon Pinpoint	<a href="#">Protokollieren von Amazon Pinpoint API-Aufrufen mit AWS CloudTrail</a>	06.02.2018
Amazon-Pinpoint-SMS- und - Sprachnachrichten-API	<a href="#">Protokollieren von Amazon Pinpoint API-Aufrufen mit AWS CloudTrail</a>	16.11.2018
Amazon Polly	<a href="#">Protokollieren von Amazon Polly API-Aufrufen mit AWS CloudTrail</a>	30.11.2016
Amazon Q (für geschäftliche Nutzung)	<a href="#">Protokollieren von Amazon Q-API-Aufrufen mit AWS CloudTrail</a>	28.11.2023
Amazon Q (zur Verwendung in AWS Builder)	<a href="#">Protokollieren von Amazon Q-API-Aufrufen mit AWS CloudTrail</a>	28.11.2023
Amazon Quantum Ledger Database (Amazon QLDB)	<a href="#">Protokollieren von Amazon-QLDB-API-Aufrufen mit AWS CloudTrail</a>	10.09.2019
Amazon QuickSight	<a href="#">Vorgänge protokollieren mit CloudTrail</a>	28.04.2017
Amazon Relational Database Service (Amazon RDS)	<a href="#">Protokollieren von Amazon RDS-API-Aufrufen mithilfe von AWS CloudTrail</a>	13.11.2013

AWS Service	CloudTrail Themen	Support seit
Amazon RDS Performance Insights	<a href="#">Protokollieren von Amazon RDS-API-Aufrufen mithilfe von AWS CloudTrail</a>  Die Amazon-RDS-Performance-Insights-API ist ein Subsatz der Amazon-RDS-API.	21.06.2018
Amazon-Redshift	<a href="#">Protokollieren Amazon Redshift Redshift-API-Aufrufen mit AWS CloudTrail</a>	10.06.2014
Amazon Rekognition	<a href="#">Protokollieren Amazon Rekognition Rekognition-API-Aufrufen mit AWS CloudTrail</a>	06.04.2018
Amazon Route 53	<a href="#">Verwenden von AWS CloudTrail zum Erfassen von an die Route-53-API gesendeten Anforderungen</a>	11.02.2015
Amazon Route 53 Application Recovery Controller	<a href="#">Protokollieren von Amazon Route 53 Application Recovery Controller-API-Aufrufen mithilfe von AWS CloudTrail</a>	27.07.2021
Amazon S3	<a href="#">Protokollieren von Amazon S3 S3-API-Aufrufen mithilfe von AWS CloudTrail</a>	Verwaltungsereignisse: 01.09.2015  Datenereignisse: 21.11.2016
Amazon S3 Glacier	<a href="#">Protokollieren von S3 Glacier-API-Aufrufen mithilfe von AWS CloudTrail</a>	11.12.2014



AWS Service	CloudTrail Themen	Support seit
Amazon SageMaker	<a href="#">SageMaker Amazon-API-Aufrufe protokollieren mit AWS CloudTrail</a>	11.01.2018
Amazon Security Lake	<a href="#">Protokollieren von Amazon Security Lake-API-Aufrufen mit CloudTrail</a>	30.05.2023
Amazon Simple Email Service (Amazon SES)	<a href="#">Protokollieren von Amazon SES SES-API-Aufrufen mithilfe von AWS CloudTrail</a>	07.05.2015
Amazon-Simple-Notification-Service (Amazon-SNS)	<a href="#">Protokollieren Amazon SNS SNS-API-Aufrufen mit AWS CloudTrail</a>	09.10.2014
Amazon-Simple-Queue-Service (Amazon SQS)	<a href="#">Protokollieren Amazon SQS SQS-API-Aktionen mithilfe von AWS CloudTrail</a>	16.07.2014
Amazon Simple Workflow Service (Amazon SWF)	<a href="#">API-Aufrufe aufzeichnen mit AWS CloudTrail</a>	Management-Veranstaltungen: 13.05.2014  Datenereignisse: 14.02.2024
Amazon Textract	<a href="#">Protokollieren Amazon Textract Textract-API-Aufrufen mit AWS CloudTrail</a>	29. 05. 2019
Amazon Timestream	<a href="#">Protokollieren von Timestream-API-Aufrufen mit AWS CloudTrail</a>	30.09.2020
Amazon Transcribe	<a href="#">Protokollieren von Amazon Transcribe API-Aufrufen mit AWS CloudTrail</a>	28.06.2018

AWS Service	CloudTrail Themen	Support seit
Amazon Translate	<a href="#">Protokollieren von Amazon-Translate-API-Aufrufen mit AWS CloudTrail</a>	04.04.2018
Amazon Verified Permissions	<a href="#">Protokollieren von API-Aufrufen von Amazon Verified Permissions mit AWS CloudTrail</a>	13.06.2023
Amazon Virtual Private Cloud (Amazon VPC)	<a href="#">API-Aufrufe protokollieren mit AWS CloudTrail</a>  Die Amazon-VPC-API ist ein Teilbereich der Amazon-EC2-API.	13.11.2013
Amazon VPC Lattice	<a href="#">CloudTrail protokolliert</a>	31.03.2023
Amazon VPC Reachability Analyzer	<a href="#">Protokollieren von Reachability Analyzer-API-Aufrufen mit AWS CloudTrail</a>	27.11.2023
Amazon WorkDocs	<a href="#">Protokollieren von WorkDocs Amazon-API-Aufrufen mithilfe von AWS CloudTrail</a>	27.08.2014
Amazon WorkMail	<a href="#">Protokollieren Amazon WorkMail Amazon-API-Aufrufen mit AWS CloudTrail</a>	12.12.2017
Amazon WorkSpaces	<a href="#">Protokollieren von WorkSpaces Amazon-API-Aufrufen mithilfe von CloudTrail</a>	09.04.2015
Amazon WorkSpaces Thin Client	<a href="#">Protokollieren von Amazon WorkSpaces Thin Client-API-Aufrufen mit AWS CloudTrail</a>	26.11.2023

AWS Service	CloudTrail Themen	Support seit
Amazon WorkSpaces Web	<a href="#">Protokollieren von Amazon WorkSpaces Web API-Aufrufen mit AWS CloudTrail</a>	30.11.2021
Application Auto Scaling	<a href="#">Protokollieren von Auto Scaling-API-Aufrufen von Anwendungen mit AWS CloudTrail</a>	31.10.2016
AWS Amplify	<a href="#">Protokollieren von Amplify-API-Aufrufen mithilfe von AWS CloudTrail</a>	30.11.2020
AWS App Mesh	<a href="#">Protokollieren von App-Mesh-API-Aufrufen mit AWS CloudTrail</a>	AWS App Mesh 30.10.2019 App Mesh Envoy Management Service 18.3.2022
AWS App Runner	<a href="#">App Runner API-Aufrufe protokollieren mit AWS CloudTrail</a>	18.05.2021
AWS AppConfig	<a href="#">Protokollierung von AWS AppConfig API-Aufrufen mit AWS CloudTrail</a>	Management-Ereignisse: 31.07.2020  Datenereignisse: 01.04.2024
AWS AppFabric	<a href="#">Protokollierung von AWS AppFabric API-Aufrufen mit AWS CloudTrail</a>	27.06.2023
AWS Cost Profiler für Anwendungen	<a href="#">AWS API-Referenz für Application Cost Profiler</a>	13.05.2021
AWS Application Discovery Service	<a href="#">Protokollieren von API-Aufrufen mit Application Discovery Service mit AWS CloudTrail</a>	12.05.2016

AWS Service	CloudTrail Themen	Support seit
AWS Service zur Transformation von Anwendungen	(Backend-Dienst, der von AWS Tools wie AWS Microservice Extractor für .NET verwendet wird)	26.08.2023
AWS AppSync	<a href="#">AWS AppSync API-Aufrufe protokollieren mit AWS CloudTrail</a>	13.02.2018
AWS Artifact	<a href="#">AWS Artifact API-Aufrufe protokollieren mit AWS CloudTrail</a>	27.01.2023
AWS Audit Manager	<a href="#">AWS Audit Manager API-Aufrufe protokollieren mit AWS CloudTrail</a>	12/07/2020
AWS Auto Scaling	<a href="#">Protokollieren von AWS Auto Scaling API-Aufrufen mithilfe von CloudTrail</a>	15.08.2018
AWS B2B-Datenaustausch	<a href="#">Protokollierung von API-Aufrufen für den AWS B2B-Datenaustausch mit AWS CloudTrail</a>	01.12.2023
AWS Backup	<a href="#">AWS Backup API-Aufrufe protokollieren mit AWS CloudTrail</a>	04.02.2019
AWS Batch	<a href="#">AWS Batch API-Aufrufe protokollieren mit AWS CloudTrail</a>	10.01.2018
AWS Billing and Cost Management	<a href="#">AWS Billing and Cost Management API-Aufrufe protokollieren mit AWS CloudTrail</a>	07.06.2018

AWS Service	CloudTrail Themen	Support seit
AWS Billing Conductor	<a href="#">AWS Billing Conductor API-Aufrufe protokollieren mit AWS CloudTrail</a>	12.03.2024
AWS BugBust	<a href="#">Protokollierung von BugBust API-Aufrufen mit CloudTrail</a>	24.06.2021
AWS Certificate Manager	<a href="#">Verwenden von AWS CloudTrail</a>	25.03.2016
AWS Clean Rooms	<a href="#">Protokollierung von AWS Clean Rooms API-Aufrufen mit AWS CloudTrail</a>	21.03.2023
AWS Cloud Map	<a href="#">AWS Cloud Map API-Aufrufe protokollieren mit AWS CloudTrail</a>	28.11.2018
AWS Cloud9	<a href="#">AWS Cloud9 API-Aufrufe protokollieren mit AWS CloudTrail</a>	21.01.2019
AWS CloudFormation	<a href="#">AWS CloudFormation API-Aufrufe protokollieren AWS CloudTrail</a>	02.04.2014
AWS CloudHSM	<a href="#">Protokollieren von AWS CloudHSM API-Aufrufen mithilfe von AWS CloudTrail</a>	08.01.2015
AWS CloudShell	<a href="#">Einloggen und Überwachen AWS CloudShell</a>	15.12.2020
AWS CloudTrail	<a href="#">AWS CloudTrail API-Referenz</a> (Alle CloudTrail API-Aufrufe werden von CloudTrail protokolliert.)	13.11.2013

AWS Service	CloudTrail Themen	Support seit
AWS CodeArtifact	<a href="#">CodeArtifact API-Aufrufe protokollieren mit AWS CloudTrail</a>	10.06.2020
AWS CodeBuild	<a href="#">AWS CodeBuild API-Aufrufe protokollieren mit AWS CloudTrail</a>	01.12.2016
AWS CodeCommit	<a href="#">AWS CodeCommit API-Aufrufe protokollieren mit AWS CloudTrail</a>	11.01.2017
AWS CodeDeploy	<a href="#">Bereitstellungen überwachen mit AWS CloudTrail</a>	16.12.2014
AWS CodePipeline	<a href="#">Protokollierung von CodePipeline API-Aufrufen mit AWS CloudTrail</a>	09.07.2015
AWS CodeStar	<a href="#">AWS CodeStar API-Aufrufe protokollieren mit AWS CloudTrail</a>	14.06.2017
AWS CodeStar Benachrichtigungen	<a href="#">API-Aufrufe für AWS CodeStar Benachrichtigungen protokollieren mit AWS CloudTrail</a>	11.05.2019
AWS Config	<a href="#">AWS Config API-Aufrufe protokollieren von mit AWS CloudTrail</a>	10.02.2015
AWS Steuerkatalog	<a href="#">Protokollierung von AWS Control Catalog-API-Aufrufen mit AWS CloudTrail</a>	08.04.2024

AWS Service	CloudTrail Themen	Support seit
AWS Control Tower	<a href="#">Aktionen protokollieren AWS Control Tower mit AWS CloudTrail</a>	12.08.2019
AWS Data Pipeline	<a href="#">Protokollieren von AWS Data Pipeline API-Aufrufen mithilfe von AWS CloudTrail</a>	02.12.2014
AWS Database Migration Service (AWS DMS)	<a href="#">Protokollieren von AWS Database Migration Service API-Aufrufen mit AWS CloudTrail</a>	04.02.2016
AWS DataSync	<a href="#">AWS DataSync API-Aufrufe protokollieren mit AWS CloudTrail</a>	26.11.2018
AWS Deadline Cloud	<a href="#">Anrufe protokollieren mit CloudTrail</a>	04/02/2024
AWS Device Farm	<a href="#">Protokollieren von AWS Device Farm API-Aufrufen mithilfe von AWS CloudTrail</a>	13.07.2015
AWS Direct Connect	<a href="#">AWS Direct Connect API-Aufrufe protokollieren AWS CloudTrail</a>	08.03.2014
AWS Directory Service	<a href="#">Protokollieren von AWS Directory Service API-Aufrufen mithilfe von CloudTrail</a>	14.05.2015
AWS Elastic Beanstalk (Elastic Beanstalk)	<a href="#">Verwenden von Elastic Beanstalk Beanstalk-API-Aufrufen mit AWS CloudTrail</a>	31.03.2014

AWS Service	CloudTrail Themen	Support seit
AWS Elastic Disaster Recovery	<a href="#">Protokollieren von AWS Elastic Disaster Recovery API-Aufrufen mit AWS CloudTrail</a>	17.11.2021
AWS Elemental MediaConnect	<a href="#">AWS Elemental MediaConnect API-Aufrufe protokollieren mit AWS CloudTrail</a>	27.11.2018
AWS Elemental MediaConvert	<a href="#">AWS Elemental MediaConvert API-Aufrufe protokollieren mit CloudTrail</a>	27.11.2017
AWS Elemental MediaLive	<a href="#">MediaLiveAPI-Aufrufe protokollieren mit AWS CloudTrail</a>	19.01.2019
AWS Elemental MediaPackage	<a href="#">AWS Elemental MediaPackage API-Aufrufe protokollieren mit AWS CloudTrail</a>	21.12.2018
AWS Elemental MediaStore	<a href="#">AWS Elemental MediaStore API-Aufrufe protokollieren mit CloudTrail</a>	27.11.2017
AWS Elemental MediaTailor	<a href="#">AWS Elemental MediaTailor API-Aufrufe protokollieren mit AWS CloudTrail</a>	11.02.2019
AWS Auflösung der Entität	<a href="#">Protokollieren von API-Aufrufen zur AWS Entitätsauflösung mit A AWS CloudTrail</a>	26.07.2023
AWS Fault Injection Service	<a href="#">API-Aufrufe protokollieren mit AWS CloudTrail</a>	15.03.2021



AWS Service	CloudTrail Themen	Support seit
AWS Firewall Manager	<a href="#">AWS Firewall Manager API-Aufrufe protokollieren mit AWS CloudTrail</a>	05.04.2018
AWS Global Accelerator	<a href="#">Loggen von AWS Global Accelerator-API-Aufrufen mit AWS CloudTrail</a>	26.11.2018
AWS Glue	<a href="#">AWS Glue Vorgänge protokollieren mit AWS CloudTrail</a>	07.11.2017
AWS Ground Station	<a href="#">AWS Ground Station API-Aufrufe protokollieren mit AWS CloudTrail</a>	31.05.2019
AWS Health	<a href="#">AWS Health API-Aufrufe protokollieren mit AWS CloudTrail</a>	21.11.2016
AWS Health Dashboard	<a href="#">AWS Health API-Aufrufe protokollieren mit AWS CloudTrail</a>	01.12.2016
AWS HealthImaging	<a href="#">AWS HealthImaging API-Aufrufe protokollieren mit AWS CloudTrail</a>	26.07.2023
AWS HealthLake	<a href="#">AWS HealthLake API-Aufrufe protokollieren mit AWS CloudTrail</a>	12/07/2020
AWS HealthOmics	<a href="#">Protokollierung von AWS HealthOmics API-Aufrufen mit AWS CloudTrail</a>	29.11.2022

AWS Service	CloudTrail Themen	Support seit
AWS IAM Identity Center	<a href="#">Protokollieren von IAM Identity Center-API-Aufrufen mit AWS CloudTrail</a>	07.12.2017
AWS Identity and Access Management (IAM)	<a href="#">Protokollieren von IAM-Ereignissen mit AWS CloudTrail</a>	13.11.2013
AWS IoT	<a href="#">Protokollieren von AWS IoT API-Aufrufen mit AWS CloudTrail</a>	11.04.2016
AWS IoT 1-Click	<a href="#">AWS IoT 1-Click API-Aufrufe protokollieren mit AWS CloudTrail</a>	14.05.2018
AWS IoT Analytik	<a href="#">AWS IoT Analytics-API-Aufrufe protokollieren mit AWS CloudTrail</a>	23.04.2018
AWS IoT Events	<a href="#">API-Aufrufe für AWS IoT Ereignisse protokollieren mit AWS CloudTrail</a>	11. 06. 2019
AWS IoT Greengrass	<a href="#">AWS IoT Greengrass API-Aufrufe protokollieren mit AWS CloudTrail</a>	29.10.2018
AWS IoT Greengrass V2	<a href="#">Loggen Sie AWS IoT Greengrass V2-API-Aufrufe mit AWS CloudTrail</a>	14.12.2020
AWS IoT SiteWise	<a href="#">AWS IoT SiteWise API-Aufrufe protokollieren mit AWS CloudTrail</a>	04/29/2020

AWS Service	CloudTrail Themen	Support seit
AWS Key Management Service (AWS KMS)	<a href="#">AWS KMS API-Aufrufe protokollieren mit AWS CloudTrail</a>	12.11.2014
AWS Lake Formation	<a href="#">AWS Lake Formation API-Aufrufe protokollieren mit AWS CloudTrail</a>	08/09/2019
AWS Lambda	<a href="#">Protokollieren von AWS Lambda API-Aufrufen mithilfe von AWS CloudTrail</a>	Verwaltungsereignisse: 09.04.2015  Datenereignisse: 30.11.2017
AWS Launch Wizard	<a href="#">Protokollieren von AWS Launch Wizard API-Aufrufen mit AWS CloudTrail</a>	11.08.2023
AWS License Manager	<a href="#">Protokollieren von AWS License Manager Manager-API-Aufrufen mit AWS CloudTrail</a>	01.03.2019
AWS Mainframe Modernization	<a href="#">Protokollieren von AWS Mainframe Modernization API-Aufrufen mit AWS CloudTrail</a>	08.06.2022
AWS Managed Services	<a href="#">Protokollverwaltung in AMS Accelerate</a>	21.12.2016
AWS Marketplace Vereinbarungen	<a href="#">API-Aufrufe für Vereinbarungen protokollieren mit AWS CloudTrail</a>	09/01/2023
AWS Marketplace Bereitstellungsservice	<a href="#">AWS Marketplace Deployment Service-Aufrufe protokollieren mit CloudTrail</a>	29.11.2023

AWS Service	CloudTrail Themen	Support seit
AWS Marketplace Entdeckung	<a href="#">Protokollieren von AWS Marketplace Discovery-API-Aufrufen mit AWS CloudTrail</a>	15.12.2022
AWS Marketplace Messdienst	<a href="#">Protokollierung von AWS Marketplace API-Aufrufen mit AWS CloudTrail</a>	22. 08. 2018
AWS Migration Hub	<a href="#">Protokollieren von AWS Migration Hub Hub-API-Aufrufen mit AWS CloudTrail</a>	14.08.2017
AWS Network Firewall	<a href="#">Aufrufe an die AWS Network Firewall API protokollieren mit AWS CloudTrail</a>	17.11.2020
AWS OpsWorks for Chef Automate	<a href="#">AWS OpsWorks for Chef Automate API-Aufrufe protokollieren mit AWS CloudTrail</a>	16.07.2018
AWS OpsWorks for Puppet Enterprise	<a href="#">Protokollierung OpsWorks von Puppet Enterprise API-Aufrufen mit AWS CloudTrail</a>	16.07.2018
AWS OpsWorks Stacks	<a href="#">AWS OpsWorks Stacks API-Aufrufe protokollieren mit AWS CloudTrail</a>	04.06.2014
AWS Organizations	<a href="#">AWS Organizations API-Aufrufe protokollieren mit AWS CloudTrail</a>	27.02.2017
AWS Outposts	<a href="#">AWS Outposts API-Aufrufe protokollieren mit AWS CloudTrail</a>	04/02/2020

AWS Service	CloudTrail Themen	Support seit
AWS Panorama	<a href="#">AWS Panorama API Referenz</a>	20.10.2021
AWS Payment Cryptography	<a href="#">Protokollierung von AWS Payment Cryptography API-Aufrufen mit AWS CloudTrail</a>	08.06.2023
AWS Privates 5G	<a href="#">Protokollierung von AWS privaten 5G-API-Aufrufen mit AWS CloudTrail</a>	11.08.2022
AWS Private Certificate Authority (AWS Private CA)	<a href="#">Verwenden CloudTrail</a>	04.04.2018
AWS Proton	<a href="#">Einloggen und Überwachen AWS Proton</a>	09.06.2021
AWS re:Post Privat	<a href="#">AWS re:Post Private API-Aufrufe protokollieren mit AWS CloudTrail</a>	26.11.2023
AWS Resilience Hub	<a href="#">AWS CloudTrail</a>	10.11.2021
AWS Resource Access Manager (AWS RAM)	<a href="#">AWS RAM API-Aufrufe protokollieren mit AWS CloudTrail</a>	20.11.2018
AWS Ressourcen Explorer	<a href="#">AWS Ressourcen Explorer API-Aufrufe protokollieren mit AWS CloudTrail</a>	11.07.2022
AWS Resource Groups	<a href="#">Protokollierung und Überwachung in Resource Groups</a>	29.06.2018
AWS RoboMaker	<a href="#">Protokollierung von AWS RoboMaker API-Aufrufen mit AWS CloudTrail</a>	16.01.2019

AWS Service	CloudTrail Themen	Support seit
AWS Secrets Manager	<a href="#">Überwachen Sie die Verwendung Ihrer AWS Secrets Manager Geheimnisse</a>	05.04.2018
AWS Security Hub	<a href="#">AWS Security Hub API-Aufrufe protokollieren mit AWS CloudTrail</a>	27.11.2018
AWS Security Token Service (AWS STS)	<a href="#">Protokollieren von IAM-Ereignissen mit AWS CloudTrail</a>  Das IAM-Thema enthält Informationen für. AWS STS	13.11.2013
AWS Serverless Application Repository	<a href="#">Protokollieren von AWS Serverless Application Repository API-Aufrufen mit AWS CloudTrail</a>	20.02.2018
AWS Service Catalog	<a href="#">Protokollieren von Service Catalog-API-Aufrufen mit AWS CloudTrail</a>	06.07.2016
AWS Shield	<a href="#">Protokollierung von Shield Advanced API-Aufrufen mit AWS CloudTrail</a>	08.02.2018
AWS Snowball Edge	<a href="#">AWS Snowball Edge-API-Aufrufe protokollieren mit AWS CloudTrail</a>	25.01.2019
AWS Step Functions	<a href="#">AWS Step Functions API-Aufrufe protokollieren mit AWS CloudTrail</a>	01.12.2016

AWS Service	CloudTrail Themen	Support seit
AWS Storage Gateway	<a href="#">Protokollieren von Storage Gateway Gateway-API-Aufrufen mithilfe von AWS CloudTrail</a>	16.12.2014
AWS Support	<a href="#">Protokollieren von AWS Support API-Aufrufen mit AWS CloudTrail</a>	21.04.2016
AWS Support Empfehlungen (Vorschau)	<a href="#">API-Aufrufe AWS Support für Empfehlungen protokollieren mit AWS CloudTrail</a>	22.05.2024
AWS Systems Manager	<a href="#">AWS Systems Manager API-Aufrufe protokollieren mit AWS CloudTrail</a>	29.11.2017
AWS Systems Manager Incident Manager	<a href="#">Protokollieren von AWS Systems Manager Incident Manager-API-Aufrufen mit AWS CloudTrail</a>	05/10/2021
AWS Telco Network Builder (TNB)AWS	<a href="#">Protokollieren von AWS Telco Network Builder-API-Aufrufen mit AWS CloudTrail</a>	21.02.2023
AWS Transfer for SFTP	<a href="#">AWS Transfer for SFTP API-Aufrufe protokollieren mit AWS CloudTrail</a>	08.01.2019
AWS Transit Gateway	<a href="#">Protokollieren von API-Aufrufen für Ihr Transit Gateway mit AWS CloudTrail</a>	26.11.2018
AWS Trusted Advisor	<a href="#">AWS Trusted Advisor Konsolenaktionen protokollieren mit AWS CloudTrail</a>	22.10.2020

AWS Service	CloudTrail Themen	Support seit
AWS Verified Access	<a href="#">AWS Verified Access API-Aufrufe protokollieren mit AWS CloudTrail</a>	27.04.2023
AWS WAF	<a href="#">AWS WAF API-Aufrufe protokollieren mit AWS CloudTrail</a>	28.04.2016
AWS Well-Architected Tool	<a href="#">AWS Well-Architected Tool API-Aufrufe protokollieren mit AWS CloudTrail</a>	15.12.2020
AWS X-Ray	<a href="#">AWS X-Ray API-Aufrufe protokollieren mit CloudTrail</a>	25.04.2018
Elastic Load Balancing	<a href="#">AWS CloudTrail Protokollierung für Ihren Classic Load Balancer</a> und <a href="#">AWS CloudTrail Protokollierung für Ihren Application Load Balancer</a>	04.04.2014
FreeRTOS-Over-the-Air-Updates (OTA)	<a href="#">Protokollieren von AWS IoT OTA-API-Aufrufen mit AWS CloudTrail</a>	22. 05. 2019
Service Quotas	<a href="#">Protokollieren von API-Aufrufen Service Quotas mithilfe von AWS CloudTrail</a>	24.06.2019

## CloudTrail nicht unterstützte Dienste

Services, die sich noch in der Vorschauversion befinden oder noch nicht für die allgemeine Verfügbarkeit (GA) freigegeben sind oder für die es keine öffentlichen APIs gibt, gelten als nicht unterstützt.

Darüber hinaus werden die folgenden AWS Dienste und Ereignisse nicht unterstützt:



- AWS Import/Export
- Richtlinienspezifische Ereignisse für Amazon-VPC-Endpunkte

Eine Liste der unterstützten AWS Dienste finden Sie unter [AWS Servicethemen für CloudTrail](#).

## Kontingente in AWS CloudTrail

In der folgenden Tabelle werden die Kontingente (früher als Grenzwerte bezeichnet) innerhalb dieser Grenzen beschrieben CloudTrail. CloudTrail hat keine einstellbaren Kontingente. Informationen zu anderen Kontingenten finden Sie unter [AWS Servicekontingenten](#). AWS

Ressource	Standardkontingent	Kommentare
Trails pro Region	5	Dieses Kontingent kann nicht erhöht werden.
Abrufen, Beschreiben und Aufführen von APIs	10 Transaktionen pro Sekunde (TPS)	Die maximale Anzahl der Operationsanforderungen, die Sie pro Sekunde ohne Drosselung senden können. Die StartQuery APIs CancelQuery LookupEvents ListInsightsMetric Data ,PutAuditEvents , und sind in dieser Kategorie nicht enthalten.
CancelQuery, StartQuery APIs	3 Transaktionen pro Sekunde (TPS)	Die maximale Anzahl der Operationsanforderungen, die Sie pro Sekunde ohne Drosselung senden können.  Dieses Kontingent kann nicht erhöht werden.

Ressource	Standardkontingent	Kommentare
LookupEvents API	2 Transaktionen pro Sekunde (TPS)	Die maximale Anzahl der Operationsanforderungen, die Sie pro Sekunde ohne Drosselung senden können.  Dieses Kontingent kann nicht erhöht werden.
ListInsightsMetricData API	1 Transaktion pro Sekunde (TPS)	Die maximale Anzahl der Operationsanforderungen, die Sie pro Sekunde ohne Drosselung senden können.  Dieses Kontingent kann nicht erhöht werden.
PutAuditEvents API	100 Transaktionen pro Sekunde (TPS)	Die maximale Anzahl der Operationsanforderungen, die Sie pro Sekunde ohne Drosselung senden können.  Dieses Kontingent kann nicht erhöht werden.
Alle weiteren APIs	1 Transaktion pro Sekunde (TPS)	Die maximale Anzahl der Operationsanforderungen, die Sie pro Sekunde ohne Drosselung senden können.  Dieses Kontingent kann nicht erhöht werden.

Ressource	Standardkontingent	Kommentare
Ereignisdatenspeicher	10	<p>Die maximale Anzahl von Ereignisdatenspeichern, die Sie in einem beliebigen AWS-Region haben können. Dazu gehören sowohl Ereignisdatenspeicher mit einer Region als auch alle Ereignisdatenspeicher mit mehreren Regionen für alle AWS-Regionen. Dies schließt Ereignisdatenspeicher in jeder <a href="#">Lebenszyklusphase</a> ein.</p> <p>Dieses Kontingent kann nicht erhöht werden.</p>
Kanäle	25	<p>Dieses Kontingent gilt für Kanäle, die für CloudTrail Lake-Integrationen mit Ereignisquellen außerhalb von verwendet werden AWS, und gilt nicht für serviceverknüpfte Kanäle.</p> <p>Dieses Kontingent kann nicht erhöht werden.</p>
Gleichzeitige Abfragen	10	<p>Die maximale Anzahl von Abfragen in der Warteschlange oder laufenden Abfragen, die Sie gleichzeitig in Lake ausführen können. CloudTrail</p> <p>Dieses Kontingent kann nicht erhöht werden.</p>

Ressource	Standardkontingent	Kommentare
Ereignisse pro Anfrage PutAuditEvents	100	<p>Sie können bis zu 100 Aktivität ereignisse (oder bis zu 1 MB) pro PutAuditEvents - Anforderung hinzufügen.</p> <p>Dieses Kontingent kann nicht erhöht werden.</p>
Ereignisauswahlen	5 pro Trail	Dieses Kontingent kann nicht erhöht werden.
Erweiterte Ereignisauswahlen	500 Bedingungen für alle erweiterten Ereignisauswahlen	<p>Wenn ein Trail oder ein Ereignisdatenspeicher erweiterte Ereignisselektoren verwendet, sind maximal 500 Gesamtwerte für alle Bedingungen in allen erweiterten Ereignisselektoren zulässig. Sofern ein Trail- oder Ereignisdatenspeicher nicht Datenereignisse auf allen Ressourcen protokolliert, wie beispielsweise alle S3-Buckets oder alle Lambda-Funktionen, sind Sie auf 250 Datenressourcen beschränkt. Die Datenressourcen können über Ereignisauswahlen verteilt werden, aber die Gesamtanzahl darf den Wert von 250 nicht überschreiten.</p> <p>Dieses Kontingent kann nicht erhöht werden.</p>

Ressource	Standardkontingent	Kommentare
Data-Ressourcen in Ereignisauswahlen	250 in allen Ereignisauswahlen in einem Trail	<p>Wenn Sie Datenereignisse mithilfe von Ereignisauswahlen oder erweiterten Ereignisauswahlen einschränken, darf die Gesamtanzahl der Datenressourcen 250 für alle Ereignisauswahlen in einem Trail nicht übersteigen. Die maximale Anzahl von Ressourcen in einer einzelnen Ereignisauswahl auf bis zu 250 eingestellt werden. Diese Obergrenze ist nur zulässig, wenn die Gesamtanzahl der Daten-Ressourcen in allen Ereignisauswahlen nicht 250 übersteigt.</p> <p>Beispiele:</p> <ul style="list-style-type: none"><li>• Ein Trail mit 5 Ereignisauswahlen, von denen jede auf 50 Daten-Ressourcen eingestellt ist, ist zulässig. (<math>5 \times 50 = 250</math>)</li><li>• Ein Trail mit 5 Ereignisauswahlen, von denen 3 mit 50 Daten-Ressourcen, 1 mit 99 Daten-Ressourcen und 1 mit 1 Daten-Ressource konfiguriert ist, ist ebenfalls zulässig. (<math>(3 \times 50) + 1 + 99 = 250</math>)</li><li>• Ein Trail mit 5 Ereignisauswahlen, von denen alle mit 100 Daten-Ressourcen</li></ul>

Ressource	Standardkontingent	Kommentare
		<p data-bbox="1101 212 1458 296">konfiguriert sind, ist nicht zulässig. (5*100=500)</p> <p data-bbox="1068 373 1484 594">Ereignisselektoren gelten nur für Trails. Sie müssen für Ereignisdatenspeicher erweiterte Ereignisselektoren verwenden.</p> <p data-bbox="1068 642 1484 726">Dieses Kontingent kann nicht erhöht werden.</p> <p data-bbox="1068 774 1503 995">Das Kontingent gilt nicht, wenn Sie Datenereignisse für alle Ressourcen protokollieren möchten, z. B. alle S3-Buckets oder alle Lambda-Funktionen.</p>

Ressource	Standardkontingent	Kommentare
Ereignis-Größe	<p>Alle Ereignisversionen: Ereignisse mit mehr als 256 KB können nicht an CloudWatch Logs gesendet werden</p> <p>Ereignisversion 1.05 und neuer: Gesamtereignisgrößenbeschränkung von 256 KB</p>	<p>Amazon CloudWatch Logs und Amazon EventBridge erlauben jeweils eine maximale Eventgröße von 256 KB. CloudTrail sendet keine Ereignisse über 256 KB an CloudWatch Logs oder EventBridge.</p> <p>Beginnend mit der Ereignisversion 1.05 haben Ereignisse eine maximale Größe von 256 KB. Dies soll dazu beitragen, die Ausnutzung durch böswillige Akteure zu verhindern und die Nutzung von Ereignissen durch andere AWS Dienste wie CloudWatch Logs und EventBridge zu ermöglichen.</p>
CloudTrail an Amazon S3 gesendete Dateigröße	50 MB ZIP-Datei, nach der Komprimierung	<p>CloudTrail sendet Ereignisse sowohl für Verwaltungs- als auch für Datenereignisse in maximal 50 MB (komprimierten) ZIP-Dateien an S3.</p> <p>Wenn die Option „On the Trail“ aktiviert ist, werden Protokollzustellungsbenachrichtigungen von Amazon SNS gesendet, nachdem ZIP-Dateien an S3 CloudTrail gesendet wurden.</p>

# Erste Schritte mit AWS CloudTrail Tutorials

Wenn Sie noch nicht damit vertraut sind AWS CloudTrail, können Ihnen diese Tutorials dabei helfen, die Funktionen zu nutzen.

## Themen

- [Erteilen Sie Nutzungsberechtigungen CloudTrail](#)
- [Event-Historie anzeigen](#)
- [Erstellen Sie einen Pfad, um Verwaltungsereignisse zu protokollieren](#)
- [Erstellen Sie einen Ereignisdatenspeicher für S3-Datenereignisse](#)
- [Kopieren Sie Trail-Ereignisse in einen CloudTrail Lake-Event-Datenspeicher](#)
- [Lake-Dashboards anzeigen CloudTrail](#)
- [CloudTrail Lake-Beispielabfragen anzeigen und ausführen](#)
- [Speichern Sie die CloudTrail Lake-Abfrageergebnisse in einem S3-Bucket](#)

## Erteilen Sie Nutzungsberechtigungen CloudTrail

Um CloudTrail Ressourcen wie Pfade, Veranstaltungsdatenpeicher und Kanäle zu erstellen, zu aktualisieren und zu verwalten, müssen Sie Nutzungsberechtigungen erteilen CloudTrail. Dieser Abschnitt enthält Informationen zu den verwalteten Richtlinien, die für verfügbar sind CloudTrail.

### Note

Die Berechtigungen, die Sie Benutzern zur Durchführung von CloudTrail Verwaltungsaufgaben gewähren, sind nicht dieselben wie die Berechtigungen, die für die Übermittlung von Protokolldateien an Amazon S3 S3-Buckets oder das Senden von Benachrichtigungen an Amazon SNS SNS-Themen CloudTrail erforderlich sind. Weitere Informationen zu diesen Berechtigungen finden Sie unter [Amazon S3 S3-Bucket-Richtlinie für CloudTrail](#).

Wenn Sie die Integration mit Amazon CloudWatch Logs konfigurieren, benötigt es CloudTrail auch eine Rolle, die es übernehmen kann, um Ereignisse an eine Amazon CloudWatch Logs-Protokollgruppe zu übermitteln. Sie müssen die Rolle erstellen, die CloudTrail verwendet. Weitere Informationen finden Sie unter [Erteilen der Berechtigung zum Anzeigen und](#)



## [Konfigurieren von Amazon CloudWatch Logs-Informationen auf der CloudTrail Konsole](#) und [Ereignisse an CloudWatch Logs senden](#).

Die folgenden AWS verwalteten Richtlinien sind verfügbar für CloudTrail:

- [AWSCloudTrail\\_FullAccess](#)— Diese Richtlinie bietet vollen Zugriff auf CloudTrail Aktionen in CloudTrail Bezug auf Ressourcen wie Pfade, Ereignisdatenspeicher und Kanäle. Diese Richtlinie bietet die erforderlichen Berechtigungen zum Erstellen, Aktualisieren und Löschen von CloudTrail Pfaden, Ereignisdatenspeichern und Kanälen.

Diese Richtlinie bietet auch Berechtigungen zur Verwaltung des Amazon S3 S3-Buckets, der Protokollgruppe für CloudWatch Logs und eines Amazon SNS SNS-Themas für einen Trail. Die `AWSCloudTrail_FullAccess` verwaltete Richtlinie bietet jedoch keine Berechtigungen zum Löschen des Amazon S3 S3-Buckets, der Protokollgruppe für CloudWatch Logs oder eines Amazon SNS SNS-Themas. Informationen zu verwalteten Richtlinien für andere AWS Dienste finden Sie im [Referenzhandbuch für AWS verwaltete Richtlinien](#).

### Note

Die `AWSCloudTrail_FullAccess` Richtlinie ist nicht für die allgemeine Verbreitung in Ihrem Unternehmen vorgesehen AWS-Konto. Benutzer mit dieser Rolle können die sensibelsten und wichtigsten Auditing-Funktionen in ihren AWS-Konten deaktivieren oder konfigurieren. Aus diesem Grund dürfen Sie diese Richtlinie nur auf Kontoadministratoren anwenden. Sie müssen die Anwendung dieser Richtlinie genau kontrollieren und überwachen.

- [AWSCloudTrail\\_ReadOnlyAccess](#)— Diese Richtlinie gewährt Berechtigungen zum Anzeigen der CloudTrail Konsole, einschließlich aktueller Ereignisse und des Ereignisverlaufs. Diese Richtlinie ermöglicht es Ihnen auch, vorhandene Trails, Ereignisdatenspeicher und Kanäle einzusehen. Rollen und Benutzer mit dieser Richtlinie können [den Ereignisverlauf herunterladen](#), aber sie können keine Trails, Ereignisdatenspeicher oder Kanäle erstellen oder aktualisieren.

Um Zugriff zu gewähren, fügen Sie Ihren Benutzern, Gruppen oder Rollen Berechtigungen hinzu:

- Benutzer und Gruppen in AWS IAM Identity Center:

Erstellen Sie einen Berechtigungssatz. Befolgen Sie die Anweisungen unter [Erstellen eines Berechtigungssatzes](#) im AWS IAM Identity Center -Benutzerhandbuch.

- Benutzer, die in IAM über einen Identitätsanbieter verwaltet werden:

Erstellen Sie eine Rolle für den Identitätsverbund. Befolgen Sie die Anweisungen unter [Erstellen einer Rolle für einen externen Identitätsanbieter \(Verbund\)](#) im IAM-Benutzerhandbuch.

- IAM-Benutzer:

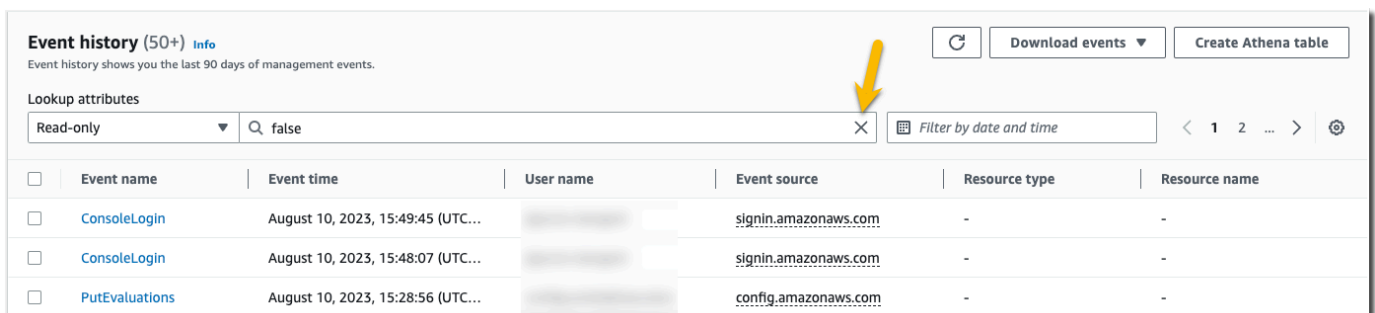
- Erstellen Sie eine Rolle, die Ihr Benutzer annehmen kann. Folgen Sie den Anweisungen unter [Erstellen einer Rolle für einen IAM-Benutzer](#) im IAM-Benutzerhandbuch.
- (Nicht empfohlen) Weisen Sie einem Benutzer eine Richtlinie direkt zu oder fügen Sie einen Benutzer zu einer Benutzergruppe hinzu. Befolgen Sie die Anweisungen unter [Hinzufügen von Berechtigungen zu einem Benutzer \(Konsole\)](#) im IAM-Benutzerhandbuch.

## Event-Historie anzeigen

In diesem Abschnitt wird beschrieben, wie Sie auf der Seite „CloudTrail Ereignisverlauf“ auf der CloudTrail Konsole die Verwaltungsereignisse der letzten 90 Tage AWS-Konto für Sie anzeigen können AWS-Region.

So zeigen Sie den Event-Verlauf an

1. Melden Sie sich bei der an AWS Management Console und öffnen Sie die CloudTrail Konsole unter <https://console.aws.amazon.com/cloudtrail/>.
2. Wählen Sie im Navigationsbereich Event history (Ereignisverlauf) aus. Sie sehen eine gefilterte Liste der Ereignisse. Die neuesten Ereignisse werden zuerst angezeigt. Der Standardfilter für Ereignisse ist Read only (Schreibgeschützt), gesetzt auf false. Sie können diesen Filter deaktivieren, indem Sie das X rechts neben dem Filter auswählen. Sie können im Ereignisverlauf nach Ereignissen suchen, indem Sie nach Ereignissen für ein einzelnes Attribut filtern.



**Event history (50+)** [Info](#)  
Event history shows you the last 90 days of management events.

Lookup attributes  
Read-only

<input type="checkbox"/>	Event name	Event time	User name	Event source	Resource type	Resource name
<input type="checkbox"/>	ConsoleLogin	August 10, 2023, 15:49:45 (UTC...)	[REDACTED]	signin.amazonaws.com	-	-
<input type="checkbox"/>	ConsoleLogin	August 10, 2023, 15:48:07 (UTC...)	[REDACTED]	signin.amazonaws.com	-	-
<input type="checkbox"/>	PutEvaluations	August 10, 2023, 15:28:56 (UTC...)	[REDACTED]	config.amazonaws.com	-	-

3. Wählen Sie ein Attribut aus, nach dem gefiltert werden soll, und geben Sie den vollständigen Wert für das Attribut ein. CloudTrail kann nicht nach einem Teilwert filtern. Um beispielsweise

alle Anmeldeereignisse auf der Konsole anzuzeigen, wählen Sie den Filter „Ereignisname“ und geben Sie ConsoleLogin den Attributwert an.

The screenshot shows the AWS CloudTrail Event history interface. The 'Lookup attributes' section has 'Event name' selected with the value 'ConsoleLogin'. The table below displays three events:

Event name	Event time	User name	Event source	Resource type	Resource name
ConsoleLogin	August 10, 2023, 15:49:45 (UTC...)	[Redacted]	signin.amazonaws.com	-	-
ConsoleLogin	August 10, 2023, 15:48:07 (UTC...)	[Redacted]	signin.amazonaws.com	-	-
ConsoleLogin	August 10, 2023, 14:22:29 (UTC...)	[Redacted]	signin.amazonaws.com	-	-

Oder, um aktuelle CloudTrail Verwaltungsereignisse anzuzeigen, wählen Sie „Ereignisquelle“ und geben Sie Folgendes `cloudtrail.amazonaws.com`.

The screenshot shows the AWS CloudTrail Event history interface with 'Event source' set to 'cloudtrail.amazonaws.com'. The table below displays four events:

Event name	Event time	User name	Event source	Resource type	Resource name
DescribeTrails	August 03, 2023, 18:48:28 (UTC...)	[Redacted]	cloudtrail.amazonaws.com	-	-
GetEventDataStore	August 03, 2023, 18:48:18 (UTC...)	[Redacted]	cloudtrail.amazonaws.com	AWS::CloudTrail::Event...	arn:aws:cloudtrail:us...
GetEventDataStore	August 03, 2023, 18:48:18 (UTC...)	[Redacted]	cloudtrail.amazonaws.com	AWS::CloudTrail::Event...	arn:aws:cloudtrail:us...
ListEventDataStores	August 03, 2023, 18:48:16 (UTC...)	[Redacted]	cloudtrail.amazonaws.com	-	-

- Um ein bestimmtes Verwaltungsereignis anzuzeigen, wählen Sie den Namen des Ereignisses aus. Auf der Seite mit den Ereignisdetails können Sie Details zu dem Ereignis, alle Referenz-Ressourcen und den Ereignisdatensatz einsehen.
- Um Ereignisse zu vergleichen, wählen Sie bis zu fünf Ereignisse aus, indem Sie ihre Kontrollkästchen am linken Rand der Ereignisverlaufstabelle ausfüllen. Sie können Details zu ausgewählten Ereignissen side-by-side in der Tabelle „Eventdetails vergleichen“ einsehen.
- Sie können den Ereignisverlauf speichern, indem Sie ihn als Datei im CSV- oder JSON-Format herunterladen. Das Herunterladen Ihres Ereignisverlaufs kann einige Minuten dauern.

The screenshot shows a close-up of the 'Download events' dropdown menu. The menu options are:

- Download events ▲
- Download as CSV
- Download as JSON

Weitere Informationen finden Sie unter [Mit dem CloudTrail Eventverlauf arbeiten](#).

## Erstellen Sie einen Pfad, um Verwaltungsereignisse zu protokollieren

Für deinen ersten Trail empfehlen wir, einen Trail zu erstellen, der alle [Verwaltungsereignisse](#) in allen AWS Regionen protokolliert und keine [Datenereignisse](#) protokolliert. Beispiele für Verwaltungsereignisse sind etwa Sicherheitsereignisse wie IAM CreateUser und AttachRolePolicy-Ereignisse, Ressourcenereignisse wie RunInstances und CreateBucket und viele mehr. Sie erstellen einen Amazon S3 S3-Bucket, in dem Sie die Protokolldateien für den Trail als Teil der Erstellung des Trails in der CloudTrail Konsole speichern.

### Note

In diesem Tutorial wird davon ausgegangen, dass Sie Ihren ersten Trail erstellen. Abhängig von der Anzahl der Trails, die Sie in Ihrem AWS Konto haben, und davon, wie diese Trails konfiguriert sind, kann das folgende Verfahren Kosten verursachen oder auch nicht. CloudTrail speichert Protokolldateien in einem Amazon S3 S3-Bucket, was Kosten verursacht. Weitere Informationen zu Preisen finden Sie unter [AWS CloudTrail -Preise](#) und [Amazon-S3-Preise](#).

Sie erstellen einen Trail wie folgt:

1. Melden Sie sich bei der an AWS Management Console und öffnen Sie die CloudTrail Konsole unter <https://console.aws.amazon.com/cloudtrail/>.
2. Wählen Sie in der Regionsauswahl die AWS Region aus, in der Ihr Trail erstellt werden soll. Hierbei handelt es sich um die Home-Region für den Trail.


### Note

Die Heimatregion ist die einzige AWS Region, in der Sie den Trail nach seiner Erstellung anzeigen und aktualisieren können, auch wenn der Trail Ereignisse in allen AWS Regionen protokolliert.

3. Wählen Sie auf der CloudTrail Service-Startseite, der Trails-Seite oder im Abschnitt Trails der Dashboard-Seite die Option Trail erstellen aus.

4. Geben Sie unter Trail name (Name des Trails) einen Namen ein, z. B. *My-Management-Events-Trail*. Verwenden Sie dazu am besten einen Namen, der den Zweck des Trails schnell identifiziert. In diesem Fall erstellen Sie einen Trail, der Verwaltungsereignisse protokolliert.
5. Behalten Sie die Standardeinstellung Für alle Konten in meiner Organisation aktivieren bei. Diese Option kann nur geändert werden, wenn Sie Konten in Organizations konfiguriert haben.
6. Wählen Sie in Speicherort für Neuen S3 Bucket erstellen, um einen neuen Bucket zu erstellen. Wenn Sie einen Bucket erstellen, werden die erforderlichen Bucket-Richtlinien CloudTrail erstellt und angewendet. Wenn Sie sich dafür entscheiden, einen neuen S3-Bucket zu erstellen, muss Ihre IAM-Richtlinie die Genehmigung für die `s3:PutEncryptionConfiguration` Aktion enthalten, da die serverseitige Verschlüsselung standardmäßig für den Bucket aktiviert ist. Geben Sie Ihrem Bucket einen Namen, anhand dessen er leicht identifiziert werden kann.

Um das Auffinden Ihrer Logs zu erleichtern, erstellen Sie in einem vorhandenen Bucket einen neuen Ordner (auch als Präfix bezeichnet), um Ihre CloudTrail Logs zu speichern.

 Note

Jeder Amazon-S3-Bucket muss einen global eindeutigen Namen haben. Weitere Informationen finden Sie unter [Benennungsregeln für Buckets](#) im Benutzerhandbuch zu Amazon Simple Storage Service.

## Choose trail attributes

### General details


#### Trail name

Enter a display name for your trail.

My-management-events-trail

3-128 characters. Only letters, numbers, periods, underscores, and dashes are allowed.

Enable for all accounts in my organization

To review accounts in your organization, open AWS Organizations. [See all accounts](#) 

#### Storage location [Info](#)

Create new S3 bucket  
Create a bucket to store logs for the trail.

Use existing S3 bucket  
Choose an existing bucket to store logs for this trail.

#### Trail log bucket and folder

Enter a new S3 bucket name and folder (prefix) to store your logs. Bucket names must be globally unique.

aws-cloudtrail-logs-08132020-my-trail|

Logs will be stored in aws-cloudtrail-logs-08132020-my-trail/AWSLogs/840881077363

#### Log file SSE-KMS encryption [Info](#)

Enabled

► **Additional settings**

7. Deaktivieren Sie das Kontrollkästchen, um die SSE-KMS-Verschlüsselung der Protokolldatei zu deaktivieren. Standardmäßig werden die Protokolldateien mit SSE-S3-Verschlüsselung verschlüsselt. Weitere Informationen zu dieser Einstellung finden Sie unter [Verwenden der serverseitigen Verschlüsselung mit verwalteten Amazon S3 S3-Schlüsseln \(SSE-S3\)](#).
8. Belassen Sie die Standardeinstellungen unter Zusätzliche Einstellungen.
9. Behalten Sie die Standardeinstellungen für Logs bei. CloudWatch Senden Sie vorerst keine Protokolle an Amazon CloudWatch Logs.
10. (Optional) Fügen Sie unter Tags ein oder mehrere benutzerdefinierte Tags (Schlüssel-Wert-Paare) zu Ihrem Trail hinzu. Mithilfe von Tags können Sie Ihre CloudTrail Trails und andere Ressourcen identifizieren, z. B. die Amazon S3 S3-Buckets, die CloudTrail Protokolldateien enthalten. Sie könnten beispielsweise ein Tag mit dem Namen **Compliance** und dem Wert **Auditing** anfügen.

 Note

Sie können zwar Tags zu Trails hinzufügen, wenn Sie sie in der CloudTrail Konsole erstellen, und Sie können einen Amazon S3 S3-Bucket erstellen, um Ihre Protokolldateien in der CloudTrail Konsole zu speichern, aber Sie können dem Amazon S3 S3-Bucket keine Tags von der CloudTrail Konsole aus hinzufügen. Weitere Informationen zum Anzeigen und Ändern der Eigenschaften eines Amazon-S3-Buckets, einschließlich Hinzufügen von Tags zu einem Bucket, finden Sie im [Benutzerhandbuch zu Amazon S3](#).

Wenn Sie fertig sind, klicken Sie auf Weiter.

11. Wählen Sie auf der Seite Protokollereignisse auswählen die zu protokollierenden Ereignistypen aus. Behalten Sie für diesen Trail die Standardeinstellung Verwaltungsereignisse bei. Wählen Sie im Bereich Verwaltungsereignisse aus, dass sowohl Lese- als auch Schreibereignisse protokolliert werden sollen, falls diese nicht bereits ausgewählt sind. Lassen Sie die Kontrollkästchen für AWS KMS Ereignisse ausschließen und Amazon RDS Data API-Ereignisse ausschließen leer, um alle Verwaltungsereignisse zu protokollieren.

## Choose log events

### Events [Info](#)

Record API activity for individual resources, or for all current and future resources in AWS account. [Additional charges apply](#) 

#### Event type

Choose the type of events that you want to log.

**Management events**

Capture management operations performed on your AWS resources.

**Data events**


Log the resource operations performed on or within a resource.

**Insights events**

Identify unusual activity, errors, or user behavior in your account.

### Management events [Info](#)

Management events show information about management operations performed on resources in your AWS account.

 No additional charges apply to log management events on this trail because this is your first copy of management events.

#### API activity

Choose the activities you want to log.

**Read**

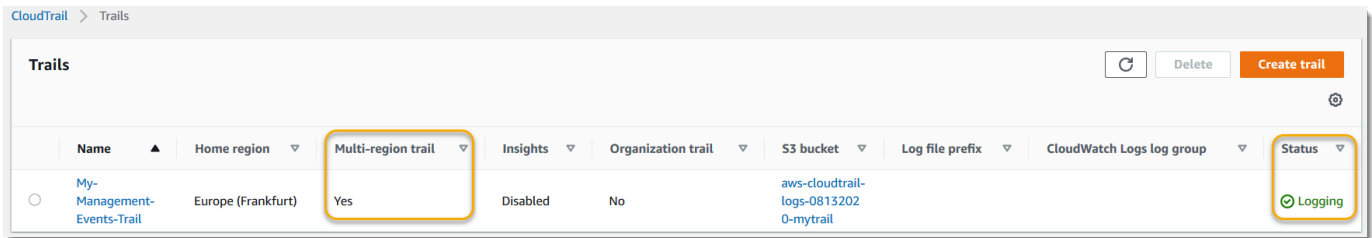
**Write**

**Exclude AWS KMS events**

**Exclude Amazon RDS Data API events**

- Behalten Sie die Standardeinstellungen für Datenereignisse und Insights-Ereignisse bei. Dieser Trail protokolliert keine Daten oder CloudTrail Insights-Ereignisse. Wählen Sie Weiter aus.
- Überprüfen Sie auf der Seite Überprüfen und erstellen die Einstellungen, die Sie für Ihren Trail ausgewählt haben. Wählen Sie Bearbeiten für einen Abschnitt aus, um zurückzugehen und Änderungen vorzunehmen. Wenn Sie bereit sind, Ihren Trail zu erstellen, wählen Sie Trail erstellen.
- Auf der Seite Trails wird Ihr neuer Trail in der Tabelle angezeigt. Beachten Sie, dass der Trail standardmäßig auf Multi-Region-Trail eingestellt ist und dass die Protokollierung für den Trail standardmäßig aktiviert ist.





The screenshot shows the AWS CloudTrail Trails console. At the top, there are buttons for 'Delete' and 'Create trail'. Below is a table with columns: Name, Home region, Multi-region trail, Insights, Organization trail, S3 bucket, Log file prefix, CloudWatch Logs log group, and Status. The first row shows a trail named 'My-Management-Events-Trail' in the 'Europe (Frankfurt)' region, with 'Multi-region trail' set to 'Yes', 'Insights' as 'Disabled', 'Organization trail' as 'No', and 'S3 bucket' as 'aws-cloudtrail-logs-08132020-mytrail'. The 'Status' column shows 'Logging' with a green checkmark. The 'Multi-region trail' and 'Status' dropdown menus are highlighted with orange boxes.

Name	Home region	Multi-region trail	Insights	Organization trail	S3 bucket	Log file prefix	CloudWatch Logs log group	Status
My-Management-Events-Trail	Europe (Frankfurt)	Yes	Disabled	No	aws-cloudtrail-logs-08132020-mytrail			Logging

## Protokolldateien ansehen

Innerhalb von durchschnittlich etwa 5 Minuten nach der Erstellung Ihres ersten Trails werden CloudTrail die ersten Protokolldateien für Ihren Trail an den Amazon S3 S3-Bucket gesendet. Sie können diese Dateien anzeigen und sich mit ihren Informationen vertraut machen.

### Note

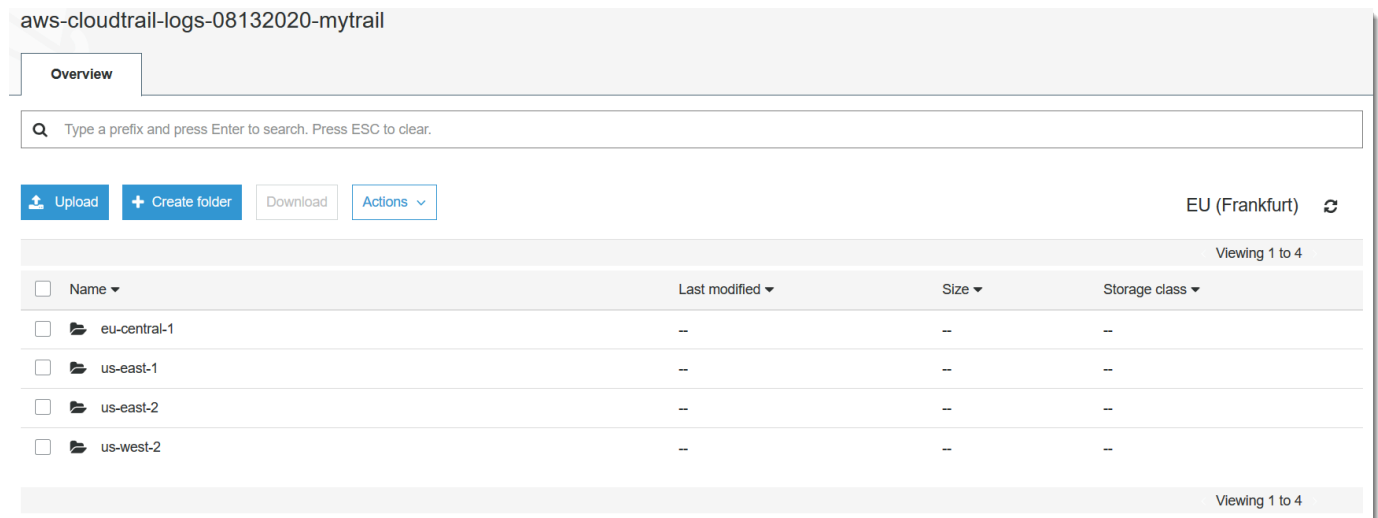
CloudTrail übermittelt Protokolle in der Regel innerhalb von durchschnittlich etwa 5 Minuten nach einem API-Aufruf. Diese Zeit ist nicht garantiert. Weitere Informationen finden Sie unter [AWS CloudTrail Service Level Agreement](#).

Wenn Sie Ihren Trail falsch konfigurieren (z. B. wenn der S3-Bucket nicht erreichbar ist), CloudTrail wird versucht, die Protokolldateien 30 Tage lang erneut in Ihren S3-Bucket zu übertragen. Für diese attempted-to-deliver Ereignisse fallen Standardgebühren an. CloudTrail Um Gebühren für einen falsch konfigurierten Trail zu vermeiden, müssen Sie den Trail löschen.

Zeigen Sie Protokolldateien wie folgt an:

1. [Melden Sie sich bei der an AWS Management Console und öffnen Sie die CloudTrail Konsole unter https://console.aws.amazon.com/cloudtrail/.](https://console.aws.amazon.com/cloudtrail/)
2. Wählen Sie im Navigationsbereich Trails aus. Suchen Sie auf der Seite Trails den Namen des Trails, den Sie gerade erstellt haben (in diesem Beispiel *My-Management-Events-Trail*).
3. Wählen Sie in der Zeile für den Trail den Wert für den S3-Bucket aus (im Beispiel *aws-cloudtrail-logs-08132020-mytrail*).
4. Die Amazon-S3-Konsole wird geöffnet und zeigt diesen Bucket auf der obersten Ebene für Protokolldateien an. Da Sie einen Trail erstellt haben, der Ereignisse in allen AWS Regionen protokolliert, wird die Anzeige auf der Ebene geöffnet, auf der Ihnen die einzelnen Region-Ordner angezeigt werden. *Die Hierarchie der Amazon S3 S3-Bucket-Navigation auf*

*dieser Ebene lautet bucket-name//AWS Logs/ account-id/*. CloudTrail Wählen Sie den Ordner für die AWS Region aus, in der Sie die Protokolldateien überprüfen möchten. Beispiel: Wenn Sie die Protokolldateien für die Region USA Ost (Ohio) überprüfen möchten, wählen Sie us-east-2.




5. Navigieren Sie durch die Bucket-Ordnerstruktur zu Jahr, Monat und Tag, für den Sie Aktivitätsprotokolle der betreffenden region überprüfen möchten. Für diesen Tag gibt es eine Reihe von Dateien. Der Name der Dateien beginnt mit Ihrer AWS Konto-ID und endet mit der Erweiterung .gz. *Wenn Ihre Konto-ID beispielsweise 123456789012 lautet, würden Sie Dateien mit ähnlichen Namen sehen: 123456789012 \_ \_ us-east-2 \_ 20190610T1255abcdeexample .json.gz. CloudTrail*

Um diese Dateien anzuzeigen, können Sie sie herunterladen, entpacken und dann in einem Texteditor oder JSON-Dateiviewer anzeigen. Einige Browser unterstützen auch die Anzeige von .gz- und JSON-Dateien direkt. Wir empfehlen die Verwendung eines JSON-Viewers CloudTrail , da dieser das Analysieren der Informationen in Protokolldateien erleichtert.

## Plan für die nächsten Schritte

Da Sie nun eine Spur haben, haben Sie Zugriff auf eine fortlaufende Aufzeichnung von Ereignissen und Aktivitäten in Ihrem AWS Konto. Dieser fortlaufenden Datensatz hilft Ihnen dabei, ihre Buchhaltungs- und Auditing-Anforderungen für Ihr AWS -Konto zu erfüllen. Es gibt jedoch noch viel mehr, was Sie mit CloudTrail CloudTrail Daten tun können.

- Fügen Sie zusätzliche Sicherheit für Ihre Traildaten hinzu. CloudTrail wendet automatisch eine bestimmte Sicherheitsstufe an, wenn Sie einen Trail erstellen. Es gibt jedoch zusätzliche Maßnahmen, die Sie ergreifen können, um Ihre Daten zu schützen.
- Standardmäßig gilt für den Amazon S3 S3-Bucket, den Sie im Rahmen der Erstellung eines Trails erstellt haben, eine Richtlinie, die das Schreiben von Protokolldateien in diesen Bucket ermöglicht CloudTrail. Der Bucket ist nicht öffentlich zugänglich, aber möglicherweise können andere Benutzer in Ihrem AWS Konto darauf zugreifen, wenn sie über Lese- und Schreibberechtigungen für Buckets in Ihrem AWS Konto verfügen. Überprüfen Sie die Richtlinie für Ihren Bucket und nehmen Sie bei Bedarf Änderungen vor, um die Zugriffsrechte einzuschränken. Weitere Informationen finden Sie in der [Amazon-S3- Sicherheitsdokumentation](#) und der [Beispielanleitung für die Absicherung eines Buckets](#).
- Die von CloudTrail an Ihren Bucket übermittelten Protokolldateien werden durch [serverseitige Amazon-Verschlüsselung mit von Amazon S3 verwalteten Verschlüsselungsschlüsseln \(SSE-S3\)](#) verschlüsselt. Um eine Sicherheitsebene bereitzustellen, die direkt verwaltet werden kann, können Sie stattdessen eine [serverseitige Verschlüsselung mit AWS KMS verwalteten Schlüsseln \(SSE-KMS\) für Ihre Protokolldateien](#) verwenden. CloudTrail Um SSE-KMS mit zu verwenden CloudTrail, erstellen und verwalten Sie einen KMS-Schlüssel, auch bekannt als [AWS KMS key](#) Weitere Informationen finden Sie unter [CloudTrail Logdateien mit AWS KMS Schlüsseln verschlüsseln \(SSE-KMS\)](#).
- Weitere Informationen zur Sicherheitsplanung finden Sie in den [bewährten Sicherheitsmethoden](#) für. CloudTrail
- Erstellen eines Trails für die Protokollierung von Datenereignissen. Wenn Sie protokollieren möchten, wann Objekte in einem oder mehreren Amazon S3 S3-Buckets hinzugefügt, abgerufen und gelöscht werden, wenn Elemente in DynamoDB-Tabellen hinzugefügt, geändert oder gelöscht werden oder wenn eine oder mehrere AWS Lambda Funktionen aufgerufen werden, handelt es sich dabei um Datenereignisse. Der Verwaltungsereignis-Trail, den Sie vorher erstellt haben, protokolliert Ereignisse dieser Art nicht. Sie können einen separaten Pfad speziell zum Protokollieren von Datenereignissen für einige oder alle unterstützten Ressourcentypen erstellen. Weitere Informationen finden Sie unter [Datenereignisse](#).

 Note

Für die Protokollierung von Datenereignissen fallen zusätzliche Gebühren an. Weitere Informationen finden Sie unter [AWS CloudTrail -Preisgestaltung](#).

- Protokollieren Sie CloudTrail Insights-Ereignisse auf Ihrem Trail. AWS CloudTrail Insights helfen AWS Benutzern, ungewöhnliche Aktivitäten im Zusammenhang mit API-Aufrufen und API-Fehlerraten zu identifizieren und darauf zu reagieren, indem CloudTrail Verwaltungsereignisse kontinuierlich analysiert werden. CloudTrail Insights verwendet mathematische Modelle, um das normale Niveau der API- und Serviceereignisaktivitäten für ein Konto zu bestimmen. Es identifiziert Verhalten, das außerhalb normaler Muster liegt, generiert Insights-Ereignisse und liefert diese Ereignisse an einen /CloudTrail-Insight-Ordner im ausgewählten Ziel-S3-Bucket für Ihren Trail. Weitere Informationen zu CloudTrail Insights finden Sie unter [Protokollieren von Insights-Ereignissen](#).

#### Note

Für die Protokollierung von Insights-Ereignissen fallen zusätzliche Gebühren an. Weitere Informationen finden Sie unter [AWS CloudTrail -Preisgestaltung](#).

- Richten Sie CloudWatch Log-Alarme ein, um Sie zu benachrichtigen, wenn bestimmte Ereignisse eintreten. CloudWatch Mithilfe von Logs können Sie bestimmte Ereignisse überwachen und Warnmeldungen erhalten, die von erfasst wurden CloudTrail. Sie können beispielsweise wichtige Sicherheits- und netzwerkbezogene Verwaltungsereignisse überwachen, z. B. [Änderungen an Sicherheitsgruppen](#), [fehlgeschlagene AWS Management Console -Anmeldeereignisse](#) oder [Änderungen an IAM-Richtlinien](#). Weitere Informationen finden Sie unter [Überwachung von CloudTrail Protokolldateien mit Amazon CloudWatch Logs](#).
- Verwenden Sie Analysetools, um Trends in Ihren CloudTrail Protokollen zu identifizieren. Während die Filter im Ereignisverlauf Ihnen dabei helfen können, bestimmte Ereignisse oder Ereignisarten in Ihren jüngsten Aktivitäten zu finden, stellen sie nicht die Möglichkeit zur Verfügung, längere Zeiträume nach Aktivitäten zu durchsuchen. Für tiefere und komplexere Analysen können Sie Amazon Athena verwenden. Weitere Informationen finden Sie unter [Abfragen von AWS CloudTrail Protokollen](#) im Amazon Athena Athena-Benutzerhandbuch.

## Erstellen Sie einen Ereignisdatenspeicher für S3-Datenereignisse

Sie können einen Ereignisdatenspeicher erstellen, um CloudTrail Ereignisse (Verwaltungsereignisse, Datenereignisse), [CloudTrail Insights-Ereignisse](#), [AWS Audit Manager Beweise](#), [AWS Config Konfigurationselemente](#) oder [AWS Nichtereignisse zu](#) protokollieren.

Wenn Sie einen Ereignisdatenspeicher für Datenereignisse erstellen, wählen Sie die Ressourcentypen AWS-Services und die Ressourcentypen aus, für die Sie Datenereignisse

protokollieren möchten. Informationen dazu AWS-Services , wie Datenereignisse protokolliert werden, finden Sie unter [Datenereignisse](#).

Diese exemplarische Vorgehensweise zeigt Ihnen, wie Sie einen Ereignisdatenspeicher für Amazon S3 S3-Datenereignisse erstellen. In diesem Tutorial wählen wir, anstatt alle Amazon-S3-Datenereignisse zu protokollieren, eine benutzerdefinierte Protokollauswahlvorlage, um Ereignisse nur zu protokollieren, wenn ein Objekt aus einem bestimmten S3-Bucket gelöscht wird.

CloudTrail Für Datenspeicher mit Ereignissen in Lake fallen Gebühren an. Beim Erstellen eines Ereignisdatenspeichers wählen Sie die [Preisoption](#) aus, die für den Ereignisdatenspeicher genutzt werden soll. Die Preisoption bestimmt die Kosten für die Erfassung und Speicherung von Ereignissen sowie die standardmäßige und maximale Aufbewahrungsdauer für den Ereignisdatenspeicher. Informationen zur CloudTrail Preisgestaltung und Verwaltung der Lake-Kosten finden Sie unter [AWS CloudTrail Preise](#) und [Verwaltung der CloudTrail Seekosten](#).

Erstellen Sie einen Ereignisdatenspeicher für S3-Datenereignisse wie folgt:

1. Melden Sie sich bei der an AWS Management Console und öffnen Sie die CloudTrail Konsole unter <https://console.aws.amazon.com/cloudtrail/>.
2. Wählen Sie im Navigationsbereich unter Lake die Option Ereignisdatenspeicher aus.
3. Wählen Sie Ereignisdatenspeicher erstellen aus.
4. Geben Sie auf der Seite „Ereignisdatenspeicher konfigurieren“ unter Allgemeine Informationen Ihrem Ereignisdatenspeicher einen Namen, z. B. *s3- data-events-eds*. Verwenden Sie dazu am besten einen Namen, der den Zweck des Ereignisdatenspeichers schnell identifiziert. Informationen zu den CloudTrail Benennungsanforderungen finden Sie unter [Benennungsanforderungen](#).
5. Wählen Sie die Preisoption aus, die Sie für den Ereignisdatenspeicher verwenden möchten. Der Preisoption bestimmt die Kosten für die Erfassung und Speicherung von Ereignissen sowie die standardmäßige und maximale Aufbewahrungsdauern für Ihren Ereignisdatenspeicher. Weitere Informationen finden Sie unter [AWS CloudTrail -Preise](#) und [Verwaltung der CloudTrail Seekosten](#).

Die folgenden Optionen sind verfügbar:

- Preisoption mit verlängerbarer Aufbewahrung für ein Jahr – Empfohlen, wenn Sie damit rechnen, weniger als 25 TB an Ereignisdaten pro Monat zu erfassen und eine flexible Aufbewahrungsdauer von bis zu 10 Jahren wünschen. In den ersten 366 Tagen (Standardaufbewahrungszeitraum) ist Speicherplatz ohne zusätzliche Kosten im Preis für die

Datenaufnahme enthalten. Nach 366 Tagen ist eine verlängerte Aufbewahrung gegen Aufpreis pay-as-you-go verfügbar. Dies ist die Standardoption.

- Standardaufbewahrungsdauer: 366 Tage.
  - Maximale Aufbewahrungsdauer: beträgt 3 653 Tage.
6. Preisoption für die Aufbewahrung über sieben Jahre – Empfohlen, wenn Sie damit rechnen, mehr als 25 TB an Ereignisdaten pro Monat zu erfassen und eine flexible Aufbewahrungsdauer von bis zu 7 Jahren wünschen. Die Aufbewahrung ist im Preis für die Erfassung ohne Zusatzkosten enthalten.
- Standardaufbewahrungsdauer: 2 557 Tage.
  - Maximale Aufbewahrungsdauer: beträgt 2 557 Tage.
6. Geben Sie einen Aufbewahrungszeitraum für den Ereignisdatenspeicher an. Die Aufbewahrungsdauern können zwischen 7 Tagen und 3 653 Tagen (etwa 10 Jahre) für die Preisoption mit verlängerbarer Aufbewahrungsdauer für ein Jahr oder zwischen 7 Tagen und 2 557 Tagen (etwa sieben Jahre) für die Preisoption mit siebenjähriger Aufbewahrungsdauer liegen.

CloudTrail Lake entscheidet, ob ein Ereignis aufbewahrt werden soll, indem es prüft, ob das Ereignis innerhalb `eventTime` des angegebenen Aufbewahrungszeitraums liegt. Wenn Sie beispielsweise einen Aufbewahrungszeitraum von 90 Tagen angeben, CloudTrail werden Ereignisse entfernt, wenn sie `eventTime` älter als 90 Tage sind.

7. (Optional) Wählen Sie unter Verschlüsselung aus, ob Sie den Ereignisdatenspeicher mit Ihrem eigenen KMS-Schlüssel verschlüsseln möchten. Standardmäßig werden alle Ereignisse in einem Ereignisdatenspeicher CloudTrail mithilfe eines KMS-Schlüssels verschlüsselt, der für Sie verantwortlich AWS ist und für Sie verwaltet wird.

Um die Verschlüsselung mit Ihrem eigenen KMS-Schlüssel zu aktivieren, wählen Sie **Meinen eigenen AWS KMS key** verwenden. Wählen Sie **Neu**, um einen für Sie AWS KMS key erstellen zu lassen, oder wählen Sie **Bestehend**, um einen vorhandenen KMS-Schlüssel zu verwenden. Geben Sie unter **KMS-Alias** eingeben einen Alias im folgenden Format an `alias/MyAliasName`. Wenn Sie Ihren eigenen KMS-Schlüssel verwenden, müssen Sie Ihre KMS-Schlüsselrichtlinie bearbeiten, um das Verschlüsseln und Entschlüsseln von CloudTrail Protokollen zuzulassen. Weitere Informationen finden Sie unter [Konfigurieren Sie AWS KMS wichtige Richtlinien für CloudTrail](#). CloudTrail unterstützt auch Schlüssel AWS KMS für mehrere Regionen. Weitere Informationen finden Sie über Multi-Regions-Schlüssel finden Sie unter [Verwenden von Schlüsseln für mehrere Regionen](#) im AWS Key Management Service - Entwicklerhandbuch.

Wenn Sie Ihren eigenen KMS-Schlüssel verwenden, fallen AWS KMS Kosten für die Verschlüsselung und Entschlüsselung an. Nachdem Sie einen KMS-Schlüssel einem Ereignisdatenspeicher zugeordnet haben, kann der KMS-Schlüssel nicht entfernt oder geändert werden.

 Note

Um die AWS Key Management Service Verschlüsselung für den Ereignisdatenspeicher einer Organisation zu aktivieren, müssen Sie einen vorhandenen KMS-Schlüssel für das Verwaltungskonto verwenden.

8. (Optional) Wenn Sie Ihre Ereignisdaten mit Amazon Athena abfragen möchten, wählen Sie Aktivieren in Lake-Abfrageverbund. Mit Verbund können Sie die mit einem Ereignisdatenspeicher verbundenen Metadaten im AWS Glue [-Datenkatalog](#) einsehen und mit Amazon Athena SQL-Abfragen zu den Ereignisdaten durchführen. Anhand der im AWS Glue Datenkatalog gespeicherten Tabellenmetadaten weiß die Athena-Abfrage-Engine, wie die Daten, die Sie abfragen möchten, gesucht, gelesen und verarbeitet werden. Weitere Informationen finden Sie unter [Verbund für einen Ereignisdatenspeicher erstellen](#).

Wählen Sie Aktivieren und gehen Sie wie folgt vor, um Lake-Abfrageverbund zu aktivieren:

- a. Wählen Sie aus, ob Sie eine neue Rolle erstellen oder eine vorhandene IAM-Rolle verwenden möchten. [AWS Lake Formation](#) verwendet diese Rolle, um die Berechtigungen für den Verbundereignisdatenspeicher zu verwalten. Wenn Sie mit der CloudTrail Konsole eine neue Rolle erstellen, CloudTrail wird automatisch eine Rolle mit den erforderlichen Berechtigungen erstellt. Wenn Sie eine bestehende Rolle auswählen, stellen Sie sicher, dass die Richtlinie für die Rolle die [erforderlichen Mindestberechtigungen](#) vorsieht.
  - b. Wenn Sie eine neue Rolle erstellen, geben Sie einen Namen zur Identifizierung der Rolle ein.
  - c. Wenn Sie eine bestehende Rolle verwenden, wählen Sie die Rolle aus, die Sie verwenden möchten. Die Rolle muss in Ihrem Konto vorhanden sein.
9. (Optional) Fügen Sie unter Tags ein oder mehrere benutzerdefinierte Tags (Schlüssel-Wert-Paare) zu Ihrem Ereignisdatenspeicher hinzu. Mithilfe von Tags können Sie Ihre CloudTrail Ereignisdatenspeicher identifizieren. Sie könnten beispielsweise ein Tag mit dem Namen **stage** und dem Wert **prod** anfügen. Sie können Tags verwenden, um den Zugriff auf Ihren

Ereignisdatenspeicher einzuschränken. Sie können Tags auch verwenden, um die Abfrage- und Aufnahmekosten für Ihren Ereignisdatenspeicher zu verfolgen.

Informationen dazu, wie Sie mithilfe von Tags Kosten nachverfolgen, finden Sie unter [Erstellen von benutzerdefinierten Kostenzuweisungs-Tags für CloudTrail Lake-Event-Datenspeicher](#). Informationen darüber, wie Sie IAM-Richtlinien verwenden, um den Zugriff auf einen Ereignisdatenspeicher basierend auf Tags zu autorisieren, finden Sie unter [Beispiele: Verweigern des Zugriffs zum Erstellen oder Löschen von Ereignisdatenspeichern basierend auf Tags](#). Informationen dazu, wie Sie Tags verwenden können AWS, finden Sie unter [Tagging Your AWS Resources User Guide](#) im Tagging AWS Resources User Guide.

10. Wählen Sie Next (Weiter) aus, um den Ereignisdatenspeicher zu konfigurieren.
11. Behalten Sie auf der Seite Ereignisse auswählen die Standardauswahl für den Ereignistyp bei.

**Event type** [Info](#)  
Choose the type of events you want to add to your event data store. [Additional charges apply](#)

**Choose event types**

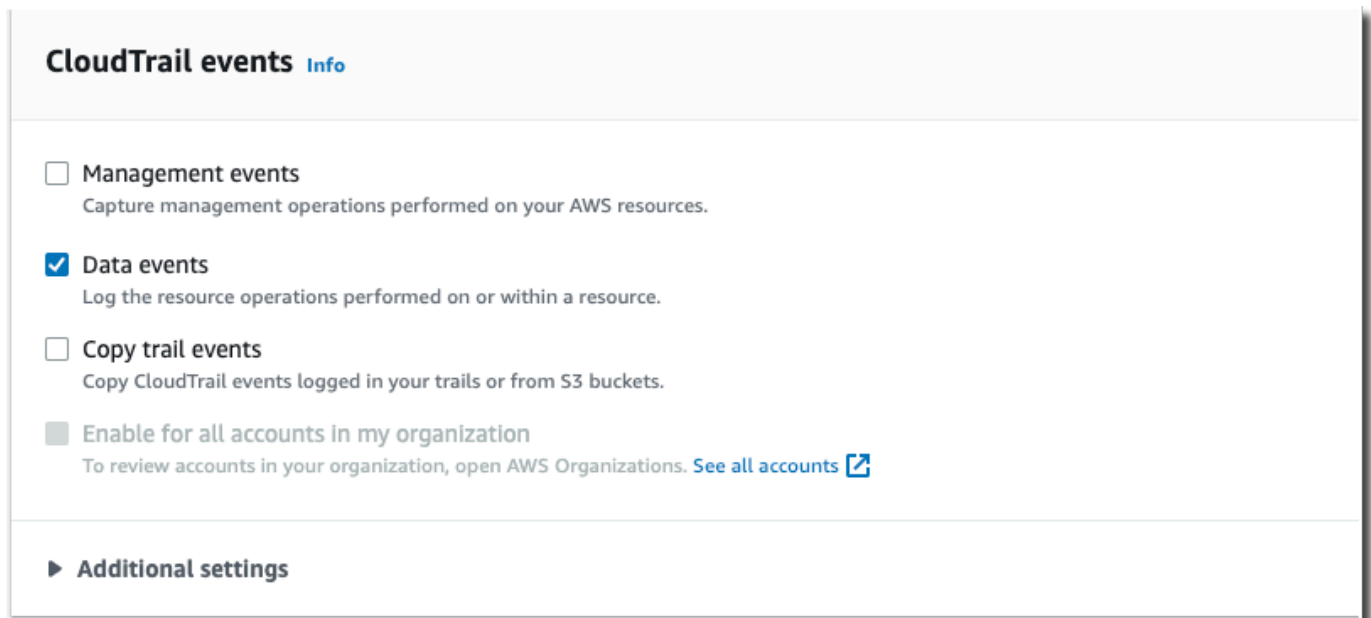
- AWS events**  
Capture operations performed on or within your AWS resources.
- Events from integrations**  
Create an integration to get events that are logged by applications outside of your AWS resources.

**Specify the type of AWS events**

- CloudTrail events**  
CloudTrail events provide a record of activity in an AWS account.
- CloudTrail Insights events**  
Insights events help identify unusual activity, errors, or user behavior in your account.
- Configuration items**  
Configuration items show changes made to the configuration of a resource, and show the resource's compliance status.

12. Wählen Sie für CloudTrail Ereignisse die Option Datenereignisse und deaktivieren Sie Verwaltungsereignisse. Weitere Informationen zu Datenereignissen finden Sie unter [Protokollieren von Datenereignissen](#).





13. Behalten Sie die Standardeinstellung für Trail-Ereignisse kopieren bei. Sie würden diese Option verwenden, um vorhandene Trail-Ereignisse in Ihren Ereignisdatenspeicher zu kopieren. Weitere Informationen finden Sie unter [Kopieren von Trail-Ereignissen in einen Ereignisdatenspeicher](#).
14. Wählen Sie Für alle Konten in meiner Organisation aktivieren aus, wenn es sich um einen Ereignisdatenspeicher für eine Organisation handelt. Diese Option kann nur geändert werden, wenn Sie Konten in AWS Organizations konfiguriert haben.
15. Behalten Sie für Zusätzliche Einstellungen die Standardauswahl bei. Standardmäßig sammelt ein Ereignisdatenspeicher Ereignisse für alle AWS-Regionen und beginnt, Ereignisse zu erfassen, sobald er erstellt wird.
16. Treffen Sie für Datenereignisse die folgenden Auswahlen:
  - a. Wählen Sie unter Datenereignistyp S3 aus. Der Datenereignistyp identifiziert die Ressource AWS-Service und die Ressource, auf der Datenereignisse protokolliert werden.
  - b. Wählen Sie unter Protokoll-Selektorstempel Benutzerdefiniert aus. Wenn Sie Benutzerdefiniert wählen, können Sie einen benutzerdefinierten Ereignisselektor festlegen, um nach den Feldern `eventName`, `resources.ARN` und `readOnly` zu filtern. Informationen zu diesen Feldern finden Sie [AdvancedFieldSelector](#) in der AWS CloudTrail API-Referenz.
  - c. (Optional) Geben Sie unter Selektorname einen Namen ein, um Ihre Auswahl zu identifizieren. Der Selektorname ist ein beschreibender Name für einen erweiterten Event-Selektor, z. B. „DeleteObject API-Aufrufe für einen bestimmten S3-Bucket protokollieren“.

Der Name des Selektors wird als Name in der erweiterten Ereignisauswahl aufgeführt und ist sichtbar, wenn Sie die JSON-Ansicht erweitern.

▼ JSON view

```
[
  {
    "Name": "Log DeleteObject API calls for a specific S3 bucket"
    "FieldSelectors": [
      {
        "Field": "eventCategory",
        "Equals": [
          "Data"
        ]
      },
      {
        "Field": "resources.type",
        "Equals": [
          "AWS::S3::Object"
        ]
      }
    ]
  }
]
```

- d. In Advanced Event Selectors erstellen wir den benutzerdefinierten Event-Selektor, um nach den Feldern und zu filtern. `eventName resources.ARN` Erweiterte Ereignisselektoren für einen Ereignisdatenspeicher funktionieren genauso wie erweiterte Ereignisselektoren, die Sie auf einen Trail anwenden. Weitere Informationen zum Erstellen von erweiterten Ereignisauswahlen finden Sie unter [Protokollieren von Datenereignissen mit erweiterten Ereignisauswahlen](#).
  - i. Wählen Sie für Feld die Option `EventName`. Wählen Sie für Operator die Option `Equals` aus. Geben Sie für Wert **DeleteObject** ein. Wählen Sie + Feld, um nach einem anderen Feld zu filtern.
  - ii. Wählen Sie für Feld `resources.ARN` aus. Wählen Sie für Operator die Option `StartsWith`. Geben Sie für Wert den ARN für Ihren Bucket ein (z. B. *arn:aws:s3:::bucket-name*). Informationen zum Abrufen des ARN finden Sie unter [Amazon-S3-Ressourcen](#) im Benutzerhandbuch von Amazon Simple Storage Service.

## Data events [Info](#)

Data events show information about the resource operations performed on or within a resource.

▼ Data event: S3 Remove

Data event type  
Choose the source of data events to log.

S3 ▼

Log selector template  
Custom ▼

Selector name - *optional*  
Log DeleteObject API calls for a specific S3 bucket  
1,000 character limit

Collect events  
Log all events, or choose a template to log specific, filtered events to your trail. You can edit templates later.

Advanced event selectors [Info](#)  
Log or exclude events from specific resources.

Field	Operator	Value	
eventName ▼	equals ▼	DeleteObject	×
AND			
	+ Condition		
resources.ARN ▼	starts with ▼	arn:aws:s3:::bucket-name	×
+ Field	+ Condition		

► JSON view

Add data event type

17. Wählen Sie Next (Weiter) aus, um Ihre Auswahl zu überprüfen.
18. Überprüfen Sie auf der Seite Prüfen und erstellen Ihre Auswahl. Wählen Sie Bearbeiten aus, um Änderungen am Schema vorzunehmen. Wenn Sie bereit sind, den Ereignisdatenspeicher zu erstellen, wählen Sie Ereignisdatenspeicher erstellen aus.

19. Der neue Ereignisdatenspeicher ist in der Tabelle Ereignisdatenspeicher auf der Seite Ereignisdatenspeicher sichtbar.

Ab diesem Zeitpunkt erfasst der Ereignisdatenspeicher Ereignisse, die mit seinen erweiterten Ereigniselektoren übereinstimmen. Ereignisse, die aufgetreten sind, bevor Sie den Ereignisdatenspeicher erstellt haben, befinden sich nicht im Ereignisdatenspeicher, es sei denn Sie haben sich für das Kopieren der bestehenden Trail-Ereignissen entschieden.

Sie können jetzt Abfragen in Ihrem neuen Ereignisdatenspeicher ausführen. Informationen zum Anzeigen und Ausführen von Beispielabfragen finden Sie unter [CloudTrail Lake-Beispielabfragen anzeigen und ausführen](#).

## Kopieren Sie Trail-Ereignisse in einen CloudTrail Lake-Event-Datenspeicher

In dieser exemplarischen Vorgehensweise erfahren Sie, wie Sie Trail-Ereignisse zur historischen Analyse in einen neuen CloudTrail Lake Event Data Store kopieren. Weitere Informationen zum Kopieren von Trail-Ereignissen finden Sie unter [Kopieren von Trail-Ereignissen in einen Ereignisdatenspeicher](#).

CloudTrail Für Datenspeicher mit Ereignissen in Lake fallen Gebühren an. Beim Erstellen eines Ereignisdatenspeichers wählen Sie die [Preisoption](#) aus, die für den Ereignisdatenspeicher genutzt werden soll. Die Preisoption bestimmt die Kosten für die Erfassung und Speicherung von Ereignissen sowie die standardmäßige und maximale Aufbewahrungsdauer für den Ereignisdatenspeicher. Informationen zur CloudTrail Preisgestaltung und Verwaltung der Lake-Kosten finden Sie unter [AWS CloudTrail Preise](#) und [Verwaltung der CloudTrail Seekosten](#).

Wenn Sie Trail-Ereignisse in einen CloudTrail Lake-Ereignisdatenspeicher kopieren, fallen Gebühren an, die auf der Menge der unkomprimierten Daten basieren, die der Ereignisdatenspeicher aufnimmt.

Wenn Sie Trail-Ereignisse nach CloudTrail Lake kopieren, werden die im komprimierten CloudTrail GZIP-Format gespeicherten Protokolle entpackt und anschließend die in den Protokollen enthaltenen Ereignisse in Ihren Ereignisdatenspeicher kopiert. Die Größe der unkomprimierten Daten könnte größer sein als die tatsächliche S3-Speichergröße. Um eine allgemeine Schätzung der Größe der unkomprimierten Daten zu erhalten, können Sie die Größe der Protokolle im S3-Bucket mit 10 multiplizieren.

Sie können die Kosten senken, indem Sie einen engeren Zeitraum für die kopierten Ereignisse angeben. Wenn Sie planen, den Ereignisdatenspeicher nur zum Abfragen Ihrer kopierten Ereignisse zu verwenden, können Sie die Ereignisaufnahme deaktivieren, um zu vermeiden, dass für zukünftige Ereignisse Gebühren anfallen. [Weitere Informationen zu den Kosten finden Sie unter AWS CloudTrail Preise und Verwaltung der CloudTrail Seekosten](#)

Kopieren Sie Trail-Ereignisse wie folgt in einen neuen Ereignisdatenspeicher:

1. Melden Sie sich bei der an AWS Management Console und öffnen Sie die CloudTrail Konsole unter <https://console.aws.amazon.com/cloudtrail/>.
2. Wählen Sie im Navigationsbereich unter Lake die Option Ereignisdatenspeicher aus.
3. Wählen Sie Ereignisdatenspeicher erstellen aus.
4. Geben Sie auf der Seite „Event-Datenspeicher konfigurieren“ unter Allgemeine Details Ihrem Event-Datenspeicher einen Namen, z. *my-management-events-eds*. Verwenden Sie dazu am besten einen Namen, der den Zweck des Ereignisdatenspeichers schnell identifiziert. Informationen zu den CloudTrail Benennungsanforderungen finden Sie unter [Benennungsanforderungen](#).
5. Wählen Sie die Preisoption aus, die Sie für den Ereignisdatenspeicher verwenden möchten. Der Preisoption bestimmt die Kosten für die Erfassung und Speicherung von Ereignissen sowie die standardmäßige und maximale Aufbewahrungsdauern für Ihren Ereignisdatenspeicher. Weitere Informationen finden Sie unter [AWS CloudTrail -Preise](#) und [Verwaltung der CloudTrail Seekosten](#).

Die folgenden Optionen sind verfügbar:

- Preisoption mit verlängerbarer Aufbewahrung für ein Jahr – Empfohlen, wenn Sie damit rechnen, weniger als 25 TB an Ereignisdaten pro Monat zu erfassen und eine flexible Aufbewahrungsdauer von bis zu 10 Jahren wünschen. In den ersten 366 Tagen (Standardaufbewahrungszeitraum) ist Speicherplatz ohne zusätzliche Kosten im Preis für die Datenaufnahme enthalten. Nach 366 Tagen ist eine verlängerte Aufbewahrung gegen Aufpreis pay-as-you-go verfügbar. Dies ist die Standardoption.
  - Standardaufbewahrungsdauer: 366 Tage.
  - Maximale Aufbewahrungsdauer: beträgt 3 653 Tage.
- Preisoption für die Aufbewahrung über sieben Jahre – Empfohlen, wenn Sie damit rechnen, mehr als 25 TB an Ereignisdaten pro Monat zu erfassen und eine flexible

Aufbewahrungsdauer von bis zu 7 Jahren wünschen. Die Aufbewahrung ist im Preis für die Erfassung ohne Zusatzkosten enthalten.

- Standardaufbewahrungsdauer: 2 557 Tage.
- Maximale Aufbewahrungsdauer: beträgt 2 557 Tage.

6. Geben Sie einen Aufbewahrungszeitraum für den Ereignisdatenspeicher an. Die Aufbewahrungsdauern können zwischen 7 Tagen und 3 653 Tagen (etwa 10 Jahre) für die Preisoption mit verlängerbarer Aufbewahrungsdauer für ein Jahr oder zwischen 7 Tagen und 2 557 Tagen (etwa sieben Jahre) für die Preisoption mit siebenjähriger Aufbewahrungsdauer liegen.

CloudTrail Lake entscheidet, ob ein Ereignis aufbewahrt werden soll, indem es prüft, ob das Ereignis innerhalb `eventTime` des angegebenen Aufbewahrungszeitraums liegt. Wenn Sie beispielsweise einen Aufbewahrungszeitraum von 90 Tagen angeben, CloudTrail werden Ereignisse entfernt, wenn sie `eventTime` älter als 90 Tage sind.

#### Note


Wenn Sie Trail-Ereignisse in diesen Ereignisdatenspeicher kopieren, CloudTrail wird ein Ereignis nicht kopiert, wenn `eventTime` es älter als der angegebene Aufbewahrungszeitraum ist. Um den geeigneten Aufbewahrungszeitraum zu ermitteln, nehmen Sie die Summe aus dem ältesten Ereignis, das Sie kopieren möchten, in Tagen und der Anzahl der Tage, an denen Sie die Ereignisse im Ereignisdatenspeicher behalten möchten (Aufbewahrungszeitraum = *oldest-event-in-days* + *number-days-to-retain*). Wenn das älteste Ereignis, das Sie kopieren, beispielsweise 45 Tage alt ist und Sie die Ereignisse weitere 45 Tage im Ereignisdatenspeicher aufbewahren möchten, würden Sie die Aufbewahrungsdauer auf 90 Tage festlegen.

7. (Optional) Wählen Sie unter Verschlüsselung aus, ob Sie den Ereignisdatenspeicher mit Ihrem eigenen KMS-Schlüssel verschlüsseln möchten. Standardmäßig werden alle Ereignisse in einem Ereignisdatenspeicher CloudTrail mithilfe eines KMS-Schlüssels verschlüsselt, der für Sie verantwortlich AWS ist und der für Sie verwaltet wird.

Um die Verschlüsselung mit Ihrem eigenen KMS-Schlüssel zu aktivieren, wählen Sie **Meinen eigenen AWS KMS key verwenden**. Wählen Sie **Neu**, um einen für Sie AWS KMS key erstellen zu lassen, oder wählen Sie **Bestehend**, um einen vorhandenen KMS-Schlüssel zu verwenden. Geben Sie unter **KMS-Alias** eingeben einen Alias im folgenden Format an `alias/MyAliasName`. Wenn Sie Ihren eigenen KMS-Schlüssel verwenden, müssen Sie Ihre

KMS-Schlüsselrichtlinie bearbeiten, um das Verschlüsseln und Entschlüsseln von CloudTrail Protokollen zuzulassen. Weitere Informationen finden Sie unter [Konfigurieren Sie AWS KMS wichtige Richtlinien für CloudTrail](#). CloudTrail unterstützt auch Schlüssel AWS KMS für mehrere Regionen. Weitere Informationen finden Sie über Multi-Regions-Schlüssel finden Sie unter [Verwenden von Schlüsseln für mehrere Regionen](#) im AWS Key Management Service - Entwicklerhandbuch.

Wenn Sie Ihren eigenen KMS-Schlüssel verwenden, fallen AWS KMS Kosten für die Verschlüsselung und Entschlüsselung an. Nachdem Sie einen KMS-Schlüssel einem Ereignisdatenspeicher zugeordnet haben, kann der KMS-Schlüssel nicht entfernt oder geändert werden.

 Note

Um die AWS Key Management Service Verschlüsselung für den Ereignisdatenspeicher einer Organisation zu aktivieren, müssen Sie einen vorhandenen KMS-Schlüssel für das Verwaltungskonto verwenden.

8. (Optional) Wenn Sie Ihre Ereignisdaten mit Amazon Athena abfragen möchten, wählen Sie Aktivieren in Lake-Abfrageverbund. Mit Verbund können Sie die mit einem Ereignisdatenspeicher verbundenen Metadaten im AWS Glue [-Datenkatalog](#) einsehen und mit Amazon Athena SQL-Abfragen zu den Ereignisdaten durchführen. Anhand der im AWS Glue Datenkatalog gespeicherten Tabellenmetadaten weiß die Athena-Abfrage-Engine, wie die Daten, die Sie abfragen möchten, gesucht, gelesen und verarbeitet werden. Weitere Informationen finden Sie unter [Verbund für einen Ereignisdatenspeicher erstellen](#).

Wählen Sie Aktivieren und gehen Sie wie folgt vor, um Lake-Abfrageverbund zu aktivieren:

- a. Wählen Sie aus, ob Sie eine neue Rolle erstellen oder eine vorhandene IAM-Rolle verwenden möchten. [AWS Lake Formation](#) verwendet diese Rolle, um die Berechtigungen für den Verbundereignisdatenspeicher zu verwalten. Wenn Sie mit der CloudTrail Konsole eine neue Rolle erstellen, CloudTrail wird automatisch eine Rolle mit den erforderlichen Berechtigungen erstellt. Wenn Sie eine bestehende Rolle auswählen, stellen Sie sicher, dass die Richtlinie für die Rolle die [erforderlichen Mindestberechtigungen](#) vorsieht.
- b. Wenn Sie eine neue Rolle erstellen, geben Sie einen Namen zur Identifizierung der Rolle ein.
- c. Wenn Sie eine bestehende Rolle verwenden, wählen Sie die Rolle aus, die Sie verwenden möchten. Die Rolle muss in Ihrem Konto vorhanden sein.

9. (Optional) Fügen Sie unter Tags ein oder mehrere benutzerdefinierte Tags (Schlüssel-Wert-Paare) zu Ihrem Ereignisdatenspeicher hinzu. Mithilfe von Tags können Sie Ihre CloudTrail Ereignisdatenspeicher identifizieren. Sie könnten beispielsweise ein Tag mit dem Namen **stage** und dem Wert **prod** anfügen. Sie können Tags verwenden, um den Zugriff auf Ihren Ereignisdatenspeicher einzuschränken. Sie können Tags auch verwenden, um die Abfrage- und Aufnahmekosten für Ihren Ereignisdatenspeicher zu verfolgen.


Informationen dazu, wie Sie mithilfe von Tags Kosten nachverfolgen, finden Sie unter [Erstellen von benutzerdefinierten Kostenzuweisungs-Tags für CloudTrail Lake-Event-Datenspeicher](#). Informationen darüber, wie Sie IAM-Richtlinien verwenden, um den Zugriff auf einen Ereignisdatenspeicher basierend auf Tags zu autorisieren, finden Sie unter [Beispiele: Verweigern des Zugriffs zum Erstellen oder Löschen von Ereignisdatenspeichern basierend auf Tags](#). Informationen dazu, wie Sie Tags verwenden können AWS, finden Sie unter [Tagging Your AWS Resources User Guide](#) im Tagging AWS Resources User Guide.

10. Wählen Sie Next (Weiter) aus, um den Ereignisdatenspeicher zu konfigurieren.
11. Behalten Sie auf der Seite Ereignisse auswählen die Standardauswahl für den Ereignistyp bei.
12. Für CloudTrail Ereignisse lassen wir die Option Management-Ereignisse ausgewählt und wählen Trail-Ereignisse kopieren. In diesem Beispiel machen wir uns keine Gedanken über die Ereignistypen, da wir den Ereignisdatenspeicher nur zur Analyse vergangener Ereignisse verwenden und keine zukünftigen Ereignisse aufnehmen.

Wenn Sie einen Ereignisdatenspeicher erstellen, der einen vorhandenen Trail ersetzen soll, wählen Sie dieselben Ereigniselektoren wie für Ihren Trail aus, um sicherzustellen, dass der Ereignisdatenspeicher die gleiche Ereignisabdeckung hat.




### CloudTrail events [Info](#)

- Management events**  
Capture management operations performed on your AWS resources.
- Data events**  
Log the resource operations performed on or within a resource.
- Copy trail events**  
Copy CloudTrail events logged in your trails or from S3 buckets.
- Enable for all accounts in my organization**  
To review accounts in your organization, open AWS Organizations. [See all accounts](#) 

▼ **Additional settings**

- Include only the current region (us-east-1) in my event data store**
- Ingest events | [Info](#)**  
Your event data store starts ingesting events when created.

13. Wählen Sie Für alle Konten in meiner Organisation aktivieren aus, wenn es sich um einen Ereignisdatenspeicher für eine Organisation handelt. Diese Option kann nur geändert werden, wenn Sie Konten in AWS Organizations konfiguriert haben.

 **Note**

Wenn Sie einen Ereignisdatenspeicher einer Organisation erstellen, müssen Sie mit dem Verwaltungskonto der Organisation angemeldet sein, da Trail-Ereignisse nur mit dem Verwaltungskonto in den Ereignisdatenspeicher einer Organisation kopiert werden können.

14. Für Zusätzliche Einstellungen deaktivieren wir die Option Ereignisse aufnehmen, da wir in diesem Beispiel nicht möchten, dass der Ereignisdatenspeicher zukünftige Ereignisse aufnimmt, da wir nur daran interessiert sind, die kopierten Ereignisse abzufragen. Standardmäßig sammelt ein Ereignisdatenspeicher Ereignisse für alle AWS-Regionen und beginnt, Ereignisse zu erfassen, sobald er erstellt wird.
15. Für Verwaltungsereignisse behalten wir die Standardeinstellungen bei.

## Management events [Info](#)

Management events show information about management operations performed on resources in your AWS account.

### API activity

Choose the activities you want to log.

- Read  Write
- Exclude AWS KMS events
- Exclude Amazon RDS Data API events
- Enable Insights  
Identify unusual activity, errors, or user behavior in your account.

16. Führen Sie im Bereich Trail-Ereignisse kopieren die folgenden Schritte aus.
  - a. Wählen Sie den Trail aus, die Sie kopieren möchten. In diesem Beispiel wählen wir einen Trail mit dem Namen *Verwaltungsergebnisse* aus.

Standardmäßig werden CloudTrail nur CloudTrail Ereignisse kopiert, die im CloudTrail Präfix des S3-Buckets und die Präfixe innerhalb des CloudTrail Präfixes enthalten sind, und überprüft keine Präfixe für andere Dienste. AWS Wenn Sie CloudTrail Ereignisse kopieren möchten, die in einem anderen Präfix enthalten sind, wählen Sie S3-URI eingeben und dann S3 durchsuchen, um zum Präfix zu wechseln. Wenn der S3-Quell-Bucket für den Trail einen KMS-Schlüssel für die Datenverschlüsselung verwendet, stellen Sie sicher, dass die KMS-Schlüsselrichtlinie das Entschlüsseln der Daten zulässt CloudTrail . Wenn Ihr S3-Quell-Bucket mehrere KMS-Schlüssel verwendet, müssen Sie die Richtlinien für jeden Schlüssel aktualisieren, damit CloudTrail die Daten im Bucket entschlüsselt werden können. Weitere Informationen zum Aktualisieren der KMS-Schlüssel-Richtlinie finden Sie unter [KMS-Schlüsselrichtlinie zum Entschlüsseln von Daten im S3-Quell-Bucket](#).

- b. Wählen Sie einen Zeitraum für das Kopieren der Ereignisse aus. CloudTrail überprüft das Präfix und den Namen der Protokolldatei, um sicherzustellen, dass der Name ein Datum zwischen dem ausgewählten Start- und Enddatum enthält, bevor versucht wird, Trail-Ereignisse zu kopieren. Sie können einen Relative range (Relativen Bereich) oder einen Absolute range (Absoluten Bereich) wählen. Um zu vermeiden, dass Ereignisse zwischen dem Quell-Trail und dem Zielergebnisdatenspeicher dupliziert werden, wählen Sie einen Zeitraum aus, der vor der Erstellung des Ereignisdatenspeichers liegt.

- Wenn Sie Relativer Bereich wählen, können Sie wählen, ob Ereignisse kopiert werden sollen, die in den letzten 6 Monaten, 1 Jahr, 2 Jahren, 7 Jahren oder in einem benutzerdefinierten Bereich protokolliert wurden. CloudTrail kopiert die Ereignisse, die innerhalb des ausgewählten Zeitraums protokolliert wurden.
- Wenn Sie „Absoluter Bereich“ wählen, können Sie ein bestimmtes Start- und Enddatum wählen. CloudTrail kopiert die Ereignisse, die zwischen dem ausgewählten Start- und Enddatum aufgetreten sind.

In diesem Beispiel wählen wir Absoluter Bereich und den gesamten Monat Juni aus.

The screenshot displays the date range selection interface in the AWS CloudTrail console. At the top, there are two tabs: "Relative range" and "Absolute range", with "Absolute range" being the active tab. Below the tabs, there are navigation arrows and the months "June 2023" and "July 2023". A calendar grid shows the days of the month. The dates from June 1st to June 30th are highlighted in blue, indicating the selected range. Below the calendar, there are four input fields: "Start date" (2023/06/01), "Start time" (00:00:00), "End date" (2023/06/30), and "End time" (23:59:59). At the bottom of the interface, there are three buttons: "Clear and dismiss", "Cancel", and "Apply".

- c. Wählen Sie für Permissions (Berechtigungen) unter den folgenden IAM-Rollenoptionen aus. Wenn Sie eine vorhandene IAM-Rolle auswählen, stellen Sie sicher, dass die IAM-Rollenrichtlinie die erforderlichen Berechtigungen bereitstellt. Weitere Informationen zum Aktualisieren der IAM-Rollenberechtigungen finden Sie unter [IAM-Berechtigungen zum Kopieren von Trail-Ereignissen](#).

- Wählen Sie **Create a new role (recommended)** (Erstellen Sie eine neue Rolle (empfohlen)), um eine neue IAM-Rolle zu erstellen. Geben Sie unter IAM-Rollennamen eingeben einen Namen für die Rolle ein. CloudTrail stellt automatisch die erforderlichen Berechtigungen für diese neue Rolle.
- Wählen Sie **Eine benutzerdefinierte IAM-Rolle verwenden** (Use a custom IAM role), um eine benutzerdefinierte IAM-Rolle zu verwenden, die nicht aufgeführt ist. Geben Sie für **Enter IAM role ARN** (IAM-Rollen-ARN eingeben) den IAM-ARN ein.
- Wählen Sie eine vorhandene IAM-Rolle aus der Drop-down-Liste aus.

In diesem Beispiel wählen wir **Neue Rolle erstellen (empfohlen)** und geben den Namen **copy-trail-events** an.

### Copy existing trail events [Info](#)

Choose trail event source

management-events ▼

S3 location of CloudTrail data (S3 URI)

s3://aws-cloudtrail-logs- /AWSLogs/ /CloudTr

Specify a time range of events

2023-06-01T00:00:00-05:00 — 2023-06-30T23:59:59-05:00

**i** All CloudTrail events in your event source are imported, regardless of your event data store's configuration.

Choose IAM role

Create a new role (recommended) ▼

Enter IAM role name

The new role name is prepended with CloudTrailLake-us-east-1-

copy-trail-events

▶ **Permission policies**

17. Wählen Sie Next (Weiter) aus, um Ihre Auswahl zu überprüfen.
18. Überprüfen Sie auf der Seite Prüfen und erstellen Ihre Auswahl. Wählen Sie Bearbeiten aus, um Änderungen am Schema vorzunehmen. Wenn Sie bereit sind, den Ereignisdatenspeicher zu erstellen, wählen Sie Ereignisdatenspeicher erstellen aus.
19. Der neue Ereignisdatenspeicher ist in der Tabelle Ereignisdatenspeicher auf der Seite Ereignisdatenspeicher sichtbar.

Event data stores (3)					
Name	Status	All regions	All accounts	Event type	
my-management-events-eds	Enabled	Yes	No	CloudTrail events	

20. Wählen Sie den Namen des Ereignisdatenspeichers aus, um die Detailseite anzuzeigen. Auf der Detailseite werden die Details zu Ihrem Ereignisdatenspeicher und der Status der Kopie angezeigt. Der Status der Ereigniskopie wird im Bereich Status der Ereigniskopie angezeigt.

Wenn eine Trail-Ereignis-Kopie abgeschlossen ist, wird der Copy status (Kopierstatus) entweder auf Completed (Abgeschlossen) festgelegt, wenn keine Fehler aufgetreten sind, oder auf Failed (Fehlgeschlagen), wenn Fehler aufgetreten sind.

Event copy status (1) <a href="#">Info</a>					
Event log S3 location	Copy status	Copy ID	Created time	Finish time	
s3://aws-cloudtrail-logs-...	Completed	...	July 18, 2023, 15:50:06 (UTC-05:00)	July 18, 2023, 15:53:07 (UTC-05:00)	

21. Um weitere Details zur Kopie anzuzeigen, wählen Sie den Namen der Kopie in der Spalte Ereignisprotokoll-S3-Speicherort aus oder wählen Sie im Menü Aktionen die Option Details anzeigen. Weitere Informationen zum Anzeigen der Details eines Trail-Ereignisses finden Sie unter [Details zur Ereigniskopie](#).

CloudTrail > Lake > Event data stores > my-management-events-trail-events >

**Copy ID** ↻ Actions ▾

**Copy details** info

Event log S3 location s3://aws-cloudtrail-logs- /AWSLogs/ /CloudTrail/	Prefixes copied 817/817 prefixes copied (0 failures)	Created time July 18, 2023, 15:50:06 (UTC-05:00)
Copy ID	Copy status <span style="color: green;">✔ Completed</span>	Finish time July 18, 2023, 16:04:51 (UTC-05:00)

**Copy failures (0)**  
Retry copying prefixes that failed to copy.

< 1 > ⚙

Event location	Error message	Error type
No failures There are currently no copy failures.		

22. Im Bereich Kopierfehler werden alle Fehler angezeigt, die beim Kopieren von Trail-Ereignissen aufgetreten sind. Wenn der Copy status (Kopierstatus) Failed (Fehlgeschlagen) lautet, beheben Sie alle Fehler, die unter Copy failures (Kopierfehler) angezeigt werden, und wählen Sie dann Retry copy (Kopie wiederholen) aus. Wenn Sie erneut versuchen, einen Kopiervorgang durchzuführen, CloudTrail wird der Kopiervorgang an der Stelle fortgesetzt, an der der Fehler aufgetreten ist.

## Lake-Dashboards anzeigen CloudTrail

In dieser exemplarischen Vorgehensweise erfahren Sie, wie Sie CloudTrail Lake-Dashboards anzeigen. CloudTrail Mit [Lake-Dashboards](#) können Sie die Ereignisse in Ihrem Ereignisdatenspeicher visualisieren und Trends erkennen, z. B. die häufigsten Benutzer und die häufigsten Fehler.

Jedes Dashboard besteht aus mehreren Widgets und jedes Widget steht für eine SQL-Abfrage. CloudTrail führt systemgenerierte Abfragen aus, um das Dashboard zu füllen. Für Abfragen fallen Gebühren an, die auf der Menge der gescannten Daten basieren.

### Note

Derzeit sind Dashboards nur für Ereignisdatenspeicher verfügbar, die CloudTrail Verwaltungsereignisse, Amazon S3 S3-Datenereignisse und Insights-Ereignisse erfassen.

Zeigen Sie Lake-Dashboards wie folgt an:

1. Melden Sie sich bei der an AWS Management Console und öffnen Sie die CloudTrail Konsole unter <https://console.aws.amazon.com/cloudtrail/>.
2. Wählen Sie im Navigationsbereich unter Lake die Option Dashboard aus.
3. Wenn Sie die Seite „Dashboards“ zum ersten Mal aufrufen, werden Sie CloudTrail aufgefordert, die mit der Ausführung von Abfragen verbundenen Kosten zu bestätigen. Wählen Sie Ich stimme zu aus, um die Kosten für die Ausführung von Abfragen zu akzeptieren. Dies ist eine einmalige Bestätigung. Weitere Informationen zur CloudTrail Preisgestaltung finden Sie unter [CloudTrailPreise](#).
4. Wählen Sie Ihren Ereignisdatenspeicher aus der Liste aus und wählen Sie dann den Dashboard-Typ aus, den Sie anzeigen möchten.

Die folgenden Dashboardtypen sind möglich:

- **Übersichts-Dashboard** — Zeigt die aktivsten Benutzer AWS-Services nach Anzahl der Ereignisse an. AWS-Regionen Sie können auch Informationen über die Aktivität von `read`- und `write`-Verwaltungsereignissen, die am stärksten beeinträchtigten Ereignisse und die häufigsten Fehler anzeigen. Dieses Dashboard ist für Ereignisdatenspeicher verfügbar, die Verwaltungsereignisse erfassen.
- **Dashboard für Verwaltungsereignisse** – Zeigt Anmeldeereignisse auf der Konsole, Ereignisse mit Zugriffsverweigerung, destruktive Aktionen und die häufigsten Fehler pro Benutzer an. Sie können auch Informationen zu TLS-Versionen und veralteten TLS-Aufrufen nach Benutzern anzeigen. Dieses Dashboard ist für Ereignisdatenspeicher verfügbar, die Verwaltungsereignisse erfassen.
- **Dashboard für S3-Datenereignisse** – Zeigt die S3-Kontoaktivitäten, die am häufigsten aufgerufenen S3-Objekte, die wichtigsten S3-Benutzer und die wichtigsten S3-Aktionen an. Dieses Dashboard ist für Ereignisdatenspeicher verfügbar, die Amazon-S3-Datenaktionen erfassen.
- **Dashboard für Insights-Ereignisse** – Zeigt den Gesamtanteil der Insights-Ereignisse nach Insights-Typ, den Anteil der Insights-Ereignisse nach Insights-Typ für die wichtigsten Benutzer und Services sowie die Anzahl der Insights-Ereignisse pro Tag. Das Dashboard enthält auch ein Widget, das Insights-Ereignisse für bis zu 30 Tage auflistet. Dieses Dashboard ist nur für Ereignisdatenspeicher verfügbar, die Insights-Ereignisse erfassen.

**Note**

- Nachdem Sie CloudTrail Insights zum ersten Mal im Quelldatenspeicher für Ereignisse aktiviert haben, kann es bis zu 7 Tage dauern, CloudTrail bis das erste Insights-Ereignis übermittelt wird, wenn ungewöhnliche Aktivitäten festgestellt werden. Weitere Informationen finden Sie unter [Grundlegendes zur Insights-Ereignisbereitstellung](#).
- Das Dashboard für Insights-Ereignisse zeigt nur Informationen zu den Insights-Ereignissen an, die vom ausgewählten Ereignisdatenspeicher erfasst wurden. Dies hängt von der Konfiguration des ursprünglichen Ereignisdatenspeicher ab. Wenn Sie beispielsweise den ursprünglichen Ereignisdatenspeicher so konfigurieren, dass Insights-Ereignisse für `ApiCallRateInsight`, aber nicht für `ApiErrorRateInsight` aktiviert werden, werden Ihnen keine Informationen über Insights-Ereignisse für `ApiErrorRateInsight` angezeigt.

In diesem Beispiel haben wir das Dashboard Übersicht ausgewählt.

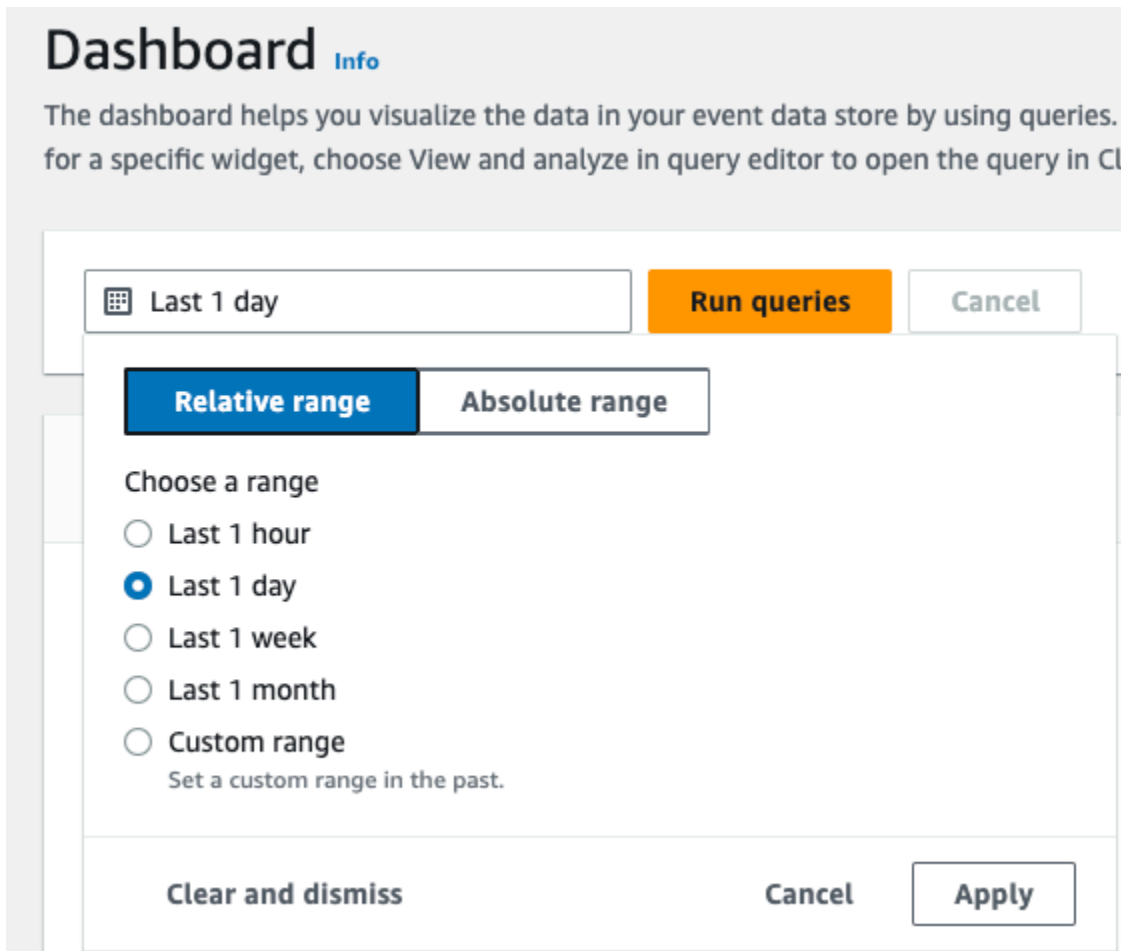
The screenshot shows the AWS CloudTrail Insights Dashboard. At the top, there is a header "Dashboard" with an "Info" link. Below the header is a descriptive paragraph: "The dashboard helps you visualize the data in your event data store by using queries. You can choose the event data store and the type of dashboard you want to view. You can also filter by a date or time range. To view the query for a specific widget, choose View and analyze in query editor to open the query in CloudTrail's query editor." Below this is a control bar with a date range selector set to "Last 1 day", a "Run queries" button, and a "Cancel" button. On the right, there is a dropdown menu for the event data store, currently showing "my-management-eve...", and another dropdown menu for the dashboard type, currently showing "Overview" and highlighted with a yellow box. The main content area is divided into two columns. The left column is titled "Account activity" and the right column is titled "Top errors". Both columns display a message: "No data available. This is because you have not run any queries before." At the bottom of each column, there is a link "View and analyze in query editor" and a refresh icon.

5. Wählen Sie das Datumsfeld aus, um nach einem Zeitraum zu filtern, und wählen Sie dann Anwenden. Wählen Sie Absoluter Bereich, um ein bestimmtes Datum und eine bestimmte Zeitspanne auszuwählen. Wählen Sie Relativer Bereich, um einen vordefinierten Zeitraum oder einen benutzerdefinierten Bereich auszuwählen. Standardmäßig zeigt das Dashboard Ereignisdaten der letzten 24 Stunden an.



**Note**

Da CloudTrail Abfragen auf der Grundlage der Menge der gescannten Daten berechnet werden, können Sie die Kosten senken, indem Sie nach einem engeren Zeitraum filtern.



6. Wählen Sie Abfragen ausführen aus, um das Dashboard mit Daten zu füllen. Jedes Widget zeigt einzeln den Status der zugehörigen Abfrage an und präsentiert Daten, wenn die Abfrage abgeschlossen ist.

Sie können zusätzliche Filter für einige Widgets durchführen, z. B. für Kontoaktivitäten, sodass Sie nach `read`- und `write`-Ereignisaktivitäten filtern können.

**Dashboard** Info

The dashboard helps you visualize the data in your event data store by using queries. You can choose the event data store and the type of dashboard you want to view. You can also filter by a date or time range. To view the query for a specific widget, choose View and analyze in query editor to open the query in CloudTrail's query editor.

2023-06-29T10:34:53-05:00 — 2023-06-30T10:34:53-05:00 Run queries Cancel my-management-eve... Overview

Query creation time: June 30, 2023 at 10:34 (UTC-5:00)

**Account activity**

Filter displayed data

Filter data

- read
- write

4K  
2K  
0

Jun 29 15:00 Jun 29 18:00 Jun 29 21:00 Jun 30 24:00 Jun 30 03:00 Jun 30 06:00 Jun 30 09:00 Jun 30 12:00

— read — write

[View and analyze in query editor](#)

**Top errors** < 1 2 >

ReplicationConfigurationNotFoundError	34
ObjectLockConfigurationNotFoundError	34
NoSuchCORSConfiguration	34
NoSuchWebsiteConfiguration	34
NoSuchLifecycleConfiguration	32
NoSuchTagSet	32
QueryIdNotFoundException	24
NoSuchPublicAccessBlockConfiguration	10

[View and analyze in query editor](#)

- Um die Abfrage für ein Widget anzuzeigen, wählen Sie Im Abfrage-Editor anzeigen und analysieren aus.

**Account activity**

Filter displayed data

Filter data

8K  
6K  
4K  
2K  
0

Jun 29 15:00 Jun 29 18:00 Jun 29 21:00 Jun 30 24:00 Jun 30 03:00 Jun 30 06:00 Jun 30 09:00 Jun 30 12:00

— read — write

[View and analyze in query editor](#)

Wenn Sie im Abfrage-Editor anzeigen und analysieren wählen, wird die Abfrage im Abfrage-Editor von CloudTrail Lake geöffnet, sodass Sie die Abfrageergebnisse außerhalb des Dashboards weiter analysieren können. Weitere Informationen zum Bearbeiten einer Abfrage finden Sie unter [Abfrage erstellen oder bearbeiten](#). Weitere Informationen zum Ausführen einer Abfrage und zum Speichern von Abfrageergebnissen finden Sie unter [Ausführen einer Abfrage und Speichern von Abfrageergebnissen](#).

The screenshot displays the AWS CloudTrail Lake Query Editor. On the left, there's a sidebar with 'Event data store' set to 'my-management-events-eds' and a list of event properties. The main area contains a SQL query editor with the following query:

```

1 SELECT
2   DATE_TRUNC('hour', eventTime) as eventDate,
3   IF(readOnly, 'read', 'write') as readOnly,
4   count(*) as eventCount
5 FROM
6   [redacted]
7 WHERE
8   eventTime > '2023-06-29T15:34:53.787Z'
9   AND eventTime < '2023-06-30T15:34:53.787Z'
10  -- AND recipientAccountId = '123456789012' -- Filter on a specific account
11 GROUP BY
12  DATE_TRUNC('hour', eventTime),
13  readOnly

```

Below the query editor are 'Run', 'Save', and 'Clear' buttons. The 'Output' section at the bottom shows a table with columns: Time stamp, Status, Delivery status, Response, Query SQL, Query ID, and Event data store. The first row shows a successful query on June 30, 2023, with 49 records matched.

Weitere Informationen zu Dashboards finden Sie unter [CloudTrail Lake-Dashboards anzeigen](#).

## CloudTrail Lake-Beispielabfragen anzeigen und ausführen

CloudTrail Lake bietet eine Reihe von Beispielabfragen, die Ihnen den Einstieg in das Schreiben eigener Abfragen erleichtern können. In dieser exemplarischen Vorgehensweise wird gezeigt, wie Sie eine Beispielabfrage auswählen und ausführen.

Für Abfragen fallen Gebühren an, die auf der Menge der gescannten Daten basieren. Um die Kosten zu kontrollieren, empfehlen wir Ihnen, Abfragen einzuschränken, indem Sie eventTime-Start- und Ende-Zeitstempel zu Abfragen hinzufügen. Weitere Informationen zur CloudTrail Preisgestaltung finden Sie unter [AWS CloudTrail Preise](#).

Führen Sie eine Beispielabfrage wie folgt durch:

1. Melden Sie sich bei der an AWS Management Console und öffnen Sie die CloudTrail Konsole unter <https://console.aws.amazon.com/cloudtrail/>.
2. Wählen Sie im Navigationsbereich unter Lake die Option Abfrage aus.
3. Wählen Sie auf der Seite Abfrage die Registerkarte Beispielabfragen aus.
4. Wählen Sie eine Beispielabfrage aus der Liste aus oder suchen Sie nach der Abfrage, um die Liste zu filtern. In diesem Beispiel öffnen wir die Abfrage Untersuchen, wer Änderungen an der Konsole vorgenommen hat, indem Sie Namen der Abfrage auswählen. Dies öffnet die Abfrage in der Registerkarte Editor.

The screenshot shows the 'Query' page in the AWS CloudTrail console. It features a navigation bar with tabs for 'Editor', 'Results history', 'Saved queries', 'Sample queries', and 'How it works'. Below the navigation bar, there is a section for 'Sample queries (45)' with a search bar and pagination controls. A table lists several sample queries. The query 'Investigate who made console changes' is highlighted with a yellow box. The table columns are 'Query name', 'Query description', and 'Query SQL'.

Query name	Query description	Query SQL
Find who is making calls using outdated TLS versions	Find the callers who used outdated Transport Layer Security (TLS) versions 1.0 and 1.1 within the past week grouped by the number of calls per service.	SELECT recipientAccountId, year(eventTime) AS year_date, month(eventTime) AS month_date, eventSource, sourceIPAddress, userAgent, useridentity.arn, useridentity.accesskeyid, COUNT(*) AS numCalls FROM \$EDS_ID WHERE tlsDetails.tlsVersion IN ('TLSv1', 'TLSv1.1') AND eventTime > '2023-06-23 00:00:00' GROUP BY recipientAccountId, year(eventTime), month(eventTime), eventSource, sourceIPAddress, userAgent, useridentity.arn, useridentity.accesskeyid ORDER BY COUNT(*) DESC
Investigate who made console changes	Find users with write permissions who made changes using the console within the past week.	SELECT useridentity.arn AS user, eventName, eventTime, .Region, requestParameters AS resourceChangedManually FROM \$EDS_ID WHERE sessionCredentialFromConsole='true' AND errorCode IS NULL AND eventTime > '2023-06-23 00:00:00'

5. Wählen Sie auf der Registerkarte Editor den Ereignisdatenspeicher aus, für den Sie die Abfrage ausführen möchten. Wenn Sie den Ereignisdatenspeicher aus der Liste auswählen, CloudTrail wird automatisch die ID des Ereignisdatenspeichers in die FROM Zeile des Abfrage-Editors eingetragen.

The screenshot shows the AWS CloudTrail Query Editor interface. On the left, the 'Event data store' dropdown is highlighted with a yellow box, showing 'my-management-events-eds' selected. Below it, the 'Event properties' section is visible. The main area contains a SQL query editor with the following query:

```
1 SELECT
2   userIdentity.arn AS user, eventName, eventTime, awsRegion, requestParameters AS resourceChangedManually
3 FROM
4   [redacted]
5 WHERE
6   sessionCredentialFromConsole='true' AND errorCode IS NULL
7   AND eventTime > '2023-06-23 00:00:00'
```

Below the query editor, the 'Run' button is highlighted with a yellow box. The 'Query results' and 'Command output' tabs are visible, with 'Command output' selected. The 'Output' section shows a table with columns: Time stamp, Status, Delivery status, Response, Query SQL, Query ID, and Event data st... The 'Status' column is highlighted with a yellow box, showing a green checkmark and the word 'Successful'.

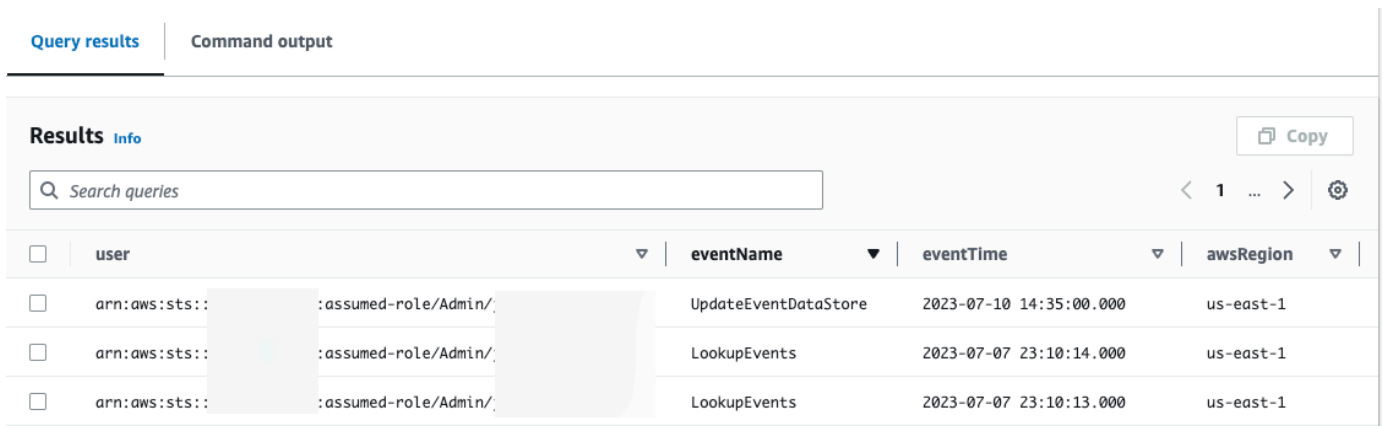
6. Wählen Sie dann Ausführen aus, um die Abfrage auszuführen.

Auf der Registerkarte Befehlsausgabe werden Metadaten zu Ihrer Abfrage angezeigt, z. B. ob die Abfrage erfolgreich war, die Anzahl der übereinstimmenden Datensätze und die Laufzeit der Abfrage.

The screenshot shows the 'Output' section of the AWS CloudTrail Query Editor. The 'Status' column is highlighted with a yellow box, showing a green checkmark and the word 'Successful'. The table below shows the following data:

Time stamp	Status	Delivery status	Response	Query SQL	Query ID	Event data st...
June 30, 2023, 2...	Successful		1467 records ma...	SELECT userIdentity.ar	[redacted]	my-management-ever

Auf der Registerkarte Abfrageergebnisse werden die Ereignisdaten im ausgewählten Ereignisdatenspeicher angezeigt, die Ihrer Abfrage entsprachen.



<input type="checkbox"/>	user	eventName	eventTime	awsRegion
<input type="checkbox"/>	arn:aws:sts:: :assumed-role/Admin/	UpdateEventDataStore	2023-07-10 14:35:00.000	us-east-1
<input type="checkbox"/>	arn:aws:sts:: :assumed-role/Admin/	LookupEvents	2023-07-07 23:10:14.000	us-east-1
<input type="checkbox"/>	arn:aws:sts:: :assumed-role/Admin/	LookupEvents	2023-07-07 23:10:13.000	us-east-1

Weitere Informationen zum Bearbeiten einer Abfrage finden Sie unter [Abfrage erstellen oder bearbeiten](#). Weitere Informationen zum Ausführen einer Abfrage und zum Speichern von Abfrageergebnissen finden Sie unter [Ausführen einer Abfrage und Speichern von Abfrageergebnissen](#).

## Speichern Sie die CloudTrail Lake-Abfrageergebnisse in einem S3-Bucket

Diese exemplarische Vorgehensweise zeigt, wie Sie CloudTrail Lake-Abfrageergebnisse in einem S3-Bucket speichern und diese Abfrageergebnisse dann herunterladen können.

Wenn Sie Abfragen in CloudTrail Lake ausführen, fallen Gebühren an, die auf der Menge der von der Abfrage gescannten Daten basieren. Für das Speichern von Abfrageergebnissen in einem S3-Bucket fallen keine zusätzlichen CloudTrail Lake-Gebühren an, es fallen jedoch S3-Speichergebühren an. Weitere Informationen zu S3-Preisen finden Sie unter [Preise für Amazon S3](#).

Wenn Sie Abfrageergebnisse speichern, werden die Abfrageergebnisse möglicherweise in der CloudTrail Konsole angezeigt, bevor sie im S3-Bucket angezeigt werden, da CloudTrail die Abfrageergebnisse erst nach Abschluss des Abfragescans angezeigt werden. Die meisten Abfragen werden zwar je nach Größe Ihres Ereignisdatenspeichers innerhalb weniger Minuten abgeschlossen, es kann jedoch erheblich länger dauern, CloudTrail bis Abfrageergebnisse an Ihren S3-Bucket übermittelt werden. CloudTrail übermittelt die Abfrageergebnisse im komprimierten Gzip-Format an den S3-Bucket. Im Durchschnitt können Sie nach Abschluss des Abfragescans mit einer Latenz von 60 bis 90 Sekunden für jedes GB an Daten rechnen, das an den S3-Bucket übermittelt wird.

## Speichern von Abfrageergebnissen in einen Amazon-S3-Bucket

1. Melden Sie sich bei der an AWS Management Console und öffnen Sie die CloudTrail Konsole unter <https://console.aws.amazon.com/cloudtrail/>.
2. Wählen Sie im Navigationsbereich unter Lake die Option Abfrage.
3. Wählen Sie auf den Registerkarten Beispielabfragen oder Gespeicherte Abfragen eine Abfrage aus, die ausgeführt werden soll, indem Sie den Abfragenamen auswählen. In diesem Beispiel wählen wir die Beispielabfrage mit dem Namen Benutzeraktionen untersuchen aus.
4. Wählen Sie auf der Registerkarte Editor für Ereignisdatenspeicher einen Ereignisdatenspeicher aus der Dropdown-Liste aus. Wenn Sie den Ereignisdatenspeicher aus der Liste auswählen, CloudTrail wird automatisch die ID des Ereignisdatenspeichers in die From Zeile eingetragen.
5. In dieser Beispielabfrage bearbeiten wir den `userIdentity.ARN`-Wert, um einen Benutzer mit dem Namen Admin anzugeben. Wir behalten die Standardwerte für `eventTime` bei. Wenn Sie eine Abfrage ausführen, wird Ihnen die Menge der gescannten Daten berechnet. Um die Kosten zu kontrollieren, empfehlen wir Ihnen, Abfragen einzuschränken, indem Sie `eventTime`-Start- und Ende-Zeitstempel zu Abfragen hinzufügen.



```
1 SELECT
2   eventID, eventName, eventSource, eventTime, userIdentity.arn AS user
3 FROM
4   2a8f2138-0caa-46c8-a194-
5 WHERE
6   userIdentity.arn LIKE '%Admin%'
7   AND eventTime > '2023-07-21 00:00:00' AND eventTime < '2023-07-24 00:00:00'
```

6. Wählen Sie die Option Ergebnisse in S3 speichern, um die Abfrageergebnisse in einem S3-Bucket zu speichern. Wenn Sie den Standard-S3-Bucket auswählen, werden die erforderlichen Bucket-Richtlinien CloudTrail erstellt und angewendet. Wenn Sie den Standard-S3-Bucket wählen, muss Ihre IAM-Richtlinie die Genehmigung für die `s3:PutEncryptionConfiguration` Aktion enthalten, da die serverseitige Verschlüsselung standardmäßig für den Bucket aktiviert ist. Weitere Informationen zum Speichern von Abfrageergebnissen finden Sie unter [Zusätzliche Informationen über gespeicherte Abfrageergebnisse](#). In diesem Beispiel wird der standardmäßige S3-Bucket verwendet.

**Note**

Um einen anderen Bucket zu verwenden, geben Sie einen Bucket-Namen an oder wählen Sie S3 durchsuchen, um einen Bucket auszuwählen. Die Bucket-Richtlinie muss die CloudTrail Erlaubnis erteilen, Abfrageergebnisse an den Bucket zu übermitteln. Informationen zur manuellen Bearbeitung der Bucket-Richtlinie finden Sie im Abschnitt [Amazon S3 S3-Bucket-Richtlinie für CloudTrail Lake-Abfrageergebnisse](#).

Investigate user actions +

```
1 SELECT
2   eventID, eventName, eventSource, eventTime, userIdentity.arn AS user
3 FROM
4   2a8f2138-0caa-46c8-a194-
5 WHERE
6   userIdentity.arn LIKE '%Admin%'
7   AND eventTime > '2023-07-21 00:00:00' AND eventTime < '2023-07-24 00:00:00'
```

Run Save Clear

Save results to S3

Q s3://aws-cloudtrail-lake-query-results- X

Browse S3

- Wählen Sie Ausführen aus. Abhängig von der Größe Ihres Ereignisdatenspeichers und der Anzahl der darin enthaltenen Daten kann die Ausführung einer Abfrage mehrere Minuten dauern. Die Registerkarte Befehlsausgabe zeigt den Status einer Abfrage an und ob eine Abfrage abgeschlossen ist. Wenn eine Abfrage abgeschlossen ist, öffnen Sie die Option Abfrageergebnisse, um eine Ergebnistabelle für die aktive Abfrage anzuzeigen (die derzeit im Editor angezeigte Abfrage).
- Wenn die Übermittlung der gespeicherten Abfrageergebnisse an Ihren S3-Bucket CloudTrail abgeschlossen ist, enthält die Spalte Lieferstatus einen Link zum S3-Bucket, der Ihre gespeicherten Abfrageergebnisdateien sowie eine [Signierdatei](#) enthält, mit der Sie Ihre gespeicherten Abfrageergebnisse überprüfen können. Wählen Sie In S3 anzeigen, um die Abfrageergebnisdateien anzuzeigen und Dateien im S3-Bucket zu signieren.



### Note

Wenn Sie Abfrageergebnisse speichern, werden die Abfrageergebnisse möglicherweise in der CloudTrail Konsole angezeigt, bevor sie im S3-Bucket sichtbar sind, da CloudTrail die Abfrageergebnisse erst nach Abschluss des Abfragescans angezeigt werden. Die meisten Abfragen werden zwar je nach Größe Ihres Ereignisdatenspeichers innerhalb weniger Minuten abgeschlossen, es kann jedoch erheblich länger dauern, CloudTrail bis Abfrageergebnisse an Ihren S3-Bucket übermittelt werden. CloudTrail übermittelt die Abfrageergebnisse im komprimierten Gzip-Format an den S3-Bucket. Im Durchschnitt können Sie nach Abschluss des Abfragescans mit einer Latenz von 60 bis 90 Sekunden für jedes GB an Daten rechnen, das an den S3-Bucket übermittelt wird.

Time stamp	Status	Delivery status	Response	Query SQL	Query ID	Event data store
July 28, 2023, 18:20...	Successful	<a href="#">View in S3</a>	468 records matche...	SELECT eventID, eventNar	52ab2728-06de-4dac-8c5	my-management-events-

9. Um Ihre Abfrageergebnisse herunterzuladen, wählen Sie die Abfrageergebnisdatei (in diesem Beispiel `result_1.csv.gz`) und klicken Sie dann auf Herunterladen.

52ab2728-06de-4dac-8c53- / Copy S3 URI

Objects Properties

Objects (2)  
Objects are the fundamental entities stored in Amazon S3. You can use [Amazon S3 Inventory](#) to get a list of all objects in your bucket. For others to access your objects, you'll need to explicitly grant them permissions. [Learn more](#)

Find objects by prefix   Show versions

Name	Type	Last modified	Size	Storage class
<input checked="" type="checkbox"/> <a href="#">result_1.csv.gz</a>	gz	July 28, 2023, 13:20:12 (UTC-05:00)	13.8 KB	Standard
<input type="checkbox"/> <a href="#">result_sign.json</a>	json	July 28, 2023, 13:20:18 (UTC-05:00)	929.0 B	Standard

Informationen zum Validieren von gespeicherten Abfrageergebnissen finden Sie unter [Validierung von gespeicherten Abfrageergebnissen](#).

# Anzeige Ihrer CloudTrail Kosten und Nutzung mit AWS Cost Explorer

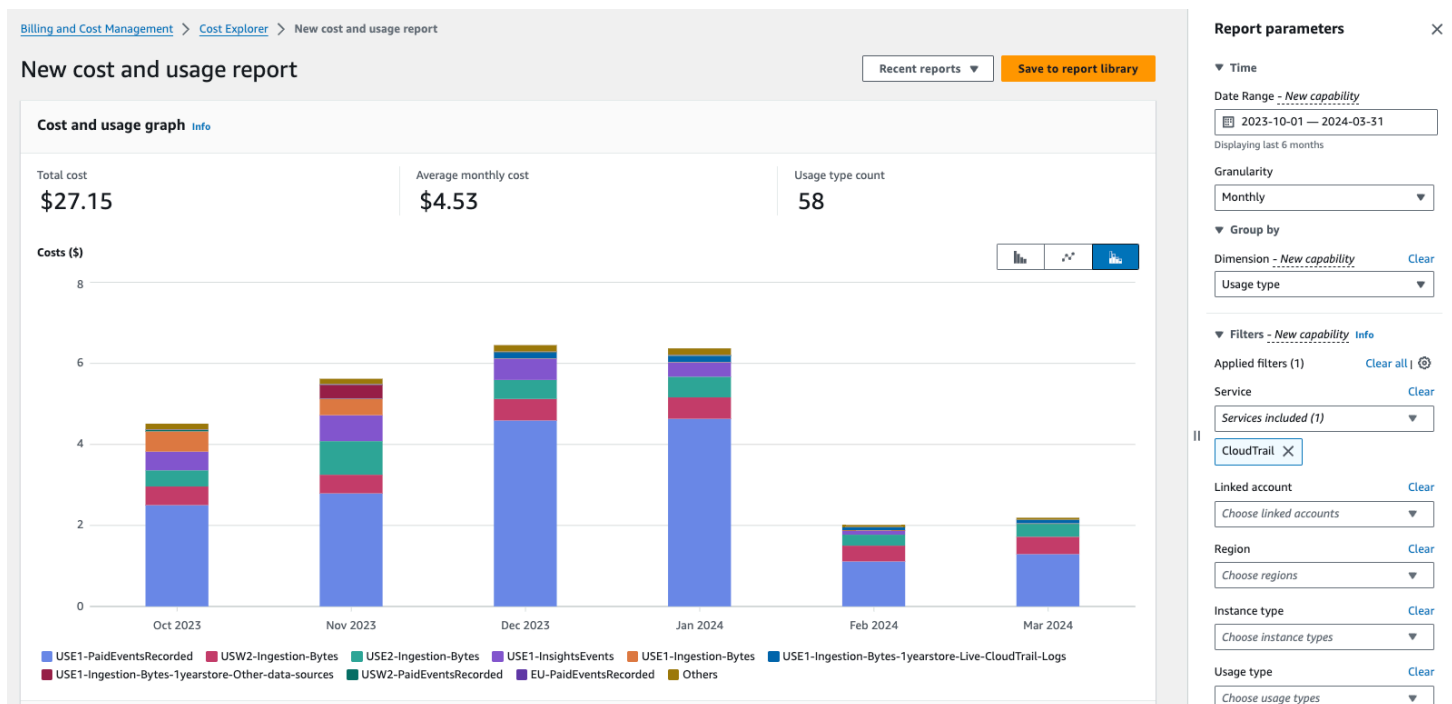
In diesem Abschnitt wird beschrieben, wie Sie Ihre CloudTrail Kosten und Ihre Nutzung einsehen können [AWS Cost Explorer](#). Mit Cost Explorer können Sie Ihre AWS Kosten und Nutzung im Laufe der Zeit visualisieren, verstehen und verwalten.

Einzelheiten zur CloudTrail Preisgestaltung finden Sie unter [AWS CloudTrail Preise](#).

So zeigen Sie CloudTrail Kosten und Nutzung mit Cost Explorer an

1. Melden Sie sich bei der an AWS Management Console und öffnen Sie die Cost Explorer Explorer-Konsole unter <https://console.aws.amazon.com/cost-management/home#/custom>.
2. Wählen Sie unter Zeit den Datumsbereich aus, den Sie analysieren möchten.
3. Wählen Sie unter Gruppieren nach für Dimension die Option Verwendungstyp aus.
4. Wählen Sie unter Filter für Service die Option aus CloudTrail.

Die folgende Abbildung zeigt ein Beispiel für einen Kostenbericht, der nach Nutzungstyp gefiltert CloudTrail und nach diesem gruppiert wurde.



Überprüfen Sie den Nutzungstyp, um zu sehen, welche CloudTrail Funktionen die meisten Kosten verursacht haben. Jeder Nutzungstyp beginnt mit dem Code für den AWS-Region Ort, an dem die Gebühr angefallen ist.

In der folgenden Tabelle werden die CloudTrail Nutzungstypen für die einzelnen CloudTrail Funktionen beschrieben.

CloudTrail Merkmal	Verwendungstyp	Beschreibung
CloudTrail Pfade	<i>region</i> -FreeEventsRecorded	Die erste Kopie von Management-Veranstaltungen wurde kostenlos an eine geliefert AWS-Region.
	<i>region</i> -PaidEventsRecorded	Die Gebühr für zusätzliche Kopien von Managementereignissen, die an eine geliefert werden AWS-Region.
	<i>region</i> -DataEventsRecorded	Die Gebühr für die Lieferung von Datenereignissen an eine AWS-Region. Für Datenereignisse fallen immer Gebühren an.
CloudTrail See	<i>region</i> -Ingestion-Bytes	Die Gebühr für die Aufnahme von Ereignissen in

CloudTrail Merkmal	Verwendungstyp	Beschreibung
		<p>einen CloudTrail Lake Event Data Store mit der Preisoption „Sieben Jahre Aufbewahrung“. Die Preise für die Datenaufnahme basieren auf dem aufgenommenen Datenvolumen und sind für alle Ereignistypen gleich.</p>
	<p><i>region</i>-Ingestion-Bytes-1yearstore-Live-CloudTrail-Logs</p>	<p>Die Gebühr für die Aufnahme von CloudTrail Datenereignissen und Verwaltungseignissen in einen CloudTrail Lake Event Data Store unter Verwendung der Preisoption „Verlängerbare Aufbewahrung um ein Jahr“.</p>

CloudTrail Merkmal	Verwendungstyp	Beschreibung
	<i>region</i> -Ingestion-Bytes-1yearstore-Other-data-sources	Die Gebühr für die Aufnahme anderer Ereignisquellen in einen CloudTrail Lake Event Data Store unter Verwendung der Preisoption „Verlängerbare Aufbewahrung um ein Jahr“. Dazu gehören CloudTrail Insights-Ereignisse, Konfigurationselemente von AWS Config, Beweise aus AWS Audit Manager, (unkomprimierte) historische CloudTrail Protokolle, die aus S3 importiert wurden, und Ereignisse außerhalb von AWS.

CloudTrail Merkmal	Verwendungstyp	Beschreibung
	<i>region</i> -QueryScanned-Bytes	Die Gebühr für die Ausführung von CloudTrail Lake-Abfragen. Wenn Sie Abfragen in CloudTrail Lake ausführen, fallen Gebühren an, die auf der Menge der gescannten optimierten und komprimierten Daten basieren.
CloudTrail Einblicke	<i>region</i> -InsightsEvents	Die Gebühr für CloudTrail Insights-Veranstaltungen. Für Insights-Ereignisse fallen Gebühren an, die auf der Anzahl der pro Insight-Typ analysierten Verwaltungsgereignisse basieren.

## Weitere Ressourcen

- [AWS CloudTrail Preise](#)
- [Verwaltung der CloudTrail Trailkosten](#)

- [Verwaltung der CloudTrail Seekosten](#)

# Mit dem CloudTrail Eventverlauf arbeiten

CloudTrail ist standardmäßig für Ihr AWS Konto aktiviert und Sie haben automatisch Zugriff auf den CloudTrail Eventverlauf. Der Ereignisverlauf stellt eine anzeigbare, durchsuchbare, herunterladbare und unveränderliche Aufzeichnung der Verwaltungsereignisse der letzten 90 Tage in einer AWS-Region bereit. Diese Ereignisse erfassen Aktivitäten AWS Management Console, die über die AWS SDKs und APIs AWS Command Line Interface,, durchgeführt wurden. In der Ereignishistorie werden Ereignisse an dem AWS-Region Ort aufgezeichnet, an dem das Ereignis stattgefunden hat. Für die Anzeige des Eventverlaufs CloudTrail fallen keine Gebühren an.

Sie können Ereignisse im Zusammenhang mit der Erstellung, Änderung oder Löschung von Ressourcen (wie IAM-Benutzern oder Amazon EC2 EC2-Instances) in Ihrer AWS-Konto eigenen Region in der CloudTrail Konsole nachschlagen, indem Sie die Seite mit dem Ereignisverlauf aufrufen. Sie können diese Ereignisse auch nachschlagen, indem Sie den Befehl [aws cloudtrail lookup-events](#) ausführen oder die [LookupEvents](#)-API verwenden.

Sie können die Seite mit dem Ereignisverlauf in der CloudTrail Konsole verwenden, um Kontoaktivitäten in Ihrer gesamten Infrastruktur anzuzeigen, zu suchen, herunterzuladen, zu archivieren, zu analysieren und darauf zu reagieren. AWS Sie können Ihre [Ansicht des Ereignisverlaufs in der Konsole anpassen](#), indem Sie auswählen, wie viele Ereignisse auf jeder Seite und welche Spalten angezeigt werden sollen. Sie können auch die Details von Ereignissen im Ereignisverlauf vergleichen side-by-side. Sie können [Ereignisse mithilfe der AWS SDKs oder programmgesteuert nachschlagen](#). AWS Command Line Interface

## Note

Im Laufe der Zeit AWS-Services können weitere Ereignisse hinzugefügt werden. CloudTrail zeichnet diese Ereignisse im Ereignisverlauf auf, aber eine vollständige 90-Tage-Aufzeichnung der Aktivitäten, einschließlich hinzugefügter Ereignisse, ist erst 90 Tage nach dem Hinzufügen der Ereignisse verfügbar.

Der Ereignisverlauf ist unabhängig von allen Trails oder Ereignisdatenspeichern, die Sie für Ihr Konto erstellen. Änderungen, die Sie an Ihren Ereignisdatenspeichern oder Trails vornehmen, wirken sich nicht auf den Ereignisverlauf aus.

In den folgenden Abschnitten wird beschrieben, wie Sie mithilfe der CloudTrail Konsole und der nach aktuellen Verwaltungsereignissen suchen. Außerdem wird beschrieben AWS CLI, wie Sie eine Datei



mit Ereignissen herunterladen. Informationen zur Verwendung der LookupEvents API zum Abrufen von Informationen aus CloudTrail Ereignissen finden Sie [LookupEvents](#) in der AWS CloudTrail API-Referenz.

## Topics

- [Einschränkungen des Ereignisverlaufs](#)
- [Aktuelle Verwaltungsereignisse mit der Konsole anzeigen](#)
- [Aktuelle Managementereignisse anzeigen mit dem AWS CLI](#)

## Einschränkungen des Ereignisverlaufs

Die folgenden Einschränkungen gelten für den Ereignisverlauf.

- Auf der Seite mit dem Ereignisverlauf in der CloudTrail Konsole werden nur Verwaltungsereignisse angezeigt. Es werden keine Datenereignisse oder Insights-Ereignisse angezeigt.
- Der Eventverlauf ist auf die Ereignisse der letzten 90 Tage beschränkt. Für eine fortlaufende Aufzeichnung der Ereignisse in Ihrem AWS-Konto, erstellen Sie einen [Ereignisdatenspeicher](#) oder einen [Trail](#).
- Wenn Sie Ereignisse von der Seite „Ereignisverlauf“ auf der CloudTrail Konsole herunterladen, können Sie bis zu 200.000 Ereignisse in einer einzigen Datei herunterladen. Wenn Sie das Limit von 200.000 Ereignissen erreichen, bietet die CloudTrail Konsole die Möglichkeit, zusätzliche Dateien herunterzuladen.
- Der Ereignisverlauf bietet keine Zusammenfassung von Ereignissen auf Organisationsebene. Um Ereignisse in Ihrer gesamten Organisation aufzuzeichnen, erstellen Sie einen Ereignisdatenspeicher für Ihre Organisation oder einen Trail.
- Eine Suche im Ereignisverlauf ist auf ein einzelnes Ereignis beschränkt AWS-Konto, gibt nur Ereignisse aus einem einzelnen AWS-Region Ereignis zurück und kann nicht mehrere Attribute abfragen. Sie können nur jeweils einen Attribut-Filter und jeweils einen Zeitbereichs-Filter anwenden.

Sie können einen CloudTrail Lake-Ereignisdatenspeicher für Abfragen über mehrere Attribute und erstellen AWS-Regionen. Sie können auch mehrere Abfragen innerhalb AWS-Konten einer AWS Organizations Organisation durchführen. In CloudTrail Lake können Sie mehrere Ereignistypen abfragen, darunter Verwaltungsereignisse, Datenereignisse, Insights-Ereignisse, AWS Config Konfigurationselemente, Audit Manager Manager-Beweise und AWS Nichtereignisse.

CloudTrail Lake-Abfragen bieten eine umfassendere und besser anpassbare Ansicht von Ereignissen als einfache Schlüssel- und Werteabfragen in der Ereignishistorie oder in der AusführungLookupEvents. Weitere Informationen finden Sie unter [Mit AWS CloudTrail Lake arbeiten](#) und [Erstellen Sie mit der Konsole einen Ereignisdatenspeicher für CloudTrail Ereignisse](#).

- Sie können keine Amazon RDS Data API-Ereignisse aus dem Event-Verlauf ausschließen AWS KMS . Einstellungen, die Sie auf einen Trail- oder Event-Datenspeicher anwenden, gelten nicht für den Event-Verlauf.

## Aktuelle Verwaltungsereignisse mit der Konsole anzeigen

Auf der Seite „Ereignisverlauf“ in der CloudTrail Konsole können Sie sich die Verwaltungsereignisse der letzten 90 Tage in einer Region anzeigen lassen. Sie können auch eine Datei mit diesen Informationen oder eine Teilmenge von Informationen basierend auf dem ausgewählten Filter und Zeitbereich herunterladen. Sie können Ihre Ansicht des Ereignisverlaufs anpassen, indem Sie auswählen, wie viele Ereignisse auf jeder Seite angezeigt werden sollen und welche Spalten in der Konsole angezeigt werden sollen. Außerdem können Sie Ereignisse nach den Ressourcentypen abfragen und filtern, die für einen bestimmten Service verfügbar sind. Sie können im Ereignisverlauf bis zu fünf Ereignisse auswählen und deren Details vergleichen side-by-side.

Ereignisverlauf zeigt keine Datenereignisse. Um Datenereignisse anzuzeigen, erstellen Sie einen [Ereignisdatenspeicher](#) oder einen [Trail](#).

Nach 90 Tagen werden Ereignisse nicht mehr unter Ereignisverlauf angezeigt. Sie können Ereignisse aus dem Ereignisverlauf nicht manuell löschen.

Weitere Informationen zu den Einzelheiten der CloudTrail Protokollierung von Ereignissen für einen bestimmten Dienst finden Sie in der Dokumentation zu diesem Dienst. Weitere Informationen finden Sie unter [AWS Servicethemen für CloudTrail](#).

### Note

Für eine fortlaufende Aufzeichnung der Aktivitäten und Ereignisse der letzten 90 Tage erstellen Sie einen [Ereignisdatenspeicher](#) oder einen [Trail](#).

Zeigen Sie den Ereignisverlauf wie folgt an:

1. Melden Sie sich bei der an AWS Management Console und öffnen Sie die CloudTrail Konsole unter <https://console.aws.amazon.com/cloudtrail/>.
2. Wählen Sie im Navigationsbereich Event history (Ereignisverlauf) aus. Sie sehen eine gefilterte Liste der Ereignisse. Die neuesten Ereignisse werden zuerst angezeigt. Der Standardfilter für Ereignisse ist Read only (Schreibgeschützt), gesetzt auf false. Sie können diesen Filter deaktivieren, indem Sie das X rechts neben dem Filter auswählen.
3. Sie können Ereignisse nach einem einzelnen Attribut filtern, das Sie aus der Dropdownliste auswählen können. Um nach einem Attribut zu filtern, wählen Sie das Attribut aus der Dropdownliste aus und geben Sie den vollständigen Wert für das Attribut ein. Um beispielsweise alle Anmeldeereignisse für die Konsole anzuzeigen, wählen Sie den Filter „Ereignisname“ und geben Sie Folgendes an ConsoleLogin. Oder, um aktuelle S3-Verwaltungsereignisse anzuzeigen, wählen Sie den Filter Ereignisquelle und geben Sie Folgendes an s3.amazonaws.com.
4. Um ein bestimmtes Verwaltungsereignis anzuzeigen, wählen Sie den Namen des Ereignisses aus. Auf der Seite mit den Ereignisdetails können Sie Details zu dem Ereignis, alle Referenz-Ressourcen und den Ereignisdatensatz einsehen.
5. Um Ereignisse zu vergleichen, wählen Sie bis zu fünf Ereignisse aus, indem Sie ihre Kontrollkästchen am linken Rand der Ereignisverlaufstabelle ausfüllen. Sie können Details zu den ausgewählten Ereignissen side-by-side in der Tabelle „Eventdetails vergleichen“ einsehen.
6. Sie können den Ereignisverlauf speichern, indem Sie ihn als Datei im CSV- oder JSON-Format herunterladen. Das Herunterladen Ihres Ereignisverlaufs kann einige Minuten dauern.

## Inhalt

- [Navigieren zwischen den Seiten](#)
- [Anpassen der Anzeige](#)
- [CloudTrail Ereignisse filtern](#)
- [Details zu einem Ereignis ansehen](#)
- [Herunterladen von Ereignissen](#)
- [Anzeigen von mit AWS Config referenzierten Ressourcen](#)

## Navigieren zwischen den Seiten

Sie können zwischen den Seiten im Ereignisverlauf navigieren, indem Sie die Seite auswählen, die Sie anzeigen möchten. Sie können sich auch die nächste und vorherige Seite im Ereignisverlauf ansehen.

Wählen Sie <, um die vorherige Seite des Ereignisverlaufs aufzurufen.

Wählen Sie >, um die nächste Seite des Ereignisverlaufs aufzurufen.

## Anpassen der Anzeige

Sie können die Ansicht des Ereignisverlaufs in der CloudTrail Konsole anpassen, indem Sie aus den folgenden Einstellungen auswählen.

- Seitengröße – Wählen Sie aus, ob Sie 10, 25 oder 50 Ereignisse auf jeder Seite anzeigen möchten.
- Zeilen umbrechen – Text umbrechen, sodass Sie den gesamten Text für jedes Ereignis sehen können.
- Gestreifte Zeilen – Schattiert jede zweite Zeile in der Tabelle.
- Anzeige der Ereigniszeit – Wählen Sie aus, ob die Uhrzeit des Ereignisses in UTC oder in der lokalen Zeitzone angezeigt werden soll.
- Sichtbare Spalten auswählen – Wählen Sie die anzuzeigenden Spalten aus. Standardmäßig werden die folgenden Spalten angezeigt:
  - Ereignisname
  - Ereigniszeit
  - Benutzername
  - Ereignisquelle
  - Ressourcentyp
  - Ressourcenname

### Note

Sie können die Reihenfolge der Spalten nicht ändern und Ereignisse aus Ereignisverlauf nicht manuell löschen.

## So passen Sie die Anzeige an

1. Melden Sie sich bei der an AWS Management Console und öffnen Sie die CloudTrail Konsole unter <https://console.aws.amazon.com/cloudtrail/>.
2. Wählen Sie im Navigationsbereich Ereignisverlauf aus.
3. Wählen Sie das Zahnradsymbol aus.
4. Wählen Sie unter Seitengröße die Anzahl der Ereignisse aus, die auf einer Seite angezeigt werden sollen.
5. Wählen Sie Zeilenumbruch, um den gesamten Text für jedes Ereignis anzuzeigen.
6. Wählen Sie Gestreifte Zeilen, um jede zweite Zeile in der Tabelle zu schattieren.
7. Wählen Sie für eine Anzeige der Ereigniszeit aus, ob die Uhrzeit des Ereignisses in UTC oder in der lokalen Zeitzone angezeigt werden soll. Standardmäßig ist UTC ausgewählt.
8. Wählen Sie unter Sichtbare Spalten auswählen die Spalten, die Sie anzeigen möchten. Deaktivieren Sie die Spalten, die Sie nicht anzeigen möchten.
9. Wenn Sie mit den Änderungen fertig sind, wählen Sie Weiter aus.

## CloudTrail Ereignisse filtern

Die Standardanzeige von Ereignissen unter Ereignisverlauf verwendet einen Attributfilter, um schreibgeschützte Ereignisse aus der Liste der angezeigten Ereignisse auszuschließen. Dieser Attributfilter mit dem Namen Read only (Nur Lesen) ist auf den Wert false eingestellt. Um sowohl Lese- als auch Schreibereignisse anzuzeigen, können Sie diesen Filter entfernen. Um nur Lese-Ereignisse anzuzeigen, können Sie den Filterwert auf true ändern. Sie können Ereignisse auch nach anderen Attributen filtern. Außerdem können Sie nach Zeitbereich filtern.

### Note

Sie können nur jeweils einen Attribut-Filter und jeweils einen Zeitbereichs-Filter anwenden. Es können nicht mehrere Attributfilter angewandt werden.

## AWS Zugriffsschlüssel

Die AWS Zugriffsschlüssel-ID, die zum Signieren der Anfrage verwendet wurde. Erfolgte die Abfrage mittels temporärer Sicherheitsanmeldeinformationen, ist dies die Zugriffsschlüssel-ID der temporären Anmeldeinformationen.

## Ereignis-ID

Die CloudTrail ID des Ereignisses. Jedes Ereignis hat eine eindeutige ID.

## Ereignisname

Der Name des Ereignisses. Beispielsweise können Sie IAM-Ereignisse wie `CreatePolicy` oder Amazon-EC2-Ereignisse wie `RunInstances` filtern.

## Ereignisquelle

Der AWS Dienst, an den die Anfrage gestellt wurde, z. B. `iam.amazonaws.com` oder `s3.amazonaws.com`. Sie können eine Liste von Ereignisquellen durchblättern, nachdem Sie den Filter `Event source` ausgewählt haben.

## Nur Leseberechtigung

Der Lesetyp des Ereignisses. Ereignisse werden als Lese- oder als Schreibereignisse kategorisiert. Bei der Einstellung `false` werden Leseereignisse nicht in die Liste der angezeigten Ereignisse eingeschlossen. Dieser Attributfilter wird standardmäßig angewandt, und als Wert wird `false` eingestellt.

## Ressourcenname

Der Name oder die ID der Ressource, auf den/die das Ereignis verweist. Beispielsweise könnte der Ressourcenname `"auto-scaling-test-group"` für eine Auto Scaling Scaling-Gruppe oder `„i-12345678910"` für eine EC2-Instance lauten.

## Ressourcentyp

Der Typ der Ressource, auf den das Ereignis verweist. Beispielsweise kann einen Ressourcentyp für EC2 Instance sein oder für RDS DBInstance. Die Ressourcentypen variieren je nach Dienst. AWS

## Zeitraum

Der Zeitraum, nach dem Sie Ereignisse filtern möchten. Sie können einen Relativen Bereich oder einen Absoluten Bereich wählen. Sie können nach Ereignissen der letzten 90 Tage filtern.

## Benutzername

Die Identität, auf die das Ereignis verweist. Dies kann z. B. ein Benutzer, der Name einer Rolle oder eine Servicerolle sein.

Wurden für das gewählte Attribut oder die gewählte Zeit keine Ereignisse protokolliert, bleibt die Ergebnisliste leer. Neben dem Filter für den Zeitraum können Sie nur noch einen Attribut-Filter anwenden. Wenn Sie einen anderen Attributfilter auswählen, wird der angegebene Zeitbereich beibehalten.

In den folgenden Schritten wird beschrieben, wie Sie nach einem Attribut filtern.

So filtern Sie nach einem Attribut

1. Um die Ergebnisse nach einem Attribut zu filtern, wählen Sie ein Attribut aus der Dropdown-Liste Lookup-Attribute aus und geben oder wählen Sie dann einen Wert für das Attribut in das Textfeld aus.
2. Um einen Attributfilter zu entfernen, klicken Sie auf das X rechts vom Feld für den Attributfilter.

In den folgenden Schritten wird beschrieben, wie Sie nach einem Start- und Enddatum und nach Uhrzeit filtern.

Nach einem Start- und Enddatum und Uhrzeit filtern

1. Um den Zeitbereich für die Ereignisse, die Sie anzeigen möchten, einzugrenzen, wählen Sie einen Zeitbereich in der Zeitbereichsleiste aus. Sie können einen Relativen Bereich oder einen Absoluten Bereich wählen.

Wählen Sie Relativer Bereich, um einen vordefinierten Zeitraum oder einen benutzerdefinierten Bereich auszuwählen. Voreingestellte Werte sind 30 Minuten, 1 Stunde, 12 Stunden oder 1 Tag. Um einen benutzerdefinierten Zeitraum anzugeben, wählen Sie Benutzerdefiniert aus.

Wählen Sie Absoluter Bereich, um eine bestimmte Start- und Endzeit anzugeben. Sie können auch zwischen UTC und lokaler Zeitzone wechseln.

2. Um einen Filter für einen Zeitraum zu entfernen, wählen Sie Leeren und verwerfen in der Zeitbereichsleiste aus.

## Details zu einem Ereignis ansehen

1. Wählen Sie ein Ereignis in der Ergebnisliste, um sich die Details anzeigen zu lassen.
2. Im Ereignis referenzierte Ressourcen werden in der Tabelle Referenzierte Ressourcen auf der Ereignisdetailseite angezeigt.

3. Einige referenzierte Ressourcen besitzen Links. Klicken Sie auf den Link, um die Konsole für diese Ressource zu öffnen.
4. Scrollen Sie auf der Detailseite zu Ereignisdatensatz, um den JSON-Ereignisdatensatz anzuzeigen, der auch als Ereignis-Nutzlast bezeichnet wird.
5. Wählen Sie im Breadcrumb der Seite Ereignisverlauf aus, um die Seite mit den Ereignisdetails zu schließen und zum Ereignisverlauf zurückzukehren.

## Herunterladen von Ereignissen

Sie können einen aufgezeichneten Ereignisverlauf als Datei im CSV- oder JSON-Format herunterladen. Sie können bis zu 200.000 Ereignisse in einer einzigen Datei herunterladen. Wenn Sie das Limit von 200.000 Ereignissen erreichen, bietet die CloudTrail Konsole die Option, zusätzliche Dateien herunterzuladen. Verwenden Sie Filter und Zeitbereiche zur Reduzierung der Größe der Datei, die Sie herunterladen.

### Note

CloudTrail Ereignisverlaufsddateien sind Datendateien, die Informationen (wie Ressourcennamen) enthalten, die von einzelnen Benutzern konfiguriert werden können. Einige Daten können potenziell als Befehle in Programmen verwendet werden, um diese Daten zu lesen und zu analysieren (CSV-Injektion). Wenn CloudTrail Ereignisse beispielsweise als CSV exportiert und in ein Tabellenkalkulationsprogramm importiert werden, warnt Sie dieses Programm möglicherweise vor Sicherheitsbedenken. Sie sollten diese Inhalte deaktivieren, um Ihr System zu schützen. Deaktivieren Sie Links oder Makros in Ereignisverlaufsddateien.

1. Fügen Sie einen Filter und einen Zeitraum für Ereignisse im Ereignisverlauf hinzu, die Sie herunterladen möchten. Sie können beispielsweise den Ereignisnamen `StartInstances` und einen Zeitrahmen für die letzten drei Tage Aktivität angeben.
2. Wählen Sie `Download events` (Ereignisse herunterladen) und dann `Download CSV` (CSV herunterladen) oder `Download JSON` (JSON herunterladen) aus. Der Download beginnt sofort.

### Note

Ihr Download kann einige Zeit in Anspruch nehmen. Verwenden Sie für schnellere Ergebnisse einen detaillierteren Filter oder einen kürzeren Zeitbereich, um die



Ergebnisse einzuschränken, bevor Sie den Download-Vorgang starten. Sie können einen Download abbrechen. Wenn Sie einen Download abbrechen, befindet sich möglicherweise ein teilweiser Download, der nur einige Ereignisdaten enthält, auf Ihrem lokalen Computer. Starten Sie den Download neu, um den vollständigen Ereignisverlauf herunterzuladen.

3. Wenn der Download abgeschlossen ist, öffnen Sie die Datei, um die Ereignisse anzuzeigen, die Sie angegeben haben.
4. Um Ihren Download abbrechen, wählen Sie Abbrechen und bestätigen Sie dann, indem Sie Download abbrechen wählen. Wenn Sie einen Download neu starten müssen, warten Sie, bis der frühere Download beendet ist.

## Anzeigen von mit AWS Config referenzierten Ressourcen

AWS Config zeichnet Konfigurationsdetails, Beziehungen und Änderungen an Ihren AWS Ressourcen auf.

Wählen Sie im Bereich Ressourcen, auf die verwiesen wird, die Spalte



in der AWS Config Ressourcen-Timeline aus, um die Ressource in der AWS Config Konsole anzuzeigen.

Wenn das



Symbol grau ist, AWS Config nicht aktiviert ist oder der Ressourcentyp nicht aufgezeichnet wird. Wählen Sie das Symbol, um zur AWS Config Konsole zu wechseln und den Dienst einzuschalten oder mit der Aufzeichnung dieses Ressourcentyps zu beginnen. Weitere Informationen finden Sie im AWS Config Entwicklerhandbuch [AWS Config unter Einrichtung mithilfe der Konsole](#).

Wenn Link not available in der Spalte nicht angezeigt wird, kann die Ressource aus einem der folgenden Gründe nicht angezeigt werden:

- AWS Config unterstützt den Ressourcentyp nicht. Weitere Informationen finden Sie unter [Unterstützte Ressourcen, Konfigurationselemente und Beziehungen](#) im AWS Config - Entwicklerhandbuch.

- AWS Config vor Kurzem wurde Unterstützung für den Ressourcentyp hinzugefügt, aber er ist noch nicht über die CloudTrail Konsole verfügbar. Sie können die Ressource in der AWS Config Konsole nachschlagen, um den Zeitplan für die Ressource zu sehen.
- Die Ressource gehört einer anderen Person AWS-Konto.
- Die Ressource gehört einer anderen Person AWS-Service, z. B. einer verwalteten IAM-Richtlinie.
- Die Ressource wurde erstellt und dann sofort gelöscht.
- Die Ressource wurde kürzlich erstellt oder aktualisiert.

Informationen darüber, wie Sie Benutzern nur Leseberechtigungen zum Anzeigen von Ressourcen in der AWS Config Konsole gewähren, finden Sie unter [Erteilen Sie die Berechtigung zum Anzeigen von AWS Config Informationen auf der Konsole CloudTrail](#)

Weitere Informationen zu AWS Config finden Sie im [AWS Config Entwicklerhandbuch](#).

## Aktuelle Managementereignisse anzeigen mit dem AWS CLI

Mit dem `aws cloudtrail lookup-events` Befehl können Sie nach CloudTrail Verwaltungsereignissen der letzten 90 Tage für den aktuellen AWS-Region Zeitraum suchen. Der `aws cloudtrail lookup-events` Befehl zeigt Ereignisse AWS-Region dort an, wo sie aufgetreten sind.

Die Suche unterstützt die folgenden Attribute für Verwaltungsereignisse:

- AWS Zugriffstaste
- Ereignis-ID
- Ereignisname
- Ereignisquelle
- Nur Lesezugriff
- Ressourcenname
- Ressourcentyp
- Benutzername

Alle Attribute sind optional.

Der Befehl [lookup-events](#) umfasst die folgenden Optionen:

- `--max-items <integer>` – Die Gesamtzahl der Elemente, die in der Ausgabe des Befehls zurückgegeben werden sollen. Ist die Gesamtzahl der verfügbaren Elemente größer als der angegebene Wert, wird ein `NextToken` in der Ausgabe des Befehls bereitgestellt. Um die Seitennummerierung fortzusetzen, geben Sie den `NextToken`-Wert im `starting-Token`-Argument eines nachfolgenden Befehls an. Verwenden Sie das `NextToken`-Antwortelement nicht direkt außerhalb der AWS CLI.
- `--start-time <timestamp>` – Gibt an, dass nur Ereignisse, die zum angegebenen Zeitpunkt oder danach eintreten, zurückgegeben werden. Falls die angegebene Anfangszeit nach der angegebenen Endzeit liegt, wird ein Fehler zurückgegeben.
- `--lookup-attributes <integer>` – Enthält eine Liste von Suchattributen. Derzeit kann die Liste nur ein Element enthalten.
- `--generate-cli-skeleton <string>` – Gibt ein JSON-Skelett in der Standardausgabe aus, ohne eine API-Anfrage zu senden. Wenn kein Wert oder die Werteingabe angegeben wird, wird ein JSON-Eingabebeispiel ausgegeben, das als Argument für `--cli-input-json` verwendet werden kann. In ähnlicher Weise wird bei Angabe einer Yaml-Eingabe ein Beispiel für die Eingabe von YAML ausgegeben, das mit `--cli-input-yaml` verwendet werden kann. Wenn es mit der Wertausgabe geliefert wird, validiert es die Befehlseingaben und gibt ein Beispiel-Ausgabe-JSON für diesen Befehl zurück. Das generierte JSON-Skelett ist zwischen den Versionen von nicht stabil, AWS CLI und es gibt keine Garantien für die Abwärtskompatibilität im generierten JSON-Skelett.
- `--cli-input-json <string>` – Liest Argumente aus der angegebenen JSON-Zeichenfolge. Die JSON-Zeichenfolge folgt dem vom `--generate-cli-skeleton`-Parameter bereitgestellten Format. Wenn andere Argumente in der Befehlszeile angegeben werden, überschreiben diese Werte die von JSON bereitgestellten Werte. Es ist nicht möglich, beliebige Binärwerte mit einem von JSON bereitgestellten Wert zu übergeben, da die Zeichenfolge wörtlich genommen wird. Dies darf nicht zusammen mit dem Parameter `--cli-input-yaml` angegeben werden.

Allgemeine Informationen zur Verwendung der AWS Befehlszeilenschnittstelle finden Sie im [AWS Command Line Interface Benutzerhandbuch](#).

## Inhalt

- [Voraussetzungen](#)
- [Erhalten der Befehlszeilenhilfe](#)
- [Suchen von Ereignissen](#)
- [Angabe der Anzahl der zurückzugebenden Ereignisse](#)
- [Suchen von Ereignissen nach Zeitbereich](#)

- [Suchen von Ereignissen nach Attribut](#)
  - [Beispiele für die Attributsuche](#)
- [Angabe der nächsten Ergebnisseite](#)
- [Abrufen der JSON-Eingabe aus einer Datei](#)
- [Ausgabefelder der Suche](#)

## Voraussetzungen

- Um AWS CLI Befehle ausführen zu können, müssen Sie den installieren AWS CLI. Weitere Informationen finden Sie unter [Erste Schritte mit dem AWS CLI](#).
- Stellen Sie sicher, dass Ihre AWS CLI Version höher als 1.6.6 ist. Sie können die CLI-Version verifizieren, indem Sie `aws --version` in der Befehlszeile ausführen.
- Verwenden Sie den `aws configure` Befehl AWS-Region, um das Konto und das Standardausgabeformat für eine AWS CLI Sitzung festzulegen. Weitere Informationen finden Sie unter [Konfiguration der AWS Befehlszeilenschnittstelle](#).

### Note

Bei den CloudTrail AWS CLI Befehlen wird zwischen Groß- und Kleinschreibung unterschieden.

## Erhalten der Befehlszeilenhilfe

Wenn Sie die Befehlszeilenhilfe zu `lookup-events` anzeigen möchten, geben Sie den folgenden Befehl ein:

```
aws cloudtrail lookup-events help
```

## Suchen von Ereignissen

### Important

Die Rate der Suchanfragen ist auf zwei pro Sekunde, pro Konto und Region begrenzt. Wenn dieses Limit überschritten wird, tritt ein Drosselungsfehler auf.

Um die zehn neuesten Ereignisse anzuzeigen, geben Sie den folgenden Befehl ein:

```
aws cloudtrail lookup-events --max-items 10
```

Ein zurückgegebenes Ereignis sieht etwa wie im Folgenden dargestellt aus. Dieses fiktive Beispiel wurde zur besseren Lesbarkeit formatiert:

```
{
  "NextToken": "kb0t5LlZe+
+mErCebpy2TgaMgmDvF1kYGFcH64JSjIbZfjsuvrSqq66b5YGssKutDYIyII4lrP4IDbeQdi0bkp9YA1ju3oXd12juy3CIZ
  "Events": [
    {
      "EventId": "0ebbaee4-6e67-431d-8225-ba0d81df5972",
      "Username": "root",
      "EventTime": 1424476529.0,
      "CloudTrailEvent": "{
        \"eventVersion\": \"1.02\",
        \"userIdentity\": {
          \"type\": \"Root\",
          \"principalId\": \"111122223333\",
          \"arn\": \"arn:aws:iam::111122223333:root\",
          \"accountId\": \"111122223333\"},
        \"eventTime\": \"2015-02-20T23:55:29Z\",
        \"eventSource\": \"signin.amazonaws.com\",
        \"eventName\": \"ConsoleLogin\",
        \"awsRegion\": \"us-east-2\",
        \"sourceIPAddress\": \"203.0.113.4\",
        \"userAgent\": \"Mozilla/5.0\",
        \"requestParameters\": null,
        \"responseElements\": {\"ConsoleLogin\": \"Success\"},
        \"additionalEventData\": {
          \"MobileVersion\": \"No\",
          \"LoginTo\": \"https://console.aws.amazon.com/console/home\",
          \"MFAUsed\": \"No\"},
        \"eventID\": \"0ebbaee4-6e67-431d-8225-ba0d81df5972\",
        \"eventType\": \"AwsApiCall\",
        \"recipientAccountId\": \"111122223333\"},
      "EventName": "ConsoleLogin",
      "Resources": []
    }
  ]
}
```

Eine Erläuterung der suchbezogenen Felder in der Ausgabe finden Sie im Abschnitt [Ausgabefelder der Suche](#) später in diesem Dokument. Eine Erläuterung der Felder in dem CloudTrail Ereignis finden Sie unter [CloudTrail Inhalt aufzeichnen](#).

## Angabe der Anzahl der zurückzugebenden Ereignisse

Geben Sie den folgenden Befehl ein, um die Anzahl der zurückzugebenden Ereignisse anzugeben:

```
aws cloudtrail lookup-events --max-items <integer>
```

Mögliche Werte: 1 bis 50. Im folgenden Beispiel wird ein Ereignis zurückgegeben.

```
aws cloudtrail lookup-events --max-items 1
```

## Suchen von Ereignissen nach Zeitbereich

Für die Suche sind die Ereignisse der letzten 90 Tage verfügbar. Geben Sie den folgenden Befehl ein, um einen Zeitbereich anzugeben:

```
aws cloudtrail lookup-events --start-time <timestamp> --end-time <timestamp>
```

`--start-time <timestamp>` gibt in UTC an, dass nur Ereignisse, die zum angegebenen Zeitpunkt oder danach eintreten, zurückgegeben werden. Falls die angegebene Anfangszeit nach der angegebenen Endzeit liegt, wird ein Fehler zurückgegeben.

`--end-time <timestamp>` gibt in UTC an, dass nur Ereignisse, die zum angegebenen Zeitpunkt oder davor eintreten, zurückgegeben werden. Falls die angegebene Endzeit vor der angegebenen Anfangszeit liegt, wird ein Fehler zurückgegeben.

Standardmäßige Anfangszeit ist das früheste Datum, an dem innerhalb der letzten 90 Tage Daten verfügbar sind. Standardmäßige Endzeit ist der Zeitpunkt des Ereignisses, das zu dem der aktuellen Zeit am nächsten liegenden Zeitpunkt eingetreten ist.

Alle Zeitstempel werden in UTC angezeigt.

## Suchen von Ereignissen nach Attribut

Geben Sie zum Filtern nach einem Attribut den folgenden Befehl ein:

```
aws cloudtrail lookup-events --lookup-attributes
  AttributeKey=<attribute>,AttributeValue=<string>
```

Für jeden lookup-events-Befehl kann nur ein Paar aus Attributsschlüssel und -wert angegeben werden. Im Folgenden sehen Sie gültige Werte für AttributeKey. Bei den Wertnamen muss die Groß- und Kleinschreibung beachtet werden.

- AccessKeyId
- EventId
- EventName
- EventSource
- ReadOnly
- ResourceName
- ResourceType
- Username

Die maximale Länge für die AttributeValue beträgt 2000 Zeichen. Die folgenden Zeichen ('\_', ", ", , '\n') gelten als zwei Zeichen im Verhältnis zur Obergrenze von 2000 Zeichen.

## Beispiele für die Attributsuche

Der folgende Beispielbefehl gibt die Ereignisse zurück, in denen der Wert von AccessKeyId AKIAIOSFODNN7EXAMPLE ist.

```
aws cloudtrail lookup-events --lookup-attributes
  AttributeKey=AccessKeyId,AttributeValue=AKIAIOSFODNN7EXAMPLE
```

Der folgende Beispielbefehl gibt das Ereignis für den angegebenen Wert zurück CloudTrailEventId.

```
aws cloudtrail lookup-events --lookup-attributes
  AttributeKey=EventId,AttributeValue=b5cc8c40-12ba-4d08-a8d9-2bceb9a3e002
```

Der folgende Beispielbefehl gibt die Ereignisse zurück, in denen der Wert von EventName RunInstances ist.

```
aws cloudtrail lookup-events --lookup-attributes
  AttributeKey=EventName,AttributeValue=RunInstances
```

Der folgende Beispielbefehl gibt die Ereignisse zurück, in denen der Wert von EventSource iam.amazonaws.com ist.

```
aws cloudtrail lookup-events --lookup-attributes
  AttributeKey=EventSource,AttributeValue=iam.amazonaws.com
```

Der folgende Beispielbefehl gibt Schreibereignisse zurück. Er schließt Leseereignisse wie GetBucketLocation und DescribeStream aus.

```
aws cloudtrail lookup-events --lookup-attributes
  AttributeKey=ReadOnly,AttributeValue=false
```

Der folgende Beispielbefehl gibt die Ereignisse zurück, in denen der Wert von ResourceName CloudTrail\_CloudWatchLogs\_Role ist.

```
aws cloudtrail lookup-events --lookup-attributes
  AttributeKey=ResourceName,AttributeValue=CloudTrail_CloudWatchLogs_Role
```

Der folgende Beispielbefehl gibt die Ereignisse zurück, in denen der Wert von ResourceType AWS::S3::Bucket ist.

```
aws cloudtrail lookup-events --lookup-attributes
  AttributeKey=ResourceType,AttributeValue=AWS::S3::Bucket
```

Der folgende Beispielbefehl gibt die Ereignisse zurück, in denen der Wert von Username root ist.

```
aws cloudtrail lookup-events --lookup-attributes
  AttributeKey=Username,AttributeValue=root
```

## Angabe der nächsten Ergebnisseite

Um die nächste Ergebnisseite eines Befehls lookup-events abzurufen, geben Sie den folgenden Befehl ein:

```
aws cloudtrail lookup-events <same parameters as previous command> --next-token=<token>
```



Der Wert für `<token>` wird dabei dem ersten Feld der Ausgabe des vorherigen Befehls entnommen.

Wenn Sie `--next-token` in einem Befehl verwenden, müssen Sie dieselben Parameter wie im vorherigen Befehl verwenden. Angenommen, Sie führen den folgenden Befehl aus:

```
aws cloudtrail lookup-events --lookup-attributes
  AttributeKey=Username,AttributeValue=root
```

Um die nächste Ergebnisseite abzurufen, würde Ihr nächster Befehl wie folgt aussehen:

```
aws cloudtrail lookup-events --lookup-attributes
  AttributeKey=Username,AttributeValue=root --next-token=kb0t5L1Ze+
+mErCebpy2TgaMgmDvF1kYGFcH64JSjIbZFjsuvrSqq66b5YGssKutDYIyII4lrP4IDbeQdi0bkp9YA1ju3oXd12juy3CIZ
```

## Abrufen der JSON-Eingabe aus einer Datei

AWS CLI Für einige AWS Dienste gibt es zwei Parameter, `--generate-cli-skeleton` mit denen Sie eine JSON-Vorlage generieren können, die Sie ändern und als Eingabe für den `--cli-input-json` Parameter verwenden können. `--cli-input-json` In diesem Abschnitt wird die Verwendung dieser Parameter mit `aws cloudtrail lookup-events` beschrieben. Allgemeinere Informationen finden Sie unter [AWS CLI Skelette und Eingabedateien](#).

So suchen Sie nach CloudTrail Ereignissen, indem Sie JSON-Eingaben aus einer Datei abrufen

1. Erstellen Sie eine Eingabevorlage für die Verwendung mit `lookup-events` und leiten Sie dazu die `--generate-cli-skeleton`-Ausgabe in eine Datei um, wie im folgenden Beispiel dargestellt.


```
aws cloudtrail lookup-events --generate-cli-skeleton > LookupEvents.txt
```

Die generierte Vorlagendatei (in diesem `LookupEvents` Fall.txt) sieht wie folgt aus:

```
{
  "LookupAttributes": [
    {
      "AttributeKey": "",
      "AttributeValue": ""
    }
  ]
}
```

```
    ],  
    "StartTime": null,  
    "EndTime": null,  
    "MaxResults": 0,  
    "NextToken": ""  
  }  
}
```

2. Ändern Sie die JSON-Daten in einem Texteditor nach Bedarf. Die JSON-Eingabe darf nur angegebene Werte umfassen.

 **Important**


Die Vorlage kann erst verwendet werden, nachdem alle leeren Werte oder Nullwerte daraus entfernt wurden.

Im folgenden Beispiel sind ein Zeitraum und die maximale Anzahl der zurückzugebenden Ergebnisse angegeben.

```
{  
  "StartTime": "2023-11-01",  
  "EndTime": "2023-12-12",  
  "MaxResults": 10  
}
```

3. Verwenden Sie die Syntax `--cli-input-json file://<filename>`, wie im folgenden Beispiel dargestellt, um die bearbeitete Datei als Eingabe zu verwenden:

```
aws cloudtrail lookup-events --cli-input-json file://LookupEvents.txt
```

 **Note**

Sie können in derselben Befehlszeile wie `--cli-input-json` weitere Argumente verwenden.

## Ausgabefelder der Suche

### Ereignisse

Eine Liste der Suchereignisse basierend auf dem angegebenen Suchattribut und Zeitbereich. Die Ereignisliste ist nach Zeit sortiert, das neueste Ereignis ist zuerst aufgeführt. Jeder Eintrag enthält Informationen über die Suchanfrage und eine Zeichenfolgendarstellung des abgerufenen CloudTrail Ereignisses.

Die folgenden Einträge beschreiben die Felder in den einzelnen Suchereignissen.

### CloudTrailEvent

Eine JSON-Zeichenfolge, die eine Objektdarstellung des zurückgegebenen Ereignisses enthält. Weitere Informationen zu den einzelnen zurückgegebenen Elementen finden Sie im Abschnitt [Datensatzinhalte](#).

### EventId

Eine Zeichenfolge, die die GUID des zurückgegebenen Ereignisses enthält.

### EventName

Eine Zeichenfolge, die den Namen des zurückgegebenen Ereignisses enthält.

### EventSource

Der AWS Dienst, an den die Anfrage gestellt wurde.

### EventTime

Datum und Uhrzeit des Ereignisses im UNIX-Zeitformat.

### Ressourcen

Eine Liste der Ressourcen, auf die von dem zurückgegebenen Ereignis verwiesen wird. In jedem Ressourceneintrag ist ein Ressourcentyp und ein Ressourcenname angegeben.

### ResourceName

Eine Zeichenfolge, die den Namen der Ressource enthält, auf die von dem Ereignis verwiesen wird.

### ResourceType

Eine Zeichenfolge, die den Typ einer Ressource enthält, auf die von dem Ereignis verwiesen wird. Wenn der Ressourcentyp nicht ermittelt werden kann, wird Null zurückgegeben.

## Username

Eine Zeichenfolge, die den Benutzernamen des Kontos für das zurückgegebene Ereignis enthält.

## NextToken

Eine Zeichenfolge zum Abrufen der nächsten Ergebnisseite eines vorherigen `lookup-events-`Befehls. Um das Token verwenden zu können, müssen die Parameter mit den Parametern im ursprünglichen Befehl übereinstimmen. Wenn es in der Ausgabe keinen `NextToken`-Eintrag gibt, sind keine weiteren Ergebnisse vorhanden, die zurückgegeben werden können.

# Mit AWS CloudTrail Lake arbeiten

AWS CloudTrail Mit Lake können Sie SQL-basierte Abfragen für Ihre Ereignisse ausführen.

CloudTrail [Lake konvertiert bestehende Ereignisse im zeilenbasierten JSON-Format in das Apache ORC-Format](#). ORC ist ein spaltenförmiges Speicherformat, das für den schnellen Abruf von Daten optimiert ist. Die Ereignisse werden in Ereignisdatenspeichern zusammengefasst, bei denen es sich um unveränderliche Sammlungen von Ereignissen handelt, die auf Kriterien basieren, die Sie mit Hilfe von [erweiterten Ereignisselektoren](#) auswählen. Sie können die Ereignisdaten bis zu 3 653 Tage (etwa 10 Jahre) in einem Ereignisdatenspeicher speichern, wenn Sie sich für die Preisoption mit verlängerbarer Aufbewahrung von einem Jahr entscheiden, oder bis zu 2 557 Tage (etwa 7 Jahre), wenn Sie sich für die Preisoption mit siebenjähriger Aufbewahrung entscheiden. Die Selektoren, die Sie auf einen Ereignisdatenspeicher anwenden, steuern, welche Ereignisse bestehen bleiben und für Abfragen zur Verfügung stehen. CloudTrail Lake ist eine Auditing-Lösung, die Ihren Compliance-Stack ergänzen und Sie bei der Problembewegung nahezu in Echtzeit unterstützen kann.

## CloudTrail Datenspeicher für Ereignisse in Lake

Beim Erstellen eines Ereignisdatenspeichers wählen Sie die Kategorie der Ereignisse aus, die im Ereignisdatenspeicher aufgenommen werden sollen. Sie können einen Ereignisdatenspeicher erstellen, der [CloudTrail Ereignisse](#), [CloudTrail Insights-Ereignisse](#), [AWS Config Konfigurationselemente](#), [AWS Audit Manager Beweise](#) oder [Ereignisse von außerhalb](#) enthält AWS. Jeder Ereignisdatenspeicher kann nur eine bestimmte Ereigniskategorie (z. B. AWS Config Konfigurationselemente) enthalten, da das [Ereignisschema](#) für die Ereigniskategorie einzigartig ist. Sie können Ereignisse aus einer Organisation AWS Organizations in einem [Ereignisdatenspeicher einer Organisation speichern](#), einschließlich Ereignisse aus mehreren Regionen und Konten. Mit den unterstützten SQL-JOIN-Schlüsselwörtern können Sie auch SQL-Abfragen in mehreren Ereignisdatenspeichern ausführen. Informationen zum Ausführen von Abfragen in mehreren Ereignisdatenspeichern finden Sie unter [Erweiterte Unterstützung für Abfragen in mehreren Tabellen](#).

Sie können Trail-Ereignisse in einen neuen oder vorhandenen Ereignisdatenspeicher kopieren, um eine point-in-time Momentaufnahme der im Trail protokollierten Ereignisse zu erstellen. Weitere Informationen finden Sie unter [Kopieren von Trail-Ereignissen in einen Ereignisdatenspeicher](#).

Sie können einen Verbund zu einem Ereignisdatenspeicher einrichten, um die mit dem Ereignisdatenspeicher verbundenen Metadaten im AWS Glue [-Datenkatalog](#) zu sehen und SQL-Abfragen über die Ereignisdaten mit Amazon Athena durchzuführen. Anhand der im AWS Glue

Datenkatalog gespeicherten Tabellenmetadaten weiß die Athena-Abfrage-Engine, wie die Daten, die Sie abfragen möchten, gesucht, gelesen und verarbeitet werden. Weitere Informationen finden Sie unter [Verbund für einen Ereignisdatenspeicher erstellen](#).


Standardmäßig werden alle Ereignisse in einem Ereignisdatenspeicher von CloudTrail verschlüsselt. Wenn Sie einen Ereignisdatenspeicher konfigurieren, können Sie wählen, ob Sie Ihren eigenen AWS Key Management Service Schlüssel verwenden möchten. Die Verwendung Ihres eigenen KMS-Schlüssels verursacht AWS KMS Kosten für die Verschlüsselung und Entschlüsselung. Nachdem Sie einen KMS-Schlüssel einem Ereignisdatenspeicher zugeordnet haben, kann der KMS-Schlüssel nicht entfernt oder geändert werden.

Sie können den Zugriff auf Aktionen in Ereignisdatenspeichern mithilfe der Autorisierung auf Grundlage von Tags steuern. Weitere Informationen finden Sie auch unter [Beispiele: Verweigern des Zugriffs zum Erstellen oder Löschen von Ereignisdatenspeichern basierend auf Tags](#) in diesem Handbuch.

Sie können CloudTrail Lake-Dashboards verwenden, um die Daten in Ihren Ereignisdatenspeichern zu visualisieren. Jedes Dashboard besteht aus mehreren Widgets und jedes Widget steht für eine SQL-Abfrage. Weitere Informationen zu Lake-Dashboards finden Sie unter [CloudTrail Lake-Dashboards anzeigen](#).

CloudTrail Für Ereignisdatenspeicher in Lake fallen Gebühren an. Beim Erstellen eines Ereignisdatenspeichers wählen Sie die [Preisoption](#) aus, die für den Ereignisdatenspeicher genutzt werden soll. Die Preisoption bestimmt die Kosten für die Erfassung und Speicherung von Ereignissen sowie die standardmäßige und maximale Aufbewahrungsdauer für den Ereignisdatenspeicher. Informationen zur CloudTrail Preisgestaltung und Verwaltung der Lake-Kosten finden Sie unter [AWS CloudTrail Preise](#) und [Verwaltung der CloudTrail Seekosten](#).

CloudTrail Lake unterstützt CloudWatch Amazon-Metriken, die Informationen über aufgenommene Daten und Speicherbytes liefern. Weitere Informationen zu unterstützten CloudWatch Metriken finden Sie unter [Unterstützte CloudWatch Metriken](#).

 Note

CloudTrail übermittelt Ereignisse in der Regel innerhalb von durchschnittlich etwa 5 Minuten nach einem API-Aufruf. Diese Zeit ist nicht garantiert.

## CloudTrail Lake-Integrationen

Sie können CloudTrail Lake-Integrationen verwenden, um Benutzeraktivitätsdaten von außerhalb zu protokollieren und zu speichern AWS; aus beliebigen Quellen in Ihren Hybridumgebungen, z. B. internen oder SaaS-Anwendungen, die vor Ort oder in der Cloud gehostet werden, virtuellen Maschinen oder Containern. Nachdem Sie in CloudTrail Lake Ereignisdatenspeicher und einen Kanal zum Protokollieren von Aktivitätsereignissen erstellt haben, rufen Sie die `PutAuditEvents` API auf, in die Ihre Anwendungsaktivitäten aufgenommen werden. CloudTrail Anschließend können Sie CloudTrail Lake verwenden, um die von Ihren Anwendungen protokollierten Daten zu suchen, abzufragen und zu analysieren.

Integrationen können auch Ereignisse von über einem Dutzend CloudTrail Partnern in Ihren Ereignisdatenspeichern protokollieren. In einer Partnerintegration erstellen Sie Datenspeicher für Zielereignisse, einen Kanal und eine Ressourcenrichtlinie. Nachdem Sie die Integration erstellt haben, stellen Sie dem Partner den Kanal-ARN zur Verfügung. Es gibt zwei Arten von Integrationen: Direkt und Lösung. Bei direkten Integrationen ruft der Partner die `PutAuditEvents` API auf, um Ereignisse an den Event-Datenspeicher für Ihr AWS Konto zu übermitteln. Bei Lösungsintegrationen wird die Anwendung in Ihrem AWS Konto ausgeführt und die Anwendung ruft die `PutAuditEvents` API auf, um Ereignisse an den Ereignisdatenspeicher für Ihr AWS Konto zu übermitteln.

Weitere Informationen zu Integrationen finden Sie unter [Erstellen einer Integration mit einer Ereignisquelle außerhalb](#) von AWS

## CloudTrail Lake-Abfragen

CloudTrail Lake-Abfragen bieten eine umfassendere und besser anpassbare Ansicht von Ereignissen als einfache Schlüssel- und Werteabfragen in der Ereignishistorie oder bei laufenden `LookupEvents` Ereignissen. Eine Suche im Ereignisverlauf ist auf ein einzelnes Objekt beschränkt AWS-Konto, gibt nur Ereignisse aus einem einzigen AWS-Region Objekt zurück und kann nicht mehrere Attribute abfragen. Im Gegensatz dazu können CloudTrail Lake-Benutzer komplexe SQL-Abfragen über mehrere Ereignisfelder hinweg ausführen. CloudTrail Lake unterstützt alle gültigen `SELECT` Presto-Anweisungen und -Funktionen. Weitere Informationen zu den unterstützten SQL-Funktionen und -Operatoren finden Sie unter [Funktionen und Operatoren](#) auf der Dokumentationswebsite für Presto.

Sie können CloudTrail Lake-Abfragen für die future Verwendung speichern und die Ergebnisse von Abfragen bis zu sieben Tage lang anzeigen. Wenn Sie Abfragen ausführen, können Sie die Abfrageergebnisse in einem Amazon S3-Bucket speichern.

Die CloudTrail Konsole bietet eine Reihe von Beispielabfragen, die Ihnen den Einstieg in das Schreiben eigener Abfragen erleichtern können. Weitere Informationen finden Sie unter [Sehen Sie sich Beispielabfragen in der CloudTrail Konsole an](#).

CloudTrail Für Lake-Abfragen fallen Gebühren an. Wenn Sie Abfragen in Lake ausführen, zahlen Sie auf der Grundlage der Menge der gescannten Daten. Informationen zur CloudTrail Preisgestaltung und Verwaltung der Lake-Kosten finden Sie unter [AWS CloudTrail Preisgestaltung](#) und [Verwaltung der CloudTrail Seekosten](#).

## Weitere Ressourcen

Die folgenden Ressourcen können Ihnen helfen, besser zu verstehen, was CloudTrail Lake ist und wie Sie es nutzen können.

- [Modernisieren Sie Ihr Audit-Log-Management mit CloudTrail Lake](#) (YouTube Video)
- [Protokollieren Sie Aktivitätsereignisse aus AWS anderen Quellen in AWS CloudTrail Lake](#) (YouTube Video)
- [Analysieren Sie Aktivitätsprotokolle mit AWS CloudTrail Lake und Amazon Athena](#) (YouTube Video)
- [Verschaffen Sie sich einen Überblick über die Aktivitätsprotokolle für Ihre Belegschaft und Kundenidentitäten \(Blog\)](#)AWS
- [Verwendung von AWS CloudTrail Lake zur Identifizierung älterer TLS-Verbindungen zu AWS Service-Endpunkten \(Blog\)](#)AWS
- [Wie Arctic Wolf AWS CloudTrail Lake nutzt, um Sicherheit und Betrieb zu vereinfachen](#) (AWS Blog)
- [CloudTrail Häufig gestellte Fragen zu Lake](#)
- [AWS CloudTrail API Reference](#)
- [AWS CloudTrail Daten-API-Referenz](#)
- [AWS CloudTrail Leitfaden zum Onboarding von Partnern](#)

## CloudTrail Von Seen unterstützte Regionen

Derzeit wird CloudTrail Lake in den folgenden Bereichen unterstützt AWS-Regionen:



Name der Region	Region
USA Ost (Nord-Virginia)	us-east-1
USA Ost (Ohio)	us-east-2
USA West (Nordkalifornien)	us-west-1
USA West (Oregon)	us-west-2
Afrika (Kapstadt)	af-south-1
Asien-Pazifik (Hongkong)	ap-east-1
Asien-Pazifik (Hyderabad)	ap-south-2
Asien-Pazifik (Jakarta)	ap-southeast-3
Asien-Pazifik (Mumbai)	ap-south-1
Asien-Pazifik (Osaka)	ap-northeast-3
Asien-Pazifik (Seoul)	ap-northeast-2
Asien-Pazifik (Singapur)	ap-southeast-1
Asien-Pazifik (Sydney)	ap-southeast-2
Asien-Pazifik (Tokio)	ap-northeast-1
Kanada (Zentral)	ca-central-1
Europa (Frankfurt)	eu-central-1
Europa (Irland)	eu-west-1
Europa (London)	eu-west-2
Europa (Mailand)	eu-south-1
Europa (Paris)	eu-west-3

Name der Region	Region
Europa (Spanien)	eu-south-2
Europa (Stockholm)	eu-north-1
Europa (Zürich)	eu-central-2
Israel (Tel Aviv)	il-central-1
Naher Osten (Bahrain)	me-south-1
Naher Osten (VAE)	me-central-1
Südamerika (São Paulo)	sa-east-1
AWS GovCloud (US-Ost)	us-gov-east-1
AWS GovCloud (US-West)	us-gov-west-1

Informationen zu CloudTrail Dienstendpunkten finden Sie unter [AWS CloudTrail Endpunkte und Kontingente](#).

Weitere Informationen zur Verwendung von CloudTrail finden Sie AWS GovCloud (US) Regions unter [Service Endpoints](#) im AWS GovCloud (US) Benutzerhandbuch.

## CloudTrail Konzepte und Terminologie von Seen

In diesem Abschnitt werden die wichtigsten Konzepte und Begriffe beschrieben, die Ihnen bei der Verwendung von AWS CloudTrail Lake helfen sollen.

### Konzepte und Begriffe

- [Ereignisdatenspeicher](#)
- [Integrationen](#)
- [Abfragen](#)
- [Dashboard](#)

## Ereignisdatenspeicher

Die Ereignisse werden in Ereignisdatenspeichern zusammengefasst, bei denen es sich um unveränderliche Sammlungen von Ereignissen handelt, die auf Kriterien basieren, die Sie mit Hilfe von erweiterten Ereignisselektoren auswählen.

Sie können einen Ereignisdatenspeicher erstellen, um [CloudTrail Verwaltungsereignisse und Datenereignisse](#), [CloudTrail Insights-Ereignisse](#), [AWS Audit Manager Beweise](#), [AWS Config Konfigurationselemente](#) oder [Ereignisse außerhalb von](#) zu protokollieren AWS.

### Erweiterte Ereignisauswahlen

Erweiterte Ereignisselektoren bestimmen, welche Ereignisse in einen Ereignisdatenspeicher aufgenommen werden sollen. Erweiterte Ereignisselektoren helfen Ihnen, die Kosten zu kontrollieren, indem sie nur die Ereignisse protokollieren, die für Sie wichtig sind.

Für Verwaltungsereignisse und Datenereignisse können Sie erweiterte Ereignisselektoren verwenden, um Ereignisse zu filtern. Wenn Sie beispielsweise einen Ereignisdatenspeicher zur Erfassung von Verwaltungsereignissen erstellen, können Sie Daten-API-Ereignisse AWS Key Management Service (AWS KMS) oder Amazon Relational Database Service (Amazon RDS) herausfiltern. In der Regel GenerateDataKey generieren AWS KMS Aktionen wie EncryptDecrypt, und mehr als 99 Prozent der Ereignisse.

Für AWS Config Konfigurationselemente, Audit Manager Manager-Beweise oder Ereignisse außerhalb von AWS erweiterten Ereignisselektoren werden nur verwendet, um Ereignisse dieses Typs in den Ereignisdatenspeicher aufzunehmen.

### Verbund

Mit Verbund können Sie die mit einem Ereignisdatenspeicher verbundenen Metadaten im AWS Glue -[Datenkatalog](#) einsehen und mit Amazon Athena SQL-Abfragen zu den Ereignisdaten durchführen. Anhand der im AWS Glue Datenkatalog gespeicherten Tabellenmetadaten weiß die Athena-Abfrage-Engine, wie die Daten, die Sie abfragen möchten, gesucht, gelesen und verarbeitet werden.

Wenn Sie den Lake-Abfrageverbund aktivieren, werden die Verbundressourcen in Ihrem Namen CloudTrail erstellt und diese Ressourcen bei registriert. [AWS Lake Formation](#) Nachdem Lake-Verbund aktiviert wurde, können Sie Ihre Ereignisdaten direkt in Athena abfragen, ohne zusätzliche Schritte ausführen zu müssen. Weitere Informationen finden Sie unter [Verbund für einen Ereignisdatenspeicher erstellen](#).

## Gebühreoption

Beim Erstellen eines Ereignisdatenspeichers wählen Sie die Preisoption aus, die für den Ereignisdatenspeicher genutzt werden soll. Der Preisoption bestimmt die Kosten für die Erfassung und Speicherung von Ereignissen sowie die standardmäßige und maximale Aufbewahrungsdauern für den Ereignisdatenspeicher. Informationen zu Preisen erhalten Sie unter [AWS CloudTrail -Preise](#) und [Verwaltung der CloudTrail Seekosten](#).

## Aufbewahrungszeitraum

Die Aufbewahrungsdauer eines Ereignisdatenspeichers bestimmt, wie lange Ereignisdaten im Ereignisdatenspeicher aufbewahrt werden. CloudTrail Lake bestimmt, ob ein Ereignis aufbewahrt werden soll, indem es prüft, ob das Ereignis innerhalb der angegebenen Aufbewahrungsfrist liegt. `eventTime` Wenn Sie beispielsweise einen Aufbewahrungszeitraum von 90 Tagen angeben, CloudTrail werden Ereignisse entfernt, wenn sie `eventTime` älter als 90 Tage sind.

## Standardaufbewahrungsdauer

Die Standardaufbewahrungsdauer eines Ereignisdatenspeichers ist die Standardanzahl von Tagen, an denen Ereignisdaten im Ereignisdatenspeicher aufbewahrt werden. Während der standardmäßigen Aufbewahrungsdauer eines Ereignisdatenspeichers ist der Speicherplatz ohne zusätzliche Kosten im Erfassungspreis enthalten. Nach Ablauf der standardmäßigen Aufbewahrungsfrist beträgt der Speicherpreis `pay-as-you-go`.

## Maximale Aufbewahrungsdauer

Die maximale Aufbewahrungsdauer eines Ereignisdatenspeichers entspricht der maximalen Anzahl von Tagen, an denen Sie Daten in einem Ereignisdatenspeicher aufbewahren können.

## Termination protection

Standardmäßig aktivieren Ereignisdatenspeicher den Beendigungsschutz, der verhindert, dass ein Ereignisdatenspeicher versehentlich gelöscht wird. Um einen Ereignisdatenspeicher mit aktiviertem Beendigungsschutz zu löschen, wählen Sie auf der Detailseite des Ereignisdatenspeichers im Menü Aktionen die Option Beendigungsschutz ändern aus. Anschließend können Sie mit dem Löschen des Ereignisdatenspeichers fortfahren. Weitere Informationen finden Sie unter [Ändern Sie den Kündigungsschutz mit der Konsole](#).

## Integrationen

Sie können CloudTrail Lake-Integrationen verwenden, um Benutzeraktivitätsdaten aus den folgenden Quellen zu protokollieren und zu speichern:

- Außerhalb von AWS
- Jede Quelle in Ihren hybriden Umgebungen, z. B. interne oder Software-as-a-Service (SaaS)-Anwendungen, die On-Premises oder in der Cloud gehostet werden, virtuelle Maschinen oder Container

Eine Integration erfordert einen Kanal für die Übertragung der Ereignisse und einen Ereignisdatenspeicher für den Empfang der Ereignisse. Nachdem Sie Ihre Integration eingerichtet haben, rufen Sie den [PutAuditEvents](#) API-Vorgang auf, in den Ihre Anwendungsaktivitäten aufgenommen werden CloudTrail sollen. Anschließend können Sie CloudTrail Lake verwenden, um die von Ihren Anwendungen protokollierten Daten zu suchen, abzufragen und zu analysieren. Weitere Informationen finden Sie unter [Erstellen Sie eine Integration mit einer Ereignisquelle außerhalb von AWS](#).

## Integrationstyp

Es gibt zwei Arten von Integrationen: direkt und Lösung. Bei direkten Integrationen ruft der Partner den PutAuditEvents-API-Vorgang auf, um Ereignisse an den Ereignisdatenspeicher für Ihr AWS-Konto zu übertragen. Bei Lösungsintegrationen läuft die Anwendung in Ihrer AWS-Konto und die Anwendung ruft den PutAuditEvents API-Vorgang auf, um Ereignisse für Sie AWS-Konto in den Ereignisdatenspeicher zu übertragen.

## Kanäle

Organisieren Sie Ereignisse aus Quellen außerhalb der AWS Arbeit, indem Sie Kanäle verwenden, um Ereignisse von externen Partnern, die mit Ihnen zusammenarbeiten CloudTrail, oder aus Ihren eigenen Quellen nach CloudTrail Lake zu bringen. Wenn Sie einen Kanal erstellen, wählen Sie einen oder mehrere Ereignisdatenspeicher aus, um Ereignisse zu speichern, die von der Kanalquelle stammen. Sie können die Zielereignisdatenspeicher für einen Kanal nach Bedarf ändern, sofern die Zielereignisdatenspeicher so eingestellt sind, dass sie `eventCategory="ActivityAuditLog"`-Ereignisse protokollieren. Wenn Sie einen Kanal für Ereignisse eines externen Partners erstellen, stellen Sie dem Partner oder der Quellanwendung einen Kanal-Amazon-Ressourcennamen (ARN) zur Verfügung.

## Ressourcenbasierte Richtlinien

Ressourcenbasierte Richtlinien sind JSON-Richtliniendokumente, die Sie an eine Ressource anfügen. Die dem Kanal beigefügte ressourcenbasierte Richtlinie ermöglicht es der Quelle, Ereignisse über den Kanal zu übertragen. Wenn der Kanal keine Ressourcenrichtlinie hat, kann

nur der Kanalbesitzer den PutAuditEvents-API-Vorgang auf dem Kanal aufrufen. Weitere Informationen finden Sie unter [AWS CloudTrail Beispiele für ressourcenbasierte Richtlinien](#).

## Abfragen

Abfragen in CloudTrail Lake werden in SQL verfasst. Sie können eine Abfrage auf der Registerkarte CloudTrail Lake Editor erstellen, indem Sie die Abfrage von Grund auf in SQL schreiben oder indem Sie eine gespeicherte Abfrage oder eine Beispielabfrage öffnen und bearbeiten. Sie können eine enthaltene Beispielabfrage nicht mit Ihren Änderungen überschreiben, aber Sie können sie als neue Abfrage speichern. Weitere Informationen finden Sie unter [Abfrage erstellen oder bearbeiten](#).

CloudTrail Lake unterstützt alle gültigen Presto SELECT Anweisungen und Funktionen. Weitere Informationen zu den unterstützten SQL-Funktionen und -Operatoren finden Sie unter [Funktionen und Operatoren](#) auf der Dokumentationswebsite für Presto.

## Dashboard

Mithilfe des CloudTrail Lake-Dashboards können Sie die Ereignisse in einem Ereignisdatenspeicher visualisieren und Trends wie die häufigsten Ereignisse AWS-Services, Benutzer und Fehler anzeigen. Weitere Informationen finden Sie unter [CloudTrail Lake-Dashboards anzeigen](#).

### Dashboard-Typ

Die verfügbaren Dashboard-Typen für einen Ereignisdatenspeicher hängen von der Konfiguration der erweiterten Ereignisselektoren des Ereignisdatenspeichers ab. Wenn ein Dashboard-Typ beispielsweise Informationen über CloudTrail Verwaltungsereignisse anzeigt, können Sie das Dashboard nur auswählen, wenn der aktuell ausgewählte Ereignisdatenspeicher CloudTrail Verwaltungsereignisse sammelt.

Die folgenden Dashboard-Typen sind verfügbar:

- **Übersichts-Dashboard** — Zeigt die aktivsten Benutzer AWS-Services nach Anzahl der Ereignisse an. AWS-Regionen Sie können auch Informationen über die Aktivität von `read`- und `write`-Verwaltungsereignissen, die am stärksten beeinträchtigten Ereignisse und die häufigsten Fehler anzeigen. Dieses Dashboard ist für Ereignisdatenspeicher verfügbar, die Verwaltungsereignisse erfassen.
- **Dashboard für Verwaltungsereignisse** – Zeigt Anmeldeereignisse auf der Konsole, Ereignisse mit Zugriffsverweigerung, destruktive Aktionen und die häufigsten Fehler pro Benutzer an. Sie

können auch Informationen zu TLS-Versionen und veralteten TLS-Aufrufen nach Benutzern anzeigen. Dieses Dashboard ist für Ereignisdatenspeicher verfügbar, die Verwaltungsereignisse erfassen.

- Dashboard für S3-Datenereignisse – Zeigt die Amazon-S3-Kontoaktivitäten, die am häufigsten aufgerufenen S3-Objekte, die wichtigsten S3-Benutzer und die wichtigsten S3-Aktionen an. Dieses Dashboard ist für Ereignisdatenspeicher verfügbar, die Amazon-S3-Datenaktionen erfassen.
- Dashboard für Insights-Ereignisse – Zeigt den Gesamtanteil der Insights-Ereignisse nach Insights-Typ, den Anteil der Insights-Ereignisse nach Insights-Typ für die wichtigsten Benutzer und Services sowie die Anzahl der Insights-Ereignisse pro Tag. Das Dashboard enthält auch ein Widget, das Insights-Ereignisse für bis zu 30 Tage auflistet. Dieses Dashboard ist nur für Ereignisdatenspeicher verfügbar, die Insights-Ereignisse erfassen.

#### Note

- Nachdem Sie CloudTrail Insights zum ersten Mal im Quell-Ereignisdatenspeicher aktiviert haben, kann es bis zu 7 Tage dauern, CloudTrail bis das erste Insights-Ereignis übermittelt wird, wenn ungewöhnliche Aktivitäten festgestellt werden. Weitere Informationen finden Sie unter [Grundlegendes zur Insights-Ereignisbereitstellung](#).
- Das Dashboard für Insights-Ereignisse zeigt nur Informationen zu den Insights-Ereignissen an, die vom ausgewählten Ereignisdatenspeicher erfasst wurden. Dies hängt von der Konfiguration des ursprünglichen Ereignisdatenspeicher ab. Wenn Sie beispielsweise den ursprünglichen Ereignisdatenspeicher so konfigurieren, dass Insights-Ereignisse für `ApiCallRateInsight`, aber nicht für `ApiErrorRateInsight` aktiviert werden, werden Ihnen keine Informationen über Insights-Ereignisse für `ApiErrorRateInsight` angezeigt.

## Widgets

Widgets sind die Komponenten, aus denen ein Dashboard besteht und die eine Visualisierung ermöglichen, z. B. ein Linien- oder Balkendiagramm. Jedes Widget steht für eine zugrunde liegende Abfrage. Wenn Sie Abfragen ausführen wählen, CloudTrail wird eine vom System generierte Abfrage ausgeführt, um die Daten für jedes Widget aufzufüllen.

## CloudTrail Datenspeicher für Ereignisse in Lake

Die Ereignisse werden in Ereignisdatenspeichern zusammengefasst, bei denen es sich um unveränderliche Sammlungen von Ereignissen handelt, die auf Kriterien basieren, die Sie mit Hilfe von erweiterten Ereignisselektoren auswählen.

Wenn Sie in CloudTrail Lake einen Ereignisdatenspeicher erstellen, wählen Sie den Typ der Ereignisse aus, die in Ihren Ereignisdatenspeicher aufgenommen werden sollen. Sie können einen Ereignisdatenspeicher erstellen, der CloudTrail Daten oder Verwaltungsereignisse, CloudTrail Insights-Ereignisse, AWS Config Konfigurationselemente oder Ereignisse außerhalb von enthält AWS. Jeder Ereignisdatenspeichertyp kann nur bestimmte Ereigniskategorien (z. B. AWS Config Konfigurationselemente) enthalten, da das Ereignisschema für die Ereigniskategorie einzigartig ist. Mit den unterstützten SQL-JOIN-Schlüsselwörtern können Sie SQL-Abfragen in mehreren Ereignisdatenspeichern ausführen. Informationen zum Ausführen von Abfragen in mehreren Ereignisdatenspeichern finden Sie unter [Erweiterte Unterstützung für Abfragen in mehreren Tabellen](#).

Die folgende Tabelle zeigt die unterstützten Ereigniskategorien für jeden Ereignisdatenspeicher-Typ. In der Spalte eventCategory wird der Wert angezeigt, den Sie in den erweiterten Ereignisauswahlen angeben würden, um Ereignisse dieses Typs zu erfassen.

Ereignistyp (Konsole)	eventCategory (API)	Beschreibung
CloudTrail Ereignisse	Management Data	Dieser Speichertyp für Ereignisdaten kann CloudTrail Verwaltungs- und Datenereignisse sammeln. Weitere Informationen finden Sie unter <a href="#">Erstellen eines Ereignisdatenspeichers für CloudTrail Ereignisse</a> .
CloudTrail Insights-Ereignisse	Insight	Dieser Ereignisdatenspeichertyp kann CloudTrail Insights-Ereignisse sammeln. Um Insights-Ereignisse zu empfangen, benötigen Sie einen <a href="#">Quelldatenspeicher</a> für Ereignisse, der CloudTrail Verwaltungsereignisse protokolliert und Insights aktiviert. Informationen zum Erstellen der Quell- und Zielergebnisdatenspeicher finden Sie unter <a href="#">Erstellen</a>



Ereignistyp (Konsole)	eventCategory (API)	Beschreibung
		<a href="#">eines Ereignisdatenspeichers für CloudTrail Insights-Ereignisse.</a>
Konfigurationselemente	ConfigurationItem	Dieser Ereignisdatenspeichertyp kann AWS Config Konfigurationselemente sammeln. Weitere Informationen finden Sie unter <a href="#">Erstellen eines Ereignisdatenspeichers für AWS Config Konfigurationselemente.</a>
Ereignisse aus der Integration	ActivityAuditLog	Dieser Speichertyp für Ereignisdaten kann Ereignisse erfassen, die keine AWS Ereignisse aus Integrationen sind. Weitere Informationen finden Sie unter <a href="#">Erstellen eines Ereignisdatenspeichers für Ereignisse außerhalb von AWS.</a>

Sie können mit der Audit Manager Manager-Konsole auch einen Ereignisdatenspeicher für AWS Audit Manager Beweise erstellen. Weitere Informationen zum Aggregieren von Nachweisen in CloudTrail Lake mithilfe von Audit Manager finden Sie im AWS Audit Manager Benutzerhandbuch unter [Grundlegendes zur Funktionsweise von Evidence Finder mit CloudTrail Lake.](#)

CloudTrail Für die Speicherung von Ereignisdaten in Lake fallen Gebühren an. Beim Erstellen eines Ereignisdatenspeichers wählen Sie die [Preisoption](#) aus, die für den Ereignisdatenspeicher genutzt werden soll. Die Preisoption bestimmt die Kosten für die Erfassung und Speicherung von Ereignissen sowie die standardmäßige und maximale Aufbewahrungsdauer für den Ereignisdatenspeicher. Informationen zur CloudTrail Preisgestaltung und Verwaltung der Lake-Kosten finden Sie unter [AWS CloudTrail Preise](#) und [Verwaltung der CloudTrail Seekosten.](#)

In den folgenden Abschnitten wird beschrieben, wie Sie Ereignisdatenspeicher erstellen, aktualisieren und verwalten.

## Themen

- [Ereignisdatenspeicher mit der Konsole erstellen, aktualisieren und verwalten](#)
- [Erstellen, aktualisieren und verwalten Sie Ereignisdatenspeicher mit dem AWS CLI](#)
- [Verwalten der Lebenszyklen von Ereignisdatenspeichern](#)

- [Kopieren von Trail-Ereignissen in einen Ereignisdatenspeicher](#)
- [Verbund für einen Ereignisdatenspeicher erstellen](#)
- [Ereignisdatenspeicher einer Organisation](#)

## Ereignisdatenspeicher mit der Konsole erstellen, aktualisieren und verwalten

Sie können die CloudTrail Konsole verwenden, um Ihre Ereignisdatenspeicher zu erstellen, zu aktualisieren und zu verwalten. Sie können auch die [Ereignisaufnahme in einem Ereignisdatenspeicher starten und beenden](#) und den [Lake-Abfrageverbund mithilfe der Konsole aktivieren](#).

Die Verwendung der CloudTrail Konsole zum Erstellen oder Aktualisieren von Ereignisdatenspeichern bietet die folgenden Vorteile:

- Wenn Sie zum ersten Mal einen Ereignisdatenspeicher erstellen, können Sie mithilfe der CloudTrail Konsole die verfügbaren Funktionen und Optionen anzeigen.
- Wenn Sie einen Ereignisdatenspeicher für die Protokollierung von Datenereignissen konfigurieren, können Sie mithilfe der CloudTrail Konsole die verfügbaren Datentypen anzeigen. Weitere Informationen finden Sie unter [Erstellen Sie mit der Konsole einen Ereignisdatenspeicher für CloudTrail Ereignisse](#) und [Protokollieren von Datenereignissen](#).
- Wenn Sie einen Ereignisdatenspeicher für die Protokollierung von Ereignissen außerhalb von konfigurieren AWS, können Sie mithilfe der CloudTrail Konsole Informationen zu verfügbaren Partnern anzeigen. Weitere Informationen finden Sie unter [Erstellen Sie einen Ereignisdatenspeicher für Ereignisse außerhalb der AWS Konsole](#).

### Themen

- [Erstellen Sie mit der Konsole einen Ereignisdatenspeicher für CloudTrail Ereignisse](#)
- [Erstellen Sie mit der Konsole einen Ereignisdatenspeicher für CloudTrail Insights-Ereignisse](#)
- [Erstellen Sie mit der Konsole einen Ereignisdatenspeicher für AWS Config Konfigurationselemente](#)
- [Erstellen Sie einen Ereignisdatenspeicher für Ereignisse außerhalb der AWS Konsole](#)
- [Aktualisieren Sie einen Ereignisdatenspeicher mit der Konsole](#)
- [Stoppen und starten Sie die Ereigniserfassung über die Konsole](#)
- [Ändern Sie den Kündigungsschutz mit der Konsole](#)

- [Löschen Sie einen Ereignisdatenspeicher mit der Konsole](#)
- [Stellen Sie einen Ereignisdatenspeicher mit der Konsole wieder her](#)

## Erstellen Sie mit der Konsole einen Ereignisdatenspeicher für CloudTrail Ereignisse

In Ereignisdatenspeichern für CloudTrail Ereignisse können CloudTrail Verwaltungs- und Datenereignisse protokolliert werden. Sie können die Ereignisdaten bis zu 3 653 Tage (etwa 10 Jahre) in einem Ereignisdatenspeicher aufbewahren, wenn Sie die Preisoption mit verlängerbarer Aufbewahrung für ein Jahr wählen, oder bis zu 2 557 Tage (ca. 7 Jahre), wenn Sie die Preisoption für die Aufbewahrung von sieben Jahren wählen.

CloudTrail Für Datenspeicher von Lake Event fallen Gebühren an. Beim Erstellen eines Ereignisdatenspeichers wählen Sie die [Preisoption](#) aus, die für den Ereignisdatenspeicher genutzt werden soll. Die Preisoption bestimmt die Kosten für die Erfassung und Speicherung von Ereignissen sowie die standardmäßige und maximale Aufbewahrungsdauer für den Ereignisdatenspeicher. Informationen zur CloudTrail Preisgestaltung und Verwaltung der Lake-Kosten finden Sie unter [AWS CloudTrail Preise](#) und [Verwaltung der CloudTrail Seekosten](#).

Um einen Ereignisdatenspeicher für CloudTrail Verwaltungs- oder Datenereignisse zu erstellen

Gehen Sie wie folgt vor, um einen Ereignisdatenspeicher zu erstellen, der CloudTrail Verwaltungsereignisse, Datenereignisse oder sowohl Verwaltungs- als auch Datenereignisse protokolliert.

1. Melden Sie sich bei der an AWS Management Console und öffnen Sie die CloudTrail Konsole unter <https://console.aws.amazon.com/cloudtrail/>.
2. Wählen Sie im Navigationsbereich unter Lake die Option Ereignisdatenspeicher aus.
3. Wählen Sie Ereignisdatenspeicher erstellen aus.
4. Geben Sie auf der Seite Konfigurieren eines Ereignisdatenspeichers in Allgemeine Angaben einen Namen für den Ereignisdatenspeicher ein. Ein Name ist erforderlich.
5. Wählen Sie die Preisoption aus, die Sie für den Ereignisdatenspeicher verwenden möchten. Der Preisoption bestimmt die Kosten für die Erfassung und Speicherung von Ereignissen sowie die standardmäßige und maximale Aufbewahrungsdauern für Ihren Ereignisdatenspeicher. Weitere Informationen finden Sie unter [AWS CloudTrail -Preise](#) und [Verwaltung der CloudTrail Seekosten](#).

Die folgenden Optionen sind verfügbar:

- Preisoption mit verlängerbarer Aufbewahrung für ein Jahr – Empfohlen, wenn Sie damit rechnen, weniger als 25 TB an Ereignisdaten pro Monat zu erfassen und eine flexible Aufbewahrungsdauer von bis zu 10 Jahren wünschen. In den ersten 366 Tagen (Standardaufbewahrungszeitraum) ist Speicherplatz ohne zusätzliche Kosten im Preis für die Datenaufnahme enthalten. Nach 366 Tagen ist eine erweiterte Aufbewahrung gegen Aufpreis pay-as-you-go verfügbar. Dies ist die Standardoption.
    - Standardaufbewahrungsdauer: 366 Tage.
    - Maximale Aufbewahrungsdauer: beträgt 3 653 Tage.
  - Preisoption für die Aufbewahrung über sieben Jahre – Empfohlen, wenn Sie damit rechnen, mehr als 25 TB an Ereignisdaten pro Monat zu erfassen und eine flexible Aufbewahrungsdauer von bis zu 7 Jahren wünschen. Die Aufbewahrung ist im Preis für die Erfassung ohne Zusatzkosten enthalten.
    - Standardaufbewahrungsdauer: 2 557 Tage.
    - Maximale Aufbewahrungsdauer: beträgt 2 557 Tage.
6. Geben Sie einen Aufbewahrungszeitraum für den Ereignisdatenspeicher an. Die Aufbewahrungsdauern können zwischen 7 Tagen und 3 653 Tagen (etwa 10 Jahre) für die Preisoption mit verlängerbarer Aufbewahrungsdauer für ein Jahr oder zwischen 7 Tagen und 2 557 Tagen (etwa sieben Jahre) für die Preisoption mit siebenjähriger Aufbewahrungsdauer liegen.

CloudTrail Lake entscheidet, ob ein Ereignis aufbewahrt werden soll, indem es prüft, ob das Ereignis innerhalb `eventTime` des angegebenen Aufbewahrungszeitraums liegt. Wenn Sie beispielsweise einen Aufbewahrungszeitraum von 90 Tagen angeben, CloudTrail werden Ereignisse entfernt, wenn sie `eventTime` älter als 90 Tage sind.


#### Note

Wenn Sie Trail-Ereignisse in diesen Ereignisdatenspeicher kopieren, CloudTrail wird ein Ereignis nicht kopiert, wenn `eventTime` es älter als der angegebene Aufbewahrungszeitraum ist. Um den geeigneten Aufbewahrungszeitraum zu ermitteln, nehmen Sie die Summe aus dem ältesten Ereignis, das Sie kopieren möchten, in Tagen und der Anzahl der Tage, an denen Sie die Ereignisse im Ereignisdatenspeicher behalten möchten (Aufbewahrungszeitraum = *oldest-event-in-days* + *number-days-to-retain*). Wenn das älteste Ereignis, das Sie kopieren, beispielsweise

45 Tage alt ist und Sie die Ereignisse weitere 45 Tage im Ereignisdatenspeicher aufbewahren möchten, würden Sie die Aufbewahrungsdauer auf 90 Tage festlegen.

7. (Optional) Um die Verschlüsselung mit zu aktivieren AWS Key Management Service, wählen Sie Eigene verwenden aus AWS KMS key. Wählen Sie Neu, um einen für Sie AWS KMS key erstellen zu lassen, oder wählen Sie Bestehend, um einen vorhandenen KMS-Schlüssel zu verwenden. Geben Sie unter KMS-Alias eingeben einen Alias im folgenden Format an `alias/MyAliasName`. Wenn Sie Ihren eigenen KMS-Schlüssel verwenden, müssen Sie Ihre KMS-Schlüsselrichtlinie bearbeiten, um das Verschlüsseln und Entschlüsseln von CloudTrail Protokollen zuzulassen. Weitere Informationen finden Sie unter [Konfigurieren Sie AWS KMS wichtige Richtlinien für CloudTrail](#). CloudTrail unterstützt auch Schlüssel AWS KMS für mehrere Regionen. Weitere Informationen finden Sie über Multi-Regions-Schlüssel finden Sie unter [Verwenden von Schlüsseln für mehrere Regionen](#) im AWS Key Management Service - Entwicklerhandbuch.

Die Verwendung Ihres eigenen KMS-Schlüssels verursacht AWS KMS Kosten für die Verschlüsselung und Entschlüsselung. Nachdem Sie einen KMS-Schlüssel einem Ereignisdatenspeicher zugeordnet haben, kann der KMS-Schlüssel nicht entfernt oder geändert werden.

 Note


Um die AWS Key Management Service Verschlüsselung für den Ereignisdatenspeicher einer Organisation zu aktivieren, müssen Sie einen vorhandenen KMS-Schlüssel für das Verwaltungskonto verwenden.

8. (Optional) Wenn Sie Ihre Ereignisdaten mit Amazon Athena abfragen möchten, wählen Sie Aktivieren in Lake-Abfrageverbund. Mit Verbund können Sie die mit einem Ereignisdatenspeicher verbundenen Metadaten im AWS Glue [Datenkatalog](#) einsehen und mit Amazon Athena SQL-Abfragen zu den Ereignisdaten durchführen. Anhand der im AWS Glue Datenkatalog gespeicherten Tabellenmetadaten weiß die Athena-Abfrage-Engine, wie die Daten, die Sie abfragen möchten, gesucht, gelesen und verarbeitet werden. Weitere Informationen finden Sie unter [Verbund für einen Ereignisdatenspeicher erstellen](#).

Wählen Sie Aktivieren und gehen Sie wie folgt vor, um Lake-Abfrageverbund zu aktivieren:

- a. Wählen Sie aus, ob Sie eine neue Rolle erstellen oder eine vorhandene IAM-Rolle verwenden möchten. [AWS Lake Formation](#) verwendet diese Rolle, um die Berechtigungen

- für den Verbundereignisdatenspeicher zu verwalten. Wenn Sie mit der CloudTrail Konsole eine neue Rolle erstellen, CloudTrail wird automatisch eine Rolle mit den erforderlichen Berechtigungen erstellt. Wenn Sie eine bestehende Rolle auswählen, stellen Sie sicher, dass die Richtlinie für die Rolle die [erforderlichen Mindestberechtigungen](#) vorsieht.
- b. Wenn Sie eine neue Rolle erstellen, geben Sie einen Namen zur Identifizierung der Rolle ein.
  - c. Wenn Sie eine bestehende Rolle verwenden, wählen Sie die Rolle aus, die Sie verwenden möchten. Die Rolle muss in Ihrem Konto vorhanden sein.
9. (Optional) Im Bereich Tags können Sie bis zu 50 Tag-Schlüssel-Paare hinzufügen, um den Zugriff auf den Ereignisdatenspeicher festzulegen, zu sortieren und zu steuern. Weitere Informationen darüber, wie Sie IAM-Richtlinien verwenden, um den Zugriff auf einen Ereignisdatenspeicher basierend auf Tags zu autorisieren, finden Sie unter [Beispiele: Verweigern des Zugriffs zum Erstellen oder Löschen von Ereignisdatenspeichern basierend auf Tags](#). Weitere Informationen zur Verwendung von Tags finden Sie unter [Tagging AWS Resources im Tagging AWS Resources User Guide](#). AWS
  10. Wählen Sie Next (Weiter) aus, um den Ereignisdatenspeicher zu konfigurieren.
  11. Wählen Sie auf der Seite Ereignisse auswählen die Option AWS Ereignisse und dann Ereignisse ausCloudTrail.
  12. Wählen Sie für CloudTrail Ereignisse mindestens einen Ereignistyp aus. Verwaltungsereignisse ist standardmäßig ausgewählt. Sie können Ihrem Ereignisdatenspeicher sowohl Verwaltungs- als auch Datenereignisse hinzufügen. Weitere Informationen zur Verwaltungsereignissen finden Sie unter [Protokollieren von Verwaltungsereignissen](#). Weitere Informationen zu Datenereignissen finden Sie unter [Protokollieren von Datenereignissen](#).
  13. (Optional) Wählen Sie Trail-Ereignisse kopieren, wenn Sie Ereignisse aus einem vorhandenen Trail kopieren möchten, um Abfragen für vergangene Ereignisse auszuführen. Um Trail-Ereignisse in den Ereignisdatenspeicher einer Organisation zu kopieren, müssen Sie das Verwaltungskonto der Organisation verwenden. Über das Konto eines delegierten Administrators können Trail-Ereignisse nicht in den Ereignisdatenspeicher einer Organisation kopiert werden. Weitere Informationen zu Überlegungen zum Kopieren von Trail-Ereignissen finden Sie unter [Überlegungen zum Kopieren von Trail-Ereignissen](#).
  14. Damit Ihr Ereignisdatenspeicher Ereignisse von allen Konten in einer AWS Organizations -Organisation erfasst, wählen Sie Für alle Konten in meiner Organisation aktivieren aus. Sie müssen beim Verwaltungskonto oder beim Konto eines delegierten Administrators der Organisation angemeldet sein, um einen Ereignisdatenspeicher zu erstellen, der Ereignisse für eine Organisation erfasst.

 Note

Um Trail-Ereignisse zu kopieren oder Insights-Ereignisse zu aktivieren, müssen Sie beim Verwaltungskonto für Ihre Organisation angemeldet sein.

15. Erweitern Sie **Zusätzliche Einstellungen**, um auszuwählen, ob Ihr Ereignisdatenspeicher Ereignisse für alle AWS-Regionen oder nur für die aktuellen Ereignisse erfassen soll AWS-Region, und wählen Sie aus, ob der Ereignisdatenspeicher Ereignisse aufnimmt. Standardmäßig erfasst der Ereignisdatenspeicher Ereignisse aus allen Regionen in Ihrem Konto und beginnt ab der Erstellung damit, Ereignisse aufzunehmen.
  - a. Wählen Sie **Nur die aktuelle Region in meinen Ereignisdatenspeicher einbeziehen** aus, um nur Ereignisse einzubeziehen, die in der aktuellen Region protokolliert werden. Wenn Sie diese Option nicht auswählen, enthält der Ereignisdatenspeicher Ereignisse aus allen Regionen.
  - b. Deaktivieren Sie die Option **Ereignisse aufnehmen**, wenn Sie nicht möchten, dass der Ereignisdatenspeicher mit der Aufnahme von Ereignissen beginnt. Es könnte zum Beispiel sinnvoll sein, die Option **Ereignisse aufnehmen** zu deaktivieren, wenn Sie Trail-Ereignisse kopieren und nicht möchten, dass der Ereignisdatenspeicher zukünftige Ereignisse enthält. Standardmäßig beginnt der Ereignisdatenspeicher mit der Aufnahme von Ereignissen, wenn er erstellt wird.
16. Wenn Ihr Ereignisdatenspeicher **Verwaltungsereignisse** enthält, haben Sie folgende Optionen zur Wahl. Weitere Informationen zur Verwaltungsereignissen finden Sie unter [Protokollieren von Verwaltungsereignissen](#).
  - a. Wählen Sie aus, ob Sie **Leseereignisse**, **Schreibereignisse** oder beides einbeziehen möchten. Mindestens eine Option muss ausgewählt werden.
  - b. Wählen Sie aus, ob Sie **Amazon RDS Data API-Ereignisse** aus Ihrem Ereignisdatenspeicher ausschließen **AWS Key Management Service** oder aus diesem ausschließen möchten.
  - c. Wählen Sie aus, ob **Insights** aktiviert werden sollen. Um Insights zu aktivieren, müssen Sie einen [Zielereignisdatenspeicher](#) einrichten, der Insights-Ereignisse auf der Grundlage der Verwaltungsereignisaktivität in diesem Ereignisdatenspeicher erfasst.

Wenn Sie Insights aktivieren möchten, gehen Sie wie folgt vor.

- i. Wählen Sie unter Insights aktivieren den Zielereignisspeicher aus, in dem Insights-Ereignisse protokolliert werden sollen. Der Zielereignisdatenspeicher erfasst Insights-Ereignisse auf der Grundlage der Verwaltungsereignisaktivität in diesem Ereignisdatenspeicher. Weitere Informationen zum Erstellen des Zielereignisdatenspeichers finden Sie unter [Erstellen eines Zielereignisdatenspeichers, der Insights-Ereignisse protokolliert](#).
  - ii. Wählen Sie die Insights-Typen aus. Sie können die API-Aufruftrate, die API-Fehlerrate oder beides auswählen. Sie müssen Schreib-Verwaltungsereignisse protokollieren, um Insights-Ereignisse für die API-Aufruftrate zu protokollieren. Sie müssen Lese- und Schreib-Verwaltungsereignisse protokollieren, um Insights-Ereignisse für die API-Fehlerrate zu protokollieren.
17. Gehen Sie wie folgt vor, um Datenereignisse in Ihren Ereignisdatenspeicher aufzunehmen.
- a. Wählen Sie einen Datenereignistyp aus. Dies ist die AWS-Service Ressource, auf der Datenereignisse protokolliert werden. Um Datenereignisse für von Lake Formation erstellte AWS Glue Tabellen zu protokollieren, wählen Sie Lake Formation als Datentyp aus.
  - b. Wählen Sie unter Protokollselektorstemplate eine Vorlage aus. Sie können alle Datenereignisse, `readOnly`-Ereignisse, `writeOnly`-Ereignisse oder Benutzerdefiniert protokollieren, um einen benutzerdefinierten Protokollselektor zu erstellen.
  - c. (Optional) Geben Sie unter Selektornamenamen einen Namen ein, um Ihre Auswahl zu identifizieren. Der Selektornamenamen ist ein optionaler, beschreibender Name für eine erweiterte Ereignisauswahl, z. B. „Datenereignisse nur für zwei S3-Buckets protokollieren“. Der Name des Selektors wird als Name in der erweiterten Ereignisauswahl aufgeführt und ist sichtbar, wenn Sie die JSON-Ansicht erweitern.
  - d. Erstellen Sie in Advanced event selectors (Erweiterte Ereignisselektoren) Ausdrücke, indem Sie Werte für Field (Feld), Operator und Value (Wert) auswählen. Erweiterte Ereignisselektoren für einen Ereignisdatenspeicher funktionieren genauso wie erweiterte Ereignisselektoren, die Sie auf einen Trail anwenden. Weitere Informationen zum Erstellen erweiterter Ereignisselektoren finden Sie unter [Filtern von Datenereignissen mithilfe erweiterter Ereignisselektoren](#).

Im folgenden Beispiel wird die Protokollselektorstemplate Benutzerdefiniert verwendet, um nur Ereignisnamen aus S3-Objekten auszuwählen, die mit Put beginnen, z. B. PutObject. Da die erweiterte Ereignisauswahl keine anderen Ereignistypen oder Ressourcen-ARNs



einschließt oder ausschließt, werden alle S3-Datenereignisse, Lese- und Schreibereignisse, deren Ereignisnamen mit Put beginnen, im Ereignisdatenspeicher gespeichert.

▼ Data event: S3
Remove

**Data event type**  
Choose the source of data events to log.

S3
▼

**Log selector template**

Custom
▼

**Selector name - optional**

my-custom-selector
▼

1,000 character limit

**Collect events**  
Log all events, or choose a template to log specific, filtered events to your trail. You can edit templates later.

**Advanced event selectors**  
Log or exclude events from specific resources.

Field	Operator	Value	
<span>eventName</span> <span>▼</span>	<span>starts with</span> <span>▼</span>	<span>Put</span> <span>▼</span>	✕
+ Field	+ Condition		


### ⚠ Important

Um Datenereignisse mit erweiterten Ereignisselektoren unter Verwendung eines S3-Bucket-ARN auszuschließen oder einzubeziehen, verwenden Sie immer den Operator **Beginnt mit**.

- e. Erweitern Sie optional die JSON-Ansicht, um Ihre erweiterten Ereignisselektoren als JSON-Block anzuzeigen.
  - f. Um einen weiteren Datentyp hinzuzufügen, für den Datenereignisse protokolliert werden sollen, wählen Sie Datenereignistyp hinzufügen. Wiederholen Sie die Schritte a bis zu diesem Schritt, um erweiterte Ereignisselektoren für den Datenereignistyp zu konfigurieren.
18. Gehen Sie wie folgt vor, um vorhandene Trail-Ereignisse in Ihren Ereignisdatenspeicher zu kopieren.
- a. Wählen Sie den Trail aus, die Sie kopieren möchten. Standardmäßig werden CloudTrail nur CloudTrail Ereignisse kopiert, die im `CloudTrail` Präfix des S3-Buckets und die Präfixe

innerhalb des CloudTrail Präfixes enthalten sind, und überprüft keine Präfixe für andere Dienste. AWS Wenn Sie CloudTrail Ereignisse kopieren möchten, die in einem anderen Präfix enthalten sind, wählen Sie S3-URI eingeben und dann S3 durchsuchen, um zum Präfix zu navigieren. Wenn der S3-Quell-Bucket für den Trail einen KMS-Schlüssel für die Datenverschlüsselung verwendet, stellen Sie sicher, dass die KMS-Schlüsselrichtlinie das Entschlüsseln der Daten zulässt CloudTrail . Wenn Ihr S3-Quell-Bucket mehrere KMS-Schlüssel verwendet, müssen Sie die Richtlinien für jeden Schlüssel aktualisieren, damit CloudTrail die Daten im Bucket entschlüsselt werden können. Weitere Informationen zum Aktualisieren der KMS-Schlüssel-Richtlinie finden Sie unter [KMS-Schlüsselrichtlinie zum Entschlüsseln von Daten im S3-Quell-Bucket](#).

- b. Wählen Sie den Zeitraum für das Kopieren der Ereignisse aus. CloudTrail überprüft das Präfix und den Namen der Protokolldatei, um sicherzustellen, dass der Name ein Datum zwischen dem ausgewählten Start- und Enddatum enthält, bevor versucht wird, Trail-Ereignisse zu kopieren. Sie können einen Relative range (Relativen Bereich) oder einen Absolute range (Absoluten Bereich) wählen. Um zu vermeiden, dass Ereignisse zwischen dem Quell-Trail und dem Zielereignisdatspeicher dupliziert werden, wählen Sie einen Zeitraum aus, der vor der Erstellung des Ereignisdatspeichers liegt.

 Note

CloudTrail kopiert nur Trail-Ereignisse, deren Aufbewahrungsfrist `eventTime` innerhalb des Ereignisdatspeichers liegt. Wenn die Aufbewahrungsfrist eines Event-Datspeichers beispielsweise 90 Tage beträgt, CloudTrail werden keine Trail-Ereignisse kopiert, die `eventTime` älter als 90 Tage sind.

- Wenn Sie Relativer Bereich wählen, können Sie wählen, ob Ereignisse kopiert werden sollen, die in den letzten 6 Monaten, 1 Jahr, 2 Jahren, 7 Jahren oder in einem benutzerdefinierten Bereich protokolliert wurden. CloudTrail kopiert die Ereignisse, die innerhalb des ausgewählten Zeitraums protokolliert wurden.
  - Wenn Sie „Absoluter Bereich“ wählen, können Sie ein bestimmtes Start- und Enddatum wählen. CloudTrail kopiert die Ereignisse, die zwischen dem ausgewählten Start- und Enddatum aufgetreten sind.
- c. Wählen Sie für Permissions (Berechtigungen) unter den folgenden IAM-Rollenoptionen aus. Wenn Sie eine vorhandene IAM-Rolle auswählen, stellen Sie sicher, dass die IAM-Rollenrichtlinie die erforderlichen Berechtigungen bereitstellt. Weitere Informationen zum

Aktualisieren der IAM-Rollenberechtigungen finden Sie unter [IAM-Berechtigungen zum Kopieren von Trail-Ereignissen](#).

- Wählen Sie **Create a new role (recommended)** (Erstellen Sie eine neue Rolle (empfohlen)), um eine neue IAM-Rolle zu erstellen. Geben Sie unter IAM-Rollennamen eingeben einen Namen für die Rolle ein. CloudTrail erstellt automatisch die erforderlichen Berechtigungen für diese neue Rolle.
- Wählen Sie **Eine benutzerdefinierte IAM-Rolle verwenden** **ARN aus**, um eine benutzerdefinierte IAM-Rolle zu verwenden, die nicht aufgeführt ist. Geben Sie für **Enter IAM role ARN (IAM-Rollen-ARN eingeben)** den IAM-ARN ein.
- Wählen Sie eine vorhandene IAM-Rolle aus der Drop-down-Liste aus.

19. Wählen Sie **Next (Weiter)** aus, um Ihre Auswahl zu überprüfen.

20. Überprüfen Sie auf der Seite **Prüfen und erstellen** Ihre Auswahl. Wählen Sie **Bearbeiten** aus, um Änderungen am Schema vorzunehmen. Wenn Sie bereit sind, den Ereignisdatenspeicher zu erstellen, wählen Sie **Ereignisdatenspeicher erstellen** aus.

21. Der neue Ereignisdatenspeicher ist in der Tabelle **Ereignisdatenspeicher** auf der Seite **Ereignisdatenspeicher** sichtbar.

Ab diesem Zeitpunkt erfasst der Ereignisdatenspeicher Ereignisse, die mit den erweiterten Ereignisauswahlen übereinstimmen (wenn die Option **Ereignisse aufnehmen** ausgewählt ist). Ereignisse, die aufgetreten sind, bevor Sie den Ereignisdatenspeicher erstellt haben, befinden sich nicht im Ereignisdatenspeicher, es sei denn Sie haben sich für das Kopieren der bestehenden Trail-Ereignissen entschieden.

Nun können Sie Abfragen in Ihrem neuen Ereignisdatenspeicher ausführen. Die Registerkarte **Sample queries** (Beispiel für Abfragen) enthält Beispielabfragen, die Ihnen den Einstieg erleichtern. Weitere Informationen zum Erstellen und Bearbeiten von Abfragen finden Sie unter [Abfrage erstellen oder bearbeiten](#).

Sie können sich auch das **CloudTrail Lake-Dashboard** ansehen, um die Ereignisse in Ihrem Event-Datenspeicher zu visualisieren. Weitere Informationen zu Lake-Dashboards finden Sie unter [CloudTrail Lake-Dashboards anzeigen](#).

**Beispiel:** Erstellen Sie einen Ereignisdatenspeicher für Verwaltungsereignisse

In dieser exemplarischen Vorgehensweise wird gezeigt, wie Sie einen Ereignisdatenspeicher erstellen, der alle [Verwaltungsereignisse](#) in allen AWS Regionen protokolliert und keine

[Datenergebnisse](#) protokolliert. Beispiele für Verwaltungsereignisse sind etwa Sicherheitsereignisse wie IAM CreateUser und AttachRolePolicy-Ereignisse, Ressourcenereignisse wie RunInstances und CreateBucket und viele mehr.

Erstellen Sie einen Ereignisdatenspeicher für Verwaltungsereignisse wie folgt:

1. Melden Sie sich bei der an AWS Management Console und öffnen Sie die CloudTrail Konsole unter <https://console.aws.amazon.com/cloudtrail/>.
2. Wählen Sie im Navigationsbereich unter Lake die Option Ereignisdatenspeicher aus.
3. Wählen Sie Ereignisdatenspeicher erstellen aus.
4. Geben Sie auf der Seite „Event-Datenspeicher konfigurieren“ unter Allgemeine Details Ihrem Event-Datenspeicher einen Namen, z. *my-management-events-eds*. Verwenden Sie dazu am besten einen Namen, der den Zweck des Ereignisdatenspeichers schnell identifiziert. Informationen zu den CloudTrail Benennungsanforderungen finden Sie unter [Benennungsanforderungen](#).
5. Wählen Sie die Preisoption aus, die Sie für den Ereignisdatenspeicher verwenden möchten. Der Preisoption bestimmt die Kosten für die Erfassung und Speicherung von Ereignissen sowie die standardmäßige und maximale Aufbewahrungsdauern für Ihren Ereignisdatenspeicher. Weitere Informationen finden Sie unter [AWS CloudTrail -Preise](#) und [Verwaltung der CloudTrail Seekosten](#).

Die folgenden Optionen sind verfügbar:

- Preisoption mit verlängerbarer Aufbewahrung für ein Jahr – Empfohlen, wenn Sie damit rechnen, weniger als 25 TB an Ereignisdaten pro Monat zu erfassen und eine flexible Aufbewahrungsdauer von bis zu 10 Jahren wünschen. In den ersten 366 Tagen (Standardaufbewahrungszeitraum) ist Speicherplatz ohne zusätzliche Kosten im Preis für die Datenaufnahme enthalten. Nach 366 Tagen ist eine verlängerte Aufbewahrung gegen Aufpreis pay-as-you-go verfügbar. Dies ist die Standardoption.
  - Standardaufbewahrungsdauer: 366 Tage.
  - Maximale Aufbewahrungsdauer: beträgt 3 653 Tage.
- Preisoption für die Aufbewahrung über sieben Jahre – Empfohlen, wenn Sie damit rechnen, mehr als 25 TB an Ereignisdaten pro Monat zu erfassen und eine flexible Aufbewahrungsdauer von bis zu 7 Jahren wünschen. Die Aufbewahrung ist im Preis für die Erfassung ohne Zusatzkosten enthalten.
  - Standardaufbewahrungsdauer: 2 557 Tage.


- Maximale Aufbewahrungsdauer: beträgt 2 557 Tage.
6. Geben Sie einen Aufbewahrungszeitraum für den Ereignisdatenspeicher an. Die Aufbewahrungsdauern können zwischen 7 Tagen und 3 653 Tagen (etwa 10 Jahre) für die Preisoption mit verlängerbarer Aufbewahrungsdauer für ein Jahr oder zwischen 7 Tagen und 2 557 Tagen (etwa sieben Jahre) für die Preisoption mit siebenjähriger Aufbewahrungsdauer liegen.

CloudTrail Lake entscheidet, ob ein Ereignis aufbewahrt werden soll, indem es prüft, ob das Ereignis innerhalb `eventTime` des angegebenen Aufbewahrungszeitraums liegt. Wenn Sie beispielsweise einen Aufbewahrungszeitraum von 90 Tagen angeben, CloudTrail werden Ereignisse entfernt, wenn sie `eventTime` älter als 90 Tage sind.

7. (Optional) Wählen Sie unter Verschlüsselung aus, ob Sie den Ereignisdatenspeicher mit Ihrem eigenen KMS-Schlüssel verschlüsseln möchten. Standardmäßig werden alle Ereignisse in einem Ereignisdatenspeicher CloudTrail mithilfe eines KMS-Schlüssels verschlüsselt, der für Sie verantwortlich AWS ist und für Sie verwaltet wird.

Um die Verschlüsselung mit Ihrem eigenen KMS-Schlüssel zu aktivieren, wählen Sie *Meinen eigenen AWS KMS key verwenden*. Wählen Sie *Neu*, um einen für Sie AWS KMS key erstellen zu lassen, oder wählen Sie *Bestehend*, um einen vorhandenen KMS-Schlüssel zu verwenden. Geben Sie unter *KMS-Alias* eingeben einen Alias im folgenden Format an `alias/MyAliasName`. Wenn Sie Ihren eigenen KMS-Schlüssel verwenden, müssen Sie Ihre KMS-Schlüsselrichtlinie bearbeiten, um das Verschlüsseln und Entschlüsseln von CloudTrail Protokollen zuzulassen. Weitere Informationen finden Sie unter [Konfigurieren Sie AWS KMS wichtige Richtlinien für CloudTrail](#). CloudTrail unterstützt auch Schlüssel AWS KMS für mehrere Regionen. Weitere Informationen finden Sie über Multi-Regions-Schlüssel finden Sie unter [Verwenden von Schlüsseln für mehrere Regionen](#) im AWS Key Management Service - Entwicklerhandbuch.

Die Verwendung Ihres eigenen KMS-Schlüssels verursacht AWS KMS Kosten für die Verschlüsselung und Entschlüsselung. Nachdem Sie einen KMS-Schlüssel einem Ereignisdatenspeicher zugeordnet haben, kann der KMS-Schlüssel nicht entfernt oder geändert werden.

 Note

Um die AWS Key Management Service Verschlüsselung für den Ereignisdatenspeicher einer Organisation zu aktivieren, müssen Sie einen vorhandenen KMS-Schlüssel für das Verwaltungskonto verwenden.

8. (Optional) Wenn Sie Ihre Ereignisdaten mit Amazon Athena abfragen möchten, wählen Sie Aktivieren in Lake-Abfrageverbund. Mit Verbund können Sie die mit einem Ereignisdatenspeicher verbundenen Metadaten im AWS Glue [Datenkatalog](#) einsehen und mit Amazon Athena SQL-Abfragen zu den Ereignisdaten durchführen. Anhand der im AWS Glue Datenkatalog gespeicherten Tabellenmetadaten weiß die Athena-Abfrage-Engine, wie die Daten, die Sie abfragen möchten, gesucht, gelesen und verarbeitet werden. Weitere Informationen finden Sie unter [Verbund für einen Ereignisdatenspeicher erstellen](#).

Wählen Sie Aktivieren und gehen Sie wie folgt vor, um Lake-Abfrageverbund zu aktivieren:

- a. Wählen Sie aus, ob Sie eine neue Rolle erstellen oder eine vorhandene IAM-Rolle verwenden möchten. [AWS Lake Formation](#) verwendet diese Rolle, um die Berechtigungen für den Verbundereignisdatenspeicher zu verwalten. Wenn Sie mit der CloudTrail Konsole eine neue Rolle erstellen, CloudTrail wird automatisch eine Rolle mit den erforderlichen Berechtigungen erstellt. Wenn Sie eine bestehende Rolle auswählen, stellen Sie sicher, dass die Richtlinie für die Rolle die [erforderlichen Mindestberechtigungen](#) vorsieht.
  - b. Wenn Sie eine neue Rolle erstellen, geben Sie einen Namen zur Identifizierung der Rolle ein.
  - c. Wenn Sie eine bestehende Rolle verwenden, wählen Sie die Rolle aus, die Sie verwenden möchten. Die Rolle muss in Ihrem Konto vorhanden sein.
9. (Optional) Fügen Sie unter Tags ein oder mehrere benutzerdefinierte Tags (Schlüssel-Wert-Paare) zu Ihrem Ereignisdatenspeicher hinzu. Mithilfe von Tags können Sie Ihre CloudTrail Ereignisdatenspeicher identifizieren. Sie könnten beispielsweise ein Tag mit dem Namen **stage** und dem Wert **prod** anfügen. Sie können Tags verwenden, um den Zugriff auf Ihren Ereignisdatenspeicher einzuschränken. Sie können Tags auch verwenden, um die Abfrage- und Aufnahmekosten für Ihren Ereignisdatenspeicher zu verfolgen.

Informationen dazu, wie Sie mithilfe von Tags Kosten nachverfolgen, finden Sie unter [Erstellen von benutzerdefinierten Kostenzuweisungs-Tags für CloudTrail Lake-Event-Datenspeicher](#). Informationen darüber, wie Sie IAM-Richtlinien verwenden, um den Zugriff auf

einen Ereignisdatenspeicher basierend auf Tags zu autorisieren, finden Sie unter [Beispiele: Verweigern des Zugriffs zum Erstellen oder Löschen von Ereignisdatenspeichern basierend auf Tags](#). Informationen darüber, wie Sie Tags verwenden können AWS, finden Sie unter [Tagging Your AWS Resources User Guide](#) im Tagging AWS Resources User Guide.

10. Wählen Sie Next (Weiter) aus, um den Ereignisdatenspeicher zu konfigurieren.
11. Behalten Sie auf der Seite Ereignisse auswählen die Standardauswahl für den Ereignistyp bei.

**Event type** [Info](#)

Choose the type of events you want to add to your event data store. [Additional charges apply](#)

### Choose event types

**AWS events**  
Capture operations performed on or within your AWS resources.

**Events from integrations**  
Create an integration to get events that are logged by applications outside of your AWS resources.

### Specify the type of AWS events


**CloudTrail events**  
CloudTrail events provide a record of activity in an AWS account.

**CloudTrail Insights events**  
Insights events help identify unusual activity, errors, or user behavior in your account.

**Configuration items**  
Configuration items show changes made to the configuration of a resource, and show the resource's compliance status.

12. Behalten Sie für CloudTrail Ereignisse die Standardauswahl bei. Standardmäßig erfassen CloudTrail Ereignisdatenspeicher Verwaltungsereignisse und keine Datenereignisse. Weitere Informationen zur Verwaltungsereignissen finden Sie unter [Protokollieren von Verwaltungsereignissen](#). Weitere Informationen zu Datenereignissen finden Sie unter [Protokollieren von Datenereignissen](#).

## CloudTrail events [Info](#)

- Management events**  
Capture management operations performed on your AWS resources.
- Data events**  
Log the resource operations performed on or within a resource.
- Copy trail events**  
Copy CloudTrail events logged in your trails or from S3 buckets.
- Enable for all accounts in my organization**  
To review accounts in your organization, open [AWS Organizations](#). [See all accounts](#) 

---

▼ **Additional settings**

- Include only the current region (us-east-1) in my event data store**
- Ingest events | [Info](#)**  
Your event data store starts ingesting events when created.

- Behalten Sie die Standardeinstellung für Trail-Ereignisse kopieren bei. Sie würden diese Option verwenden, um vorhandene Trail-Ereignisse in Ihren Ereignisdatenspeicher zu kopieren. Weitere Informationen finden Sie unter [Kopieren von Trail-Ereignissen in einen Ereignisdatenspeicher](#).
- Wählen Sie Für alle Konten in meiner Organisation aktivieren aus, wenn es sich um einen Ereignisdatenspeicher für eine Organisation handelt. Diese Option kann nur geändert werden, wenn Sie Konten in AWS Organizations konfiguriert haben.
- Behalten Sie für Zusätzliche Einstellungen die Standardauswahl bei. Standardmäßig sammelt ein Ereignisdatenspeicher Ereignisse für alle AWS-Regionen und beginnt, Ereignisse zu erfassen, sobald er erstellt wird.
- Wählen Sie für Verwaltungsereignisse sowohl Lese- als auch Schreib-ereignisse aus. Lassen Sie die Kontrollkästchen für AWS KMS Ereignisse ausschließen und Amazon RDS Data API-Ereignisse ausschließen leer, um alle Verwaltungsereignisse zu sammeln. Lassen Sie das Kontrollkästchen für Insights-Ereignisse aktivieren leer.



## Management events [Info](#)

Management events show information about management operations performed on resources in your AWS account.

### API activity

Choose the activities you want to log.

- Read  Write
- Exclude AWS KMS events
- Exclude Amazon RDS Data API events
- Enable Insights  
Identify unusual activity, errors, or user behavior in your account.

17. Wählen Sie Next (Weiter) aus, um Ihre Auswahl zu überprüfen.
18. Überprüfen Sie auf der Seite Prüfen und erstellen Ihre Auswahl. Wählen Sie Bearbeiten aus, um Änderungen am Schema vorzunehmen. Wenn Sie bereit sind, den Ereignisdatenspeicher zu erstellen, wählen Sie Ereignisdatenspeicher erstellen aus.
19. Der neue Ereignisdatenspeicher ist in der Tabelle Ereignisdatenspeicher auf der Seite Ereignisdatenspeicher sichtbar.

Ab diesem Zeitpunkt erfasst der Ereignisdatenspeicher Ereignisse, die mit seinen erweiterten Ereignisselectoren übereinstimmen. Ereignisse, die aufgetreten sind, bevor Sie den Ereignisdatenspeicher erstellt haben, befinden sich nicht im Ereignisdatenspeicher, es sei denn Sie haben sich für das Kopieren der bestehenden Trail-Ereignissen entschieden.

Beispiel: Erstellen Sie einen Ereignisdatenspeicher für S3-Datenereignisse

Diese exemplarische Vorgehensweise zeigt Ihnen, wie Sie einen Ereignisdatenspeicher für Amazon S3 S3-Datenereignisse erstellen. In diesem Szenario wählen wir, anstatt alle Amazon S3 S3-Datenereignisse zu protokollieren, eine benutzerdefinierte Protokollauswahlvorlage, um Ereignisse nur zu protokollieren, wenn ein Objekt aus einem bestimmten S3-Bucket gelöscht wird.

Erstellen Sie einen Ereignisdatenspeicher für S3-Datenereignisse wie folgt:

1. Melden Sie sich bei der an AWS Management Console und öffnen Sie die CloudTrail Konsole unter <https://console.aws.amazon.com/cloudtrail/>.
2. Wählen Sie im Navigationsbereich unter Lake die Option Ereignisdatenspeicher aus.

3. Wählen Sie Ereignisdatenspeicher erstellen aus.
4. Geben Sie auf der Seite „Ereignisdatenspeicher konfigurieren“ unter Allgemeine Informationen Ihrem Ereignisdatenspeicher einen Namen, z. B. *s3- data-events-eds*. Verwenden Sie dazu am besten einen Namen, der den Zweck des Ereignisdatenspeichers schnell identifiziert. Informationen zu den CloudTrail Benennungsanforderungen finden Sie unter [Benennungsanforderungen](#).
5. Wählen Sie die Preisoption aus, die Sie für den Ereignisdatenspeicher verwenden möchten. Der Preisoption bestimmt die Kosten für die Erfassung und Speicherung von Ereignissen sowie die standardmäßige und maximale Aufbewahrungsdauern für Ihren Ereignisdatenspeicher. Weitere Informationen finden Sie unter [AWS CloudTrail -Preise](#) und [Verwaltung der CloudTrail Seekosten](#).

Die folgenden Optionen sind verfügbar:

- Preisoption mit verlängerbarer Aufbewahrung für ein Jahr – Empfohlen, wenn Sie damit rechnen, weniger als 25 TB an Ereignisdaten pro Monat zu erfassen und eine flexible Aufbewahrungsdauer von bis zu 10 Jahren wünschen. In den ersten 366 Tagen (Standardaufbewahrungszeitraum) ist Speicherplatz ohne zusätzliche Kosten im Preis für die Datenaufnahme enthalten. Nach 366 Tagen ist eine verlängerte Aufbewahrung gegen Aufpreis pay-as-you-go verfügbar. Dies ist die Standardoption.
    - Standardaufbewahrungsdauer: 366 Tage.
    - Maximale Aufbewahrungsdauer: beträgt 3 653 Tage.
  - Preisoption für die Aufbewahrung über sieben Jahre – Empfohlen, wenn Sie damit rechnen, mehr als 25 TB an Ereignisdaten pro Monat zu erfassen und eine flexible Aufbewahrungsdauer von bis zu 7 Jahren wünschen. Die Aufbewahrung ist im Preis für die Erfassung ohne Zusatzkosten enthalten.
    - Standardaufbewahrungsdauer: 2 557 Tage.
    - Maximale Aufbewahrungsdauer: beträgt 2 557 Tage.
6. Geben Sie einen Aufbewahrungszeitraum für den Ereignisdatenspeicher an. Die Aufbewahrungsdauern können zwischen 7 Tagen und 3 653 Tagen (etwa 10 Jahre) für die Preisoption mit verlängerbarer Aufbewahrungsdauer für ein Jahr oder zwischen 7 Tagen und 2 557 Tagen (etwa sieben Jahre) für die Preisoption mit siebenjähriger Aufbewahrungsdauer liegen.


CloudTrail Lake entscheidet, ob ein Ereignis aufbewahrt werden soll, indem es prüft, ob das Ereignis innerhalb `eventTime` des angegebenen Aufbewahrungszeitraums liegt. Wenn Sie

beispielsweise einen Aufbewahrungszeitraum von 90 Tagen angeben, CloudTrail werden Ereignisse entfernt, wenn sie `eventTime` älter als 90 Tage sind.

7. (Optional) Wählen Sie unter Verschlüsselung aus, ob Sie den Ereignisdatenspeicher mit Ihrem eigenen KMS-Schlüssel verschlüsseln möchten. Standardmäßig werden alle Ereignisse in einem Ereignisdatenspeicher CloudTrail mithilfe eines KMS-Schlüssels verschlüsselt, der für Sie verantwortlich AWS ist und für Sie verwaltet wird.

Um die Verschlüsselung mit Ihrem eigenen KMS-Schlüssel zu aktivieren, wählen Sie **Meinen eigenen AWS KMS key verwenden**. Wählen Sie **Neu**, um einen für Sie AWS KMS key erstellen zu lassen, oder wählen Sie **Bestehend**, um einen vorhandenen KMS-Schlüssel zu verwenden. Geben Sie unter KMS-Alias eingeben einen Alias im folgenden Format an `alias/MyAliasName`. Wenn Sie Ihren eigenen KMS-Schlüssel verwenden, müssen Sie Ihre KMS-Schlüsselrichtlinie bearbeiten, um das Verschlüsseln und Entschlüsseln von CloudTrail Protokollen zuzulassen. Weitere Informationen finden Sie unter [Konfigurieren Sie AWS KMS wichtige Richtlinien für CloudTrail](#). CloudTrail unterstützt auch Schlüssel AWS KMS für mehrere Regionen. Weitere Informationen finden Sie über Multi-Regions-Schlüssel finden Sie unter [Verwenden von Schlüsseln für mehrere Regionen](#) im AWS Key Management Service - Entwicklerhandbuch.

Die Verwendung Ihres eigenen KMS-Schlüssels verursacht AWS KMS Kosten für die Verschlüsselung und Entschlüsselung. Nachdem Sie einen KMS-Schlüssel einem Ereignisdatenspeicher zugeordnet haben, kann der KMS-Schlüssel nicht entfernt oder geändert werden.

 Note

Um die AWS Key Management Service Verschlüsselung für den Ereignisdatenspeicher einer Organisation zu aktivieren, müssen Sie einen vorhandenen KMS-Schlüssel für das Verwaltungskonto verwenden.

8. (Optional) Wenn Sie Ihre Ereignisdaten mit Amazon Athena abfragen möchten, wählen Sie **Aktivieren in Lake-Abfrageverbund**. Mit Verbund können Sie die mit einem Ereignisdatenspeicher verbundenen Metadaten im AWS Glue [Datenkatalog](#) einsehen und mit Amazon Athena SQL-Abfragen zu den Ereignisdaten durchführen. Anhand der im AWS Glue Datenkatalog gespeicherten Tabellenmetadaten weiß die Athena-Abfrage-Engine, wie die Daten, die Sie abfragen möchten, gesucht, gelesen und verarbeitet werden. Weitere Informationen finden Sie unter [Verbund für einen Ereignisdatenspeicher erstellen](#).

Wählen Sie Aktivieren und gehen Sie wie folgt vor, um Lake-Abfrageverbund zu aktivieren:

- a. Wählen Sie aus, ob Sie eine neue Rolle erstellen oder eine vorhandene IAM-Rolle verwenden möchten. [AWS Lake Formation](#) verwendet diese Rolle, um die Berechtigungen für den Verbundereignisdatenspeicher zu verwalten. Wenn Sie mit der CloudTrail Konsole eine neue Rolle erstellen, CloudTrail wird automatisch eine Rolle mit den erforderlichen Berechtigungen erstellt. Wenn Sie eine bestehende Rolle auswählen, stellen Sie sicher, dass die Richtlinie für die Rolle die [erforderlichen Mindestberechtigungen](#) vorsieht.
  - b. Wenn Sie eine neue Rolle erstellen, geben Sie einen Namen zur Identifizierung der Rolle ein.
  - c. Wenn Sie eine bestehende Rolle verwenden, wählen Sie die Rolle aus, die Sie verwenden möchten. Die Rolle muss in Ihrem Konto vorhanden sein.
9. (Optional) Fügen Sie unter Tags ein oder mehrere benutzerdefinierte Tags (Schlüssel-Wert-Paare) zu Ihrem Ereignisdatenspeicher hinzu. Mithilfe von Tags können Sie Ihre CloudTrail Ereignisdatenspeicher identifizieren. Sie könnten beispielsweise ein Tag mit dem Namen **stage** und dem Wert **prod** anfügen. Sie können Tags verwenden, um den Zugriff auf Ihren Ereignisdatenspeicher einzuschränken. Sie können Tags auch verwenden, um die Abfrage- und Aufnahmekosten für Ihren Ereignisdatenspeicher zu verfolgen.

Informationen dazu, wie Sie mithilfe von Tags Kosten nachverfolgen, finden Sie unter [Erstellen von benutzerdefinierten Kostenzuweisungs-Tags für CloudTrail Lake-Event-Datenspeicher](#). Informationen darüber, wie Sie IAM-Richtlinien verwenden, um den Zugriff auf einen Ereignisdatenspeicher basierend auf Tags zu autorisieren, finden Sie unter [Beispiele: Verweigern des Zugriffs zum Erstellen oder Löschen von Ereignisdatenspeichern basierend auf Tags](#). Informationen darüber, wie Sie Tags verwenden können AWS, finden Sie unter [Tagging Your AWS Resources User Guide](#) im Tagging AWS Resources User Guide.

10. Wählen Sie Next (Weiter) aus, um den Ereignisdatenspeicher zu konfigurieren.
11. Behalten Sie auf der Seite Ereignisse auswählen die Standardauswahl für den Ereignistyp bei.

### Event type [Info](#)

Choose the type of events you want to add to your event data store. [Additional charges apply](#)

#### Choose event types

**AWS events**  
Capture operations performed on or within your AWS resources.

**Events from integrations**  
Create an integration to get events that are logged by applications outside of your AWS resources.

#### Specify the type of AWS events

**CloudTrail events**  
CloudTrail events provide a record of activity in an AWS account.

**CloudTrail Insights events**  
Insights events help identify unusual activity, errors, or user behavior in your account.

**Configuration items**  
Configuration items show changes made to the configuration of a resource, and show the resource's compliance status.

12. Wählen Sie für CloudTrail Ereignisse die Option Datenereignisse und deaktivieren Sie Verwaltungsereignisse. Weitere Informationen zu Datenereignissen finden Sie unter [Protokollieren von Datenereignissen](#).

### CloudTrail events [Info](#)

**Management events**  
Capture management operations performed on your AWS resources.

**Data events**  
Log the resource operations performed on or within a resource.

**Copy trail events**  
Copy CloudTrail events logged in your trails or from S3 buckets.

**Enable for all accounts in my organization**  
To review accounts in your organization, open AWS Organizations. [See all accounts](#)

► **Additional settings**

13. Behalten Sie die Standardeinstellung für Trail-Ereignisse kopieren bei. Sie würden diese Option verwenden, um vorhandene Trail-Ereignisse in Ihren Ereignisdatenspeicher zu kopieren. Weitere Informationen finden Sie unter [Kopieren von Trail-Ereignissen in einen Ereignisdatenspeicher](#).

14. Wählen Sie Für alle Konten in meiner Organisation aktivieren aus, wenn es sich um einen Ereignisdatenspeicher für eine Organisation handelt. Diese Option kann nur geändert werden, wenn Sie Konten in AWS Organizations konfiguriert haben.
15. Behalten Sie für Zusätzliche Einstellungen die Standardauswahl bei. Standardmäßig sammelt ein Ereignisdatenspeicher Ereignisse für alle AWS-Regionen und beginnt, Ereignisse zu erfassen, sobald er erstellt wird.
16. Treffen Sie für Datenereignisse die folgenden Auswahlen:
  - a. Wählen Sie unter Datenereignistyp S3 aus. Der Datenereignistyp identifiziert die Ressource AWS-Service und die Ressource, auf der Datenereignisse protokolliert werden.
  - b. Wählen Sie unter Protokoll-Selektorstempel Benutzerdefiniert aus. Wenn Sie Benutzerdefiniert wählen, können Sie einen benutzerdefinierten Ereignisselektor festlegen, um nach den Feldern `eventName`, `resources.ARN` und `readOnly` zu filtern. Informationen zu diesen Feldern finden Sie [AdvancedFieldSelector](#) in der AWS CloudTrail API-Referenz.
  - c. (Optional) Geben Sie unter Selektorname einen Namen ein, um Ihre Auswahl zu identifizieren. Der Selektorname ist ein beschreibender Name für einen erweiterten Event-Selektor, z. B. „DeleteObject API-Aufrufe für einen bestimmten S3-Bucket protokollieren“. Der Name des Selektors wird als Name in der erweiterten Ereignisauswahl aufgeführt und ist sichtbar, wenn Sie die JSON-Ansicht erweitern.

▼ JSON view

```
[
  {
    "Name": "Log DeleteObject API calls for a specific S3 bucket"
    "FieldSelectors": [
      {
        "Field": "eventName",
        "Equals": [
          "Data"
        ]
      },
      {
        "Field": "resources.type",
        "Equals": [
          "AWS::S3::Object"
        ]
      }
    ]
  },
]
```

- d. In Advanced Event Selectors erstellen wir den benutzerdefinierten Event-Selektor, um nach den Feldern und zu filtern. `eventName resources .ARN` Erweiterte Ereignisselectoren für einen Ereignisdatenspeicher funktionieren genauso wie erweiterte Ereignisselectoren, die Sie auf einen Trail anwenden. Weitere Informationen zum Erstellen von erweiterten Ereignisauswahlen finden Sie unter [Protokollieren von Datenereignissen mit erweiterten Ereignisauswahlen](#).
  - i. Wählen Sie für Feld die Option `eventName`. Wählen Sie für Operator die Option `Equals` aus. Geben Sie für Wert **DeleteObject** ein. Wählen Sie `+` Feld, um nach einem anderen Feld zu filtern.
  - ii. Wählen Sie für Feld `resources.ARN` aus. Wählen Sie für Operator die Option `StartsWith`. Geben Sie für Wert den ARN für Ihren Bucket ein (z. B. *arn:aws:s3:::bucket-name*). Informationen zum Abrufen des ARN finden Sie unter [Amazon-S3-Ressourcen](#) im Benutzerhandbuch von Amazon Simple Storage Service.

### Data events [Info](#)

Data events show information about the resource operations performed on or within a resource.

▼ **Data event: S3**

Remove

**Data event type**  
Choose the source of data events to log.

S3
▼

**Log selector template**

Custom
▼

**Selector name - optional**

Log DeleteObject API calls for a specific S3 bucket

1,000 character limit

**Collect events**  
Log all events, or choose a template to log specific, filtered events to your trail. You can edit templates later.

**Advanced event selectors** [Info](#)  
Log or exclude events from specific resources.

Field	Operator	Value	✕
<span>eventName</span> <span style="font-size: 0.8em;">▼</span>	<span>equals</span> <span style="font-size: 0.8em;">▼</span>	DeleteObject	✕
AND			
+ Condition			
<span>resources.ARN</span> <span style="font-size: 0.8em;">▼</span>	<span>starts with</span> <span style="font-size: 0.8em;">▼</span>	arn:aws:s3:::bucket-name	✕
+ Field			
+ Condition			

▶ **JSON view**

Add data event type

17. Wählen Sie Next (Weiter) aus, um Ihre Auswahl zu überprüfen.

18. Überprüfen Sie auf der Seite Prüfen und erstellen Ihre Auswahl. Wählen Sie Bearbeiten aus, um Änderungen am Schema vorzunehmen. Wenn Sie bereit sind, den Ereignisdatenspeicher zu erstellen, wählen Sie Ereignisdatenspeicher erstellen aus.



19. Der neue Ereignisdatenspeicher ist in der Tabelle Ereignisdatenspeicher auf der Seite Ereignisdatenspeicher sichtbar.

Ab diesem Zeitpunkt erfasst der Ereignisdatenspeicher Ereignisse, die mit seinen erweiterten Ereigniselektoren übereinstimmen. Ereignisse, die aufgetreten sind, bevor Sie den Ereignisdatenspeicher erstellt haben, befinden sich nicht im Ereignisdatenspeicher, es sei denn Sie haben sich für das Kopieren der bestehenden Trail-Ereignissen entschieden.

## Erstellen Sie mit der Konsole einen Ereignisdatenspeicher für CloudTrail Insights-Ereignisse

AWS CloudTrail Insights helfen AWS Benutzern, ungewöhnliche Aktivitäten im Zusammenhang mit API-Aufrufen und API-Fehlerraten zu identifizieren und darauf zu reagieren, indem CloudTrail Verwaltungsereignisse kontinuierlich analysiert werden. CloudTrail Insights analysiert Ihre normalen Muster des API-Aufrufvolumens und der API-Fehlerraten, auch Basiswerte genannt, und generiert Insights-Ereignisse, wenn das Aufrufvolumen oder die Fehlerraten außerhalb der normalen Muster liegen. Insights-Ereignisse zum API-Aufrufvolumen werden für `write`-Verwaltungs-APIs und Insights-Ereignisse zur API-Fehlerrate für `read`- und `write`-Verwaltungs-APIs generiert.

Um Insights-Ereignisse in CloudTrail Lake zu protokollieren, benötigen Sie einen Zielereignisdatenspeicher, der Insights-Ereignisse protokolliert, und einen Quellereignisdatenspeicher, der Insights aktiviert und Verwaltungsereignisse protokolliert.

### Note

Um Insights-Ereignisse anhand des API-Aufrufvolumens zu protokollieren, muss der Quellereignisdatenspeicher `write`-Verwaltungsereignisse protokollieren. Um Insights-Ereignisse anhand der API-Fehlerrate zu protokollieren, muss der Quellereignisdatenspeicher `read`- oder `write`-Verwaltungsereignisse protokollieren.

Wenn Sie CloudTrail Insights in einem Quell-Eventdatenspeicher aktiviert haben und ungewöhnliche CloudTrail Aktivitäten erkennen, werden CloudTrail Insights-Ereignisse an Ihren Zielereignisdatenspeicher übermittelt. Im Gegensatz zu anderen Arten von Ereignissen, die in einem CloudTrail Ereignisdatenspeicher erfasst werden, werden Insights-Ereignisse nur protokolliert, wenn Änderungen in der API-Nutzung Ihres Kontos CloudTrail festgestellt werden, die sich erheblich von den typischen Nutzungsmustern des Kontos unterscheiden.

Nachdem Sie CloudTrail Insights zum ersten Mal in einem Ereignisdatenspeicher aktiviert haben, kann es bis zu 7 Tage dauern, CloudTrail bis das erste Insights-Ereignis übermittelt wird, wenn ungewöhnliche Aktivitäten festgestellt werden.

CloudTrail Insights analysiert Verwaltungsereignisse, die in einer einzelnen Region und nicht global auftreten. Ein CloudTrail Insights-Ereignis wird in derselben Region generiert, in der auch die unterstützenden Managementereignisse generiert werden.

CloudTrail analysiert bei einem Datenspeicher für Organisationsereignisse Verwaltungsereignisse aus den Konten der einzelnen Mitglieder, anstatt die Aggregation aller Verwaltungsereignisse für die Organisation zu analysieren.

Für die Aufnahme von Insights-Veranstaltungen in Lake fallen zusätzliche Gebühren an CloudTrail . Wenn Sie Insights sowohl für Trails als auch für CloudTrail Lake Event Data Stores aktivieren, fallen separate Gebühren an. Informationen zur CloudTrail Preisgestaltung finden Sie unter [AWS CloudTrail Preise](#).

## Themen

- [Erstellen eines Zielereignisdatenspeichers, der Insights-Ereignisse protokolliert](#)
- [Erstellen eines Quellereignisdatenspeichers, der Insights-Ereignisse aktiviert](#)

## Erstellen eines Zielereignisdatenspeichers, der Insights-Ereignisse protokolliert

Wenn Sie einen Insights-Ereignisdatenspeicher erstellen, haben Sie die Option, einen vorhandenen Quellereignisdatenspeicher auszuwählen, der Verwaltungsereignisse protokolliert, und dann die Insights-Typen anzugeben, die Sie empfangen möchten. Alternativ können Sie Insights auch in einem neuen oder vorhandenen Ereignisdatenspeicher aktivieren, nachdem Sie Ihren Insights-Ereignisdatenspeicher erstellt haben und ihn dann als Zielereignisdatenspeicher auswählen.

Mit den folgenden Schritten erstellen Sie einen Zielereignisdatenspeicher, der Insights-Ereignisse protokolliert.

1. Melden Sie sich bei der an AWS Management Console und öffnen Sie die CloudTrail Konsole unter <https://console.aws.amazon.com/cloudtrail/>.
2. Öffnen Sie im Navigationsbereich das Untermenü Lake und wählen Sie dann Event Data Stores (Ereignisdatenspeicher) aus.
3. Wählen Sie Ereignisdatenspeicher erstellen aus.


4. Geben Sie auf der Seite Konfigurieren eines Ereignisdatenspeichers in Allgemeine Angaben einen Namen für den Ereignisdatenspeicher ein. Ein Name ist erforderlich.
5. Wählen Sie die Preisoption aus, die Sie für den Ereignisdatenspeicher verwenden möchten. Der Preisoption bestimmt die Kosten für die Erfassung und Speicherung von Ereignissen sowie die standardmäßige und maximale Aufbewahrungsdauern für Ihren Ereignisdatenspeicher. Weitere Informationen finden Sie unter [AWS CloudTrail -Preise](#) und [Verwaltung der CloudTrail Seekosten](#).

Die folgenden Optionen sind verfügbar:

- Preisoption mit verlängerbarer Aufbewahrung für ein Jahr – Empfohlen, wenn Sie damit rechnen, weniger als 25 TB an Ereignisdaten pro Monat zu erfassen und eine flexible Aufbewahrungsdauer von bis zu 10 Jahren wünschen. In den ersten 366 Tagen (Standardaufbewahrungszeitraum) ist Speicherplatz ohne zusätzliche Kosten im Preis für die Datenaufnahme enthalten. Nach 366 Tagen ist eine erweiterte Aufbewahrung gegen Aufpreis pay-as-you-go verfügbar. Dies ist die Standardoption.
    - Standardaufbewahrungsdauer: 366 Tage.
    - Maximale Aufbewahrungsdauer: beträgt 3 653 Tage.
  - Preisoption für die Aufbewahrung über sieben Jahre – Empfohlen, wenn Sie damit rechnen, mehr als 25 TB an Ereignisdaten pro Monat zu erfassen und eine flexible Aufbewahrungsdauer von bis zu 7 Jahren wünschen. Die Aufbewahrung ist im Preis für die Erfassung ohne Zusatzkosten enthalten.
    - Standardaufbewahrungsdauer: 2 557 Tage.
    - Maximale Aufbewahrungsdauer: beträgt 2 557 Tage.
6. Geben Sie einen Aufbewahrungszeitraum für den Ereignisdatenspeicher in Tagen an. Die Aufbewahrungsdauern können zwischen 7 Tagen und 3 653 Tagen (etwa 10 Jahre) für die Preisoption mit verlängerbarer Aufbewahrungsdauer für ein Jahr oder zwischen 7 Tagen und 2 557 Tagen (etwa sieben Jahre) für die Preisoption mit siebenjähriger Aufbewahrungsdauer liegen. Der Ereignisdatenspeicher behält Ereignisdaten für die angegebene Anzahl von Tagen bei.
  7. (Optional) Um die Verschlüsselung mit zu aktivieren AWS Key Management Service, wählen Sie Eigene verwenden aus AWS KMS key. Wählen Sie Neu, um einen für Sie AWS KMS key erstellen zu lassen, oder wählen Sie Bestehend, um einen vorhandenen KMS-Schlüssel zu verwenden. Geben Sie unter KMS-Alias eingeben einen Alias im folgenden Format an `alias/MyAliasName`. Wenn Sie Ihren eigenen KMS-Schlüssel verwenden, müssen Sie Ihre KMS-Schlüsselrichtlinie bearbeiten, um das Verschlüsseln und Entschlüsseln von CloudTrail

Protokollen zuzulassen. Weitere Informationen finden Sie unter [Konfigurieren Sie AWS KMS wichtige Richtlinien für CloudTrail](#). CloudTrail unterstützt auch Schlüssel AWS KMS für mehrere Regionen. Weitere Informationen finden Sie über Multi-Regions-Schlüssel finden Sie unter [Verwenden von Schlüsseln für mehrere Regionen](#) im AWS Key Management Service - Entwicklerhandbuch.

Die Verwendung Ihres eigenen KMS-Schlüssels verursacht AWS KMS Kosten für die Verschlüsselung und Entschlüsselung. Nachdem Sie einen KMS-Schlüssel einem Ereignisdatenspeicher zugeordnet haben, kann der KMS-Schlüssel nicht entfernt oder geändert werden.

 Note

Um die AWS Key Management Service Verschlüsselung für den Ereignisdatenspeicher einer Organisation zu aktivieren, müssen Sie einen vorhandenen KMS-Schlüssel für das Verwaltungskonto verwenden.

8. (Optional) Wenn Sie Ihre Ereignisdaten mit Amazon Athena abfragen möchten, wählen Sie Aktivieren in Lake-Abfrageverbund. Mit Verbund können Sie die mit einem Ereignisdatenspeicher verbundenen Metadaten im AWS Glue [-Datenkatalog](#) einsehen und mit Amazon Athena SQL-Abfragen zu den Ereignisdaten durchführen. Anhand der im AWS Glue Datenkatalog gespeicherten Tabellenmetadaten weiß die Athena-Abfrage-Engine, wie die Daten, die Sie abfragen möchten, gesucht, gelesen und verarbeitet werden. Weitere Informationen finden Sie unter [Verbund für einen Ereignisdatenspeicher erstellen](#).

Wählen Sie Aktivieren und gehen Sie wie folgt vor, um Lake-Abfrageverbund zu aktivieren:

- a. Wählen Sie aus, ob Sie eine neue Rolle erstellen oder eine vorhandene IAM-Rolle verwenden möchten. [AWS Lake Formation](#) verwendet diese Rolle, um die Berechtigungen für den Verbundereignisdatenspeicher zu verwalten. Wenn Sie mit der CloudTrail Konsole eine neue Rolle erstellen, CloudTrail wird automatisch eine Rolle mit den erforderlichen Berechtigungen erstellt. Wenn Sie eine bestehende Rolle auswählen, stellen Sie sicher, dass die Richtlinie für die Rolle die [erforderlichen Mindestberechtigungen](#) vorsieht.
- b. Wenn Sie eine neue Rolle erstellen, geben Sie einen Namen zur Identifizierung der Rolle ein.
- c. Wenn Sie eine bestehende Rolle verwenden, wählen Sie die Rolle aus, die Sie verwenden möchten. Die Rolle muss in Ihrem Konto vorhanden sein.

9. (Optional) Im Bereich Tags können Sie bis zu 50 Tag-Schlüssel-Paare hinzufügen, um den Zugriff auf den Ereignisdatenspeicher festzulegen, zu sortieren und zu steuern. Weitere Informationen darüber, wie Sie IAM-Richtlinien verwenden, um den Zugriff auf einen Ereignisdatenspeicher basierend auf Tags zu autorisieren, finden Sie unter [Beispiele: Verweigern des Zugriffs zum Erstellen oder Löschen von Ereignisdatenspeichern basierend auf Tags](#). Weitere Informationen zur Verwendung von Tags finden Sie unter [Tagging Your AWS Resources User Guide im Tagging AWS Resources User Guide](#). AWS
10. Wählen Sie Next (Weiter) aus, um den Ereignisdatenspeicher zu konfigurieren.
11. Wählen Sie auf der Seite Ereignisse auswählen die Option AWS Ereignisse und dann CloudTrailInsights-Ereignisse aus.
12. Gehen Sie CloudTrail unter Insights-Ereignisse wie folgt vor.
  - a. Wählen Sie Delegierten Administratorzugriff zulassen, wenn Sie dem delegierten Administrator Ihrer Organisation Zugriff auf diesen Ereignisdatenspeicher gewähren möchten. Diese Option ist nur verfügbar, wenn Sie mit dem Verwaltungskonto einer AWS Organizations Organisation angemeldet sind.
  - b. (Optional) Wählen Sie einen vorhandenen Quellereignisdatenspeicher aus, der Verwaltungsereignisse protokolliert, und geben Sie die Insights-Typen an, die Sie empfangen möchten.

Führen Sie die folgenden Schritte aus, um einen Quellereignisdatenspeicher hinzuzufügen:

- i. Wählen Sie Quell-Ereignisdatenspeicher hinzufügen aus.
- ii. Wählen Sie den gewünschten Quellereignisdatenspeicher aus.
- iii. Wählen Sie den Instance-Typen aus, den Sie empfangen möchten.
  - `ApiCallRateInsight`: Der Insights-Typ `ApiCallRateInsight` analysiert nur schreibgeschützte Verwaltungs-API-Aufrufe, die pro Minute anhand eines festgelegten API-Aufruf-Volumens aggregiert werden. Um Insights zu `ApiCallRateInsight` empfangen zu können, muss der Quellereignisdatenspeicher Schreib-Verwaltungsereignisse protokollieren.
  - `ApiErrorRateInsight`: Der Insights-Typ `ApiErrorRateInsight` analysiert Verwaltungs-API-Aufrufe, die zu Fehlercodes führen. Der Fehler wird angezeigt, wenn der API-Aufruf fehlschlägt. Um Insights zu `ApiErrorRateInsight` empfangen zu können, muss der Quellereignisdatenspeicher Schreib- und Leseverwaltungsereignisse protokollieren.

- iv. Wiederholen Sie die beiden vorherigen Schritte (ii und iii), um weitere Insights-Typen hinzuzufügen, die Sie empfangen möchten.
13. Wählen Sie Next (Weiter) aus, um Ihre Auswahl zu überprüfen.
  14. Überprüfen Sie auf der Seite Prüfen und erstellen Ihre Auswahl. Wählen Sie Bearbeiten aus, um Änderungen am Schema vorzunehmen. Wenn Sie bereit sind, den Ereignisdatenspeicher zu erstellen, wählen Sie Ereignisdatenspeicher erstellen aus.
  15. Der neue Ereignisdatenspeicher ist in der Tabelle Ereignisdatenspeicher auf der Seite Ereignisdatenspeicher sichtbar.
  16. Wenn Sie in Schritt 10 keinen Quellereignisdatenspeicher ausgewählt haben, folgen Sie den Schritten unter [Erstellen eines Quellereignisdatenspeichers, der Insights-Ereignisse aktiviert](#), um Quellereignisdatenspeicher zu erstellen.

### Erstellen eines Quellereignisdatenspeichers, der Insights-Ereignisse aktiviert

Mit den folgenden Schritten erstellen Sie einen Quellereignisdatenspeicher, der Insights-Ereignisse aktiviert und Verwaltungsereignisse protokolliert.

1. Melden Sie sich bei der an AWS Management Console und öffnen Sie die CloudTrail Konsole unter <https://console.aws.amazon.com/cloudtrail/>.
2. Öffnen Sie im Navigationsbereich das Untermenü Lake und wählen Sie dann Event Data Stores (Ereignisdatenspeicher) aus.
3. Wählen Sie Ereignisdatenspeicher erstellen aus.
4. Geben Sie auf der Seite Konfigurieren eines Ereignisdatenspeichers in Allgemeine Angaben einen Namen für den Ereignisdatenspeicher ein. Ein Name ist erforderlich.
5. Wählen Sie die Preisoption aus, die Sie für den Ereignisdatenspeicher verwenden möchten. Der Preisoption bestimmt die Kosten für die Erfassung und Speicherung von Ereignissen sowie die standardmäßige und maximale Aufbewahrungsdauern für Ihren Ereignisdatenspeicher. Weitere Informationen finden Sie unter [AWS CloudTrail -Preise](#) und [Verwaltung der CloudTrail Seekosten](#).

Die folgenden Optionen sind verfügbar:

- Preisoption mit verlängerbarer Aufbewahrung für ein Jahr – Empfohlen, wenn Sie damit rechnen, weniger als 25 TB an Ereignisdaten pro Monat zu erfassen und eine flexible Aufbewahrungsdauer von bis zu 10 Jahren wünschen. In den ersten 366 Tagen (Standardaufbewahrungszeitraum) ist Speicherplatz ohne zusätzliche Kosten im Preis für die


Datenaufnahme enthalten. Nach 366 Tagen ist eine erweiterte Aufbewahrung gegen Aufpreis pay-as-you-go verfügbar. Dies ist die Standardoption.

- Standardaufbewahrungsdauer: 366 Tage.
  - Maximale Aufbewahrungsdauer: beträgt 3 653 Tage.
6. Preisoption für die Aufbewahrung über sieben Jahre – Empfohlen, wenn Sie damit rechnen, mehr als 25 TB an Ereignisdaten pro Monat zu erfassen und eine flexible Aufbewahrungsdauer von bis zu 7 Jahren wünschen. Die Aufbewahrung ist im Preis für die Erfassung ohne Zusatzkosten enthalten.
- Standardaufbewahrungsdauer: 2 557 Tage.
  - Maximale Aufbewahrungsdauer: beträgt 2 557 Tage.
6. Geben Sie einen Aufbewahrungszeitraum für den Ereignisdatenspeicher an. Die Aufbewahrungsdauern können zwischen 7 Tagen und 3 653 Tagen (etwa 10 Jahre) für die Preisoption mit verlängerbarer Aufbewahrungsdauer für ein Jahr oder zwischen 7 Tagen und 2 557 Tagen (etwa sieben Jahre) für die Preisoption mit siebenjähriger Aufbewahrungsdauer liegen.

CloudTrail Lake entscheidet, ob ein Ereignis aufbewahrt werden soll, indem es prüft, ob das Ereignis innerhalb `eventTime` des angegebenen Aufbewahrungszeitraums liegt. Wenn Sie beispielsweise einen Aufbewahrungszeitraum von 90 Tagen angeben, CloudTrail werden Ereignisse entfernt, wenn sie `eventTime` älter als 90 Tage sind.

7. (Optional) Um die Verschlüsselung mit zu aktivieren AWS Key Management Service, wählen Sie Eigene verwenden aus AWS KMS key. Wählen Sie Neu, um einen für Sie AWS KMS key erstellen zu lassen, oder wählen Sie Bestehend, um einen vorhandenen KMS-Schlüssel zu verwenden. Geben Sie unter KMS-Alias eingeben einen Alias im folgenden Format an `alias/MyAliasName`. Wenn Sie Ihren eigenen KMS-Schlüssel verwenden, müssen Sie Ihre KMS-Schlüsselrichtlinie bearbeiten, um das Verschlüsseln und Entschlüsseln von CloudTrail Protokollen zuzulassen. Weitere Informationen finden Sie unter [Konfigurieren Sie AWS KMS wichtige Richtlinien für CloudTrail](#). CloudTrail unterstützt auch Schlüssel AWS KMS für mehrere Regionen. Weitere Informationen finden Sie über Multi-Regions-Schlüssel finden Sie unter [Verwenden von Schlüsseln für mehrere Regionen](#) im AWS Key Management Service - Entwicklerhandbuch.

Die Verwendung Ihres eigenen KMS-Schlüssels verursacht AWS KMS Kosten für die Verschlüsselung und Entschlüsselung. Nachdem Sie einen KMS-Schlüssel einem Ereignisdatenspeicher zugeordnet haben, kann der KMS-Schlüssel nicht entfernt oder geändert werden.

 Note

Um die AWS Key Management Service Verschlüsselung für den Ereignisdatenspeicher einer Organisation zu aktivieren, müssen Sie einen vorhandenen KMS-Schlüssel für das Verwaltungskonto verwenden.

8. (Optional) Wenn Sie Ihre Ereignisdaten mit Amazon Athena abfragen möchten, wählen Sie Aktivieren in Lake-Abfrageverbund. Mit Verbund können Sie die mit einem Ereignisdatenspeicher verbundenen Metadaten im AWS Glue [-Datenkatalog](#) einsehen und mit Amazon Athena SQL-Abfragen zu den Ereignisdaten durchführen. Anhand der im AWS Glue Datenkatalog gespeicherten Tabellenmetadaten weiß die Athena-Abfrage-Engine, wie die Daten, die Sie abfragen möchten, gesucht, gelesen und verarbeitet werden. Weitere Informationen finden Sie unter [Verbund für einen Ereignisdatenspeicher erstellen](#).

Wählen Sie Aktivieren und gehen Sie wie folgt vor, um Lake-Abfrageverbund zu aktivieren:

- a. Wählen Sie aus, ob Sie eine neue Rolle erstellen oder eine vorhandene IAM-Rolle verwenden möchten. [AWS Lake Formation](#) verwendet diese Rolle, um die Berechtigungen für den Verbundereignisdatenspeicher zu verwalten. Wenn Sie mit der CloudTrail Konsole eine neue Rolle erstellen, CloudTrail wird automatisch eine Rolle mit den erforderlichen Berechtigungen erstellt. Wenn Sie eine bestehende Rolle auswählen, stellen Sie sicher, dass die Richtlinie für die Rolle die [erforderlichen Mindestberechtigungen](#) vorsieht.
  - b. Wenn Sie eine neue Rolle erstellen, geben Sie einen Namen zur Identifizierung der Rolle ein.
  - c. Wenn Sie eine bestehende Rolle verwenden, wählen Sie die Rolle aus, die Sie verwenden möchten. Die Rolle muss in Ihrem Konto vorhanden sein.
9. (Optional) Im Bereich Tags können Sie bis zu 50 Tag-Schlüssel-Paare hinzufügen, um den Zugriff auf den Ereignisdatenspeicher festzulegen, zu sortieren und zu steuern. Weitere Informationen darüber, wie Sie IAM-Richtlinien verwenden, um den Zugriff auf einen Ereignisdatenspeicher basierend auf Tags zu autorisieren, finden Sie unter [Beispiele: Verweigern des Zugriffs zum Erstellen oder Löschen von Ereignisdatenspeichern basierend auf Tags](#). Weitere Informationen zur Verwendung von Tags finden Sie unter [Tagging Your AWS Resources User Guide im Tagging AWS Resources User Guide](#). AWS
  10. Wählen Sie Next (Weiter) aus, um den Ereignisdatenspeicher zu konfigurieren.
  11. Wählen Sie auf der Seite Ereignisse auswählen die Option AWS Ereignisse und dann Ereignisse ausCloudTrail.



12. Lassen Sie CloudTrail unter Ereignisse die Option Management-Ereignisse ausgewählt.
13. Damit Ihr Ereignisdatenspeicher Ereignisse von allen Konten in einer AWS Organizations -Organisation erfasst, wählen Sie Für alle Konten in meiner Organisation aktivieren aus. Sie müssen beim Verwaltungskonto der Organisation angemeldet sein, um einen Ereignisdatenspeicher zu erstellen, der Insights aktiviert.
14. Erweitern Sie Zusätzliche Einstellungen, um auszuwählen, ob Ihr Ereignisdatenspeicher Ereignisse für alle AWS-Regionen oder nur für die aktuellen Ereignisse erfassen soll AWS-Region, und wählen Sie aus, ob der Ereignisdatenspeicher Ereignisse aufnimmt. Standardmäßig erfasst der Ereignisdatenspeicher Ereignisse aus allen Regionen in Ihrem Konto und beginnt ab der Erstellung damit, Ereignisse aufzunehmen.
  - a. Wählen Sie Nur die aktuelle Region in meinen Ereignisdatenspeicher einbeziehen aus, um nur Ereignisse einzubeziehen, die in der aktuellen Region protokolliert werden. Wenn Sie diese Option nicht auswählen, enthält der Ereignisdatenspeicher Ereignisse aus allen Regionen.
  - b. Lassen Sie die Option Ereignisse aufnehmen ausgewählt.
15. Wählen Sie die Verwaltungsereignistypen aus, die in den Ereignisdatenspeicher einbezogen werden sollen. Sie können Lesen, Schreiben oder beides auswählen. Mindestens eine Option muss ausgewählt werden.

 Note

Um Insights-Ereignisse anhand des API-Aufrufvolumens zu protokollieren, muss der Ereignisdatenspeicher `write`-Verwaltungsereignisse protokollieren. Um Insights-Ereignisse anhand der API-Fehlerrate zu protokollieren, muss der Ereignisdatenspeicher `read`- oder `write`-Verwaltungsereignisse protokollieren.

16. Sie können wählen, ob Sie Amazon RDS Data API-Ereignisse aus Ihrem Ereignisdatenspeicher ausschließen AWS Key Management Service oder aus diesem ausschließen möchten. Weitere Informationen zu diesen Optionen finden Sie unter [Protokollieren von Verwaltungsereignissen](#).
17. Wählen Sie Insights aktivieren aus.
18. Wählen Sie unter Insights aktivieren den Zielereignisspeicher aus, in dem Insights-Ereignisse protokolliert werden sollen. Der Zielereignisdatenspeicher erfasst Insights-Ereignisse auf der Grundlage der Verwaltungsereignisaktivität in diesem Ereignisdatenspeicher. Weitere Informationen zum Erstellen des Zielereignisdatenspeichers finden Sie unter [Erstellen eines Zielereignisdatenspeichers, der Insights-Ereignisse protokolliert](#).

19. Wählen Sie die Insights-Typen aus. Sie können die API-Aufruftrate, die API-Fehlerrate oder beides auswählen. Sie müssen Schreib-Verwaltungsereignisse protokollieren, um Insights-Ereignisse für die API-Aufruftrate zu protokollieren. Sie müssen Lese- und Schreib-Verwaltungsereignisse protokollieren, um Insights-Ereignisse für die API-Fehlerrate zu protokollieren.
20. Wählen Sie Next (Weiter) aus, um Ihre Auswahl zu überprüfen.
21. Überprüfen Sie auf der Seite Prüfen und erstellen Ihre Auswahl. Wählen Sie Bearbeiten aus, um Änderungen am Schema vorzunehmen. Wenn Sie bereit sind, den Ereignisdatenspeicher zu erstellen, wählen Sie Ereignisdatenspeicher erstellen aus.
22. Der neue Ereignisdatenspeicher ist in der Tabelle Ereignisdatenspeicher auf der Seite Ereignisdatenspeicher sichtbar.

Ab diesem Zeitpunkt erfasst der Ereignisdatenspeicher Ereignisse, die mit seinen erweiterten Ereigniselektoren übereinstimmen. Nachdem Sie CloudTrail Insights zum ersten Mal in Ihrem Quell-Ereignisdatenspeicher aktiviert haben, kann es bis zu 7 Tage dauern, CloudTrail bis das erste Insights-Ereignis an Ihren Ziel-Ereignisdatenspeicher übermittelt wird, falls ungewöhnliche Aktivitäten festgestellt werden.

Sie können das CloudTrail Lake-Dashboard aufrufen, um die Insights-Ereignisse in Ihrem Zielergebnisdatenspeicher zu visualisieren. Weitere Informationen zu Lake-Dashboards finden Sie unter [CloudTrail Lake-Dashboards anzeigen](#).

Für die Aufnahme von Insights-Veranstaltungen in CloudTrail Lake fallen zusätzliche Gebühren an. Wenn Sie Insights sowohl für Trails als auch für Ereignisdatenspeicher aktivieren, wird Ihnen eine separate Gebühr in Rechnung gestellt. Informationen zur CloudTrail Preisgestaltung finden Sie unter [AWS CloudTrail Preise](#).

## Erstellen Sie mit der Konsole einen Ereignisdatenspeicher für AWS Config Konfigurationselemente

Sie können einen Ereignisdatenspeicher erstellen, der [AWS Config -Konfigurationselemente](#) enthält, und damit nicht-konforme Änderungen an Ihren Produktionsumgebungen untersuchen. Mit einem Ereignisdatenspeicher können Sie nicht-konforme Regeln den Benutzern und Ressourcen zuordnen, die mit den jeweiligen Änderungen im Zusammenhang stehen. Ein Konfigurationselement stellt eine point-in-time Ansicht der Attribute einer unterstützten AWS Ressource dar, die in Ihrem Konto vorhanden ist. AWS Config erstellt ein Konfigurationselement, wenn es eine Änderung an einem

Ressourcentyp feststellt, den es aufzeichnet. AWS Config erstellt auch Konfigurationselemente, wenn ein Konfigurations-Snapshot erfasst wird.

Sie können AWS Config sowohl als auch CloudTrail Lake verwenden, um Abfragen für Ihre Konfigurationselemente auszuführen. Sie können AWS Config damit den aktuellen Konfigurationsstatus von AWS Ressourcen auf der Grundlage von Konfigurationseigenschaften für ein einzelnes AWS-Konto und AWS-Region oder für mehrere Konten und Regionen abfragen. Im Gegensatz dazu können Sie CloudTrail Lake verwenden, um verschiedene Datenquellen wie CloudTrail Ereignisse, Konfigurationselemente und Regelauswertungen abzufragen. CloudTrail Lake-Abfragen decken alle AWS Config Konfigurationselemente ab, einschließlich der Ressourcenkonfiguration und des Kompatibilitätsverlaufs.

Das Erstellen eines Ereignisdatenspeichers für Konfigurationselemente hat keine Auswirkungen auf bestehende AWS Config erweiterte Abfragen oder konfigurierte AWS Config Aggregatoren. Sie können weiterhin erweiterte Abfragen mit Ihren AWS Config S3-Buckets ausführen und diese AWS Config weiterhin an Ihre S3-Buckets senden.

CloudTrail Für Datenspeicher mit Lake-Ereignissen fallen Gebühren an. Beim Erstellen eines Ereignisdatenspeichers wählen Sie die [Preisoption](#) aus, die für den Ereignisdatenspeicher genutzt werden soll. Die Preisoption bestimmt die Kosten für die Erfassung und Speicherung von Ereignissen sowie die standardmäßige und maximale Aufbewahrungsdauer für den Ereignisdatenspeicher. Informationen zur CloudTrail Preisgestaltung und Verwaltung der Lake-Kosten finden Sie unter [AWS CloudTrail Preise](#) und [Verwaltung der CloudTrail Seekosten](#).

## Einschränkungen

Bezüglich der Ereignisdatenspeicher für Konfigurationselemente gelten die folgenden Einschränkungen.

- Keine Unterstützung für benutzerdefinierte Konfigurationselemente
- Keine Unterstützung für die Ereignisfilterung mit erweiterten Ereignisselektoren

## Voraussetzungen

Bevor Sie Ihren Veranstaltungsdatspeicher erstellen, richten Sie die AWS Config Aufzeichnung für alle Ihre Konten und Regionen ein. Sie können [Quick Setup](#), eine Funktion von, verwenden AWS Systems Manager, um schnell einen Konfigurationsrekorder zu erstellen, der von unterstützt wird AWS Config.

**Note**

Wenn Sie mit der Aufzeichnung von Konfigurationen AWS Config beginnen, werden Ihnen Gebühren für die Nutzung des Dienstes berechnet. Weitere Informationen über die Preise finden Sie unter [AWS Config – Preise](#). Weitere Informationen zur Verwaltung des Konfigurations-Recorders finden Sie unter [Verwalten des Konfigurations-Recorders](#) im Entwicklerhandbuch zu AWS Config .

Darüber hinaus werden die folgenden Aktionen empfohlen. Sie sind jedoch nicht erforderlich, um einen Ereignisdatenspeicher zu erstellen.

- Richten Sie einen Amazon-S3-Bucket für den Empfang eines Konfigurations-Snapshots (auf Anfrage) und eines Konfigurationsverlaufs ein. Weitere Informationen zu Snapshots finden Sie unter [Verwalten des Übermittlungskanals](#) und [Übermitteln eines Konfigurations-Snapshots an einen Amazon-S3-Bucket](#) im Entwicklerhandbuch zu AWS Config .
- Geben Sie die Regeln an, anhand derer Sie AWS Config die Konformitätsinformationen für die aufgezeichneten Ressourcentypen auswerten möchten. Einige der CloudTrail Lake-Beispielabfragen für AWS Config erfordern AWS-Config-Regeln die Bewertung des Konformitätsstatus Ihrer AWS Ressourcen. Weitere Informationen dazu finden Sie AWS-Config-Regeln unter [Evaluierung von Ressourcen mit AWS-Config-Regeln](#) im AWS Config Entwicklerhandbuch.

So erstellen Sie einen Ereignisdatenspeicher für Konfigurationselemente

1. Melden Sie sich bei der an AWS Management Console und öffnen Sie die CloudTrail Konsole unter <https://console.aws.amazon.com/cloudtrail/>.
2. Wählen Sie im Navigationsbereich unter Lake die Option Ereignisdatenspeicher aus.
3. Wählen Sie Ereignisdatenspeicher erstellen aus.
4. Geben Sie auf der Seite Konfigurieren eines Ereignisdatenspeichers in Allgemeine Angaben einen Namen für den Ereignisdatenspeicher ein. Ein Name ist erforderlich.
5. Wählen Sie die Preisoption aus, die Sie für den Ereignisdatenspeicher verwenden möchten. Der Preisoption bestimmt die Kosten für die Erfassung und Speicherung von Ereignissen sowie die standardmäßige und maximale Aufbewahrungsdauern für Ihren Ereignisdatenspeicher. Weitere Informationen finden Sie unter [AWS CloudTrail -Preise](#) und [Verwaltung der CloudTrail Seekosten](#).

Die folgenden Optionen sind verfügbar:


- Preisoption mit verlängerbarer Aufbewahrung für ein Jahr – Empfohlen, wenn Sie damit rechnen, weniger als 25 TB an Ereignisdaten pro Monat zu erfassen und eine flexible Aufbewahrungsdauer von bis zu 10 Jahren wünschen. In den ersten 366 Tagen (Standardaufbewahrungszeitraum) ist Speicherplatz ohne zusätzliche Kosten im Preis für die Datenaufnahme enthalten. Nach 366 Tagen ist eine erweiterte Aufbewahrung gegen Aufpreis pay-as-you-go verfügbar. Dies ist die Standardoption.
    - Standardaufbewahrungsdauer: 366 Tage.
    - Maximale Aufbewahrungsdauer: beträgt 3 653 Tage.
  - Preisoption für die Aufbewahrung über sieben Jahre – Empfohlen, wenn Sie damit rechnen, mehr als 25 TB an Ereignisdaten pro Monat zu erfassen und eine flexible Aufbewahrungsdauer von bis zu 7 Jahren wünschen. Die Aufbewahrung ist im Preis für die Erfassung ohne Zusatzkosten enthalten.
    - Standardaufbewahrungsdauer: 2 557 Tage.
    - Maximale Aufbewahrungsdauer: beträgt 2 557 Tage.
6. Geben Sie einen Aufbewahrungszeitraum für den Ereignisdatenspeicher an. Die Aufbewahrungsdauern können zwischen 7 Tagen und 3 653 Tagen (etwa 10 Jahre) für die Preisoption mit verlängerbarer Aufbewahrungsdauer für ein Jahr oder zwischen 7 Tagen und 2 557 Tagen (etwa sieben Jahre) für die Preisoption mit siebenjähriger Aufbewahrungsdauer liegen.

CloudTrail Lake entscheidet, ob ein Ereignis aufbewahrt werden soll, indem es prüft, ob das Ereignis innerhalb `eventTime` des angegebenen Aufbewahrungszeitraums liegt. Wenn Sie beispielsweise einen Aufbewahrungszeitraum von 90 Tagen angeben, CloudTrail werden Ereignisse entfernt, wenn sie `eventTime` älter als 90 Tage sind.

7. (Optional) Um die Verschlüsselung mit zu aktivieren AWS Key Management Service, wählen Sie Eigene verwenden aus AWS KMS key. Wählen Sie Neu, um einen für Sie AWS KMS key erstellen zu lassen, oder wählen Sie Bestehend, um einen vorhandenen KMS-Schlüssel zu verwenden. Geben Sie unter KMS-Alias eingeben einen Alias im folgenden Format an `alias/MyAliasName`. Wenn Sie Ihren eigenen KMS-Schlüssel verwenden, müssen Sie Ihre KMS-Schlüsselrichtlinie bearbeiten, um das Verschlüsseln und Entschlüsseln von CloudTrail Protokollen zuzulassen. Weitere Informationen finden Sie unter [Konfigurieren Sie AWS KMS wichtige Richtlinien für CloudTrail](#). CloudTrail unterstützt auch Schlüssel AWS KMS für mehrere Regionen. Weitere Informationen finden Sie über Multi-Regions-Schlüssel finden Sie

unter [Verwenden von Schlüsseln für mehrere Regionen](#) im AWS Key Management Service - Entwicklerhandbuch.

Wenn Sie Ihren eigenen KMS-Schlüssel verwenden, fallen AWS KMS Kosten für die Verschlüsselung und Entschlüsselung an. Nachdem Sie einen KMS-Schlüssel einem Ereignisdatenspeicher zugeordnet haben, kann der KMS-Schlüssel nicht entfernt oder geändert werden.

 Note

Um die AWS Key Management Service Verschlüsselung für den Ereignisdatenspeicher einer Organisation zu aktivieren, müssen Sie einen vorhandenen KMS-Schlüssel für das Verwaltungskonto verwenden.

8. (Optional) Wenn Sie Ihre Ereignisdaten mit Amazon Athena abfragen möchten, wählen Sie Aktivieren in Lake-Abfrageverbund. Mit Verbund können Sie die mit einem Ereignisdatenspeicher verbundenen Metadaten im AWS Glue [-Datenkatalog](#) einsehen und mit Amazon Athena SQL-Abfragen zu den Ereignisdaten durchführen. Anhand der im AWS Glue Datenkatalog gespeicherten Tabellenmetadaten weiß die Athena-Abfrage-Engine, wie die Daten, die Sie abfragen möchten, gesucht, gelesen und verarbeitet werden. Weitere Informationen finden Sie unter [Verbund für einen Ereignisdatenspeicher erstellen](#).

Wählen Sie Aktivieren und gehen Sie wie folgt vor, um Lake-Abfrageverbund zu aktivieren:

- a. Wählen Sie aus, ob Sie eine neue Rolle erstellen oder eine vorhandene IAM-Rolle verwenden möchten. [AWS Lake Formation](#) verwendet diese Rolle, um die Berechtigungen für den Verbundereignisdatenspeicher zu verwalten. Wenn Sie mit der CloudTrail Konsole eine neue Rolle erstellen, CloudTrail wird automatisch eine Rolle mit den erforderlichen Berechtigungen erstellt. Wenn Sie eine bestehende Rolle auswählen, stellen Sie sicher, dass die Richtlinie für die Rolle die [erforderlichen Mindestberechtigungen](#) vorsieht.
  - b. Wenn Sie eine neue Rolle erstellen, geben Sie einen Namen zur Identifizierung der Rolle ein.
  - c. Wenn Sie eine bestehende Rolle verwenden, wählen Sie die Rolle aus, die Sie verwenden möchten. Die Rolle muss in Ihrem Konto vorhanden sein.
9. (Optional) Im Bereich Tags können Sie bis zu 50 Tag-Schlüssel-Paare hinzufügen, um den Zugriff auf den Ereignisdatenspeicher festzulegen, zu sortieren und zu steuern. Weitere Informationen darüber, wie Sie IAM-Richtlinien verwenden, um den Zugriff auf einen

Ereignisdatenspeicher basierend auf Tags zu autorisieren, finden Sie unter [Beispiele: Verweigern des Zugriffs zum Erstellen oder Löschen von Ereignisdatenspeichern basierend auf Tags](#). Weitere Informationen zur Verwendung von Tags finden Sie unter [Tagging Your AWS Resources User Guide im Tagging AWS Resources User Guide](#). AWS

10. Wählen Sie Weiter aus.
11. Wählen Sie auf der Seite Ereignisse auswählen die Option AWS -Ereignisse und dann Konfigurationselemente aus.
12. CloudTrail speichert die Datenspeicherressource für Ereignisse in der Region, in der Sie sie erstellen. Standardmäßig stammen die im Datenspeicher gesammelten Konfigurationselemente jedoch aus allen Regionen in Ihrem Konto, für die die Aufzeichnung aktiviert ist. Optional können Sie Include only the current region in my event data store (Nur die aktuelle Region in meinen Ereignisdatenspeicher einbeziehen) auswählen, um nur Konfigurationselemente einzubeziehen, die in der aktuellen Region erfasst werden. Wenn Sie diese Option nicht auswählen, enthält Ihr Ereignisdatenspeicher Konfigurationselemente aus allen Regionen, für die die Aufzeichnung aktiviert ist.
13. Damit Ihr Event-Datenspeicher Konfigurationselemente von allen Konten in einer AWS Organizations Organisation sammelt, wählen Sie Für alle Konten in meiner Organisation aktivieren aus. Sie müssen beim Verwaltungskonto oder beim Konto eines delegierten Administrators der Organisation angemeldet sein, um einen Ereignisdatenspeicher zu erstellen, der Konfigurationselemente für eine Organisation erfasst.
14. Wählen Sie Next (Weiter) aus, um Ihre Auswahl zu überprüfen.
15. Überprüfen Sie auf der Seite Prüfen und erstellen Ihre Auswahl. Wählen Sie Bearbeiten aus, um Änderungen am Schema vorzunehmen. Wenn Sie bereit sind, den Ereignisdatenspeicher zu erstellen, wählen Sie Ereignisdatenspeicher erstellen aus.
16. Der neue Ereignisdatenspeicher ist in der Tabelle Ereignisdatenspeicher auf der Seite Ereignisdatenspeicher sichtbar.

Konfigurationselemente werden ab diesem Zeitpunkt vom Ereignisdatenspeicher erfasst. Konfigurationselemente, die vor der Erstellung des Ereignisdatenspeichers aufgetreten sind, befinden sich nicht darin.

## Beispielabfragen

Nun können Sie Abfragen in Ihrem neuen Ereignisdatenspeicher ausführen. Auf der Registerkarte Beispielabfragen in der CloudTrail Konsole finden Sie Beispielabfragen, um Ihnen den Einstieg

zu erleichtern. Im Folgenden sind einige der Beispielabfragen aufgeführt, die Sie in Ihrem Ereignisdatenspeicher für Konfigurationselemente ausführen können.

Beschreibung	Abfrage
<p>Finden Sie heraus, welcher Benutzer eine Aktion ausgeführt hat, die zu einem Status „Nicht konform“ geführt hat, indem Sie einen Ereignisdatenspeicher für ein Konfigurationselement mit einem CloudTrail Ereignisdatenspeicher verknüpfen.</p>	<pre>SELECT     element_at(config1.eventData.configuration, 'targetResourceId')     as targetResourceId,     element_at(config1.eventData.configuration, 'complianceType')     as complianceType,     config2.eventData.resourceType,     cloudtrail.userIdentity FROM     <i>config_event_data_store_ID</i> as     config1 JOIN     <i>config_event_data_store_ID</i>     as config2 on element_at(config1     .eventData.configuration, 'targetResourceId') = config2.eventData.     resourceId JOIN     <i>cloudtrail_event_data_store_ID</i>     as cloudtrail on config2.eventData.     arn = element_at(cloudtrail.resources, 1).arn WHERE     element_at(config1.eventData.configuration, 'configRuleList')     is not null AND     element_at(config1.eventData.configuration, 'complianceType') =     'NON_COMPLIANT' AND     cloudtrail.eventTime &gt; '2022-11-     14 00:00:00' AND     config2.eventData.resourceType =     'AWS::DynamoDB::Table'</pre>



Beschreibung	Abfrage
<p>Finden Sie alle AWS Config Regeln und geben Sie den Konformitätsstatus anhand der am letzten Tag generierten Konfigurationselemente zurück.</p>	<pre>SELECT     eventData.configuration,     eventData.accountId, eventData     .awsRegion,     eventData.resourceName, eventData     .resourceCreationTime,     element_at(eventData.config uration, 'complianceType') AS     complianceType,     element_at(eventData.config uration, 'configRuleList') AS     configRuleList,     element_at(eventData.config uration, 'resourceId') AS resourceI d,     element_at(eventData.config uration, 'resourceType') AS resourceT ype FROM     <i>config_event_data_store_ID</i> WHERE     eventData.resourceType =     'AWS::Config::ResourceCompliance' AND     eventTime &gt; '2022-11-22 00:00:00' ORDER BY     eventData.resourceCreationTime DESC     limit 10</pre>

Beschreibung	Abfrage
<p>Finden Sie die Gesamtzahl der AWS Config Ressourcen, gruppiert nach Ressourcentyp, Konto-ID und Region.</p>	<pre>SELECT     eventData.resourceType, eventData     .awsRegion, eventData.accountId,     COUNT (*) AS resourceCount FROM     <i>config_event_data_store_ID</i> WHERE     eventTime &gt; '2022-11-22 00:00:00' GROUP BY     eventData.resourceType, eventData     .awsRegion, eventData.accountId</pre>
<p>Ermitteln Sie die Erstellungszeit der Ressourcen für alle AWS Config Konfigurationselemente, die an einem bestimmten Datum generiert wurden.</p>	<pre>SELECT     eventData.configuration,     eventData.accountId,     eventData.awsRegion, eventData     .resourceId,     eventData.resourceName, eventData     .resourceType,     eventData.availabilityZone,     eventData.resourceCreationTime FROM     <i>config_event_data_store_ID</i> WHERE     eventTime &gt; '2022-11-16 00:00:00' AND     eventTime &lt; '2022-11-17 00:00:00'  ORDER BY     eventData.resourceCreationTime DESC     limit 10;</pre>

Weitere Informationen zum Erstellen und Bearbeiten von Abfragen finden Sie unter [Abfrage erstellen oder bearbeiten](#).

## Schema für Konfigurationselemente

In der folgenden Tabelle werden die erforderlichen und optionalen Schemaelemente beschrieben, die denen in den Aufzeichnungen der Konfigurationselemente entsprechen. Der Inhalt von `eventData` wird durch Ihre Konfigurationselemente bereitgestellt; andere Felder werden von CloudTrail nach der Aufnahme bereitgestellt.

CloudTrail Der Inhalt des Ereignisdatensatzes wird unter ausführlicher beschrieben. [CloudTrail Inhalt aufzeichnen](#)

- [Felder, die CloudTrail nach der Aufnahme bereitgestellt werden](#)
- [Felder, die durch Ihre Ereignisse bereitgestellt werden](#)

Felder, die von after ingestion bereitgestellt werden CloudTrail

Feldname	Eingabetyp	Anforderung	Beschreibung
<code>eventVersion</code>	Zeichenfolge	Erforderlich	Die Version des AWS Ereignisformats.
<code>eventCategory</code>	Zeichenfolge	Erforderlich	Die Kategorie des Ereignisses. Für Konfigurationselemente lautet der gültige Wert <code>ConfigurationItem</code> .
<code>eventType</code>	Zeichenfolge	Erforderlich	Der Ereignistyp. Für Konfigurationselemente lautet der gültige Wert <code>AwsConfigurationItem</code> .
<code>eventID</code>	Zeichenfolge	Erforderlich	Eine eindeutige ID für ein Ereignis.
<code>eventTime</code>	Zeichenfolge	Erforderlich	Der Zeitstempel des Ereignisses im Format <code>yyyy-MM-D</code>

Feldname	Eingabetyp	Anforderung	Beschreibung
			DTHH:mm:ss , in Universal Coordinated Time (UTC).
awsRegion	Zeichenfolge	Erforderlich	Die AWS-Region , der ein Ereignis zugewiesen werden soll.
recipientAccountId	Zeichenfolge	Erforderlich	Stellt die AWS-Konto ID dar, die dieses Ereignis empfangen hat.
addendum	addendum	Optional	Zeigt Informationen dazu an, warum sich ein Ereignis verzögert hat. Wenn Informationen zu einem bestehenden Ereignis fehlten, enthält der Nachtragsblock die fehlenden Informationen und einen Grund für das Fehlen.

Die Felder in **eventData** werden durch Ihre Konfigurationselemente bereitgestellt.

Feldname	Eingabetyp	Anforderung	Beschreibung
eventData	-	Erforderlich	Felder in eventData werden durch Ihre Konfigurationselemente bereitgestellt.

Feldname	Eingabetyp	Anforderung	Beschreibung
<ul style="list-style-type: none"> <li>configurationItemVersion</li> </ul>	Zeichenfolge	Optional	Die Version des Konfigurationselements aus der zugehörigen Quelle.
<ul style="list-style-type: none"> <li>configurationItemCaptureZeit</li> </ul>	Zeichenfolge	Optional	Die Uhrzeit, zu der die Konfigurationsaufzeichnung initiiert wurde.
<ul style="list-style-type: none"> <li>configurationItemStatus</li> </ul>	Zeichenfolge	Optional	Der Status des Konfigurationselements. Gültige Werte sind OK, ResourceDiscovered, ResourceNotRecorded, ResourceDeleted und ResourceDeletedNotRecorded.
<ul style="list-style-type: none"> <li>accountId</li> </ul>	Zeichenfolge	Optional	Die 12-stellige AWS-Konto ID, die der Ressource zugeordnet ist.
<ul style="list-style-type: none"> <li>RessourcenTyp</li> </ul>	Zeichenfolge	Optional	Der Typ der AWS Ressource. Weitere Informationen zu gültigen Ressourcentypen finden Sie <a href="#">ConfigurationItem</a> in der AWS Config API-Referenz.

Feldname	Eingabetyp	Anforderung	Beschreibung
• resourceId	Zeichenfolge	Optional	Die ID der Ressource (z. B. sg-xxxxxx).
• RessourcenNamen	Zeichenfolge	Optional	Der benutzerdefinierte Name der Ressource, sofern verfügbar.
• arn	Zeichenfolge	Optional	Der Amazon-Ressourcenname (ARN), der der Ressource zugeordnet ist.
• awsRegion	Zeichenfolge	Optional	Der AWS-Region Ort, an dem sich die Ressource befindet.
• availabilityZone	Zeichenfolge	Optional	Die Availability Zone, die der Ressource zugeordnet ist.
• resourceCreationTime	Zeichenfolge	Optional	Der Zeitstempel für die Erstellung der Ressource.
• Konfiguration	JSON	Optional	Die Beschreibung der Ressourcenkonfiguration.

Feldname	Eingabetyp	Anforderung	Beschreibung
<ul style="list-style-type: none"> <li>• supplementaryConfiguration</li> </ul>	JSON	Optional	Konfigurationsattribute, die für bestimmte Ressourcentypen AWS Config zurückgegeben werden, um die für den Konfigurationsparameter zurückgegebenen Informationen zu ergänzen.
<ul style="list-style-type: none"> <li>• relatedEvents</li> </ul>	Zeichenfolge	Optional	Eine Liste von CloudTrail Ereignis-IDs.
<ul style="list-style-type: none"> <li>• relationships</li> </ul>	-	Optional	Eine Liste verwandter AWS Ressourcen.
<ul style="list-style-type: none"> <li>• • Name</li> </ul>	Zeichenfolge	Optional	Die Art der Beziehung mit der zugehörigen Ressource.
<ul style="list-style-type: none"> <li>• • Ressourcentyp</li> </ul>	Zeichenfolge	Optional	Der Ressourcentyp der zugehörigen Ressource.
<ul style="list-style-type: none"> <li>• • resourceId</li> </ul>	Zeichenfolge	Optional	Die ID der zugehörigen Ressource (z. B. <code>sg-xxxxxx</code> ).
<ul style="list-style-type: none"> <li>• • RessourcenName</li> </ul>	Zeichenfolge	Optional	Der benutzerdefinierte Name der zugehörigen Ressource, sofern verfügbar.

Feldname	Eingabetyp	Anforderung	Beschreibung
• tags	JSON	Optional	Schlüssel-Wert-Tag s, die der Ressource zugeordnet sind.

Das folgende Beispiel zeigt die Hierarchie von Schemaelementen, die denen in den Aufzeichnungen von Konfigurationselementen entsprechen.

```
{
  "eventVersion": String,
  "eventCategory": String,
  "eventType": String,
  "eventID": String,
  "eventTime": String,
  "awsRegion": String,
  "recipientAccountId": String,
  "addendum": Addendum,
  "eventData": {
    "configurationItemVersion": String,
    "configurationItemCaptureTime": String,
    "configurationItemStatus": String,
    "configurationStateId": String,
    "accountId": String,
    "resourceType": String,
    "resourceId": String,
    "resourceName": String,
    "arn": String,
    "awsRegion": String,
    "availabilityZone": String,
    "resourceCreationTime": String,
    "configuration": {
      JSON,
    },
    "supplementaryConfiguration": {
      JSON,
    },
    "relatedEvents": [
      String
    ],
    "relationships": [
```



```
    struct{
      "name" : String,
      "resourceType": String,
      "resourceId": String,
      "resourceName": String
    }
  ],
  "tags": {
    JSON
  }
}
}
```

## Erstellen Sie einen Ereignisdatenspeicher für Ereignisse außerhalb der AWS Konsole

Sie können einen Ereignisdatenspeicher erstellen, der Ereignisse außerhalb von enthält AWS, und dann CloudTrail Lake verwenden, um die Daten zu suchen, abzufragen und zu analysieren, die in Ihren Anwendungen protokolliert werden.

Sie können CloudTrail Lake-Integrationen verwenden, um Benutzeraktivitätsdaten von außerhalb zu protokollieren und zu speichern AWS; aus beliebigen Quellen in Ihren Hybridumgebungen, z. B. internen oder SaaS-Anwendungen, die vor Ort oder in der Cloud gehostet werden, virtuellen Maschinen oder Containern.

Wenn Sie einen Ereignisdatenspeicher für eine Integration erstellen, erstellen Sie auch einen Kanal und fügen dem Kanal eine Ressourcenrichtlinie hinzu.

CloudTrail Für die Speicherung von Ereignisdaten in Lake fallen Gebühren an. Beim Erstellen eines Ereignisdatenspeichers wählen Sie die [Preisoption](#) aus, die für den Ereignisdatenspeicher genutzt werden soll. Die Preisoption bestimmt die Kosten für die Erfassung und Speicherung von Ereignissen sowie die standardmäßige und maximale Aufbewahrungsdauer für den Ereignisdatenspeicher. Informationen zur CloudTrail Preisgestaltung und Verwaltung der Lake-Kosten finden Sie unter [AWS CloudTrail Preise](#) und [Verwaltung der CloudTrail Seekosten](#).

Um einen Ereignisdatenspeicher für Ereignisse außerhalb von zu erstellen AWS

1. Melden Sie sich bei der an AWS Management Console und öffnen Sie die CloudTrail Konsole unter <https://console.aws.amazon.com/cloudtrail/>.
2. Wählen Sie im Navigationsbereich unter Lake die Option Ereignisdatenspeicher aus.
3. Wählen Sie Ereignisdatenspeicher erstellen aus.

4. Geben Sie auf der Seite Konfigurieren eines Ereignisdatenspeichers in Allgemeine Angaben einen Namen für den Ereignisdatenspeicher ein. Ein Name ist erforderlich.
5. Wählen Sie die Preisoption aus, die Sie für den Ereignisdatenspeicher verwenden möchten. Der Preisoption bestimmt die Kosten für die Erfassung und Speicherung von Ereignissen sowie die standardmäßige und maximale Aufbewahrungsdauern für Ihren Ereignisdatenspeicher. Weitere Informationen finden Sie unter [AWS CloudTrail -Preise](#) und [Verwaltung der CloudTrail Seekosten](#).

Die folgenden Optionen sind verfügbar:


- Preisoption mit verlängerbarer Aufbewahrung für ein Jahr – Empfohlen, wenn Sie damit rechnen, weniger als 25 TB an Ereignisdaten pro Monat zu erfassen und eine flexible Aufbewahrungsdauer von bis zu 10 Jahren wünschen. In den ersten 366 Tagen (Standardaufbewahrungszeitraum) ist Speicherplatz ohne zusätzliche Kosten im Preis für die Datenaufnahme enthalten. Nach 366 Tagen ist eine erweiterte Aufbewahrung gegen Aufpreis pay-as-you-go verfügbar. Dies ist die Standardoption.
    - Standardaufbewahrungsdauer: 366 Tage.
    - Maximale Aufbewahrungsdauer: beträgt 3 653 Tage.
  - Preisoption für die Aufbewahrung über sieben Jahre – Empfohlen, wenn Sie damit rechnen, mehr als 25 TB an Ereignisdaten pro Monat zu erfassen und eine flexible Aufbewahrungsdauer von bis zu 7 Jahren wünschen. Die Aufbewahrung ist im Preis für die Erfassung ohne Zusatzkosten enthalten.
    - Standardaufbewahrungsdauer: 2 557 Tage.
    - Maximale Aufbewahrungsdauer: beträgt 2 557 Tage.
6. Geben Sie einen Aufbewahrungszeitraum für den Ereignisdatenspeicher an. Die Aufbewahrungsdauern können zwischen 7 Tagen und 3 653 Tagen (etwa 10 Jahre) für die Preisoption mit verlängerbarer Aufbewahrungsdauer für ein Jahr oder zwischen 7 Tagen und 2 557 Tagen (etwa sieben Jahre) für die Preisoption mit siebenjähriger Aufbewahrungsdauer liegen.

CloudTrail Lake entscheidet, ob ein Ereignis aufbewahrt werden soll, indem es prüft, ob das Ereignis innerhalb `eventTime` des angegebenen Aufbewahrungszeitraums liegt. Wenn Sie beispielsweise einen Aufbewahrungszeitraum von 90 Tagen angeben, CloudTrail werden Ereignisse entfernt, wenn sie `eventTime` älter als 90 Tage sind.

7. (Optional) Um die Verschlüsselung mit zu aktivieren AWS Key Management Service, wählen Sie Eigene verwenden aus AWS KMS key. Wählen Sie Neu, um einen für Sie AWS KMS

key erstellen zu lassen, oder wählen Sie Bestehend, um einen vorhandenen KMS-Schlüssel zu verwenden. Geben Sie unter KMS-Alias eingeben einen Alias im folgenden Format an `alias/MyAliasName`. Wenn Sie Ihren eigenen KMS-Schlüssel verwenden, müssen Sie Ihre KMS-Schlüsselrichtlinie bearbeiten, um das Verschlüsseln und Entschlüsseln von CloudTrail Protokollen zuzulassen. Weitere Informationen finden Sie unter [Konfigurieren Sie AWS KMS wichtige Richtlinien für CloudTrail](#). CloudTrail unterstützt auch Schlüssel AWS KMS für mehrere Regionen. Weitere Informationen finden Sie über Multi-Regions-Schlüssel finden Sie unter [Verwenden von Schlüsseln für mehrere Regionen](#) im AWS Key Management Service - Entwicklerhandbuch.

Wenn Sie Ihren eigenen KMS-Schlüssel verwenden, fallen AWS KMS Kosten für die Verschlüsselung und Entschlüsselung an. Nachdem Sie einen KMS-Schlüssel einem Ereignisdatenspeicher zugeordnet haben, kann der KMS-Schlüssel nicht entfernt oder geändert werden.

 Note

Um die AWS Key Management Service Verschlüsselung für den Ereignisdatenspeicher einer Organisation zu aktivieren, müssen Sie einen vorhandenen KMS-Schlüssel für das Verwaltungskonto verwenden.

8. (Optional) Wenn Sie Ihre Ereignisdaten mit Amazon Athena abfragen möchten, wählen Sie Aktivieren in Lake-Abfrageverbund. Mit Verbund können Sie die mit einem Ereignisdatenspeicher verbundenen Metadaten im AWS Glue [-Datenkatalog](#) einsehen und mit Amazon Athena SQL-Abfragen zu den Ereignisdaten durchführen. Anhand der im AWS Glue Datenkatalog gespeicherten Tabellenmetadaten weiß die Athena-Abfrage-Engine, wie die Daten, die Sie abfragen möchten, gesucht, gelesen und verarbeitet werden. Weitere Informationen finden Sie unter [Verbund für einen Ereignisdatenspeicher erstellen](#).

Wählen Sie Aktivieren und gehen Sie wie folgt vor, um Lake-Abfrageverbund zu aktivieren:

- a. Wählen Sie aus, ob Sie eine neue Rolle erstellen oder eine vorhandene IAM-Rolle verwenden möchten. [AWS Lake Formation](#) verwendet diese Rolle, um die Berechtigungen für den Verbundereignisdatenspeicher zu verwalten. Wenn Sie mit der CloudTrail Konsole eine neue Rolle erstellen, CloudTrail wird automatisch eine Rolle mit den erforderlichen Berechtigungen erstellt. Wenn Sie eine bestehende Rolle auswählen, stellen Sie sicher, dass die Richtlinie für die Rolle die [erforderlichen Mindestberechtigungen](#) vorsieht.

- b. Wenn Sie eine neue Rolle erstellen, geben Sie einen Namen zur Identifizierung der Rolle ein.
  - c. Wenn Sie eine bestehende Rolle verwenden, wählen Sie die Rolle aus, die Sie verwenden möchten. Die Rolle muss in Ihrem Konto vorhanden sein.
9. (Optional) Im Bereich Tags können Sie bis zu 50 Tag-Schlüssel-Paare hinzufügen, um den Zugriff auf den Ereignisdatenspeicher festzulegen, zu sortieren und zu steuern. Weitere Informationen darüber, wie Sie IAM-Richtlinien verwenden, um den Zugriff auf einen Ereignisdatenspeicher basierend auf Tags zu autorisieren, finden Sie unter [Beispiele: Verweigern des Zugriffs zum Erstellen oder Löschen von Ereignisdatenspeichern basierend auf Tags](#). Weitere Informationen zur Verwendung von Tags finden Sie unter [Tagging Your AWS Resources User Guide im Tagging AWS Resources User Guide](#). AWS
  10. Wählen Sie Next (Weiter) aus, um den Ereignisdatenspeicher zu konfigurieren.
  11. Wählen Sie auf der Seite Choose events (Ereignisse auswählen) die Option Events from integrations (Ereignisse aus Integrationen) aus.
  12. Wählen Sie unter Events from integration (Ereignisse aus Integration) die Quelle aus, aus der Ereignisse an den Ereignisdatenspeicher übermittelt werden sollen.
  13. Stellen Sie einen Namen zur Verfügung, um den Kanal der Integration zu identifizieren. Der Name kann eine Länge von 3–128 Zeichen haben. Namen dürfen nur Buchstaben, Zahlen, Punkte, Unterstriche und Schrägstriche enthalten.
  14. Konfigurieren Sie unter Resource policy (Ressourcenrichtlinie) die Ressourcenrichtlinie für den Kanal der Integration. Ressourcenbasierte Richtlinien sind JSON-Richtliniendokumente, die angeben, welche Aktionen ein bestimmter Prinzipal unter welchen Bedingungen für die Ressource ausführen kann. Die Konten, die in der Ressourcenrichtlinie als Prinzipale definiert sind, können die PutAuditEvents-API aufrufen, um Ereignisse an Ihren Kanal zu senden. Der Ressourcenbesitzer hat impliziten Zugriff auf die Ressource, sofern seine IAM-Richtlinie die `cloudtrail-data:PutAuditEvents`-Aktion zulässt.

Die für die Richtlinie erforderlichen Informationen werden durch den Integrationstyp bestimmt. Bei einer Direktionsintegration CloudTrail werden automatisch die AWS Konto-IDs des Partners hinzugefügt und Sie müssen die vom Partner bereitgestellte eindeutige externe ID eingeben. Für eine Lösungsintegration müssen Sie mindestens eine AWS Konto-ID als Principal angeben und können optional eine externe ID eingeben, um zu verhindern, dass Ihr Stellvertreter verwirrt wird.

**Note**

Wenn Sie keine Ressourcenrichtlinie für den Kanal erstellen, kann nur der Kanalbesitzer die `PutAuditEvents`-API auf dem Kanal aufrufen.

- a. Für eine direkte Integration geben Sie die von Ihrem Partner bereitgestellte externe ID ein. Der Integrationspartner stellt eine eindeutige externe ID zur Verfügung, z. B. eine Konto-ID oder eine zufällig generierte Zeichenfolge, die für die Integration verwendet wird, um zu verhindern, dass der Stellvertreter verwirrt wird. Der Partner ist für die Erstellung und Bereitstellung einer eindeutigen externen ID verantwortlich.

Sie können [How to find this? \(Wie finde ich das?\)](#) verwenden, um die Dokumentation des Partners einzusehen, in der beschrieben wird, wie Sie die externe ID finden.

**External ID**

Enter the unique account identifier provided by Nordcloud. [How to find this?](#) 

**Note**

Wenn die Ressourcenrichtlinie eine externe ID enthält, müssen alle Aufrufe der `PutAuditEvents`-API die externe ID enthalten. Wenn die Richtlinie jedoch keine externe ID definiert, kann der Partner die `PutAuditEvents`-API trotzdem aufrufen und einen `externalId`-Parameter angeben.

- b. Für eine Lösungsintegration wählen Sie `AWS Konto hinzufügen` aus, um jede AWS Konto-ID anzugeben, die der Richtlinie als Prinzipal hinzugefügt werden soll.
15. Wählen Sie `Next (Weiter)` aus, um Ihre Auswahl zu überprüfen.
  16. Überprüfen Sie auf der Seite `Prüfen` und erstellen Ihre Auswahl. Wählen Sie `Bearbeiten` aus, um Änderungen am Schema vorzunehmen. Wenn Sie bereit sind, den Ereignisdatenspeicher zu erstellen, wählen Sie `Ereignisdatenspeicher erstellen` aus.
  17. Der neue Ereignisdatenspeicher ist in der Tabelle `Ereignisdatenspeicher` auf der Seite `Ereignisdatenspeicher` sichtbar.
  18. Stellen Sie der Partneranwendung den Amazon-Ressourcennamen (ARN) für den Kanal zur Verfügung. Anweisungen zur Bereitstellung des Kanal-ARN für die Partneranwendung finden

Sie auf der Website mit der Partnerdokumentation. Um weitere Informationen zu erhalten, wählen Sie auf der Registerkarte Available sources (Verfügbare Quellen) der Seite Integrations (Integrationen) den Link Learn more (Weitere Informationen) für den Partner aus, um die Seite des Partners in AWS Marketplace zu öffnen.

Der Ereignisdatenspeicher beginnt mit der Aufnahme von Partnerereignissen CloudTrail über den Integrationskanal, wenn Sie, der Partner oder die Partneranwendungen die PutAuditEvents API auf dem Kanal aufrufen.

## Aktualisieren Sie einen Ereignisdatenspeicher mit der Konsole

In diesem Abschnitt wird beschrieben, wie Sie die Einstellungen eines Ereignisdatenspeichers mithilfe der AWS Management Console aktualisieren. Hinweise zum Aktualisieren eines Ereignisdatenspeichers mithilfe von finden Sie unter [Aktualisieren Sie einen Ereignisdatenspeicher mit dem AWS CLI](#). AWS CLI

So aktualisieren Sie einen Ereignisdatenspeicher

1. Melden Sie sich unter <https://console.aws.amazon.com/cloudtrail/> bei der an AWS Management Console und öffnen Sie die CloudTrail Konsole.
2. Wählen Sie im Navigationsbereich unter Lake die Option Ereignisdatenspeicher aus.
3. Wählen Sie den Ereignisdatenspeicher, den Sie aktualisieren möchten. Diese Aktion öffnet die Detailseite des Ereignisdatenspeichers.
4. Wählen Sie unter Allgemeine Details Bearbeiten aus, um die folgenden Einstellungen zu ändern:
  - Name des Ereignisdatenspeichers – Ändern Sie den Namen, der Ihren Ereignisdatenspeicher identifiziert.
  - [Preisoption](#) – Für Ereignisdatenspeicher, die die Preisoption mit siebenjähriger Aufbewahrungsdauer verwenden, können Sie stattdessen die Preisoption mit verlängerbarer Aufbewahrungsdauer für ein Jahr wählen. Für Ereignisdatenspeicher, die weniger als 25 TB an Ereignisdaten pro Monat erfassen, empfehlen wir eine verlängerbare Aufbewahrungsdauer für ein Jahr. Wenn Sie eine flexible Aufbewahrungsdauer von bis zu 10 Jahren anstreben, empfehlen wir außerdem eine verlängerbare Aufbewahrungsdauer für ein Jahr. Weitere Informationen finden Sie unter [AWS CloudTrail -Preise](#) und [Verwaltung der CloudTrail Seekosten](#).

**Note**

Sie können die Preisoption für Ereignisdatenspeicher, für die eine verlängerbare Aufbewahrungsdauer für ein Jahr verwendet wird, nicht ändern. Wenn Sie die Preisgestaltung für eine Aufbewahrung von sieben Jahren verwenden möchten, [beenden Sie die Erfassung](#) in Ihren aktuellen Ereignisdatenspeicher. Erstellen Sie anschließend einen neuen Speicher für Ereignisdaten mit der Preisoption für die Aufbewahrung von sieben Jahren.

- **Aufbewahrungsdauer** – Ändern Sie die Aufbewahrungsdauer für den Ereignisdatenspeicher. Die Aufbewahrungsdauer bestimmt, wie lange Ereignisdaten im Ereignisdatenspeicher aufbewahrt werden. Die Aufbewahrungsdauern können zwischen 7 Tagen und 3 653 Tagen (etwa 10 Jahre) für die Preisoption mit verlängerbarer Aufbewahrungsdauer für ein Jahr oder zwischen 7 Tagen und 2 557 Tagen (etwa sieben Jahre) für die Preisoption mit siebenjähriger Aufbewahrungsdauer liegen.

**Note**

Wenn Sie die Aufbewahrungsdauer eines Ereignisdatenspeichers verringern, CloudTrail werden alle Ereignisse entfernt, deren Aufbewahrungszeitraum `eventTime` älter als der neue ist. Wenn der vorherige Aufbewahrungszeitraum beispielsweise 365 Tage betrug und Sie ihn auf 100 Tage reduzieren, CloudTrail werden Ereignisse entfernt, deren Aufbewahrungszeitraum `eventTime` älter als 100 Tage ist.

- **Verschlüsselung** – Um die Verschlüsselung mit Ihrem eigenen KMS-Schlüssel zu aktivieren, wählen Sie `Meinen eigenen AWS KMS key verwenden`. Standardmäßig werden alle Ereignisse in einem Ereignisdatenspeicher von verschlüsselt CloudTrail. Wenn Sie Ihren eigenen KMS-Schlüssel verwenden, fallen AWS KMS Kosten für die Verschlüsselung und Entschlüsselung an.

**Note**

Nachdem Sie einen KMS-Schlüssel einem Ereignisdatenspeicher zugeordnet haben, kann der KMS-Schlüssel nicht entfernt oder geändert werden.

- Um nur Ereignisse einzuschließen, die in der aktuellen AWS-Region protokolliert werden, wählen Sie `In der aktuellen Region in meinem Ereignisdatenspeicher einschließen`. Wenn

Sie diese Option nicht auswählen, enthält der Ereignisdatenspeicher Ereignisse aus allen Regionen.

- Damit Ihr Ereignisdatenspeicher Ereignisse von allen Konten in einer AWS Organizations Organisation sammelt, wählen Sie Für alle Konten in meiner Organisation aktivieren aus. Diese Option ist nur verfügbar, wenn Sie mit dem Verwaltungskonto für Ihre Organisation angemeldet sind und der Ereignistyp für den Veranstaltungsdatspeicher CloudTrailEreignisse oder Konfigurationselemente lautet.

Wenn Sie fertig sind, wählen Sie Änderungen speichern aus.

5. Wählen Sie in Lake-Abfrageverbund die Option Bearbeiten aus, um Lake-Abfrageverbund zu aktivieren oder zu deaktivieren. Wenn Sie den [Lake-Abfrageverbund aktivieren](#), können Sie die Metadaten für Ihren Ereignisdatenspeicher im AWS Glue [Datenkatalog](#) anzeigen und mithilfe von Amazon Athena SQL-Abfragen für die Ereignisdaten ausführen. Wenn Sie den [Lake Query Federation deaktivieren](#), wird die Integration mit AWS Glue AWS Lake Formation, und Amazon Athena deaktiviert. Nachdem Sie den Lake-Abfrageverbund deaktiviert haben, können Sie Ihre Daten in Athena nicht mehr abfragen. Wenn Sie den Verbund deaktivieren, werden keine CloudTrail Lake-Daten gelöscht und Sie können weiterhin Abfragen in Lake ausführen. CloudTrail

Gehen Sie wie folgt vor, um den Verbund zu aktivieren:

- a. Wählen Sie Enable (Aktivieren) aus.
- b. Wählen Sie, ob Sie eine neue IAM-Rolle erstellen oder eine vorhandene Rolle verwenden möchten. Wenn Sie eine neue Rolle erstellen, CloudTrail wird automatisch eine Rolle mit den erforderlichen Berechtigungen erstellt. Wenn Sie eine bestehende Rolle verwenden, stellen Sie sicher, dass die Richtlinie für die Rolle die [erforderlichen Mindestberechtigungen](#) vorsieht.
- c. Wenn Sie eine neue IAM-Rolle erstellen, geben Sie einen Namen für die Rolle ein.
- d. Wenn Sie eine bestehende IAM-Rolle wählen, wählen Sie die Rolle aus, die Sie verwenden möchten. Die Rolle muss in Ihrem Konto vorhanden sein.

Klicken Sie auf Änderungen speichern, wenn Sie fertig sind.

6. Bearbeiten Sie alle zusätzlichen Einstellungen für Ihren Ereignistyp.



Ereignistyp	Bearbeitbare Einstellungen
CloudTrail Ereignisse	<p>Sie können die folgenden Einstellungen für CloudTrail Ereignisse bearbeiten:</p> <ul style="list-style-type: none"><li>• Um zu ändern, welche Ereignisse Ihr Ereignisdatenspeicher protokolliert, wählen Sie unter CloudTrail Ereignisse die Option Bearbeiten aus.</li><li>• Wählen Sie unter Verwaltungsereignisse die Option Bearbeiten aus, um die Einstellungen für Verwaltungsereignisse zu ändern. Weitere Informationen finden Sie in <a href="#">Protokollieren von Verwaltungsereignissen mit AWS Management Console</a> (Schritt 3).</li><li>• Wählen Sie unter Datenereignisse Bearbeiten aus, um die Einstellungen für die Datenereignisse zu ändern. Sie können auswählen, welche Datenereignistypen Sie protokollieren möchten, und die Protokollauswahlvorlage auswählen, die Sie verwenden möchten. Weitere Informationen finden Sie unter <a href="#">Aktualisierung eines vorhandenen Ereignisdatenspeichers zur Protokollierung von Datenereignissen in AWS Management Console</a>.</li></ul> <p>Wenn Sie fertig sind, wählen Sie Änderungen speichern aus.</p>

Ereignistyp	Bearbeitbare Einstellungen
Ereignisse aus der Integration	<p>Wählen Sie unter Integrationen Ihre Integration aus. Wählen Sie dann Bearbeiten aus, um die folgenden Einstellungen zu ändern.</p> <ul style="list-style-type: none"> <li>• Ändern Sie in den Integrationsdetails den Namen, der den Kanal Ihrer Integration identifiziert.</li> <li>• Wählen Sie unter Ort der Ereigniszustellung das Ziel für Ihre Ereignisse aus.</li> <li>• Konfigurieren Sie unter Resource policy (Ressourcenrichtlinie) die Ressourcenrichtlinie für den Kanal der Integration.</li> </ul> <p>Wenn Sie fertig sind, wählen Sie Änderungen speichern aus.</p> <p>Weitere Informationen zu diesen Einstellungen finden Sie unter <a href="#">Erstellen Sie eine Integration mit einer Ereignisquelle außerhalb von AWS</a>.</p>

- Um Stichwörter hinzuzufügen, zu ändern oder zu entfernen, wählen Sie unter Tags die Option Bearbeiten. Sie können bis zu 50 Tag-Schlüssel-Paare hinzufügen, um den Zugriff auf den Ereignisdatenspeicher festzulegen, zu sortieren und zu steuern. Wenn Sie fertig sind, wählen Sie Änderungen speichern aus.

## Stoppen und starten Sie die Ereigniserfassung über die Konsole

Standardmäßig sind Ereignisdatenspeicher dafür konfiguriert, Ereignisse aufzunehmen. Sie können verhindern, dass ein Ereignisdatenspeicher Ereignisse aufnimmt, AWS CLI indem Sie die Konsole oder APIs verwenden.

Die Optionen Aufnahme starten und Aufnahme beenden sind nur für Ereignisdatenspeicher verfügbar, die entweder CloudTrail Ereignisse (Verwaltungs- und Datenereignisse) oder Konfigurationselemente enthalten. AWS Config

Wenn Sie die Aufnahme für einen Ereignisdatenspeicher beenden, ändert sich sein Status zu STOPPED\_INGESTION. Sie können weiterhin Abfragen für Ereignisse ausführen, die sich bereits im Ereignisdatenspeicher befinden. Sie können Trail-Ereignisse auch in den Ereignisdatenspeicher kopieren (wenn dieser nur CloudTrail Verwaltungs- oder Datenereignisse enthält).

Die Aufnahme von Ereignissen in einen Ereignisdatenspeicher beenden Sie wie folgt:

1. Melden Sie sich bei der an AWS Management Console und öffnen Sie die CloudTrail Konsole unter <https://console.aws.amazon.com/cloudtrail/>.
2. Wählen Sie im Navigationsbereich unter Lake die Option Ereignisdatenspeicher aus.
3. Wählen Sie den Ereignisdatenspeicher aus.
4. Wählen Sie unter Aktionen die Option Aufnahme beenden aus.
5. Wenn Sie aufgefordert werden, den Vorgang zu bestätigen, wählen Sie Aufnahme beenden aus. Der Ereignisdatenspeicher nimmt dann keine Live-Ereignisse mehr auf.
6. Um die Aufnahme wieder fortzusetzen, wählen Sie Aufnahme starten aus.

So starten Sie die Ereigniserfassung neu

1. Melden Sie sich bei der an AWS Management Console und öffnen Sie die CloudTrail Konsole unter <https://console.aws.amazon.com/cloudtrail/>.
2. Wählen Sie im Navigationsbereich unter Lake die Option Ereignisdatenspeicher aus.
3. Wählen Sie den Ereignisdatenspeicher aus.
4. Wählen Sie unter Aktionen die Option Erfassung starten aus.

## Ändern Sie den Kündigungsschutz mit der Konsole

Standardmäßig sind Ereignisdatenspeicher in AWS CloudTrail Lake mit aktiviertem Kündigungsschutz konfiguriert. Der Beendigungsschutz verhindert, dass ein Ereignisdatenspeicher versehentlich gelöscht wird. Wenn Sie den Ereignisdatenspeicher löschen möchten, müssen Sie zuerst den Beendigungsschutz deaktivieren. Sie können den Kündigungsschutz mithilfe der API-Operationen AWS Management Console AWS CLI, oder deaktivieren.

So deaktivieren Sie den Beendigungsschutz

1. Melden Sie sich bei der an AWS Management Console und öffnen Sie die CloudTrail Konsole unter <https://console.aws.amazon.com/cloudtrail/>.

2. Wählen Sie im Navigationsbereich unter Lake die Option Ereignisdatenspeicher aus.
3. Wählen Sie den Ereignisdatenspeicher aus.
4. Wählen Sie Aktionen und dann Beendigungsschutz ändern.
5. Wählen Sie Deaktiviert aus.
6. Wählen Sie Speichern. Jetzt können Sie den Ereignisdatenspeicher löschen.

### So aktivieren Sie den Beendigungsschutz

1. Melden Sie sich bei der an AWS Management Console und öffnen Sie die CloudTrail Konsole unter <https://console.aws.amazon.com/cloudtrail/>.
2. Wählen Sie im Navigationsbereich unter Lake die Option Ereignisdatenspeicher aus.
3. Wählen Sie den Ereignisdatenspeicher aus.
4. Wählen Sie Aktionen und dann Beendigungsschutz ändern.
5. Um den Beendigungsschutz zu aktivieren, wählen Sie Aktiviert aus.
6. Wählen Sie Speichern.

### Löschen Sie einen Ereignisdatenspeicher mit der Konsole

In diesem Abschnitt wird beschrieben, wie Sie einen Ereignisdatenspeicher mithilfe der AWS CloudTrail -Konsole löschen. Hinweise zum Löschen eines Ereignisdatenspeichers mithilfe von finden Sie unter [Löschen Sie einen Ereignisdatenspeicher mit dem AWS CLI](#). AWS CLI

#### Note

Sie können einen Ereignisdatenspeicher nicht löschen, wenn entweder der [Beendigungsschutz](#) oder der [Lake-Abfrageverbund](#) aktiviert ist. CloudTrail Aktiviert standardmäßig den Kündigungsschutz, um einen Ereignisdatenspeicher vor dem versehentlichen Löschen zu schützen.

Um einen Ereignisdatenspeicher mit dem Ereignistyp Ereignisse aus der Integration zu löschen, müssen Sie zuerst den Kanal der Integration löschen. Sie können den Kanal auf der Detailseite der Integration oder mithilfe des Befehls `aws cloudtrail delete-channel` löschen. Weitere Informationen finden Sie unter [Löschen Sie einen Kanal, um eine Integration mit dem zu löschen AWS CLI](#).

## So löschen Sie einen Ereignisdatenspeicher

1. Melden Sie sich bei der an AWS Management Console und öffnen Sie die CloudTrail Konsole unter <https://console.aws.amazon.com/cloudtrail/>.
2. Wählen Sie im Navigationsbereich unter Lake die Option Ereignisdatenspeicher aus.
3. Wählen Sie den Ereignisdatenspeicher aus.
4. Klicken Sie bei Actions auf Delete.
5. Geben Sie den Namen des Ereignisdatenspeichers ein, um zu bestätigen, dass Sie ihn löschen möchten.
6. Wählen Sie Löschen aus.

Nachdem Sie einen Ereignisdatenspeicher gelöscht haben, ändert sich sein Status in PENDING\_DELETION und bleibt 7 Tage lang im Speicher. Sie können einen Ereignisdatenspeicher während der siebentägigen Wartezeit [wiederherstellen](#). Im Status PENDING\_DELETION ist ein Ereignisdatenspeicher nicht für Abfragen verfügbar und es können keine anderen Operationen mit dem Ereignisdatenspeicher durchgeführt werden, außer Wiederherstellungsoperationen. Ein Ereignisdatenspeicher mit ausstehendem Löschvorgang nimmt keine Ereignisse auf und verursacht keine Kosten. Ereignisdatenspeicher, deren Löschung noch aussteht, werden auf das Kontingent der Ereignisdatenspeicher angerechnet, die in einem Speicher vorhanden sein können AWS-Region.

## Stellen Sie einen Ereignisdatenspeicher mit der Konsole wieder her

Nachdem Sie einen Ereignisdatenspeicher in AWS CloudTrail Lake gelöscht haben, ändert sich sein Status in diesen Status PENDING\_DELETION und bleibt 7 Tage lang in diesem Zustand. Während dieser Zeit können Sie den Ereignisdatenspeicher mithilfe der [RestoreEventDataStore](#) API-Operation AWS Management Console AWS CLI, oder wiederherstellen.

In diesem Abschnitt wird beschrieben, wie Sie einen Ereignisdatenspeicher mithilfe der Konsole wiederherstellen. Hinweise zum Wiederherstellen eines Ereignisdatenspeichers mithilfe von finden Sie unter [Stellen Sie einen Ereignisdatenspeicher wieder her mit dem AWS CLI](#). AWS CLI

### So stellen Sie einen Ereignisdatenspeicher wieder her

1. Melden Sie sich unter <https://console.aws.amazon.com/cloudtrail/> bei der an AWS Management Console und öffnen Sie die CloudTrail Konsole.
2. Wählen Sie im Navigationsbereich unter Lake die Option Ereignisdatenspeicher aus.
3. Wählen Sie den Ereignisdatenspeicher aus.

4. Wählen Sie unter Aktionen die Option Wiederherstellen aus.

## Erstellen, aktualisieren und verwalten Sie Ereignisdatenspeicher mit dem AWS CLI

Sie können den verwenden, AWS CLI um Ihre Event-Datenspeicher zu erstellen, zu aktualisieren und zu verwalten. Denken Sie bei der Verwendung von daran AWS CLI, dass Ihre Befehle in der für Ihr Profil AWS-Region konfigurierten Version ausgeführt werden. Wenn Sie die Befehle in einer anderen Region ausführen möchten, ändern Sie entweder die Standardregion für Ihr Profil, oder verwenden Sie den `--region`-Parameter mit dem Befehl.

### Verfügbare Befehle für Ereignisdatenspeicher

Zu den Befehlen zum Erstellen und Aktualisieren von Ereignisdatenspeichern in CloudTrail Lake gehören:

- [create-event-data-store](#)um einen Ereignisdatenspeicher zu erstellen.
- [get-event-data-store](#)um Informationen über den Ereignisdatenspeicher zurückzugeben, einschließlich der erweiterten Ereigniselektoren, die für den Ereignisdatenspeicher konfiguriert sind.
- [update-event-data-store](#)um die Konfiguration eines vorhandenen Ereignisdatenspeichers zu ändern.
- [list-event-data-stores](#)um die Ereignisdatenspeicher aufzulisten.
- [delete-event-data-store](#)um einen Ereignisdatenspeicher zu löschen.
- [restore-event-data-store](#)um einen Ereignisdatenspeicher wiederherzustellen, dessen Löschung noch aussteht.
- [start-import](#)um einen Import von Trail-Ereignissen in einen Ereignisdatenspeicher zu starten oder einen fehlgeschlagenen Import erneut zu versuchen.
- [get-import](#)um Informationen über einen bestimmten Import zurückzugeben.
- [stop-import](#)um den Import von Trail-Ereignissen in einen Event-Datenspeicher zu stoppen.
- [list-imports](#)um Informationen zu allen Importen oder einer ausgewählten Gruppe von Importen von ImportStatus oder zurückzugebenDestination.
- [list-import-failures](#)um Importfehler für den angegebenen Import aufzulisten.
- [stop-event-data-store-ingestion](#)um die Aufnahme von Ereignissen in einen Ereignisdatenspeicher zu stoppen.

- [start-event-data-store-ingestion](#) um die Ereignisaufnahme in einem Ereignisdatenspeicher neu zu starten.
- [enable-federation](#) um den Verbund für einen Ereignisdatenspeicher zu aktivieren, um den Ereignisdatenspeicher in Amazon Athena abzufragen.
- [disable-federation](#) um den Verbund in einem Ereignisdatenspeicher zu deaktivieren. Nachdem Sie den Verbund deaktiviert haben, können Sie die Daten des Event-Datenspeichers in Amazon Athena nicht mehr abfragen. Sie können weiterhin Abfragen in CloudTrail Lake durchführen.
- [put-insight-selectors](#) um Insights-Ereignisselektoren für einen vorhandenen Ereignisdatenspeicher hinzuzufügen oder zu ändern und Insights-Ereignisse zu aktivieren oder zu deaktivieren.
- [get-insight-selectors](#) um Informationen über Insights-Ereignisselektoren zurückzugeben, die für einen Ereignisdatenspeicher konfiguriert sind.
- [add-tags](#) um einem vorhandenen Ereignisdatenspeicher ein oder mehrere Tags (Schlüssel-Wert-Paare) hinzuzufügen.
- [remove-tags](#) um ein oder mehrere Tags aus einem Ereignisdatenspeicher zu entfernen.
- [list-tags](#) um eine Liste von Tags zurückzugeben, die einem Ereignisdatenspeicher zugeordnet sind.

Eine Liste der verfügbaren Befehle für CloudTrail Lake-Abfragen finden Sie unter [Verfügbare Befehle für CloudTrail Lake-Abfragen](#).

Eine Liste der verfügbaren Befehle für CloudTrail Lake-Integrationen finden Sie unter [Verfügbare Befehle für CloudTrail Lake-Integrationen](#).

## Erstellen Sie einen Ereignisdatenspeicher mit dem AWS CLI

Verwenden Sie den Befehl [create-event-data-store](#), um einen Ereignisdatenspeicher zu erstellen.

Beim Erstellen eines Ereignisdatenspeichers ist der einzige erforderliche Parameter der `--name`, der zur Identifizierung des Ereignisdatenspeichers verwendet wird. Sie können zusätzliche optionale Parameter konfigurieren, darunter:

- `--advanced-event-selectors` – Gibt die Kategorie der Ereignisse an, die im Ereignisdatenspeicher aufgenommen werden sollen. Standardmäßig protokollieren

Ereignisdatenquellen alle Verwaltungsereignisse. Weitere Informationen zu erweiterten Event-Selektoren finden Sie [AdvancedEventSelector](#) in der CloudTrail API-Referenz.

- `--kms-key-id`— Gibt die AWS-KMS-Schlüssel-ID an, die zur Verschlüsselung der von CloudTrail übermittelten Ereignisse verwendet werden soll. Der Wert kann ein Alias-Name mit dem Präfix `alias/`, ein vollständig spezifizierter ARN für einen Alias, ein vollständig spezifizierter ARN für einen Schlüssel oder ein global eindeutiger Bezeichner sein.
- `--multi-region-enabled`— Erstellt einen regionsübergreifenden Ereignisdatenspeicher, der Ereignisse für alle Ereignisse AWS-Regionen in Ihrem Konto protokolliert. Standardmäßig ist `--multi-region-enabled` festgelegt, auch wenn der Parameter nicht hinzugefügt wurde.
- `--organization-enabled`— Ermöglicht es einem Ereignisdatenspeicher, Ereignisse für alle Konten in einer Organisation zu erfassen. Der Ereignisdatenspeicher ist standardmäßig nicht für alle Konten in einer Organisation aktiviert.
- `--billing-mode`— Bestimmt die Kosten für die Erfassung und Speicherung von Ereignissen sowie die standardmäßige und maximale Aufbewahrungsdauer für den Ereignisdatenspeicher.

Die folgenden Werte sind möglich:

- `EXTENDABLE_RETENTION_PRICING`— Dieser Abrechnungsmodus wird generell empfohlen, wenn Sie weniger als 25 TB an Ereignisdaten pro Monat erfassen und einen flexiblen Aufbewahrungszeitraum von bis zu 3 653 Tagen (etwa 10 Jahre) wünschen. Der Standardaufbewahrungszeitraum für diesen Abrechnungsmodus beträgt 366 Tage.
- `FIXED_RETENTION_PRICING`— Dieser Abrechnungsmodus wird empfohlen, wenn Sie damit rechnen, mehr als 25 TB an Ereignisdaten pro Monat zu erfassen und eine flexible Aufbewahrungsdauer von bis zu 2 557 Tagen (ca. 7 Jahren) wünschen. Der Standardaufbewahrungszeitraum für diesen Abrechnungsmodus beträgt 2 557 Tage.

Der Standardwert ist `EXTENDABLE_RETENTION_PRICING`.

- `--retention-period`— Die Anzahl der Tage, wie lange Ereignisse im Ereignisdatenspeicher aufbewahrt werden sollen. Gültige Werte sind Ganzzahlen zwischen 7 und 3 653, wenn der `--billing-mode` `EXTENDABLE_RETENTION_PRICING` ist, oder zwischen 7 und 2 557, wenn der `--billing-mode` auf `FIXED_RETENTION_PRICING` gesetzt ist. Wenn Sie dies nicht angeben `--retention-period`, CloudTrail wird der Standardaufbewahrungszeitraum für verwendet. `--billing-mode`
- `--start-ingestion`— Der Parameter `--start-ingestion` startet die Erfassung von Ereignissen im Ereignisdatenspeicher, wenn er erstellt wird. Dieser Parameter wird auch dann festgelegt, wenn der Parameter nicht hinzugefügt wurde.



Geben Sie `--no-start-ingestion` an, wenn der Ereignisdatenspeicher keine Live-Ereignisse erfassen soll. Sie können diesen Parameter beispielsweise festlegen, wenn Sie Ereignisse in den Ereignisdatenspeicher kopieren und die Ereignisdaten nur für die Analyse vergangener Ereignisse verwenden möchten. Der Parameter `--no-start-ingestion` ist nur gültig, wenn der `eventCategory` des Workflows Management, Data oder ConfigurationItem ist.

Die folgenden Beispiele veranschaulichen, wie Sie verschiedene Typen von Ereignisdatenspeichern erstellen können.

## Themen

- [Erstellen Sie einen Ereignisdatenspeicher für S3-Datenereignisse mit dem AWS CLI](#)
- [Erstellen Sie einen Ereignisdatenspeicher für AWS Config Konfigurationselemente mit dem AWS CLI](#)
- [Erstellen Sie einen Datenspeicher für Organisationsereignisse für Verwaltungsereignisse mit dem AWS CLI](#)
- [Erstellen Sie Ereignisdatenspeicher für Insights-Ereignisse mit dem AWS CLI](#)

Erstellen Sie einen Ereignisdatenspeicher für S3-Datenereignisse mit dem AWS CLI

Der folgende `create-event-data-store` Beispielbefehl AWS Command Line Interface (AWS CLI) erstellt einen Ereignisdatenspeicher mit dem Namen `my-event-data-store`, der alle Amazon S3 S3-Datenereignisse auswählt und mit einem KMS-Schlüssel verschlüsselt wird.

```
aws cloudtrail create-event-data-store \  
--name my-event-data-store \  
--kms-key-id "arn:aws:kms:us-east-1:123456789012:alias/KMS_key_alias" \  
--advanced-event-selectors '[  
  {  
    "Name": "Select all S3 data events",  
    "FieldSelectors": [  
      { "Field": "eventCategory", "Equals": ["Data"] },  
      { "Field": "resources.type", "Equals": ["AWS::S3::Object"] },  
      { "Field": "resources.ARN", "StartsWith": ["arn:aws:s3"] }  
    ]  
  }  
]'
```

Nachfolgend finden Sie eine Beispielantwort.

```
{
  "EventDataStoreArn": "arn:aws:cloudtrail:us-east-1:123456789012:eventdatastore/
EXAMPLE-ee54-4813-92d5-999aeEXAMPLE",
  "Name": "my-event-data-store",
  "Status": "CREATED",
  "AdvancedEventSelectors": [
    {
      "Name": "Select all S3 data events",
      "FieldSelectors": [
        {
          "Field": "eventCategory",
          "Equals": [
            "Data"
          ]
        },
        {
          "Field": "resources.type",
          "Equals": [
            "AWS::S3::Object"
          ]
        },
        {
          "Field": "resources.ARN",
          "StartsWith": [
            "arn:aws:s3"
          ]
        }
      ]
    }
  ],
  "MultiRegionEnabled": true,
  "OrganizationEnabled": false,
  "BillingMode": "EXTENDABLE_RETENTION_PRICING",
  "RetentionPeriod": 366,
  "KmsKeyId": "arn:aws:kms:us-east-1:123456789012:alias/KMS_key_alias",
  "TerminationProtectionEnabled": true,
  "CreatedTimestamp": "2023-11-09T22:19:39.417000-05:00",
  "UpdatedTimestamp": "2023-11-09T22:19:39.603000-05:00"
}
```

Erstellen Sie einen Ereignisdatenspeicher für AWS Config Konfigurationselemente mit dem AWS CLI

Der folgende AWS CLI `create-event-data-store` Beispielfehl erstellt einen Ereignisdatenspeicher mit dem Namen `config-items-eds`, der AWS Config Konfigurationselemente auswählt.

Um Konfigurationselemente zu erfassen, geben Sie an, dass das Feld `eventCategory` dem `ConfigurationItem` in den erweiterten Ereignisselektoren entspricht.

```
aws cloudtrail create-event-data-store \  
--name config-items-eds \  
--advanced-event-selectors '[  
  {  
    "Name": "Select AWS Config configuration items",  
    "FieldSelectors": [  
      { "Field": "eventCategory", "Equals": ["ConfigurationItem"] }  
    ]  
  }  
]'
```

Nachfolgend finden Sie eine Beispielantwort.

```
{  
  "EventDataStoreArn": "arn:aws:cloudtrail:us-east-1:123456789012:eventdatastore/  
EXAMPLE-ee54-4813-92d5-999aeEXAMPLE",  
  "Name": "config-items-eds",  
  "Status": "CREATED",  
  "AdvancedEventSelectors": [  
    {  
      "Name": "Select AWS Config configuration items",  
      "FieldSelectors": [  
        {  
          "Field": "eventCategory",  
          "Equals": [  
            "ConfigurationItem"  
          ]  
        }  
      ]  
    }  
  ],  
  "MultiRegionEnabled": true,  
  "OrganizationEnabled": false,  
  "BillingMode": "EXTENDABLE_RETENTION_PRICING",  
  "RetentionPeriod": 366,  
}
```

```
"TerminationProtectionEnabled": true,  
"CreatedTimestamp": "2023-11-07T19:03:24.277000+00:00",  
"UpdatedTimestamp": "2023-11-07T19:03:24.468000+00:00"  
}
```

Erstellen Sie einen Datenspeicher für Organisationsereignisse für Verwaltungsereignisse mit dem AWS CLI

Der folgende AWS CLI `create-event-data-store` Beispielbefehl erstellt einen Datenspeicher für Organisationsereignisse, der alle Verwaltungsereignisse sammelt und den `--billing-mode` Parameter auf `FIXED_RETENTION_PRICING` festlegt.

```
aws cloudtrail create-event-data-store --name org-management-eds --organization-enabled  
--billing-mode FIXED_RETENTION_PRICING
```

Nachfolgend finden Sie eine Beispielantwort.

```
{  
  "EventDataStoreArn": "arn:aws:cloudtrail:us-east-1:123456789012:eventdatastore/  
EXAMPLE6-d493-4914-9182-e52a7934b207",  
  "Name": "org-management-eds",  
  "Status": "CREATED",  
  "AdvancedEventSelectors": [  
    {  
      "Name": "Default management events",  
      "FieldSelectors": [  
        {  
          "Field": "eventCategory",  
          "Equals": [  
            "Management"  
          ]  
        }  
      ]  
    }  
  ],  
  "MultiRegionEnabled": true,  
  "OrganizationEnabled": true,  
  "BillingMode": "FIXED_RETENTION_PRICING",  
  "RetentionPeriod": 2557,  
  "TerminationProtectionEnabled": true,  
  "CreatedTimestamp": "2023-11-16T15:30:50.689000+00:00",  
  "UpdatedTimestamp": "2023-11-16T15:30:50.851000+00:00"  
}
```

}

Erstellen Sie Ereignisdatenspeicher für Insights-Ereignisse mit dem AWS CLI

Um Insights-Ereignisse in CloudTrail Lake zu protokollieren, benötigen Sie einen Ziel-Ereignisdatenspeicher, der Insights-Ereignisse sammelt, und einen Quell-Ereignisdatenspeicher, der Insights aktiviert und Verwaltungsereignisse protokolliert.

Dieses Verfahren zeigt, wie Sie die Ziel- und Quellereignisdatenspeicher erstellen und anschließend Insights-Ereignisse aktivieren.

1. Führen Sie den Befehl [aws cloudtrail create-event-data-store](#) aus, um einen Zielereignisdatenspeicher zu erstellen, der Insights-Ereignisse sammelt. Der Wert für `eventCategory` muss `Insight` sein. *retention-period-days* Ersetzen Sie es durch die Anzahl der Tage, an denen Sie Ereignisse in Ihrem Ereignisdatenspeicher speichern möchten. Gültige Werte sind Ganzzahlen zwischen 7 und 3 653, wenn der `--billing-mode` `EXTENDABLE_RETENTION_PRICING` ist, oder zwischen 7 und 2 557, wenn der `--billing-mode` auf `FIXED_RETENTION_PRICING` gesetzt ist. Wenn Sie keine Angabe machen `--retention-period`, CloudTrail verwendet die Standardaufbewahrungsdauer für `--billing-mode`.

Wenn Sie mit dem Verwaltungskonto einer AWS Organizations Organisation angemeldet sind, geben Sie den `--organization-enabled` Parameter an, wenn Sie Ihrem [delegierten Administrator](#) Zugriff auf den Ereignisdatenspeicher gewähren möchten.

```
aws cloudtrail create-event-data-store \  
--name insights-event-data-store \  
--no-multi-region-enabled \  
--retention-period retention-period-days \  
--advanced-event-selectors '[  
  {  
    "Name": "Select Insights events",  
    "FieldSelectors": [  
      { "Field": "eventCategory", "Equals": ["Insight"] }  
    ]  
  }  
]'
```

Nachfolgend finden Sie eine Beispielantwort.

```
{
  "Name": "insights-event-data-store",
  "ARN": "arn:aws:cloudtrail:us-east-1:111122223333:eventdatastore/
EXAMPLEf852-4e8f-8bd1-bcf6cEXAMPLE",
  "AdvancedEventSelectors": [
    {
      "Name": "Select Insights events",
      "FieldSelectors": [
        {
          "Field": "eventCategory",
          "Equals": [
            "Insight"
          ]
        }
      ]
    }
  ],
  "MultiRegionEnabled": false,
  "OrganizationEnabled": false,
  "BillingMode": "EXTENDABLE_RETENTION_PRICING",
  "RetentionPeriod": "90",
  "TerminationProtectionEnabled": true,
  "CreatedTimestamp": "2023-05-08T15:22:33.578000+00:00",
  "UpdatedTimestamp": "2023-05-08T15:22:33.714000+00:00"
}
```

Sie verwenden die ARN (oder das ID-Suffix des ARN) aus der Antwort als Wert für den Parameter `--insights-destination` in Schritt 3.

- Um einen Quellereignisdatenspeicher zu erstellen, der Verwaltungsereignisse protokolliert, führen Sie den Befehl [aws cloudtrail create-event-data-store](#) aus. Standardmäßig protokollieren Ereignisdatenquellen alle Verwaltungsereignisse. Sie müssen keine erweiterten Ereignisselectoren angeben, um alle Verwaltungsereignisse zu protokollieren. *retention-period-days* Ersetzen Sie ihn durch die Anzahl der Tage, an denen Sie Ereignisse in Ihrem Ereignisdatenspeicher speichern möchten. Gültige Werte sind Ganzzahlen zwischen 7 und 3 653, wenn der `--billing-mode` `EXTENDABLE_RETENTION_PRICING` ist, oder zwischen 7 und 2 557, wenn der `--billing-mode` auf `FIXED_RETENTION_PRICING` gesetzt ist. Wenn Sie keine Angabe machen `--retention-period`, CloudTrail verwendet die Standardaufbewahrungsdauer für `--billing-mode`. Wenn Sie einen Datenspeicher für Organisationsereignisse erstellen, fügen Sie den Parameter `--organization-enabled` hinzu.

```
aws cloudtrail create-event-data-store --name source-event-data-store --retention-period retention-period-days
```

Nachfolgend finden Sie eine Beispielantwort.

```
{
  "EventDataStoreArn": "arn:aws:cloudtrail:us-east-1:111122223333:eventdatastore/EXAMPLE9952-4ab9-49c0-b788-f4f3EXAMPLE",
  "Name": "source-event-data-store",
  "Status": "CREATED",
  "AdvancedEventSelectors": [
    {
      "Name": "Default management events",
      "FieldSelectors": [
        {
          "Field": "eventCategory",
          "Equals": [
            "Management"
          ]
        }
      ]
    }
  ],
  "MultiRegionEnabled": true,
  "OrganizationEnabled": false,
  "BillingMode": "EXTENDABLE_RETENTION_PRICING",
  "RetentionPeriod": 90,
  "TerminationProtectionEnabled": true,
  "CreatedTimestamp": "2023-05-08T15:25:35.578000+00:00",
  "UpdatedTimestamp": "2023-05-08T15:25:35.714000+00:00"
}
```

Sie verwenden die ARN (oder das ID-Suffix des ARN) aus der Antwort als Wert für den Parameter `--event-data-store` in Schritt 3.

3. Führen Sie den Befehl [put-insight-selectors](#) aus, um Insights-Ereignisse zu aktivieren. Insights-Selektorergebnisse können `ApiCallRateInsight` und/oder `ApiErrorRateInsight` sein. Geben Sie für den Parameter `--event-data-store` den ARN (oder das ID-Suffix der ARN) des Quellereignisdatenspeichers an, der Verwaltungsereignisse protokolliert und Insights aktiviert. Geben Sie für den Parameter `--insights-destination` den ARN (oder das ID-Suffix des ARN) des Zielereignisdatenspeichers an, der Insights-Ereignisse protokolliert.

```
aws cloudtrail put-insight-selectors --event-data-store arn:aws:cloudtrail:us-east-1:111122223333:eventdatastore/EXAMPLE9952-4ab9-49c0-b788-f4f3EXAMPLE --insights-destination arn:aws:cloudtrail:us-east-1:111122223333:eventdatastore/EXAMPLEf852-4e8f-8bd1-bcf6cEXAMPLE --insight-selectors '[{"InsightType": "ApiCallRateInsight"}, {"InsightType": "ApiErrorRateInsight"}]'
```

Das folgende Ergebnis zeigt den Insights-Ereignisselektor, der für den Ereignisdatenspeicher konfiguriert wurde.

```
{
  "EventDataStoreARN": "arn:aws:cloudtrail:us-east-1:111122223333:eventdatastore/EXAMPLE9952-4ab9-49c0-b788-f4f3EXAMPLE",
  "InsightsDestination": "arn:aws:cloudtrail:us-east-1:111122223333:eventdatastore/EXAMPLEf852-4e8f-8bd1-bcf6cEXAMPLE",
  "InsightSelectors":
    [
      {
        "InsightType": "ApiErrorRateInsight"
      },
      {
        "InsightType": "ApiCallRateInsight"
      }
    ]
}
```

Nachdem Sie CloudTrail Insights zum ersten Mal in einem Ereignisdatenspeicher aktiviert haben, kann es bis zu 7 Tage dauern, CloudTrail bis das erste Insights-Ereignis übermittelt wird, wenn ungewöhnliche Aktivitäten festgestellt werden.

CloudTrail Insights analysiert Verwaltungsereignisse, die in einer einzelnen Region und nicht global auftreten. Ein CloudTrail Insights-Ereignis wird in derselben Region generiert, in der auch die zugehörigen Managementereignisse generiert werden.

CloudTrail analysiert bei einem Datenspeicher für Organisationsereignisse Verwaltungsereignisse aus den Konten der einzelnen Mitglieder, anstatt die Aggregation aller Verwaltungsereignisse für die Organisation zu analysieren.

Für die Aufnahme von Insights-Veranstaltungen in Lake fallen zusätzliche Gebühren an CloudTrail . Wenn Sie Insights sowohl für Trails als auch für Ereignisdatenspeicher aktivieren, wird Ihnen eine



separate Gebühr in Rechnung gestellt. Informationen zur CloudTrail Preisgestaltung finden Sie unter [AWS CloudTrail Preise](#).

## Importieren Sie Trail-Ereignisse in einen Event-Datenspeicher mit dem AWS CLI

In der AWS CLI können Sie Trail-Ereignisse in einen Ereignisdatenspeicher importieren. Das Verfahren in diesem Abschnitt zeigt, wie Sie einen Ereignisdatenspeicher erstellen und konfigurieren, indem Sie den Befehl [create-event-data-store](#) ausführen und dann die Ereignisse mithilfe des Befehls [start-import](#) in diesen Ereignisdatenspeicher importieren. Weitere Informationen zum Importieren von Trail-Ereignissen, einschließlich Informationen zu Überlegungen und erforderlichen Berechtigungen, finden Sie unter [Kopieren von Trail-Ereignissen in einen Ereignisdatenspeicher](#).

### Vorbereiten des Imports von Trail-Ereignissen

Treffen Sie die folgenden Vorbereitungen, bevor Sie Trail-Ereignisse importieren.

- Stellen Sie sicher, dass Sie über eine Rolle mit den [erforderlichen Berechtigungen](#) zum Importieren von Trail-Ereignissen in einen Ereignisdatenspeicher verfügen.
- Ermitteln Sie den [--billing-mode](#)-Wert, den Sie für den Ereignisdatenspeicher angeben möchten. Der `--billing-mode` bestimmt die Kosten für die Erfassung und Speicherung von Ereignissen sowie die standardmäßige und maximale Aufbewahrungsdauer für den Ereignisdatenspeicher.

Wenn Sie Trail-Ereignisse nach CloudTrail Lake importieren, werden die im komprimierten CloudTrail GZIP-Format gespeicherten Protokolle entpackt. CloudTrail kopiert dann die in den Protokollen enthaltenen Ereignisse in Ihren Ereignisdatenspeicher. Die Größe der unkomprimierten Daten könnte größer sein als die tatsächliche Amazon-S3-Speichergöße. Um eine allgemeine Schätzung der Größe der unkomprimierten Daten zu erhalten, multiplizieren Sie die Größe der Protokolle im S3-Bucket mit 10. Sie können diese Schätzung verwenden, um den `--billing-mode`-Wert für Ihren Anwendungsfall auszuwählen.

- Ermitteln Sie den Wert, den Sie für den `--retention-period` angeben möchten. CloudTrail kopiert ein Ereignis nicht, wenn `eventTime` es älter als die angegebene Aufbewahrungsfrist ist.

Um die geeignete Aufbewahrungsdauer zu ermitteln, nehmen Sie die Summe aus dem ältesten Ereignis, das Sie kopieren möchten, in Tagen und der Anzahl der Tage, an denen Sie die Ereignisse im Ereignisdatenspeicher aufbewahren möchten, wie in der folgenden Gleichung dargestellt:

Aufbewahrungszeitraum = *oldest-event-in-days* + *number-days-to-retain*

Wenn das älteste Ereignis, das Sie kopieren, beispielsweise 45 Tage alt ist und Sie die Ereignisse weitere 45 Tage im Ereignisdatenspeicher aufbewahren möchten, würden Sie die Aufbewahrungsdauer auf 90 Tage festlegen.

- Entscheiden Sie, ob Sie den Ereignisdatenspeicher verwenden möchten, um zukünftige Ereignisse zu analysieren. Wenn Sie keine zukünftigen Ereignisse aufnehmen möchten, fügen Sie den Parameter `--no-start-ingestion` bei der Erstellung des Ereignisdatenspeichers hinzu. Standardmäßig beginnen Ereignisdatenspeicher mit der Erfassung von Ereignissen, wenn sie erstellt werden.

## Erstellen eines Ereignisdatenspeichers und Importieren von Trail-Ereignissen in diesen Ereignisdatenspeicher

1. Führen Sie den Befehl `create-event-data-store` aus, um den neuen Ereignisdatenspeicher zu erstellen. In diesem Beispiel ist `--retention-period` auf 120 gesetzt, weil das älteste kopierte Ereignis 90 Tage alt ist und wir die Ereignisse 30 Tage lang beibehalten möchten. Der Parameter `--no-start-ingestion` ist gesetzt, weil wir keine zukünftigen Ereignisse erfassen möchten. In diesem Beispiel wurde `--billing-mode` nicht gesetzt, da wir den Standardwert `EXTENDABLE_RETENTION_PRICING` verwenden, weil wir davon ausgehen, dass weniger als 25 TB an Ereignisdaten erfasst werden.

### Note

Wenn Sie den Ereignisdatenspeicher erstellen, der Ihren Trail ersetzen soll, empfehlen wir, die `--advanced-event-selectors` so zu konfigurieren, dass sie den Ereignisselektoren Ihres Trails entsprechen, um sicherzustellen, dass Sie die gleiche Ereignisabdeckung haben. Standardmäßig protokollieren Ereignisdatenquellen alle Verwaltungsereignisse.

```
aws cloudtrail create-event-data-store --name import-trail-eds --retention-period
120 --no-start-ingestion
```

Nachfolgend finden Sie eine Beispielantwort:

```
{
```

```

    "EventDataStoreArn": "arn:aws:cloudtrail:us-east-1:123456789012:eventdatastore/
EXAMPLEa-4357-45cd-bce5-17ec652719d9",
    "Name": "import-trail-eds",
    "Status": "CREATED",
    "AdvancedEventSelectors": [
      {
        "Name": "Default management events",
        "FieldSelectors": [
          {
            "Field": "eventCategory",
            "Equals": [
              "Management"
            ]
          }
        ]
      }
    ],
    "MultiRegionEnabled": true,
    "OrganizationEnabled": false,
    "BillingMode": "EXTENDABLE_RETENTION_PRICING",
    "RetentionPeriod": 120,
    "TerminationProtectionEnabled": true,
    "CreatedTimestamp": "2023-11-09T16:52:25.444000+00:00",
    "UpdatedTimestamp": "2023-11-09T16:52:25.569000+00:00"
  }
}

```

Der Status ist zunächst CREATED, deshalb führen wir den Befehl `get-event-data-store` aus, um sicherzustellen, dass die Erfassung gestoppt ist.

```
aws cloudtrail get-event-data-store --event-data-store eds-id
```

Die Antwort zeigt, dass der Status jetzt STOPPED\_INGESTION ist, was darauf hindeutet, dass der Ereignisdatenspeicher keine Live-Ereignisse erfasst.

```

{
  "EventDataStoreArn": "arn:aws:cloudtrail:us-east-1:123456789012:eventdatastore/
EXAMPLEa-4357-45cd-bce5-17ec652719d9",
  "Name": "import-trail-eds",
  "Status": "STOPPED_INGESTION",
  "AdvancedEventSelectors": [
    {
      "Name": "Default management events",

```

```

        "FieldSelectors": [
            {
                "Field": "eventCategory",
                "Equals": [
                    "Management"
                ]
            }
        ]
    },
    "MultiRegionEnabled": true,
    "OrganizationEnabled": false,
    "BillingMode": "EXTENDABLE_RETENTION_PRICING",
    "RetentionPeriod": 120,
    "TerminationProtectionEnabled": true,
    "CreatedTimestamp": "2023-11-09T16:52:25.444000+00:00",
    "UpdatedTimestamp": "2023-11-09T16:52:25.569000+00:00"
}

```

2. Führen Sie den Befehl `start-import` aus, um die Trail-Ereignisse in den Ereignisdatenspeicher zu importieren, der in Schritt 1 erstellt wurde. Geben Sie den ARN (oder das ID-Suffix des ARN) des Ereignisdatenspeichers als Wert für den Parameter `--destinations` an. Für `--start-event-time` geben Sie die `eventTime` für das älteste Ereignis an, das Sie kopieren möchten, und für `--end-event-time` geben Sie die `eventTime` des neuesten Ereignisses an, das Sie kopieren möchten. `--import-source` Geben Sie den S3-URI für den S3-Bucket an, der Ihre Trail-Logs enthält, den AWS-Region für den S3-Bucket und den ARN der Rolle, die für den Import von Trail-Ereignissen verwendet wird.

```

aws cloudtrail start-import \
--destinations ["arn:aws:cloudtrail:us-east-1:123456789012:eventdatastore/
EXAMPLEa-4357-45cd-bce5-17ec652719d9"] \
--start-event-time 2023-08-11T16:08:12.934000+00:00 \
--end-event-time 2023-11-09T17:08:20.705000+00:00 \
--import-source {"S3": {"S3LocationUri": "s3://aws-cloudtrail-
logs-123456789012-612ff1f6/AWSLogs/123456789012/CloudTrail/", "S3BucketRegion": "us-
east-1", "S3BucketAccessRoleArn": "arn:aws:iam::123456789012:role/service-role/
CloudTrailLake-us-east-1-copy-events-eds"}}

```

Nachfolgend finden Sie eine Beispielantwort.

```
{
  "CreatedTimestamp": "2023-11-09T17:08:20.705000+00:00",
  "Destinations": [
    "arn:aws:cloudtrail:us-east-1:123456789012:eventdatastore/
EXAMPLEEa-4357-45cd-bce5-17ec652719d9"
  ],
  "EndEventTime": "2023-11-09T17:08:20.705000+00:00",
  "ImportId": "EXAMPLEe-7be2-4658-9204-b38c3257fcd1",
  "ImportSource": {
    "S3": {
      "S3BucketAccessRoleArn": "arn:aws:iam::123456789012:role/service-role/
CloudTrailLake-us-east-1-copy-events-eds",
      "S3BucketRegion": "us-east-1",
      "S3LocationUri": "s3://aws-cloudtrail-logs-123456789012-111ff1f6/
AWSLogs/123456789012/CloudTrail/"
    }
  },
  "ImportStatus": "INITIALIZING",
  "StartEventTime": "2023-08-11T16:08:12.934000+00:00",
  "UpdatedTimestamp": "2023-11-09T17:08:20.806000+00:00"
}
```

3. Führen Sie den Befehl [get-import](#) aus, um Informationen zum Import abzurufen.

```
aws cloudtrail get-import --import-id import-id
```

Nachfolgend finden Sie eine Beispielantwort.

```
{
  "ImportId": "EXAMPLEe-7be2-4658-9204-b38c3EXAMPLE",
  "Destinations": [
    "arn:aws:cloudtrail:us-east-1:123456789012:eventdatastore/
EXAMPLEEa-4357-45cd-bce5-17ec652719d9"
  ],
  "ImportSource": {
    "S3": {
      "S3LocationUri": "s3://aws-cloudtrail-logs-123456789012-111ff1f6/
AWSLogs/123456789012/CloudTrail/",
      "S3BucketRegion": "us-east-1",
      "S3BucketAccessRoleArn": "arn:aws:iam::123456789012:role/service-role/
CloudTrailLake-us-east-1-copy-events-eds"
    }
  }
}
```

```
  },
  "StartEventTime": "2023-08-11T16:08:12.934000+00:00",
  "EndEventTime": "2023-11-09T17:08:20.705000+00:00",
  "ImportStatus": "COMPLETED",
  "CreatedTimestamp": "2023-11-09T17:08:20.705000+00:00",
  "ImportStatistics": {
    "PrefixesFound": 1548,
    "PrefixesCompleted": 1548,
    "FilesCompleted": 92845,
    "EventsCompleted": 577249,
    "FailedEntries": 0
  }
}
```

Ein Import endet mit einem `ImportStatus` `COMPLETED`, wenn es keine Fehler gab, oder `FAILED`, wenn es Fehler gab.

Wenn beim Import ein `FailedEntries` aufgetreten ist, können Sie den Befehl [list-import-failures](#) ausführen, um eine Liste der Fehler zurückzugeben.

```
aws cloudtrail list-import-failures --import-id import-id
```

Um einen fehlgeschlagenen Import erneut zu versuchen, führen Sie den Befehl `start-import` nur mit dem Parameter `--import-id` aus. Wenn Sie einen Import erneut versuchen, CloudTrail setzt er den Import an der Stelle fort, an der der Fehler aufgetreten ist.

```
aws cloudtrail start-import --import-id import-id
```

## Rufen Sie einen Ereignisdatenspeicher mit dem AWS CLI

Der folgende AWS CLI `get-event-data-store` Beispielbefehl gibt Informationen über den durch den erforderlichen `--event-data-store` Parameter angegebenen Ereignisdatenspeicher zurück, der einen ARN oder das ID-Suffix des ARN akzeptiert.

```
aws cloudtrail get-event-data-store
--event-data-store arn:aws:cloudtrail:us-east-1:123456789012:eventdatastore/EXAMPLE-
f852-4e8f-8bd1-bcf6cEXAMPLE
```

Nachfolgend finden Sie eine Beispielantwort. Die Erstellung und die letzten aktualisierten Zeiten sind im timestamp-Format.

```
{
  "EventDataStoreARN": "arn:aws:cloudtrail:us-east-1:123456789012:eventdatastore/
EXAMPLE-f852-4e8f-8bd1-bcf6cEXAMPLE",
  "Name": "s3-data-events-eds",
  "Status": "ENABLED",
  "AdvancedEventSelectors": [
    {
      "Name": "Log DeleteObject API calls for a specific S3 bucket",
      "FieldSelectors": [
        {
          "Field": "eventCategory",
          "Equals": [
            "Data"
          ]
        },
        {
          "Field": "eventName",
          "Equals": [
            "DeleteObject"
          ]
        },
        {
          "Field": "resources.ARN",
          "StartsWith": [
            "arn:aws:s3:::bucketName"
          ]
        },
        {
          "Field": "readOnly",
          "Equals": [
            "false"
          ]
        },
        {
          "Field": "resources.type",
          "Equals": [
            "AWS::S3::Object"
          ]
        }
      ]
    }
  ]
}
```

```
    }
  ],
  "MultiRegionEnabled": true,
  "OrganizationEnabled": false,
  "BillingMode": "FIXED_RETENTION_PRICING",
  "RetentionPeriod": 2557,
  "TerminationProtectionEnabled": true,
  "CreatedTimestamp": "2023-11-09T22:20:36.344000+00:00",
  "UpdatedTimestamp": "2023-11-09T22:20:36.476000+00:00"
}
```

## Listet alle Ereignisdatenspeicher in einem Konto auf mit AWS CLI

Der folgende AWS CLI `list-event-data-stores` Beispielbefehl gibt Informationen über alle Ereignisdatenspeicher in einem Konto in der aktuellen Region zurück. Optionale Parameter umfassen `--max-results`, um eine maximale Anzahl von Ergebnissen anzugeben, die der Befehl auf einer einzelnen Seite zurückgeben soll. Wenn es mehr Ergebnisse als den von Ihnen angegebenen `--max-results`-Wert gibt, führen Sie den Befehl `NextToken` erneut aus und fügen den zurückgegebenen Wert hinzu, um die nächste Seite mit Ergebnissen zu erhalten.

```
aws cloudtrail list-event-data-stores
```

Nachfolgend finden Sie eine Beispielantwort.

```
{
  "EventDataStores": [
    {
      "EventDataStoreArn": "arn:aws:cloudtrail:us-
east-1:123456789012:eventdatastore/EXAMPLE7-cad6-4357-a84b-318f9868e969",
      "Name": "management-events-eds"
    },
    {
      "EventDataStoreArn": "arn:aws:cloudtrail:us-
east-1:123456789012:eventdatastore/EXAMPLE6-88e1-43b7-b066-9c046b4fd47a",
      "Name": "config-items-eds"
    },
    {
      "EventDataStoreArn": "arn:aws:cloudtrail:us-
east-1:123456789012:eventdatastore/EXAMPLEf-b314-4c85-964e-3e43b1e8c3b4",
      "Name": "s3-data-events"
    }
  ]
}
```



```
}
```

## Aktualisieren Sie einen Ereignisdatenspeicher mit dem AWS CLI

Die folgenden Beispiele veranschaulichen, wie Sie einen Ereignisdatenspeicher aktualisieren.

### Themen

- [Aktualisieren Sie den Abrechnungsmodus mit dem AWS CLI](#)
- [Aktualisieren Sie den Aufbewahrungsmodus, aktivieren Sie den Kündigungsschutz und geben Sie a AWS KMS key mit AWS CLI](#)
- [Deaktivieren Sie den Kündigungsschutz mit dem AWS CLI](#)

### Aktualisieren Sie den Abrechnungsmodus mit dem AWS CLI

Der `--billing-mode` für den Ereignisdatenspeicher bestimmt die Kosten für die Erfassung und Speicherung von Ereignissen sowie die standardmäßige und maximale Aufbewahrungsdauer für den Ereignisdatenspeicher. Wenn der `--billing-mode` eines Ereignisdatenspeichers auf `FIXED_RETENTION_PRICING` eingestellt ist, können Sie den Wert auf `EXTENDABLE_RETENTION_PRICING` ändern. `EXTENDABLE_RETENTION_PRICING` wird generell empfohlen, wenn Ihr Ereignisdatenspeicher weniger als 25 TB an Ereignisdaten pro Monat erfasst und Sie einen flexiblen Aufbewahrungszeitraum von bis zu 3653 Tagen wünschen. Informationen zu Preisen erhalten Sie unter [AWS CloudTrail -Preise](#) und [Verwaltung der CloudTrail Seekosten](#).

#### Note

Sie können den Wert für `--billing-mode` von `EXTENDABLE_RETENTION_PRICING` nicht in `FIXED_RETENTION_PRICING` ändern. Wenn der Abrechnungsmodus des Ereignisdatenspeichers auf `EXTENDABLE_RETENTION_PRICING` eingestellt ist und Sie stattdessen `FIXED_RETENTION_PRICING` verwenden möchten, können Sie die [Aufnahme im Ereignisdatenspeicher beenden](#) und einen neuen Ereignisdatenspeicher erstellen, der `FIXED_RETENTION_PRICING` verwendet.

Der folgende AWS CLI `update-event-data-store` Beispielbefehl ändert den Wert `--billing-mode` für den Ereignisdatenspeicher von `FIXED_RETENTION_PRICING` auf `EXTENDABLE_RETENTION_PRICING`. Der erforderliche `--event-data-store`-Parameterwert ist ein ARN (oder das ID-Suffix des ARN) und ist erforderlich; andere Parameter sind optional.

```
aws cloudtrail update-event-data-store \  
--region us-east-1 \  
--event-data-store arn:aws:cloudtrail:us-east-1:123456789012:eventdatastore/EXAMPLE-  
f852-4e8f-8bd1-bcf6cEXAMPLE \  
--billing-mode EXTENDABLE_RETENTION_PRICING
```

Nachfolgend finden Sie eine Beispielantwort.

```
{  
  "EventDataStoreArn": "event-data-store arn:aws:cloudtrail:us-  
east-1:123456789012:eventdatastore/EXAMPLE-f852-4e8f-8bd1-bcf6cEXAMPLE",  
  "Name": "management-events-eds",  
  "Status": "ENABLED",  
  "AdvancedEventSelectors": [  
    {  
      "Name": "Default management events",  
      "FieldSelectors": [  
        {  
          "Field": "eventCategory",  
          "Equals": [  
            "Management"  
          ]  
        }  
      ]  
    }  
  ],  
  "MultiRegionEnabled": true,  
  "OrganizationEnabled": false,  
  "BillingMode": "EXTENDABLE_RETENTION_PRICING",  
  "RetentionPeriod": 2557,  
  "TerminationProtectionEnabled": true,  
  "CreatedTimestamp": "2023-10-27T10:55:55.384000-04:00",  
  "UpdatedTimestamp": "2023-10-27T10:57:05.549000-04:00"  
}
```

Aktualisieren Sie den Aufbewahrungsmodus, aktivieren Sie den Kündigungsschutz und geben Sie a AWS KMS key mit AWS CLI

Der folgende AWS CLI update-event-data-store Beispielbefehl aktualisiert einen Ereignisdatenspeicher, um dessen Aufbewahrungsdauer auf 100 Tage zu ändern und den Kündigungsschutz zu aktivieren. Der erforderliche --event-data-store-Parameterwert ist ein ARN (oder das ID-Suffix des ARN) und ist erforderlich; andere Parameter sind optional. In diesem

Beispiel wird der Parameter `--retention-period` hinzugefügt, um den Aufbewahrungszeitraum auf 100 Tage zu ändern. Optional können Sie die AWS Key Management Service Verschlüsselung aktivieren und eine angeben, AWS KMS key indem Sie dem Befehl etwas `--kms-key-id` hinzufügen und einen KMS-Schlüssel-ARN als Wert angeben. `--termination-protection-enabled` wird hinzugefügt, um den Kündigungsschutz für einen Ereignisdatenspeicher zu aktivieren, für den der Terminierungsschutz nicht aktiviert war.

Ein Ereignisdatenspeicher, der Ereignisse von außen protokolliert, AWS kann nicht so aktualisiert werden, dass er AWS Ereignisse protokolliert. Ebenso kann ein Ereignisdatenspeicher, der AWS Ereignisse protokolliert, nicht so aktualisiert werden, dass er Ereignisse von außen protokolliert AWS.

### Note

Wenn Sie die Aufbewahrungsdauer eines Ereignisdatenspeichers verringern, CloudTrail werden alle Ereignisse entfernt, deren Aufbewahrungszeitraum `eventTime` älter als der neue ist. Wenn der vorherige Aufbewahrungszeitraum beispielsweise 365 Tage betrug und Sie ihn auf 100 Tage reduzieren, CloudTrail werden Ereignisse entfernt, deren Aufbewahrungszeitraum `eventTime` älter als 100 Tage ist.

```
aws cloudtrail update-event-data-store \
--event-data-store arn:aws:cloudtrail:us-east-1:123456789012:eventdatastore/EXAMPLE-
f852-4e8f-8bd1-bcf6cEXAMPLE \
--retention-period 100 \
--kms-key-id "arn:aws:kms:us-east-1:0123456789:alias/KMS_key_alias" \
--termination-protection-enabled
```

Nachfolgend finden Sie eine Beispielantwort.

```
{
  "EventDataStoreArn": "arn:aws:cloudtrail:us-east-1:123456789012:eventdatastore/
EXAMPLE-ee54-4813-92d5-999aeEXAMPLE",
  "Name": "my-event-data-store",
  "Status": "ENABLED",
  "AdvancedEventSelectors": [
    {
      "Name": "Select all S3 data events",
      "FieldSelectors": [
        {
          "Field": "eventCategory",
```

```
        "Equals": [
            "Data"
        ]
    },
    {
        "Field": "resources.type",
        "Equals": [
            "AWS::S3::Object"
        ]
    },
    {
        "Field": "resources.ARN",
        "StartsWith": [
            "arn:aws:s3"
        ]
    }
]
}
],
"MultiRegionEnabled": true,
"OrganizationEnabled": false,
"BillingMode": "EXTENDABLE_RETENTION_PRICING",
"RetentionPeriod": 100,
"KmsKeyId": "arn:aws:kms:us-east-1:0123456789:alias/KMS_key_alias",
"TerminationProtectionEnabled": true,
"CreatedTimestamp": "2023-10-27T10:55:55.384000-04:00",
"UpdatedTimestamp": "2023-10-27T10:57:05.549000-04:00"
}
```

## Deaktivieren Sie den Kündigungsschutz mit dem AWS CLI

Standardmäßig ist der Beendigungsschutz für einen Ereignisdatenspeicher aktiviert, um den Ereignisdatenspeicher vor versehentlicher Löschung zu schützen. Sie können einen Ereignisdatenspeicher nicht löschen, wenn der Beendigungsschutz aktiviert ist. Wenn Sie den Ereignisdatenspeicher löschen möchten, müssen Sie zuerst den Beendigungsschutz deaktivieren.

Der folgende AWS CLI `update-event-data-store` Beispielbefehl deaktiviert den Kündigungsschutz, indem der `--no-termination-protection-enabled` Parameter übergeben wird.

```
aws cloudtrail update-event-data-store \
--region us-east-1 \
--no-termination-protection-enabled \
```

```
--event-data-store arn:aws:cloudtrail:us-east-1:123456789012:eventdatastore/EXAMPLE-f852-4e8f-8bd1-bcf6cEXAMPLE
```

Nachfolgend finden Sie eine Beispielantwort.

```
{
  "EventDataStoreArn": "arn:aws:cloudtrail:us-east-1:123456789012:eventdatastore/EXAMPLE-f852-4e8f-8bd1-bcf6cEXAMPLE",
  "Name": "management-events-eds",
  "Status": "ENABLED",
  "AdvancedEventSelectors": [
    {
      "Name": "Default management events",
      "FieldSelectors": [
        {
          "Field": "eventCategory",
          "Equals": [
            "Management"
          ]
        }
      ]
    }
  ],
  "MultiRegionEnabled": true,
  "OrganizationEnabled": false,
  "BillingMode": "EXTENDABLE_RETENTION_PRICING",
  "RetentionPeriod": 366,
  "TerminationProtectionEnabled": false,
  "CreatedTimestamp": "2023-10-27T10:55:55.384000-04:00",
  "UpdatedTimestamp": "2023-10-27T10:57:05.549000-04:00"
}
```

## Stoppen Sie die Aufnahme in einen Ereignisdatenspeicher mit dem AWS CLI

Mit dem folgenden AWS CLI `stop-event-data-store-ingestion` Beispielbefehl wird verhindert, dass ein Ereignisdatenspeicher Ereignisse aufnimmt. Um die Aufnahme zu beenden, muss der Status-Ereignisdatenspeicher `ENABLED` sein und `eventCategory` muss `Management`, `Data` oder `ConfigurationItem` sein. Der Ereignisdatenspeicher wird durch `--event-data-store` angegeben, der einen Ereignisdatenspeicher-ARN oder das ID-Suffix des ARN akzeptiert. Nach der Ausführung von `stop-event-data-store-ingestion` ändert sich der Status des Ereignisdatenspeichers zu `STOPPED_INGESTION`.

Der Ereignisdatenspeicher wird auf die maximale Anzahl von zehn Ereignisdatenspeichern in Ihrem Konto angerechnet, wenn dessen Status STOPPED\_INGESTION ist.

```
aws cloudtrail stop-event-data-store-ingestion
--event-data-store arn:aws:cloudtrail:us-east-1:123456789012:eventdatastore/EXAMPLE-
f852-4e8f-8bd1-bcf6cEXAMPLE
```

Wenn der Befehl erfolgreich ausgeführt wird, erfolgt keine Reaktion.

## Starten Sie die Aufnahme in einen Ereignisdatenspeicher mit dem AWS CLI

Der folgende AWS CLI start-event-data-store-ingestion Beispielbefehl startet die Ereignisaufnahme in einem Ereignisdatenspeicher. Um die Aufnahme zu starten, muss der Status-Ereignisdatenspeicher STOPPED\_INGESTION sein und eventCategory muss Management, Data oder ConfigurationItem sein. Der Ereignisdatenspeicher wird durch --event-data-store angegeben, der einen Ereignisdatenspeicher-ARN oder das ID-Suffix des ARN akzeptiert. Nach der Ausführung von start-event-data-store-ingestion ändert sich der Status des Ereignisdatenspeichers zu ENABLED.

```
aws cloudtrail start-event-data-store-ingestion --event-data-store
arn:aws:cloudtrail:us-east-1:123456789012:eventdatastore/EXAMPLE-f852-4e8f-8bd1-
bcf6cEXAMPLE
```

Wenn der Befehl erfolgreich ausgeführt wird, erfolgt keine Reaktion.

## Aktivieren eines Verbunds zu einem Ereignisdatenspeicher

Um den Verbund zu aktivieren, führen Sie den Befehl aws cloudtrail enable-federation aus und geben Sie die erforderlichen Parameter --event-data-store und --role ein. Geben Sie für --event-data-store den ARN des Ereignisdatenspeichers (oder das ID-Suffix des ARN) an. Geben Sie für --role den ARN für Ihre Verbundrolle an. Die Rolle muss in Ihrem Konto vorhanden sein und über die [erforderlichen Mindestberechtigungen verfügen](#).

```
aws cloudtrail enable-federation
--event-data-store arn:aws:cloudtrail:region:account-id:eventdatastore/eds-id
--role arn:aws:iam::account-id:role/federation-role-name
```

Dieses Beispiel zeigt, wie ein delegierter Administrator den Verbund für den Ereignisdatenspeicher einer Organisation aktivieren kann, indem er den ARN des Ereignisdatenspeichers im Verwaltungskonto und den ARN der Verbundrolle im delegierten Administratorkonto angibt.

```
aws cloudtrail enable-federation
--event-data-store arn:aws:cloudtrail:region:management-account-id:eventdatastore/eds-id
--role arn:aws:iam::delegated-administrator-account-id:role/federation-role-name
```

## Deaktivieren eines Verbunds zu einem Ereignisdatenspeicher

Führen Sie den Befehl `aws cloudtrail disable-federation` aus, um den Verbund im Ereignisdatenspeicher zu deaktivieren. Der Ereignisdatenspeicher wird durch `--event-data-store` angegeben, der einen Ereignisdatenspeicher-ARN oder das ID-Suffix des ARN akzeptiert.

```
aws cloudtrail disable-federation
--event-data-store arn:aws:cloudtrail:region:account-id:eventdatastore/eds-id
```

### Note

Wenn es sich um den Ereignisdatenspeicher einer Organisation handelt, geben Sie die Konto-ID für das Verwaltungskonto an.

## Löschen Sie einen Ereignisdatenspeicher mit dem AWS CLI

Der folgende AWS CLI `delete-event-data-store`-Beispielbefehl deaktiviert den durch `--event-data-store` angegebenen Ereignisdatenspeicher, der einen Ereignisdatenspeicher-ARN oder das ID-Suffix des ARN annimmt. Nachdem Sie `delete-event-data-store` ausgeführt haben, ist der endgültige Status des Ereignisdatenspeichers `PENDING_DELETION`, und der Ereignisdatenspeicher wird nach einer Wartezeit von 7 Tagen automatisch gelöscht.

Nachdem Sie `delete-event-data-store` auf einem Ereignisdatenspeicher ausgeführt haben, können Sie weder `list-queries`, `describe-query` noch `get-query-results` auf Abfragen ausführen, die den deaktivierten Datenspeicher verwenden. Der Ereignisdatenspeicher wird auf die maximale Anzahl von zehn Ereignisdatenspeichern in Ihrem Konto angerechnet, wenn er zur Löschung ansteht.

### Note

Sie können einen Ereignisdatenspeicher nicht löschen, wenn `--termination-protection-enabled` festgelegt ist oder sein `FederationStatus` `ENABLED` lautet.

```
aws cloudtrail delete-event-data-store
--event-data-store arn:aws:cloudtrail:us-east-1:123456789012:eventdatastore/EXAMPLE-
f852-4e8f-8bd1-bcf6cEXAMPLE
```

Wenn der Befehl erfolgreich ausgeführt wird, erfolgt keine Reaktion.

## Stellen Sie einen Ereignisdatenspeicher wieder her mit dem AWS CLI

Der folgende AWS CLI `restore-event-data-store`-Beispielbefehl stellt einen Ereignisdatenspeicher wieder her, der zum Löschen ansteht. Der Ereignisdatenspeicher wird durch `--event-data-store` angegeben, der einen Ereignisdatenspeicher-ARN oder das ID-Suffix des ARN akzeptiert. Sie können einen gelöschten Ereignisdatenspeicher nur innerhalb der siebentägigen Wartezeit nach dem Löschen wiederherstellen.

```
aws cloudtrail restore-event-data-store
--event-data-store EXAMPLE-f852-4e8f-8bd1-bcf6cEXAMPLE
```

Die Antwort enthält Informationen über den Ereignisdatenspeicher, einschließlich des ARN, der erweiterten Ereigniselektoren und des Status der Wiederherstellung.

## Verwalten der Lebenszyklen von Ereignisdatenspeichern

Im Folgenden sind die Lebenszyklusphasen eines Ereignisdatenspeichers aufgeführt.

- **CREATED** – Ein kurzfristiger Status, der angibt, dass der Ereignisdatenspeicher erstellt wurde.
- **ENABLED**: Der Ereignisdatenspeicher ist aktiv und nimmt Ereignisse auf. Sie können Abfragen ausführen und Trail-Ereignisse in den Ereignisdatenspeicher kopieren.
- **STARTING\_INGESTION**: Ein kurzfristiger Status, der angibt, dass der Ereignisdatenspeicher beginnt, Live-Ereignisse aufzunehmen.
- **STOPPING\_INGESTION**: Ein kurzfristiger Status, der angibt, dass der Ereignisdatenspeicher die Aufnahme von Live-Ereignissen beendet.
- **STOPPED\_INGESTION**: Der Ereignisdatenspeicher nimmt keine Live-Ereignisse auf. Sie können weiterhin Abfragen für Ereignisse ausführen, die sich bereits im Ereignisdatenspeicher befinden, und Trail-Ereignisse weiterhin in den Ereignisdatenspeicher kopieren.
- **PENDING\_DELETION** – Der Ereignisdatenspeicher befand sich im Status **ENABLED** oder **STOPPED\_INGESTION** und wurde gelöscht, liegt jedoch innerhalb der siebentägigen Wartezeit vor



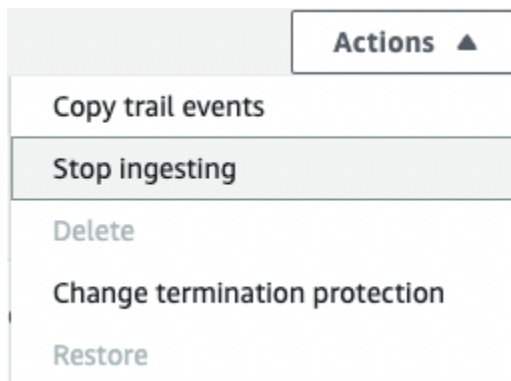
dem dauerhaften Löschen. Sie können keine Abfragen im Ereignisdatenspeicher ausführen und außer der Wiederherstellung können keine Vorgänge im Ereignisdatenspeicher ausgeführt werden.

Sie können einen Ereignisdatenspeicher nur löschen, wenn sowohl der Verbund als auch der Beendigungsschutz deaktiviert sind. Der Beendigungsschutz verhindert, dass ein Ereignisdatenspeicher versehentlich gelöscht wird. Standardmäßig ist der Beendigungsschutz in einem Ereignisdatenspeicher aktiviert. Mit [Verbund](#) können Sie Ihre Ereignisdatenspeicherdaten in Athena abfragen und er ist standardmäßig deaktiviert.

Nachdem Sie einen Ereignisdatenspeicher gelöscht haben, bleibt er sieben Tage lang im Status PENDING\_DELETION, bevor er dauerhaft gelöscht wird. Sie können einen Ereignisdatenspeicher während der siebentägigen Wartezeit wiederherstellen. Im Status PENDING\_DELETION ist ein Ereignisdatenspeicher nicht für Abfragen verfügbar und es können keine anderen Operationen mit dem Ereignisdatenspeicher durchgeführt werden, außer Wiederherstellungsoperationen. Ein Ereignisdatenspeicher mit ausstehendem Löschvorgang nimmt keine Ereignisse auf und verursacht keine Kosten. Ereignisdatenspeicher, deren Löschung noch aussteht, werden jedoch auf das Kontingent der Ereignisdatenspeicher angerechnet, die in einem Speicher vorhanden sein können AWS-Region.

#### Verfügbare Aktionen für Ereignisdatenspeicher

Über die Befehle im Menü Aktionen der Detailseite des Ereignisdatenspeichers können Sie einen Ereignisdatenspeicher [löschen](#) oder [wiederherstellen](#), Trail-Ereignisse kopieren, die Erfassung von Ereignissen starten oder beenden oder den Beendigungsschutz aktivieren oder deaktivieren.



Die Option zum Kopieren von Trail-Ereignissen ist nur für Ereignisdatenspeicher verfügbar, die CloudTrail Verwaltungs- und Datenereignisse enthalten. Die Optionen Aufnahme starten und Aufnahme beenden sind nur für Ereignisdatenspeicher verfügbar, die entweder CloudTrail Ereignisse (Verwaltungs- und Datenereignisse) oder Konfigurationselemente enthalten. AWS Config

## Kopieren von Trail-Ereignissen in einen Ereignisdatenspeicher

Sie können Trail-Ereignisse in einen CloudTrail Lake Event Data Store kopieren, um eine point-in-time Momentaufnahme der im Trail protokollierten Ereignisse zu erstellen. Das Kopieren der Ereignisse eines Trails beeinträchtigt nicht die Fähigkeit des Trails, Ereignisse zu protokollieren, und ändert den Trail in keiner Weise.

Sie können Trail-Ereignisse in einen vorhandenen, für CloudTrail Ereignisse konfigurierten Ereignisdatenspeicher kopieren, oder Sie können einen neuen CloudTrail Ereignisdatenspeicher erstellen und bei der Erstellung des Ereignisdatenspeichers die Option Trail-Ereignisse kopieren auswählen. Weitere Informationen zum Kopieren von Trail-Ereignissen in einen bestehenden Ereignisdatenspeicher finden Sie unter [Kopieren von Trail-Ereignissen in einen vorhandenen Ereignisdatenspeicher](#). Weitere Informationen zum Erstellen eines neuen Ereignisdatenspeichers finden Sie unter [Erstellen Sie mit der Konsole einen Ereignisdatenspeicher für CloudTrail Ereignisse](#).

Wenn Sie Trail-Ereignisse in den Ereignisdatenspeicher einer Organisation kopieren, müssen Sie das Verwaltungskonto der Organisation verwenden. Trail-Ereignisse lassen sich nicht mit dem Konto eines delegierten Administrators einer Organisation kopieren.

CloudTrail Für Datenspeicher von Lake Events fallen Gebühren an. Beim Erstellen eines Ereignisdatenspeichers wählen Sie die [Preisoption](#) aus, die für den Ereignisdatenspeicher genutzt werden soll. Die Preisoption bestimmt die Kosten für die Erfassung und Speicherung von Ereignissen sowie die standardmäßige und maximale Aufbewahrungsdauer für den Ereignisdatenspeicher. Informationen zur CloudTrail Preisgestaltung und Verwaltung der Lake-Kosten finden Sie unter [AWS CloudTrail Preise](#) und [Verwaltung der CloudTrail Seekosten](#).

Wenn Sie Trail-Ereignisse in einen CloudTrail Lake-Ereignisdatenspeicher kopieren, fallen Gebühren an, die auf der Menge der unkomprimierten Daten basieren, die der Ereignisdatenspeicher aufnimmt.

Wenn Sie Trail-Ereignisse nach CloudTrail Lake kopieren, werden die im komprimierten CloudTrail GZIP-Format gespeicherten Protokolle entpackt und anschließend die in den Protokollen enthaltenen Ereignisse in Ihren Ereignisdatenspeicher kopiert. Die Größe der unkomprimierten Daten könnte größer sein als die tatsächliche S3-Speichergröße. Um eine allgemeine Schätzung der Größe der unkomprimierten Daten zu erhalten, können Sie die Größe der Protokolle im S3-Bucket mit 10 multiplizieren.

Sie können die Kosten senken, indem Sie einen engeren Zeitraum für die kopierten Ereignisse angeben. Wenn Sie planen, den Ereignisdatenspeicher nur zum Abfragen Ihrer kopierten Ereignisse zu verwenden, können Sie die Ereignisaufnahme deaktivieren, um zu vermeiden, dass für zukünftige

Ereignisse Gebühren anfallen. Weitere Informationen finden Sie unter [AWS CloudTrail -Preise](#) und [Verwaltung der CloudTrail Seekosten](#).

## Szenarien

In der folgenden Tabelle werden einige gängige Szenarien für das Kopieren von Trail-Ereignissen beschrieben. Außerdem wird beschrieben, wie Sie die einzelnen Szenarien mithilfe der Konsole ausführen.

Szenario	Wie erreiche ich das in der Konsole?
Analysieren und fragen Sie historische Trail-Ereignisse in CloudTrail Lake ab, ohne neue Ereignisse zu übernehmen	Erstellen Sie einen <a href="#">neuen Ereignisdatenspeicher</a> und wählen Sie im Rahmen der Erstellung des Ereignisdatenspeichers die Option Trail-Ereignisse kopieren aus. Deaktivieren Sie beim Erstellen des Ereignisdatenspeichers die Option Ereignisse aufnehmen (Schritt 15 des Verfahrens), um sicherzustellen, dass der Ereignisdatenspeicher nur die Verlaufsereignisse für Ihren Trail und keine zukünftigen Ereignisse enthält.
Ersetzen Sie Ihren vorhandenen Trail durch einen CloudTrail Lake Event Data Store	<p>Erstellen Sie einen Ereignisdatenspeicher mit den gleichen Ereignisselektoren wie bei Ihrem Trail, um sicherzustellen, dass der Ereignisdatenspeicher die gleiche Ereignisabdeckung hat wie Ihr Trail.</p> <p>Um zu vermeiden, dass Ereignisse zwischen dem Quell-Trail und dem Zielereignisdatenspeicher dupliziert werden, wählen Sie einen Zeitraum für die kopierten Ereignisse aus, der vor der Erstellung des Ereignisdatenspeichers liegt.</p> <p>Nachdem Ihr Ereignisdatenspeicher erstellt wurde, können Sie die Protokollierung für den Trail deaktivieren, um zusätzliche Gebühren zu vermeiden.</p>

## Themen

- [Überlegungen zum Kopieren von Trail-Ereignissen](#)
- [Erforderliche Berechtigungen zum Kopieren von Trail-Ereignissen](#)
- [Kopieren von Trail-Ereignissen in einen vorhandenen Ereignisdatenspeicher](#)

- [Details zur Ereigniskopie](#)
- [Beispiel: Kopieren Sie Trail-Ereignisse in einen neuen Ereignisdatenspeicher](#)

## Überlegungen zum Kopieren von Trail-Ereignissen

Berücksichtigen Sie beim Kopieren von Trail-Ereignissen die folgenden Faktoren.

- CloudTrail verwendet beim Kopieren von Trail-Ereignissen den [GetObject](#) S3-API-Vorgang, um die Trail-Ereignisse im S3-Quell-Bucket abzurufen. Es gibt einige archivierte Speicherklassen von S3, wie S3 Glacier Flexible Retrieval, S3 Glacier Deep Archive, S3 Outposts und S3 Intelligent-Tiering Deep Archive, auf die mithilfe von `GetObject` nicht zugegriffen werden kann. Um in diesen archivierten Speicherklassen gespeicherte Trail-Ereignisse zu kopieren, müssen Sie zunächst eine Kopie mithilfe des S3-Vorgangs `RestoreObject` wiederherstellen. Informationen zum Wiederherstellen archivierter Objekte finden Sie unter [Wiederherstellen archivierter Objekte](#) im Benutzerhandbuch von Amazon S3.
- Wenn Sie Trail-Ereignisse in einen Event-Datenspeicher CloudTrail kopieren, werden alle Trail-Ereignisse unabhängig von der Konfiguration der Ereignistypen des Ziel-Event-Datenspeichers, den erweiterten Event-Selektoren oder AWS-Region kopiert.
- Bevor Sie Trail-Ereignisse in einen vorhandenen Ereignisdatenspeicher kopieren, stellen Sie sicher, dass die Preisoption und der Aufbewahrungszeitraum des Ereignisdatenspeichers für Ihren Anwendungsfall entsprechend konfiguriert sind.
  - Preisoption: Die Preisoption bestimmt die Kosten für die Erfassung und Speicherung von Ereignissen. Weitere Informationen zu Preisoptionen und Details finden Sie unter [AWS CloudTrail -Preise](#) und [Preisoptionen für den Ereignisdatenspeicher](#).
  - Aufbewahrungszeitraum: Der Aufbewahrungszeitraum bestimmt, wie lange Ereignisdaten im Ereignisdatenspeicher aufbewahrt werden. CloudTrail kopiert nur Ereignisse, die `eventTime` innerhalb der Aufbewahrungsfrist des Veranstaltungsdatspeichers liegen. Um den geeigneten Aufbewahrungszeitraum zu ermitteln, nehmen Sie die Summe aus dem ältesten Ereignis, das Sie kopieren möchten, in Tagen und der Anzahl der Tage, an denen Sie die Ereignisse im Ereignisdatenspeicher speichern möchten (Aufbewahrungszeitraum = *oldest-event-in-days* + *number-days-to-retain*). Wenn das älteste Ereignis, das Sie kopieren, beispielsweise 45 Tage alt ist und Sie die Ereignisse weitere 45 Tage im Ereignisdatenspeicher aufbewahren möchten, würden Sie die Aufbewahrungsdauer auf 90 Tage festlegen.
- Wenn Sie Trail-Ereignisse zur Untersuchung in einen Ereignisdatenspeicher kopieren und keine zukünftigen Ereignisse aufnehmen möchten, können Sie die Aufnahme in den Ereignisdatenspeicher beenden. Deaktivieren Sie beim Erstellen des Ereignisdatenspeichers

die Option Ereignisse aufnehmen (Schritt 15 des [Verfahrens](#)), um sicherzustellen, dass der Ereignisdatenspeicher nur die Verlaufereignisse für Ihren Trail und keine zukünftigen Ereignisse enthält.

- Deaktivieren Sie vor dem Kopieren von Trailer-Eignissen alle Zugriffssteuerungslisten (ACL), die an den S3-Quell-Bucket angehängt sind, und aktualisieren Sie die S3-Bucket-Richtlinie für den Zielereignisdatenspeicher. Weitere Informationen zum Aktualisieren der S3-Bucket-Richtlinie finden Sie unter [Amazon-S3-Bucket-Richtlinie für das Kopieren von Trail-Ereignissen](#). Weitere Informationen zum Deaktivieren von ACLs finden Sie unter [Steuern des Eigentums an Objekten und Deaktivieren von ACLs für Ihren Bucket](#) im Benutzerhandbuch von Amazon S3.
- CloudTrail kopiert nur Trail-Ereignisse aus Gzip-komprimierten Protokolldateien, die sich im S3-Quell-Bucket befinden. CloudTrail kopiert keine Trail-Ereignisse aus unkomprimierten Protokolldateien oder Protokolldateien, die in einem anderen Format als Gzip komprimiert wurden.
- Um zu vermeiden, dass Ereignisse zwischen dem Quell-Trail und dem Zielereignisdatenspeicher dupliziert werden, wählen Sie einen Zeitraum für die kopierten Ereignisse aus, der vor der Erstellung des Ereignisdatenspeichers liegt.
- Standardmäßig werden CloudTrail nur CloudTrail Ereignisse kopiert, die im `CloudTrail` Präfix des S3-Buckets und die Präfixe innerhalb des `CloudTrail` Präfixes enthalten sind, und überprüft keine Präfixe für andere Dienste. AWS Wenn Sie CloudTrail Ereignisse kopieren möchten, die in einem anderen Präfix enthalten sind, müssen Sie das Präfix beim Kopieren von Trail-Ereignissen auswählen.
- Um Trail-Ereignisse in den Ereignisdatenspeicher einer Organisation zu kopieren, müssen Sie das Verwaltungskonto der Organisation verwenden. Über das Konto eines delegierten Administrators können Trail-Ereignisse nicht in den Ereignisdatenspeicher einer Organisation kopiert werden.

## Erforderliche Berechtigungen zum Kopieren von Trail-Ereignissen

Stellen Sie vor dem Kopieren von Trail-Ereignissen sicher, dass Sie über alle erforderlichen Berechtigungen für Ihre IAM-Rolle verfügen. Sie müssen die IAM-Rollenberechtigungen nur aktualisieren, wenn Sie eine vorhandene IAM-Rolle zum Kopieren von Trail-Ereignissen auswählen. Wenn Sie sich dafür entscheiden, eine neue IAM-Rolle zu erstellen, CloudTrail stellt alle erforderlichen Berechtigungen für die Rolle bereit.

Wenn der S3-Quell-Bucket einen KMS-Schlüssel für die Datenverschlüsselung verwendet, stellen Sie sicher, dass die KMS-Schlüsselrichtlinie das Entschlüsseln von Daten im Bucket zulässt CloudTrail . Wenn der S3-Quell-Bucket mehrere KMS-Schlüssel verwendet, müssen Sie die Richtlinien der

einzelnen Schlüssel aktualisieren, um die Entschlüsselung der Daten im Bucket CloudTrail zu ermöglichen.

## Themen

- [IAM-Berechtigungen zum Kopieren von Trail-Ereignissen](#)
- [Amazon-S3-Bucket-Richtlinie für das Kopieren von Trail-Ereignissen](#)
- [KMS-Schlüsselrichtlinie zum Entschlüsseln von Daten im S3-Quell-Bucket](#)

## IAM-Berechtigungen zum Kopieren von Trail-Ereignissen

Beim Kopieren von Trail-Ereignissen haben Sie die Möglichkeit, eine neue IAM-Rolle zu erstellen oder eine vorhandene IAM-Rolle zu verwenden. Wenn Sie eine neue IAM-Rolle auswählen, CloudTrail wird eine IAM-Rolle mit den erforderlichen Berechtigungen erstellt, sodass keine weiteren Maßnahmen Ihrerseits erforderlich sind.

Wenn Sie sich für eine bestehende Rolle entscheiden, stellen Sie sicher, dass die Richtlinien der IAM-Rolle das Kopieren von Trail-Ereignissen aus dem S3-Quell-Bucket zulassen CloudTrail . Dieser Abschnitt enthält Beispiele für die erforderlichen IAM-Rollenberechtigungen und Vertrauensrichtlinien.

Das folgende Beispiel enthält die Berechtigungsrichtlinie, die es ermöglicht, Trail-Ereignisse aus dem S3-Quell-Bucket CloudTrail zu kopieren. Ersetzen Sie *myBucketNameMyAccountID*, *Region*, *Präfix* und *eventDataStoreId* durch die entsprechenden Werte für Ihre Konfiguration. Die *MyAccountID* ist die für CloudTrail Lake verwendete AWS Konto-ID, die möglicherweise nicht mit der AWS Konto-ID für den S3-Bucket identisch ist.

Ersetzen Sie *key-region*, *keyAccountID* und *keyID* durch die Werte für den KMS-Schlüssel, der zur Verschlüsselung des S3-Quell-Buckets verwendet wird. Sie können die *AWSCloudTrailImportKeyAccess*-Anweisung weglassen, wenn der S3-Quell-Bucket keinen KMS-Schlüssel für die Verschlüsselung verwendet.

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Sid": "AWSCloudTrailImportBucketAccess",
      "Effect": "Allow",
      "Action": ["s3:ListBucket", "s3:GetBucketAcl"],
      "Resource": [
        "arn:aws:s3:::myBucketName"
      ]
    }
  ]
}
```

```

    ],
    "Condition": {
      "StringEquals": {
        "aws:SourceAccount": "myAccountID",
        "aws:SourceArn":
"arn:aws:cloudtrail:region:myAccountID:eventdataStore/eventDataStoreId"
      }
    }
  },
  {
    "Sid": "AWSCloudTrailImportObjectAccess",
    "Effect": "Allow",
    "Action": ["s3:GetObject"],
    "Resource": [
      "arn:aws:s3::myBucketName/prefix",
      "arn:aws:s3::myBucketName/prefix/*"
    ],
    "Condition": {
      "StringEquals": {
        "aws:SourceAccount": "myAccountID",
        "aws:SourceArn":
"arn:aws:cloudtrail:region:myAccountID:eventdataStore/eventDataStoreId"
      }
    }
  },
  {
    "Sid": "AWSCloudTrailImportKeyAccess",
    "Effect": "Allow",
    "Action": ["kms:GenerateDataKey", "kms:Decrypt"],
    "Resource": [
      "arn:aws:kms:key-region:keyAccountID:key/keyID"
    ]
  }
]
}

```

Das folgende Beispiel enthält die IAM-Vertrauensrichtlinie, die es ermöglicht, eine IAM-Rolle anzunehmen, CloudTrail um Trail-Ereignisse aus dem S3-Quell-Bucket zu kopieren. Ersetzen Sie *MyAccountID*, *Region* und *eventDataStoreArn* durch die entsprechenden Werte für Ihre Konfiguration. Die *MyAccountID* ist die für CloudTrail Lake verwendete AWS-Konto ID, die möglicherweise nicht mit der AWS Konto-ID für den S3-Bucket identisch ist.

```
{
```

```
"Version": "2012-10-17",
"Statement": [
  {
    "Effect": "Allow",
    "Principal": {
      "Service": "cloudtrail.amazonaws.com"
    },
    "Action": "sts:AssumeRole",
    "Condition": {
      "StringEquals": {
        "aws:SourceAccount": "myAccountID",
        "aws:SourceArn":
"arn:aws:cloudtrail:region:myAccountID:eventdataStore/eventDataStoreId"
      }
    }
  }
]
```

## Amazon-S3-Bucket-Richtlinie für das Kopieren von Trail-Ereignissen

Standardmäßig werden Amazon-S3-Buckets und -Objekte als privat eingestuft. Nur der Ressourcenbesitzer (das AWS -Konto, das den Bucket erstellt hat) kann auf den Bucket und die darin enthaltenen Objekte zugreifen. Der Ressourcenbesitzer kann anderen Ressourcen und Benutzern Zugriffsberechtigungen gewähren, indem er eine Zugriffsrichtlinie schreibt.

Bevor Sie Trail-Ereignisse kopieren, müssen Sie die S3-Bucket-Richtlinie aktualisieren, damit CloudTrail Trail-Ereignisse aus dem S3-Quell-Bucket kopiert werden können.

Sie können der S3-Bucket-Richtlinie die folgende Anweisung hinzufügen, um diese Berechtigungen zu gewähren. Ersetzen *roleArn* und *myBucketName* durch die entsprechenden Werte für Ihre Konfiguration.

```
{
  "Sid": "AWSCloudTrailImportBucketAccess",
  "Effect": "Allow",
  "Action": [
    "s3:ListBucket",
    "s3:GetBucketAcl",
    "s3:GetObject"
  ]
}
```



```
],
  "Principal": {
    "AWS": "roleArn"
  },
  "Resource": [
    "arn:aws:s3:::myBucketName",
    "arn:aws:s3:::myBucketName/*"
  ]
},
```

## KMS-Schlüsselrichtlinie zum Entschlüsseln von Daten im S3-Quell-Bucket

Wenn der Quell-S3-Bucket einen KMS-Schlüssel für die Datenverschlüsselung verwendet, stellen Sie sicher, dass die KMS-Schlüsselrichtlinie über die `kms:Decrypt` erforderlichen `kms:GenerateDataKey` Berechtigungen verfügt CloudTrail, um Trail-Ereignisse aus einem S3-Bucket mit aktivierter SSE-KMS-Verschlüsselung zu kopieren. Wenn Ihr S3-Quell-Bucket mehrere KMS-Schlüssel verwendet, müssen Sie die Richtlinien jedes Schlüssels aktualisieren. Durch die Aktualisierung der KMS-Schlüsselrichtlinie können CloudTrail Daten im S3-Quell-Bucket entschlüsselt, Validierungsprüfungen durchgeführt werden, um sicherzustellen, dass Ereignisse den CloudTrail Standards entsprechen, und Ereignisse in den CloudTrail Lake-Ereignisdatenspeicher kopiert werden.

Das folgende Beispiel enthält die KMS-Schlüsselrichtlinie, mit der die Daten im CloudTrail S3-Quell-Bucket entschlüsselt werden können. *Ersetzen Sie RoleARN myBucketName, MyAccountID, Region und eventDataStore Id durch die entsprechenden Werte für Ihre Konfiguration.* Die *myAccountID* ist die für CloudTrail Lake verwendete AWS Konto-ID, die möglicherweise nicht mit der AWS Konto-ID für den S3-Bucket identisch ist.

```
{
  "Sid": "AWSCloudTrailImportDecrypt",
  "Effect": "Allow",
  "Action": [
    "kms:Decrypt",
    "kms:GenerateDataKey"
  ],
  "Principal": {
    "AWS": "roleArn"
  },
  "Resource": "*",
  "Condition": {
    "StringLike": {
```

```
    "kms:EncryptionContext:aws:s3:arn": "arn:aws:s3:::myBucketName/*"
  },
  "StringEquals": {
    "aws:SourceAccount": "myAccountID",
    "aws:SourceArn":
"arn:aws:cloudtrail:region:myAccountID:eventdataStore/eventDataStoreId"
  }
}
}
```

## Kopieren von Trail-Ereignissen in einen vorhandenen Ereignisdatenspeicher

Gehen Sie wie folgt vor, um Trail-Ereignisse in einen bestehenden Ereignisdatenspeicher zu kopieren. Weitere Informationen zum Erstellen eines neuen Ereignisdatenspeichers finden Sie unter [Erstellen Sie mit der Konsole einen Ereignisdatenspeicher für CloudTrail Ereignisse](#).

### Note

Bevor Sie Trail-Ereignisse in einen vorhandenen Ereignisdatenspeicher kopieren, stellen Sie sicher, dass die Preisoption und der Aufbewahrungszeitraum des Ereignisdatenspeichers für Ihren Anwendungsfall entsprechend konfiguriert sind.

- **Preisoption:** Die Preisoption bestimmt die Kosten für die Erfassung und Speicherung von Ereignissen. Weitere Informationen zu Preisoptionen und Details finden Sie unter [AWS CloudTrail -Preise](#) und [Preisoptionen für den Ereignisdatenspeicher](#).
- **Aufbewahrungszeitraum:** Die Aufbewahrungsfrist bestimmt, wie lange Ereignisdaten im Ereignisdatenspeicher aufbewahrt werden. CloudTrail kopiert nur Ereignisse, die `eventTime` innerhalb der Aufbewahrungsfrist des Veranstaltungsdatspeichers liegen. Um den geeigneten Aufbewahrungszeitraum zu ermitteln, nehmen Sie die Summe aus dem ältesten Ereignis, das Sie kopieren möchten, in Tagen und der Anzahl der Tage, an denen Sie die Ereignisse im Ereignisdatenspeicher speichern möchten (Aufbewahrungszeitraum = *oldest-event-in-days* + *number-days-to-retain*). Wenn das älteste Ereignis, das Sie kopieren, beispielsweise 45 Tage alt ist und Sie die Ereignisse weitere 45 Tage im Ereignisdatenspeicher aufbewahren möchten, würden Sie die Aufbewahrungsdauer auf 90 Tage festlegen.

## So kopieren Sie Trail-Ereignisse in einen Ereignisdatenspeicher

1. Melden Sie sich bei der an AWS Management Console und öffnen Sie die CloudTrail Konsole unter <https://console.aws.amazon.com/cloudtrail/>.
2. Wählen Sie im Navigationsbereich unter Lake Ereignisdatenspeicher aus.
3. Wählen Sie Copy trail events (Kopieren von Trail-Ereignissen).
4. Wählen Sie auf der Seite Copy trail events (Trail-Ereignisse kopieren) für Event source (Ereignisquelle) den Pfad aus, den Sie kopieren möchten. Standardmäßig werden CloudTrail nur CloudTrail Ereignisse kopiert, die im `CloudTrail` Präfix des S3-Buckets und die Präfixe innerhalb des `CloudTrail` Präfixes enthalten sind, und überprüft keine Präfixe für andere AWS Dienste. Wenn Sie CloudTrail Ereignisse kopieren möchten, die in einem anderen Präfix enthalten sind, wählen Sie S3-URL eingeben und dann S3 durchsuchen, um zum Präfix zu wechseln. Wenn der S3-Quell-Bucket für den Trail einen KMS-Schlüssel für die Datenverschlüsselung verwendet, stellen Sie sicher, dass die KMS-Schlüsselrichtlinie das Entschlüsseln der Daten zulässt CloudTrail . Wenn Ihr S3-Quell-Bucket mehrere KMS-Schlüssel verwendet, müssen Sie die Richtlinien für jeden Schlüssel aktualisieren, damit CloudTrail die Daten im Bucket entschlüsselt werden können. Weitere Informationen zum Aktualisieren der KMS-Schlüssel-Richtlinie finden Sie unter [KMS-Schlüsselrichtlinie zum Entschlüsseln von Daten im S3-Quell-Bucket](#).

Die S3-Bucket-Richtlinie muss CloudTrail Zugriff gewähren, um Trail-Ereignisse aus Ihrem S3-Bucket zu kopieren. Weitere Informationen zum Aktualisieren der S3-Bucket-Richtlinie finden Sie unter [Amazon-S3-Bucket-Richtlinie für das Kopieren von Trail-Ereignissen](#).

5. Wählen Sie unter Geben Sie einen Zeitraum für Ereignisse an den Zeitraum aus, in dem die Ereignisse kopiert werden sollen. CloudTrail überprüft das Präfix und den Namen der Protokolldatei, um sicherzustellen, dass der Name ein Datum zwischen dem ausgewählten Start- und Enddatum enthält, bevor versucht wird, Trail-Ereignisse zu kopieren. Sie können einen Relative range (Relativen Bereich) oder einen Absolute range (Absoluten Bereich) wählen. Um zu vermeiden, dass Ereignisse zwischen dem Quell-Trail und dem Zielergebnisdatenspeicher dupliziert werden, wählen Sie einen Zeitraum aus, der vor der Erstellung des Ereignisdatenspeichers liegt.

### Note

CloudTrail kopiert nur Trail-Ereignisse, die `eventTime` innerhalb der Aufbewahrungsfrist des Event-Datenspeichers liegen. Wenn die Aufbewahrungsfrist eines Event-

Datenspeichers beispielsweise 90 Tage beträgt, CloudTrail werden keine Trail-Ereignisse kopiert, die eventTime älter als 90 Tage sind.

- Wenn Sie Relativer Bereich wählen, können Sie wählen, ob Ereignisse kopiert werden sollen, die in den letzten 6 Monaten, 1 Jahr, 2 Jahren, 7 Jahren oder in einem benutzerdefinierten Bereich protokolliert wurden. CloudTrail kopiert die Ereignisse, die innerhalb des ausgewählten Zeitraums protokolliert wurden.
  - Wenn Sie „Absoluter Bereich“ wählen, können Sie ein bestimmtes Start- und Enddatum wählen. CloudTrail kopiert die Ereignisse, die zwischen dem ausgewählten Start- und Enddatum aufgetreten sind.
6. Wählen Sie für Delivery location (Zustellungsort) den Zielereignisdatspeicher aus der Dropdown-Liste aus.
  7. Wählen Sie für Permissions (Berechtigungen) unter den folgenden IAM-Rollenoptionen aus. Wenn Sie eine vorhandene IAM-Rolle auswählen, stellen Sie sicher, dass die IAM-Rollenrichtlinie die erforderlichen Berechtigungen bereitstellt. Weitere Informationen zum Aktualisieren der IAM-Rollenberechtigungen finden Sie unter [IAM-Berechtigungen zum Kopieren von Trail-Ereignissen](#).
    - Wählen Sie Create a new role (recommended) (Erstellen Sie eine neue Rolle (empfohlen)), um eine neue IAM-Rolle zu erstellen. Geben Sie für Enter IAM role name (IAM-Rollennamen eingeben) einen Namen für die Rolle ein. CloudTrail erstellt automatisch die erforderlichen Berechtigungen für diese neue Rolle.
    - Wählen Sie Eine benutzerdefinierte IAM-Rolle verwenden ARN aus, um eine benutzerdefinierte IAM-Rolle zu verwenden, die nicht aufgeführt ist. Geben Sie für Enter IAM role ARN (IAM-Rollen-ARN eingeben) den IAM-ARN ein.
    - Wählen Sie eine vorhandene IAM-Rolle aus der Drop-down-Liste aus.
  8. Wählen Sie Copy events (Kopieren von Ereignissen).
  9. Sie werden zur Bestätigung aufgefordert. Sobald Sie bereit sind zu bestätigen, wählen Sie Copy trail events to Lake (Trail-Ereignisse nach Lake kopieren) aus und dann wählen Sie Copy events (Ereignisse kopieren).
  10. Auf der Seite Copy details (Kopieren von Details) können Sie den Kopierstatus anzeigen und eventuelle Fehler überprüfen. Wenn eine Trail-Ereignis-Kopie abgeschlossen ist, wird der Copy status (Kopierstatus) entweder auf Completed (Abgeschlossen) festgelegt, wenn keine Fehler aufgetreten sind, oder auf Failed (Fehlgeschlagen), wenn Fehler aufgetreten sind.

**Note**

Details, die auf der Detailseite der Ereigniskopie angezeigt werden, sind nicht in Echtzeit. Die tatsächlichen Werte für Details wie Kopierte Präfixe können höher sein als die, die auf der Seite angezeigt werden. CloudTrail aktualisiert die Details im Verlauf der Ereigniskopie schrittweise.

11. Wenn der Copy status (Kopierstatus) Failed (Fehlgeschlagen) lautet, beheben Sie alle Fehler, die unter Copy failures (Kopierfehler) angezeigt werden, und wählen Sie dann Retry copy (Kopie wiederholen) aus. Wenn Sie erneut versuchen, eine Kopie zu erstellen, CloudTrail wird der Kopiervorgang an der Stelle fortgesetzt, an der der Fehler aufgetreten ist.

Weitere Informationen zum Anzeigen der Details eines Trail-Ereignisses finden Sie unter [Details zur Ereigniskopie](#).

## Details zur Ereigniskopie

Nachdem eine Kopie eines Trail-Ereignisses gestartet wurde, können Sie die Details der Ereigniskopie, einschließlich des Status der Kopie, und Informationen zu Kopierfehlern anzeigen.

**Note**

Details, die auf der Detailseite der Ereigniskopie angezeigt werden, sind nicht in Echtzeit. Die tatsächlichen Werte für Details wie Kopierte Präfixe können höher sein als die, die auf der Seite angezeigt werden. CloudTrail aktualisiert die Details im Verlauf der Event-Kopie schrittweise.

So greifen Sie auf die Seite mit den Details zu Ereigniskopien zu

1. Melden Sie sich bei der an AWS Management Console und öffnen Sie die CloudTrail Konsole unter <https://console.aws.amazon.com/cloudtrail/>.
2. Wählen Sie im linken Navigationsbereich unter Lake die Option Ereignisdatenspeicher aus.
3. Wählen Sie den Ereignisdatenspeicher aus.
4. Wählen Sie die Ereigniskopie im Abschnitt Status der Ereigniskopie aus.

## Details kopieren

Unter Copy details (Details kopieren) können Sie sich die folgenden Details über die Trail-Ereignis-Kopie ansehen.

- Event log S3 location (Ereignisprotokoll-S3-Speicherort) – Der Speicherort des Quell-S3-Buckets, der die Trail-Ereignisprotokolldateien enthält.
- Copy ID (ID kopieren) – Der ID für die Kopie.
- Prefixes copied (Kopierte Präfixe) – Stellt die Anzahl der kopierten S3-Präfixe dar. CloudTrail kopiert beim Kopieren von Trail-Ereignissen die Ereignisse in den Trail-Protokolldateien, die in den Präfixen gespeichert sind.
- Copy status (Status kopieren) – Der Status der Kopie.
  - Initializing (Initialisieren) – Der Anfangsstatus wird angezeigt, wenn die Kopie des Trail-Ereignisses beginnt.
  - In progress (In Bearbeitung) – Zeigt an, dass die Kopie des Trail-Ereignisses in Bearbeitung ist.

### Note

Sie können Trail-Ereignisse nicht kopieren, wenn eine andere Trail-Ereigniskopie In progress (In Bearbeitung) ist. Um eine Kopie eines Trail-Ereignisses zu stoppen, wählen Sie Stop copy (Kopieren anhalten).

- Stopped (Angehalten) – Gibt an, dass eine Aktion Stop copy (zum Beenden der Kopie) ausgeführt wurde. Um eine Kopie eines Trail-Ereignisses erneut zu versuchen, wählen Sie Retry copy (Kopieren wiederholen).
- Failed (Fehlgeschlagen) – Die Kopie wurde abgeschlossen, aber einige Trail-Ereignisse konnten nicht kopiert werden. Überprüfen Sie die Fehlermeldungen in Copy failures (Fehler beim Kopieren). Um eine Kopie eines Trail-Ereignisses erneut zu versuchen, wählen Sie Retry copy (Kopieren wiederholen). Wenn Sie erneut versuchen, eine Kopie zu erstellen, CloudTrail wird der Kopiervorgang an der Stelle fortgesetzt, an der der Fehler aufgetreten ist.
- Completed (Fertiggestellt) – Die Kopie wurde ohne Fehler abgeschlossen. Sie können die kopierten Trail-Ereignisse im Ereignisdatenspeicher abfragen.
- Created time (Erstellungszeit) – Zeigt an, wann die Trail-Ereigniskopie gestartet wurde.
- Finish time (Endzeit) – Zeigt an, wann die Kopie des Trail-Ereignisses abgeschlossen oder beendet wurde.

## Kopierfehler

Unter Copy failures (Kopierfehler) können Sie den Fehlerspeicherort, die Fehlermeldung und den Fehlertyp für jeden Kopierfehler überprüfen. Zu den häufigsten Fehlerursachen gehört, dass ein S3-Präfix eine unkomprimierte Datei oder eine Datei enthielt, die von einem anderen Dienst als bereitgestellt wurde. CloudTrail Eine weitere mögliche Fehlerursache sind Zugriffsprobleme. Wenn beispielsweise der S3-Bucket des Ereignisdatenspeichers keinen CloudTrail Zugriff auf den Import der Ereignisse gewährt, wird eine AccessDenied Fehlermeldung angezeigt.

Überprüfen Sie für jeden Kopierfehler die folgenden Fehlerinformationen.

- Der Error location (Fehlerspeicherort) – Zeigt den Speicherort im S3-Bucket an, an dem der Fehler aufgetreten ist. Wenn ein Fehler auftrat, weil der Quell-S3-Bucket eine unkomprimierte Datei enthielt, würde der Error location (Fehlerspeicherort) das Präfix enthalten, unter dem Sie diese Datei finden würden.
- Die Error message (Fehlermeldung) – Sie enthält eine Erklärung, warum der Fehler aufgetreten ist.
- Der Error type (Fehlertyp) – Dies gibt den Fehlertyp an. Ein Error type (Fehlertyp) von AccessDenied gibt beispielsweise an, dass der Fehler aufgrund eines Berechtigungsproblems aufgetreten ist. Weitere Informationen zu den erforderlichen Berechtigungen zum Kopieren von Trail-Ereignissen finden Sie unter [Erforderliche Berechtigungen zum Kopieren von Trail-Ereignissen](#).

Nachdem Sie alle Fehler behoben haben, wählen Sie Retry copy (Kopieren wiederholen). Wenn Sie erneut versuchen, eine Kopie zu erstellen, CloudTrail wird die Kopie an der Stelle fortgesetzt, an der der Fehler aufgetreten ist.

### Beispiel: Kopieren Sie Trail-Ereignisse in einen neuen Ereignisdatenspeicher

In dieser exemplarischen Vorgehensweise erfahren Sie, wie Sie Trail-Ereignisse zur historischen Analyse in einen neuen Datenspeicher für Ereignisse in CloudTrail Lake kopieren. Weitere Informationen zum Kopieren von Trail-Ereignissen finden Sie unter [Kopieren von Trail-Ereignissen in einen Ereignisdatenspeicher](#).

Kopieren Sie Trail-Ereignisse wie folgt in einen neuen Ereignisdatenspeicher:

1. Melden Sie sich bei der an AWS Management Console und öffnen Sie die CloudTrail Konsole unter <https://console.aws.amazon.com/cloudtrail/>.
2. Wählen Sie im Navigationsbereich unter Lake die Option Ereignisdatenspeicher aus.

3. Wählen Sie Ereignisdatenspeicher erstellen aus.
4. Geben Sie auf der Seite „Event-Datenspeicher konfigurieren“ unter Allgemeine Details Ihrem Event-Datenspeicher einen Namen, z. *my-management-events-eds*. Verwenden Sie dazu am besten einen Namen, der den Zweck des Ereignisdatenspeichers schnell identifiziert. Informationen zu den CloudTrail Benennungsanforderungen finden Sie unter [Benennungsanforderungen](#).
5. Wählen Sie die Preisoption aus, die Sie für den Ereignisdatenspeicher verwenden möchten. Der Preisoption bestimmt die Kosten für die Erfassung und Speicherung von Ereignissen sowie die standardmäßige und maximale Aufbewahrungsdauern für Ihren Ereignisdatenspeicher. Weitere Informationen finden Sie unter [AWS CloudTrail -Preise](#) und [Verwaltung der CloudTrail Seekosten](#).


Die folgenden Optionen sind verfügbar:

- Preisoption mit verlängerbarer Aufbewahrung für ein Jahr – Empfohlen, wenn Sie damit rechnen, weniger als 25 TB an Ereignisdaten pro Monat zu erfassen und eine flexible Aufbewahrungsdauer von bis zu 10 Jahren wünschen. In den ersten 366 Tagen (Standardaufbewahrungszeitraum) ist Speicherplatz ohne zusätzliche Kosten im Preis für die Datenaufnahme enthalten. Nach 366 Tagen ist eine verlängerte Aufbewahrung gegen Aufpreis pay-as-you-go verfügbar. Dies ist die Standardoption.
    - Standardaufbewahrungsdauer: 366 Tage.
    - Maximale Aufbewahrungsdauer: beträgt 3 653 Tage.
  - Preisoption für die Aufbewahrung über sieben Jahre – Empfohlen, wenn Sie damit rechnen, mehr als 25 TB an Ereignisdaten pro Monat zu erfassen und eine flexible Aufbewahrungsdauer von bis zu 7 Jahren wünschen. Die Aufbewahrung ist im Preis für die Erfassung ohne Zusatzkosten enthalten.
    - Standardaufbewahrungsdauer: 2 557 Tage.
    - Maximale Aufbewahrungsdauer: beträgt 2 557 Tage.
6. Geben Sie einen Aufbewahrungszeitraum für den Ereignisdatenspeicher an. Die Aufbewahrungsdauern können zwischen 7 Tagen und 3 653 Tagen (etwa 10 Jahre) für die Preisoption mit verlängerbarer Aufbewahrungsdauer für ein Jahr oder zwischen 7 Tagen und 2 557 Tagen (etwa sieben Jahre) für die Preisoption mit siebenjähriger Aufbewahrungsdauer liegen.

CloudTrail Lake entscheidet, ob ein Ereignis aufbewahrt werden soll, indem es prüft, ob das Ereignis innerhalb `eventTime` des angegebenen Aufbewahrungszeitraums liegt. Wenn Sie



beispielsweise einen Aufbewahrungszeitraum von 90 Tagen angeben, CloudTrail werden Ereignisse entfernt, wenn sie `eventTime` älter als 90 Tage sind.

 Note

CloudTrail kopiert ein Ereignis nicht, wenn `eventTime` es älter als die angegebene Aufbewahrungsfrist ist.

Um den geeigneten Aufbewahrungszeitraum zu ermitteln, nehmen Sie die Summe aus dem ältesten Ereignis, das Sie kopieren möchten, in Tagen und der Anzahl der Tage, an denen Sie die Ereignisse im Ereignisdatenspeicher speichern möchten (Aufbewahrungszeitraum = *oldest-event-in-days* + *number-days-to-retain*).

Wenn das älteste Ereignis, das Sie kopieren, beispielsweise 45 Tage alt ist und Sie die Ereignisse weitere 45 Tage im Ereignisdatenspeicher aufbewahren möchten, würden Sie die Aufbewahrungsdauer auf 90 Tage festlegen.

7. (Optional) Wählen Sie unter Verschlüsselung aus, ob Sie den Ereignisdatenspeicher mit Ihrem eigenen KMS-Schlüssel verschlüsseln möchten. Standardmäßig werden alle Ereignisse in einem Ereignisdatenspeicher CloudTrail mithilfe eines KMS-Schlüssels verschlüsselt, der für Sie verantwortlich AWS ist und der für Sie verwaltet wird.

Um die Verschlüsselung mit Ihrem eigenen KMS-Schlüssel zu aktivieren, wählen Sie *Meinen eigenen AWS KMS key verwenden*. Wählen Sie *Neu*, um einen für Sie AWS KMS key erstellen zu lassen, oder wählen Sie *Bestehend*, um einen vorhandenen KMS-Schlüssel zu verwenden. Geben Sie unter *KMS-Alias* eingeben einen Alias im folgenden Format an `alias/MyAliasName`. Wenn Sie Ihren eigenen KMS-Schlüssel verwenden, müssen Sie Ihre KMS-Schlüsselrichtlinie bearbeiten, um das Verschlüsseln und Entschlüsseln von CloudTrail Protokollen zuzulassen. Weitere Informationen finden Sie unter [Konfigurieren Sie AWS KMS wichtige Richtlinien für CloudTrail](#). CloudTrail unterstützt auch Schlüssel AWS KMS für mehrere Regionen. Weitere Informationen finden Sie über Multi-Regions-Schlüssel finden Sie unter [Verwenden von Schlüsseln für mehrere Regionen](#) im AWS Key Management Service - Entwicklerhandbuch.

Wenn Sie Ihren eigenen KMS-Schlüssel verwenden, fallen AWS KMS Kosten für die Verschlüsselung und Entschlüsselung an. Nachdem Sie einen KMS-Schlüssel einem Ereignisdatenspeicher zugeordnet haben, kann der KMS-Schlüssel nicht entfernt oder geändert werden.

**Note**

Um die AWS Key Management Service Verschlüsselung für den Ereignisdatenspeicher einer Organisation zu aktivieren, müssen Sie einen vorhandenen KMS-Schlüssel für das Verwaltungskonto verwenden.

**General details** [Info](#)

Enter general details about your event data store.

**Event data store name**

Enter a display name for your store.

3-128 characters. Only letters, numbers, periods, underscores, and dashes are allowed.

**Pricing option** [Info](#)

Choose a pricing option that is cost effective for your specific use-case.

- One-year extendable retention pricing**  
Generally recommended pricing option if your monthly usage is under 25 TB. The first year of retention is included at no additional charge to your ingestion cost. You can extend your retention period to a maximum of 10 years.

- Seven-year retention pricing**  
Recommended if your monthly usage exceeds 25 TB. Seven years of retention is included at no additional charge to your ingestion cost. The retention period cannot be extended past 7 years.

**Note** You cannot switch an existing event data store from one-year extendable retention pricing to seven-year retention pricing.

**Retention period**

Enter the time period that you want to retain data in your event data store.

- 1 year (included with ingestion pricing at no additional charge)**  
 3 years  
 10 years (maximum)  
 Custom period

**Encryption** [Info](#)

By default, your data is encrypted with a KMS key that AWS owns and manages for you. To choose a different key, customize your encryption settings.

- Use my own AWS KMS key

8. (Optional) Wenn Sie Ihre Ereignisdaten mit Amazon Athena abfragen möchten, wählen Sie Aktivieren in Lake-Abfrageverbund. Mit Verbund können Sie die mit einem Ereignisdatenspeicher verbundenen Metadaten im AWS Glue [-Datenkatalog](#) einsehen und mit Amazon Athena SQL-Abfragen zu den Ereignisdaten durchführen. Anhand der im AWS Glue Datenkatalog gespeicherten Tabellenmetadaten weiß die Athena-Abfrage-Engine, wie die Daten, die Sie abfragen möchten, gesucht, gelesen und verarbeitet werden. Weitere Informationen finden Sie unter [Verbund für einen Ereignisdatenspeicher erstellen](#).

Wählen Sie Aktivieren und gehen Sie wie folgt vor, um Lake-Abfrageverbund zu aktivieren:

- a. Wählen Sie aus, ob Sie eine neue Rolle erstellen oder eine vorhandene IAM-Rolle verwenden möchten. [AWS Lake Formation](#) verwendet diese Rolle, um die Berechtigungen für den Verbundereignisdatenspeicher zu verwalten. Wenn Sie mit der CloudTrail Konsole eine neue Rolle erstellen, CloudTrail wird automatisch eine Rolle mit den erforderlichen Berechtigungen erstellt. Wenn Sie eine bestehende Rolle auswählen, stellen Sie sicher, dass die Richtlinie für die Rolle die [erforderlichen Mindestberechtigungen](#) vorsieht.
  - b. Wenn Sie eine neue Rolle erstellen, geben Sie einen Namen zur Identifizierung der Rolle ein.
  - c. Wenn Sie eine bestehende Rolle verwenden, wählen Sie die Rolle aus, die Sie verwenden möchten. Die Rolle muss in Ihrem Konto vorhanden sein.
9. (Optional) Fügen Sie unter Tags ein oder mehrere benutzerdefinierte Tags (Schlüssel-Wert-Paare) zu Ihrem Ereignisdatenspeicher hinzu. Mithilfe von Tags können Sie Ihre CloudTrail Ereignisdatenspeicher identifizieren. Sie könnten beispielsweise ein Tag mit dem Namen **stage** und dem Wert **prod** anfügen. Sie können Tags verwenden, um den Zugriff auf Ihren Ereignisdatenspeicher einzuschränken. Sie können Tags auch verwenden, um die Abfrage- und Aufnahmekosten für Ihren Ereignisdatenspeicher zu verfolgen.

Informationen dazu, wie Sie mithilfe von Tags Kosten nachverfolgen, finden Sie unter [Erstellen von benutzerdefinierten Kostenzuweisungs-Tags für CloudTrail Lake-Event-Datenspeicher](#). Informationen darüber, wie Sie IAM-Richtlinien verwenden, um den Zugriff auf einen Ereignisdatenspeicher basierend auf Tags zu autorisieren, finden Sie unter [Beispiele: Verweigern des Zugriffs zum Erstellen oder Löschen von Ereignisdatenspeichern basierend auf Tags](#). Informationen darüber, wie Sie Tags verwenden können AWS, finden Sie unter [Tagging Your AWS Resources User Guide](#) im Tagging AWS Resources User Guide.

**Tags - optional** [Info](#)

You can add one or more tags to help you manage and organize your resources, including event data stores.

Key	Value - optional	
<input type="text" value="stage"/>	<input type="text" value="prod"/>	<input type="button" value="Remove"/>
<input type="button" value="Add tag"/>		

You can add 49 more tags

10. Wählen Sie Next (Weiter) aus, um den Ereignisdatenspeicher zu konfigurieren.
11. Behalten Sie auf der Seite Ereignisse auswählen die Standardauswahl für den Ereignistyp bei.

**Event type** [Info](#)

Choose the type of events you want to add to your event data store. [Additional charges apply](#)

**Choose event types**

**AWS events**  
Capture operations performed on or within your AWS resources.

**Events from integrations**  
Create an integration to get events that are logged by applications outside of your AWS resources.

**Specify the type of AWS events**

**CloudTrail events**  
CloudTrail events provide a record of activity in an AWS account.


**CloudTrail Insights events**  
Insights events help identify unusual activity, errors, or user behavior in your account.

**Configuration items**  
Configuration items show changes made to the configuration of a resource, and show the resource's compliance status.

12. Für CloudTrail Ereignisse lassen wir die Option Management-Ereignisse ausgewählt und wählen Trail-Ereignisse kopieren. In diesem Beispiel machen wir uns keine Gedanken über die Ereignistypen, da wir den Ereignisdatenspeicher nur zur Analyse vergangener Ereignisse verwenden und keine zukünftigen Ereignisse aufnehmen.

Wenn Sie einen Ereignisdatenspeicher erstellen, der einen vorhandenen Trail ersetzen soll, wählen Sie dieselben Ereignisselektoren wie für Ihren Trail aus, um sicherzustellen, dass der Ereignisdatenspeicher die gleiche Ereignisabdeckung hat.


### CloudTrail events [Info](#)

- Management events**  
Capture management operations performed on your AWS resources.
- Data events**  
Log the resource operations performed on or within a resource.
- Copy trail events**  
Copy CloudTrail events logged in your trails or from S3 buckets.
- Enable for all accounts in my organization**  
To review accounts in your organization, open AWS Organizations. [See all accounts](#) 

▼ **Additional settings**

- Include only the current region (us-east-1) in my event data store**
- Ingest events | [Info](#)**  
Your event data store starts ingesting events when created.

13. Wählen Sie Für alle Konten in meiner Organisation aktivieren aus, wenn es sich um einen Ereignisdatenspeicher für eine Organisation handelt. Diese Option kann nur geändert werden, wenn Sie Konten in AWS Organizations konfiguriert haben.

 **Note**

Wenn Sie einen Ereignisdatenspeicher einer Organisation erstellen, müssen Sie mit dem Verwaltungskonto der Organisation angemeldet sein, da Trail-Ereignisse nur mit dem Verwaltungskonto in den Ereignisdatenspeicher einer Organisation kopiert werden können.

14. Für Zusätzliche Einstellungen deaktivieren wir die Option Ereignisse aufnehmen, da wir in diesem Beispiel nicht möchten, dass der Ereignisdatenspeicher zukünftige Ereignisse aufnimmt, da wir nur daran interessiert sind, die kopierten Ereignisse abzufragen. Standardmäßig sammelt ein Ereignisdatenspeicher Ereignisse für alle AWS-Regionen und beginnt, Ereignisse zu erfassen, sobald er erstellt wird.
15. Für Verwaltungsereignisse behalten wir die Standardeinstellungen bei.

## Management events [Info](#)

Management events show information about management operations performed on resources in your AWS account.

### API activity

Choose the activities you want to log.

- Read  Write
- Exclude AWS KMS events
- Exclude Amazon RDS Data API events
- Enable Insights  
Identify unusual activity, errors, or user behavior in your account.

16. Führen Sie im Bereich Trail-Ereignisse kopieren die folgenden Schritte aus.
  - a. Wählen Sie den Trail aus, die Sie kopieren möchten. In diesem Beispiel wählen wir einen Trail mit dem Namen *Verwaltungseignisse* aus.

Standardmäßig werden CloudTrail nur CloudTrail Ereignisse kopiert, die im CloudTrail Präfix des S3-Buckets und die Präfixe innerhalb des CloudTrail Präfixes enthalten sind, und überprüft keine Präfixe für andere Dienste. AWS Wenn Sie CloudTrail Ereignisse kopieren möchten, die in einem anderen Präfix enthalten sind, wählen Sie S3-URI eingeben und dann S3 durchsuchen, um zum Präfix zu wechseln. Wenn der S3-Quell-Bucket für den Trail einen KMS-Schlüssel für die Datenverschlüsselung verwendet, stellen Sie sicher, dass die KMS-Schlüsselrichtlinie das Entschlüsseln der Daten zulässt CloudTrail . Wenn Ihr S3-Quell-Bucket mehrere KMS-Schlüssel verwendet, müssen Sie die Richtlinien für jeden Schlüssel aktualisieren, damit CloudTrail die Daten im Bucket entschlüsselt werden können. Weitere Informationen zum Aktualisieren der KMS-Schlüssel-Richtlinie finden Sie unter [KMS-Schlüsselrichtlinie zum Entschlüsseln von Daten im S3-Quell-Bucket](#).

- b. Wählen Sie einen Zeitraum für das Kopieren der Ereignisse aus. CloudTrail überprüft das Präfix und den Namen der Protokolldatei, um sicherzustellen, dass der Name ein Datum zwischen dem ausgewählten Start- und Enddatum enthält, bevor versucht wird, Trail-Ereignisse zu kopieren. Sie können einen Relative range (Relativen Bereich) oder einen Absolute range (Absoluten Bereich) wählen. Um zu vermeiden, dass Ereignisse zwischen dem Quell-Trail und dem Zielergebnisdatenspeicher dupliziert werden, wählen Sie einen Zeitraum aus, der vor der Erstellung des Ereignisdatenspeichers liegt.

- Wenn Sie Relativer Bereich wählen, können Sie wählen, ob Ereignisse kopiert werden sollen, die in den letzten 6 Monaten, 1 Jahr, 2 Jahren, 7 Jahren oder in einem benutzerdefinierten Bereich protokolliert wurden. CloudTrail kopiert die Ereignisse, die innerhalb des ausgewählten Zeitraums protokolliert wurden.
- Wenn Sie „Absoluter Bereich“ wählen, können Sie ein bestimmtes Start- und Enddatum wählen. CloudTrail kopiert die Ereignisse, die zwischen dem ausgewählten Start- und Enddatum aufgetreten sind.

In diesem Beispiel wählen wir Absoluter Bereich und den gesamten Monat Juni aus.

The screenshot displays the date range selection interface in the AWS CloudTrail console. At the top, there are two tabs: "Relative range" and "Absolute range", with "Absolute range" selected. Below the tabs, there are navigation arrows and the months "June 2023" and "July 2023". A calendar grid shows the days of the month. The dates from June 1st to June 30th are highlighted in blue, indicating the selected range. Below the calendar, there are four input fields for date and time selection: "Start date" (2023/06/01), "Start time" (00:00:00), "End date" (2023/06/30), and "End time" (23:59:59). At the bottom, there are three buttons: "Clear and dismiss", "Cancel", and "Apply".

- c. Wählen Sie für Permissions (Berechtigungen) unter den folgenden IAM-Rollenoptionen aus. Wenn Sie eine vorhandene IAM-Rolle auswählen, stellen Sie sicher, dass die IAM-Rollenrichtlinie die erforderlichen Berechtigungen bereitstellt. Weitere Informationen zum Aktualisieren der IAM-Rollenberechtigungen finden Sie unter [IAM-Berechtigungen zum Kopieren von Trail-Ereignissen](#).

- Wählen Sie **Create a new role (recommended)** (Erstellen Sie eine neue Rolle (empfohlen)), um eine neue IAM-Rolle zu erstellen. Geben Sie unter IAM-Rollennamen eingeben einen Namen für die Rolle ein. CloudTrail erstellt automatisch die erforderlichen Berechtigungen für diese neue Rolle.
- Wählen Sie **Eine benutzerdefinierte IAM-Rolle verwenden** (Use a custom IAM role), um eine benutzerdefinierte IAM-Rolle zu verwenden, die nicht aufgeführt ist. Geben Sie für Enter IAM role ARN (IAM-Rollen-ARN eingeben) den IAM-ARN ein.
- Wählen Sie eine vorhandene IAM-Rolle aus der Drop-down-Liste aus.

In diesem Beispiel wählen wir **Neue Rolle erstellen (empfohlen)** und geben den Namen **copy-trail-events** an.

### Copy existing trail events [Info](#)

Choose trail event source

management-events ▼

S3 location of CloudTrail data (S3 URI)

s3://aws-cloudtrail-logs- /AWSLogs/ /CloudTr

Specify a time range of events

2023-06-01T00:00:00-05:00 — 2023-06-30T23:59:59-05:00

**i** All CloudTrail events in your event source are imported, regardless of your event data store's configuration.

Choose IAM role

Create a new role (recommended) ▼

Enter IAM role name

The new role name is prepended with CloudTrailLake-us-east-1-

copy-trail-events

▶ **Permission policies**



17. Wählen Sie Next (Weiter) aus, um Ihre Auswahl zu überprüfen.
18. Überprüfen Sie auf der Seite Prüfen und erstellen Ihre Auswahl. Wählen Sie Bearbeiten aus, um Änderungen am Schema vorzunehmen. Wenn Sie bereit sind, den Ereignisdatenspeicher zu erstellen, wählen Sie Ereignisdatenspeicher erstellen aus.
19. Der neue Ereignisdatenspeicher ist in der Tabelle Ereignisdatenspeicher auf der Seite Ereignisdatenspeicher sichtbar.

Event data stores (3)					
Name	Status	All regions	All accounts	Event type	
my-management-events-eds	Enabled	Yes	No	CloudTrail events	

20. Wählen Sie den Namen des Ereignisdatenspeichers aus, um die Detailseite anzuzeigen. Auf der Detailseite werden die Details zu Ihrem Ereignisdatenspeicher und der Status der Kopie angezeigt. Der Status der Ereigniskopie wird im Bereich Status der Ereigniskopie angezeigt.

Wenn eine Trail-Ereignis-Kopie abgeschlossen ist, wird der Copy status (Kopierstatus) entweder auf Completed (Abgeschlossen) festgelegt, wenn keine Fehler aufgetreten sind, oder auf Failed (Fehlgeschlagen), wenn Fehler aufgetreten sind.

Event copy status (1) <a href="#">Info</a>					
Event log S3 location	Copy status	Copy ID	Created time	Finish time	
s3://aws-cloudtrail-logs-...	Completed	...	July 18, 2023, 15:50:06 (UTC-05:00)	July 18, 2023, 15:53:07 (UTC-05:00)	

21. Um weitere Details zur Kopie anzuzeigen, wählen Sie den Namen der Kopie in der Spalte Ereignisprotokoll-S3-Speicherort aus oder wählen Sie im Menü Aktionen die Option Details anzeigen. Weitere Informationen zum Anzeigen der Details eines Trail-Ereignisses finden Sie unter [Details zur Ereigniskopie](#).

CloudTrail > Lake > Event data stores > my-management-events-trail-events >

**Copy ID** [redacted] Refresh Actions

**Copy details** info

Event log S3 location s3://aws-cloudtrail-logs- [redacted] /AWSLogs/[redacted] /CloudTrail/	Prefixes copied 817/817 prefixes copied (0 failures)	Created time July 18, 2023, 15:50:06 (UTC-05:00)
Copy ID [redacted]	Copy status <span>Completed</span>	Finish time July 18, 2023, 16:04:51 (UTC-05:00)

**Copy failures (0)**  
Retry copying prefixes that failed to copy.

< 1 > Refresh

Event location	Error message	Error type
No failures There are currently no copy failures.		

22. Im Bereich Kopierfehler werden alle Fehler angezeigt, die beim Kopieren von Trail-Ereignissen aufgetreten sind. Wenn der Copy status (Kopierstatus) Failed (Fehlgeschlagen) lautet, beheben Sie alle Fehler, die unter Copy failures (Kopierfehler) angezeigt werden, und wählen Sie dann Retry copy (Kopie wiederholen) aus. Wenn Sie erneut versuchen, einen Kopiervorgang durchzuführen, CloudTrail wird der Kopiervorgang an der Stelle fortgesetzt, an der der Fehler aufgetreten ist.

## Verbund für einen Ereignisdatenspeicher erstellen

Durch das Zusammenführen eines Ereignisdatenspeichers können Sie die mit dem Ereignisdatenspeicher verknüpften Metadaten im AWS Glue [Datenkatalog](#) anzeigen, den Datenkatalog bei AWS Lake Formation registrieren und mithilfe von Amazon Athena SQL-Abfragen für Ihre Ereignisdaten ausführen. Anhand der im AWS Glue Datenkatalog gespeicherten Tabellenmetadaten weiß die Athena-Abfrage-Engine, wie die Daten, die Sie abfragen möchten, gesucht, gelesen und verarbeitet werden.

Sie können den Verbund mithilfe der CloudTrail Konsole oder der [EnableFederation](#) API-Operation aktivieren. AWS CLI Wenn Sie den Lake-Abfrageverbund aktivieren, werden eine verwaltete Datenbank mit dem Namen `aws:cloudtrail` (falls die Datenbank noch nicht vorhanden ist) und eine verwaltete Verbundtabelle im AWS Glue Datenkatalog CloudTrail erstellt. Die ID des Ereignisdatenspeichers wird für den Tabellennamen verwendet. CloudTrail registriert den ARN der Verbundrolle und den Ereignisdatenspeicher in [AWS Lake Formation](#), dem Dienst, der für die detaillierte Zugriffskontrolle der Verbundressourcen im AWS Glue Datenkatalog verantwortlich ist.

Um Lake-Abfrageverbund zu aktivieren, müssen Sie eine neue IAM-Rolle erstellen oder eine vorhandene Rolle auswählen. Lake Formation verwendet diese Rolle, um Berechtigungen für den Verbundereignisdatenspeicher zu verwalten. Wenn Sie mithilfe der CloudTrail Konsole eine neue Rolle erstellen, CloudTrail werden automatisch die erforderlichen Berechtigungen für die Rolle erstellt. Wenn Sie eine bestehende Rolle auswählen, stellen Sie sicher, dass die Rolle die [Mindestberechtigungen](#) vorsieht.

Sie können den Verbund mithilfe der CloudTrail Konsole oder der [DisableFederation](#) API-Operation deaktivieren. AWS CLI Wenn Sie den Verbund CloudTrail deaktivieren, wird die Integration mit AWS Glue AWS Lake Formation, und Amazon Athena deaktiviert. Nachdem Sie den Lake-Abfrageverbund deaktiviert haben, können Sie Ihre Ereignisdaten in Athena nicht mehr abfragen. Wenn Sie den Verbund deaktivieren, werden keine CloudTrail Lake-Daten gelöscht und Sie können weiterhin Abfragen in CloudTrail Lake ausführen.

Für die Zusammenführung eines CloudTrail Lake-Ereignisdatenspeichers CloudTrail fallen keine Gebühren an. Für die Ausführung von Abfragen in Amazon Athena fallen Kosten an. Weitere Informationen zur Preisgestaltung von Athena finden Sie unter [Amazon Athena – Preise](#).

## [Analysieren Sie Aktivitätsprotokolle mit AWS CloudTrail Lake und Amazon Athena](#)

### Themen

- [Überlegungen](#)
- [Erforderliche Berechtigungen für den Verbund](#)
- [Lake-Abfrageverbund aktivieren](#)
- [Lake-Abfrageverbund deaktivieren](#)
- [Verwaltung der Ressourcen von CloudTrail Lake Federation mit AWS Lake Formation](#)

### Überlegungen

Berücksichtigen Sie bei der Verbunderstellung eines Ereignisdatenspeichers die folgenden Faktoren:

- Für die Zusammenführung eines CloudTrail Lake-Event-Datenspeichers CloudTrail fallen keine Gebühren an. Für die Ausführung von Abfragen in Amazon Athena fallen Kosten an. Weitere Informationen zur Preisgestaltung von Athena finden Sie unter [Amazon Athena – Preise](#).
- Lake Formation wird verwendet, um Berechtigungen für die Verbundressourcen zu verwalten. Wenn Sie die Verbundrolle löschen oder die Berechtigungen für die Ressourcen von Lake Formation widerrufen oder AWS Glue, können Sie keine Abfragen von Athena ausführen. Weitere

Informationen zur Arbeit mit Lake Formation finden Sie unter [Verwaltung der Ressourcen von CloudTrail Lake Federation mit AWS Lake Formation](#).

- Jeder, der Amazon Athena zum Abfragen von bei Lake Formation registrierten Daten verwendet, muss über eine IAM-Berechtigungsrichtlinie verfügen, die die `lakeformation:GetDataAccess`-Aktion zulässt. Die AWS verwaltete Richtlinie: [AmazonAthenaFullAccess](#) ermöglicht diese Aktion. Wenn Sie eingebundenen Richtlinien verwenden, stellen Sie sicher, dass Sie die Berechtigungsrichtlinien aktualisieren, um diese Aktion zuzulassen. Weitere Informationen finden Sie unter [Verwalten von Lake-Formation- und Athena-Benutzerberechtigungen](#).
- Um Ansichten für Verbundtabellen in Athena zu erstellen, benötigen Sie eine andere Zieldatenbank als `aws:cloudtrail`. Das liegt daran, dass die `aws:cloudtrail` Datenbank von verwaltet wird CloudTrail.
- Um einen Datensatz in Amazon zu erstellen QuickSight, müssen Sie die Option Benutzerdefiniertes SQL verwenden wählen. Weitere Informationen finden Sie unter [Erstellen eines Datensatzes mit Amazon-Athena-Daten](#).
- Wenn der Verbund aktiviert ist, können Sie einen Ereignisdatenspeicher nicht löschen. Um einen Verbundereignisdatenspeicher zu löschen, müssen Sie zunächst den [Verbund](#) und den [Beendigungsschutz deaktivieren](#), falls dieser aktiviert ist.
- Für Ereignisdatenspeicher von Organisationen gelten die folgenden Überlegungen:
  - Nur ein einziges delegiertes Administratorkonto oder das Verwaltungskonto können den Verbund für den Ereignisdatenspeicher einer Organisation aktivieren. Andere delegierte Administratorkonten können mithilfe des [Lake-Formation-Datenfreigabefeatures](#) immer noch Informationen abfragen und austauschen.
  - Jedes delegierte Administratorkonto oder das Verwaltungskonto der Organisation können den Verbund deaktivieren.

## Erforderliche Berechtigungen für den Verbund

Bevor Sie einen Verbund des Ereignisdatenspeichers erstellen, stellen Sie sicher, dass Sie über alle erforderlichen Berechtigungen für die Verbundrolle und für die Aktivierung und Deaktivierung des Verbunds verfügen. Sie müssen die Berechtigungen für die Verbundrolle nur aktualisieren, wenn Sie eine bestehende IAM-Rolle für die Aktivierung des Verbunds auswählen. Wenn Sie mithilfe der CloudTrail Konsole eine neue IAM-Rolle erstellen möchten, CloudTrail werden alle erforderlichen Berechtigungen für die Rolle bereitgestellt.

## Themen

- [IAM-Berechtigungen für den Verbund eines Ereignisdatenspeichers](#)
- [Erforderliche Berechtigungen für das Aktivieren des Verbunds](#)
- [Erforderliche Berechtigungen für das Deaktivieren des Verbunds](#)

## IAM-Berechtigungen für den Verbund eines Ereignisdatenspeichers

Beim Aktivieren des Verbunds haben Sie die Möglichkeit, eine neue IAM-Rolle zu erstellen oder eine vorhandene IAM-Rolle zu verwenden. Wenn Sie eine neue IAM-Rolle auswählen, CloudTrail wird eine IAM-Rolle mit den erforderlichen Berechtigungen erstellt, sodass keine weiteren Maßnahmen Ihrerseits erforderlich sind.

Wenn Sie eine vorhandene Rolle auswählen, stellen Sie sicher, dass die Richtlinien der IAM-Rolle über die erforderlichen Berechtigungen verfügen, um den Verbund zu aktivieren. Dieser Abschnitt enthält Beispiele für die erforderlichen IAM-Rollenberechtigungen und Vertrauensrichtlinien.

Das folgende Beispiel enthält die Berechtigungsrichtlinie für die Verbundrolle. Geben Sie für die erste Anweisung den vollständigen ARN Ihres Ereignisdatenspeichers für Resource an.

Die zweite Aussage in dieser Richtlinie ermöglicht Lake Formation, Daten für einen mit einem KMS-Schlüssel verschlüsselten Ereignisdatenspeicher zu entschlüsseln. Ersetzen Sie *key-region*, *account-id* und *key-id* durch die Werte für Ihren KMS-Schlüssel. Sie können diese Anweisung weglassen, wenn der Ereignisdatenspeicher keinen KMS-Schlüssel für die Verschlüsselung verwendet.

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Sid": "LakeFederationEDSDataAccess",
      "Effect": "Allow",
      "Action": "cloudtrail:GetEventDataStoreData",
      "Resource": "arn:aws:cloudtrail:eds-region:account-id:eventdatastore/eds-id"
    },
    {
      "Sid": "LakeFederationKMSDecryptAccess",
      "Effect": "Allow",
      "Action": [
        "kms:Decrypt",
        "kms:GenerateDataKey"
      ]
    }
  ]
}
```

```

    ],
    "Resource": "arn:aws:kms:key-region:account-id:key/key-id"
  }
]
}

```

Im folgenden Beispiel wird die IAM-Vertrauensrichtlinie bereitgestellt, die es AWS Lake Formation ermöglicht, eine IAM-Rolle zur Verwaltung von Berechtigungen für den Verbundereignisdatenspeicher anzunehmen.

```

{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Principal": {
        "Service": "lakeformation.amazonaws.com"
      },
      "Action": "sts:AssumeRole"
    }
  ]
}

```

### Erforderliche Berechtigungen für das Aktivieren des Verbunds

Die folgende Beispielrichtlinie bietet die mindestens erforderlichen Berechtigungen, um den Verbund für einen Ereignisdatenspeicher zu aktivieren. Diese Richtlinie ermöglicht es CloudTrail, den Verbund im Ereignisdatenspeicher AWS Glue zu aktivieren, die Verbundressourcen im AWS Glue Datenkatalog zu erstellen und die Ressourcenregistrierung AWS Lake Formation zu verwalten.

```

{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Sid": "Allow CloudTrail to enable federation on the event data store",
      "Effect": "Allow",
      "Action": "cloudtrail:EnableFederation",
      "Resource": "arn:aws:cloudtrail:region:account-id:eventdatastore/eds-id"
    },
    {
      "Sid": "Allow access to the federation role",
      "Effect": "Allow",

```

```

    "Action": [
      "iam:PassRole",
      "iam:GetRole"
    ],
    "Resource": "arn:aws:iam::region:role/federation-role-name"
  },
  {
    "Sid": "Allow AWS Glue to create the federated resources in the Data
Catalog",
    "Effect": "Allow",
    "Action": [
      "glue:CreateDatabase",
      "glue:CreateTable",
      "glue:PassConnection"
    ],
    "Resource": [
      "arn:aws:glue:region:account-id:catalog",
      "arn:aws:glue:region:account-id:database/aws:cloudtrail",
      "arn:aws:glue:region:account-id:table/aws:cloudtrail/eds-id",
      "arn:aws:glue:region:account-id:connection/aws:cloudtrail"
    ]
  },
  {
    "Sid": "Allow Lake Formation to manage resource registration",
    "Effect": "Allow",
    "Action": [
      "lakeformation:RegisterResource",
      "lakeformation:DeregisterResource"
    ],
    "Resource": "arn:aws:lakeformation:region:account-id:catalog:account-id"
  }
]
}

```

## Erforderliche Berechtigungen für das Deaktivieren des Verbunds

Die folgende Beispielrichtlinie bietet die mindestens erforderlichen Ressourcen, um den Verbund für einen Ereignisdatenspeicher zu deaktivieren. Diese Richtlinie ermöglicht es, den Verbund im Ereignisdatenspeicher CloudTrail AWS Glue zu deaktivieren, die verwaltete Verbundtabelle im AWS Glue Datenkatalog zu löschen und Lake Formation die Registrierung der Verbundressource aufzuheben.

```
{
```

```

"Version": "2012-10-17",
"Statement": [
  {
    "Sid": "Allow CloudTrail to disable federation on the event data store",
    "Effect": "Allow",
    "Action": "cloudtrail:DisableFederation",
    "Resource": "arn:aws:cloudtrail:region:account-id:eventdatastore/eds-id"
  },
  {
    "Sid": "Allow AWS Glue to delete the managed federated table from the AWS
Glue Data Catalog",
    "Effect": "Allow",
    "Action": "glue:DeleteTable",
    "Resource": [
      "arn:aws:glue:region:account-id:catalog",
      "arn:aws:glue:region:account-id:database/aws:cloudtrail",
      "arn:aws:glue:region:account-id:table/aws:cloudtrail/eds-id"
    ]
  },
  {
    "Sid": "Allow Lake Formation to deregister the resource",
    "Effect": "Allow",
    "Action": "lakeformation:DeregisterResource",
    "Resource": "arn:aws:lakeformation:region:account-id:catalog:account-id"
  }
]
}

```

## Lake-Abfrageverbund aktivieren

Sie können den Lake-Abfrageverbund mithilfe der CloudTrail Konsole oder der [EnableFederation](#) API-Operation aktivieren. AWS CLI Wenn Sie den Lake-Abfrageverbund aktivieren, werden eine verwaltete Datenbank mit dem Namen `aws:cloudtrail` (falls die Datenbank noch nicht vorhanden ist) und eine verwaltete Verbundtabelle im AWS Glue Datenkatalog CloudTrail erstellt. Die ID des Ereignisdatenspeichers wird für den Tabellennamen verwendet. CloudTrail registriert den ARN der Verbundrolle und den Ereignisdatenspeicher in [AWS Lake Formation](#), dem Dienst, der für die detaillierte Zugriffskontrolle der Verbundressourcen im AWS Glue Datenkatalog verantwortlich ist.

In diesem Abschnitt wird beschrieben, wie Sie den Verbund mithilfe der CloudTrail Konsole und aktivieren. AWS CLI



## CloudTrail console

Das folgende Verfahren zeigt, wie Sie den Lake-Abfrageverbund für einen vorhandenen Ereignisdatenspeicher aktivieren.

1. Melden Sie sich bei der an AWS Management Console und öffnen Sie die CloudTrail Konsole unter <https://console.aws.amazon.com/cloudtrail/>.
2. Wählen Sie im Navigationsbereich unter Lake die Option Ereignisdatenspeicher aus.
3. Wählen Sie den Ereignisdatenspeicher, den Sie aktualisieren möchten. Diese Aktion öffnet die Detailseite des Ereignisdatenspeichers.
4. Wählen Sie in Lake-Abfrageverbund die Option Bearbeiten und dann Aktivieren aus.
5. Wählen Sie, ob Sie eine neue IAM-Rolle erstellen oder eine vorhandene Rolle verwenden möchten. Wenn Sie eine neue Rolle erstellen, CloudTrail wird automatisch eine Rolle mit den erforderlichen Berechtigungen erstellt. Wenn Sie eine bestehende Rolle verwenden, stellen Sie sicher, dass die Richtlinie für die Rolle die [erforderlichen Mindestberechtigungen](#) vorsieht.
6. Wenn Sie eine neue IAM-Rolle erstellen, geben Sie einen Namen für die Rolle ein.
7. Wenn Sie eine bestehende IAM-Rolle wählen, wählen Sie die Rolle aus, die Sie verwenden möchten. Die Rolle muss in Ihrem Konto vorhanden sein.
8. Wählen Sie Änderungen speichern aus. Der Verbundstatus ändert sich in Enabled.

## AWS CLI

Um den Verbund zu aktivieren, führen Sie den Befehl `aws cloudtrail enable-federation` aus und geben Sie die erforderlichen Parameter `--event-data-store` und `--role` ein. Geben Sie für `--event-data-store` den ARN des Ereignisdatenspeichers (oder das ID-Suffix des ARN) an. Geben Sie für `--role` den ARN für Ihre Verbundrolle an. Die Rolle muss in Ihrem Konto vorhanden sein und über die [erforderlichen Mindestberechtigungen verfügen](#).

```
aws cloudtrail enable-federation
--event-data-store arn:aws:cloudtrail:region:account-id:eventdatastore/eds-id
--role arn:aws:iam::account-id:role/federation-role-name
```

Dieses Beispiel zeigt, wie ein delegierter Administrator den Verbund für den Ereignisdatenspeicher einer Organisation aktivieren kann, indem er den ARN des Ereignisdatenspeichers im Verwaltungskonto und den ARN der Verbundrolle im delegierten Administratorkonto angibt.

```
aws cloudtrail enable-federation
--event-data-store arn:aws:cloudtrail:region:management-account-id:eventdatastore/eds-id
--role arn:aws:iam::delegated-administrator-account-id:role/federation-role-name
```

## Lake-Abfrageverbund deaktivieren

Sie können den Verbund mithilfe der CloudTrail Konsole oder der [DisableFederation](#) API-Operation deaktivieren. AWS CLI Wenn Sie den Verbund CloudTrail deaktivieren, wird die Integration mit AWS Glue AWS Lake Formation, und Amazon Athena deaktiviert. Nachdem Sie den Lake-Abfrageverbund deaktiviert haben, können Sie Ihre Ereignisdaten in Athena nicht mehr abfragen. Wenn Sie den Verbund deaktivieren, werden keine CloudTrail Lake-Daten gelöscht und Sie können weiterhin Abfragen in CloudTrail Lake ausführen.

In diesem Abschnitt wird beschrieben, wie Sie den Verbund mithilfe der CloudTrail Konsole und deaktivieren AWS CLI.

### CloudTrail console

Das folgende Verfahren zeigt, wie Sie den Lake-Abfrageverbund für einen vorhandenen Ereignisdatenspeicher deaktivieren.

1. Melden Sie sich bei der an AWS Management Console und öffnen Sie die CloudTrail Konsole unter <https://console.aws.amazon.com/cloudtrail/>.
2. Wählen Sie im Navigationsbereich unter Lake die Option Ereignisdatenspeicher aus.
3. Wählen Sie den Ereignisdatenspeicher, den Sie aktualisieren möchten. Diese Aktion öffnet die Detailseite des Ereignisdatenspeichers.
4. Wählen Sie in Lake-Abfrageverbund die Option Bearbeiten und dann Deaktivieren aus.
5. Wählen Sie Änderungen speichern aus. Der Verbundstatus ändert sich in Disabled.

### AWS CLI

Führen Sie den Befehl `aws cloudtrail disable-federation` aus, um den Verbund im Ereignisdatenspeicher zu deaktivieren. Der Ereignisdatenspeicher wird durch `--event-data-store` angegeben, der einen Ereignisdatenspeicher-ARN oder das ID-Suffix des ARN akzeptiert.

```
aws cloudtrail disable-federation
```

```
--event-data-store arn:aws:cloudtrail:region:account-id:eventdatastore/eds-id
```

**Note**

Wenn es sich um den Ereignisdatenspeicher einer Organisation handelt, geben Sie die Konto-ID für das Verwaltungskonto an.

## Verwaltung der Ressourcen von CloudTrail Lake Federation mit AWS Lake Formation

Wenn Sie einen Ereignisdatenspeicher verbinden, registriert CloudTrail die Verbundrolle ARN und den Ereignisdatenspeicher in dem Dienst AWS Lake Formation, der für die detaillierte Zugriffskontrolle der Verbundressourcen im Datenkatalog verantwortlich ist. AWS Glue In diesem Abschnitt wird beschrieben, wie Sie Lake Formation verwenden können, um die Ressourcen der CloudTrail Lake Federation zu verwalten.

Wenn Sie den Verbund aktivieren, werden die folgenden Ressourcen im AWS Glue Datenkatalog CloudTrail erstellt.

- **Verwaltete Datenbank** — CloudTrail erstellt eine Datenbank mit dem Namen `aws:cloudtrail` pro Konto. CloudTrail verwaltet die Datenbank. Sie können die Datenbank nicht löschen oder ändern AWS Glue.
- **Verwaltete Verbundtabelle** — CloudTrail erstellt eine Tabelle für jeden föderierten Ereignisdatenspeicher und verwendet die ID des Ereignisdatenspeichers als Tabellennamen. CloudTrail verwaltet die Tabellen. Sie können die Tabellen nicht löschen oder ändern AWS Glue. Um eine Tabelle zu löschen, müssen Sie den [Verbund im Ereignisdatenspeicher deaktivieren](#).

### Steuern des Zugriffs auf Verbundressourcen

Sie können eine von zwei Berechtigungsmethoden verwenden, um den Zugriff auf die verwaltete Datenbank und die Tabellen zu steuern.

- **Nur IAM-Zugriffskontrolle** – Bei der reinen IAM-Zugriffskontrolle erhalten alle Benutzer des Kontos mit den erforderlichen IAM-Berechtigungen Zugriff auf alle Datenkatalogressourcen. Informationen zur AWS Glue Funktionsweise mit IAM finden Sie unter [Wie AWS Glue funktioniert mit IAM](#).

In der Lake-Formation-Konsole wird diese Methode als Nur IAM-Zugriffskontrolle verwenden angezeigt.

**Note**

Wenn Sie Datenfilter erstellen und andere Lake-Formation-Features verwenden möchten, müssen Sie die Lake-Formation-Zugriffskontrolle verwenden.

- Lake-Formation-Zugriffskontrolle – Diese Methode bietet die folgenden Vorteile.
  - Sie können die Sicherheit auf Spalten-, Zeilen- und Zellenebene implementieren, indem Sie [Datenfilter](#) erstellen.
  - Datenbank und Tabellen sind nur für Lake-Formation-Administratoren und Ersteller der Datenbank und der Ressourcen sichtbar. Wenn ein anderer Benutzer Zugriff auf diese Ressourcen benötigt, müssen Sie den [Zugriff mithilfe von Lake-Formation-Berechtigungen explizit gewähren](#).

Weitere Informationen zur differenzierten Zugriffskontrolle finden Sie unter [Methoden für die differenzierte Zugriffskontrolle](#).

### Ermitteln der Berechtigungsmethode für eine Verbundressource

Wenn Sie den Verbund zum ersten Mal aktivieren, werden mithilfe Ihrer Lake Formation Data Lake-Einstellungen eine verwaltete Datenbank und eine verwaltete Verbundtabelle CloudTrail erstellt.

Nachdem Sie den Verbund CloudTrail aktiviert haben, können Sie überprüfen, welche Berechtigungsmethode Sie für die verwaltete Datenbank und die verwaltete Verbundtabelle verwenden, indem Sie die Berechtigungen für diese Ressourcen überprüfen. Wenn die Einstellung ALL (Super) auf IAM\_ALLOWED\_PRINCIPALS für die Ressource vorhanden ist, wird die Ressource ausschließlich über IAM-Berechtigungen verwaltet. Wenn die Einstellung fehlt, wird die Ressource über Lake-Formation-Berechtigungen verwaltet. Weitere Informationen zu Lake-Formation-Berechtigungen finden Sie in der [Referenz zu Lake-Formation-Berechtigungen](#).

Die Berechtigungsmethode für die verwaltete Datenbank und die verwaltete Verbundtabelle kann unterschiedlich sein. Wenn Sie beispielsweise die Werte für die Datenbank und die Tabelle überprüfen, könnten Sie Folgendes sehen:

- Für die Datenbank ist der Wert, der ALL (Super) auf IAM\_ALLOWED\_PRINCIPALS zuweist, in den Berechtigungen enthalten, was darauf hinweist, dass Sie nur die IAM-Zugriffskontrolle für die Datenbank verwenden.

- Für die Tabelle ist der Wert, der ALL (Super) auf IAM\_ALLOWED\_PRINCIPALS zuweist, nicht vorhanden, was auf eine Zugriffskontrolle durch Lake-Formation-Berechtigungen hinweist.

Sie können jederzeit zwischen den Zugriffsmethoden wechseln, indem Sie die Berechtigung ALL (Super) auf IAM\_ALLOWED\_PRINCIPALS für eine beliebige Verbundressource in Lake Formation hinzufügen oder entfernen.

### Kontoübergreifendes Teilen mit Lake Formation

In diesem Abschnitt wird beschrieben, wie Sie mithilfe von Lake Formation eine verwaltete Datenbank und eine verwaltete Verbundtabelle für mehrere Konten gemeinsam nutzen können.

Gehen Sie wie folgt vor, um eine verwaltete Datenbank für mehrere Konten gemeinsam zu nutzen:

1. Aktualisieren Sie die Version für die [kontoübergreifende gemeinsame Nutzung von Daten](#) auf Version 4.
2. Entfernen die Berechtigungen Super auf IAM\_ALLOWED\_PRINCIPALS aus der Datenbank, falls vorhanden, um zur Lake-Formation-Zugriffskontrolle zu wechseln.
3. Erteilen Sie dem externen Konto in der Datenbank Describe-Berechtigungen.
4. Wenn eine Datenkatalogressource mit Ihnen gemeinsam genutzt wird AWS-Konto und Ihr Konto nicht derselben AWS Organisation angehört wie das gemeinsam genutzte Konto, nehmen Sie die Einladung von AWS Resource Access Manager (AWS RAM) zur gemeinsamen Nutzung der Ressource an. Weitere Informationen finden Sie unter [Eine Einladung zur gemeinsamen Nutzung einer Ressource aus dem AWS RAM annehmen](#).

Nach Abschluss dieser Schritte sollte die Datenbank für das externe Konto sichtbar sein.

Standardmäßig gewährt die gemeinsame Nutzung der Datenbank keinen Zugriff auf Tabellen in der Datenbank.

Gehen Sie wie folgt vor, um alle oder einzelne verwaltete Verbundtabellen für ein externes Konto freizugeben:

1. Aktualisieren Sie die Version für die [kontoübergreifende gemeinsame Nutzung von Daten](#) auf Version 4.
2. Entfernen die Berechtigungen Super auf IAM\_ALLOWED\_PRINCIPALS aus der Tabelle, falls vorhanden, um zur Lake-Formation-Zugriffskontrolle zu wechseln.
3. (Optional) Geben Sie beliebige [Datenfilter](#) an, um Spalten oder Zeilen einzuschränken.

4. Erteilen Sie dem externen Konto in der Tabelle Select-Berechtigungen.
5. Wenn eine Datenkatalogressource mit Ihnen geteilt wird AWS-Konto und Ihr Konto nicht in derselben AWS Organisation wie das gemeinsam genutzte Konto ist, akzeptieren Sie die Einladung von AWS Resource Access Manager (AWS RAM) zur gemeinsamen Nutzung von Ressourcen. Für eine Organisation können Sie die Einladung mithilfe der RAM-Einstellungen automatisch akzeptieren. Weitere Informationen finden Sie unter [Eine Einladung zur gemeinsamen Nutzung einer Ressource aus dem AWS RAM annehmen](#).
6. Die Tabelle sollte jetzt sichtbar sein. Um Amazon-Athena-Abfragen für diese Tabelle zu aktivieren, erstellen Sie [in diesem Konto einen Ressourcenlink](#) zur gemeinsam genutzten Tabelle.

Das Eigentümerkonto kann die gemeinsame Nutzung jederzeit widerrufen, indem es die Berechtigungen für das externe Konto von Lake Formation entfernt oder den [Verbund in deaktiviert](#). CloudTrail

## Ereignisdatenspeicher einer Organisation

Wenn Sie eine Organisation in erstellt haben AWS Organizations, können Sie einen Datenspeicher für Organisationsereignisse erstellen, der alle Ereignisse für alle Mitglieder AWS-Konten dieser Organisation protokolliert. Datenspeicher für Organisationsereignisse können für alle AWS-Regionen oder für die aktuelle Region gelten. Ereignisdatenspeicher einer Organisation können nicht zum Sammeln von Ereignissen außerhalb von AWS verwendet werden.

Sie können [einen Datenspeicher für Organisationsereignisse](#) entweder mithilfe des Verwaltungskontos oder des delegierten Administratorkontos erstellen. Wenn ein delegierter Administrator einen Ereignisdatenspeicher einer Organisation erstellt, ist der Ereignisdatenspeicher im Verwaltungskonto der Organisation vorhanden. Dieser Ansatz ist darauf zurückzuführen, dass das Verwaltungskonto das Eigentum an allen Ressourcen der Organisation behält.

Das Verwaltungskonto für eine Organisation kann einen [Ereignisdatenspeicher auf Kontoebene aktualisieren, um ihn auf eine](#) Organisation anzuwenden.

Wenn der Ereignisdatenspeicher für eine Organisation angegeben wird, wird er automatisch auf alle Mitgliedskonten der Organisation angewendet. Mitgliedskonten können den Ereignisdatenspeicher einer Organisation sehen, diesen aber weder ändern noch löschen. Standardmäßig haben Mitgliedskonten weder Zugriff auf den Ereignisdatenspeicher einer Organisation, noch können sie Abfragen in Ereignisdatenspeichern einer Organisation ausführen.

Die folgende Tabelle zeigt die Funktionen des Verwaltungskontos und der delegierten Administratorkonten innerhalb der Organisation. AWS Organizations

Funktionen	Verwaltungskonto	Delegiertes Administratorkonto
Registrieren oder entfernen Sie delegierte Administratorkonten.	Ja	Nein
Erstellen Sie einen Organisationsereignisdatenspeicher für AWS CloudTrail Ereignisse oder AWS Config Konfigurationselemente.	Ja	Ja
Insights im Ereignisdatenspeicher einer Organisation aktivieren	Ja	Nein
Ereignisdatenspeicher einer Organisation aktualisieren	Ja	Ja <sup>1</sup>
Lake-Abfrageverbund im Ereignisdatenspeicher einer Organisation aktivieren <sup>2</sup>	Ja	Ja
Lake-Abfrageverbund im Ereignisdatenspeicher einer Organisation deaktivieren	Ja	Ja
Ereignisdatenspeicher einer Organisation löschen	Ja	Ja
Trail-Ereignisse in einen Ereignisdatenspeicher kopieren	Ja	Nein
Abfragen in Ereignisdatenspeichern einer Organisation ausführen	Ja	Ja
Sehen Sie sich das CloudTrail Lake-Dashboard für einen Datenspeicher für Organisationsereignisse an.	Ja	Ja

<sup>1</sup> Nur das Verwaltungskonto kann einen Ereignisdatenspeicher einer Organisation in einen Ereignisdatenspeicher auf Kontoebene oder einen Ereignisdatenspeicher auf Kontoebene in einen Ereignisdatenspeicher der Organisation konvertieren. Diese Aktionen sind für den delegierten Administrator nicht zulässig, da Ereignisdatenspeicher von Organisationen nur im Verwaltungskonto vorhanden sind. Wenn ein Organisationsereignisdatenspeicher in einen Ereignisdatenspeicher auf Kontoebene konvertiert wird, hat nur das Verwaltungskonto Zugriff auf den Ereignisdatenspeicher. Ebenso kann nur ein Ereignisdatenspeicher auf Kontoebene im Verwaltungskonto in einen Organisationsereignisdatenspeicher konvertiert werden.

<sup>2</sup> Nur ein einziges delegiertes Administratorkonto oder das Verwaltungskonto können den Verbund für den Ereignisdatenspeicher einer Organisation aktivieren. Andere delegierte Administratorkonten können mithilfe des [Lake-Formation-Datenfreigabefeatures](#) Informationen abfragen und austauschen. Jedes delegierte Administratorkonto sowie das Verwaltungskonto der Organisation können den Verbund deaktivieren.

## Erstellen Sie einen Datenspeicher für Organisationsereignisse

Das Verwaltungskonto oder das delegierte Administratorkonto einer Organisation kann einen Datenspeicher für Organisationsereignisse erstellen, um entweder CloudTrail Ereignisse (Verwaltungsereignisse, Datenereignisse) oder AWS Config Konfigurationselemente zu sammeln.

### Note

Nur das Verwaltungskonto der Organisation kann Trail-Ereignisse in einen Ereignisdatenspeicher kopieren.

## CloudTrail console

So erstellen Sie mithilfe der Konsole einen Veranstaltungsdatspeicher für Organisationen

1. Folgen Sie den Schritten im Verfahren [Erstellen eines Ereignisdatenspeichers für CloudTrail Ereignisse](#), um einen Organisationsdatenspeicher für CloudTrail Verwaltungs- oder Datenereignisse zu erstellen.

ODER

Folgen Sie den Schritten im Verfahren [Erstellen eines Ereignisdatenspeichers für AWS Config Konfigurationselemente](#), um einen Organisationsereignisdatenspeicher für AWS Config Konfigurationselemente zu erstellen.



2. Wählen Sie auf der Seite Ereignisse auswählen die Option Für alle Konten in meiner Organisation aktivieren aus.

## AWS CLI

Um einen Datenspeicher für Organisationsereignisse zu erstellen, führen Sie den [create-event-data-store](#) Befehl aus und fügen Sie die `--organization-enabled` Option hinzu.

Der folgende AWS CLI `create-event-data-store` Beispielbefehl erstellt einen Datenspeicher für Organisationsereignisse, der alle Verwaltungsereignisse sammelt. Da Verwaltungsereignisse standardmäßig CloudTrail protokolliert werden, müssen Sie keine erweiterten Ereignisauswahlen angeben, wenn Ihr Ereignisdatenspeicher alle Verwaltungsereignisse protokolliert und keine Datenereignisse sammelt.

```
aws cloudtrail create-event-data-store --name org-management-eds --organization-enabled
```

Nachfolgend finden Sie eine Beispielantwort.

```
{
  "EventDataStoreArn": "arn:aws:cloudtrail:us-east-1:123456789012:eventdatastore/EXAMPLE6-d493-4914-9182-e52a7934b207",
  "Name": "org-management-eds",
  "Status": "CREATED",
  "AdvancedEventSelectors": [
    {
      "Name": "Default management events",
      "FieldSelectors": [
        {
          "Field": "eventCategory",
          "Equals": [
            "Management"
          ]
        }
      ]
    }
  ],
  "MultiRegionEnabled": true,
  "OrganizationEnabled": true,
  "BillingMode": "EXTENDABLE_RETENTION_PRICING",
  "RetentionPeriod": 366,
}
```

```
"TerminationProtectionEnabled": true,  
"CreatedTimestamp": "2023-11-16T15:30:50.689000+00:00",  
"UpdatedTimestamp": "2023-11-16T15:30:50.851000+00:00"  
}
```

Der nächste AWS CLI `create-event-data-store` Beispielbefehl erstellt einen Organisationsereignisdatenspeicher mit dem Namen `config-items-org-eds`, der AWS Config Konfigurationselemente sammelt. Um Konfigurationselemente zu sammeln, geben Sie `ConfigurationItem` in den erweiterten Event-Selektoren an, dass das `eventCategory` Feld „Gleich“ ist.

```
aws cloudtrail create-event-data-store --name config-items-org-eds \  
--organization-enabled \  
--advanced-event-selectors '[  
  {  
    "Name": "Select AWS Config configuration items",  
    "FieldSelectors": [  
      { "Field": "eventCategory", "Equals": ["ConfigurationItem"] }  
    ]  
  }  
]'
```

Wenden Sie einen Ereignisdatenspeicher auf Kontoebene auf eine Organisation an

Das Verwaltungskonto der Organisation kann einen Ereignisdatenspeicher auf Kontoebene konvertieren, um ihn auf eine Organisation anzuwenden.

#### CloudTrail console

Um einen Ereignisdatenspeicher auf Kontoebene mithilfe der Konsole zu aktualisieren

1. [Melden Sie sich bei der an AWS Management Console und öffnen Sie die CloudTrail Konsole unter https://console.aws.amazon.com/cloudtrail/.](https://console.aws.amazon.com/cloudtrail/)
2. Wählen Sie im Navigationsbereich unter Lake die Option Ereignisdatenspeicher aus.
3. Wählen Sie den Ereignisdatenspeicher, den Sie aktualisieren möchten. Diese Aktion öffnet die Detailseite des Ereignisdatenspeichers.
4. Wählen Sie unter Allgemeine Details Bearbeiten aus.
5. Wählen Sie „Für alle Konten in meiner Organisation aktivieren“.

## 6. Wählen Sie Änderungen speichern aus.

Weitere Informationen zum Aktualisieren eines Ereignisdatenspeichers finden Sie unter [Aktualisieren Sie einen Ereignisdatenspeicher mit der Konsole](#).

### AWS CLI

Um einen Ereignisdatenspeicher auf Kontoebene so zu aktualisieren, dass er für eine Organisation gilt, führen Sie den [update-event-data-store](#) Befehl aus und fügen Sie die Option hinzu. `--organization-enabled`

```
aws cloudtrail update-event-data-store --region us-east-1 \  
--organization-enabled \  
--event-data-store arn:aws:cloudtrail:us-east-1:123456789012:eventdatastore/EXAMPLE-  
f852-4e8f-8bd1-bcf6cEXAMPLE
```

Weitere Informationen finden Sie auch unter

- [Delegierte Administratoren einer Organisation](#)
- [Fügen Sie einen delegierten Administrator hinzu CloudTrail](#)
- [Entfernen Sie einen CloudTrail delegierten Administrator](#)

## Erstellen Sie eine Integration mit einer Ereignisquelle außerhalb von AWS

Sie können CloudTrail damit Benutzeraktivitätsdaten aus beliebigen Quellen in Ihren Hybridumgebungen protokollieren und speichern, z. B. interne oder SaaS-Anwendungen, die vor Ort oder in der Cloud gehostet werden, virtuelle Maschinen oder Container. Sie können diese Daten speichern, darauf zugreifen, analysieren, Fehler beheben und Maßnahmen ergreifen, ohne mehrere Protokollaggregatoren und Berichtstools verwalten zu müssen.

Aktivitätsereignisse aus AWS anderen Quellen nutzen Kanäle, um Ereignisse von externen Partnern, die mit Ihnen zusammenarbeiten CloudTrail, oder aus Ihren eigenen Quellen nach CloudTrail Lake zu bringen. Wenn Sie einen Kanal erstellen, wählen Sie einen oder mehrere Ereignisdatenspeicher aus, um Ereignisse zu speichern, die von der Kanalquelle stammen. Sie können die Zielergebnisdatenspeicher für einen Kanal nach Bedarf ändern, sofern die Zielergebnisdatenspeicher so eingestellt sind, dass sie `eventCategory="ActivityAuditLog"`

Ereignisse protokollieren. Wenn Sie einen Kanal für Ereignisse eines externen Partners erstellen, stellen Sie dem Partner oder der Quellanwendung einen Kanal-ARN zur Verfügung. Die dem Kanal beigefügte Ressourcenrichtlinie ermöglicht es der Quelle, Ereignisse über den Kanal zu übertragen. Wenn der Kanal keine Ressourcenrichtlinie hat, kann nur der Kanalbesitzer die `PutAuditEvents`-API auf dem Kanal aufrufen.

CloudTrail hat mit vielen Anbietern von Eventquellen zusammengearbeitet, wie Okta und LaunchDarkly. Wenn Sie eine Integration mit einer externen Eventquelle erstellen, können Sie einen dieser Partner als Ihre Eventquelle wählen oder eine benutzerdefinierte Integration wählen, um Ereignisse aus Ihren eigenen Quellen in diese zu integrieren. CloudTrail Pro Quelle ist maximal ein Kanal zulässig.

Es gibt zwei Arten von Integrationen: direkt und Lösung. Bei direkten Integrationen ruft der Partner die `PutAuditEvents` API auf, um Ereignisse an den Event-Datenspeicher für Ihr AWS Konto zu übermitteln. Bei Lösungsintegrationen wird die Anwendung in Ihrem AWS Konto ausgeführt und die Anwendung ruft die `PutAuditEvents` API auf, um Ereignisse an den Ereignisdatenspeicher für Ihr AWS Konto zu übermitteln.

Auf der Seite Integrations (Integrationen) können Sie die Registerkarte Available sources (Verfügbare Quellen) wählen, um den Integration type (Integrationstyp) für Partner anzuzeigen.

The screenshot displays the 'Browse available sources (18)' section in the AWS CloudTrail console. It features a search bar with the placeholder text 'Find sources' and a pagination control showing '1' of 18 items. Below the search bar, three integration cards are visible:

- My custom integration:** Description: 'Add an integration with any application, container, virtual machine, database, or on-premises component that generates events compatible with the CloudTrail event schema.' Integration Type: 'Solution'. Button: 'Add Integration'.
- Cloud Storage Security:** Description: 'Cloud Storage Security (CSS) provides antivirus and data classification services. Audit CSS events such as problem file discovery and bucket configuration changes in CloudTrail with this integration. [Learn more](#)' Integration Type: 'Solution'. Button: 'Add Integration'.
- Clumio:** Description: 'This app allows you to seamlessly integrate your Clumio Audit logs directly into CloudTrail Lake. [Learn more](#)'. Integration Type: 'Direct' (highlighted with a red box). Button: 'Add integration'.

Erstellen Sie zunächst eine Integration, um Ereignisse von Partnern oder anderen Anwendungsquellen mithilfe der CloudTrail Konsole zu protokollieren.

## Themen

- [Erstellen Sie mit der Konsole eine Integration mit einem CloudTrail Partner](#)
- [Erstellen Sie eine benutzerdefinierte Integration mit der Konsole](#)
- [Erstellen, aktualisieren und verwalten Sie CloudTrail Lake-Integrationen mit dem AWS CLI](#)
- [Zusätzliche Informationen über Integrationspartner](#)
- [CloudTrail Ereignisschema für Lake Integrations](#)

## Erstellen Sie mit der Konsole eine Integration mit einem CloudTrail Partner

Wenn Sie eine Integration mit einer externen Eventquelle erstellen AWS, können Sie einen dieser Partner als Ihre Eventquelle auswählen. Wenn Sie eine Integration CloudTrail mit einer Partneranwendung erstellen, benötigt der Partner den Amazon-Ressourcennamen (ARN) des Kanals, den Sie in diesem Workflow erstellen, um Ereignisse zu senden CloudTrail. Nachdem Sie die Integration erstellt haben, beenden Sie die Konfiguration der Integration, indem Sie den Anweisungen des Partners folgen, um dem Partner den erforderlichen Kanal-ARN zur Verfügung zu stellen. Die Integration beginnt mit der Aufnahme von Partnerereignissen, CloudTrail nachdem der Partner den PutAuditEvents Kanal der Integration aufgerufen hat.

1. Melden Sie sich bei der an AWS Management Console und öffnen Sie die CloudTrail Konsole unter <https://console.aws.amazon.com/cloudtrail/>.
2. Wählen Sie im Navigationsbereich unter Lake die Option Integrationen aus.
3. Geben Sie auf der Seite Integration hinzufügen einen Namen für Ihren Kanal ein. Der Name kann eine Länge von 3–128 Zeichen haben. Namen dürfen nur Buchstaben, Zahlen, Punkte, Unterstriche und Schrägstriche enthalten.
4. Wählen Sie die Partneranwendungsquelle aus, von der Sie Ereignisse abrufen möchten. Wenn Sie Ereignisse aus Ihren eigenen Anwendungen integrieren, die On-Premises oder in der Cloud gehostet werden, wählen Sie My custom integration (Meine benutzerdefinierte Integration).
5. Wählen Sie unter Event delivery location (Ereignisübermittlungsort) aus, ob dieselben Aktivitätsereignisse in vorhandenen Ereignisdatenspeichern protokolliert werden sollen, oder ob Sie einen neuen Ereignisdatenspeicher erstellen möchten.

Wenn Sie einen neuen Ereignisdatenspeicher erstellen, geben Sie einen Namen für den Ereignisdatenspeicher ein, wählen Sie die Preisoption und geben Sie die Aufbewahrungsdauer in Tagen an. Der Ereignisdatenspeicher behält Ereignisdaten für die angegebene Anzahl von Tagen bei.

Wenn Sie Aktivitätsereignisse in einem oder mehreren vorhandenen Ereignisdatenspeichern protokollieren möchten, wählen Sie die Ereignisdatenspeicher aus der Liste aus. Die Ereignisdatenspeicher können nur Aktivitätsereignisse enthalten. Der Ereignistyp in der Konsole muss Events from integrations (Ereignisse aus Integrationen) sein. In der API muss der `eventCategory`-Wert `ActivityAuditLog` sein.

6. Konfigurieren Sie unter Resource policy (Ressourcenrichtlinie) die Ressourcenrichtlinie für den Kanal der Integration. Ressourcenbasierte Richtlinien sind JSON-Richtliniendokumente, die angeben, welche Aktionen ein bestimmter Prinzipal unter welchen Bedingungen für die Ressource ausführen kann. Die Konten, die in der Ressourcenrichtlinie als Prinzipale definiert sind, können die `PutAuditEvents`-API aufrufen, um Ereignisse an Ihren Kanal zu senden. Der Ressourcenbesitzer hat impliziten Zugriff auf die Ressource, sofern seine IAM-Richtlinie die `cloudtrail-data:PutAuditEvents`-Aktion zulässt.

Die für die Richtlinie erforderlichen Informationen werden durch den Integrationstyp bestimmt. Bei einer Direction-Integration CloudTrail werden automatisch die AWS Konto-IDs des Partners hinzugefügt und Sie müssen die vom Partner bereitgestellte eindeutige externe ID eingeben. Für eine Lösungsintegration müssen Sie mindestens eine AWS Konto-ID als Principal angeben und können optional eine externe ID eingeben, um zu verhindern, dass Ihr Stellvertreter verwirrt wird.

#### Note

Wenn Sie keine Ressourcenrichtlinie für den Kanal erstellen, kann nur der Kanalbesitzer die `PutAuditEvents`-API auf dem Kanal aufrufen.

- a. Für eine direkte Integration geben Sie die von Ihrem Partner bereitgestellte externe ID ein. Der Integrationspartner stellt eine eindeutige externe ID zur Verfügung, z. B. eine Konto-ID oder eine zufällig generierte Zeichenfolge, die für die Integration verwendet wird, um zu verhindern, dass der Stellvertreter verwirrt wird. Der Partner ist für die Erstellung und Bereitstellung einer eindeutigen externen ID verantwortlich.

Sie können [How to find this? \(Wie finde ich das?\)](#) verwenden, um die Dokumentation des Partners einzusehen, in der beschrieben wird, wie Sie die externe ID finden.

External ID

Enter the unique account identifier provided by Nordcloud. [How to find this?](#) 

**Note**

Wenn die Ressourcenrichtlinie eine externe ID enthält, müssen alle Aufrufe der PutAuditEvents-API die externe ID enthalten. Wenn die Richtlinie jedoch keine externe ID definiert, kann der Partner die PutAuditEvents-API trotzdem aufrufen und einen externalId-Parameter angeben.

- b. Für eine Lösungsintegration wählen Sie **AWS Konto hinzufügen** aus, um eine AWS Konto-ID anzugeben, die der Richtlinie als Prinzipal hinzugefügt werden soll.
7. (Optional) Im Bereich **Tags** können Sie bis zu 50 Tag-Schlüssel- und Wertepaare hinzufügen, um den Zugriff auf Ihren Ereignisdatenspeicher und -kanal zu identifizieren, zu sortieren und zu steuern. Weitere Informationen darüber, wie Sie IAM-Richtlinien verwenden, um den Zugriff auf einen Ereignisdatenspeicher basierend auf Tags zu autorisieren, finden Sie unter [Beispiele: Verweigern des Zugriffs zum Erstellen oder Löschen von Ereignisdatenspeichern basierend auf Tags](#). Weitere Informationen darüber, wie Sie Tags verwenden können AWS, finden Sie unter [Tagging AWS Resources](#) in der Allgemeine AWS-Referenz.
8. Wenn Sie bereit sind, die neue Integration zu erstellen, wählen Sie **Integration hinzufügen**. Es gibt keine Bewertungsseite. CloudTrail erstellt die Integration, aber Sie müssen der Partneranwendung den Channel Amazon Resource Name (ARN) zur Verfügung stellen. Anweisungen zur Bereitstellung des Kanal-ARN für die Partneranwendung finden Sie auf der Website mit der Partnerdokumentation. Um weitere Informationen zu erhalten, wählen Sie auf der Registerkarte **Available sources (Verfügbare Quellen)** der Seite **Integrations (Integrationen)** den Link **Learn more (Weitere Informationen)** für den Partner aus, um die Seite des Partners in AWS Marketplace zu öffnen.

Um die Einrichtung für Ihre Integration abzuschließen, stellen Sie den Kanal-ARN für den Partner oder die Quellanwendung zur Verfügung. Je nach Integrationstyp führen entweder Sie, der Partner oder die Anwendung die PutAuditEvents-API aus, um Aktivitätsereignisse an den Ereignisdatenspeicher für Ihr AWS -Konto zu übermitteln. Nachdem Ihre Aktivitätsereignisse übermittelt wurden, können Sie CloudTrail Lake verwenden, um die in Ihren Anwendungen protokollierten Daten zu suchen, abzufragen und zu analysieren. Ihre Ereignisdaten enthalten Felder, die der Nutzlast für CloudTrail Ereignisse entsprechen, z. B. `eventVersion`, `eventSource`, und `userIdentity`.

## Erstellen Sie eine benutzerdefinierte Integration mit der Konsole

Sie können CloudTrail damit Benutzeraktivitätsdaten aus beliebigen Quellen in Ihren Hybridumgebungen protokollieren und speichern, z. B. interne oder SaaS-Anwendungen, die vor Ort oder in der Cloud gehostet werden, virtuelle Maschinen oder Container. Führen Sie die erste Hälfte dieses Verfahrens in der CloudTrail Lake-Konsole durch und rufen Sie dann die [PutAuditEvents](#) API auf, um Ereignisse zu erfassen, wobei Sie Ihren Kanal-ARN und Ihre Event-Payload bereitstellen. Nachdem Sie die PutAuditEvents API zum Ingestieren Ihrer Anwendungsaktivitäten verwendet haben, können Sie CloudTrail Lake verwenden CloudTrail, um die Daten zu suchen, abzufragen und zu analysieren, die von Ihren Anwendungen protokolliert wurden.

1. Melden Sie sich bei der an AWS Management Console und öffnen Sie die CloudTrail Konsole unter <https://console.aws.amazon.com/cloudtrail/>.
2. Wählen Sie im Navigationsbereich unter Lake die Option Integrationen aus.
3. Geben Sie auf der Seite Integration hinzufügen einen Namen für Ihren Kanal ein. Der Name kann eine Länge von 3–128 Zeichen haben. Namen dürfen nur Buchstaben, Zahlen, Punkte, Unterstriche und Schrägstriche enthalten.
4. Wählen Sie My custom integration (Meine benutzerdefinierte Integration).
5. Wählen Sie unter Event delivery location (Ereignisübermittlungsort) aus, ob dieselben Aktivitätsereignisse in vorhandenen Ereignisdatenspeichern protokolliert werden sollen, oder ob Sie einen neuen Ereignisdatenspeicher erstellen möchten.


Wenn Sie einen neuen Ereignisdatenspeicher erstellen, geben Sie einen Namen für den Ereignisdatenspeicher ein und geben Sie die Aufbewahrungsdauer in Tagen an. Sie können die Ereignisdaten bis zu 3 653 Tage (etwa 10 Jahre) in einem Ereignisdatenspeicher speichern, wenn Sie sich für die Preisoption mit verlängerbarer Aufbewahrung von einem Jahr entscheiden, oder bis zu 2 557 Tage (etwa 7 Jahre), wenn Sie sich für die Preisoption mit siebenjähriger Aufbewahrung entscheiden.

Wenn Sie Aktivitätsereignisse in einem oder mehreren vorhandenen Ereignisdatenspeichern protokollieren möchten, wählen Sie die Ereignisdatenspeicher aus der Liste aus. Die Ereignisdatenspeicher können nur Aktivitätsereignisse enthalten. Der Ereignistyp in der Konsole muss Events from integrations (Ereignisse aus Integrationen) sein. In der API muss der eventCategory-Wert ActivityAuditLog sein.

6. Konfigurieren Sie unter Resource policy (Ressourcenrichtlinie) die Ressourcenrichtlinie für den Kanal der Integration. Ressourcenbasierte Richtlinien sind JSON-Richtliniendokumente, die angeben, welche Aktionen ein bestimmter Prinzipal unter welchen Bedingungen für die




Ressource ausführen kann. Die Konten, die in der Ressourcenrichtlinie als Prinzipale definiert sind, können die PutAuditEvents-API aufrufen, um Ereignisse an Ihren Kanal zu senden.

 Note

Wenn Sie keine Ressourcenrichtlinie für den Kanal erstellen, kann nur der Kanalbesitzer die PutAuditEvents-API auf dem Kanal aufrufen.

- a. (Optional) Stellen Sie eine eindeutige externe ID zur Verfügung, um eine zusätzliche Schutzebene zu bieten. Die externe ID ist eine eindeutige Zeichenfolge, wie beispielsweise eine Konto-ID, oder eine zufällig generierte Zeichenfolge, um Verwirrung des Stellvertreters zu vermeiden.

 Note

Wenn die Ressourcenrichtlinie eine externe ID enthält, müssen alle Aufrufe der PutAuditEvents-API die externe ID enthalten. Wenn die Richtlinie jedoch keine externe ID definiert, können Sie die PutAuditEvents-API trotzdem aufrufen und einen externalId-Parameter angeben.

- b. Wählen Sie AWS Konto hinzufügen, um in der Ressourcenrichtlinie für den Kanal jede AWS Konto-ID anzugeben, die als Principal hinzugefügt werden soll.
7. (Optional) Im Bereich Tags können Sie bis zu 50 Tag-Schlüssel- und Wertepaare hinzufügen, um den Zugriff auf Ihren Ereignisdatenspeicher und -kanal zu identifizieren, zu sortieren und zu steuern. Weitere Informationen darüber, wie Sie IAM-Richtlinien verwenden, um den Zugriff auf einen Ereignisdatenspeicher basierend auf Tags zu autorisieren, finden Sie unter [Beispiele: Verweigern des Zugriffs zum Erstellen oder Löschen von Ereignisdatenspeichern basierend auf Tags](#). Weitere Informationen darüber, wie Sie Tags verwenden können AWS, finden Sie unter [Taggen Ihrer AWS Ressourcen](#) in der Allgemeine AWS-Referenz.
8. Wenn Sie bereit sind, die neue Integration zu erstellen, wählen Sie Integration hinzufügen. Es gibt keine Bewertungsseite. CloudTrail erstellt die Integration, aber um Ihre benutzerdefinierten Ereignisse zu integrieren, müssen Sie den Kanal-ARN in einer [PutAuditEvents](#)Anfrage angeben.
9. Rufen Sie die PutAuditEvents API auf, in die Sie Ihre Aktivitätsereignisse aufnehmen CloudTrail möchten. Sie können bis zu 100 Aktivitätsereignisse (oder bis zu 1 MB) pro PutAuditEvents-Anforderung hinzufügen. Sie benötigen den Kanal-ARN, den Sie in den

vorherigen Schritten erstellt haben, die Payload der Ereignisse, die Sie hinzufügen CloudTrail möchten, und die externe ID (sofern für Ihre Ressourcenrichtlinie angegeben). Stellen Sie sicher, dass die Event-Payload keine sensiblen oder persönlich identifizierbaren Informationen enthält, bevor Sie sie in die Payload aufnehmen. CloudTrail Ereignisse, in die Sie aufnehmen, müssen dem folgen. CloudTrail [CloudTrail Ereignisschema für Lake Integrations](#)

 Tip

Verwenden Sie [AWS CloudShell](#) diese Option, um sicherzustellen, dass Sie die aktuellsten AWS APIs verwenden.

Die folgenden Beispiele demonstrieren die Verwendung des CLI-Befehls `put-audit-events`. Die Parameter `--audit-events` und `--channel-arn` müssen angegeben werden. Sie benötigen den ARN des Kanals, den Sie in den vorherigen Schritten erstellt haben. Diesen können Sie von der Seite mit den Integrationsdetails kopieren. Der Wert von `--audit-events` ist ein JSON-Array von Ereignisobjekten. `--audit-events` enthält eine erforderliche ID aus dem Ereignis, die erforderliche Nutzlast des Ereignisses als Wert von `eventData` und eine [optionale Prüfsumme EventData](#), um die Integrität des Ereignisses nach der Aufnahme in zu überprüfen. CloudTrail

```
aws cloudtrail-data put-audit-events \
--region region \
--channel-arn $ChannelArn \
--audit-events \
id="event_ID",eventData="{event_payload}" \
id="event_ID",eventData="{event_payload}",eventDataChecksum="optional_checksum"
```

Nachfolgend finden Sie einen Beispielbefehl mit zwei Ereignisbeispielen.

```
aws cloudtrail-data put-audit-events \
--region us-east-1 \
--channel-arn arn:aws:cloudtrail:us-east-1:01234567890:channel/EXAMPLE8-0558-4f7e-
a06a-43969EXAMPLE \
--audit-events \
id="EXAMPLE3-0f1f-4a85-9664-d50a3EXAMPLE",eventData="{\"eventVersion\":\0.01\",
\"eventSource\": \"custom1.domain.com\", ...
}" \
id="EXAMPLE7-a999-486d-b241-b33a1EXAMPLE",eventData="{\"eventVersion\":\0.02\",
\"eventSource\": \"custom2.domain.com\", ...
}"
```

```
\}"', eventDataChecksum="EXAMPLE6e7dd61f3ead...93a691d8EXAMPLE"
```

Der folgende Beispielbefehl fügt den `--cli-input-json`-Parameter hinzu, um eine JSON-Datei (`custom-events.json`) mit Ereignis-Nutzlast anzugeben.

```
aws cloudtrail-data put-audit-events \
--channel-arn $channelArn \
--cli-input-json file://custom-events.json \
--region us-east-1
```

Es folgen Beispiele für den Inhalt der Beispiel-JSON-Datei `custom-events.json`.

```
{
  "auditEvents": [
    {
      "eventData": "{\"version\":\"eventData.version\",\"UID\":\"UID\",
        \"userIdentity\":{\"type\":\"CustomUserIdentity\",\"principalId\":
        \"principalId\",
        \"details\":{\"key\":\"value\"}},\"eventTime\":\"2021-10-27T12:13:14Z\",
        \"eventName\":\"eventName\",
        \"userAgent\":\"userAgent\",\"eventSource\":\"eventSource\",
        \"requestParameters\":{\"key\":\"value\"},\"responseElements\":{\"key\":
        \"value\"},
        \"additionalEventData\":{\"key\":\"value\"},
        \"sourceIPAddress\":\"source_IP_address\",\"recipientAccountId\":
        \"recipient_account_ID\"}",
      "id": "1"
    }
  ]
}
```

## (Optional) Berechnen Sie einen Prüfsummenwert

Mithilfe der Prüfsumme, die Sie `EventDataChecksum` in einer `PutAuditEvents` Anfrage als Wert für angeben, können Sie überprüfen, ob das Ereignis CloudTrail empfangen wird, das mit der Prüfsumme übereinstimmt. Sie hilft Ihnen dabei, die Integrität von Ereignissen zu überprüfen. Der Prüfsummenwert ist ein Base64-SHA256-Algorithmus, den Sie berechnen, indem Sie den folgenden Befehl ausführen.

```
printf %s "{\"eventData\": \"{\\\"version\\\":\\\"eventData.version\\\",\\\"UID\\\":\\\"UID\\\",
```

```

    \"userIdentity\":{\"type\": \"CustomUserIdentity\", \"principalId\": \"principalId
\",
    \"details\":{\"key\": \"value\"}}, \"eventTime\": \"2021-10-27T12:13:14Z\",
\"eventName\": \"eventName\",
    \"userAgent\": \"userAgent\", \"eventSource\": \"eventSource\",
    \"requestParameters\":{\"key\": \"value\"}, \"responseElements\":{\"key\": \"value
\"}},
    \"additionalEventData\":{\"key\": \"value\"},
    \"sourceIPAddress\": \"source_IP_address\",
    \"recipientAccountId\": \"recipient_account_ID\"},
    \"id\": \"1\"} \\
| openssl dgst -binary -sha256 | base64

```

Der Befehl gibt die Prüfsumme zurück. Im Folgenden wird ein Beispiel gezeigt.

```
EXAMPLEHjkI8iehvCUCWTIAbNYk0g0/t0YNw+7rrQE=
```

Der Prüfsummenwert wird der Wert von `EventDataChecksum` in Ihrer `PutAuditEvents`-Anfrage. Wenn die Prüfsumme nicht mit der für das angegebene Ereignis übereinstimmt, wird das Ereignis mit einem CloudTrail Fehler zurückgewiesen. `InvalidChecksum`

## Erstellen, aktualisieren und verwalten Sie CloudTrail Lake-Integrationen mit dem AWS CLI

Sie können die verwenden, AWS CLI um Ihre CloudTrail Lake-Integrationen zu erstellen, zu aktualisieren und zu verwalten. Denken Sie bei der Verwendung von daran AWS CLI, dass Ihre Befehle in der für Ihr Profil AWS-Region konfigurierten Version ausgeführt werden. Wenn Sie die Befehle in einer anderen Region ausführen möchten, ändern Sie entweder die Standardregion für Ihr Profil, oder verwenden Sie den `--region`-Parameter mit dem Befehl.

### Verfügbare Befehle für CloudTrail Lake-Integrationen

Zu den Befehlen zum Erstellen, Aktualisieren und Verwalten von Integrationen in CloudTrail Lake gehören:

- [create-event-data-store](#) um einen Ereignisdatenspeicher für Ereignisse außerhalb von AWS zu erstellen.
- [delete-channel](#) um einen Kanal zu löschen, der für eine Integration verwendet wird.
- [delete-resource-policy](#) um die Ressourcenrichtlinie zu löschen, die einem Kanal für eine CloudTrail Lake-Integration zugeordnet ist.

- [get-channel](#) Informationen über einen CloudTrail Kanal zurückzugeben.
- [get-resource-policy](#) den JSON-Text des ressourcenbasierten Richtliniendokuments abzurufen, das dem Kanal beigefügt ist. CloudTrail
- [list-channels](#) die Kanäle im Girokonto und ihre Quellnamen aufzulisten.
- [put-audit-events](#) Ihre Anwendungsereignisse in CloudTrail Lake aufzunehmen. Ein erforderlicher Parameter akzeptiert die JSON-Datensätze (auch Payload genannt) von Ereignissen, die Sie aufnehmen CloudTrail möchten. `auditEvents` Sie können bis zu 100 dieser Ereignisse (oder bis zu 1 MB) pro `PutAuditEvents` Anfrage hinzufügen.
- [put-resource-policy](#) einem CloudTrail Kanal, der für eine Integration mit einer Ereignisquelle außerhalb von verwendet wird, eine ressourcenbasierte Berechtigungsrichtlinie zuzuweisen. [AWS Weitere Informationen zu ressourcenbasierten Richtlinien finden Sie unter AWS CloudTrail Beispiele für ressourcenbasierte Richtlinien.](#)
- [update-channel](#) um einen Kanal zu aktualisieren, der durch einen erforderlichen Kanal-ARN oder eine UUID angegeben ist.

Eine Liste der verfügbaren Befehle für CloudTrail Lake-Ereignisdatenspeicher finden Sie unter.

[Verfügbare Befehle für Ereignisdatenspeicher](#)

Eine Liste der verfügbaren Befehle für CloudTrail Lake-Abfragen finden Sie unter [Verfügbare Befehle für CloudTrail Lake-Abfragen](#).

## Erstellen Sie eine Integration zur Protokollierung von Ereignissen von außen AWS mit dem AWS CLI

In der erstellen Sie eine Integration AWS CLI, die Ereignisse von außen AWS in vier Befehlen protokolliert (drei, wenn Sie bereits über einen Ereignisdatenspeicher verfügen, der die Kriterien erfüllt). Ereignisdatenspeicher, die Sie als Ziele für eine Integration verwenden, müssen für eine einzelne Region und ein einzelnes Konto bestimmt sein. Sie können nicht für mehrere Regionen verwendet werden, sie können keine Ereignisse für Organisationen protokollieren, in denen sie sich befinden AWS Organizations, und sie können nur Aktivitätsereignisse enthalten. Der Ereignistyp in der Konsole muss `Events from integrations` (Ereignisse aus Integrationen) sein. In der API muss der `eventCategory`-Wert `ActivityAuditLog` sein. Weitere Informationen über Integrationen finden Sie unter [Erstellen Sie eine Integration mit einer Ereignisquelle außerhalb von AWS](#).

1. Führen Sie den Vorgang [create-event-data-store](#) aus, um einen Ereignisdatenspeicher zu erstellen, falls Sie nicht bereits über einen oder mehrere Ereignisdatenspeicher verfügen, die Sie für die Integration verwenden können.

Mit dem folgenden AWS CLI Beispielbefehl wird ein Ereignisdatenspeicher erstellt, der Ereignisse von außen AWS protokolliert. Für Aktivitätsereignisse lautet der `eventCategory`-Feldauswahlwert `ActivityAuditLog`. Der Aufbewahrungszeitraum des Ereignisdatenspeichers beträgt 90 Tage. Standardmäßig sammelt der Ereignisdatenspeicher Ereignisse aus allen Regionen. Da es sich jedoch um AWS Nichtereignisse handelt, legen Sie ihn auf eine einzelne Region fest, indem Sie die `--no-multi-region-enabled` Option hinzufügen. Der Kündigungsschutz ist standardmäßig aktiviert, und der Ereignisdatenspeicher erfasst keine Ereignisse für Konten in einer Organisation.

```
aws cloudtrail create-event-data-store \  
--name my-event-data-store \  
--no-multi-region-enabled \  
--retention-period 90 \  
--advanced-event-selectors '[  
  {  
    "Name": "Select all external events",  
    "FieldSelectors": [  
      { "Field": "eventCategory", "Equals": ["ActivityAuditLog"] }  
    ]  
  }  
]'
```

Nachfolgend finden Sie eine Beispielantwort.

```
{  
  "EventDataStoreArn": "arn:aws:cloudtrail:us-east-1:123456789012:eventdatastore/  
EXAMPLEf852-4e8f-8bd1-bcf6cEXAMPLE",  
  "Name": "my-event-data-store",  
  "AdvancedEventSelectors": [  
    {  
      "Name": "Select all external events",  
      "FieldSelectors": [  
        {  
          "Field": "eventCategory",  
          "Equals": [  
            "ActivityAuditLog"  
          ]  
        }  
      ]  
    }  
  ]  
}
```

```
    }
  ]
}
],
"MultiRegionEnabled": true,
"OrganizationEnabled": false,
"BillingMode": "EXTENDABLE_RETENTION_PRICING",
"RetentionPeriod": 90,
"TerminationProtectionEnabled": true,
"CreatedTimestamp": "2023-10-27T10:55:55.384000-04:00",
"UpdatedTimestamp": "2023-10-27T10:57:05.549000-04:00"
}
```

Sie benötigen die Ereignisdatenspeicher-ID (das Suffix des ARN oder EXAMPLEf852-4e8f-8bd1-bcf6cEXAMPLE im vorherigen Antwortbeispiel), um mit dem nächsten Schritt fortzufahren und Ihren Kanal zu erstellen.

2. Führen Sie den [create-channel](#) Befehl aus, um einen Kanal zu erstellen, der es einer Partner- oder Quellanwendung ermöglicht, Ereignisse an einen Ereignisdatenspeicher in zu senden CloudTrail.

Ein Kanal umfasst die folgenden Komponenten:

#### Quelle

CloudTrail verwendet diese Informationen, um die Partner zu ermitteln, an die in CloudTrail Ihrem Namen Ereignisdaten gesendet werden. Eine Quelle ist erforderlich und kann entweder Custom für alle gültigen Nicht-AWS -Ereignisse oder für den Namen einer Partnerereignisquelle verwendet werden. Pro Quelle ist maximal ein Kanal zulässig.

Informationen zu den Source-Werten für verfügbare Partner finden Sie unter [Zusätzliche Informationen über Integrationspartner](#).

#### Status der Aufnahme

Der Kanalstatus zeigt an, wann die letzten Ereignisse von einer Kanalquelle empfangen wurden.

#### Ziele

Die Ziele sind die CloudTrail Lake-Ereignisdatenspeicher, die Ereignisse vom Kanal empfangen. Sie können die Zielergebnisdatenspeicher für einen Kanal ändern.

Um keine Ereignisse mehr von einer Quelle zu empfangen, löschen Sie den Kanal.

Sie benötigen die ID von mindestens einem Zielereignisdatenspeicher, um diesen Befehl auszuführen. Der gültige Zieltyp ist `EVENT_DATA_STORE`. Sie können aufgenommene Ereignisse an mehr als einen Ereignisdatenspeicher senden. Mit dem folgenden Beispielbefehl wird ein Kanal erstellt, der Ereignisse an zwei Ereignisdatenspeicher sendet, die durch ihre IDs im `Location`-Attribut des `--destinations`-Parameters dargestellt werden. Die Parameter `--destinations`, `--name` und `--source` müssen angegeben werden. Um Ereignisse von einem CloudTrail Partner aufzunehmen, geben Sie den Namen des Partners als Wert von `an--source`. Wenn Sie Ereignisse aus Ihren eigenen externen Anwendungen aufnehmen möchten AWS, geben Sie `Custom` den Wert von `an--source`.

```
aws cloudtrail create-channel \  
  --region us-east-1 \  
  --destinations '[{"Type": "EVENT_DATA_STORE", "Location":  
"EXAMPLEf852-4e8f-8bd1-bcf6cEXAMPLE"}, {"Type": "EVENT_DATA_STORE", "Location":  
"EXAMPLEg922-5n2l-3vz1- apqw8EXAMPLE"}]'  
  --name my-partner-channel \  
  --source $partnerSourceName \  

```

Kopieren Sie als Antwort auf Ihren `create-channel`-Befehl den ARN des neuen Kanals. Sie benötigen den ARN, um die `put-resource-policy`- und `put-audit-events`-Befehle und in den nächsten Schritten auszuführen.

3. Führen Sie den `put-resource-policy`-Befehl aus, um eine Ressourcenrichtlinie an den Kanal anzuhängen. Ressourcenrichtlinien sind JSON-Richtliniendokumente, die angeben, welche Aktionen ein bestimmter Prinzipal unter welchen Bedingungen für die Ressource ausführen kann. Die in der Ressourcenrichtlinie des Kanals als Prinzipale definierten Konten können die `PutAuditEvents`-API aufrufen, um Ereignisse zu übermitteln.

#### Note

Wenn Sie keine Ressourcenrichtlinie für den Kanal erstellen, kann nur der Kanalbesitzer die `PutAuditEvents`-API auf dem Kanal aufrufen.

Die für die Richtlinie erforderlichen Informationen werden durch den Integrationstyp bestimmt.



- Bei einer Direktionsintegration CloudTrail muss die Richtlinie die AWS Konto-IDs des Partners enthalten und Sie müssen die vom Partner bereitgestellte eindeutige externe ID eingeben. CloudTrail fügt automatisch die AWS Konto-IDs des Partners zur Ressourcenrichtlinie hinzu, wenn Sie eine Integration mithilfe der CloudTrail Konsole erstellen. In der [Dokumentation des Partners](#) erfahren Sie, wie Sie die für die Richtlinie erforderlichen AWS Kontonummern erhalten.
- Für eine Lösungsintegration müssen Sie mindestens eine AWS Konto-ID als Principal angeben und können optional eine externe ID eingeben, um zu verhindern, dass der Stellvertreter verwirrt wird.

Die folgenden Anforderungen sind für die Ressourcenrichtlinie erforderlich:

- Der in der Richtlinie definierte Ressourcen-ARN muss mit dem Kanal-ARN übereinstimmen, an den die Richtlinie angehängt ist.
- Die Richtlinie enthält nur eine Aktion: `cloudtrail-data: PutAuditEvents`
- Jede Richtlinie muss mindestens eine Aussage enthalten. Die Richtlinie kann maximal 20 Aussagen umfassen.
- Jede Aussage enthält mindestens einen Prinzipal. Eine Aussage kann maximal 50 Prinzipale haben.

```
aws cloudtrail put-resource-policy \  
  --resource-arn "channelARN" \  
  --policy "{  
    "Version": "2012-10-17",  
    "Statement":  
    [  
      {  
        "Sid": "ChannelPolicy",  
        "Effect": "Allow",  
        "Principal":  
        {  
          "AWS":  
          [  
            "arn:aws:iam::111122223333:root",  
            "arn:aws:iam::444455556666:root",  
            "arn:aws:iam::123456789012:root"  
          ]  
        }  
      ]  
    }  
  ]  
}
```

```

    },
    "Action": "cloudtrail-data:PutAuditEvents",
    "Resource": "arn:aws:cloudtrail:us-east-1:777788889999:channel/
EXAMPLE-80b5-40a7-ae65-6e099392355b",
    "Condition":
    {
        "StringEquals":
        {
            "cloudtrail:ExternalId": "UniqueExternalIDFromPartner"
        }
    }
}
]
}"

```

Weitere Informationen zu Ressourcenrichtlinien finden Sie unter [AWS CloudTrail Beispiele für ressourcenbasierte Richtlinien](#).

4. Führen Sie die [PutAuditEvents](#) API aus, in die Ihre Aktivitätsereignisse aufgenommen werden sollen. CloudTrail Sie benötigen die Payload der Ereignisse, die Sie hinzufügen CloudTrail möchten. Stellen Sie sicher, dass die Event-Payload keine sensiblen oder persönlich identifizierbaren Informationen enthält, bevor Sie sie aufnehmen. CloudTrail Beachten Sie, dass die PutAuditEvents-API den `cloudtrail-data-CLI`-Endpunkt verwendet, nicht den `cloudtrail`-Endpunkt.

Die folgenden Beispiele demonstrieren die Verwendung des CLI-Befehls `put-audit-events`. Die Parameter `--audit-events` und `--channel-arn` müssen angegeben werden. Der `--external-id`-Parameter ist erforderlich, wenn in der Ressourcenrichtlinie eine externe ID definiert ist. Sie benötigen den ARN des Kanals, den Sie im vorherigen Schritt erstellt haben. Der Wert von `--audit-events` ist ein JSON-Array von Ereignisobjekten. `--audit-event` enthält eine erforderliche ID aus dem Ereignis, die erforderliche Nutzlast des Ereignisses als Wert von und eine [optionale Prüfsumme EventData](#), um die Integrität des Ereignisses nach der Aufnahme in zu überprüfen. CloudTrail

```

aws cloudtrail-data put-audit-events \
--channel-arn $ChannelArn \
--external-id $UniqueExternalIDFromPartner \
--audit-events \
id="event_ID",eventData='"{event_payload}"' \

```

```
id="event_ID",eventData="{event_payload}",eventDataChecksum="optional_checksum"
```

Nachfolgend finden Sie einen Beispielbefehl mit zwei Ereignisbeispielen.

```
aws cloudtrail-data put-audit-events \
--channel-arn arn:aws:cloudtrail:us-east-1:123456789012:channel/EXAMPLE8-0558-4f7e-
a06a-43969EXAMPLE \
--external-id UniqueExternalIDFromPartner \
--audit-events \
id="EXAMPLE3-0f1f-4a85-9664-d50a3EXAMPLE",eventData="{\"eventVersion\":\0.01\",
\"eventSource\":\\"custom1.domain.com\"", ...
}" \
id="EXAMPLE7-a999-486d-b241-b33a1EXAMPLE",eventData="{\"eventVersion\":\0.02\",
\"eventSource\":\\"custom2.domain.com\"", ...
}",eventDataChecksum="EXAMPLE6e7dd61f3ead...93a691d8EXAMPLE"
```

Der folgende Beispielbefehl fügt den `--cli-input-json`-Parameter hinzu, um eine JSON-Datei (`custom-events.json`) mit Ereignis-Nutzlast anzugeben.

```
aws cloudtrail-data put-audit-events --channel-arn $channelArn --external-id
$UniqueExternalIDFromPartner --cli-input-json file://custom-events.json --region
us-east-1
```

Es folgen Beispiele für den Inhalt der Beispiel-JSON-Datei `custom-events.json`.

```
{
  "auditEvents": [
    {
      "eventData": "{\"version\": \"eventData.version\", \"UID\": \"UID\",
        \"userIdentity\": {\"type\": \"CustomUserIdentity\", \"principalId\":
        \"principalId\",
        \"details\": {\"key\": \"value\"}}, \"eventTime\": \"2021-10-27T12:13:14Z\",
        \"eventName\": \"eventName\",
        \"userAgent\": \"userAgent\", \"eventSource\": \"eventSource\",
        \"requestParameters\": {\"key\": \"value\"}, \"responseElements\": {\"key\":
        \"value\"},
        \"additionalEventData\": {\"key\": \"value\"},
        \"sourceIPAddress\": \"12.34.56.78\", \"recipientAccountId\":
        \"152089810396\"}",
      "id": "1"
    }
  ]
}
```

```
]
}
```

Sie können überprüfen, ob die Integration funktioniert und Ereignisse aus der Quelle CloudTrail korrekt aufnimmt, indem Sie den Befehl ausführen. [get-channel](#) Die Ausgabe von `get-channel` zeigt den letzten Zeitstempel, mit dem Ereignisse CloudTrail empfangen wurden.

```
aws cloudtrail get-channel --channel arn:aws:cloudtrail:us-east-1:01234567890:channel/
EXAMPLE8-0558-4f7e-a06a-43969EXAMPLE
```

(Optional) Berechnen Sie einen Prüfsummenwert

Anhand der Prüfsumme, die Sie `EventDataChecksum` in einer `PutAuditEvents` Anforderung als Wert angeben, können Sie überprüfen, ob das Ereignis CloudTrail empfangen wird, das mit der Prüfsumme übereinstimmt. Sie hilft Ihnen dabei, die Integrität von Ereignissen zu überprüfen. Der Prüfsummenwert ist ein Base64-SHA256-Algorithmus, den Sie berechnen, indem Sie den folgenden Befehl ausführen.

```
printf %s '{"eventData": {"\version\":"eventData.version","\UID\":"UID",
  \userIdentity\":{"type\":"CustomUserIdentity","\principalId\":"principalId
\},
  \details\":{"key\":"value"}},\eventTime\":"2021-10-27T12:13:14Z",
\eventName\":"eventName",
  \userAgent\":"userAgent","\eventSource\":"eventSource",
  \requestParameters\":{"key\":"value"},\responseElements\":{"key\":"value
\}},
  \additionalEventData\":{"key\":"value"},
  \sourceIPAddress\":"source_IP_address",
  \recipientAccountId\":"recipient_account_ID"}',
  "id": "1"}" \
| openssl dgst -binary -sha256 | base64
```

Der Befehl gibt die Prüfsumme zurück. Im Folgenden wird ein Beispiel gezeigt.

```
EXAMPLEDHjkI8iehvCUCWTIAbNYk0g0/t0YNw+7rrQE=
```

Der Prüfsummenwert wird der Wert von `EventDataChecksum` in Ihrer `PutAuditEvents`-Anfrage. Wenn die Prüfsumme nicht mit der für das angegebene Ereignis übereinstimmt, wird das Ereignis mit einem CloudTrail Fehler zurückgewiesen. `InvalidChecksum`

## Aktualisiere einen Kanal mit AWS CLI

Führen Sie den `update-channel`-Befehl aus, um den Namen oder die Zielereignisdatenspeicher eines Kanals zu aktualisieren. Der Parameter `--channel` muss angegeben werden. Sie können die Quelle eines Kanals nicht aktualisieren. Im Folgenden wird ein Beispiel gezeigt.

```
aws cloudtrail update-channel \
--channel aws:cloudtrail:us-east-1:123456789012:channel/EXAMPLE8-0558-4f7e-
a06a-43969EXAMPLE \
--name "new-channel-name" \
--destinations '[{"Type": "EVENT_DATA_STORE", "Location": "EXAMPLEf852-4e8f-8bd1-
bcf6cEXAMPLE"}, {"Type": "EVENT_DATA_STORE", "Location": "EXAMPLEg922-5n2l-3vz1-
apqw8EXAMPLE"}]'
```

## Löschen Sie einen Kanal, um eine Integration mit dem zu löschen AWS CLI

Um zu verhindern, dass Partner- oder andere Aktivitätsereignisse von außerhalb aufgenommen werden AWS, löschen Sie den Kanal, indem Sie den `delete-channel` Befehl ausführen. Der ARN oder die Kanal-ID (das ARN-Suffix) des Kanals, den Sie löschen möchten, ist erforderlich. Im Folgenden wird ein Beispiel gezeigt.

```
aws cloudtrail delete-channel \
--channel EXAMPLE8-0558-4f7e-a06a-43969EXAMPLE
```

## Zusätzliche Informationen über Integrationspartner

Die Tabelle in diesem Abschnitt enthält den Quellnamen für jeden Integrationspartner und identifiziert den Integrationstyp (Direkt oder Lösung).

Die Informationen in der Spalte Quellname sind erforderlich, wenn die `CreateChannel`-API aufgerufen wird. Sie geben den Quellnamen als Wert für den `Source`-Parameter an.

Partnername (Konsole)	Quellname (API)	Integrationstyp
Meine benutzerdefinierte Integration	Custom	Lösung
Cloud-Speichersicherheit	CloudStorageSecurityConsole	Lösung

Partnername (Konsole)	Quellname (API)	Integrationstyp
Clumio	Clumio	Direkt
CrowdStrike	CrowdStrike	Lösung
CyberArk	CyberArk	Lösung
GitHub	GitHub	Lösung
Kong Inc	KongGatewayEnterprise	Lösung
LaunchDarkly	LaunchDarkly	Direkt
Netskope	NetskopeCloudExchange	Lösung
Nordcloud, ein IBM-Unternehmen	IBMMulticloud	Direkt
MontyCloud	MontyCloud	Direkt
Okta	OktaSystemLogEvents	Lösung
One Identity	OneLogin	Lösung
Shoreline.io	Shoreline	Lösung
Snyk.io	Snyk	Direkt
Wiz	WizAuditLogs	Lösung

## Partnerdokumentation anzeigen

Sie können mehr über die Integration eines Partners mit CloudTrail Lake erfahren, indem Sie sich dessen Dokumentation ansehen.

### Wie Sie die Partnerdokumentation anzeigen

1. Melden Sie sich bei der an AWS Management Console und öffnen Sie die CloudTrail Konsole unter <https://console.aws.amazon.com/cloudtrail/>.
2. Wählen Sie im Navigationsbereich unter Lake die Option Integrationen aus.
3. Wählen Sie auf der Seite Integrationen die Option Verfügbare Quellen und dann Weitere Informationen für den Partner aus, dessen Dokumentation Sie ansehen möchten.

## CloudTrail Ereignisschema für Lake Integrations

In der folgenden Tabelle werden die erforderlichen und optionalen Schemaelemente beschrieben, die denen in den CloudTrail Ereignisdatensätzen entsprechen. Der Inhalt von eventData wird durch Ihre Ereignisse bereitgestellt; andere Felder werden von CloudTrail After Ingestion bereitgestellt.

CloudTrail Der Inhalt des Ereignisdatensatzes wird unter ausführlicher beschrieben. [CloudTrail Inhalt aufzeichnen](#)

- [Felder, die CloudTrail nach der Aufnahme bereitgestellt werden](#)
- [Felder, die durch Ihre Ereignisse bereitgestellt werden](#)

Felder, die von after ingestion bereitgestellt werden CloudTrail

Feldname	Eingabetyp	Anforderung	Beschreibung
eventVersion	Zeichenfolge	Erforderlich	Die Ereignisversion.
eventCategory	Zeichenfolge	Erforderlich	Die Kategorie des Ereignisses. Für AWS Nichtereignisse ist der Wert. ActivityAuditLog
eventType	Zeichenfolge	Erforderlich	Der Ereignistyp. Für AWS Nichtereignisse ist der gültige WertActivityLog .
eventID	Zeichenfolge	Erforderlich	Eine eindeutige ID für ein Ereignis.

Feldname	Eingabetyp	Anforderung	Beschreibung
eventTime	Zeichenfolge	Erforderlich	Der Zeitstempel des Ereignisses im Format yyyy-MM-DDTHH:mm:ss , in Universal Coordinated Time (UTC).
awsRegion	Zeichenfolge	Erforderlich	Der AWS-Region Ort, PutAuditEvents an dem der Anruf getätigt wurde.
recipientAccountId	Zeichenfolge	Erforderlich	Stellt die Konto-ID dar, die dieses Ereignis empfangen hat. CloudTrail füllt dieses Feld aus, indem es anhand der Nutzdaten des Ereignisses berechnet wird.
addendum	-	Optional	Zeigt Informationen dazu an, warum sich eine Ereignisausführung verzögert hat. Wenn Informationen zu einem bestehenden Ereignis fehlten, enthält der Nachtragsblock die fehlenden Informationen und einen Grund für das Fehlen.



Feldname	Eingabetyp	Anforderung	Beschreibung
• Grund	Zeichenfolge	Optional	Der Grund, dass das Ereignis oder einige seiner Inhalte fehlten.
• updatedFields	Zeichenfolge	Optional	Die Ereignisdatensatzfelder, die durch das Addendum aktualisiert werden. Dies wird nur angegeben, wenn der Grund UPDATED_DATA ist.
• originalUID	Zeichenfolge	Optional	Die ursprüngliche Ereignis-UID aus der Quelle. Dies wird nur angegeben, wenn der Grund UPDATED_DATA ist.
• originalEventID	Zeichenfolge	Optional	Die ursprüngliche Ereignis-ID. Dies wird nur angegeben, wenn der Grund UPDATED_DATA ist.
Metadaten	-	Erforderlich	Informationen über den Kanal, den das Ereignis verwendet hat.

Feldname	Eingabetyp	Anforderung	Beschreibung
• ingestionTime	Zeichenfolge	Erforderlich	Der Zeitstempel des Ereignisses im yyyy-MM-DDTHH:mm:ss - Format, in Universal Coordinated Time (UTC).
• channelARN	Zeichenfolge	Erforderlich	Der ARN des Kanals, den das Ereignis verwendet hat.

#### Felder, die durch Kundenereignisse bereitgestellt werden

Feldname	Eingabetyp	Anforderung	Beschreibung
eventData	-	Erforderlich	Die Prüfdaten, an die CloudTrail im Rahmen eines PutAuditEvents-Anrufs gesendet wurden.
• version	Zeichenfolge	Erforderlich	Die Version des Ereignisses aus seiner Quelle.  Längenbeschränkung en: Maximale Länge von 256.
• userIdentity	-	Erforderlich	Informationen über den Benutzer, der eine Anforderung gestellt hat.

Feldname	Eingabetyp	Anforderung	Beschreibung
• • Typ	Zeichenfolge	Erforderlich	Der Typ der Benutzeridentität.  Längenbeschränkungen: Maximale Länge von 128.
• • principalId	Zeichenfolge	Erforderlich	Die eindeutige ID für den Ausführenden dieses Ereignis.  Längenbeschränkungen: Maximale Länge von 1024.
• • Details	JSON-Objekt	Optional	Zusätzliche Informationen über die Identität.
• userAgent	Zeichenfolge	Optional	Der Agent über den die Anfrage erfolgte.  Längenbeschränkungen: Maximale Länge von 1024.
• eventSource	Zeichenfolge	Erforderlich	Dies ist die Partnerereignisquelle oder die benutzerdefinierte Anwendung, für die Ereignisse protokolliert werden.  Längenbeschränkungen: Maximale Länge von 1024.

Feldname	Eingabetyp	Anforderung	Beschreibung
• eventName	Zeichenfolge	Erforderlich	Die angeforderte Aktion, eine der Aktionen in der API für den Quellservice oder die Quellanwendung.  Längenbeschränkung en: Maximale Länge von 1024.
• eventTime	Zeichenfolge	Erforderlich	Der Zeitstempel des Ereignisses im Format yyyy-MM-DDTHH:mm:ss , in UTC (Universal Coordinated Time).
• Benutzerkennung (UID)	Zeichenfolge	Erforderlich	Der UID-Wert, anhand dessen die Anforderung identifiziert wird. Der aufgerufene Service oder die aufgerufene Anwendung generiert diesen Wert.  Längenbeschränkung en: Maximale Länge von 1024.

Feldname	Eingabetyp	Anforderung	Beschreibung
<ul style="list-style-type: none"><li>requestParameters</li></ul>	JSON-Objekt	Optional	Die Parameter, die mit der Anforderung gesendet wurden, sofern zutreffend. Dieses Feld hat eine maximale Größe von 100 KB; Inhalte, die diesen Grenzwert überschreiten, werden abgelehnt.
<ul style="list-style-type: none"><li>responseElements</li></ul>	JSON-Objekt	Optional	Das Antwortelement für Aktionen, die Änderungen vornehmen (Erstellungs-, Aktualisierungs- oder Löschaktionen). Dieses Feld hat eine maximale Größe von 100 KB; Inhalte, die diesen Grenzwert überschreiten, werden abgelehnt.
<ul style="list-style-type: none"><li>errorCode</li></ul>	Zeichenfolge	Optional	Eine Zeichenfolge, die einen Fehler für das Ereignis darstellt.  Längenbeschränkungen: Maximale Länge von 256.

Feldname	Eingabetyp	Anforderung	Beschreibung
<ul style="list-style-type: none"><li>• errorMessage</li></ul>	Zeichenfolge	Optional	Die Beschreibung des Fehlers.  Längenbeschränkung en: Maximale Länge von 256.
<ul style="list-style-type: none"><li>• sourceIPAddress</li></ul>	Zeichenfolge	Optional	Die IP-Adresse, von der die Anforderung erfolgt ist. Es werden IPv4- und IPv6-Adressen akzeptiert.
<ul style="list-style-type: none"><li>• recipientAccountId</li></ul>	Zeichenfolge	Erforderlich	Repräsentiert die Konto-ID, die das Ereignis empfangen hat. Die Konto-ID muss mit der AWS Konto-ID identisch sein, der der Kanal gehört.
<ul style="list-style-type: none"><li>• additionalEventData</li></ul>	JSON-Objekt	Optional	Zusätzliche Daten zu dem Ereignis, die nicht Teil der Anforderung oder Antwort waren. Dieses Feld hat eine maximale Größe von 28 KB; Inhalte, die diesen Grenzwert überschreiten, werden abgelehnt.

Das folgende Beispiel zeigt die Hierarchie der Schemaelemente, die denen in den CloudTrail Ereignisdatensätzen entsprechen.

```
{
  "eventVersion": String,
  "eventCategory": String,
  "eventType": String,
  "eventID": String,
  "eventTime": String,
  "awsRegion": String,
  "recipientAccountId": String,
  "addendum": {
    "reason": String,
    "updatedFields": String,
    "originalUID": String,
    "originalEventID": String
  },
  "metadata" : {
    "ingestionTime": String,
    "channelARN": String
  },
  "eventData": {
    "version": String,
    "userIdentity": {
      "type": String,
      "principalId": String,
      "details": {
        JSON
      }
    },
    "userAgent": String,
    "eventSource": String,
    "eventName": String,
    "eventTime": String,
    "UID": String,
    "requestParameters": {
      JSON
    },
    "responseElements": {
      JSON
    },
    "errorCode": String,
    "errorMessage": String,
```

```
    "sourceIPAddress": String,  
    "recipientAccountId": String,  
    "additionalEventData": {  
        JSON  
    }  
}  
}
```

## CloudTrail Lake-Dashboards anzeigen

Sie können CloudTrail Lake-Dashboards verwenden, um die Ereignisse in einem Ereignisdatenspeicher zu visualisieren. Sie haben mehrere verschiedene Dashboardtypen zur Auswahl. Die verfügbaren Dashboardtypen für einen Ereignisdatenspeicher hängen von der Konfiguration der erweiterten Ereigniselektoren des Ereignisdatenspeichers ab. Wenn ein Dashboard-Typ beispielsweise Informationen über CloudTrail Verwaltungsereignisse anzeigt, können Sie das Dashboard nur auswählen, wenn der aktuell ausgewählte Ereignisdatenspeicher CloudTrail Verwaltungsereignisse sammelt.

Jeder Dashboardtyp besteht aus mehreren Widgets und jedes Widget steht für eine SQL-Abfrage. Um die Abfrage für ein Widget anzuzeigen, wählen Sie **Im Abfrage-Editor anzeigen und analysieren** aus, um den Abfrage-Editor zu öffnen. Sie können die vom System generierte Abfrage, die zum Füllen des Widgets verwendet wird, nicht ändern. Sie können jedoch Änderungen an der Abfrage vornehmen und die Abfrage zur weiteren Analyse im Abfrage-Editor ausführen.

Um ein Dashboard aufzufüllen und zu aktualisieren, wählen Sie **Abfragen ausführen** aus. Wenn Sie **Abfragen ausführen** wählen, werden systemgenerierte Abfragen in Ihrem Namen CloudTrail ausgeführt. Da das Ausführen von Abfragen Kosten verursacht, werden Sie CloudTrail aufgefordert, die mit der Ausführung von Abfragen verbundenen Kosten zu bestätigen. Dies ist eine einmalige Bestätigung. Weitere Informationen zur Preisgestaltung finden Sie unter CloudTrail [CloudTrail Preisgestaltung](#).

### Themen

- [Einschränkungen](#)
- [Voraussetzungen](#)
- [Auswählen eines Dashboards](#)
- [Filtern eines Dashboards nach Datum oder Zeitraum](#)
- [Anzeigen der Abfrage für ein Dashboard-Widget](#)



## Einschränkungen

Die folgenden Einschränkungen gelten für die aktuelle Version.

- Die aktuelle Version unterstützt keine benutzerdefinierten Dashboards, Widgets oder Abfragen.
- Die aktuelle Version bietet nur Dashboards für Ereignisdatenspeicher, in denen CloudTrail Ereignisse (Datenereignisse, Verwaltungsereignisse) und Insights-Ereignisse erfasst werden.
- Die aktuelle Version unterstützt nicht die Bearbeitung der systemgenerierten Abfragen, die zum Füllen des Dashboards verwendet werden. Sie können die zugrunde liegende Abfrage für jedes Widget auf der Registerkarte Abfrage-Editor anzeigen und bearbeiten. Alle Änderungen, die Sie an der Abfrage vornehmen, sind jedoch für zusätzliche Analysen außerhalb des Dashboards vorgesehen.

## Voraussetzungen

Die folgenden Voraussetzungen gelten für Lake-Dashboards.

- Um Lake-Dashboards anzeigen und verwenden zu können, müssen Sie mindestens einen CloudTrail Lake-Ereignisdatenspeicher erstellen. Sie können Ereignisdatenspeicher mithilfe der Konsole oder mithilfe von SDKs erstellen. AWS CLI Weitere Informationen zum Erstellen eines Ereignisdatenspeichers mit der Konsole finden Sie unter [Erstellen Sie mit der Konsole einen Ereignisdatenspeicher für CloudTrail Ereignisse](#). Hinweise zum Erstellen eines Ereignisdatenspeichers mithilfe von finden Sie AWS CLI unter [Erstellen, aktualisieren und verwalten Sie Ereignisdatenspeicher mit dem AWS CLI](#).
- CloudTrail führt Abfragen in Ihrem Namen aus, um das Dashboard zu füllen. Wenn Sie die Seite „Dashboards“ zum ersten Mal aufrufen, werden Sie CloudTrail aufgefordert, die mit der Ausführung von Abfragen verbundenen Kosten zu bestätigen. Wählen Sie Ich stimme zu aus, um die Kosten für die Ausführung von Abfragen zu akzeptieren.

## Auswählen eines Dashboards

Gehen Sie wie folgt vor, um einen Ereignisdatenspeicher und einen Dashboardtyp für die Anzeige auszuwählen.

1. Melden Sie sich bei der an AWS Management Console und öffnen Sie die CloudTrail Konsole unter <https://console.aws.amazon.com/cloudtrail/>.

2. Wählen Sie im linken Navigationsbereich unter Lake die Option Dashboard aus.
3. Wählen Sie den Ereignisdatenspeicher aus, für den Sie Daten visualisieren möchten.
4. Wählen Sie den Dashboardtyp aus, den Sie anzeigen möchten. Die Liste der Dashboards wird basierend auf der Konfiguration der erweiterten Ereigniselektoren des ausgewählten Ereignisdatenspeichers ausgefüllt.

Die folgenden Dashboardtypen sind möglich:

- **Übersichts-Dashboard** — Zeigt die aktivsten Benutzer AWS-Services nach Anzahl der Ereignisse an. AWS-Regionen Sie können auch Informationen über die Aktivität von `read`- und `write`-Verwaltungsereignissen, die am stärksten beeinträchtigten Ereignisse und die häufigsten Fehler anzeigen. Dieses Dashboard ist für Ereignisdatenspeicher verfügbar, die Verwaltungsereignisse erfassen.
- **Dashboard für Verwaltungsereignisse** – Zeigt Anmeldeereignisse auf der Konsole, Ereignisse mit Zugriffsverweigerung, destruktive Aktionen und die häufigsten Fehler pro Benutzer an. Sie können auch Informationen zu TLS-Versionen und veralteten TLS-Aufrufen nach Benutzern anzeigen. Dieses Dashboard ist für Ereignisdatenspeicher verfügbar, die Verwaltungsereignisse erfassen.
- **Dashboard für S3-Datenereignisse** – Zeigt die S3-Kontoaktivitäten, die am häufigsten aufgerufenen S3-Objekte, die wichtigsten S3-Benutzer und die wichtigsten S3-Aktionen an. Dieses Dashboard ist für Ereignisdatenspeicher verfügbar, die Amazon-S3-Datenaktionen erfassen.
- **Dashboard für Insights-Ereignisse** – Zeigt den Gesamtanteil der Insights-Ereignisse nach Insights-Typ, den Anteil der Insights-Ereignisse nach Insights-Typ für die wichtigsten Benutzer und Services sowie die Anzahl der Insights-Ereignisse pro Tag. Das Dashboard enthält auch ein Widget, das Insights-Ereignisse für bis zu 30 Tage auflistet. Dieses Dashboard ist nur für Ereignisdatenspeicher verfügbar, die Insights-Ereignisse erfassen.

#### Note

- Nachdem Sie CloudTrail Insights zum ersten Mal im Quelldatenspeicher für Ereignisse aktiviert haben, kann es bis zu 7 Tage dauern, CloudTrail bis das erste Insights-Ereignis übermittelt wird, wenn ungewöhnliche Aktivitäten festgestellt werden. Weitere Informationen finden Sie unter [Grundlegendes zur Insights-Ereignisbereitstellung](#).

- Das Dashboard für Insights-Ereignisse zeigt nur Informationen zu den Insights-Ereignissen an, die vom ausgewählten Ereignisdatenspeicher erfasst wurden. Dies hängt von der Konfiguration des ursprünglichen Ereignisdatenspeicher ab. Wenn Sie beispielsweise den ursprünglichen Ereignisdatenspeicher so konfigurieren, dass Insights-Ereignisse für `ApiCallRateInsight`, aber nicht für `ApiErrorRateInsight` aktiviert werden, werden Ihnen keine Informationen über Insights-Ereignisse für `ApiErrorRateInsight` angezeigt.

5. Wählen Sie, ob Sie die Dashboard-Daten nach einem absoluten Bereich oder einem relativen Bereich filtern möchten. Wählen Sie Absoluter Bereich, um ein bestimmtes Datum und eine bestimmte Zeitspanne auszuwählen. Wählen Sie Relativer Bereich, um einen vordefinierten Zeitraum oder einen benutzerdefinierten Bereich auszuwählen. Standardmäßig zeigt das Dashboard Ereignisdaten der letzten 24 Stunden an.

#### Note

CloudTrail Bei Lake-Abfragen fallen Kosten an, die von der Menge der gescannten Daten abhängen. Für eine bessere Kostenkontrolle können Sie nach einem engeren Zeitrahmen filtern. Weitere Informationen zur CloudTrail Preisgestaltung finden Sie unter [AWS CloudTrail Preise](#).

6. Wählen Sie Abfragen ausführen aus, um die Abfragen für die Dashboard-Widgets auszuführen.

## Filtern eines Dashboards nach Datum oder Zeitraum

Standardmäßig zeigt das Dashboard Daten der letzten 24 Stunden an. Sie können ein Dashboard nach einem absoluten Bereich oder einem relativen Bereich filtern.

Wählen Sie Absoluter Bereich, um ein bestimmtes Datum und eine bestimmte Zeitspanne auszuwählen.

Wählen Sie Relativer Bereich, um einen vordefinierten Zeitraum oder einen benutzerdefinierten Bereich auszuwählen.

Nachdem Sie den Zeitraum ausgewählt haben, wählen Sie Abfragen ausführen aus, um das Dashboard zu aktualisieren.

**Note**

CloudTrail Bei Lake-Abfragen fallen Kosten an, die von der Menge der gescannten Daten abhängen. Für eine bessere Kostenkontrolle können Sie nach einem engeren Zeitrahmen filtern. Weitere Informationen zur CloudTrail Preisgestaltung finden Sie unter [AWS CloudTrail Preise](#).

## Anzeigen der Abfrage für ein Dashboard-Widget

Jedes Widget steht für eine SQL-Abfrage. Um die Abfrage für ein Widget anzuzeigen, wählen Sie Im Abfrage-Editor anzeigen und analysieren aus, um den Abfrage-Editor zu öffnen. Mithilfe des Abfrage-Editors können Sie die Abfrage außerhalb des Dashboards präzisieren und die Abfrage ausführen, um die Ergebnisse Ihrer aktualisierten Abfrage zu sehen. Weitere Informationen zum Arbeiten mit Abfragen finden Sie unter [Abfrage erstellen oder bearbeiten](#).

**Note**

Sie können die vom System generierte Abfrage für ein Dashboard-Widget nicht ändern. Alle Änderungen, die an der Abfrage auf der Registerkarte Abfrage-Editor vorgenommen werden, dienen ausschließlich der weiteren Analyse außerhalb des Dashboards.

## CloudTrail Anfragen zum See

Abfragen in CloudTrail Lake werden in SQL verfasst. Sie können eine Abfrage auf der Registerkarte CloudTrail Lake Editor erstellen, indem Sie die Abfrage von Grund auf in SQL schreiben oder indem Sie eine gespeicherte Abfrage oder eine Beispielabfrage öffnen und bearbeiten. Sie können eine enthaltene Beispielabfrage nicht mit Ihren Änderungen überschreiben, aber Sie können sie als neue Abfrage speichern. Weitere Informationen über die zulässige SQL-Abfragesprache finden Sie unter [CloudTrail Lake-SQL-Einschränkungen](#).

Eine unbegrenzte Abfrage (wie `SELECT * FROM edsID`) scannt alle Daten in Ihrem Ereignisdatenspeicher. Um die Kosten zu kontrollieren, empfehlen wir Ihnen, Abfragen einzuschränken, indem Sie eventTime-Start- und Ende-Zeitstempel zu Abfragen hinzufügen. Im folgenden Beispiel wird nach allen Ereignissen in einem angegebenen Ereignisdatenspeicher gesucht, bei denen die Ereigniszeit nach (>) 5. Januar 2023 um 13:51 Uhr und vor (<) 19. Januar

2023 um 13:51 Uhr liegt. Da ein Ereignisdatenspeicher eine Mindestaufbewahrungsfrist von sieben Tagen hat, ist die minimale Zeitspanne zwischen eventTime-Start- und Endwerten ebenfalls sieben Tage.

```
SELECT *
FROM eds-ID
WHERE
    eventtime >='2023-01-05 13:51:00' and eventtime < ='2023-01-19 13:51:00'
```

## Themen

- [Tools für Abfrageeditor](#)
- [Sehen Sie sich Beispielabfragen in der CloudTrail Konsole an](#)
- [Abfrage erstellen oder bearbeiten](#)
- [Ausführen einer Abfrage und Speichern von Abfrageergebnissen](#)
- [Abfrageergebnisse anzeigen](#)
- [Gespeicherte Abfrageergebnisse herunterladen](#)
- [Validierung von gespeicherten Abfrageergebnissen](#)
- [Führen Sie CloudTrail Lake-Abfragen aus und verwalten Sie sie mit dem AWS CLI](#)

## Tools für Abfrageeditor

Eine Symbolleiste oben rechts im Abfrage-Editor bietet Befehle, mit denen Sie Ihre SQL-Abfrage erstellen und formatieren können.



In den folgenden Abschnitten werden die Befehle der Symbolleiste beschrieben.

- Rückgängig machen – Macht die letzte im Abfrageeditor vorgenommene Inhaltsänderung rückgängig.
- Wiederholen – Wiederholt die letzte im Abfrageeditor vorgenommene Inhaltsänderung.
- Ausgewählte formatieren – Ordnet den Inhalt des Abfrageeditors gemäß den Konventionen für SQL-Formatierung und -Abstand an.
- Ausgewählte Option kommentieren/Kommentar entfernen – Kommentiert den ausgewählten Teil der Abfrage, sofern er nicht bereits kommentiert ist. Wenn der ausgewählte Teil bereits kommentiert ist, wird bei Auswahl dieser Option der Kommentar entfernt.

## Sehen Sie sich Beispielabfragen in der CloudTrail Konsole an

Die CloudTrail Konsole bietet eine Reihe von Beispielabfragen, die Ihnen den Einstieg in das Schreiben eigener Abfragen erleichtern können.

CloudTrail Für Abfragen fallen Gebühren an, die sich nach der Menge der gescannten Daten richten. Um die Kosten zu kontrollieren, empfehlen wir Ihnen, Abfragen einzuschränken, indem Sie eventTime-Start- und Ende-Zeitstempel zu Abfragen hinzufügen. Weitere Informationen zur CloudTrail Preisgestaltung finden Sie unter [AWS CloudTrail Preise](#).

### Note

Sie können sich auch Abfragen ansehen, die von der GitHub Community erstellt wurden. Weitere Informationen und die Ansicht dieser Beispielabfragen finden Sie unter [CloudTrailLake-Beispielabfragen](#) auf der GitHub Website. AWS CloudTrail hat die Abfragen in nicht ausgewertet GitHub.

Führen Sie eine Beispielabfrage wie folgt durch:

1. Melden Sie sich bei der an AWS Management Console und öffnen Sie die CloudTrail Konsole unter <https://console.aws.amazon.com/cloudtrail/>.
2. Wählen Sie im Navigationsbereich unter Lake die Option Abfrage aus.
3. Wählen Sie auf der Seite Abfrage die Registerkarte Beispielabfragen aus.
4. Wählen Sie eine Beispielabfrage aus der Liste aus oder suchen Sie nach der Abfrage, um die Liste zu filtern. In diesem Beispiel öffnen wir die Abfrage Untersuchen, wer Änderungen an der Konsole vorgenommen hat, indem Sie Namen der Abfrage auswählen. Dies öffnet die Abfrage in der Registerkarte Editor.

**Query** Info

Editor | Results history | Saved queries | **Sample queries** | How it works

**Sample queries (45)** Info

Q Search queries < 1 2 3 4 5 > ⚙

Query name	Query description	Query SQL
<a href="#">Find who is making calls using outdated TLS versions</a>	Find the callers who used outdated Transport Layer Security (TLS) versions 1.0 and 1.1 within the past week grouped by the number of calls per service.	SELECT recipientAccountId, year(eventTime) AS year_date, month(eventTime) AS month_date, eventSource, sourceIPAddress, userAgent, useridentity.arn, useridentity.accesskeyid, COUNT(*) AS numCalls FROM \$EDS_ID WHERE tlsDetails.tlsVersion IN ('TLSv1', 'TLSv1.1') AND eventTime > '2023-06-23 00:00:00' GROUP BY recipientAccountId, year(eventTime), month(eventTime), eventSource, sourceIPAddress, userAgent, useridentity.arn, useridentity.accesskeyid ORDER BY COUNT(*) DESC
<a href="#">Investigate who made console changes</a>	Find users with write permissions who made changes using the console within the past week.	SELECT useridentity.arn AS user, eventName, eventTime, _Region, requestParameters AS resourceChangedManually FROM \$EDS_ID WHERE sessionCredentialFromConsole='true' AND errorCode IS NULL AND eventTime > '2023-06-23 00:00:00'

- Wählen Sie auf der Registerkarte Editor den Ereignisdatenspeicher aus, für den Sie die Abfrage ausführen möchten. Wenn Sie den Ereignisdatenspeicher aus der Liste auswählen, CloudTrail wird die ID des Ereignisdatenspeichers automatisch in die FROM Zeile des Abfrage-Editors eingetragen.

**Query** Info

Editor | Results history | Saved queries | **Sample queries** | How it works

**Event data store** Info Investigate who made console changes +

Event data store Info  
Choose an event data store.  
my-management-events-eds  
Event data store ID  
[Redacted]

**Event properties**  
Q Search event properties  
< 1 2 >

additionalEventData  
annotation  
apiVersion  
awsRegion  
edgeDeviceDetails  
errorCode  
errorMessage  
eventID  
eventJson  
eventName  
eventSource

```

1 SELECT
2   useridentity.arn AS user, eventName, eventTime, awsRegion, requestParameters AS resourceChangedManually
3 FROM
4   [Redacted]
5 WHERE
6   sessionCredentialFromConsole='true' AND errorCode IS NULL
7   AND eventTime > '2023-06-23 00:00:00'

```

**Run** Save Clear  Save results to S3

Query results | **Command output**

**Output**

< 1 > ⚙

Time stamp | Status | Delivery status | Response | Query SQL | Query ID | Event data st...

- Wählen Sie dann Ausführen aus, um die Abfrage auszuführen.

Auf der Registerkarte Befehlsausgabe werden Metadaten zu Ihrer Abfrage angezeigt, z. B. ob die Abfrage erfolgreich war, die Anzahl der übereinstimmenden Datensätze und die Laufzeit der Abfrage.

Time stamp	Status	Delivery status	Response	Query SQL	Query ID	Event data st...
June 30, 2023, 2...	Successful		1467 records ma...	SELECT useridentity.ar		my-management-ever

Auf der Registerkarte Abfrageergebnisse werden die Ereignisdaten im ausgewählten Ereignisdatenspeicher angezeigt, die Ihrer Abfrage entsprachen.

user	eventName	eventTime	awsRegion
arn:aws:sts:: :assumed-role/Admin/	UpdateEventDataStore	2023-07-10 14:35:00.000	us-east-1
arn:aws:sts:: :assumed-role/Admin/	LookupEvents	2023-07-07 23:10:14.000	us-east-1
arn:aws:sts:: :assumed-role/Admin/	LookupEvents	2023-07-07 23:10:13.000	us-east-1

Weitere Informationen zum Bearbeiten einer Abfrage finden Sie unter [Abfrage erstellen oder bearbeiten](#). Weitere Informationen zum Ausführen einer Abfrage und zum Speichern von Abfrageergebnissen finden Sie unter [Ausführen einer Abfrage und Speichern von Abfrageergebnissen](#).

## Abfrage erstellen oder bearbeiten

In dieser Schritt-für-Schritt-Anleitung öffnen wir eine der Beispielabfragen, bearbeiten sie, um die Aktionen eines bestimmten Benutzers namens Alice zu finden, und speichern sie als neue Abfrage. Sie können auch eine gespeicherte Abfrage auf der Registerkarte Gespeicherte Abfragen bearbeiten, wenn Sie gespeicherte Abfragen haben. Um die Kosten zu kontrollieren, empfehlen wir



Ihnen, Abfragen einzuschränken, indem Sie eventTime-Start- und Ende-Zeitstempel zu Abfragen hinzufügen.

1. Melden Sie sich bei der an AWS Management Console und öffnen Sie die CloudTrail Konsole unter <https://console.aws.amazon.com/cloudtrail/>.
2. Wählen Sie im Navigationsbereich unter Lake die Option Abfrage aus.
3. Wählen Sie auf der Seite Abfrage die Registerkarte Beispielabfragen aus.
4. Öffnen Sie eine Beispielabfrage, indem Sie den Abfragenamen auswählen. Dies öffnet die Abfrage in der Registerkarte Editor. In diesem Beispiel wählen wir die Abfrage mit dem Namen Benutzeraktionen untersuchen aus und bearbeiten die Abfrage, um die Aktionen für einen bestimmten Benutzer namens Alice zu finden.
5. Bearbeiten Sie auf der Registerkarte Editor die Zeile WHERE, um den zu untersuchenden Benutzer anzugeben, und aktualisieren Sie die eventTime-Werte nach Bedarf. Der Wert von FROM ist der ID-Teil des ARN des Ereignisdatenspeichers und wird automatisch aufgefüllt, CloudTrail wenn Sie den Ereignisdatenspeicher auswählen.

```
SELECT
    eventID, eventName, eventSource, eventTime, userIdentity.arn AS user
FROM
    event-data-store-id
WHERE
    userIdentity.arn LIKE '%Alice%'
    AND eventTime > '2023-06-23 00:00:00' AND eventTime < '2023-06-26 00:00:00'
```

6. Sie können eine Abfrage ausführen, bevor Sie sie speichern, um zu überprüfen, ob die Abfrage funktioniert. Um eine Abfrage auszuführen, wählen Sie einen Ereignisdatenspeicher aus der Dropdown-Liste Datenspeicher aus und wählen Sie dann Ausführen aus. Sehen Sie sich die Spalte Status auf der Registerkarte Befehlsausgabe für die aktive Abfrage an, um zu überprüfen, ob eine Abfrage erfolgreich ausgeführt wurde.
7. Wenn Sie die Beispielabfrage aktualisiert haben, wählen Sie Speichern aus.
8. Geben Sie unter Abfrage speichern einen Namen und eine Beschreibung für die Abfrage ein. Wählen Sie Abfrage speichern aus, um Ihre Änderungen als neue Abfrage zu speichern. Um Änderungen an einer Abfrage zu verwerfen, wählen Sie Abbrechen oder schließen Sie das Fenster Abfrage speichern.

## Save query ✕

**Query name**

Investigate actions taken by Alice


3-64 characters. Only letters, numbers, periods, underscores, hyphens, and spaces are allowed.

**Query description**

This query returns all actions taken by a user named Alice.

3-256 characters. Only letters, numbers, periods, underscores, hyphens, and spaces are allowed.

Cancel
Save query

 **Note**

Gespeicherte Abfragen sind an Ihren Browser gebunden. Wenn Sie einen anderen Browser oder ein anderes Gerät für den Zugriff auf die CloudTrail Konsole verwenden, sind die gespeicherten Abfragen nicht verfügbar.

- Öffnen Sie die Registerkarte Gespeicherte Abfragen, um die neue Abfrage in der Tabelle anzuzeigen.

**Query** Info

Editor | Results history | **Saved queries** | Sample queries | How it works

---

**Saved queries (1)** Info 🔄 Delete Edit

< 1 > ⌂

	Query name	Query description	Query SQL	Time stamp
<input type="checkbox"/>	<a href="#">Investigate actions taken by Alice</a>	This query returns all actions taken by a user named Alice.	<pre>SELECT eventId, eventName, eventSource, eventTime, userIdentity.arn AS user FROM WHERE userIdentity.arn LIKE '%Alice%' AND eventTime &gt; '2023-06-23 00:00:00' AND eventTime &lt; '2023-06-26 00:00:00'</pre>	June 30, 2023, 17:17:50 (UTC-05:00)

## Ausführen einer Abfrage und Speichern von Abfrageergebnissen

Nachdem Sie eine Abfrage ausgewählt oder gespeichert haben, können Sie eine Abfrage in einem Ereignisdatenspeicher ausführen.

Wenn Sie eine Abfrage ausführen, haben Sie die Möglichkeit, die Abfrageergebnisse in einem Amazon S3-Bucket zu speichern. Wenn Sie Abfragen in CloudTrail Lake ausführen, fallen Gebühren an, die auf der Menge der von der Abfrage gescannten Daten basieren. Für das Speichern von Abfrageergebnissen in einem S3-Bucket fallen keine zusätzlichen CloudTrail Lake-Gebühren an, es fallen jedoch S3-Speichergebühren an. Weitere Informationen zu S3-Preisen finden Sie unter [Preise für Amazon S3](#).

Wenn Sie Abfrageergebnisse speichern, werden die Abfrageergebnisse möglicherweise in der CloudTrail Konsole angezeigt, bevor sie im S3-Bucket angezeigt werden, da CloudTrail die Abfrageergebnisse erst nach Abschluss des Abfragescans angezeigt werden. Die meisten Abfragen werden zwar je nach Größe Ihres Ereignisdatenspeichers innerhalb weniger Minuten abgeschlossen, es kann jedoch erheblich länger dauern, CloudTrail bis Abfrageergebnisse an Ihren S3-Bucket übermittelt werden. CloudTrail übermittelt die Abfrageergebnisse im komprimierten Gzip-Format an den S3-Bucket. Im Durchschnitt können Sie nach Abschluss des Abfragescans mit einer Latenz von 60 bis 90 Sekunden für jedes GB an Daten rechnen, das an den S3-Bucket übermittelt wird.

Um eine Abfrage mit CloudTrail Lake auszuführen


1. Melden Sie sich bei der an AWS Management Console und öffnen Sie die CloudTrail Konsole unter <https://console.aws.amazon.com/cloudtrail/>.
2. Wählen Sie im Navigationsbereich unter Lake die Option Abfrage aus.
3. Wählen Sie auf den Registerkarten Gespeicherte Abfragen oder Beispielabfragen eine Abfrage aus, die ausgeführt werden soll, indem Sie den Abfragenamen auswählen.
4. Wählen Sie auf der Registerkarte Editor für Ereignisdatenspeicher einen Ereignisdatenspeicher aus der Dropdown-Liste aus.
5. (Optional) Wählen Sie auf der Registerkarte Editor die Option Ergebnisse in S3 speichern, um die Abfrageergebnisse in einem S3-Bucket zu speichern. Wenn Sie den Standard-S3-Bucket auswählen, werden die erforderlichen Bucket-Richtlinien CloudTrail erstellt und angewendet. Wenn Sie den Standard-S3-Bucket wählen, muss Ihre IAM-Richtlinie die Genehmigung für die `s3:PutEncryptionConfiguration` Aktion enthalten, da die serverseitige Verschlüsselung standardmäßig für den Bucket aktiviert ist. Weitere Informationen zum Speichern von Abfrageergebnissen finden Sie unter [Zusätzliche Informationen über gespeicherte Abfrageergebnisse](#).

 Note

Um einen anderen Bucket zu verwenden, geben Sie einen Bucket-Namen an oder wählen Sie S3 durchsuchen, um einen Bucket auszuwählen. Die Bucket-Richtlinie muss die CloudTrail Erlaubnis erteilen, Abfrageergebnisse an den Bucket zu übermitteln. Informationen zur manuellen Bearbeitung der Bucket-Richtlinie finden Sie im Abschnitt [Amazon S3 S3-Bucket-Richtlinie für CloudTrail Lake-Abfrageergebnisse](#).

6. Wählen Sie auf der Registerkarte Editor die Option Ausführen aus.

Abhängig von der Größe Ihres Ereignisdatenspeichers und der Anzahl der darin enthaltenen Daten kann die Ausführung einer Abfrage mehrere Minuten dauern. Die Registerkarte Befehlsausgabe zeigt den Status einer Abfrage an und ob eine Abfrage abgeschlossen ist. Wenn eine Abfrage abgeschlossen ist, öffnen Sie die Option Abfrageergebnisse, um eine Ergebnistabelle für die aktive Abfrage anzuzeigen (die derzeit im Editor angezeigte Abfrage).

 Note

Abfragen, die länger als eine Stunde laufen, können ablaufen. Sie können immer noch Teilergebnisse abrufen, die vor dem Timeout der Abfrage verarbeitet wurden. CloudTrail liefert keine unvollständigen Abfrageergebnisse an einen S3-Bucket. Um eine Zeitüberschreitung zu vermeiden, können Sie Ihre Abfrage verfeinern, um die Menge der gescannten Daten zu begrenzen, indem Sie einen kürzeren Zeitbereich angeben.

## Zusätzliche Informationen über gespeicherte Abfrageergebnisse

Nachdem Sie die Abfrageergebnisse gespeichert haben, können Sie die gespeicherten Abfrageergebnisse aus dem S3-Bucket herunterladen. Weitere Informationen zum Suchen und Herunterladen von gespeicherten Abfrageergebnissen finden Sie unter [Gespeicherte Abfrageergebnisse herunterladen](#).

Sie können auch gespeicherte Abfrageergebnisse überprüfen, um festzustellen, ob die Abfrageergebnisse nach CloudTrail der Übermittlung der Abfrageergebnisse geändert, gelöscht oder unverändert wurden. Weitere Informationen zum Validieren von gespeicherten Abfrageergebnissen finden Sie unter [Validierung von gespeicherten Abfrageergebnissen](#).

## Beispiel: Abfrageergebnisse in einem Amazon S3 S3-Bucket speichern

Diese exemplarische Vorgehensweise zeigt, wie Sie Abfrageergebnisse in einem S3-Bucket speichern und diese Abfrageergebnisse dann herunterladen können.

### Speichern von Abfrageergebnissen in einen Amazon-S3-Bucket

1. Melden Sie sich bei der an AWS Management Console und öffnen Sie die CloudTrail Konsole unter <https://console.aws.amazon.com/cloudtrail/>.
2. Wählen Sie im Navigationsbereich unter Lake die Option Abfrage.
3. Wählen Sie auf den Registerkarten Beispielabfragen oder Gespeicherte Abfragen eine Abfrage aus, die ausgeführt werden soll, indem Sie den Abfragenamen auswählen. In diesem Beispiel wählen wir die Beispielabfrage mit dem Namen Benutzeraktionen untersuchen aus.
4. Wählen Sie auf der Registerkarte Editor für Ereignisdatenspeicher einen Ereignisdatenspeicher aus der Dropdown-Liste aus. Wenn Sie den Ereignisdatenspeicher aus der Liste auswählen, CloudTrail wird automatisch die ID des Ereignisdatenspeichers in die From Zeile eingetragen.
5. In dieser Beispielabfrage bearbeiten wir den `userIdentity.arn`-Wert, um einen Benutzer mit dem Namen Admin anzugeben. Wir behalten die Standardwerte für `eventTime` bei. Wenn Sie eine Abfrage ausführen, wird Ihnen die Menge der gescannten Daten berechnet. Um die Kosten zu kontrollieren, empfehlen wir Ihnen, Abfragen einzuschränken, indem Sie `eventTime`-Start- und Ende-Zeitstempel zu Abfragen hinzufügen.



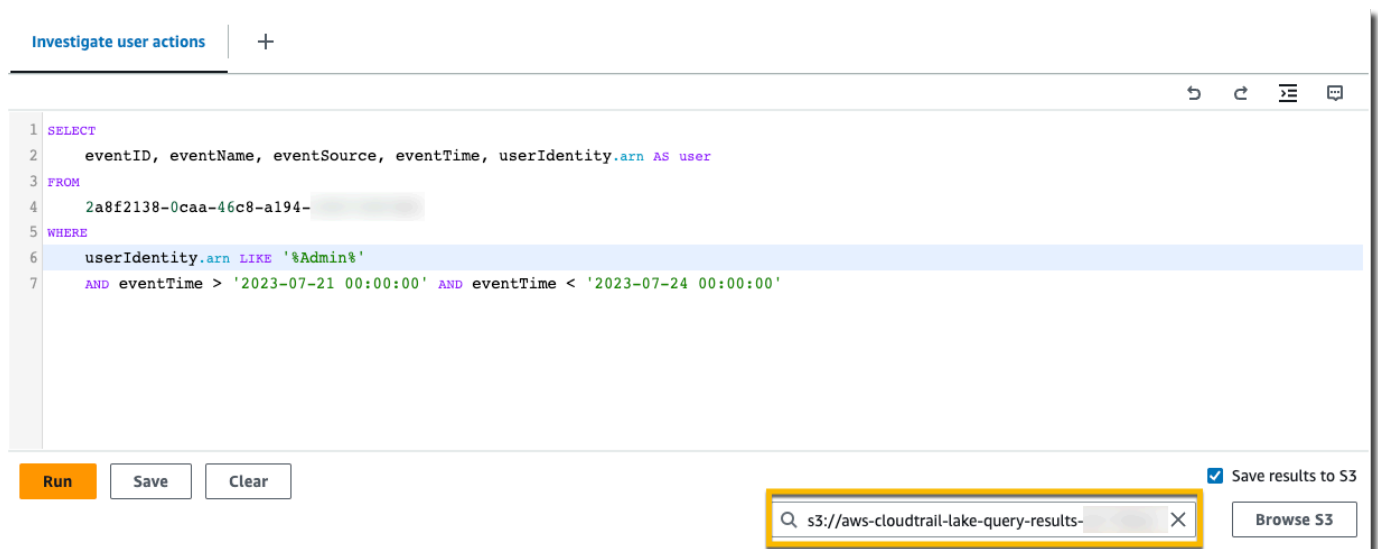
```
1 SELECT
2   eventID, eventName, eventSource, eventTime, userIdentity.arn AS user
3 FROM
4   2a8f2138-0caa-46c8-a194-
5 WHERE
6   userIdentity.arn LIKE '%Admin%'
7   AND eventTime > '2023-07-21 00:00:00' AND eventTime < '2023-07-24 00:00:00'
```

6. Wählen Sie die Option Ergebnisse in S3 speichern, um die Abfrageergebnisse in einem S3-Bucket zu speichern. Wenn Sie den Standard-S3-Bucket auswählen, werden die erforderlichen Bucket-Richtlinien CloudTrail erstellt und angewendet. Wenn Sie den Standard-S3-Bucket wählen, muss Ihre IAM-Richtlinie die Genehmigung für die `s3:PutEncryptionConfiguration` Aktion enthalten, da die serverseitige Verschlüsselung

standardmäßig für den Bucket aktiviert ist. In diesem Beispiel wird der standardmäßige S3-Bucket verwendet.

### Note

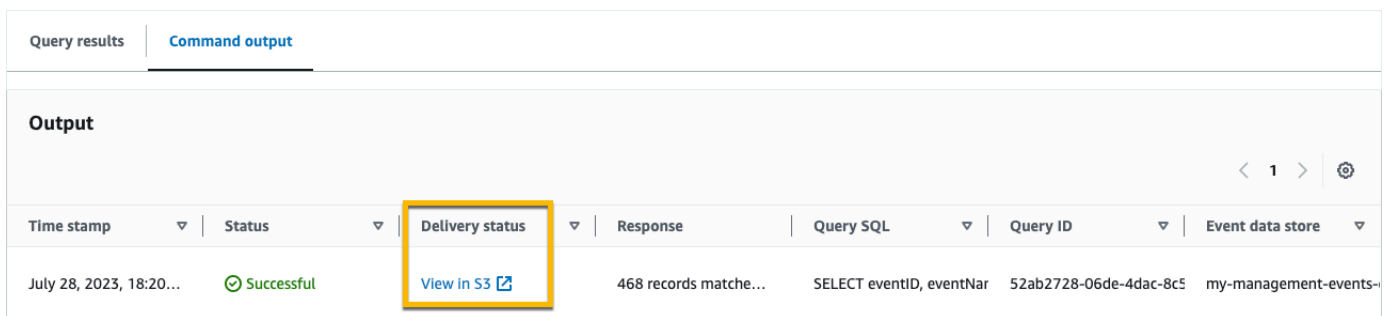
Um einen anderen Bucket zu verwenden, geben Sie einen Bucket-Namen an oder wählen Sie S3 durchsuchen, um einen Bucket auszuwählen. Die Bucket-Richtlinie muss die CloudTrail Erlaubnis erteilen, Abfrageergebnisse an den Bucket zu übermitteln. Informationen zur manuellen Bearbeitung der Bucket-Richtlinie finden Sie im Abschnitt [Amazon S3 S3-Bucket-Richtlinie für CloudTrail Lake-Abfrageergebnisse](#).



- Wählen Sie Ausführen aus. Abhängig von der Größe Ihres Ereignisdatenspeichers und der Anzahl der darin enthaltenen Daten kann die Ausführung einer Abfrage mehrere Minuten dauern. Die Registerkarte Befehlsausgabe zeigt den Status einer Abfrage an und ob eine Abfrage abgeschlossen ist. Wenn eine Abfrage abgeschlossen ist, öffnen Sie die Option Abfrageergebnisse, um eine Ergebnistabelle für die aktive Abfrage anzuzeigen (die derzeit im Editor angezeigte Abfrage).
- Wenn die Übermittlung der gespeicherten Abfrageergebnisse an Ihren S3-Bucket CloudTrail abgeschlossen ist, enthält die Spalte Lieferstatus einen Link zum S3-Bucket, der Ihre gespeicherten Abfrageergebnisdateien sowie eine [Signierdatei](#) enthält, mit der Sie Ihre gespeicherten Abfrageergebnisse überprüfen können. Wählen Sie In S3 anzeigen, um die Abfrageergebnisdateien anzuzeigen und Dateien im S3-Bucket zu signieren.

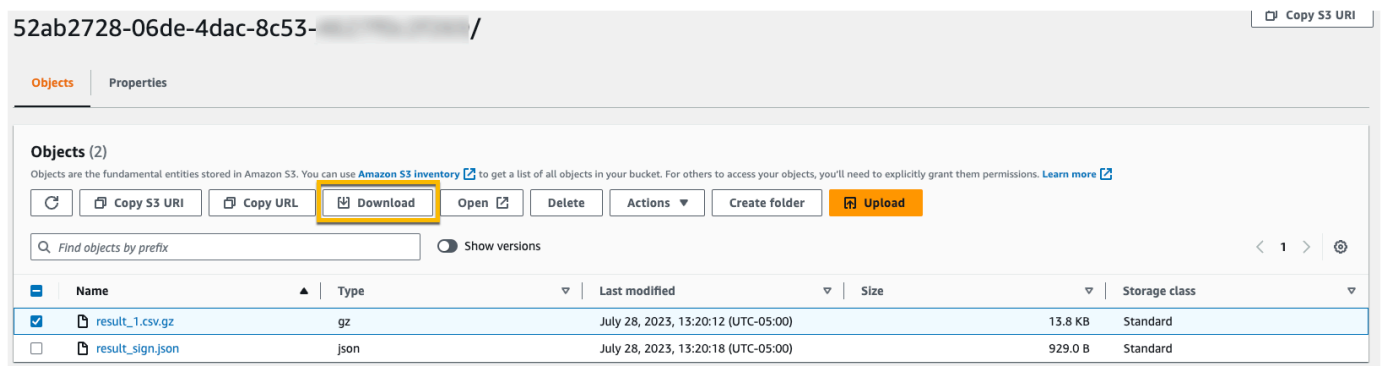
**Note**

Wenn Sie Abfrageergebnisse speichern, werden die Abfrageergebnisse möglicherweise in der CloudTrail Konsole angezeigt, bevor sie im S3-Bucket sichtbar sind, da CloudTrail die Abfrageergebnisse erst nach Abschluss des Abfragescans angezeigt werden. Die meisten Abfragen werden zwar je nach Größe Ihres Ereignisdatenspeichers innerhalb weniger Minuten abgeschlossen, es kann jedoch erheblich länger dauern, CloudTrail bis Abfrageergebnisse an Ihren S3-Bucket übermittelt werden. CloudTrail übermittelt die Abfrageergebnisse im komprimierten Gzip-Format an den S3-Bucket. Im Durchschnitt können Sie nach Abschluss des Abfragescans mit einer Latenz von 60 bis 90 Sekunden für jedes GB an Daten rechnen, das an den S3-Bucket übermittelt wird.



Time stamp	Status	Delivery status	Response	Query SQL	Query ID	Event data store
July 28, 2023, 18:20...	Successful	<a href="#">View in S3</a>	468 records matche...	SELECT eventID, eventNar	52ab2728-06de-4dac-8c5	my-management-events-

9. Um Ihre Abfrageergebnisse herunterzuladen, wählen Sie die Abfrageergebnisdatei (in diesem Beispiel `result_1.csv.gz`) und klicken Sie dann auf Herunterladen.



Name	Type	Last modified	Size	Storage class
<input checked="" type="checkbox"/> <a href="#">result_1.csv.gz</a>	gz	July 28, 2023, 13:20:12 (UTC-05:00)	13.8 KB	Standard
<input type="checkbox"/> <a href="#">result_sign.json</a>	json	July 28, 2023, 13:20:18 (UTC-05:00)	929.0 B	Standard

Informationen zum Validieren von gespeicherten Abfrageergebnissen finden Sie unter [Validierung von gespeicherten Abfrageergebnissen](#).

## Abfrageergebnisse anzeigen

Nachdem Ihre Abfrage abgeschlossen ist, können Sie ihre Ergebnisse anzeigen. Die Ergebnisse einer Abfrage sind sieben Tage lang verfügbar, nachdem die Abfrage beendet wurde. Sie können die Ergebnisse für die aktive Abfrage auf der Registerkarte Abfrageergebnisse anzeigen, oder Sie können die Ergebnisse für alle letzten Abfragen auf der Registerkarte Ergebnisverlauf auf der Startseite von Lake einsehen.

Abfrageergebnisse können sich von älteren Abfrageabläufen zu neueren ändern, da spätere Ereignisse im Abfragezeitraum zwischen Abfragen protokolliert werden können.

Wenn Sie Abfrageergebnisse speichern, werden die Abfrageergebnisse möglicherweise in der CloudTrail Konsole angezeigt, bevor sie im S3-Bucket angezeigt werden, da CloudTrail die Abfrageergebnisse erst nach Abschluss des Abfragescans angezeigt werden. Die meisten Abfragen werden zwar je nach Größe Ihres Ereignisdatenspeichers innerhalb weniger Minuten abgeschlossen, es kann jedoch erheblich länger dauern, CloudTrail bis Abfrageergebnisse an Ihren S3-Bucket übermittelt werden. CloudTrail übermittelt die Abfrageergebnisse im komprimierten Gzip-Format an den S3-Bucket. Im Durchschnitt können Sie nach Abschluss des Abfragescans mit einer Latenz von 60 bis 90 Sekunden für jedes GB an Daten rechnen, das an den S3-Bucket geliefert wird. Weitere Informationen zum Suchen und Herunterladen von gespeicherten Abfrageergebnissen finden Sie unter [Gespeicherte Abfrageergebnisse herunterladen](#).

### Note

Abfragen, die länger als eine Stunde laufen, können ablaufen. Sie können immer noch Teilergebnisse erhalten, die vor dem Timeout der Abfrage verarbeitet wurden. CloudTrail liefert keine unvollständigen Abfrageergebnisse an einen S3-Bucket. Um eine Zeitüberschreitung zu vermeiden, können Sie Ihre Abfrage verfeinern, um die Menge der gescannten Daten zu begrenzen, indem Sie einen kürzeren Zeitbereich angeben.

1. Auf der Registerkarte Abfrageergebnisse für eine aktive Abfrage stellt jede Zeile ein Ereignisergebnis dar, das mit der Abfrage übereinstimmt. Filtern Sie Ergebnisse, indem Sie einen Wert eines Ereignisfelds ganz oder teilweise in die Suchleiste eingeben. Um ein Ereignis zu kopieren, wählen Sie das zu kopierende Ereignis aus und klicken Sie dann auf Kopieren.



Query results		Command output		
Results <a href="#">Info</a>				
<input type="text" value="Search queries"/>		<span>&lt; 1 ... &gt;</span> <span>⚙️</span>		
<input type="checkbox"/>	eventID	eventName	eventSource	eventTime
<input type="checkbox"/>	550c75c7-711b-449f-9450-	GetEventDataStore	cloudtrail	2023-06-23 19:21:16.000
<input type="checkbox"/>	1bd8253a-80ae-4814-a57a-	GetEventDataStore	cloudtrail	2023-06-23 19:21:16.000
<input type="checkbox"/>	b56d9af8-7097-4119-9b5d-	GetEventDataStore	cloudtrail	2023-06-23 19:21:09.000
<input type="checkbox"/>	f874e2f4-d426-4a6b-ab46-	GetEventDataStore	cloudtrail	2023-06-23 19:21:09.000
<input type="checkbox"/>	c1053f2c-5b2d-457d-9655-	GetEventDataStore	cloudtrail	2023-06-23 19:21:08.000
<input type="checkbox"/>	5820dec3-c550-491f-a8c3-	GetEventDataStore	cloudtrail	2023-06-23 19:21:16.000
<input type="checkbox"/>	064ccc03-0011-48f9-9fbc-	ListEventDataStores	cloudtrail	2023-07-11 19:18:51.000
<input type="checkbox"/>	94aa8a00-523f-46f0-9b61-	ListEventDataStores	cloudtrail	2023-07-10 14:34:40.000

- Zeigen Sie auf der Registerkarte Befehlsausgabe Metadaten über die ausgeführte Abfrage an, z. B. die ID des Ereignisdatenspeichers, die Laufzeit, die Anzahl der gescannten Ergebnisse und ob die Abfrage erfolgreich war oder nicht. Wenn Sie die Abfrageergebnisse in einem Amazon S3-Bucket gespeichert haben, enthalten die Metadaten auch einen Link zum S3-Bucket, der die gespeicherten Abfrageergebnisse enthält.

Query results		Command output		
Output				
Time stamp	Status	Delivery status	Response	Query SQL
2022-10-17T21:28:17.277Z	<span style="color: green;">✔ Successful</span>	<a href="#">View in S3</a>	195 records matched   464 records (125.5 kB) scanned in 0.4s @ 1145.7 records/s (309.9 kB/s)	SELECT eventID, eventName, eventSource, eventTime FROM 3ft

## Gespeicherte Abfrageergebnisse herunterladen

Nachdem Sie die Abfrageergebnisse gespeichert haben, müssen Sie in der Lage sein, die Datei mit den Abfrageergebnissen zu finden. CloudTrail übermittelt Ihre Abfrageergebnisse an einen Amazon S3 S3-Bucket, den Sie beim Speichern der Abfrageergebnisse angeben.

### i Note

Wenn Sie Abfrageergebnisse speichern, werden die Abfrageergebnisse möglicherweise in der Konsole angezeigt, bevor sie im S3-Bucket sichtbar sind, da CloudTrail die

Abfrageergebnisse erst nach Abschluss des Abfragescans geliefert werden. Die meisten Abfragen werden zwar je nach Größe Ihres Ereignisdatenspeichers innerhalb weniger Minuten abgeschlossen, es kann jedoch erheblich länger dauern, CloudTrail bis Abfrageergebnisse an Ihren S3-Bucket übermittelt werden. CloudTrail übermittelt die Abfrageergebnisse im komprimierten Gzip-Format an den S3-Bucket. Im Durchschnitt können Sie nach Abschluss des Abfragescans mit einer Latenz von 60 bis 90 Sekunden für jedes GB an Daten rechnen, das an den S3-Bucket übermittelt wird.

## Themen

- [Finden Sie Ihre gespeicherten Abfrageergebnisse in CloudTrail Lake](#)
- [Laden Sie Ihre in CloudTrail Lake gespeicherten Abfrageergebnisse herunter](#)

## Finden Sie Ihre gespeicherten Abfrageergebnisse in CloudTrail Lake

CloudTrail veröffentlicht das Abfrageergebnis und signiert Dateien in Ihrem S3-Bucket. Die Abfrageergebnisdatei enthält die Ausgabe der gespeicherten Abfrage und die Sign-Datei stellt die Signatur und den Hashwert für die Abfrageergebnisse bereit. Sie können die Sign-Datei verwenden, um die Abfrageergebnisse zu validieren. Weitere Informationen zur Validierung von Abfrageergebnissen finden Sie unter [Validierung von gespeicherten Abfrageergebnissen](#).

Zum Abrufen einer Abfrageergebnis- oder Sign-Datei können Sie die Amazon-S3-Konsole, die Amazon-S3-Befehlszeilenschnittstelle (CLI) oder die API verwenden.

Suchen Sie Abfrageergebnisse und Sign-Dateien mit der Amazon-S3-Konsole wie folgt

1. Öffnen Sie die Amazon S3-Konsole.
2. Wählen Sie den Bucket aus, den Sie angegeben haben.
3. Navigieren Sie durch die Objekthierarchie, bis Sie die Abfrageergebnis- und Sign-Dateien finden. Die Abfrageergebnisdatei hat die Erweiterung `.csv.gz` und die Sign-Datei hat die Erweiterung `.json`.

Sie navigieren dabei durch eine Objekthierarchie, die dem folgenden Beispiel ähnelt, Bucket-Name, Konto-ID, Region, Datum und Abfrage-ID sind jedoch anders.

```
All Buckets
  Bucket_Name
    AWSLogs
      Account_ID;
        CloudTrail-Lake
          Query
            2022
              06
                20
                  Query_ID
```

## Laden Sie Ihre in CloudTrail Lake gespeicherten Abfrageergebnisse herunter

Wenn Sie Abfrageergebnisse speichern, CloudTrail werden zwei Arten von Dateien an Ihren Amazon S3 S3-Bucket übermittelt.

- Eine Sign-Datei im JSON-Format, mit der Sie die Abfrageergebnisdateien validieren können. Die Sign-Datei heißt `result_sign.json`. Weitere Informationen zur Sign-Datei finden Sie unter [CloudTrail Struktur der Datei signieren](#).
- Eine oder mehrere Abfrageergebnisdateien im CSV-Format, die die Ergebnisse der Abfrage enthalten. Die Anzahl der gelieferten Abfrageergebnisdateien hängt von der Gesamtgröße der Abfrageergebnisse ab. Die maximale Dateigröße für eine Abfrageergebnisdatei beträgt 1 TB. Jede Abfrageergebnisdatei hat den Namen `result_ number .csv.gz`. Wenn die Gesamtgröße der Abfrageergebnisse beispielsweise 2 TB beträgt, hätten Sie zwei Abfrageergebnisdateien, `result_1.csv.gz` und `result_2.csv.gz`.

CloudTrail Abfrageergebnis und Signierdateien sind Amazon S3 S3-Objekte. Sie können die S3-Konsole, die AWS Command Line Interface (CLI) oder die S3-API verwenden, um Abfrageergebnisse abzurufen und Dateien zu signieren.

Im folgenden Verfahren wird beschrieben, wie Sie die Abfrageergebnis- und Sign-Dateien mit der Amazon-S3-Konsole herunterladen.

Laden Sie eine Abfrageergebnis- oder eine Sign-Datei mit der Amazon-S3-Konsole wie folgt herunter

1. Öffnen Sie die Amazon S3-Konsole.
2. Wählen Sie den Bucket und die Datei, die Sie herunterladen möchten.

**Objects (2)**

Objects are the fundamental entities stored in Amazon S3. You can use [Amazon S3 Inventory](#) to get a list of all objects in your bucket. For others to access your objects, you'll need to explicitly grant them permissions. [Learn more](#)

Find objects by prefix

<input type="checkbox"/>	Name	Type	Last modified	Size	Storage class
<input type="checkbox"/>	<a href="#">result_1.csv.gz</a>	gz	October 17, 2022, 16:18:17 (UTC-05:00)	5.4 KB	Standard
<input type="checkbox"/>	<a href="#">result_sign.json</a>	json	October 17, 2022, 16:18:19 (UTC-05:00)	929.0 B	Standard

- Wählen Sie **Download** und befolgen Sie die Anweisungen, um die Datei zu speichern.

### Note

Einige Browser, wie beispielsweise Chrome, extrahieren die Abfrageergebnisdatei automatisch für Sie. Wenn Ihr Browser dies unterstützt, fahren Sie mit Schritt 5 fort.

- Verwenden Sie ein Produkt wie [7-Zip](#), um die Abfrageergebnisdatei zu extrahieren.
- Öffnen Sie die Abfrageergebnis- oder Sign-Datei.

## Validierung von gespeicherten Abfrageergebnissen

Um festzustellen, ob die Abfrageergebnisse nach CloudTrail der Übermittlung der Abfrageergebnisse geändert, gelöscht oder unverändert wurden, können Sie die Integritätsprüfung der CloudTrail Abfrageergebnisse verwenden. Dieses Feature wurde mit dem Branchenstandard entsprechenden Algorithmen entwickelt: SHA-256 für die Hashfunktion und SHA-256 mit RSA für digitale Signaturen. Dadurch ist es rechnerisch unmöglich, CloudTrail Abfrageergebnisdateien unbemerkt zu ändern, zu löschen oder zu fälschen. Sie können die Befehlszeilenschnittstelle zur Validierung von Abfrageergebnisdateien verwenden.

### Warum sollten Sie diese Funktion nutzen?

Validierte Abfrageergebnisdateien sind bei Sicherheits- und kriminaltechnischen Ermittlungen unersetzlich. Mit einer validierten Abfrageergebnisdatei können Sie beispielsweise bestätigen, dass sich die Abfrageergebnisdatei selbst nicht geändert hat. Bei der Integritätsprüfung der CloudTrail Abfrageergebnisdatei erfahren Sie auch, ob eine Abfrageergebnisdatei gelöscht oder geändert wurde.

### Themen

- [Überprüfen Sie die gespeicherten Abfrageergebnisse mit AWS CLI](#)
- [CloudTrail Struktur der Datei signieren](#)

- [Benutzerdefinierte Implementierungen der Integritätsprüfung von CloudTrail Abfrageergebnisdateien](#)

## Überprüfen Sie die gespeicherten Abfrageergebnisse mit AWS CLI

Sie können die Integrität der Abfrageergebnisdateien und der Sign-Datei mit dem Befehl [aws cloudtrail verify-query-results](#) überprüfen.

### Voraussetzungen

Zum Überprüfen der Integrität von Abfrageergebnissen mit der Befehlszeile müssen die folgenden Bedingungen erfüllt sein:

- Sie müssen über eine Online-Verbindung zu verfügen AWS.
- Sie müssen AWS CLI Version 2 verwenden.
- Um Abfrageergebnisdateien zu validieren und die Datei lokal zu signieren, gelten die folgenden Bedingungen:
  - Sie müssen die Abfrageergebnisdateien und die Sign-Datei im angegebenen Dateipfad ablegen. Geben Sie den Dateipfad als Wert für den `--local-export-path`-Parameter an.
  - Sie dürfen die Abfrageergebnisdateien und die Sign-Datei nicht umbenennen.
- Um die Abfrageergebnisdateien zu validieren und die Datei im S3-Bucket zu signieren, gelten die folgenden Bedingungen:
  - Sie dürfen die Abfrageergebnisdateien und die Sign-Datei nicht umbenennen.
  - Sie müssen über Lesezugriff auf den Amazon-S3-Bucket verfügen, der die Abfrageergebnisdateien und die Sign-Datei enthält.
  - Das angegebene S3-Präfix muss die Abfrageergebnisdateien und die Sign-Datei enthalten. Geben Sie das S3-Präfix als Wert für den `--s3-prefix`-Parameter an.

### verify-query-results

Der Befehl `verify-query-results` überprüft den Hashwert jeder Abfrageergebnisdatei, indem er den Wert mit dem `fileHashValue` in der Sign-Datei vergleicht und validiert dann den Wert `hashSignature` in der Sign-Datei.

Wenn Sie Abfrageergebnisse überprüfen, können Sie entweder die Befehlszeilenoptionen `--s3-bucket` und `--s3-prefix` verwenden, um die Abfrageergebnisdateien zu validieren und die in einem S3-Bucket gespeicherte Datei zu signieren, oder Sie verwenden die Befehlszeilenoption `--local-export-`

path, um eine lokale Überprüfung der heruntergeladenen Abfrageergebnisdateien und der Sign-Datei durchzuführen.

### Note

Der Befehl `verify-query-results` ist regionsspezifisch. Sie müssen die `--region` globale Option angeben, um die Abfrageergebnisse für einen bestimmten Bereich zu überprüfen AWS-Region.

Im Folgenden werden die Optionen für den Befehl `verify-query-results` aufgeführt.

`--s3-bucket` *<string>*

Gibt den S3-Bucket-Namen an, der die Abfrageergebnisdateien und die Sign-Datei speichert. Sie können diesen Parameter nicht mit `--local-export-path` verwenden.

`--s3-prefix` *<string>*

Gibt den S3-Pfad des S3-Ordners an, der die Abfrageergebnisdateien und die Sign-Datei enthält (z. B. `s3/path/`). Sie können diesen Parameter nicht mit `--local-export-path` verwenden. Sie müssen diesen Parameter nicht angeben, wenn sich die Dateien im Stammverzeichnis des S3-Buckets befinden.

`--local-export-path` *<string>*

Gibt das lokale Verzeichnis an, das die Abfrageergebnisdateien und die Sign-Datei enthält (z. B. `/local/path/to/export/file/`). Sie können diesen Parameter nicht mit `--s3-bucket` oder `--s3-prefix` verwenden.

### Beispiele

Im folgenden Beispiel werden Abfrageergebnisse mithilfe der Befehlszeilenoptionen `--s3-bucket` und `--s3-prefix` überprüft, um den Namen und das Präfix des S3-Buckets anzugeben, der die Abfrageergebnisdateien und die Sign-Datei enthält.

```
aws cloudtrail verify-query-results --s3-bucket bucket_name --s3-prefix prefix --  
region region
```

Im folgenden Beispiel werden heruntergeladene Abfrageergebnisse mithilfe der `--local-export-path`-Befehlszeilenoption überprüft, um den lokalen Pfad für die Abfrageergebnisdateien und die Sign-Datei anzugeben. Weitere Informationen zum Herunterladen von Abfrageergebnisdateien finden Sie unter [Laden Sie Ihre in CloudTrail Lake gespeicherten Abfrageergebnisse herunter](#).

```
aws cloudtrail verify-query-results --local-export-path local_file_path --region region
```

## Validierungsergebnisse

Die folgende Tabelle beschreibt die möglichen Validierungsmeldungen für Abfrageergebnisdateien und der Sign-Datei.

Dateityp	Validierungsmeldung	Beschreibung
Sign file	Successfully validated sign and query result files	Die Signatur der Sign-Datei ist gültig. Die Abfrageergebnisdateien, auf die sie verweist, können überprüft werden.
Query result file	ValidationError: "File <i>file_name</i> has inconsistent hash value with hash value recorded in sign file, hash value in sign file is <i>expected_hash</i> , but get <i>computed_hash</i>	Die Überprüfung ist fehlgeschlagen, weil der Hashwert für die Abfrageergebnisdatei nicht mit dem <code>fileHashValue</code> in der Sign-Datei übereinstimmt.
Sign file	ValidationError: Invalid signature in sign file	Die Überprüfung der Sign-Datei ist fehlgeschlagen, da die Signatur nicht gültig ist.

## CloudTrail Struktur der Datei signieren

Die Sign-Datei enthält den Namen von allen Abfrageergebnissen, die an Ihren Amazon-S3-Bucket übermittelt wurden, als Sie die Abfrageergebnisse gespeichert haben, den Hash-Wert für jede Abfrageergebnisdatei und die digitale Signatur der Datei. Die digitale Signatur und Hash-

Werte werden zur Validierung der Integrität der Abfrageergebnisdateien und der Sign-Datei selbst verwendet.

## Speicherort von Sign-Dateien

Die Sign-Datei wird an einen Amazon-S3-Bucket-Speicherort übermittelt, der dieser Syntax folgt.

```
s3://s3-bucket-name/optional-prefix/AWSLogs/aws-account-ID/CloudTrail-Lake/  
Query/year/month/date/query-ID/result_sign.json
```

## Beispiel von Sign-Dateiinhalten

Die folgende Beispielsigndatei enthält Informationen für CloudTrail Lake-Abfrageergebnisse.

```
{  
  "version": "1.0",  
  "region": "us-east-1",  
  "files": [  
    {  
      "fileHashValue" :  
"de85a48b8a363033c891abd723181243620a3af3b6505f0a44db77e147e9c188",  
      "fileName" : "result_1.csv.gz"  
    }  
  ],  
  "hashAlgorithm" : "SHA-256",  
  "signatureAlgorithm" : "SHA256withRSA",  
  "queryCompleteTime": "2022-05-10T22:06:30Z",  
  "hashSignature" :  
"7664652aaf1d5a17a12ba50abe6aca77c0ec76264bdf7dce71ac6d1c7781117c2a412e5820bccf473b1361306dff6",  
  "publicKeyFingerprint" : "67b9fa73676d86966b449dd677850753"  
}
```

## Beschreibungen der Felder in Sign-Dateien

Im Folgenden sind Beschreibungen für die einzelnen Felder in der Sign-Datei aufgeführt:

### version

Die Version der Sign-Datei.

### region

Die Region für das AWS Konto, das zum Speichern der Abfrageergebnisse verwendet wurde.



### `files.fileHashValue`

Der im Hexadezimalformat verschlüsselte Hash-Wert des komprimierten Inhalts der Abfrageergebnisdatei.

### `files.fileName`

Der Name der Abfrageergebnisdatei.

### `hashAlgorithm`

Der für das Hashing der Abfrageergebnisdatei verwendete Hash-Algorithmus.

### `signatureAlgorithm`

Der zum Signieren der Datei verwendete Algorithmus.

### `queryCompleteTime`

Gibt an, wann die Abfrageergebnisse an den S3-Bucket CloudTrail übermittelt wurden. Sie können diesen Wert verwenden, um den öffentlichen Schlüssel zu finden.

### `hashSignature`

Die Hash-Signatur für die Datei.

### `publicKeyFingerprint`

Der im Hexadezimalformat verschlüsselte Fingerabdruck des öffentlichen Schlüssels, der zum Signieren der Datei verwendet wurde.

## Benutzerdefinierte Implementierungen der Integritätsprüfung von CloudTrail Abfrageergebnisdateien

Da branchenübliche, offen verfügbare kryptografische Algorithmen und Hashfunktionen CloudTrail verwendet werden, können Sie Ihre eigenen Tools erstellen, um die Integrität der CloudTrail Abfrageergebnisdateien zu überprüfen. Wenn Sie Abfrageergebnisse in einem Amazon S3 S3-Bucket

speichern, wird CloudTrail eine Signierdatei an Ihren S3-Bucket gesendet. Sie können Ihre eigene Validierungslösung implementieren, um die Signatur- und Abfrageergebnisdateien zu überprüfen. Weitere Informationen zur Sign-Datei finden Sie unter [CloudTrail Struktur der Datei signieren](#).

In diesem Thema wird das Signieren von Sign-Dateien beschrieben. Zudem werden detailliert die Schritte dargelegt, die zur Implementierung einer Lösung für die Validierung von Sign-Dateien sowie den von der Sign-Datei referenzierten Abfrageergebnisdateien ausgeführt werden müssen.

### Verstehen, wie CloudTrail Signdateien signiert werden

CloudTrail Signierdateien werden mit digitalen RSA-Signaturen signiert. CloudTrail führt für jede Signierdatei Folgendes aus:

1. Erstellt eine Hashliste, die den Hashwert für jede Abfrageergebnisdatei enthält.
2. Ein privater Schlüssel, der für die Region eindeutig ist, wird abgerufen.
3. Der SHA-256-Hash der Zeichenfolge und der private Schlüssel werden an den RSA-Signaturalgorithmus übergeben, der die digitale Signatur generiert.
4. Der Byte-Signaturcode wird im Hexadezimalformat verschlüsselt.
5. Fügt die digitale Signatur in die Sign-Datei ein.

### Inhalt der Datensignatur-Zeichenfolge

Die Datensignierungszeichenfolge besteht aus dem Hashwert für jede Abfrageergebnisdatei, getrennt durch ein Leerzeichen. Die Sign-Datei listet den `fileHashValue` für jede Abfrageergebnisdatei auf.

### Schritte der benutzerdefinierten Validierungsimplementierung

Bei der Implementierung einer benutzerdefinierten Validierungslösung müssen Sie zunächst die Sign-Datei und anschließend die von ihr referenzierten Abfrageergebnisdateien validieren.

### Validieren der Sign-Datei

Zur Validierung einer Sign-Datei benötigen Sie die Signatur, den öffentlichen Schlüssel, dessen privater Schlüssel zum Signieren verwendet wurde und eine berechnete Datensignatur-Zeichenfolge.

1. Rufen Sie die Sign-Datei ab.
2. Überprüfen Sie, ob die Sign-Datei vom ursprünglichen Speicherort abgerufen wurde.
3. Rufen Sie die im Hexadezimalformat verschlüsselte Signatur der Sign-Datei ab.

4. Rufen Sie den im Hexadezimalformat verschlüsselten Fingerabdruck des öffentlichen Schlüssels ab, dessen privater Schlüssel zum Signieren der Sign-Datei verwendet wurde.
5. Rufen Sie den öffentlichen Schlüssel für den `queryCompleteTime` entsprechenden Zeitraum der Sign-Datei ab. Wählen Sie für den Zeitraum eine frühere `StartTime` als die `queryCompleteTime` und eine spätere `EndTime` als die `queryCompleteTime`.
6. Wählen Sie aus den abgerufenen öffentlichen Schlüsseln denjenigen aus, dessen Fingerabdruck mit dem `publicKeyFingerprint`-Wert in der Sign-Datei übereinstimmt.
7. Erstellen Sie mithilfe einer Hashliste, die den Hashwert für jede Abfrageergebnisdatei durch ein Leerzeichen getrennt enthält, die Datensignaturzeichenfolge neu, die zur Überprüfung der Signatur der Sign-Datei verwendet wird. Die Sign-Datei listet den `fileHashValue` für jede Abfrageergebnisdatei auf.

Wenn das `files`-Array Ihrer Sign-Datei beispielsweise die folgenden drei Abfrageergebnisdateien enthält, lautet Ihre Hashliste „aaa bbb ccc“.

```
"files": [  
  {  
    "fileHashValue" : "aaa",  
    "fileName" : "result_1.csv.gz"  
  },  
  {  
    "fileHashValue" : "bbb",  
    "fileName" : "result_2.csv.gz"  
  },  
  {  
    "fileHashValue" : "ccc",  
    "fileName" : "result_3.csv.gz"  
  }  
],
```

- Überprüfen Sie die Signatur, indem Sie den SHA-256-Hash der Zeichenfolge, den öffentlichen Schlüssel und die Signatur als Parameter an den RSA-Signaturprüfalgorithmus übergeben. Wenn das Ergebnis "True" lautet, ist die Sign-Datei gültig.

## Validieren der Abfrageergebnisdateien

Überprüfen Sie die Abfrageergebnisdateien, auf die die Sign-Datei verweist, wenn die Sign-Datei gültig ist. Um die Integrität einer Abfrageergebnisdatei zu überprüfen, berechnen Sie ihren SHA-256-Hashwert für ihren komprimierten Inhalt und vergleichen Sie die Ergebnisse mit dem `fileHashValue` für die Abfrageergebnisdatei, die in der Sign-Datei aufgezeichnet wurde. Stimmen die Hashwerte überein, ist die Abfrageergebnisdatei gültig.

In den folgenden Abschnitten wird dieser Validierungsprozess ausführlich beschrieben.

### A. Abrufen der Sign-Datei

Die ersten Schritte bestehen darin, die Sign-Datei und den Fingerabdruck des öffentlichen Schlüssels abzurufen.

- Rufen Sie die Sign-Datei aus Ihrem Amazon S3-Bucket für die Abfrageergebnisse ab, die Sie validieren möchten.
- Rufen Sie als Nächstes den `hashSignature`-Wert aus der Sign-Datei ab.
- Rufen Sie in der Sign-Datei den Fingerabdruck des öffentlichen Schlüssels, dessen privater Schlüssel zum Signieren der Datei verwendet wurde, aus dem Feld `publicKeyFingerprint` ab.

### B. Abrufen des öffentlichen Schlüssels zur Validierung der Sign-Datei

Um den öffentlichen Schlüssel zur Validierung der Signdatei zu erhalten, können Sie entweder die AWS CLI oder die CloudTrail API verwenden. In beiden Fällen geben Sie einen Zeitraum (Start- und Endzeitpunkt) für die zu validierende Sign-Datei an. Verwenden Sie einen Zeitraum, der der `queryCompleteTime` in der Sign-Datei entspricht. Für den angegebenen Zeitraum können ein oder mehrere öffentliche Schlüssel zurückgegeben werden. Möglicherweise überschneiden sich die Gültigkeitszeiträume der zurückgegebenen Schlüssel.

#### Note

Da pro Region unterschiedliche private/öffentliche Schlüsselpaare CloudTrail verwendet werden, ist jede Signierdatei mit einem privaten Schlüssel signiert, der für ihre Region

einzigartig ist. Wenn Sie also die Sign-Datei einer bestimmten Region validieren, müssen Sie den öffentlichen Schlüssel dieser Region abrufen.

Verwenden Sie die, um öffentliche Schlüssel AWS CLI abzurufen

Um mit dem einen öffentlichen Schlüssel für eine Signdatei abzurufen AWS CLI, verwenden Sie den `cloudtrail list-public-keys` Befehl. Der Befehl hat das folgende Format:

```
aws cloudtrail list-public-keys [--start-time <start-time>] [--end-time <end-time>]
```

Bei den Parametern für den Start- und den Endzeitpunkt handelt es sich um optionale UTC-Zeitstempel. Wenn diese Parameter nicht angegeben werden, wird die aktuelle Uhrzeit verwendet und der aktuell aktive öffentliche Schlüssel (oder mehrere) wird zurückgegeben.

Beispielantwort

Die Antwort besteht aus einer Liste mit JSON-Objekten, die den bzw. die zurückgegebenen Schlüssel darstellen:

Verwenden Sie die CloudTrail API, um öffentliche Schlüssel abzurufen

Um mithilfe der CloudTrail API einen öffentlichen Schlüssel für eine Signdatei abzurufen, übergeben Sie Werte für die Startzeit und die Endzeit an die `ListPublicKeys` API. Die API `ListPublicKeys` gibt die öffentlichen Schlüssel, deren private Schlüssel zum Signieren der Sign-Datei verwendet wurden, für den angegebenen Zeitraum zurück. Für jeden öffentlichen Schlüssel gibt die API außerdem den entsprechenden Fingerabdruck zurück.

## ListPublicKeys

In diesem Abschnitt werden die Anforderungsparameter sowie die Antwortelemente der `ListPublicKeys`-API beschrieben.

### Note

Hinsichtlich der Codierung der binären Felder von `ListPublicKeys` sind Änderungen vorbehalten.

## Anfrageparameter

Name	Beschreibung
StartTime	Gibt optional in UTC den Beginn des Zeitbereichs an, in dem der öffentliche Schlüssel für die CloudTrail Signdatei nachgeschlagen werden soll. Wenn StartTime nicht angegeben, wird die aktuelle Uhrzeit verwendet und der aktuelle öffentliche Schlüssel zurückgegeben.  Typ: DateTime
EndTime	Gibt optional in UTC das Ende des Zeitbereichs an, in dem nach öffentlichen Schlüsseln für Signaturdateien gesucht CloudTrail werden soll. Wenn nicht angegeben, EndTime wird die aktuelle Uhrzeit verwendet.  Typ: DateTime

## Antwortelemente

PublicKeyList ist ein Array aus PublicKey-Objekten und enthält folgende Elemente:

Name	Beschreibung
Value	Dies gibt den mit DER-verschlüsselten öffentlichen Schlüsselwert im PKCS #1-Format an.  Typ: Blob
ValidityStartTime	Dies gibt den Beginn des Gültigkeitszeitraums für den öffentlichen Schlüssel an.  Typ: DateTime
ValidityEndTime	Dies gibt das Ende des Gültigkeitszeitraums für den öffentlichen Schlüssel an.  Typ: DateTime
Fingerprint	Die Fingerabdruck des öffentlichen Schlüssels. Mit dem Fingerabdruck kann der öffentliche Schlüssel identifiziert werden, der zur Validierung der Sign-Datei verwendet werden muss.

## Typ: Zeichenfolge

### C. Auswählen des öffentlichen Schlüssels für die Validierung

Wählen Sie aus den von `list-public-keys` oder `ListPublicKeys` abgerufenen öffentlichen Schlüsseln denjenigen aus, dessen Fingerabdruck mit dem im Feld `publicKeyFingerprint` der Sign-Datei aufgezeichneten Fingerabdruck übereinstimmt. Diesen öffentlichen Schlüssel verwenden Sie für die Validierung der Sign-Datei.

### D. Neues Erstellen der Datensignatur-Zeichenfolge

Nachdem Sie über die Signatur der Sign-Datei und dem entsprechenden öffentlichen Schlüssel verfügen, berechnen Sie die Datensignatur-Zeichenfolge. Wenn Sie die Datensignatur-Zeichenfolge berechnet haben, stehen Ihnen alle für die Signaturvalidierung benötigten Daten zur Verfügung.

Die Datensignierungszeichenfolge besteht aus dem Hashwert für jede Abfrageergebnisdatei, getrennt durch ein Leerzeichen. Wenn Sie diese Zeichenfolge neu erstellt haben, können Sie die Sign-Datei validieren.

### E. Validieren der Sign-Datei

Übergeben Sie die neu erstellten Datensignatur-Zeichenfolge, die digitale Signatur und den öffentlichen Schlüssel an den RSA-Signaturprüfalgorithmus. Wenn das Ergebnis "True" lautet, wurde die Signatur der Sign-Datei überprüft und die Sign-Datei ist gültig.

### F. Validieren der Abfrageergebnisdateien

Nachdem Sie die Sign-Dateien validiert haben, können Sie die referenzierten Abfrageergebnisdateien überprüfen. Die Sign-Datei enthält die SHA-256-Hashwerte der Abfrageergebnisdateien. Wenn eine der Abfrageergebnisdateien nach der CloudTrail Lieferung geändert wurde, ändern sich die SHA-256-Hashes und die Signatur der Signdatei stimmt nicht überein.

Verwenden Sie das folgende Verfahren, um die im `files`-Array der Sign-Datei aufgelisteten Abfrageergebnisdateien zu validieren.

1. Rufen Sie den ursprünglichen Hash der Datei aus dem Feld `files.fileHashValue` der Sign-Datei ab.
2. Führen Sie für den komprimierten Inhalt der Abfrageergebnisdatei einen Hash mit dem Hash-Algorithmus in `hashAlgorithm` aus.

3. Vergleichen Sie den Hashwert, den Sie für jede Abfrageergebnisdatei generiert haben, mit dem `files.fileHashValue` in der Sign-Datei. Wenn die Hashes übereinstimmen, sind die Abfrageergebnisdateien gültig.

## Überprüfen von Signatur- und Abfrageergebnisdateien offline

Wenn Sie Sign- und Abfrageergebnisdateien offline validieren möchten, können Sie dazu die in den vorherigen Abschnitten beschriebenen Verfahren nutzen. Sie müssen jedoch die folgenden Informationen zu öffentlichen Schlüsseln berücksichtigen.

### Öffentliche Schlüssel

Bei einer Offline-Validierung muss der öffentliche Schlüssel, der für die Validierung der Abfrageergebnisdateien in einem bestimmten Zeitraum erforderlich ist, zuvor online abgerufen (z. B. über den Aufruf von `ListPublicKeys`) und dann offline gespeichert werden. Dieser Schritt muss stets wiederholt werden, wenn Sie weitere Dateien außerhalb des ursprünglich angegebenen Zeitraums validieren möchten.

### Snippet mit Beispielvalidierung

Der folgende Beispielausschnitt enthält einen Grundcode für die Überprüfung von Zeichen- und Abfrageergebnisdateien. CloudTrail Das Code-Skelett basiert nicht auf einer Online- oder Offline-Validierung, sodass Sie entscheiden können, ob es mit oder ohne Online-Verbindung zu AWS implementiert werden soll. Die empfohlene Implementierung nutzt [Java Cryptography Extension \(JCE\)](#) und [Bouncy Castle](#) als Sicherheitsanbieter.

Das Beispiel-Snippet zeigt die folgenden Schritte:

- So erstellen Sie die Datensignatur-Zeichenfolge für die Validierung der Sign-Dateisignatur.
- So überprüfen Sie die Sign-Dateisignatur.
- So berechnen Sie den Hashwert für die Abfrageergebnisdatei und vergleichen ihn mit dem in der Sign-Datei aufgeführten Wert `fileHashValue`, um die Authentizität der Abfrageergebnisdatei zu überprüfen.

```
import org.apache.commons.codec.binary.Hex;
import org.bouncycastle.asn1.pkcs.PKCSObjectIdentifiers;
import org.bouncycastle.asn1.pkcs.RSAPublicKey;
import org.bouncycastle.asn1.x509.AlgorithmIdentifier;
import org.bouncycastle.asn1.x509.SubjectPublicKeyInfo;
```



```
import org.bouncycastle.jce.provider.BouncyCastleProvider;
import org.json.JSONArray;
import org.json.JSONObject;

import java.security.KeyFactory;
import java.security.MessageDigest;
import java.security.PublicKey;
import java.security.Security;
import java.security.Signature;
import java.security.spec.X509EncodedKeySpec;
import java.util.ArrayList;
import java.util.Arrays;
import java.util.List;
import java.util.stream.Collectors;

public class SignFileValidationSampleCode {

    public void validateSignFile(String s3Bucket, String s3PrefixPath) throws Exception
    {
        MessageDigest messageDigest = MessageDigest.getInstance("SHA-256");

        // Load the sign file from S3 (using Amazon S3 Client) or from your local copy
        JSONObject signFile = loadSignFileToMemory(s3Bucket, String.format("%s/%s",
s3PrefixPath, "result_sign.json"));

        // Using the Bouncy Castle provider as a JCE security provider - http://
www.bouncycastle.org/
        Security.addProvider(new BouncyCastleProvider());

        List<String> hashList = new ArrayList<>();

        JSONArray jsonArray = signFile.getJSONArray("files");

        for (int i = 0; i < jsonArray.length(); i++) {
            JSONObject file = jsonArray.getJSONObject(i);
            String fileS3objectKey = String.format("%s/%s", s3PrefixPath,
file.getString("fileName"));

            // Load the export file from S3 (using Amazon S3 Client) or from your local
copy
            byte[] exportFileContent = loadCompressedExportFileInMemory(s3Bucket,
fileS3objectKey);
            messageDigest.update(exportFileContent);
```

```

byte[] exportFileHash = messageDigest.digest();
messageDigest.reset();
byte[] expectedHash = Hex.decodeHex(file.getString("fileHashValue"));

boolean signaturesMatch = Arrays.equals(expectedHash, exportFileHash);
if (!signaturesMatch) {
    System.err.println(String.format("Export file: %s/%s hash doesn't
match.\tExpected: %s Actual: %s",
        s3Bucket, fileS3ObjectKey,
        Hex.encodeHexString(expectedHash),
Hex.encodeHexString(exportFileHash)));
} else {
    System.out.println(String.format("Export file: %s/%s hash match",
        s3Bucket, fileS3ObjectKey));
}

hashList.add(file.getString("fileHashValue"));
}
String hashListString = hashList.stream().collect(Collectors.joining(" "));

/*
NOTE:
To find the right public key to verify the signature, call CloudTrail
ListPublicKey API to get a list
of public keys, then match by the publicKeyFingerprint in the sign file.
Also, the public key bytes
returned from ListPublicKey API are DER encoded in PKCS#1 format:

PublicKeyInfo ::= SEQUENCE {
    algorithm      AlgorithmIdentifier,
    PublicKey      BIT STRING
}

AlgorithmIdentifier ::= SEQUENCE {
    algorithm      OBJECT IDENTIFIER,
    parameters    ANY DEFINED BY algorithm OPTIONAL
}
*/
byte[] pkcs1PublicKeyBytes =
getPublicKey(signFile.getString("queryCompleteTime"),
    signFile.getString("publicKeyFingerprint"));
byte[] signatureContent = Hex.decodeHex(signFile.getString("hashSignature"));

// Transform the PKCS#1 formatted public key to x.509 format.

```

```
RSAPublicKey rsaPublicKey = RSAPublicKey.getInstance(pkcs1PublicKeyBytes);
AlgorithmIdentifier rsaEncryption = new
AlgorithmIdentifier(PKCSObjectIdentifiers.rsaEncryption, null);
SubjectPublicKeyInfo publicKeyInfo = new SubjectPublicKeyInfo(rsaEncryption,
rsaPublicKey);

// Create the PublicKey object needed for the signature validation
PublicKey publicKey = KeyFactory.getInstance("RSA", "BC")
    .generatePublic(new X509EncodedKeySpec(publicKeyInfo.getEncoded()));

// Verify signature
Signature signature = Signature.getInstance("SHA256withRSA", "BC");
signature.initVerify(publicKey);
signature.update(hashListString.getBytes("UTF-8"));

if (signature.verify(signatureContent)) {
    System.out.println("Sign file signature is valid.");
} else {
    System.err.println("Sign file signature failed validation.");
}

System.out.println("Sign file validation completed.");
}
}
```

## Führen Sie CloudTrail Lake-Abfragen aus und verwalten Sie sie mit dem AWS CLI

Sie können den verwenden AWS CLI , um Ihre CloudTrail Lake-Abfragen auszuführen und zu verwalten. Denken Sie bei der Verwendung von daran AWS CLI, dass Ihre Befehle in der für Ihr Profil AWS-Region konfigurierten Version ausgeführt werden. Wenn Sie die Befehle in einer anderen Region ausführen möchten, ändern Sie entweder die Standardregion für Ihr Profil, oder verwenden Sie den `--region`-Parameter mit dem Befehl.

### Verfügbare Befehle für CloudTrail Lake-Abfragen

Zu den Befehlen zum Ausführen und Verwalten von Abfragen in CloudTrail Lake gehören:

- [start-query](#)um eine Abfrage auszuführen.
- [describe-query](#)um Metadaten zu einer Abfrage zurückzugeben.
- [get-query-results](#)um Abfrageergebnisse für die angegebene Abfrage-ID zurückzugeben.

- [list-queries](#) um eine Liste von Abfragen für den angegebenen Ereignisdatenspeicher abzurufen.
- [cancel-query](#) um eine laufende Abfrage abzuberechnen.

Eine Liste der verfügbaren Befehle für CloudTrail Lake-Ereignisdatenspeicher finden Sie unter [Verfügbare Befehle für Ereignisdatenspeicher](#).

Eine Liste der verfügbaren Befehle für CloudTrail Lake-Integrationen finden Sie unter [Verfügbare Befehle für CloudTrail Lake-Integrationen](#).

## Starten Sie eine Abfrage mit AWS CLI

Mit dem folgenden AWS CLI start-query Beispielbefehl wird eine Abfrage für den Ereignisdatenspeicher ausgeführt, der in der Abfrageanweisung als ID angegeben ist, und die Abfrageergebnisse werden an einen angegebenen S3-Bucket gesendet. Der --query-statement-Parameter stellt eine SQL-Abfrage bereit, die in einfache Anführungszeichen eingeschlossen ist. Optionale Parameter umfassen --delivery-s3uri, um die Abfrageergebnisse an einen angegebenen S3-Bucket zu liefern. Weitere Informationen zur Abfragesprache, die Sie in CloudTrail Lake verwenden können, finden Sie unter [CloudTrail Lake-SQL-Einschränkungen](#).

```
aws cloudtrail start-query
--query-statement 'SELECT eventID, eventTime FROM EXAMPLE-f852-4e8f-8bd1-bcf6cEXAMPLE
LIMIT 10'
--delivery-s3uri "s3://aws-cloudtrail-lake-query-results-123456789012-us-east-1"
```

Die Antwort ist eine QueryId-Zeichenfolge. Um den Status einer Abfrage zu abzurufen, führen Sie describe-query mit dem von start-query zurückgegebenen Wert QueryId aus. Wenn die Abfrage erfolgreich ist, können Sie get-query-results ausführen, um Ergebnisse zu erzielen.

## Ausgabe

```
{
  "QueryId": "EXAMPLE2-0add-4207-8135-2d8a4EXAMPLE"
}
```

### Note

Abfragen, die länger als eine Stunde laufen, können ablaufen. Sie können immer noch Teilergebnisse erhalten, die vor dem Timeout der Abfrage verarbeitet wurden.

Wenn Sie die Abfrageergebnisse mithilfe des optionalen `--delivery-s3uri` Parameters an einen S3-Bucket übermitteln, muss die Bucket-Richtlinie die CloudTrail Erlaubnis erteilen, Abfrageergebnisse an den Bucket zu senden. Informationen zur manuellen Bearbeitung der Bucket-Richtlinie finden Sie im Abschnitt [Amazon S3 S3-Bucket-Richtlinie für CloudTrail Lake-Abfrageergebnisse](#).

## Rufen Sie Metadaten zu einer Abfrage ab mit AWS CLI

Mit dem folgenden AWS CLI `describe-query` Beispielbefehl werden Metadaten zu einer Abfrage abgerufen, einschließlich der Abfragelaufzeit in Millisekunden, der Anzahl der gescannten und abgeglichenen Ereignisse, der Gesamtzahl der gescannten Byte und des Abfragestatus. Der `BytesScanned`-Wert entspricht der Anzahl der Bytes, für die Ihrem Konto die Abfrage in Rechnung gestellt wird, es sei denn, die Abfrage wird noch ausgeführt. Wenn die Abfrageergebnisse an einen S3-Bucket übermitteln wurden, enthält die Antwort auch den S3-URI und den Übermittlungsstatus.

Sie müssen entweder einen Wert für den `--query-id`- oder den `--query-alias`-Parameter angeben. Die Angabe des `--query-alias`-Parameters gibt Informationen über den letzten Abfragelauf für den Alias zurück.

```
aws cloudtrail describe-query --query-id EXAMPLEd-17a7-47c3-a9a1-eccf7EXAMPLE
```

Nachfolgend finden Sie eine Beispielantwort.

```
{
  "QueryId": "EXAMPLE2-0add-4207-8135-2d8a4EXAMPLE",
  "QueryString": "SELECT eventID, eventTime FROM EXAMPLE-f852-4e8f-8bd1-bcf6cEXAMPLE
LIMIT 10",
  "QueryStatus": "RUNNING",
  "QueryStatistics": {
    "EventsMatched": 10,
    "EventsScanned": 1000,
    "BytesScanned": 35059,
    "ExecutionTimeInMillis": 3821,
    "CreationTime": "1598911142"
  }
}
```

## Rufen Sie Abfrageergebnisse ab mit AWS CLI

Der folgende AWS CLI `get-query-results`-Beispielbefehl ruft Ereignisdatenergebnisse einer Abfrage ab. Sie müssen das vom Befehl `start-query` zurückgegebene `--query-id` angeben. Der `BytesScanned`-Wert entspricht der Anzahl der Bytes, für die Ihrem Konto die Abfrage in Rechnung gestellt wird, es sei denn, die Abfrage wird noch ausgeführt. Optionale Parameter umfassen `--max-query-results`, um eine maximale Anzahl von Ergebnissen anzugeben, die der Befehl auf einer einzelnen Seite zurückgeben soll. Wenn es mehr Ergebnisse als den von Ihnen angegebenen `--max-query-results`-Wert gibt, führen Sie den Befehl `NextToken` erneut aus und fügen den zurückgegebenen Wert hinzu, um die nächste Seite mit Ergebnissen zu erhalten.

```
aws cloudtrail get-query-results
--query-id EXAMPLEd-17a7-47c3-a9a1-eccf7EXAMPLE
```

### Ausgabe

```
{
  "QueryStatus": "RUNNING",
  "QueryStatistics": {
    "ResultsCount": 244,
    "TotalResultsCount": 1582,
    "BytesScanned":27044
  },
  "QueryResults": [
    {
      "key": "eventName",
      "value": "StartQuery",
    }
  ],
  "QueryId": "EXAMPLE2-0add-4207-8135-2d8a4EXAMPLE",
  "QueryString": "SELECT eventID, eventTime FROM EXAMPLE-f852-4e8f-8bd1-bcf6cEXAMPLE
LIMIT 10",
  "NextToken": "20add42078135EXAMPLE"
}
```

## Listet alle Abfragen in einem Ereignisdatenspeicher auf mit AWS CLI

Der folgende AWS CLI `list-queries`-Beispielbefehl gibt eine Liste von Abfragen und deren Abfragestatus in einem bestimmten Ereignisdatenspeicher für die letzten sieben Tage zurück. Sie müssen einen ARN oder das ID-Suffix eines ARN-Wertes für `--event-data-store` angeben.

Um die Liste der Ergebnisse zu verkürzen, können Sie optional einen als Zeitstempel formatierten Zeitbereich angeben, indem Sie die Parameter `--start-time` und `--end-time` und einen `--query-status`-Wert hinzufügen. Gültige Werte für `QueryStatus` sind u. a.: `QUEUED`, `RUNNING`, `FINISHED`, `FAILED` oder `CANCELLED`.

`list-queries` hat auch optionale Paginierungsparameter. Verwenden Sie `--max-results`, um eine maximale Anzahl von Ergebnissen anzugeben, die der Befehl auf einer einzelnen Seite zurückgeben soll. Wenn es mehr Ergebnisse als den von Ihnen angegebenen `--max-results`-Wert gibt, führen Sie den Befehl `NextToken` erneut aus und fügen den zurückgegebenen Wert hinzu, um die nächste Seite mit Ergebnissen zu erhalten.

```
aws cloudtrail list-queries
--event-data-store EXAMPLE-f852-4e8f-8bd1-bcf6cEXAMPLE
--query-status CANCELLED
--start-time 1598384589
--end-time 1598384602
--max-results 10
```

## Ausgabe

```
{
  "Queries": [
    {
      "QueryId": "EXAMPLE2-0add-4207-8135-2d8a4EXAMPLE",
      "QueryStatus": "CANCELLED",
      "CreationTime": 1598911142
    },
    {
      "QueryId": "EXAMPLE2-4e89-9230-2127-5dr3aEXAMPLE",
      "QueryStatus": "CANCELLED",
      "CreationTime": 1598296624
    }
  ],
  "NextToken": "20add42078135EXAMPLE"
}
```

## Brechen Sie eine laufende Abfrage ab mit AWS CLI

Der folgende AWS CLI `cancel-query` Beispielbefehl storniert eine Abfrage mit dem Status `RUNNING`. Sie müssen einen Wert für `--query-id` angeben. Wenn Sie `cancel-query` ausführen, wird der

Abfragestatus möglicherweise als CANCELLED angezeigt, auch wenn der cancel-query-Vorgang noch nicht abgeschlossen ist.

#### Note

Für eine abgebrochene Anfrage können Gebühren anfallen. Ihr Konto wird immer noch für die Datenmenge belastet, die gescannt wurde, bevor Sie die Abfrage abgebrochen haben.

Im Folgenden sehen Sie ein CLI-Beispiel:

```
aws cloudtrail cancel-query
--query-id EXAMPLEd-17a7-47c3-a9a1-eccf7EXAMPLE
```

Ausgabe

```
QueryId -> (string)
QueryStatus -> (string)
```

## CloudTrail Lake-SQL-Einschränkungen

CloudTrail Lake-Abfragen sind SQL-Zeichenfolgen. Dieser Abschnitt enthält Informationen zu den unterstützten Funktionen, Operatoren und Schemas.

Nur SELECT-Anweisungen sind zulässig. Keine Abfragezeichenfolgen können Daten ändern.

CloudTrail Lake unterstützt alle gültigen SELECT Presto-SQL-Anweisungen, -Funktionen und -Operatoren. Weitere Informationen zu den unterstützten SQL-Funktionen und -Operatoren finden Sie unter [Funktionen und Operatoren](#) auf der Dokumentationswebsite für Presto.

Die CloudTrail Konsole bietet eine Reihe von Beispielabfragen, die Ihnen den Einstieg in das Schreiben eigener Abfragen erleichtern können. Weitere Informationen finden Sie unter [Sehen Sie sich Beispielabfragen in der CloudTrail Konsole an](#).

Themen

- [Unterstützte Funktionen, Bedingungs- und Verknüpfungsoperatoren](#)
- [Erweiterte Unterstützung für Abfragen in mehreren Tabellen](#)



# Unterstützte Funktionen, Bedingungs- und Verknüpfungsoperatoren

## Unterstützte Funktionen

CloudTrail Lake unterstützt alle Presto-Funktionen. Weitere Informationen zu den unterstützten Funktionen finden Sie unter [Funktionen und Operatoren](#) auf der Dokumentationswebsite für Presto.

CloudTrail Lake unterstützt das INTERVAL Schlüsselwort nicht.

## Unterstützte Bedingungsoperatoren

Folgende Bedingungsoperatoren werden unterstützt:

```
AND
OR
IN
NOT
IS (NOT) NULL
LIKE
BETWEEN
GREATEST
LEAST
IS DISTINCT FROM
IS NOT DISTINCT FROM
<
>
<=
>=
<>
!=
( conditions ) #parenthesised conditions
```

## Unterstützte Verknüpfungsoperatoren

Folgende JOIN-Operationen werden unterstützt: Weitere Informationen zum Ausführen von Abfragen in mehreren Tabellen finden Sie unter [Erweiterte Unterstützung für Abfragen in mehreren Tabellen](#).

```
UNION
UNION ALL
EXCEPT
INTERSECT
```

```
LEFT JOIN
RIGHT JOIN
INNER JOIN
```

## Erweiterte Unterstützung für Abfragen in mehreren Tabellen

CloudTrail Lake unterstützt die erweiterte Abfragesprache für mehrere Ereignisdatenspeicher.

- [UNION|UNION ALL|EXCEPT|INTERSECT](#)
- [LEFT|RIGHT|INNER JOIN](#)

Um eine Abfrage auszuführen, verwenden Sie den Befehl `start-query` in der AWS CLI. Im Folgenden finden Sie ein Beispiel, bei dem eine der Beispielabfragen aus diesem Abschnitt zum Einsatz kommt.

```
aws cloudtrail start-query
--query-statement "Select eventId, eventName from EXAMPLEf852-4e8f-8bd1-bcf6cEXAMPLE
UNION Select eventId, eventName from EXAMPLEg741-6y1x-9p3v-bnh6iEXAMPLE UNION ALL
Select eventId, eventName from EXAMPLEb529-4e8f913d-6m2z-1kp5sEXAMPLE ORDER BY eventId
LIMIT 10;"
```

Die Antwort ist eine `QueryId`-Zeichenfolge. Um den Status einer Abfrage zu abzurufen, führen Sie `describe-query` mit dem von `start-query` zurückgegebenen Wert `QueryId` aus. Wenn die Abfrage erfolgreich ist, können Sie `get-query-results` ausführen, um Ergebnisse zu erzielen.

### **UNION|UNION ALL|EXCEPT|INTERSECT**

Im Folgenden finden Sie eine Beispielabfrage, die `UNION` und `UNION ALL` verwendet, um anhand der Ereignis-ID und des Ereignisnamens in den drei Ereignisdatenspeichern `EDS1`, `EDS2` und `EDS3` nach Ereignissen zu suchen. Die Ergebnisse werden zunächst aus den einzelnen Ereignisdatenspeichern ausgewählt. Anschließend werden die Ergebnisse verkettet, nach Ereignis-ID sortiert und auf zehn Ereignisse begrenzt.

```
Select eventId, eventName from EDS1
UNION
Select eventId, eventName from EDS2
UNION ALL
Select eventId, eventName from EDS3
ORDER BY eventId LIMIT 10;
```

## LEFT|RIGHT|INNER JOIN

Im Folgenden finden Sie eine Beispielabfrage, die mithilfe von LEFT JOIN nach allen Ereignissen aus einem edsB zugeordneten Ereignisdatenspeicher namens eds2 sucht, die denen im primären (linken) Ereignisdatenspeicher edsA entsprechen. Die zurückgegebenen Ereignisse erfolgen am oder vor dem 1. Januar 2020 und es werden nur die Ereignisnamen zurückgegeben.

```
SELECT edsA.eventName, edsB.eventName, element_at(edsA.map, 'test')
FROM eds1 as edsA
LEFT JOIN eds2 as edsB
ON edsA.eventId = edsB.eventId
WHERE edsA.eventtime <= '2020-01-01'
ORDER BY edsB.eventName;
```

## Unterstützte SQL-Schemas für Ereignisdatenspeicher

In den folgenden Abschnitten finden Sie das unterstützte SQL-Schema für jeden Ereignisdatenspeichertyp.

### Themen

- [Unterstütztes Schema für CloudTrail Ereignisdatensatzfelder](#)
- [Unterstütztes Schema für CloudTrail Insights-Ereignisdatensatzfelder](#)
- [Unterstütztes Schema für Datensatzfelder für Konfigurationselemente von AWS Config](#)
- [Unterstütztes Schema für AWS Audit Manager Nachweisdatensatzfelder](#)
- [Unterstütztes Schema für Felder ohne AWS Ereignisse](#)

## Unterstütztes Schema für CloudTrail Ereignisdatensatzfelder

Im Folgenden finden Sie das gültige SQL-Schema für CloudTrail Verwaltungs- und Datenergebnisdatensatzfelder. Weitere Hinweise zu CloudTrail Ereignisdatensatzfeldern finden Sie unter [CloudTrail Inhalt aufzeichnen](#).

```
[
  {
    "Name": "eventversion",
    "Type": "string"
  },
  {
```

```

    "Name": "useridentity",
    "Type":
"struct<type:string,principalid:string,arn:string,accountid:string,accesskeyid:string,
username:string,sessioncontext:struct<attributes:struct<creationdate:timestamp,
mfaauthenticated:string>,sessionissuer:struct<type:string,principalid:string,arn:string,
accountid:string,username:string>,webidfederateddata:struct<federatedprovider:string,
attributes:map<string,string>>,sourceidentity:string,ec2roledelivery:string,
ec2issuedinvpc:string>,invokedby:string,identityprovider:string>"
  },
  {
    "Name": "eventtime",
    "Type": "timestamp"
  },
  {
    "Name": "eventsource",
    "Type": "string"
  },
  {
    "Name": "eventname",
    "Type": "string"
  },
  {
    "Name": "awsregion",
    "Type": "string"
  },
  {
    "Name": "sourceipaddress",
    "Type": "string"
  },
  {
    "Name": "useragent",
    "Type": "string"
  },
  {
    "Name": "errorcode",
    "Type": "string"
  },
  {
    "Name": "errormessage",
    "Type": "string"
  }

```

```
    },
    {
      "Name": "requestparameters",
      "Type": "map<string,string>"
    },
    {
      "Name": "responseelements",
      "Type": "map<string,string>"
    },
    {
      "Name": "additionaleventdata",
      "Type": "map<string,string>"
    },
    {
      "Name": "requestid",
      "Type": "string"
    },
    {
      "Name": "eventid",
      "Type": "string"
    },
    {
      "Name": "readonly",
      "Type": "boolean"
    },
    {
      "Name": "resources",
      "Type":
"array<struct<accountid:string,type:string,arn:string,arnprefix:string>>"
    },
    {
      "Name": "eventtype",
      "Type": "string"
    },
    {
      "Name": "apiversion",
      "Type": "string"
    },
    {
      "Name": "managementevent",
      "Type": "boolean"
    },
    {
      "Name": "recipientaccountid",
```

```

    "Type": "string"
  },
  {
    "Name": "sharedeventid",
    "Type": "string"
  },
  {
    "Name": "annotation",
    "Type": "string"
  },
  {
    "Name": "vpcendpointid",
    "Type": "string"
  },
  {
    "Name": "serviceeventdetails",
    "Type": "map<string,string>"
  },
  {
    "Name": "addendum",
    "Type": "map<string,string>"
  },
  {
    "Name": "edgedevicedetails",
    "Type": "map<string,string>"
  },
  {
    "Name": "insightdetails",
    "Type": "map<string,string>"
  },
  {
    "Name": "eventcategory",
    "Type": "string"
  },
  {
    "Name": "tlsdetails",
    "Type":
"struct<tlsversion:string,ciphersuite:string,clientprovidedhostheader:string>"
  },
  {
    "Name": "sessioncredentialfromconsole",
    "Type": "string"
  },
  {

```

```
    "Name": "eventjson",
    "Type": "string"
  }
  {
    "Name": "eventjsonchecksum",
    "Type": "string"
  }
]
```

## Unterstütztes Schema für CloudTrail Insights-Ereignisdatensatzfelder

Im Folgenden finden Sie das gültige SQL-Schema für Insights-Ereignisdatensatzfelder. Bei Insights-Ereignissen ist der Wert von `eventcategory` `Insight` und der Wert von `eventtype` ist `AwsCloudTrailInsight`.

```
[
  {
    "Name": "eventversion",
    "Type": "string"
  },
  {
    "Name": "eventcategory",
    "Type": "string"
  },
  {
    "Name": "eventtype",
    "Type": "string"
  },
  {
    "Name": "eventid",
    "Type": "string"
  },
  {
    "Name": "eventtime",
    "Type": "timestamp"
  },
  {
    "Name": "awsregion",
    "Type": "string"
  },
  {
    "Name": "recipientaccountid",
    "Type": "string"
  },
]
```

```

{
  "Name": "sharedeventid",
  "Type": "string"
},
{
  "Name": "addendum",
  "Type": "map<string,string>"
},
{
  "Name": "insightsource",
  "Type": "string"
},
{
  "Name": "insightstate",
  "Type": "string"
},
{
  "Name": "insighteventsourcesource",
  "Type": "string"
},
{
  "Name": "insighteventname",
  "Type": "string"
},
{
  "Name": "insighterrorcode",
  "Type": "string"
},
{
  "Name": "insighttype",
  "Type": "string"
},
{
  "Name": "insightContext",
  "Type":
"struct<baselineaverage:double,insightaverage:double,baselineduration:integer,
insightduration:integer,attributions:struct<attribute:string,insightvalue:string,
insightaverage:double,baselinevalue:string,baselineaverage:double>>"
}
]

```



## Unterstütztes Schema für Datensatzfelder für Konfigurationselemente von AWS Config

Im Folgenden finden Sie das gültige SQL-Schema für Datensatzfelder für Konfigurationselemente. Für Konfigurationselemente lautet Wert von eventcategory ConfigurationItem und der Wert von eventtype AwsConfigurationItem.

```
[
  {
    "Name": "eventversion",
    "Type": "string"
  },
  {
    "Name": "eventcategory",
    "Type": "string"
  },
  {
    "Name": "eventtype",
    "Type": "string"
  },
  {
    "Name": "eventid",
    "Type": "string"
  },
  {
    "Name": "eventtime",
    "Type": "timestamp"
  },
  {
    "Name": "awsregion",
    "Type": "string"
  },
  {
    "Name": "recipientaccountid",
    "Type": "string"
  },
  {
    "Name": "addendum",
    "Type": "map<string,string>"
  },
  {
    "Name": "eventdata",
    "Type": "struct<configurationitemversion:string,configurationitemcapturetime:"
```

```

string,configurationitemstatus:string,configurationitemstateid:string,accountid:string,
resourcetype:string,resourceid:string,resourcearn:string,awsregion:string,
availabilityzone:string,resourcecreationtime:string,configuration:map<string,string>,
    supplementaryconfiguration:map<string,string>,relatedevents:string,
relationships:struct<name:string,resourcetype:string,resourceid:string,
    resourcearn:string>,tags:map<string,string>>"
}
]

```

## Unterstütztes Schema für AWS Audit Manager Nachweisdatensatzfelder

Im Folgenden finden Sie das gültige SQL-Schema für Nachweisdatensatzfelder von Audit Manager. Für die Nachweisdatensatzfelder von Audit Manager lautet der Wert von `eventcategory` `Evidence` und der Wert von `eventtype` `AwsAuditManagerEvidence`. Weitere Informationen zur Aggregation von Nachweisen in CloudTrail Lake mithilfe von Audit Manager finden Sie unter [Evidence Finder](#) im AWS Audit Manager Benutzerhandbuch.

```

[
  {
    "Name": "eventversion",
    "Type": "string"
  },
  {
    "Name": "eventcategory",
    "Type": "string"
  },
  {
    "Name": "eventtype",
    "Type": "string"
  },
  {
    "Name": "eventid",
    "Type": "string"
  },
  {
    "Name": "eventtime",
    "Type": "timestamp"
  },
  {

```

```

    "Name": "awsregion",
    "Type": "string"
  },
  {
    "Name": "recipientaccountid",
    "Type": "string"
  },
  {
    "Name": "addendum",
    "Type": "map<string,string>"
  },
  {
    "Name": "eventdata",
    "Type":
"struct<attributes:map<string,string>,awsaccountid:string,awsorganization:string,
compliancecheck:string,datasource:string,eventname:string,eventsourcetype:string,
evidenceawsaccountid:string,evidencebytype:string,iamid:string,evidenceid:string,
time:timestamp,assessmentid:string,controlsetid:string,controlid:string,
controlname:string,controldomainname:string,frameworkname:string,frameworkid:string,
service:string,servicecategory:string,resourcearn:string,resourcetype:string,
evidencefolderid:string,description:string,manualevidences3resourcepath:string,
evidencefoldername:string,resourcecompliancecheck:string>"
  }
]

```

## Unterstütztes Schema für Felder ohne AWS Ereignisse

Das Folgende ist das gültige SQL-Schema für AWS Nicht-Ereignisse. Für AWS Nichtereignisse ist der Wert von eventcategory is ActivityAuditLog und der Wert von eventtype isActivityLog.

```

[
  {
    "Name": "eventversion",
    "Type": "string"
  },
  {

```

```

    "Name": "eventcategory",
    "Type": "string"
  },
  {
    "Name": "eventtype",
    "Type": "string"
  },
  {
    "Name": "eventid",
    "Type": "string"
  },
  {
    "Name": "eventtime",
    "Type": "timestamp"
  },
  {
    "Name": "awsregion",
    "Type": "string"
  },
  {
    "Name": "recipientaccountid",
    "Type": "string"
  },
  {
    "Name": "addendum",
    "Type":
"struct<reason:string,updatedfields:string,originalUID:string,originaleventid:string>"
  },
  {
    "Name": "metadata",
    "Type": "struct<ingestiontime:string,channelarn:string>"
  },
  {
    "Name": "eventdata",
    "Type": "struct<version:string,useridentity:struct<type:string,
principalid:string,details:map<string,string>>,useragent:string,eventsource:string,
eventname:string,eventtime:string,uid:string,requestparameters:map<string,string>>,
responseelements":map<string,string>>,errorcode:string,errormessage:string,sourceipaddress:stri
recipientaccountid:string,additionaleventdata":map<string,string>>"
  }
]

```

# Steuern von Benutzerberechtigungen für CloudTrail Lake

AWS CloudTrail lässt sich in AWS Identity and Access Management (IAM) integrieren, sodass Sie den Zugriff auf CloudTrail Lake und andere benötigte AWS Ressourcen kontrollieren können. CloudTrail Mit IAM können Sie steuern, welche AWS Benutzer CloudTrail Ereignisdatenspeicher oder Kanäle erstellen, konfigurieren oder löschen, die Erfassung von Ereignissen starten und beenden und Trail-Ereignisse kopieren können. Weitere Informationen hierzu finden Sie unter [Identity and Access Management für AWS CloudTrail](#).

In den folgenden Themen finden Sie Informationen zu Berechtigungen, Richtlinien und Sicherheit: CloudTrail

- [Erteilen von Berechtigungen für die CloudTrail Verwaltung](#)
- [Amazon S3 S3-Bucket-Richtlinie für CloudTrail Lake-Abfrageergebnisse](#)
- [Erforderliche Berechtigungen zum Kopieren von Trail-Ereignissen](#)
- [Erforderliche Berechtigungen für den Verbund](#)
- Eine Beispielrichtlinie, die den Zugriff auf einen Ereignisdatenspeicher basierend auf Tags einschränkt: [Beispiele: Verweigern des Zugriffs zum Erstellen oder Löschen von Ereignisdatenspeichern basierend auf Tags](#)
- [AWS CloudTrail Beispiele für ressourcenbasierte Richtlinien](#)
- [Erforderliche Berechtigungen zum Zuweisen delegierter Administratoren](#)
- [Standardmäßige KMS-Schlüsselrichtlinie für CloudTrail Lake-Ereignisdatenspeicher](#)

## Verwaltung der CloudTrail Seekosten

AWS CloudTrail Für Datenspeicher und Abfragen von Ereignissen in Lake fallen Gebühren an. Als bewährte Methode empfehlen wir die Verwendung von AWS-Services Tools, die Ihnen bei der CloudTrail Kostenkontrolle helfen können. Sie können Ereignisdatenspeicher auch so konfigurieren und verwalten, dass die benötigten Daten erfasst werden und gleichzeitig kostengünstig bleiben. Informationen zu CloudTrail -Preisen erhalten Sie unter [AWS CloudTrail Pricing](#) (Preise für WAF).

Themen

- [Preisoptionen für den Ereignisdatenspeicher](#)
- [Die Gebühren von CloudTrail Lake verstehen](#)

- [Empfehlungen, wie Sie Kosten senken können](#)
- [Tools zur Kostenverwaltung](#)
- [Weitere Informationen finden Sie auch unter](#)

## Preisoptionen für den Ereignisdatenspeicher

Beim Erstellen eines Ereignisdatenspeichers wählen Sie die Preisoption aus, die für den Ereignisdatenspeicher genutzt werden soll. Die Preisoption bestimmt die Kosten für die Erfassung und Speicherung von Ereignissen sowie die standardmäßige und maximale Aufbewahrungsdauern für den Ereignisdatenspeicher.

Die folgende Tabelle beschreibt die verfügbaren Preisoptionen. Die Tabelle zeigt die Preisoption in der Konsole und den entsprechenden `BillingMode`-Wert für die API und listet die standardmäßige und maximale Aufbewahrungsdauer für jede Option auf.


Preisoption (Konsole)	BillingMode (API)	Beschreibung
Verlängerbare Aufbewahrung von einem Jahr	EXTENDABLE_RETENTION_PRICING	<p>Empfohlen, wenn Sie damit rechnen, weniger als 25 TB an Ereignisdaten pro Monat zu erfassen und eine flexible Aufbewahrungsdauer von bis zu 10 Jahren wünschen. Diese Option wird auch empfohlen, wenn Ihr Ereignisdatenspeicher Konfigurationselemente von AWS Config, Audit-Manager-Nachweise und Ereignisse außerhalb von AWS erfasst.</p> <p>In den ersten 366 Tagen (Standardaufbewahrungszeitraum) ist Speicherplatz ohne zusätzliche Kosten im Preis für die Datenerfassung enthalten. Nach 366 Tagen ist eine verlängerte Aufbewahrung gegen Aufpreis pay-as-you-go verfügbar.</p> <p>Dies ist die Standardoption.</p> <p>Standardaufbewahrungsdauer: 366 Tage.</p>

Preisoption (Konsole)	BillingMode (API)	Beschreibung
		Maximale Aufbewahrungsdauer: beträgt 3 653 Tage.
Preisgestaltung für die Aufbewahrung von sieben Jahren	FIXED_RETENTION_PRICING	<p>Empfohlen, wenn Sie damit rechnen, mehr als 25 TB an Ereignisdaten pro Monat zu erfassen und eine flexible Aufbewahrungsdauer von bis zu 7 Jahren wünschen.</p> <p>Die Aufbewahrung ist im Preis für die Erfassung ohne Zusatzkosten enthalten.</p> <p>Standardaufbewahrungsdauer: 2 557 Tage.</p> <p>Maximale Aufbewahrungsdauer: beträgt 2 557 Tage.</p>

## Die Gebühren von CloudTrail Lake verstehen

Die folgenden Tabellen enthalten Informationen darüber, wie Gebühren für Datenspeicher und Abfragen von CloudTrail Lake-Ereignissen anfallen. Informationen zu CloudTrail -Preisen erhalten Sie unter [AWS CloudTrail Pricing](#) (Preise für WAF).

Abrechnungsart	Wie fallen für Sie Gebühren an
Datenerfassung (unkomprimierte Daten)	<p>Für CloudTrail Lake zahlen Sie auf der Grundlage der aufgenommenen unkomprimierten Daten. Die <a href="#">Preisoption</a> für den Ereignisdatenspeicher bestimmt die Kosten für die Erfassung von Ereignissen:</p> <ul style="list-style-type: none"> <li>• Preise für verlängerbare Aufbewahrung von einem Jahr: Bietet Preise für die Datenerfassung je nach Ereignistyp.</li> <li>• Preisgestaltung für die Aufbewahrung von sieben Jahren: Bietet Preise für die Datenerfassung, die auf dem erfassten Datenvolumen basieren. Die größten Einsparungen werden</li> </ul>

Abrechnungsart	Wie fallen für Sie Gebühren an
	<p>erzielt, wenn das monatlich erfasste Datenvolumen 25 TB übersteigt.</p> <p>Kopieren von Trail-Ereignissen</p> <p>Wenn Sie <a href="#">Trail-Ereignisse nach CloudTrail Lake kopieren</a>, werden die im komprimierten CloudTrail GZIP-Format gespeicherten Protokolle entpackt. CloudTrail kopiert dann die in den Protokollen enthaltenen Ereignisse in Ihren Ereignisdatenspeicher. Die Größe der unkomprimierten Daten könnte größer sein als die tatsächliche Amazon-S3-Speichergröße. Um eine allgemeine Schätzung der Größe der unkomprimierten Daten zu erhalten, multiplizieren Sie die Größe der Protokolle im S3-Bucket mit 10.</p> <div data-bbox="592 907 1507 1743" style="border: 1px solid #add8e6; border-radius: 15px; padding: 15px;"><p> <b>Note</b></p><p>CloudTrail kopiert ein Ereignis nicht, wenn dessen Ereigniszeit älter als die angegebene Aufbewahrungsfrist ist. Um die geeignete Aufbewahrungsdauer zu ermitteln, nehmen Sie die Summe aus dem ältesten Ereignis, das Sie kopieren möchten, in Tagen und der Anzahl der Tage, an denen Sie die Ereignisse im Ereignisdatenspeicher aufbewahren möchten, wie in der folgenden Gleichung dargestellt:</p><math display="block">\text{Aufbewahrungszeitraum} = \text{oldest-event-in-days} + \text{number-days-to-retain}</math><p>Wenn das älteste Ereignis, das Sie kopieren, beispielsweise 45 Tage alt ist und Sie die Ereignisse weitere 45 Tage im Ereignisdatenspeicher aufbewahren möchten, würden Sie die Aufbewahrungsdauer auf 90 Tage festlegen.</p></div>



Abrechnungsart	Wie fallen für Sie Gebühren an
Datenaufbewahrung (optimierte und komprimierte Daten)	<p>CloudTrail Lake konvertiert bestehende Ereignisse im zeilenbasierten JSON-Format in das <a href="#">Apache ORC-Format</a>. ORC ist ein spaltenförmiges Speicherformat, das für den schnellen Abruf von komprimierten Daten optimiert ist.</p> <p>Die Aufbewahrungsdauer eines Ereignisdatenspeichers bestimmt, wie lange Ereignisdaten im Ereignisdatenspeicher aufbewahrt werden. CloudTrail Lake bestimmt, ob ein Ereignis aufbewahrt werden soll, indem es prüft, ob die Ereigniszeit eines Ereignisses innerhalb der angegebenen Aufbewahrungsfrist liegt. Wenn Sie beispielsweise einen Aufbewahrungszeitraum von 90 Tagen angeben, CloudTrail werden Ereignisse entfernt, deren Veranstaltungszeit älter als 90 Tage ist.</p> <p>Bei Speichern von Ereignisdaten, die die Preisoption für die Aufbewahrung von sieben Jahren verwenden, ist der Speicherplatz ohne zusätzliche Kosten im Erfassungspreis enthalten.</p> <p>Bei Speichern von Ereignisdaten, die die Preisoption Verlängerbare Aufbewahrung für ein Jahr verwenden, ist der Speicherplatz für die ersten 366 Tage (Standardaufbewahrungszeitraum) kostenlos im Preis für die Datenaufnahme enthalten. Nach 366 Tagen wird Speicherplatz zum Preis der optimierten pay-as-you-price und komprimierten Daten im Ereignisdatenspeicher angeboten und entsprechend berechnet.</p>
Abfragen in CloudTrail Lake ausführen (optimierte und komprimierte Daten)	Wenn Sie Abfragen in CloudTrail Lake ausführen, zahlen Sie auf der Grundlage der Menge der gescannten optimierten und komprimierten Daten.

## Empfehlungen, wie Sie Kosten senken können

Dieser Abschnitt enthält Empfehlungen, wie Sie bei der Arbeit mit CloudTrail Lake die Kosten senken können.

Wählen Sie eine Preisoption, die auf der Art der Ereignisse, die Ihr Ereignisdatenspeicher erfasst, und Ihrer voraussichtlichen monatlichen Besucherzahl basiert

Wenn Sie einen Ereignisdatenspeicher erstellen, wählen Sie eine Preisoption auf der Grundlage der Art der Ereignisse, die Ihr Ereignisdatenspeicher erfassen soll, und der erwarteten monatlichen Erfassung.

Wenn Sie voraussichtlich weniger als 25 TB an Ereignisdaten pro Monat erfassen werden und eine flexible Aufbewahrungsdauer von bis zu 10 Jahren wünschen, wählen Sie die Preisoption Verlängerbare Aufbewahrung für ein Jahr. Wir empfehlen diese Option auch generell für Ereignisdatenspeicher, in denen AWS Config Konfigurationselemente, Audit Manager Manager-Nachweise und Ereignisse von außerhalb gesammelt AWS werden.

Wenn Sie voraussichtlich mehr als 25 TB an Ereignisdaten pro Monat erfassen werden und eine Aufbewahrungsdauer von 7 Jahren benötigen, wählen Sie die Preisoption für die Aufbewahrung von sieben Jahren.

Analysieren der monatlichen Datenerfassung Ihres Ereignisdatenspeichers im Laufe der Zeit

Analysieren Sie die historische monatliche Datenerfassung Ihres Ereignisdatenspeichers, um festzustellen, ob es eine Preisoption gibt, die Ihren Bedürfnissen besser entspricht.

Wenn Sie bereits über einen Ereignisdatenspeicher verfügen, der die Preisoption für die Aufbewahrung von sieben Jahren nutzt, und Sie weniger als 25 TB an Daten pro Monat erfassen, sollten Sie in Erwägung ziehen, den Ereignisdatenspeicher zu aktualisieren und die Preisoption für die verlängerbare Aufbewahrung für ein Jahr zu nutzen. Bei Ereignisdatenspeichern, die die Preisoption für die Aufbewahrung von sieben Jahren verwenden, können Sie die Preisoption über die [CloudTrail Konsole](#) oder über die [UpdateEventDataStore](#)API ändern. [AWS CLI](#)

Wenn Sie bereits über einen Ereignisdatenspeicher verfügen, der die Preisoption für die verlängerbare Aufbewahrung für ein Jahr nutzt, und Sie mehr als 25 TB an Daten pro Monat erfassen, sollten Sie in Erwägung ziehen, den Ereignisdatenspeicher zu aktualisieren und die Preisoption für die Aufbewahrung von sieben Jahren zu nutzen. Um die neue Preisoption zu nutzen, [beenden Sie die Erfassung](#) in Ihrem Ereignisdatenspeicher und erstellen Sie einen neuen Ereignisdatenspeicher mit der Preisoption für die Aufbewahrung über sieben Jahre.

Verwenden von erweiterten Ereignisselectoren, um Ereignisse herauszufiltern, die nicht von Interesse sind

Wenn Sie einen Ereignisdatenspeicher für CloudTrail Verwaltungs- oder Datenereignisse konfigurieren, filtern Sie Ereignisse heraus, die nicht von Interesse sind, indem Sie erweiterte Event-Selektoren verwenden.

Wenn Sie einen Ereignisdatenspeicher zur Erfassung von Verwaltungsereignissen erstellen, können Sie Daten-API-Ereignisse AWS Key Management Service (AWS KMS) oder Amazon Relational Database Service (Amazon RDS) herausfiltern. In der Regel GenerateDataKey generieren AWS KMS Aktionen wie EncryptDecrypt, und mehr als 99 Prozent der Ereignisse.

Wenn Sie einen Ereignisdatenspeicher zum Erfassen von Datenereignissen erstellen, können Sie erweiterte Ereignisauswahlfunktionen verwenden, um nach den Feldern `eventName`, `resources.type`, `resources.ARN` und `readOnly` zu filtern. Ein Beispiel finden Sie unter [Beispiel: Erstellen Sie einen Ereignisdatenspeicher für S3-Datenereignisse](#).

Wählen eines engeren Zeitraums beim Kopieren von Trail-Ereignissen

Geben Sie beim Kopieren von Trail-Ereignissen nach CloudTrail Lake eine kürzere Startzeit und eine kürzere Endzeit für das Ereignis an, um die Menge der aufgenommenen Daten zu reduzieren.

Wenn Sie Trail-Ereignisse zur historischen Analyse nach CloudTrail Lake kopieren und keine future Ereignisse aufnehmen möchten, deaktivieren Sie die Option zum Ingestieren von Ereignissen, damit Ihnen keine Gebühren für die Aufnahme zusätzlicher Ereignisse entstehen.

Formatieren von Abfragen, dass sie einen **eventTime** für Start und Ende verwenden

Wenn Sie Abfragen in Lake ausführen, zahlen Sie auf der Grundlage der Menge der gescannten Daten. Sie können die Kosten einschränken, indem Sie einen `eventTime` für Start und Ende für die Abfrage angeben.

## Tools zur Kostenverwaltung

AWS Budgets, eine Funktion von AWS Billing and Cost Management, ermöglicht es Ihnen, benutzerdefinierte Budgets festzulegen, die Sie benachrichtigen, wenn Ihre Kosten oder Nutzung Ihren budgetierten Betrag überschreiten (oder voraussichtlich überschreiten werden).

Wenn Sie Datenspeicher für Veranstaltungen erstellen, empfiehlt es sich, mithilfe CloudTrail von AWS Budgets ein Budget für zu erstellen, das Ihnen dabei helfen kann, Ihre CloudTrail

Ausgaben nachzuverfolgen. Kostenbasierte Budgets tragen dazu bei, das Bewusstsein dafür zu schärfen, wie viel Ihnen für Ihre CloudTrail Nutzung in Rechnung gestellt werden könnte. [Über Budgetbenachrichtigungen](#) werden Sie benachrichtigt, wenn Ihre Rechnung einen von Ihnen definierten Schwellenwert erreicht. Wenn Sie eine Budget-Warnung erhalten, können Sie Änderungen vor dem Ende des Abrechnungszeitraums vornehmen, um Ihre Kosten zu verwalten.

Nachdem Sie [ein Budget erstellt](#) haben, können Sie AWS Cost Explorer damit sehen, wie sich Ihre CloudTrail Kosten auf Ihre AWS Gesamtrechnung auswirken. Im AWS Cost Explorer können Sie nach dem Hinzufügen CloudTrail zum Servicefilter Ihre historischen CloudTrail Ausgaben mit denen Ihrer aktuellen Ausgaben month-to-date (MTD) vergleichen, sowohl nach Region als auch nach Konto. Mit dieser Funktion können Sie unerwartete Kosten in Ihren monatlichen CloudTrail Ausgaben überwachen und erkennen. Zusätzliche Funktionen im Cost Explorer ermöglichen es Ihnen, die CloudTrail Ausgaben mit den monatlichen Ausgaben auf der jeweiligen Ressourcenebene zu vergleichen und so Informationen darüber zu erhalten, was zu Kostenerhöhungen oder -senkungen in Ihrer Rechnung führen könnte.

Um mit AWS Budgets zu beginnen [AWS Billing and Cost Management](#), öffnen Sie das Fenster und wählen Sie dann in der linken Navigationsleiste Budgets aus. Wir empfehlen, bei der Erstellung eines Budgets Budgetwarnungen zu konfigurieren, um die CloudTrail Ausgaben nachzuverfolgen. Weitere Informationen zur Verwendung von AWS Budgets finden Sie unter [Kosten verwalten AWS Budgets](#) und [Bewährte Methoden für AWS Budgets](#).

## Erstellen von benutzerdefinierten Kostenzuweisungs-Tags für CloudTrail Lake-Event-Datenspeicher

Sie können [benutzerdefinierte Kostenzuordnungs-Tags](#) erstellen, um die Abfrage- und Aufnahmekosten für Ihre CloudTrail Lake-Ereignisdatenpeicher nachzuverfolgen. Ein benutzerdefiniertes Kostenzuordnungs-Tag ist ein Schlüssel-Wert-Paar, das Sie mit einem Ereignisdatenpeicher verknüpfen können. Nachdem Sie die Kostenzuordnungs-Tags aktiviert haben, AWS verwendet diese Tags, um Ihre Ressourcenkosten in Ihrem Kostenzuordnungsbericht zu organisieren.

- Informationen zum Erstellen von Tags in der Konsole finden Sie in Schritt 9 des [Um einen Ereignisdatenpeicher für CloudTrail Verwaltungs- oder Datenereignisse zu erstellen](#)-Verfahrens.
- Informationen zum Erstellen von Tags mithilfe der CloudTrail API finden Sie unter [CreateEventDataStore](#) und [AddTags](#) in der AWS CloudTrail API-Referenz.
- [Informationen zum Erstellen von Tags mithilfe der AWS CLI, finden Sie in der AWS CLI Befehlsreferenz unter create-event-data-store und fügen Sie sie hinzu.](#)

Weitere Informationen zum Aktivieren von Tags finden Sie unter [Aktivieren von benutzerdefinierten Kostenzuordnungs-Tags](#).

Weitere Informationen finden Sie auch unter

- [AWS CloudTrail – Preise](#)
- [Unterstützte Metriken CloudWatch](#)
- [Managen Sie Ihre Kosten mit AWS Budgets](#)
- [Erste Schritte mit Cost Explorer](#)

## Unterstützte CloudWatch Metriken

CloudTrail Lake unterstützt CloudWatch Amazon-Metriken. CloudWatch ist ein Dienst zur Überwachung von AWS Ressourcen. Sie können CloudWatch damit Kennzahlen sammeln und verfolgen, Alarme einrichten und automatisch auf Änderungen Ihrer AWS Ressourcen reagieren.

Der AWS/CloudTrail Namespace umfasst die folgenden Metriken für CloudTrail Lake.

Metrik	Beschreibung	Einheiten
HourlyDataIngested	Die Datenmenge, die während der letzten Stunde in den Ereignisdatenspeicher erfasst wurde. Diese Metrik wird stündlich aktualisiert.  Diese Metrik ist für alle Arten von Ereignisdatenspeichern verfügbar.	Bytes
TotalDataRetained	Die Datenmenge, die während des gesamten Aufbewahrungszeitraums im Ereignisdatenspeicher aufbewahrt wird. Diese Metrik wird jede Nacht aktualisiert.	Bytes

Metrik	Beschreibung	Einheiten
	Diese Metrik ist für alle Arten von Ereignisdatenspeichern verfügbar.	
TotalStorageBytes	Die Gesamtzahl der komprimierten Byte im Ereignisdatenspeicher am aktuellen Tag.  Diese Metrik ist für alle Arten von Ereignisdatenspeichern verfügbar.	Bytes

Metrik	Beschreibung	Einheiten
TotalPaidStorageBytes	<p>Bei Ereignisdatenspeichern, die die <a href="#">Preisoption</a> mit erweiterbarer Aufbewahrung für ein Jahr verwenden, entspricht dies der gesamten komprimierten Bytemenge nach 366 Tagen bis zur maximalen Aufbewahrungsdauer, die für den Ereignisdatenspeicher konfiguriert wurde.</p> <p>Bei Ereignisdatenspeichern, die die Preisoption für eine einjährige verlängerbare Aufbewahrung nutzen, ist der Speicherplatz für die ersten 366 Tage, die Standardaufbewahrungsdauer für den Ereignisdatenspeicher, ohne zusätzliche Kosten im Erfassungspreis enthalten. Nach 366 Tagen ist pay-as-you-go der Speicher. Informationen zu Preisen erhalten Sie unter <a href="#">AWS CloudTrail -Preise</a>.</p> <p>Diese Metrik ist nur für Ereignisdatenspeicher verfügbar, die die Preisoption mit verlängerbarer Aufbewahrung für ein Jahr verwenden.</p>	Bytes

Metrik	Beschreibung	Einheiten
HourlyEventsAnalyzed	<p>Die Gesamtzahl der von CloudTrail Insights analysierten Ereignisse im Ereignisdatenspeicher. Diese Metrik wird stündlich aktualisiert.</p> <p>Diese Metrik gilt für CloudTrail Ereignisdatenspeicher, die CloudTrail Insights aktivieren.</p>	Anzahl

Weitere Informationen zu CloudWatch Metriken finden Sie in den folgenden Themen.

- [Verwenden von CloudWatch Amazon-Metriken](#)
- [CloudWatch Amazon-Alarme verwenden](#)



# Mit CloudTrail Trails arbeiten

Trails zeichnet AWS Aktivitäten auf, übermittelt und speichert diese Ereignisse in einem Amazon S3 S3-Bucket, mit optionaler Übermittlung an [CloudWatch Logs](#) und [Amazon EventBridge](#).

Sie können eine Kopie Ihrer laufenden Verwaltungsereignisse kostenlos an Ihren S3-Bucket senden, CloudTrail indem Sie einen Trail erstellen. Es fallen jedoch Amazon S3 S3-Speichergebühren an. Weitere Informationen zur CloudTrail Preisgestaltung finden Sie unter [AWS CloudTrail Preise](#). Informationen zu Amazon-S3-Preisen finden Sie unter [Amazon S3-Preise](#).

Sie können zwei Arten von Wanderwegen für einen erstellen AWS-Konto: Wanderwege mit mehreren Regionen und Wanderwege mit nur einer Region.

## Wanderwege mit mehreren Regionen

Wenn Sie einen Trail mit mehreren Regionen erstellen, CloudTrail zeichnet er alle Ereignisse AWS-Regionen in der [AWS Partition](#) auf, in der Sie arbeiten, und übermittelt die CloudTrail Ereignisprotokolldateien an einen von Ihnen angegebenen S3-Bucket. Wenn ein Trail hinzugefügt AWS-Region wird, nachdem Sie einen Trail mit mehreren Regionen erstellt haben, wird diese neue Region automatisch hinzugefügt, und Ereignisse in dieser Region werden protokolliert. Das Erstellen eines Trails mit mehreren Regionen wird als bewährte Methode empfohlen, da Sie Aktivitäten in allen Regionen in Ihrem Konto erfassen. Alle Trails, die Sie mit der CloudTrail Konsole erstellen, sind regionsübergreifend. Sie können einen Pfad mit einer einzelnen Region in einen Pfad mit mehreren Regionen konvertieren, indem Sie den verwenden. [AWS CLI](#) Weitere Informationen finden Sie unter [Erstellen eines Trails in der Konsole](#) und [Umwandeln eines Trails, der für eine Region gilt, zu einem Trail für alle Regionen](#).

## Wanderwege für eine einzelne Region

Wenn Sie einen Pfad mit nur einer Region erstellen, werden nur die Ereignisse in dieser Region CloudTrail aufgezeichnet. Anschließend werden die CloudTrail Ereignisprotokolldateien an einen von Ihnen angegebenen Amazon S3 S3-Bucket gesendet. Sie können nur einen einzelnen Regions-Trail erstellen, indem Sie die AWS CLI verwenden. Wenn Sie zusätzliche einzelne Trails erstellen, können Sie festlegen, dass diese Trails CloudTrail Ereignisprotokolldateien an denselben S3-Bucket oder an separate Buckets liefern. Dies ist die Standardoption, wenn Sie einen Trail mithilfe der AWS CLI oder der CloudTrail API erstellen. Weitere Informationen finden Sie unter [Trails erstellen, aktualisieren und verwalten mit dem AWS CLI](#).

**Note**

Für beide Arten von Trails können Sie einen Amazon-S3-Bucket aus einer beliebigen Region angeben.

Wenn Sie in eine Organisation erstellt haben AWS Organizations, können Sie einen Organisationspfad erstellen, der alle Ereignisse für alle AWS Konten in dieser Organisation protokolliert. Organisationspfade können für alle AWS Regionen oder für die aktuelle Region gelten. Organisations-Trails müssen im Verwaltungskonto oder mit dem Konto eines delegierten Administrators erstellt werden. Sobald sie auf eine Organisation angewendet werden, gelten sie automatisch auch für alle Mitgliedskonten in der Organisation. Mitgliedskonten können den Organisationspfad sehen, ihn aber nicht ändern oder löschen. Standardmäßig wird Mitgliedskonten kein Zugriff auf die Protokolldateien für den Organisations-Trail im Amazon-S3-Bucket gewährt. Weitere Informationen finden Sie unter [Erstellen eines Trails für eine Organisation](#).

**Themen**

- [Erstellen Sie einen Trail für Ihren AWS-Konto](#)
- [Erstellen eines Trails für eine Organisation](#)
- [CloudTrail Insights-Ereignisse für Wanderwege anzeigen](#)
- [Trailereignisse nach CloudTrail Lake kopieren](#)
- [CloudTrail Logdateien abrufen und einsehen](#)
- [Konfiguration von Amazon SNS SNS-Benachrichtigungen für CloudTrail](#)
- [Tipps zum Verwalten von Trails](#)
- [Benutzerberechtigungen für CloudTrail Trails kontrollieren](#)
- [Verwendung AWS CloudTrail mit VPC-Endpunkten mit Schnittstelle](#)
- [AWS-Konto Sperrung und Wege](#)

## Erstellen Sie einen Trail für Ihren AWS-Konto

Wenn Sie einen Trail erstellen, ermöglichen Sie die fortlaufende Übermittlung von Ereignissen als Protokolldateien an den von Ihnen angegebenen Amazon-S3-Bucket. Das Erstellen eines Trails bietet zahlreiche Vorteile. Einige davon sind:

- Ein Datensatz zu Ereignissen, der sich über mehr als 90 Tagen erstreckt

- Die Option, bestimmte Ereignisse automatisch zu überwachen und bei bestimmten Ereignissen Alarm zu schlagen, indem Protokollereignisse an Amazon CloudWatch Logs gesendet werden.
- Die Option, Protokolle abzufragen und AWS Serviceaktivitäten mit Amazon Athena zu analysieren.

Ab dem 12. April 2019 können Sie sich Trails nur noch in den AWS Regionen ansehen, in denen Ereignisse protokolliert werden. Wenn Sie einen Trail erstellen, der Ereignisse in allen AWS Regionen protokolliert, wird er in der Konsole in allen Regionen der AWS Partition, in der Sie arbeiten, angezeigt. Wenn Sie einen Trail erstellen, der nur Ereignisse in einer einzelnen -Region protokolliert, können Sie ihn nur in dieser -Region anzeigen und verwalten. Das Erstellen eines Trails mit mehreren Regionen ist die Standardoption, wenn Sie einen Trail mithilfe der AWS CloudTrail Konsole erstellen. Dies ist eine empfohlene bewährte Methode. Wenn Sie einen Trail für eine einzelne Region erstellen möchten, müssen Sie die AWS CLI verwenden.

Wenn Sie dies verwenden AWS Organizations, können Sie einen Trail erstellen, der Ereignisse für alle AWS Konten in der Organisation protokolliert. In jedem Mitgliedskonto wird ein Trail mit dem gleichen Namen erstellt und Ereignisse aus jedem Trail werden an den von Ihnen angegebenen Amazon-S3-Bucket übermittelt.

#### Note

Das Erstellen eines Organisations-Trails ist nur über das Verwaltungskonto oder das Konto eines delegierten Administrators der Organisation möglich. Das Erstellen eines Pfads für eine Organisation ermöglicht automatisch die Integration zwischen CloudTrail und Organizations. Weitere Informationen finden Sie unter [Erstellen eines Trails für eine Organisation](#).

## Themen

- [Erstellen und Aktualisieren eines Trails mit der Konsole](#)
- [Trails erstellen, aktualisieren und verwalten mit dem AWS CLI](#)

## Erstellen und Aktualisieren eines Trails mit der Konsole

Du kannst die CloudTrail Konsole verwenden, um deine Trails zu erstellen, zu aktualisieren oder zu löschen. Trails, die mit der Konsole erstellt wurden, sind multiregional. Um einen Trail zu erstellen, der Ereignisse nur in einem protokolliert AWS-Region, [verwenden Sie den AWS CLI](#).

Sie können bis zu fünf Trails für jede Region erstellen. Nachdem Sie einen Trail erstellt haben, beginnt er CloudTrail automatisch mit der Protokollierung von API-Aufrufen und verwandten Ereignissen in Ihrem Konto in dem von Ihnen angegebenen Amazon S3 S3-Bucket. Wenn Sie die Protokollierung stoppen möchten, können Sie die Protokollierung für den Trail deaktivieren oder diesen löschen.

Die Verwendung der CloudTrail Konsole zum Erstellen oder Aktualisieren eines Trails bietet die folgenden Vorteile.

- Wenn Sie zum ersten Mal einen Trail erstellen, können Sie sich mithilfe der CloudTrail Konsole die verfügbaren Funktionen und Optionen ansehen.
- Wenn Sie einen Trail zur Protokollierung von Datenereignissen konfigurieren, können Sie mithilfe der CloudTrail Konsole die verfügbaren Datentypen anzeigen. Weitere Informationen zum Protokollieren von Datenereignissen finden Sie unter [Protokollieren von Datenereignissen](#).

Spezifische Informationen zur Erstellung eines Trails für eine Organisation in AWS Organizations finden Sie unter [Erstellen eines Trails für eine Organisation](#).

## Themen

- [Erstellen eines Trails](#)
- [Aktualisieren eines Trails](#)
- [Löschen eines Trails](#)
- [Deaktivieren der Protokollierung für einen Trail](#)

## Erstellen eines Trails

Als bewährte Methode sollten Sie einen Trail erstellen, der für alle AWS-Regionen gilt. Dies ist die Standardeinstellung, wenn Sie einen Trail in der CloudTrail Konsole erstellen. Wenn ein Trail für alle Regionen gilt, CloudTrail werden Protokolldateien aus allen Regionen der [AWS Partition](#), in der Sie arbeiten, an einen von Ihnen angegebenen S3-Bucket übermittelt. Nachdem Sie den Trail erstellt haben, beginnt AWS CloudTrail automatisch die Protokollierung der von Ihnen angegebenen Ereignisse.

### Note

Nachdem Sie einen Trail erstellt haben, können Sie andere so konfigurieren, AWS-Services dass sie die in den CloudTrail Protokollen gesammelten Ereignisdaten weiter analysieren

und darauf reagieren. Weitere Informationen finden Sie unter [AWS Serviceintegrationen mit Protokollen CloudTrail](#).

## Themen

- [Erstellen eines Trails in der Konsole](#)
- [Nächste Schritte](#)

## Erstellen eines Trails in der Konsole

Gehen Sie wie folgt vor, um einen Trail zu erstellen, der alle Ereignisse AWS-Regionen in der AWS Partition protokolliert, in der Sie arbeiten. Dies ist eine empfohlene bewährte Methode. Um Ereignisse in einer einzelnen Region zu protokollieren (nicht empfohlen), [verwenden Sie AWS CLI](#).

Um einen CloudTrail Trail mit dem zu erstellen AWS Management Console

1. Melden Sie sich bei der an AWS Management Console und öffnen Sie die CloudTrail Konsole unter <https://console.aws.amazon.com/cloudtrail/>.
2. Wählen Sie auf der CloudTrail Service-Startseite, der Trails-Seite oder im Abschnitt Trails der Dashboard-Seite die Option Trail erstellen aus.
3. Geben Sie auf der Seite Create Trail in Trail name einen Namen für den Trail ein. Weitere Informationen finden Sie unter [Benennungsanforderungen](#).
4. Wenn es sich um einen AWS Organizations Organisations-Trail handelt, können Sie den Trail für alle Konten in Ihrer Organisation aktivieren. Diese Option wird nur angezeigt, wenn Sie sich mit einem Benutzer oder einer Rolle im Verwaltungskonto oder im Konto eines delegierten Administrators bei der Konsole anmelden. Zur Erstellung eines Organisations-Trails müssen dem Benutzer oder der Rolle [ausreichende Berechtigungen](#) zugewiesen sein. Weitere Informationen finden Sie unter [Erstellen eines Trails für eine Organisation](#).
5. Wählen Sie in Speicherort für Neuen S3 Bucket erstellen, um einen neuen Bucket zu erstellen. Wenn Sie einen Bucket erstellen, werden die erforderlichen Bucket-Richtlinien CloudTrail erstellt und angewendet. Wenn Sie sich dafür entscheiden, einen neuen S3-Bucket zu erstellen, muss Ihre IAM-Richtlinie die Genehmigung für die `s3:PutEncryptionConfiguration` Aktion enthalten, da die serverseitige Verschlüsselung standardmäßig für den Bucket aktiviert ist.

**Note**

Wenn Sie die Option Vorhandenen S3-Bucket verwenden ausgewählt haben, geben Sie in Name des Trail-Protokoll-Buckets einen Bucket an oder wählen Sie Durchsuchen aus, um einen Bucket in Ihrem Konto auszuwählen. Wenn Sie einen Bucket aus einem anderen Konto verwenden möchten, müssen Sie den Bucket-Namen angeben. Die Bucket-Richtlinie muss die CloudTrail Schreibberechtigung für den Bucket gewähren. Informationen zur manuellen Bearbeitung der Bucket-Richtlinie finden Sie im Abschnitt [Amazon S3 S3-Bucket-Richtlinie für CloudTrail](#).

Um das Auffinden Ihrer Logs zu erleichtern, erstellen Sie in einem vorhandenen Bucket einen neuen Ordner (auch als Präfix bezeichnet), um Ihre CloudTrail Logs zu speichern. Geben Sie das Präfix in Präfix ein.

- Wählen Sie unter Log file SSE-KMS encryption (SSE-KMS-Verschlüsselung der Protokolldatei) die Option Enabled (Aktiviert) aus, wenn Sie Ihre Protokolldateien mit der SSE-KMS-Verschlüsselung anstelle der SSE-S3-Verschlüsselung verschlüsseln möchten. Der Standard ist aktiviert. Wenn Sie die SSE-KMS-Verschlüsselung nicht aktivieren, werden die Protokolle mit der SSE-S3-Verschlüsselung verschlüsselt. Weitere Informationen zur SSE-KMS-Verschlüsselung finden Sie unter [Verwenden der serverseitigen Verschlüsselung mit AWS Key Management Service \(SSE-KMS\)](#). Weitere Informationen zur SSE-S3-Verschlüsselung finden Sie unter [Verwenden der serverseitigen Verschlüsselung mit von Amazon S3 verwalteten Verschlüsselungsschlüsseln \(SSE-S3\)](#).

Wenn Sie die SSE-KMS-Verschlüsselung aktivieren, wählen Sie Neu oder Bestehend aus. AWS KMS key Geben Sie AWS KMS unter Alias einen Alias im Format an. `alias/MyAliasName` Weitere Informationen finden Sie unter [Aktualisieren einer Ressource zur Verwendung des KMS-Schlüssels](#). CloudTrail unterstützt auch Schlüssel AWS KMS für mehrere Regionen. Weitere Informationen finden Sie über Multi-Regions-Schlüssel finden Sie unter [Verwenden von Schlüsseln für mehrere Regionen](#) im AWS Key Management Service -Entwicklerhandbuch.

**Note**

Sie können auch den ARN eines Schlüssels aus einem anderen Konto eingeben. Weitere Informationen finden Sie unter [Aktualisieren einer Ressource zur Verwendung des KMS-Schlüssels](#). Die Schlüsselrichtlinie muss die Verwendung des Schlüssels zum

Verschlüsseln Ihrer Protokolldateien ermöglichen und den von Ihnen angegebenen Benutzern das Lesen von Protokolldateien in unverschlüsselter Form ermöglichen. CloudTrail Informationen zur manuellen Bearbeitung der Schlüsselrichtlinie finden Sie unter [Konfigurieren Sie AWS KMS wichtige Richtlinien für CloudTrail](#).


7. Konfigurieren Sie unter Zusätzliche Einstellungen Folgendes.
  - a. Wählen Sie für Protokolldateivalidierung Aktiviert, damit Ihrem S3 Bucket Protokoll-Digests übermittelt werden. Sie können die Digest-Dateien verwenden, um zu überprüfen, ob sich Ihre Protokolldateien nach CloudTrail der Übermittlung nicht geändert haben. Weitere Informationen finden Sie unter [Überprüfen der Integrität der CloudTrail Protokolldatei](#).
  - b. Wählen Sie für die Zustellung von SNS-Benachrichtigungen die Option Aktiviert aus, um jedes Mal benachrichtigt zu werden, wenn ein Protokoll an Ihren Bucket gesendet wird. CloudTrail speichert mehrere Ereignisse in einer Protokolldatei. SNS-Benachrichtigungen werden für jede Protokolldatei, nicht für jedes Ereignis gesendet. Weitere Informationen finden Sie unter [Konfiguration von Amazon SNS SNS-Benachrichtigungen für CloudTrail](#).

Wenn Sie SNS-Benachrichtigungen aktivieren, wählen Sie für Neues SNS-Thema erstellen die Option Neu aus, um ein Thema zu erstellen, oder wählen Sie Vorhanden aus, um ein vorhandenes Thema zu verwenden. Wenn Sie einen Trail erstellen, der für alle Regionen gilt, werden SNS-Benachrichtigungen für Protokolldateizustellungen aus allen Regionen an das von Ihnen erstellte einzelne SNS-Thema gesendet.

Wenn Sie Neu wählen, CloudTrail gibt Sie einen Namen für das neue Thema an, oder Sie können einen Namen eingeben. Wenn Sie Vorhanden wählen, wählen Sie ein SNS-Thema aus der Dropdown-Liste aus. Sie können auch den ARN eines Themas aus einer anderen Region oder aus einem Konto mit den entsprechenden Berechtigungen eingeben. Weitere Informationen finden Sie unter [Amazon SNS SNS-Themenrichtlinie für CloudTrail](#).

Wenn Sie ein Thema erstellen, müssen Sie das Thema abonnieren, um über die Zustellung von Protokolldateien benachrichtigt zu werden. Sie können das Abonnement von der Amazon-SNS-Konsole aus vornehmen. Aufgrund der Häufigkeit der Benachrichtigungen empfehlen wir, das Abonnement so zu konfigurieren, dass eine Amazon-SQS-Warteschlange zur programmgesteuerten Bearbeitung der Benachrichtigungen verwendet wird. Weitere Informationen finden Sie unter [Erste Schritte mit Amazon SNS](#) im Benutzerhandbuch für Amazon Simple Notification Service.

8. Optional können Sie konfigurieren, CloudTrail dass Protokolldateien an CloudWatch Protokolle gesendet werden, indem Sie in CloudWatch Protokollen die Option Aktiviert auswählen. Weitere Informationen finden Sie unter [Ereignisse an CloudWatch Logs senden](#).
  - a. Wenn Sie die Integration mit CloudWatch Logs aktivieren, wählen Sie Neu, um eine neue Protokollgruppe zu erstellen, oder Existiert, um eine bestehende zu verwenden. Wenn Sie „Neu“ wählen CloudTrail , geben Sie einen Namen für die neue Protokollgruppe an, oder Sie können einen Namen eingeben.
  - b. Wenn Sie Vorhanden wählen, wählen Sie eine Protokollgruppe aus der Dropdown-Liste aus.
  - c. Wählen Sie Neu, um eine neue IAM-Rolle für Berechtigungen zum Senden von Protokollen an Logs zu CloudWatch erstellen. Wählen Sie Vorhanden, um eine vorhandene IAM-Rolle aus der Dropdown-Liste auszuwählen. Die Richtlinienanweisung für die neue oder vorhandene Rolle wird angezeigt, wenn Sie das Richtliniendokument erweitern. Weitere Informationen über diese Rolle finden Sie unter [Rollenrichtlinien-Dokument CloudTrail zur Verwendung von CloudWatch Logs zur Überwachung](#).

 Note

- Beim Konfigurieren eines Trails können Sie einen S3 Bucket und ein SNS-Thema auswählen, die zu einem anderen Konto gehören. Wenn Sie jedoch Ereignisse CloudTrail an eine CloudWatch Logs-Protokollgruppe übermitteln möchten, müssen Sie eine Protokollgruppe auswählen, die in Ihrem aktuellen Konto vorhanden ist.
- Nur das Verwaltungskonto kann mithilfe der Konsole eine CloudWatch Logs-Protokollgruppe für einen Organisations-Trail konfigurieren. Der delegierte Administrator kann eine CloudWatch Logs-Protokollgruppe mithilfe der UpdateTrail API-Operationen AWS CLI oder CloudTrail CreateTrail oder konfigurieren.

9. Fügen Sie für Tags ein oder mehrere benutzerdefinierte Tags (Schlüssel-Wert-Paare) zu Ihrem Trail hinzu. Mithilfe von Tags können Sie sowohl Ihre CloudTrail Trails als auch die Amazon S3 S3-Buckets identifizieren, die CloudTrail Protokolldateien enthalten. Anschließend können Sie Ressourcengruppen für Ihre CloudTrail Ressourcen verwenden. Weitere Informationen finden Sie unter [AWS Resource Groups](#) und [Tags](#).




10. Wählen Sie auf der Seite Protokollereignisse auswählen die Ereignistypen aus, die Sie protokollieren möchten. Führen Sie unter Management events (Verwaltungsereignisse) die folgenden Schritte aus.
  - a. Wählen Sie für API-Aktivität aus, ob Ihr Trail Leseereignisse, Schreibereignisse oder beides protokollieren soll. Weitere Informationen finden Sie unter [Verwaltungsereignisse](#).
  - b. Wählen Sie AWS KMS Ereignisse ausschließen, um Ereignisse aus Ihrem Trail herauszufiltern AWS Key Management Service (AWS KMS). Die Standardeinstellung ist, alle AWS KMS Ereignisse einzubeziehen.

Die Option, AWS KMS Ereignisse zu protokollieren oder auszuschließen, ist nur verfügbar, wenn Sie Verwaltungsereignisse protokollieren. Wenn Sie sich dafür entscheiden, Verwaltungsereignisse nicht zu protokollieren, werden AWS KMS Ereignisse nicht protokolliert, und Sie können die Einstellungen für die AWS KMS Ereignisprotokollierung nicht ändern.


AWS KMS Aktionen wie `EncryptDecrypt`, und erzeugen `GenerateDataKey` in der Regel ein großes Volumen (mehr als 99%) von Ereignissen. Diese Aktionen werden nun als Leseereignisse protokolliert. Relevante AWS KMS Aktionen mit geringem Volumen wie `DisableDelete`, und `ScheduleKey` (die in der Regel weniger als 0,5% des AWS KMS Ereignisvolumens ausmachen) werden als Write-Ereignisse protokolliert.

Wenn Sie Ereignisse mit hohem Volumen wie **Encrypt**, und ausschließen möchten **DecryptGenerateDataKey**, aber dennoch relevante Ereignisse wie, **Delete** und protokollieren möchten **DisableScheduleKey**, wählen Sie die Option Schreibverwaltungsereignisse protokollieren und deaktivieren Sie das Kontrollkästchen für Ereignisse ausschließen. AWS KMS

- c. Klicken Sie auf Amazon-RDS-Daten-API ausschließen zum Filtern von Ereignissen der Amazon-Relational-Database-Service-Daten-API aus Ihrem Trail. Die Standardeinstellung besteht darin, alle Amazon-RDS-Daten-API-Ereignisse einzubeziehen. Weitere Informationen über die Amazon-RDS-Daten-API finden Sie unter [Protokollieren von Daten-API-Aufrufen mit AWS CloudTrail](#) im Amazon-RDS-Benutzerhandbuch für Aurora.
11. Zum Protokollieren von Datenereignissen wählen Sie Datenereignisse aus. Für die Protokollierung von Datenereignissen fallen zusätzliche Gebühren an. Weitere Informationen finden Sie unter [AWS CloudTrail -Preisgestaltung](#).


12.  **Important**
- Die Schritte 12 bis 16 betreffen die Konfiguration von Datenereignissen mithilfe erweiterter Ereignisauswahlen, was die Standardeinstellung ist. Mithilfe erweiterter Ereignisauswahlen können Sie mehr [Datenereignistypen](#) konfigurieren und genau steuern, welche Datenereignisse in Ihrem Trail erfasst werden. Wenn Sie sich für die Verwendung grundlegender Ereignisauswahlen entschieden haben, führen Sie die Schritte unter [Konfigurieren von Datenereigniseinstellungen mithilfe grundlegender Ereignisauswahlen](#) aus und fahren Sie anschließend mit Schritt 17 dieses Verfahrens fort.

Wählen Sie für Datenereignistyp den Ressourcentyp aus, für den Sie Datenereignisse protokollieren möchten. Weitere Informationen zu den verfügbaren Datenereignistypen finden Sie unter [Datenereignisse](#).

 **Note**

Um Datenereignisse für von Lake Formation erstellte AWS Glue Tabellen zu protokollieren, wählen Sie Lake Formation.

13. Wählen Sie eine Protokollauswahlvorlage aus. CloudTrail enthält vordefinierte Vorlagen, die alle Datenereignisse für den Ressourcentyp protokollieren. Um eine benutzerdefinierte Protokoll-Selektorvorlage zu erstellen, wählen Sie Benutzerdefiniert aus.

 **Note**

Wenn Sie eine vordefinierte Vorlage für S3-Buckets auswählen, wird die Protokollierung von Datenereignissen für alle Buckets aktiviert, die sich derzeit in Ihrem AWS Konto befinden, sowie für alle Buckets, die Sie nach Abschluss der Erstellung des Trails erstellen. Es ermöglicht auch die Protokollierung von Datenereignisaktivitäten, die von einer beliebigen IAM-Identität in Ihrem AWS Konto ausgeführt werden, selbst wenn diese Aktivität in einem Bucket ausgeführt wird, der zu einem anderen Konto gehört. AWS Wenn der Trail nur für eine Region gilt, aktiviert die Auswahl einer vordefinierten Vorlage, die alle S3 Buckets protokolliert, die Datenereignisprotokollierung für alle Buckets in derselben Region wie Ihr Trail und alle Buckets, die Sie später in dieser Region erstellen.

Es werden keine Datenereignisse für Amazon S3 S3-Buckets in anderen Regionen in Ihrem AWS Konto protokolliert.


Wenn Sie einen Trail für alle Regionen erstellen, aktiviert die Auswahl einer vordefinierten Vorlage für Lambda-Funktionen die Datenereignisprotokollierung für alle Funktionen, die sich derzeit in Ihrem AWS Konto befinden, sowie für alle Lambda-Funktionen, die Sie möglicherweise in einer beliebigen Region erstellen, nachdem Sie den Trail erstellt haben. Wenn Sie einen Trail für eine einzelne Region erstellen (mithilfe von AWS CLI), aktiviert diese Auswahl die Datenereignisprotokollierung für alle Funktionen, die sich derzeit in dieser Region in Ihrem AWS Konto befinden, sowie für alle Lambda-Funktionen, die Sie möglicherweise in dieser Region erstellen, nachdem Sie den Trail erstellt haben. Es wird keine Datenereignisprotokollierung für Lambda-Funktionen aktiviert, die in anderen Regionen erstellt wurden.

Das Protokollieren von Datenereignissen für alle Funktionen ermöglicht auch die Protokollierung von Datenereignisaktivitäten, die von einer beliebigen IAM-Identität in Ihrem AWS Konto ausgeführt werden, selbst wenn diese Aktivität für eine Funktion ausgeführt wird, die zu einem anderen AWS Konto gehört.

14. (Optional) Geben Sie unter Selektornamen einen Namen ein, um Ihre Auswahl zu identifizieren. Der Selektornamen ist ein optionaler, beschreibender Name für eine erweiterte Ereignisauswahl, z. B. „Datenereignisse nur für zwei S3-Buckets protokollieren“. Der Name des Selektors wird als Name in der erweiterten Ereignisauswahl aufgeführt und ist sichtbar, wenn Sie die JSON-Ansicht erweitern.
15. Erstellen Sie in den erweiterten Ereignisselektoren einen Ausdruck für die spezifischen Ressourcen, für die Sie Datenereignisse protokollieren möchten. Sie können diesen Schritt überspringen, wenn Sie eine vordefinierte Protokollvorlage verwenden.
  - a. Wählen Sie aus den folgenden Feldern.
    - **readOnly**- readOnly kann auf den Wert `true` oder `false` gesetzt werden. Schreibgeschützte Datenereignisse sind Ereignisse, die den Zustand einer Ressource nicht ändern, z. B. `Get*`- oder `Describe*`-Ereignisse. Schreibereignisse fügen Ressourcen, Attribute oder Artefakte hinzu, ändern oder löschen sie, wie z. B. `Put*`-, `Delete*`- oder `Write*`-Ereignisse. Um sowohl `read`- als auch `write`-Ereignisse zu protokollieren, fügen Sie keinen `readOnly`-Selektor hinzu.
    - **eventName** – eventName kann einen beliebigen Operator verwenden. Sie können damit jedes Datenereignis, für das protokolliert wurde, ein- oder ausschließen CloudTrail, z. B. `PutBucketPutItem`, oder `GetSnapshotBlock`.

- **resources.ARN**- Sie können jeden Operator mit verwenden `resources.ARN`, aber wenn Sie `equals` oder `ungleich` verwenden, muss der Wert genau dem ARN einer gültigen Ressource des Typs entsprechen, den Sie in der Vorlage als Wert von `resources.type` angegeben haben.

In der folgenden Tabelle wird das gültige ARN-Format für alle `resources.type`-Werte aufgeführt.

 Note

Sie können das `resources.ARN` Feld nicht verwenden, um Ressourcentypen zu filtern, die keine ARNs haben.

resources.type	resources.ARN
AWS::DynamoDB::Table <sup>1</sup>	arn: <i>partition</i> :dynamodb : <i>region</i> : <i>account_ID</i> :table/ <i>table_name</i>
AWS::Lambda::Function	arn: <i>partition</i> :lambda: <i>region</i> : <i>account_ID</i> : <i>function</i> : <i>function_name</i>
AWS::S3::Object <sup>2</sup>	arn: <i>partition</i> :s3:: <i>bucket_name</i> / arn: <i>partition</i> :s3:: <i>bucket_name</i> / <i>object_or_file_name</i> /
AWS::AppConfig::Configuration	arn: <i>partition</i> :appconfi g: <i>region</i> : <i>account_ID</i> :applicat ion/ <i>application_ID</i> /environm ent/ <i>environment_ID</i> /configur ation/ <i>configuration_profile_ID</i>
AWS::B2BI::Transformer	arn: <i>partition</i> :b2bi: <i>region</i> : <i>account_ID</i> : <i>transformer</i> / <i>transformer_ID</i>

resources.type	resources.ARN
AWS::Bedrock::AgentAlias	<pre>arn:<i>partition</i> :bedrock:   <i>region</i>:<i>account_ID</i> :agent-alias/   <i>agent_ID</i>/<i>alias_ID</i></pre>
AWS::Bedrock::KnowledgeBase	<pre>arn:<i>partition</i> :bedrock:   <i>region</i>:<i>account_ID</i> :knowledge-base/   <i>knowledge_base_ID</i></pre>
AWS::Cassandra::Table	<pre>arn:<i>partition</i> :cassandra:   <i>region</i>:<i>account_ID</i> :keyspace/   <i>keyspace_name</i> /table/<i>table_name</i></pre>
AWS::CloudFront::KeyValueStore	<pre>arn:<i>partition</i> :cloudfront:   <i>region</i>:<i>account_ID</i> :key-value-store/   <i>KVS_name</i></pre>
AWS::CloudTrail::Channel	<pre>arn:<i>partition</i> :cloudtrail:   <i>region</i>:<i>account_ID</i> :channel/   <i>channel_UUID</i></pre>
AWS::CodeWhisperer::Customization	<pre>arn:<i>partition</i> :codewhisperer:   <i>region</i>:<i>account_ID</i> :customization/   <i>customization_ID</i></pre>
AWS::CodeWhisperer::Profile	<pre>arn:<i>partition</i> :codewhisperer:   <i>region</i>:<i>account_ID</i> :profile/   <i>profile_ID</i></pre>
AWS::Cognito::IdentityPool	<pre>arn:<i>partition</i> :cognito-identity:   <i>region</i>:<i>account_ID</i> :identity-pool/   <i>identity_pool_ID</i></pre>

resources.type	resources.ARN
AWS::DynamoDB::Stream	<pre>arn:partition :dynamodb : region:account_ID :table/table_name / stream/date_time</pre>
AWS::EC2::Snapshot	<pre>arn:partition :ec2:region::snapsho t/ snapshot_ID</pre>
AWS::EMRWALES::Workspace	<pre>arn:partition :emrwal:region:account_I D :workspace/ workspace_name</pre>
AWS::FinSpace::Environment	<pre>arn:partition :finspace : region:account_ID :environm ent/ environment_ID</pre>
AWS::Glue::Table	<pre>arn:partition :glue:region:account_I D :table/database_name /table_name</pre>
AWS::GreengrassV2::ComponentVersion	<pre>arn:partition :greengra ss: region:account_ID :componen ts/ component_name</pre>
AWS::GreengrassV2::Deployment	<pre>arn:partition :greengra ss: region:account_ID :deployme nts/ deployment_ID</pre>
AWS::GuardDuty::Detector	<pre>arn:partition :guarddut y: region:account_ID :detector / detector_ID</pre>
AWS::IoT::Certificate	<pre>arn:partition :iot:region:account_I D :cert/certificate_ID</pre>

resources.type	resources.ARN
AWS::IoT::Thing	arn: <i>partition</i> :iot: <i>region</i> : <i>account_ID</i> :thing/ <i>thing_ID</i>
AWS::IoTSiteWise::Asset	arn: <i>partition</i> :iotsitewise: <i>region</i> : <i>account_ID</i> :asset/ <i>asset_ID</i>
AWS::IoTSiteWise::TimeSeries	arn: <i>partition</i> :iotsitewise: <i>region</i> : <i>account_ID</i> :timeseries/ <i>timeseries_ID</i>
AWS::IoTTwinMaker::Entity	arn: <i>partition</i> :iottwinmaker: <i>region</i> : <i>account_ID</i> :workspace/ <i>workspace_ID</i> /entity/ <i>entity_ID</i>
AWS::IoTTwinMaker::Workspace	arn: <i>partition</i> :iottwinmaker: <i>region</i> : <i>account_ID</i> :workspace/ <i>workspace_ID</i>
AWS::KendraRanking::ExecutionPlan	arn: <i>partition</i> :kendra-ranking: <i>region</i> : <i>account_ID</i> :rescore-execution-plan/ <i>rescore_execution_plan_ID</i>
AWS::Kinesis::Stream	arn: <i>partition</i> :kinesis: <i>region</i> : <i>account_ID</i> :stream/ <i>stream_name</i>
AWS::Kinesis::StreamConsumer	arn: <i>partition</i> :kinesis: <i>region</i> : <i>account_ID</i> :stream_type/ <i>stream_name</i> /consumer/ <i>consumer_name</i> : <i>consumer_creation_timestamp</i>

resources.type	resources.ARN
AWS::KinesisVideo::Stream	<pre>arn:partition :kinesisv ideo: region:account_I D :stream/stream_name /creation_time</pre>
AWS::ManagedBlockchain::Network	<pre>arn:partition :managedblockchain :::networks/ network_name</pre>
AWS::ManagedBlockchain::Node	<pre>arn:partition :managedblockchain : region:account_ID :nodes/node_ID</pre>
AWS::MedicalImaging::Datastore	<pre>arn:partition :medical- imaging: region:account_ID :datastor e/ data_store_ID</pre>
AWS::NeptuneGraph::Graph	<pre>arn:partition :neptune- graph: region:account_I D :graph/graph_ID</pre>
AWS::PCAConectorAD::Connector	<pre>arn:partition :pca-connector- ad: region:account_ID :connecto r/ connector_ID</pre>
AWS::QApps:QApp	<pre>arn:partition :qapps:region:account_I D :application/ application_UUID / qapp/qapp_UUID</pre>
AWS::QBusiness::Application	<pre>arn:partition :qbusines s: region:account_ID :applicat ion/ application_ID</pre>



resources.type	resources.ARN
AWS::QBusiness::DataSource	<pre>arn:partition :qbusines s: region:account_ID :applicat ion/ application_ID /index/index_ID/ data-source/ datasource_ID</pre>
AWS::QBusiness::Index	<pre>arn:partition :qbusines s: region:account_ID :applicat ion/ application_ID /index/index_ID</pre>
AWS::QBusiness::WebExperience	<pre>arn:partition :qbusines s: region:account_ID :applicat ion/ application_ID /web-expe rience/ web_experienc_ID</pre>
AWS::RDS::DBCluster	<pre>arn:partition :rds:region:account_I D :cluster/ cluster_name</pre>
AWS::S3::AccessPoint <sup>3</sup>	<pre>arn:partition :s3:region:account_I D :accesspoint/ access_point_name</pre>
AWS::S3ObjectLambda::AccessPoint	<pre>arn:partition :s3-object-lambda: region:account_ID :accesspo int/ access_point_name</pre>
AWS::S3Outposts::Object	<pre>arn:partition :s3-outpo sts: region:account_ID :object_path</pre>
AWS::SageMaker::Endpoint	<pre>arn:partition :sagemake r: region:account_ID :endpoint / endpoint_name</pre>

resources.type	resources.ARN
AWS::SageMaker::ExperimentTrialComponent	<pre>arn:partition:sagemake r: region:account_ID :experiment- trial-component/ experiment_trial_c omponent_name</pre>
AWS::SageMaker::FeatureGroup	<pre>arn:partition:sagemake r: region:account_ID :feature- group/ feature_group_name</pre>
AWS::SCN::Instance	<pre>arn:partition:scn:region:account_I D :instance/ instance_ID</pre>
AWS::ServiceDiscovery::Namespace	<pre>arn:partition:servicediscovery: region:account_ID :namespac e/ namespace_ID</pre>
AWS::ServiceDiscovery::Service	<pre>arn:partition:servicediscovery: region:account_ID :service/ service_I D</pre>
AWS::SNS::PlatformEndpoint	<pre>arn:partition:sns:region:account_I D :endpoint/ endpoint_type /endpoint_ name /endpoint_ID</pre>
AWS::SNS::Topic	<pre>arn:partition:sns:region:account_I D :topic_name</pre>
AWS::SQS::Queue	<pre>arn:partition:sqs:region:account_I D :queue_name</pre>

resources.type	resources.ARN
AWS::SSM::ManagedNode	<p>Der ARN muss in einem der folgenden Formate vorliegen:</p> <ul style="list-style-type: none"> <li>• <code>arn:partition :ssm:region:account_ID :managed-instance/ instance_ID</code></li> <li>• <code>arn:partition :ec2:region:account_ID :instance / instance_ID</code></li> </ul>
AWS::SSMMessages::ControlChannel	<pre>arn:partition :ssmmessages: region:account_ID :control-channel/ control_channel_ID</pre>
AWS::StepFunctions::StateMachine	<p>Der ARN muss in einem der folgenden Formate vorliegen:</p> <ul style="list-style-type: none"> <li>• <code>arn:partition :states:region:account_ID :stateMachine: stateMachine_name</code></li> <li>• <code>arn:partition :states:region:account_ID :stateMachine: stateMachine_name /label_name</code></li> </ul>
AWS::SWF::Domain	<pre>arn:partition :swf:region:account_ID :domain/ domain_name</pre>
AWS::ThinClient::Device	<pre>arn:partition :thinclient: region:account_ID :device/device_ID</pre>

resources.type	resources.ARN
AWS::ThinClient::Environment	arn: <i>partition</i> :thinclient: <i>region</i> : <i>account_ID</i> :environment/ <i>environment_ID</i>
AWS::Timestream::Database	arn: <i>partition</i> :timestream: <i>region</i> : <i>account_ID</i> :database/ <i>database_name</i>
AWS::Timestream::Table	arn: <i>partition</i> :timestream: <i>region</i> : <i>account_ID</i> :database/ <i>database_name</i> /table/ <i>table_name</i>
AWS::VerifiedPermissions::PolicyStore	arn: <i>partition</i> :verifiedpermissions: <i>region</i> : <i>account_ID</i> :policy-store/ <i>policy_store_ID</i>

<sup>1</sup> Bei Tabellen mit aktivierten Streams enthält das resources-Feld im Datenereignis sowohl AWS::DynamoDB::Stream als auch AWS::DynamoDB::Table. Wenn Sie AWS::DynamoDB::Table als resources.type angeben, werden standardmäßig sowohl DynamoDB-Tabellen- als auch DynamoDB-Stream-Ereignisse protokolliert. Um [Streams-Ereignisse](#) auszuschließen, fügen Sie dem eventName Feld einen Filter hinzu.


<sup>2</sup> Um alle Datenereignisse für alle Objekte in einem bestimmten S3-Bucket zu protokollieren, verwenden Sie den StartsWith-Operator und geben Sie nur die Bucket-ARN als übereinstimmenden Wert an. Der abschließende Schrägstrich ist beabsichtigt; schließen Sie ihn nicht aus.

<sup>3</sup> Um Ereignisse zu allen Objekten in einem S3-Zugangspunkt zu protokollieren, empfehlen wir, nur die Zugangspunkt-ARN zu verwenden, den Objektpfad nicht einzuschließen und die StartsWith- oder NotStartsWith-Operatoren oder zu verwenden.

Weitere Informationen zu den ARN-Formaten von Datenereignisressourcen finden Sie unter [Actions, resources, and condition keys](#) (Aktionen, Ressourcen und Bedingungsschlüssel) im AWS Identity and Access Management -Benutzerhandbuch.

- b. Wählen Sie für jedes Feld + Bedingung aus, um beliebig viele Bedingungen hinzuzufügen, bis zu maximal 500 angegebene Werte für alle Bedingungen. Um beispielsweise Datenereignisse für zwei S3-Buckets von Datenereignissen auszuschließen, die in Ihrem Trail protokolliert werden, können Sie das Feld auf Resources.ARN festlegen, den Operator für beginnt nicht mit festlegen und dann entweder einen S3-Bucket-ARN einfügen oder nach den S3-Buckets suchen, für die Sie keine Ereignisse protokollieren möchten.

Um den zweiten S3-Bucket hinzuzufügen, wählen Sie + Bedingung und wiederholen Sie dann die vorherige Anweisung, indem Sie den ARN für einen anderen Bucket einfügen oder nach einem anderen Bucket suchen.

 Note

Sie können maximal 500 Werte für alle Selektoren auf einem Trail haben. Dies schließt Arrays mit mehreren Werten für einen Selektor wie eventName ein. Wenn Sie einzelne Werte für alle Selektoren haben, können Sie einem Selektor maximal 500 Bedingungen hinzufügen.

Wenn Sie mehr als 15.000 Lambda-Funktionen in Ihrem Konto haben, können Sie beim Erstellen eines Trails nicht alle Funktionen in der CloudTrail Konsole anzeigen oder auswählen. Sie können jedoch alle Funktionen mit einer vordefinierten Selektorvorlage protokollieren, auch wenn sie nicht angezeigt werden. Wenn Sie Datenereignisse für bestimmte Funktionen protokollieren möchten, können Sie eine Funktion manuell hinzufügen, wenn Sie deren ARN kennen. Sie können die Erstellung des Trails auch in der Konsole abschließen und dann den Befehl AWS CLI und den put-event-selectors Befehl verwenden, um die Datenereignisprotokollierung für bestimmte Lambda-Funktionen zu konfigurieren. Weitere Informationen finden Sie unter [Verwaltung von Wanderwegen mit dem AWS CLI](#).

- c. Wählen Sie + Feld, um bei Bedarf zusätzliche Felder hinzuzufügen. Um Fehler zu vermeiden, legen Sie keine widersprüchlichen oder doppelten Werte für Felder fest. Geben Sie beispielsweise nicht an, dass ein ARN in einem Selektor einem Wert entspricht, und

geben Sie dann an, dass der ARN in einem anderen Selektor nicht dem gleichen Wert entspricht.

16. Um einen weiteren Datentyp hinzuzufügen, für den Datenereignisse protokolliert werden sollen, wählen Sie Datenereignistyp hinzufügen. Wiederholen Sie die Schritte 12 bis zu diesem Schritt, um erweiterte Ereignisselectoren für den Datenereignistyp zu konfigurieren.
17. Wählen Sie Insights-Ereignisse, wenn Ihr Trail CloudTrail Insights-Ereignisse protokollieren soll.

Wählen Sie unter Ereignistyp Insights-Ereignisse aus. Sie müssen Schreib-Verwaltungsereignisse protokollieren, um Insights-Ereignisse für die API-Aufruftrate zu protokollieren. Sie müssen Lese- und Schreib-Verwaltungsereignisse protokollieren, um Insights-Ereignisse für die API-Fehlerrate zu protokollieren.

CloudTrail Insights analysiert Verwaltungsereignisse auf ungewöhnliche Aktivitäten und protokolliert Ereignisse, wenn Anomalien festgestellt werden. Standardmäßig werden für Trails keine Insights-Ereignisse protokolliert. Weitere Informationen zu Insights-Ereignissen erhalten Sie unter [Protokollieren von Insights-Ereignissen](#). Für die Protokollierung von Insights-Ereignissen fallen zusätzliche Gebühren an. [Preisinformationen finden Sie unter CloudTrail AWS CloudTrail Preisgestaltung](#).

Insights-Ereignisse werden in einen anderen Ordner übertragen, /CloudTrail-Insight der nach demselben S3-Bucket benannt ist, der auf der Seite mit den Trail-Details im Bereich Speicherort angegeben ist. CloudTrail erstellt das neue Präfix für Sie. Wenn beispielsweise Ihr aktueller S3-Ziel-Bucket den Namen S3bucketName/AWSLogs/CloudTrail/ hat, lautet der Name mit dem Präfix als Zusatz S3bucketName/AWSLogs/CloudTrail-Insight/.

18. Wenn Sie die Auswahl der zu protokollierenden Ereignistypen abgeschlossen haben, wählen Sie Weiter aus.
19. Überprüfen Sie auf der Seite Prüfen und erstellen Ihre Auswahl. Wählen Sie Bearbeiten in einem Abschnitt, um die in diesem Abschnitt angezeigten Trail-Einstellungen zu ändern. Wenn Sie bereit sind, den Trail zu erstellen, wählen Sie Trail erstellen.
20. Der neue Trail wird auf der Seite Trails angezeigt. Veröffentlicht in etwa 5 Minuten Protokolldateien CloudTrail , in denen die AWS API-Aufrufe aufgeführt sind, die in Ihrem Konto getätigt wurden. Sie können die Protokolldateien in dem von Ihnen angegebenen S3-Bucket anzeigen. Es kann bis zu 36 Stunden dauern, CloudTrail bis das erste Insights-Ereignis zugestellt wird, wenn Sie die Insights-Ereignisprotokollierung aktiviert haben und ungewöhnliche Aktivitäten festgestellt werden.

**Note**

CloudTrail übermittelt Protokolle in der Regel innerhalb von durchschnittlich etwa 5 Minuten nach einem API-Aufruf. Diese Zeit ist nicht garantiert. Weitere Informationen finden Sie unter [AWS CloudTrail Service Level Agreement](#).

Wenn Sie Ihren Trail falsch konfigurieren (z. B. wenn der S3-Bucket nicht erreichbar ist), CloudTrail wird versucht, die Protokolldateien 30 Tage lang erneut in Ihren S3-Bucket zu übertragen. Für diese attempted-to-deliver Ereignisse fallen Standardgebühren an. CloudTrail Um Gebühren für einen falsch konfigurierten Trail zu vermeiden, müssen Sie den Trail löschen.

## Konfigurieren von Datenereigniseinstellungen mithilfe grundlegender Ereignisauswahlen

Sie können erweiterte Event-Selektoren verwenden, um alle Datenereignistypen zu konfigurieren. Mit erweiterten Ereignisselektoren können Sie detaillierte Selektoren erstellen, um nur die Ereignisse zu protokollieren, die für Sie von Interesse sind.

Wenn Sie grundlegende Event-Selektoren verwenden, um Datenereignisse zu protokollieren, sind Sie darauf beschränkt, Datenereignisse für Amazon S3 S3-Buckets, AWS Lambda Funktionen und Amazon DynamoDB-Tabellen zu protokollieren. Sie können das eventName Feld nicht mit einfachen Event-Selektoren filtern.

**Data events** [Info](#)

Data events show information about the resource operations performed on or within a resource. [Additional charges apply](#)

**Basic event selectors are enabled** [Switch to advanced event selectors](#)

Switch to advanced data event selectors for fine-grained control over the data events captured by your trail.

**Data event: S3** [Info](#) [Remove](#)

**Data event source**

Select source of data events to log.

- S3 ▲
- S3 ✓
- Lambda
- DynamoDB

**Individual bucket selection**

Choose Browse to select multiple buckets, then choose to log Read, Write or both event types on all selected buckets.

[Browse](#)  Read  Write ×

[Add bucket](#)

[Add data event type](#)


Führen Sie die folgenden Schritte aus, um Datenereigniseinstellungen mithilfe grundlegender Ereignisauswahlen zu konfigurieren.

Konfigurieren von Datenereigniseinstellungen mithilfe grundlegender Ereignisauswahlen

1. Wählen Sie unter Ereignisse die Option Datenereignisse aus, um Datenereignisse zu protokollieren. Für die Protokollierung von Datenereignissen fallen zusätzliche Gebühren an. Weitere Informationen finden Sie unter [AWS CloudTrail -Preisgestaltung](#).
2. Für Amazon-S3-Buckets:
  - a. Wählen Sie für Daten-Ereignisquelle S3 aus.



- b. Sie können wählen, ob Sie alle aktuellen und zukünftigen S3 Buckets protokollieren oder einzelne Buckets oder Funktionen angeben möchten. Standardmäßig werden Datenereignisse für alle aktuellen und zukünftigen S3 Buckets protokolliert.

 Note

Wenn Sie die Standardoption Alle aktuellen und future S3-Buckets beibehalten, wird die Datenereignisprotokollierung für alle Buckets aktiviert, die sich derzeit in Ihrem AWS Konto befinden, sowie für alle Buckets, die Sie erstellen, nachdem Sie den Trail erstellt haben. Sie ermöglicht auch die Protokollierung von Datenereignisaktivitäten, die von einer beliebigen IAM-Identität in Ihrem AWS Konto ausgeführt werden, selbst wenn diese Aktivität in einem Bucket ausgeführt wird, der zu einem anderen Konto gehört. AWS

Wenn Sie einen Trail für eine einzelne Region erstellen (mithilfe von AWS CLI), aktiviert die Auswahl von Alle aktuellen und future S3-Buckets die Datenereignisprotokollierung für alle Buckets in derselben Region wie Ihr Trail und für alle Buckets, die Sie später in dieser Region erstellen. Es werden keine Datenereignisse für Amazon S3 S3-Buckets in anderen Regionen in Ihrem AWS Konto protokolliert.


- c. Wenn Sie die Standardeinstellung Alle aktuellen und zukünftigen S3 Buckets beibehalten, können Sie Leseereignisse, Schreibereignisse oder beides protokollieren.
- d. Um einzelne Buckets auszuwählen, leeren Sie die Kontrollkästchen Lesen und Schreiben für Alle aktuellen und zukünftigen S3 Buckets. Suchen Sie unter Individuelle Bucket-Auswahl nach einem Bucket, in dem Datenereignisse protokolliert werden sollen. Suchen Sie nach bestimmten Buckets, indem Sie ein Bucket-Präfix für den gewünschten Bucket eingeben. Sie können in diesem Fenster mehrere Buckets auswählen. Wählen Sie Bucket hinzufügen, um Datenereignisse für weitere Buckets zu protokollieren. Wählen Sie, ob Sie Read (Lesen)-Ereignisse wie `GetObject`, Write (Schreiben)-Ereignisse wie `PutObject` oder Ereignisse beider Typen protokolliert werden sollen.

Diese Einstellung hat Vorrang vor individuellen Einstellungen, die Sie für einzelne Buckets konfigurieren. Wenn Sie beispielsweise die Protokollierung von Lese-Ereignissen für alle S3-Buckets festlegen und dann einen bestimmten Bucket für die Protokollierung von Datenereignissen hinzufügen, ist für den hinzugefügten Bucket bereits Lesen ausgewählt. Sie können die Auswahl nicht löschen. Sie können die Option nur für Write (Schreiben) konfigurieren.

Um einen Bucket aus der Protokollierung zu entfernen, wählen Sie X aus.

3. Um einen weiteren Datentyp hinzuzufügen, für den Datenereignisse protokolliert werden sollen, wählen Sie Datenereignistyp hinzufügen.
4. Für Lambda-Funktionen:
  - a. Wählen Sie für Daten-Ereignisquelle Lambda aus.
  - b. Wählen Sie in der Lambda-Funktion Alle Regionen aus, um alle Lambda-Funktionen zu protokollieren, oder Eingabefunktion als ARN, um Datenereignisse für eine bestimmte Funktion zu protokollieren.

Um Datenereignisse für alle Lambda-Funktionen in Ihrem AWS Konto zu protokollieren, wählen Sie Alle aktuellen und future Funktionen protokollieren aus. Diese Einstellung hat Vorrang vor individuellen Einstellungen, die Sie für einzelne Funktionen vornehmen. Alle Funktionen werden protokolliert, auch wenn nicht alle Funktionen angezeigt werden.

 Note

Wenn Sie einen Trail für alle Regionen erstellen, wird durch diese Auswahl die Datenereignisprotokollierung für alle Funktionen aktiviert, die sich derzeit in Ihrem AWS -Konto befinden, sowie für alle Lambda-Funktionen, die Sie ggf. in einer Region erstellen, nachdem Sie den Trail erstellt haben. Wenn Sie einen Trail für eine einzelne Region erstellen (mithilfe von AWS CLI), aktiviert diese Auswahl die Datenereignisprotokollierung für alle Funktionen, die sich derzeit in dieser Region in Ihrem AWS Konto befinden, sowie für alle Lambda-Funktionen, die Sie möglicherweise in dieser Region erstellen, nachdem Sie den Trail erstellt haben. Es wird keine Datenereignisprotokollierung für Lambda-Funktionen aktiviert, die in anderen Regionen erstellt wurden.

Das Protokollieren von Datenereignissen für alle Funktionen ermöglicht auch die Protokollierung von Datenereignisaktivitäten, die von einer beliebigen IAM-Identität in Ihrem AWS Konto ausgeführt werden, selbst wenn diese Aktivität für eine Funktion ausgeführt wird, die zu einem anderen AWS Konto gehört.

- c. Wenn Sie Eingabefunktion als ARN wählen, geben Sie den ARN einer Lambda-Funktion ein.

**Note**

Wenn Sie mehr als 15.000 Lambda-Funktionen in Ihrem Konto haben, können Sie beim Erstellen eines Trails nicht alle Funktionen in der CloudTrail Konsole anzeigen oder auswählen. Sie können weiterhin die Option wählen, alle Funktionen zu protokollieren, auch wenn sie nicht angezeigt werden. Wenn Sie Datenereignisse für bestimmte Funktionen protokollieren möchten, können Sie eine Funktion manuell hinzufügen, wenn Sie deren ARN kennen. Sie können die Erstellung des Trails auch in der Konsole abschließen und dann den Befehl AWS CLI und den `put-event-selectors` Befehl verwenden, um die Datenereignisprotokollierung für bestimmte Lambda-Funktionen zu konfigurieren. Weitere Informationen finden Sie unter [Verwaltung von Wanderwegen mit dem AWS CLI](#).

5. Für DynamoDB-Tabellen:
  - a. Wählen Sie für Daten-Ereignisquelle DynamoDB aus.
  - b. Wählen Sie unter DynamoDB table selection (DynamoDB-Tabellenauswahl) die Option Browse (Durchsuchen), um eine Tabelle auszuwählen, oder fügen Sie den ARN einer DynamoDB-Tabelle ein, auf die Sie Zugriff haben. Ein DynamoDB-Tabellen-ARN verwendet das folgende Format:

```
arn:partition:dynamodb:region:account_ID:table/table_name
```

Um eine weitere Tabelle hinzuzufügen, wählen Sie Add row (Zeile hinzufügen) und suchen Sie nach einer Tabelle oder fügen Sie den ARN einer Tabelle ein, auf die Sie Zugriff haben.

6. Um Insights-Ereignisse und andere Einstellungen für Ihren Trail zu konfigurieren, kehren Sie zum vorherigen Verfahren in diesem Thema zurück, [???](#).

### Nächste Schritte

Nach der Trail-Erstellung können Sie zu dem Trail zurückkehren, um Änderungen vorzunehmen:

- Falls Sie dies noch nicht getan haben, können Sie so konfigurieren, CloudTrail dass Protokolldateien an CloudWatch Logs gesendet werden. Weitere Informationen finden Sie unter [Ereignisse an CloudWatch Logs senden](#).

- Erstellen Sie eine Tabelle zur Ausführung einer Abfrage in Amazon Athena, um die AWS -Service-Aktivitäten zu analysieren. Weitere Informationen finden Sie unter [Erstellen einer Tabelle für CloudTrail Protokolle in der CloudTrail Konsole](#) im [Amazon Athena Athena-Benutzerhandbuch](#).
- Fügen Sie benutzerdefinierte Tags (Schlüssel-Wert-Paare) zum Trail hinzu.
- Um einen weiteren Trail zu erstellen, öffnen Sie die Seite Trails und wählen Sie Trail erstellen aus.

## Aktualisieren eines Trails

In diesem Abschnitt wird beschrieben, wie Sie die Trail-Einstellungen ändern.

Um einen Trail mit einer Region zu aktualisieren, sodass alle Ereignisse in der [AWS Partition](#), AWS-Regionen in der Sie arbeiten, protokolliert werden, oder um einen Trail mit mehreren Regionen zu aktualisieren, sodass Ereignisse nur in einer einzigen Region protokolliert werden, müssen Sie den verwenden. AWS CLI Weitere Informationen zum Aktualisieren eines Trails für eine einzelne Region, um Ereignisse in allen Regionen zu protokollieren, finden Sie unter [Umwandeln eines Trails, der für eine Region gilt, zu einem Trail für alle Regionen](#). Weitere Informationen zum Aktualisieren eines multiregionalen Trails, um Ereignisse in einer einzigen Region zu protokollieren, finden Sie unter [Umwandeln eines multiregionalen Trails in einen Trail für eine einzelne Region](#).

Wenn Sie CloudTrail Verwaltungsereignisse in Amazon Security Lake aktiviert haben, müssen Sie mindestens einen organisatorischen Pfad verwalten, der mehrere Regionen umfasst `read` und sowohl Verwaltungsereignisse als auch `write` Verwaltungsereignisse protokolliert. Sie können einen relevanten Trail nicht so aktualisieren, dass er gegen die Security-Lake-Anforderungen verstößt, beispielsweise, indem Sie den Trail zu einem Trail für einzelne Regionen ändern oder indem Sie die Protokollierung von `read`- oder `write`-Verwaltungsereignissen deaktivieren.

### Note


CloudTrail aktualisiert die Organisationspfade in Mitgliedskonten, auch wenn eine Ressourcenvalidierung fehlschlägt. Beispiele für fehlgeschlagene Überprüfungen sind:

- eine falsche Amazon S3 S3-Bucket-Richtlinie
- eine falsche Amazon SNS SNS-Themenrichtlinie
- Unfähigkeit, an eine CloudWatch Logs-Protokollgruppe zu liefern
- unzureichende Rechte zur Verschlüsselung mit einem KMS-Schlüssel

Ein Mitgliedskonto mit CloudTrail Berechtigungen kann alle Validierungsfehler für einen Organisationspfad anzeigen, indem es die Detailseite des Trails in der CloudTrail Konsole aufruft oder den AWS CLI [get-trail-status](#) Befehl ausführt.

Um einen Trail mit dem zu aktualisieren AWS Management Console


1. Melden Sie sich bei der an AWS Management Console und öffnen Sie die CloudTrail Konsole unter <https://console.aws.amazon.com/cloudtrail/>.
2. Wählen Sie im Navigationsbereich die Option Trails und dann den Namen des Pfades aus.
3. Wählen Sie unter Allgemeine Details Bearbeiten aus, um die folgenden Einstellungen zu ändern. Sie können den Namen eines Trails nicht ändern.
  - Trail auf meine Organisation anwenden — Ändern Sie, ob es sich bei diesem Trail um einen AWS Organizations Organisations-Trail handelt.

 Note

Nur das Verwaltungskonto der Organisation kann einen Organisations-Trail in einen Nicht-Organisations-Trail und einen Nicht-Organisations-Trail in einen Organisations-Trail umwandeln.

- Ort des Trail-Protokolls – Ändern Sie den Namen des S3 Buckets oder das Präfix, in dem Sie Protokolle für diesen Trail speichern.
  - SSE-KMS-Verschlüsselung der Protokolldatei – Aktivieren oder deaktivieren Sie die Verschlüsselung von Protokolldateien mit SSE-KMS anstelle von SSE-S3.
  - Protokolldateivalidierung – Aktivieren oder deaktivieren Sie die Validierung der Integrität von Protokolldateien.
  - Zustellung von SNS-Benachrichtigungen – Aktivieren oder deaktivieren Sie die Benachrichtigungen des Amazon Simple Notification Service (Amazon SNS), dass Protokolldateien an den für den Trail angegebenen Bucket zugestellt wurden.
- a. Um den Trail in einen AWS Organizations Organisationspfad umzuwandeln, können Sie den Trail für alle Accounts in Ihrer Organisation aktivieren. Weitere Informationen finden Sie unter [Erstellen eines Trails für eine Organisation](#).

- b. Um den angegebenen Bucket im Speicherort zu ändern, wählen Sie Neuen S3 Bucket erstellen, um einen Bucket zu erstellen. Wenn Sie einen Bucket erstellen, werden die erforderlichen Bucket-Richtlinien CloudTrail erstellt und angewendet. Wenn Sie sich dafür entscheiden, einen neuen S3-Bucket zu erstellen, muss Ihre IAM-Richtlinie die Genehmigung für die `s3:PutEncryptionConfiguration` Aktion enthalten, da die serverseitige Verschlüsselung standardmäßig für den Bucket aktiviert ist.

 Note

Wenn Sie Vorhandenen S3 Bucket verwenden ausgewählt haben, geben Sie einen Bucket im Namen des Trail-Protokoll-Buckets an oder wählen Sie Durchsuchen, um einen Bucket auszuwählen. Die Bucket-Richtlinie muss die CloudTrail Schreibberechtigung für den Bucket gewähren. Informationen zur manuellen Bearbeitung der Bucket-Richtlinie finden Sie im Abschnitt [Amazon S3 S3-Bucket-Richtlinie für CloudTrail](#).

Um das Auffinden Ihrer Logs zu erleichtern, erstellen Sie in einem vorhandenen Bucket einen neuen Ordner (auch als Präfix bezeichnet), um Ihre CloudTrail Logs zu speichern. Geben Sie das Präfix in Präfix ein.

- c. Wählen Sie unter Log file SSE-KMS encryption (SSE-KMS-Verschlüsselung der Protokolldatei) die Option Enabled (Aktiviert) aus, wenn Sie Ihre Protokolldateien mit der SSE-KMS-Verschlüsselung anstelle der SSE-S3-Verschlüsselung verschlüsseln möchten. Der Standard ist aktiviert. Wenn Sie die SSE-KMS-Verschlüsselung nicht aktivieren, werden die Protokolle mit der SSE-S3-Verschlüsselung verschlüsselt. Weitere Informationen zur SSE-KMS-Verschlüsselung finden Sie unter [Verwenden der serverseitigen Verschlüsselung mit AWS Key Management Service \(SSE-KMS\)](#). Weitere Informationen zur SSE-S3-Verschlüsselung finden Sie unter [Verwenden der serverseitigen Verschlüsselung mit von Amazon S3 verwalteten Verschlüsselungsschlüsseln \(SSE-S3\)](#).

Wenn Sie die SSE-KMS-Verschlüsselung aktivieren, wählen Sie Neu oder Bestehend aus. AWS KMS key Geben Sie AWS KMS unter Alias einen Alias im Format an. `alias/MyAliasName` Weitere Informationen finden Sie unter [Aktualisieren einer Ressource zur Verwendung des KMS-Schlüssels](#). CloudTrail unterstützt auch Schlüssel AWS KMS für mehrere Regionen. Weitere Informationen finden Sie über Multi-Regions-Schlüssel finden Sie unter [Verwenden von Schlüsseln für mehrere Regionen](#) im AWS Key Management Service -Entwicklerhandbuch.

**Note**

Sie können auch den ARN eines Schlüssels aus einem anderen Konto eingeben. Weitere Informationen finden Sie unter [Aktualisieren einer Ressource zur Verwendung des KMS-Schlüssels](#). Die Schlüsselrichtlinie muss die Verwendung des Schlüssels zum Verschlüsseln Ihrer Protokolldateien ermöglichen und den von Ihnen angegebenen Benutzern das Lesen von Protokolldateien in unverschlüsselter Form ermöglichen. CloudTrail Informationen zur manuellen Bearbeitung der Schlüsselrichtlinie finden Sie unter [Konfigurieren Sie AWS KMS wichtige Richtlinien für CloudTrail](#).

- d. Wählen Sie für Protokolldateivalidierung Aktiviert, damit Ihrem S3 Bucket Protokoll-Digests übermittelt werden. Mithilfe der Digest-Dateien können Sie überprüfen, ob sich Ihre Protokolldateien nach CloudTrail der Übermittlung nicht geändert haben. Weitere Informationen finden Sie unter [Überprüfen der Integrität der CloudTrail Protokolldatei](#).
- e. Wählen Sie für die Zustellung von SNS-Benachrichtigungen die Option Aktiviert aus, um jedes Mal benachrichtigt zu werden, wenn ein Protokoll an Ihren Bucket gesendet wird. CloudTrail speichert mehrere Ereignisse in einer Protokolldatei. SNS-Benachrichtigungen werden für jede Protokolldatei, nicht für jedes Ereignis gesendet. Weitere Informationen finden Sie unter [Konfiguration von Amazon SNS SNS-Benachrichtigungen für CloudTrail](#).


Wenn Sie SNS-Benachrichtigungen aktivieren, wählen Sie für Neues SNS-Thema erstellen die Option Neu aus, um ein Thema zu erstellen, oder wählen Sie Vorhanden aus, um ein vorhandenes Thema zu verwenden. Wenn Sie einen Trail erstellen, der für alle Regionen gilt, werden SNS-Benachrichtigungen für Protokolldateizustellungen aus allen Regionen an das von Ihnen erstellte einzelne SNS-Thema gesendet.

Wenn Sie Neu wählen, CloudTrail gibt Sie einen Namen für das neue Thema an, oder Sie können einen Namen eingeben. Wenn Sie Vorhanden wählen, wählen Sie ein SNS-Thema aus der Dropdown-Liste aus. Sie können auch den ARN eines Themas aus einer anderen Region oder aus einem Konto mit den entsprechenden Berechtigungen eingeben. Weitere Informationen finden Sie unter [Amazon SNS SNS-Themenrichtlinie für CloudTrail](#).

Wenn Sie ein Thema erstellen, müssen Sie das Thema abonnieren, um über die Zustellung von Protokolldateien benachrichtigt zu werden. Sie können das Abonnement von der Amazon-SNS-Konsole aus vornehmen. Aufgrund der Häufigkeit der Benachrichtigungen empfehlen wir, das Abonnement so zu konfigurieren, dass eine Amazon-SQS-

Warteschlange zur programmgesteuerten Bearbeitung der Benachrichtigungen verwendet wird. Weitere Informationen finden Sie unter [Erste Schritte mit Amazon SNS](#) im Benutzerhandbuch für Amazon Simple Notification Service.

4. Wählen Sie unter CloudWatch Logs die Option Bearbeiten aus, um die Einstellungen für das Senden von CloudTrail Logdateien an CloudWatch Logs zu ändern. Wählen Sie unter CloudWatch Protokolle die Option Aktiviert aus, um das Senden von Protokolldateien zu aktivieren. Weitere Informationen finden Sie unter [Ereignisse an CloudWatch Logs senden](#).
  - a. Wenn Sie die Integration mit CloudWatch Logs aktivieren, wählen Sie Neu, um eine neue Protokollgruppe zu erstellen, oder Existierend, um eine bestehende zu verwenden. Wenn Sie „Neu“ wählen CloudTrail, geben Sie einen Namen für die neue Protokollgruppe an, oder Sie können einen Namen eingeben.
  - b. Wenn Sie Vorhanden wählen, wählen Sie eine Protokollgruppe aus der Dropdown-Liste aus.
  - c. Wählen Sie Neu, um eine neue IAM-Rolle für Berechtigungen zum Senden von Protokollen an Logs zu CloudWatch erstellen. Wählen Sie Vorhanden, um eine vorhandene IAM-Rolle aus der Dropdown-Liste auszuwählen. Die Richtlinienanweisung für die neue oder vorhandene Rolle wird angezeigt, wenn Sie das Richtliniendokument erweitern. Weitere Informationen über diese Rolle finden Sie unter [Rollenrichtlinien-Dokument CloudTrail zur Verwendung von CloudWatch Logs zur Überwachung](#).

 Note

- Beim Konfigurieren eines Trails können Sie einen S3 Bucket und ein SNS-Thema auswählen, die zu einem anderen Konto gehören. Wenn Sie jedoch Ereignisse CloudTrail an eine CloudWatch Logs-Protokollgruppe übermitteln möchten, müssen Sie eine Protokollgruppe auswählen, die in Ihrem aktuellen Konto vorhanden ist.
- Nur das Verwaltungskonto kann mithilfe der Konsole eine CloudWatch Logs-Protokollgruppe für einen Organisations-Trail konfigurieren. Der delegierte Administrator kann eine CloudWatch Logs-Protokollgruppe mithilfe der UpdateTrail API-Operationen AWS CLI oder CloudTrail CreateTrail oder konfigurieren.

5. Wählen Sie unter Tags Bearbeiten aus, um Tags auf dem Trail zu ändern, hinzuzufügen oder zu löschen. Fügen Sie ein oder mehrere benutzerdefinierte Tags (Schlüssel-Wert-Paare) zu Ihrem Trail hinzu. Mithilfe von Tags können Sie sowohl Ihre CloudTrail Trails als auch die Amazon S3



S3-Buckets identifizieren, die CloudTrail Protokolldateien enthalten. Anschließend können Sie Ressourcengruppen für Ihre CloudTrail Ressourcen verwenden. Weitere Informationen finden Sie unter [AWS Resource Groups](#) und [Tags](#).

6. Wählen Sie unter Verwaltungsereignisse die Option Bearbeiten aus, um die Protokollierungseinstellungen für Verwaltungsereignisse zu ändern.
  - a. Wählen Sie für API-Aktivität aus, ob Ihr Trail Leseereignisse, Schreibereignisse oder beides protokollieren soll. Weitere Informationen finden Sie unter [Verwaltungsereignisse](#).
  - b. Wähle AWS KMS Ereignisse ausschließen, um Ereignisse aus deinem Trail herauszufiltern AWS Key Management Service (AWS KMS). Die Standardeinstellung besteht darin, alle AWS KMS -Ereignissen einzuschließen.


Die Option, AWS KMS Ereignisse zu protokollieren oder auszuschließen, ist nur verfügbar, wenn Sie Verwaltungsereignisse auf Ihrem Trail protokollieren. Wenn Sie sich dafür entscheiden, Verwaltungsereignisse nicht zu protokollieren, werden AWS KMS Ereignisse nicht protokolliert, und Sie können die Einstellungen für die AWS KMS Ereignisprotokollierung nicht ändern.

AWS KMS Aktionen wie `EncryptDecrypt`, und erzeugen `GenerateDataKey` in der Regel ein großes Volumen (mehr als 99%) von Ereignissen. Diese Aktionen werden nun als Leseereignisse protokolliert. Relevante AWS KMS Aktionen mit geringem Volumen wie `DisableDelete`, und `ScheduleKey` (die in der Regel weniger als 0,5% des AWS KMS Ereignisvolumens ausmachen) werden als Write-Ereignisse protokolliert.

Um Ereignisse mit hohem Volume wie `Encrypt`, `Decrypt` und `GenerateDataKey` auszuschließen, aber dennoch relevante Ereignisse wie `Disable`, `Delete` und `ScheduleKey` zu protokollieren, wählen Sie Schreibverwaltungsereignisse protokollieren und deaktivieren Sie das Kontrollkästchen für AWS KMS -Ereignisse ausschließen.

- c. Klicken Sie auf Amazon-RDS-Daten-API ausschließen zum Filtern von Ereignissen der Amazon-Relational-Database-Service-Daten-API aus Ihrem Trail. Die Standardeinstellung besteht darin, alle Amazon-RDS-Daten-API-Ereignisse einzubeziehen. Weitere Informationen über die Amazon-RDS-Daten-API finden Sie unter [Protokollieren von Daten-API-Aufrufen mit AWS CloudTrail](#) im Amazon-RDS-Benutzerhandbuch für Aurora.

7.


 **Important**

Die Schritte 7 bis 11 betreffen die Konfiguration von Datenereignissen mithilfe erweiterter Ereignisauswahlen. Mithilfe erweiterter Ereignisauswahlen können Sie mehr

[Datenergebnistypen](#) konfigurieren und genau steuern, welche Datenergebnisse in Ihrem Trail erfasst werden. Wenn Sie bereits erweiterte Ereignisauswahlen verwenden, lesen Sie [Aktualisieren von Datenergebniseinstellungen mit grundlegenden Ereignisauswahlen](#) und machen Sie dann bei Schritt 12 dieses Verfahrens weiter.


Wählen Sie unter Datenergebnisse Bearbeiten aus, um die Einstellungen für die Datenergebnisprotokollierung zu ändern. Standardmäßig werden Datenergebnisse nicht von den Trails protokolliert. Für die Protokollierung von Datenergebnissen fallen zusätzliche Gebühren an. Informationen zu CloudTrail-Preisen finden Sie unter [AWS CloudTrail – Preise](#).

Wählen Sie für Datenergebnistyp den Ressourcentyp aus, für den Sie Datenergebnisse protokollieren möchten. Weitere Informationen zu den verfügbaren Datenergebnistypen finden Sie unter [Datenergebnisse](#).

 Note

Um Datenergebnisse für von Lake Formation erstellte AWS Glue Tabellen zu protokollieren, wählen Sie Lake Formation.

8. Wählen Sie eine Protokollauswahlvorlage. CloudTrail enthält vordefinierte Vorlagen, die alle Datenergebnisse für den Ressourcentyp protokollieren. Um eine benutzerdefinierte Protokoll-Selektorvorlage zu erstellen, wählen Sie Benutzerdefiniert aus.

 Note

Wenn Sie eine vordefinierte Vorlage für S3-Buckets auswählen, wird die Protokollierung von Datenergebnissen für alle Buckets aktiviert, die sich derzeit in Ihrem AWS Konto befinden, sowie für alle Buckets, die Sie nach Abschluss der Erstellung des Trails erstellen. Es ermöglicht auch die Protokollierung der Datenergebnisaktivitäten, die von einem beliebigen Benutzer oder einer Rolle in Ihrem AWS Konto ausgeführt werden, selbst wenn diese Aktivität in einem Bucket ausgeführt wird, der zu einem anderen Konto gehört. AWS


Wenn der Trail nur für eine Region gilt, aktiviert die Auswahl einer vordefinierten Vorlage, die alle S3 Buckets protokolliert, die Datenergebnisprotokollierung für alle Buckets in derselben Region wie Ihr Trail und alle Buckets, die Sie später in dieser Region erstellen. Es werden keine Protokolldatenergebnisse für Amazon-S3-Buckets in anderen Regionen in Ihrem AWS -Konto protokolliert.

Wenn Sie einen Trail für alle Regionen erstellen, aktiviert die Auswahl einer vordefinierten Vorlage für Lambda-Funktionen die Datenereignisprotokollierung für alle Funktionen, die sich derzeit in Ihrem AWS Konto befinden, sowie für alle Lambda-Funktionen, die Sie möglicherweise in einer beliebigen Region erstellen, nachdem Sie den Trail erstellt haben. Wenn Sie einen Trail für eine einzelne Region erstellen (mithilfe von AWS CLI), aktiviert diese Auswahl die Datenereignisprotokollierung für alle Funktionen, die sich derzeit in dieser Region in Ihrem AWS Konto befinden, sowie für alle Lambda-Funktionen, die Sie möglicherweise in dieser Region erstellen, nachdem Sie den Trail erstellt haben. Es wird keine Datenereignisprotokollierung für Lambda-Funktionen aktiviert, die in anderen Regionen erstellt wurden.

Das Protokollieren von Datenereignissen für alle Funktionen ermöglicht auch die Protokollierung von Datenereignisaktivitäten, die von einem beliebigen Benutzer oder einer Rolle in Ihrem AWS Konto ausgeführt werden, selbst wenn diese Aktivität für eine Funktion ausgeführt wird, die zu einem anderen AWS Konto gehört.

9. (Optional) Geben Sie unter Selektornamen einen Namen ein, um Ihre Auswahl zu identifizieren. Der Selektornamen ist ein optionaler, beschreibender Name für eine erweiterte Ereignisauswahl, z. B. „Datenereignisse nur für zwei S3-Buckets protokollieren“. Der Name des Selektors wird als Name in der erweiterten Ereignisauswahl aufgeführt und ist sichtbar, wenn Sie die JSON-Ansicht erweitern.
10. Erstellen Sie in den erweiterten Ereignisselektoren einen Ausdruck für die spezifischen Ressourcen, für die Sie Datenereignisse sammeln möchten. Sie können diesen Schritt überspringen, wenn Sie eine vordefinierte Protokollvorlage verwenden.
  - a. Wählen Sie aus den folgenden Feldern.
    - **readOnly**- `readOnly` kann auf den Wert **true** oder **false** gesetzt werden. Um sowohl `read`- als auch `write`-Ereignisse zu protokollieren, fügen Sie keinen `readOnly`-Selektor hinzu.
    - **eventName** – `eventName` kann einen beliebigen Operator verwenden. Sie können damit jedes Datenereignis, für das protokolliert wurde, ein- oder ausschließen CloudTrail, z. B. `PutBucket` oder `GetSnapshotBlock`.
    - **resources.ARN**- Sie können jeden Operator mit verwenden `resources.ARN`, aber wenn Sie `equals` oder `ungleich` verwenden, muss der Wert genau dem ARN einer gültigen Ressource des Typs entsprechen, den Sie in der Vorlage als Wert von `resources.type` angegeben haben.

In der folgenden Tabelle wird das gültige ARN-Format für alle `resources.type`-Werte aufgeführt.

 Note

Sie können das `resources.ARN` Feld nicht verwenden, um Ressourcentypen zu filtern, die keine ARNs haben.

resources.type	resources.ARN
AWS::DynamoDB::Table <sup>1</sup>	arn: <i>partition</i> :dynamodb : <i>region:account_ID</i> :table/ <i>table_name</i>
AWS::Lambda::Function	arn: <i>partition</i> :lambda: <i>region:account_ID</i> :function: <i>function_name</i>
AWS::S3::Object <sup>2</sup>	arn: <i>partition</i> :s3::: <i>bucket_name</i> / arn: <i>partition</i> :s3::: <i>bucket_name</i> / <i>object_or_file_name</i> /
AWS::AppConfig::Configuration	arn: <i>partition</i> :appconfi g: <i>region:account_ID</i> :applicat ion/ <i>application_ID</i> /environm ent/ <i>environment_ID</i> /configur ation/ <i>configuration_profile_ID</i>
AWS::B2BI::Transformer	arn: <i>partition</i> :b2bi: <i>region:account_ID</i> :transformer/ <i>transformer_ID</i>
AWS::Bedrock::AgentAlias	arn: <i>partition</i> :bedrock: <i>region:account_ID</i> :agent-al ias/ <i>agent_ID/alias_ID</i>

resources.type	resources.ARN
AWS::Bedrock::KnowledgeBase	arn: <i>partition</i> :bedrock: : <i>region</i> : <i>account_ID</i> :knowledge- base/ <i>knowledge_base_ID</i>
AWS::Cassandra::Table	arn: <i>partition</i> :cassandr a: <i>region</i> : <i>account_ID</i> :keyspace / <i>keyspace_name</i> /table/ <i>table_name</i>
AWS::CloudFront::KeyValueStore	arn: <i>partition</i> :cloudfro nt: <i>region</i> : <i>account_ID</i> :key-value- store/ <i>KVS_name</i>
AWS::CloudTrail::Channel	arn: <i>partition</i> :cloudtra il: <i>region</i> : <i>account_ID</i> :channel/ <i>channel_UUID</i>
AWS::CodeWhisperer::Customi zation	arn: <i>partition</i> :codewhis perer: <i>region</i> : <i>account_ID</i> :customiz ation/ <i>customization_ID</i>
AWS::CodeWhisperer::Profile	arn: <i>partition</i> :codewhis perer: <i>region</i> : <i>account_ID</i> :profile/ <i>profile_ID</i>
AWS::Cognito::IdentityPool	arn: <i>partition</i> :cognito-identity: : <i>region</i> : <i>account_ID</i> :identity pool/ <i>identity_pool_ID</i>
AWS::DynamoDB::Stream	arn: <i>partition</i> :dynamodb : <i>region</i> : <i>account_ID</i> :table/ <i>table_name</i> / stream/ <i>date_time</i>

resources.type	resources.ARN
AWS::EC2::Snapshot	arn: <i>partition</i> :ec2: <i>region</i> ::snapshot/ <i>snapshot_ID</i>
AWS::EMRWALES::Workspace	arn: <i>partition</i> :emrwal: <i>region</i> : <i>account_ID</i> :workspace/ <i>workspace_name</i>
AWS::FinSpace::Environment	arn: <i>partition</i> :finspace : <i>region</i> : <i>account_ID</i> :environment/ <i>environment_ID</i>
AWS::Glue::Table	arn: <i>partition</i> :glue: <i>region</i> : <i>account_ID</i> :table/ <i>database_name</i> / <i>table_name</i>
AWS::GreengrassV2::ComponentVersion	arn: <i>partition</i> :greengrass : <i>region</i> : <i>account_ID</i> :components/ <i>component_name</i>
AWS::GreengrassV2::Deployment	arn: <i>partition</i> :greengrass : <i>region</i> : <i>account_ID</i> :deployments/ <i>deployment_ID</i>
AWS::GuardDuty::Detector	arn: <i>partition</i> :guardduty : <i>region</i> : <i>account_ID</i> :detector / <i>detector_ID</i>
AWS::IoT::Certificate	arn: <i>partition</i> :iot: <i>region</i> : <i>account_ID</i> :cert/ <i>certificate_ID</i>
AWS::IoT::Thing	arn: <i>partition</i> :iot: <i>region</i> : <i>account_ID</i> :thing/ <i>thing_ID</i>

resources.type	resources.ARN
AWS::IoTSiteWise::Asset	arn: <i>partition</i> :iotsitew ise: <i>region:account_ID</i> :asset/ <i>asset_ID</i>
AWS::IoTSiteWise::TimeSeries	arn: <i>partition</i> :iotsitew ise: <i>region:account_ID</i> :timeseri es/ <i>timeseries_ID</i>
AWS::IoTtwinMaker::Entity	arn: <i>partition</i> :iottwinm aker: <i>region:account_ID</i> :workspac e/ <i>workspace_ID</i> /entity/ <i>entity_ID</i>
AWS::IoTtwinMaker::Workspace	arn: <i>partition</i> :iottwinm aker: <i>region:account_ID</i> :workspac e/ <i>workspace_ID</i>
AWS::KendraRanking::ExecutionPlan	arn: <i>partition</i> :kendra-r anking: <i>region:account_ID</i> :rescore- execution-plan/ <i>rescore_execution_</i> <i>plan_ID</i>
AWS::Kinesis::Stream	arn: <i>partition</i> :kinesis: <i>region:account_ID</i> :stream/ <i>stream_name</i>
AWS::Kinesis::StreamConsumer	arn: <i>partition</i> :kinesis: <i>region:account_ID</i> : <i>stream_ty</i> <i>pe</i> / <i>stream_name</i> /consumer/ <i>consumer_</i> <i>name</i> : <i>consumer_creation_timestamp</i>
AWS::KinesisVideo::Stream	arn: <i>partition</i> :kinesisv ideo: <i>region:account_I</i> <i>D</i> :stream/ <i>stream_name</i> / <i>creation_time</i>

resources.type	resources.ARN
AWS::ManagedBlockchain::Network	arn: <i>partition</i> :managedblockchain ::networks/ <i>network_name</i>
AWS::ManagedBlockchain::Node	arn: <i>partition</i> :managedblockchain : <i>region:account_ID</i> :nodes/ <i>node_ID</i>
AWS::MedicalImaging::Datastore	arn: <i>partition</i> :medical- imaging: <i>region:account_ID</i> :datastor e/ <i>data_store_ID</i>
AWS::NeptuneGraph::Graph	arn: <i>partition</i> :neptune- graph: <i>region:account_I</i> <i>D</i> :graph/ <i>graph_ID</i>
AWS::PCACConnectorAD::Connector	arn: <i>partition</i> :pca-connector- ad: <i>region:account_ID</i> :connecto r/ <i>connector_ID</i>
AWS::QApps:QApp	arn: <i>partition</i> :qapps: <i>region:account_I</i> <i>D</i> :application/ <i>application_UUID</i> / qapp/ <i>qapp_UUID</i>
AWS::QBusiness::Application	arn: <i>partition</i> :qbusines s: <i>region:account_ID</i> :applicat ion/ <i>application_ID</i>
AWS::QBusiness::DataSource	arn: <i>partition</i> :qbusines s: <i>region:account_ID</i> :applicat ion/ <i>application_ID</i> /index/ <i>index_ID</i> / data-source/ <i>datasource_ID</i>



resources.type	resources.ARN
AWS::QBusiness::Index	<pre>arn:partition :qbusines s: region:account_ID :applicat ion/ application_ID /index/index_ID</pre>
AWS::QBusiness::WebExperience	<pre>arn:partition :qbusines s: region:account_ID :applicat ion/ application_ID /web-expe rience/ web_experienc_ID</pre>
AWS::RDS::DBCluster	<pre>arn:partition :rds:region:account_I D :cluster/ cluster_name</pre>
AWS::S3::AccessPoint <sup>3</sup>	<pre>arn:partition :s3:region:account_I D :accesspoint/ access_point_name</pre>
AWS::S3ObjectLambda::AccessPoint	<pre>arn:partition :s3-object-lambda: region:account_ID :accesspo int/ access_point_name</pre>
AWS::S3Outposts::Object	<pre>arn:partition :s3-outpo sts: region:account_ID :object_path</pre>
AWS::SageMaker::Endpoint	<pre>arn:partition :sagemake r: region:account_ID :endpoint / endpoint_name</pre>
AWS::SageMaker::ExperimentTrialComponent	<pre>arn:partition :sagemake r: region:account_ID :experiment- trial-component/ experiment_trial_c omponent_name</pre>

resources.type	resources.ARN
AWS::SageMaker::FeatureGroup	<pre>arn:partition :sagemake r: region:account_ID :feature- group/ feature_group_name</pre>
AWS::SCN::Instance	<pre>arn:partition :scn:region:account_I D :instance/ instance_ID</pre>
AWS::ServiceDiscovery::Namespace	<pre>arn:partition :servicediscovery: region:account_ID :namespac e/ namespace_ID</pre>
AWS::ServiceDiscovery::Service	<pre>arn:partition :servicediscovery: region:account_ID :service/ service_I D</pre>
AWS::SNS::PlatformEndpoint	<pre>arn:partition :sns:region:account_I D :endpoint/ endpoint_type /endpoint_ name /endpoint_ID</pre>
AWS::SNS::Topic	<pre>arn:partition :sns:region:account_I D :topic_name</pre>
AWS::SQS::Queue	<pre>arn:partition :sqs:region:account_I D :queue_name</pre>

resources.type	resources.ARN
AWS::SSM::ManagedNode	<p>Der ARN muss in einem der folgenden Formate vorliegen:</p> <ul style="list-style-type: none"> <li>• <code>arn:partition :ssm:region:account_ID :managed-instance/ instance_ID</code></li> <li>• <code>arn:partition :ec2:region:account_ID :instance / instance_ID</code></li> </ul>
AWS::SSMMessages::ControlChannel	<pre>arn:partition :ssmmessages: region:account_ID :control-channel/ control_channel_ID</pre>
AWS::StepFunctions::StateMachine	<p>Der ARN muss in einem der folgenden Formate vorliegen:</p> <ul style="list-style-type: none"> <li>• <code>arn:partition :states:region:account_ID :stateMachine: stateMachine_name</code></li> <li>• <code>arn:partition :states:region:account_ID :stateMachine: stateMachine_name /label_name</code></li> </ul>
AWS::SWF::Domain	<pre>arn:partition :swf:region:account_ID :domain/ domain_name</pre>
AWS::ThinClient::Device	<pre>arn:partition :thinclient: region:account_ID :device/device_ID</pre>

resources.type	resources.ARN
AWS::ThinClient::Environment	<pre>arn:<i>partition</i> :thinclient: <i>region</i>:<i>account_ID</i> :environment/ <i>environment_ID</i></pre>
AWS::Timestream::Database	<pre>arn:<i>partition</i> :timestream: <i>region</i>:<i>account_ID</i> :database/ <i>database_name</i></pre>
AWS::Timestream::Table	<pre>arn:<i>partition</i> :timestream: <i>region</i>:<i>account_ID</i> :database/ <i>database_name</i> /table/<i>table_name</i></pre>
AWS::VerifiedPermissions::PolicyStore	<pre>arn:<i>partition</i> :verifiedpermissions: <i>region</i>:<i>account_ID</i> :policy-store/ <i>policy_store_ID</i></pre>

<sup>1</sup> Bei Tabellen mit aktivierten Streams enthält das resources-Feld im Datenereignis sowohl AWS::DynamoDB::Stream als auch AWS::DynamoDB::Table. Wenn Sie AWS::DynamoDB::Table als resources.type angeben, werden standardmäßig sowohl DynamoDB-Tabellen- als auch DynamoDB-Stream-Ereignisse protokolliert. Um [Streams-Ereignisse](#) auszuschließen, fügen Sie dem eventName Feld einen Filter hinzu.


<sup>2</sup> Um alle Datenereignisse für alle Objekte in einem bestimmten S3-Bucket zu protokollieren, verwenden Sie den StartsWith-Operator und geben Sie nur die Bucket-ARN als übereinstimmenden Wert an. Der abschließende Schrägstrich ist beabsichtigt; schließen Sie ihn nicht aus.

<sup>3</sup> Um Ereignisse zu allen Objekten in einem S3-Zugangspunkt zu protokollieren, empfehlen wir, nur die Zugangspunkt-ARN zu verwenden, den Objektpfad nicht einzuschließen und die StartsWith- oder NotStartsWith-Operatoren oder zu verwenden.

Weitere Informationen zu den ARN-Formaten von Datenereignisressourcen finden Sie unter [Actions, resources, and condition keys](#) (Aktionen, Ressourcen und Bedingungsschlüssel) im AWS Identity and Access Management -Benutzerhandbuch.

- b. Wählen Sie für jedes Feld + Bedingung aus, um beliebig viele Bedingungen hinzuzufügen, bis zu maximal 500 angegebene Werte für alle Bedingungen. Um beispielsweise Datenereignisse für zwei S3-Buckets von Datenereignissen auszuschließen, die in Ihrem Trail protokolliert werden, können Sie das Feld auf Resources.ARN festlegen, den Operator für beginnt nicht mit festlegen und dann entweder einen S3-Bucket-ARN einfügen oder nach den S3-Buckets suchen, für die Sie keine Ereignisse protokollieren möchten.

Um den zweiten S3-Bucket hinzuzufügen, wählen Sie + Bedingung und wiederholen Sie dann die vorherige Anweisung, indem Sie den ARN für einen anderen Bucket einfügen oder nach einem anderen Bucket suchen.

 Note

Sie können maximal 500 Werte für alle Selektoren auf einem Trail haben. Dies schließt Arrays mit mehreren Werten für einen Selektor wie eventName ein. Wenn Sie einzelne Werte für alle Selektoren haben, können Sie einem Selektor maximal 500 Bedingungen hinzufügen.

Wenn Sie mehr als 15.000 Lambda-Funktionen in Ihrem Konto haben, können Sie beim Erstellen eines Trails nicht alle Funktionen in der CloudTrail Konsole anzeigen oder auswählen. Sie können jedoch alle Funktionen mit einer vordefinierten Selektorvorlage protokollieren, auch wenn sie nicht angezeigt werden. Wenn Sie Datenereignisse für bestimmte Funktionen protokollieren möchten, können Sie eine Funktion manuell hinzufügen, wenn Sie deren ARN kennen. Sie können die Erstellung des Trails auch in der Konsole abschließen und dann den Befehl AWS CLI und den put-event-selectors Befehl verwenden, um die Datenereignisprotokollierung für bestimmte Lambda-Funktionen zu konfigurieren. Weitere Informationen finden Sie unter [Verwaltung von Wanderwegen mit dem AWS CLI](#).

- c. Wählen Sie + Feld, um bei Bedarf zusätzliche Felder hinzuzufügen. Um Fehler zu vermeiden, legen Sie keine widersprüchlichen oder doppelten Werte für Felder fest. Geben Sie beispielsweise nicht an, dass ein ARN in einem Selektor einem Wert entspricht, und

geben Sie dann an, dass der ARN in einem anderen Selektor nicht dem gleichen Wert entspricht.

- Um einen weiteren Datentyp hinzuzufügen, für den Datenereignisse protokolliert werden sollen, wählen Sie Datenereignistyp hinzufügen. Wiederholen Sie die Schritte 3 bis zu diesem Schritt, um erweiterte Ereignisselektoren für den Datenereignistyp zu konfigurieren.
- Wählen Sie unter Insights-Ereignisse die Option Bearbeiten aus, wenn Ihr Trail CloudTrail Insights-Ereignisse protokollieren soll.

Wählen Sie unter Ereignistyp Insights-Ereignisse aus.

Wählen Sie in Insights-Ereignisse API-Aufruftrate und/oder API-Fehlerrate aus. Sie müssen Schreib-Verwaltungsereignisse protokollieren, um Insights-Ereignisse für die API-Aufruftrate zu protokollieren. Sie müssen Lese- und Schreib-Verwaltungsereignisse protokollieren, um Insights-Ereignisse für die API-Fehlerrate zu protokollieren.

CloudTrail Insights analysiert Verwaltungsereignisse auf ungewöhnliche Aktivitäten und protokolliert Ereignisse, wenn Anomalien festgestellt werden. Standardmäßig werden für Trails keine Insights-Ereignisse protokolliert. Weitere Informationen zu Insights-Ereignissen erhalten Sie unter [Protokollieren von Insights-Ereignissen](#). Für die Protokollierung von Insights-Ereignissen fallen zusätzliche Gebühren an. [Preise finden Sie unter CloudTrail AWS CloudTrail Preisgestaltung](#).

Insights-Ereignisse werden in einen anderen Ordner übertragen, /CloudTrail-Insight der nach demselben S3-Bucket benannt ist, der auf der Seite mit den Trail-Details im Bereich Speicherort angegeben ist. CloudTrail erstellt das neue Präfix für Sie. Wenn beispielsweise Ihr aktueller S3-Ziel-Bucket den Namen S3bucketName/AWSLogs/CloudTrail/ hat, lautet der Name mit dem Präfix als Zusatz S3bucketName/AWSLogs/CloudTrail-Insight/.

- Wenn Sie mit dem Ändern der Einstellungen für Ihren Trail fertig sind, wählen Sie Trail aktualisieren.

### Aktualisieren von Datenereigniseinstellungen mit grundlegenden Ereignisauswahlen

Sie können erweiterte Event-Selektoren verwenden, um alle Datenereignistypen zu konfigurieren. Mit erweiterten Ereignisselektoren können Sie detaillierte Selektoren erstellen, um nur die Ereignisse zu protokollieren, die für Sie von Interesse sind.

Wenn Sie grundlegende Event-Selektoren verwenden, um Datenereignisse zu protokollieren, sind Sie darauf beschränkt, Datenereignisse für Amazon S3 S3-Buckets, AWS Lambda Funktionen und

Amazon DynamoDB-Tabellen zu protokollieren. Sie können das eventName Feld nicht mit einfachen Event-Selektoren filtern.

**Data events** [Info](#)  
Data events show information about the resource operations performed on or within a resource. [Additional charges apply](#)

**Basic event selectors are enabled**  
Switch to advanced data event selectors for fine-grained control over the data events captured by your trail. [Switch to advanced event selectors](#)

**Data event: S3** [Info](#) [Remove](#)

**Data event source**  
Select source of data events to log.

S3	▲
S3	✓
Lambda	
DynamoDB	

**Individual bucket selection**  
Choose Browse to select multiple buckets, then choose to log Read, Write or both event types on all selected buckets.

[Browse](#)  Read  Write [×](#)

[Add bucket](#)

[Add data event type](#)


Führen Sie die folgenden Schritte aus, um Datenereigniseinstellungen mithilfe grundlegender Ereignisauswahlen zu konfigurieren.

1. Wählen Sie unter Datenereignisse Bearbeiten aus, um die Einstellungen für die Datenereignisprotokollierung zu ändern. Mit grundlegenden Event-Selektoren können Sie die Protokollierung von Datenereignissen für Amazon S3 S3-Buckets, AWS Lambda Funktionen, DynamoDB-Tabellen oder eine Kombination dieser Ressourcen angeben. Zusätzliche Datenereignistypen werden mit erweiterten Ereignisselektoren unterstützt. Standardmäßig werden Datenereignisse nicht von den Trails protokolliert. Für die Protokollierung von

Datenereignissen fallen zusätzliche Gebühren an. Weitere Informationen finden Sie unter [Datenereignisse](#). Informationen zu CloudTrail-Preisen finden Sie unter [AWS CloudTrail – Preise](#).

Für Amazon-S3-Buckets:

- a. Wählen Sie für Daten-Ereignisquelle S3 aus.
- b. Sie können wählen, ob Sie alle aktuellen und zukünftigen S3 Buckets protokollieren oder einzelne Buckets oder Funktionen angeben möchten. Standardmäßig werden Datenereignisse für alle aktuellen und zukünftigen S3 Buckets protokolliert.

 Note

Wenn Sie die Standardoption Alle aktuellen und future S3-Buckets beibehalten, wird die Datenereignisprotokollierung für alle Buckets aktiviert, die sich derzeit in Ihrem AWS Konto befinden, sowie für alle Buckets, die Sie erstellen, nachdem Sie den Trail erstellt haben. Es ermöglicht auch die Protokollierung der Datenereignisaktivitäten, die von einem beliebigen Benutzer oder einer Rolle in Ihrem AWS Konto ausgeführt werden, selbst wenn diese Aktivität in einem Bucket ausgeführt wird, der zu einem anderen Konto gehört. AWS

Wenn der Trail nur für eine Region gilt, aktiviert die Auswahl von Alle aktuellen und zukünftigen S3 Buckets die Datenereignisprotokollierung für alle Buckets in derselben Region wie Ihr Trail und alle Buckets, die Sie später in dieser Region erstellen. Es werden keine Datenereignisse für Amazon S3 S3-Buckets in anderen Regionen in Ihrem AWS Konto protokolliert.

- c. Wenn Sie die Standardeinstellung Alle aktuellen und zukünftigen S3 Buckets beibehalten, können Sie Leseereignisse, Schreibereignisse oder beides protokollieren.
- d. Um einzelne Buckets auszuwählen, leeren Sie die Kontrollkästchen Lesen und Schreiben für Alle aktuellen und zukünftigen S3 Buckets. Suchen Sie unter Individuelle Bucket-Auswahl nach einem Bucket, in dem Datenereignisse protokolliert werden sollen. Um bestimmte Buckets zu suchen, geben Sie ein Bucket-Präfix für den gewünschten Bucket ein. Sie können in diesem Fenster mehrere Buckets auswählen. Wählen Sie Bucket hinzufügen, um Datenereignisse für weitere Buckets zu protokollieren. Wählen Sie, ob Sie Read (Lesen)-Ereignisse wie GetObject, Write (Schreiben)-Ereignisse wie PutObject oder Ereignisse beider Typen protokolliert werden sollen.

Diese Einstellung hat Vorrang vor individuellen Einstellungen, die Sie für einzelne Buckets konfigurieren. Wenn Sie beispielsweise die Protokollierung von Lese-Ereignissen für



alle S3-Buckets festlegen und dann einen bestimmten Bucket für die Protokollierung von Datenereignissen hinzufügen, ist für den hinzugefügten Bucket bereits Lesen ausgewählt. Sie können die Auswahl nicht löschen. Sie können die Option nur für Write (Schreiben) konfigurieren.

Um einen Bucket aus der Protokollierung zu entfernen, wählen Sie X aus.

2. Um einen weiteren Datentyp hinzuzufügen, für den Datenereignisse protokolliert werden sollen, wählen Sie Datenereignistyp hinzufügen.
3. Für Lambda-Funktionen:
  - a. Wählen Sie für Daten-Ereignisquelle Lambda aus.
  - b. Wählen Sie in der Lambda-Funktion Alle Regionen aus, um alle Lambda-Funktionen zu protokollieren, oder Eingabefunktion als ARN, um Datenereignisse für eine bestimmte Funktion zu protokollieren.


Um Datenereignisse für alle Lambda-Funktionen in Ihrem AWS Konto zu protokollieren, wählen Sie Alle aktuellen und future Funktionen protokollieren aus. Diese Einstellung hat Vorrang vor individuellen Einstellungen, die Sie für einzelne Funktionen vornehmen. Alle Funktionen werden protokolliert, auch wenn nicht alle Funktionen angezeigt werden.

#### Note

Wenn Sie einen Trail für alle Regionen erstellen, aktiviert diese Auswahl die Datenereignisprotokollierung für alle Funktionen, die sich derzeit in Ihrem AWS Konto befinden, sowie für alle Lambda-Funktionen, die Sie möglicherweise in einer beliebigen Region erstellen, nachdem Sie den Trail erstellt haben. Wenn Sie einen Trail für eine einzelne Region erstellen (mithilfe von AWS CLI), aktiviert diese Auswahl die Datenereignisprotokollierung für alle Funktionen, die sich derzeit in dieser Region in Ihrem AWS Konto befinden, sowie für alle Lambda-Funktionen, die Sie möglicherweise in dieser Region erstellen, nachdem Sie den Trail erstellt haben. Es wird keine Datenereignisprotokollierung für Lambda-Funktionen aktiviert, die in anderen Regionen erstellt wurden.

Das Protokollieren von Datenereignissen für alle Funktionen ermöglicht auch die Protokollierung von Datenereignisaktivitäten, die von einem beliebigen Benutzer oder einer Rolle in Ihrem AWS Konto ausgeführt werden, selbst wenn diese Aktivität für eine Funktion ausgeführt wird, die zu einem anderen AWS Konto gehört.

- c. Wenn Sie Eingabefunktion als ARN wählen, geben Sie den ARN einer Lambda-Funktion ein.

 Note

Wenn Sie mehr als 15.000 Lambda-Funktionen in Ihrem Konto haben, können Sie beim Erstellen eines Trails nicht alle Funktionen in der CloudTrail Konsole anzeigen oder auswählen. Sie können weiterhin die Option wählen, alle Funktionen zu protokollieren, auch wenn sie nicht angezeigt werden. Wenn Sie Datenereignisse für bestimmte Funktionen protokollieren möchten, können Sie eine Funktion manuell hinzufügen, wenn Sie deren ARN kennen. Sie können die Erstellung des Trails auch in der Konsole abschließen und dann die AWS CLI und den Befehl `put-event-selectors` verwenden, um die Datenereignisprotokollierung für bestimmte Lambda-Funktionen zu konfigurieren. Für weitere Informationen, siehe [Verwaltung von Wanderwegen mit dem AWS CLI](#).

4. Um einen weiteren Datentyp hinzuzufügen, für den Datenereignisse protokolliert werden sollen, wählen Sie Datenereignistyp hinzufügen.
5. Für DynamoDB-Tabellen:
  - a. Wählen Sie für Daten-Ereignisquelle DynamoDB aus.
  - b. Wählen Sie in der DynamoDB-Tabellenauswahl die Option Durchsuchen, um eine Tabelle auszuwählen, oder fügen Sie den ARN einer DynamoDB-Tabelle ein, auf die Sie Zugriff haben. Ein DynamoDB-Tabellen-ARN hat das folgende Format:

```
arn:partition:dynamodb:region:account_ID:table/table_name
```

Um eine weitere Tabelle hinzuzufügen, wählen Sie Zeile hinzufügen und suchen Sie nach einer Tabelle oder fügen Sie den ARN einer Tabelle ein, auf die Sie Zugriff haben.

6. Um Insights-Ereignisse und andere Einstellungen für Ihren Trail zu konfigurieren, kehren Sie zum vorherigen Verfahren in diesem Thema zurück, [Aktualisieren eines Trails](#).


## Löschen eines Trails

Sie können Trails mit der CloudTrail Konsole löschen. Wenn ein Organisations-Trail über das Verwaltungskonto oder das Konto eines delegierten Administrators einer Organisation gelöscht wird, wird der Trail aus allen Mitgliedskonten der Organisation entfernt.

Wenn Sie CloudTrail Verwaltungsereignisse in Amazon Security Lake aktiviert haben, müssen Sie mindestens einen organisatorischen Pfad verwalten, der mehrere Regionen umfasst `read` und sowohl Verwaltungsereignisse als auch `write` Verwaltungsereignisse protokolliert. Sie können einen Trail nicht löschen, wenn er der einzige Trail ist, den Sie haben, der diese Anforderung erfüllt, es sei denn, Sie deaktivieren CloudTrail Verwaltungsereignisse in Security Lake.

Um einen Trail mit der CloudTrail Konsole zu löschen

1. Melden Sie sich bei der an AWS Management Console und öffnen Sie die CloudTrail Konsole unter <https://console.aws.amazon.com/cloudtrail/>.
2. Öffnen Sie die Trails-Seite der CloudTrail Konsole.
3. Wählen Sie den Trail-Namen aus.
4. Wählen Sie oben auf der Trail-Details-Seite Löschen aus.
5. Wenn Sie zur Bestätigung aufgefordert werden, wählen Sie Löschen, um den Trail dauerhaft zu löschen. Der Trail wird aus der Liste mit den Trails entfernt. Protokolldateien, die bereits für den Amazon-S3-Bucket bereitgestellt wurden, werden nicht gelöscht.

 Note

Inhalte, die an Amazon-S3-Buckets geliefert werden, können Kundeninhalte enthalten. Weitere Informationen zum Entfernen vertraulicher Daten finden Sie unter [Leeren eines Buckets](#) und [Löschen eines Buckets](#) im Amazon S3 S3-Benutzerhandbuch.

## Deaktivieren der Protokollierung für einen Trail

Wenn Sie einen Trail erstellen, ist die Protokollierung automatisch aktiviert. Sie können die Protokollierung für einen Trail deaktivieren.

Wenn Sie die Protokollierung deaktivieren, werden vorhandene Protokolle weiterhin im Amazon-S3-Bucket des Trails gespeichert und es fallen weiterhin S3-Gebühren an.

Um die Protokollierung für einen Trail mit der CloudTrail Konsole auszuschalten

1. Melden Sie sich bei der an AWS Management Console und öffnen Sie die CloudTrail Konsole unter <https://console.aws.amazon.com/cloudtrail/>.
2. Wählen Sie im Navigationsbereich die Option Trails und dann den Namen des Trails aus.

3. Wählen Sie oben auf der Trail-Detail-Seite Protokollierung stoppen, um die Protokollierung für den Trail zu deaktivieren.
4. Wenn Sie zur Bestätigung aufgefordert werden, wählen Sie Protokollierung beenden. CloudTrail beendet die Protokollierung der Aktivitäten für diesen Trail.
5. Um die Protokollierung für diesen Trail fortzusetzen, wählen Sie auf der Trail-Konfigurationsseite die Option Protokollierung starten.

## Trails erstellen, aktualisieren und verwalten mit dem AWS CLI

Sie können die verwenden, AWS CLI um Ihre Trails zu erstellen, zu aktualisieren und zu verwalten. Denken Sie bei der Verwendung von daran AWS CLI, dass Ihre Befehle in der für Ihr Profil konfigurierten AWS Region ausgeführt werden. Wenn Sie die Befehle in einer anderen Region ausführen möchten, ändern Sie entweder die Standardregion für Ihr Profil, oder verwenden Sie den `--region`-Parameter mit dem Befehl.

### Note

Sie benötigen die AWS Befehlszeilentools, um die Befehle AWS Command Line Interface (AWS CLI) in diesem Thema auszuführen. Stellen Sie sicher, dass Sie eine aktuelle Version von AWS CLI installiert haben. Weitere Informationen finden Sie im [AWS Command Line Interface -Benutzerhandbuch](#). Wenn Sie Hilfe zu CloudTrail Befehlen in der AWS CLI Befehlszeile benötigen, geben Sie ein `aws cloudtrail help`.

## Häufig verwendete Befehle für Trail-Erstellung, Verwaltung und Status

Zu den am häufigsten verwendeten Befehlen zum Erstellen und Aktualisieren von Pfaden CloudTrail gehören:

- [create-trail](#) zum Erstellen eines Trails.
- [update-trail](#) zum Ändern der Konfiguration eines vorhandenen Trails.
- [add-tags](#) zum Hinzufügen eines oder mehrerer Tags (Schlüssel-Wert-Paare) zu einem vorhandenen Trail.
- [remove-tags](#) zum Entfernen eines oder mehrerer Tags aus einem Trail.
- [list-tags](#) zur Ausgabe einer Liste der mit dem Trail verbundenen Tags.
- [put-event-selectors](#) zum Hinzufügen oder Ändern von Ereignis auswählen für einen Trail.

- [put-insight-selectors](#) zum Hinzufügen oder Ändern der Insights Ereignisauswahl für einen vorhandenen Trail und zum Aktivieren bzw. Deaktivieren von Insights Ereignissen.
- [start-logging](#) zum Start der Protokollierung von Ereignissen mit Ihrem Trail.
- [stop-logging](#) zum Anhalten der Protokollierung von Ereignissen mit Ihrem Trail.
- [delete-trail](#) zum Löschen eines Trails. Dieser Befehl löscht nicht den Amazon-S3-Bucket, der eventuell die Protokolldateien für den betreffenden Trail enthält.
- [describe-trails](#) um Informationen über Wanderwege in einer AWS Region zurückzugeben.
- [get-trail](#), um Einstellungsinformationen für einen Trail zurückzugeben.
- [get-trail-status](#) zur Ausgabe von Informationen über den aktuellen Status eines Trails.
- [get-event-selectors](#) zur Ausgabe von Informationen zu Ereignis auswählen, die für einen Trail konfiguriert sind.
- [get-insight-selectors](#) zur Ausgabe von Informationen zu Insights-Ereignisauswahlen, die für einen Trail konfiguriert sind.

Unterstützte Befehle für das Erstellen und Aktualisieren von Trails: `create-trail` und `update-trail`

Die Befehle `create-trail` und `update-trail` bieten eine Vielzahl von Funktionen zum Erstellen und Verwalten von Trails, darunter:

- Erstellen eines Trails, der Protokolle über Regionen hinweg empfängt oder einen Trail aktualisiert mit der Option `--is-multi-region-trail`. In den meisten Fällen sollten Sie Trails erstellen, die Ereignisse in allen AWS Regionen protokollieren.
- Mit dieser `--is-organization-trail` Option können Sie einen Trail erstellen, der Protokolle für alle AWS Konten in einer Organisation empfängt.
- Konvertieren eines multiregionalen Trails in einen Trail für eine einzelne Region mit der Option `--no-is-multi-region-trail`.
- Aktivieren oder Deaktivieren der Dateiverschlüsselung mit der Option `--kms-key-id`. Die Option gibt einen AWS KMS Schlüssel an, den Sie bereits erstellt haben und an den Sie eine Richtlinie angehängt haben, mit der CloudTrail Sie Ihre Protokolle verschlüsseln können. Weitere Informationen finden Sie unter [Aktivieren und Deaktivieren der CloudTrail Protokolldateiverschlüsselung mit dem AWS CLI](#).
- Aktivieren oder Deaktivieren der Validierung von Protokolldateien mit den Optionen `--enable-log-file-validation` und `--no-enable-log-file-validation`. Weitere Informationen finden Sie unter [Überprüfen der Integrität der CloudTrail Protokolldatei](#).

- Angabe einer CloudWatch Protokollgruppe und einer Rolle für Logs, sodass Ereignisse an eine CloudWatch Logs-Protokollgruppe übermittelt werden CloudTrail können. Weitere Informationen finden Sie unter [Überwachung von CloudTrail Protokolldateien mit Amazon CloudWatch Logs](#).

Veraltete Befehle: `create-subscription` und `update-subscription`

#### Important

Die Befehle `create-subscription` und `update-subscription` wurden zum Erstellen und Aktualisieren von Trails verwendet, aber sie sind veraltet. Verwenden Sie keinen dieser Befehle. Sie stellen keine vollständige Funktionalität zum Erstellen und Verwalten von Trails bereit.

Wenn Sie Automatisierungen konfiguriert haben, die einen oder beide dieser Befehle verwenden, sollten Sie Ihren Code oder Ihre Scripts so aktualisieren, dass sie unterstützte Befehle wie `create-trail` verwenden.

## Verwendung von „`create-trail`“

Mit dem Befehl `create-trail` können Sie Trails ausführen, die speziell konfiguriert werden, um Ihre geschäftlichen Anforderungen zu erfüllen. Denken Sie bei der Verwendung von `create-trail` mit der AWS CLI, dass Ihre Befehle in der für Ihr Profil konfigurierten AWS Region ausgeführt werden. Wenn Sie die Befehle in einer anderen Region ausführen möchten, ändern Sie entweder die Standardregion für Ihr Profil, oder verwenden Sie den `--region`-Parameter mit dem Befehl.

### Erstellen eines für alle Regionen geltenden Trails

Um einen Trail zu erstellen, der für alle Regionen gilt, verwenden Sie die Option `--is-multi-region-trail`. Standardmäßig erstellt der `create-trail`-Befehl einen Trail, der Ereignisse nur in der AWS -Region protokolliert, in der der Trail erstellt wurde. Um sicherzustellen, dass Sie globale Serviceereignisse protokollieren und alle Aktivitäten von Verwaltungsereignissen in Ihrem AWS Konto erfassen, sollten Sie Trails erstellen, die Ereignisse in allen AWS Regionen protokollieren.

#### Note

Wenn Sie einen Trail erstellen und einen Amazon S3 S3-Bucket angeben, der nicht mit `create-trail` erstellt wurde, müssen Sie die entsprechende Richtlinie anhängen. Siehe [Amazon S3 S3-Bucket-Richtlinie für CloudTrail](#).

Das folgende Beispiel erstellt einen Trail mit dem Namen *my-Trail* und ein Tag mit einem Schlüssel mit dem Namen *Group* (Gruppe) und dem Wert *Marketing*, der Protokolle aus allen Regionen in einem vorhandenen Bucket mit dem Namen *my-bucket* empfängt.

```
aws cloudtrail create-trail --name my-trail --s3-bucket-name my-bucket --is-multi-region-trail --tags-list [key=Group,value=Marketing]
```

Um zu bestätigen, dass Ihr Trail in allen Regionen vorhanden ist, zeigt das Element `IsMultiRegionTrail` in der Ausgabe `true` an.

```
{
  "IncludeGlobalServiceEvents": true,
  "Name": "my-trail",
  "TrailARN": "arn:aws:cloudtrail:us-east-2:123456789012:trail/my-trail",
  "LogFileValidationEnabled": false,
  "IsMultiRegionTrail": true,
  "IsOrganizationTrail": false,
  "S3BucketName": "my-bucket"
}
```

#### Note

Verwenden Sie den Befehl `start-logging`, um die Protokollierung für den Trail zu starten.

### Starten der Protokollierung für den Trail

Nachdem der `create-trail`-Befehl ausgeführt wurde, führen Sie den `start-logging`-Befehl für diesen Trail aus.

#### Note

Wenn Sie mit der CloudTrail Konsole einen Trail erstellen, wird die Protokollierung automatisch aktiviert.

Das folgende Beispiel startet die Protokollierung für einen Trail.

```
aws cloudtrail start-logging --name my-trail
```

Dieser Befehl gibt keine Ausgabe zurück, aber Sie können mit dem `get-trail-status`-Befehl prüfen, ob die Protokollierung gestartet wurde.

```
aws cloudtrail get-trail-status --name my-trail
```

Um zu bestätigen, dass in dem Trail eine Protokollierung erfolgt, zeigt das Element `IsLogging` in der Ausgabe `true` an:

```
{
  "LatestDeliveryTime": 1441139757.497,
  "LatestDeliveryAttemptTime": "2015-09-01T20:35:57Z",
  "LatestNotificationAttemptSucceeded": "2015-09-01T20:35:57Z",
  "LatestDeliveryAttemptSucceeded": "2015-09-01T20:35:57Z",
  "IsLogging": true,
  "TimeLoggingStarted": "2015-09-01T00:54:02Z",
  "StartLoggingTime": 1441068842.76,
  "LatestDigestDeliveryTime": 1441140723.629,
  "LatestNotificationAttemptTime": "2015-09-01T20:35:57Z",
  "TimeLoggingStopped": ""
}
```

## Erstellen eines Trails für eine einzelne Region

Mit dem folgenden Befehl erstellen Sie einen Trail für eine einzelne Region. Der angegebene Amazon S3 S3-Bucket muss bereits vorhanden sein und über die entsprechenden CloudTrail Berechtigungen verfügen. Weitere Informationen finden Sie unter [Amazon S3 S3-Bucket-Richtlinie für CloudTrail](#).

```
aws cloudtrail create-trail --name my-trail --s3-bucket-name my-bucket
```

Weitere Informationen finden Sie unter [Benennungsanforderungen](#).

Es folgt eine Beispielausgabe.

```
{
  "IncludeGlobalServiceEvents": true,
  "Name": "my-trail",
  "TrailARN": "arn:aws:cloudtrail:us-east-2:123456789012:trail/my-trail",
  "LogFileValidationEnabled": false,
  "IsMultiRegionTrail": false,
  "IsOrganizationTrail": false,
}
```



```
"S3BucketName": "my-bucket"  
}
```

Erstellen einer Spur, die für alle Regionen gilt und bei der die Validierung der Protokolldatei aktiviert ist

Um die Validierung von Protokolldateien bei Anwendung von `create-trail` zu aktivieren, verwenden Sie die Option `--enable-log-file-validation`.

Weitere Informationen zur Validierung von Protokolldateien finden Sie unter [Überprüfen der Integrität der CloudTrail Protokolldatei](#).

Im folgenden Beispiel wird ein Trail angelegt, der Protokolle aus allen Regionen in dem angegebenen Bucket bereitstellt. Für den Befehl wird die `--enable-log-file-validation`-Option verwendet.

```
aws cloudtrail create-trail --name my-trail --s3-bucket-name my-bucket --is-multi-region-trail --enable-log-file-validation
```

Um zu bestätigen, dass die Validierung der Protokolldatei aktiviert ist, zeigt das `LogFileValidationEnabled`-Element in der Ausgabe `true` an.

```
{  
  "IncludeGlobalServiceEvents": true,  
  "Name": "my-trail",  
  "TrailARN": "arn:aws:cloudtrail:us-east-2:123456789012:trail/my-trail",  
  "LogFileValidationEnabled": true,  
  "IsMultiRegionTrail": true,  
  "IsOrganizationTrail": false,  
  "S3BucketName": "my-bucket"  
}
```

## Verwenden von `update-trail`

### Important

Am 22. November 2021 wurde die Art und Weise AWS CloudTrail geändert, wie Trails globale Serviceereignisse erfassen. Jetzt AWS STS werden Ereignisse, die von Amazon CloudFront, AWS Identity and Access Management, erstellt und in der Region aufgezeichnet wurden, in der sie erstellt wurden, der Region USA Ost (Nord-Virginia), `us-east-1`. Dadurch wird die Art und Weise, wie diese Dienste CloudTrail behandelt werden, mit der anderer

AWS globaler Dienste konsistent. Um weiterhin globale Service-Events außerhalb von USA Ost (Nord-Virginia) zu erhalten, sollten Sie einzelregionale Trails unter Verwendung globaler Serviceereignisse außerhalb von USA Ost (Nord-Virginia) in multiregionale Trails konvertieren. Weitere Informationen zum Erfassen von globalen Serviceereignissen finden Sie [Aktivieren und Deaktivieren der Protokollierung von globalen Serviceereignissen](#) später in diesem Abschnitt.

Im Gegensatz dazu zeigen der Ereignisverlauf in der CloudTrail Konsole und der `aws cloudtrail lookup-events` Befehl diese Ereignisse dort an, AWS-Region wo sie aufgetreten sind.

Sie können den `update-trail`-Befehl verwenden, um die Konfigurationseinstellungen für einen Trail zu ändern. Sie können auch die `add-tags`- und `remove-tags`-Befehle zum Hinzufügen und Entfernen von Tags für einen Trail verwenden. Sie können nur Trails aus der AWS Region aktualisieren, in der der Trail erstellt wurde (seine Heimatregion). Denken Sie bei der Verwendung von `aws CLI`, dass Ihre Befehle in der für Ihr Profil konfigurierten AWS Region ausgeführt werden. Wenn Sie die Befehle in einer anderen Region ausführen möchten, ändern Sie entweder die Standardregion für Ihr Profil, oder verwenden Sie den `--region`-Parameter mit dem Befehl.

Wenn Sie CloudTrail Verwaltungsereignisse in Amazon Security Lake aktiviert haben, müssen Sie mindestens einen organisatorischen Pfad verwalten, der mehrere Regionen umfasst `read` und sowohl Verwaltungsereignisse als auch `write` Verwaltungsereignisse protokolliert. Sie können einen relevanten Trail nicht so aktualisieren, dass er gegen die Security-Lake-Anforderungen verstößt, beispielsweise, indem Sie den Trail zu einem Trail für einzelne Regionen ändern oder indem Sie die Protokollierung von `read`- oder `write`-Verwaltungsereignissen deaktivieren.

#### Note

Wenn Sie das AWS CLI oder eines der AWS SDKs verwenden, um einen Trail zu ändern, stellen Sie sicher, dass die Bucket-Richtlinie für den Trail gilt. `up-to-date` Damit Ihr Bucket automatisch Ereignisse von einem neuen Bucket empfängt AWS-Region, muss die Richtlinie den vollständigen Servicenamen, `cloudtrail.amazonaws.com` enthalten. Weitere Informationen finden Sie unter [Amazon S3 S3-Bucket-Richtlinie für CloudTrail](#).

## Themen

- [Umwandeln eines Trails, der für eine Region gilt, zu einem Trail für alle Regionen](#)

- [Umwandeln eines multiregionalen Trails in einen Trail für eine einzelne Region](#)
- [Aktivieren und Deaktivieren der Protokollierung von globalen Serviceereignissen](#)
- [Aktivieren der Validierung von Protokolldateien](#)
- [Deaktivieren der Validierung von Protokolldateien](#)

Umwandeln eines Trails, der für eine Region gilt, zu einem Trail für alle Regionen

Um einen vorhandenen Trail so zu ändern, dass er für alle Regionen gilt, verwenden Sie die Option `--is-multi-region-trail`.

```
aws cloudtrail update-trail --name my-trail --is-multi-region-trail
```

Um zu bestätigen, dass der Trail nun für alle Regionen gilt, zeigt das `IsMultiRegionTrail`-Element in der Ausgabe `true` an.

```
{
  "IncludeGlobalServiceEvents": true,
  "Name": "my-trail",
  "TrailARN": "arn:aws:cloudtrail:us-east-2:123456789012:trail/my-trail",
  "LogFileValidationEnabled": false,
  "IsMultiRegionTrail": true,
  "IsOrganizationTrail": false,
  "S3BucketName": "my-bucket"
}
```

Umwandeln eines multiregionalen Trails in einen Trail für eine einzelne Region

Um einen vorhandenen multiregionalen Trail so zu ändern, dass er nur für die Region gilt, in der er erstellt wurde, verwenden Sie die Option `--no-is-multi-region-trail`.

```
aws cloudtrail update-trail --name my-trail --no-is-multi-region-trail
```

Um zu bestätigen, dass der Trail nun für eine einzelne Region gilt, zeigt das `IsMultiRegionTrail`-Element in der Ausgabe `false` an.

```
{
  "IncludeGlobalServiceEvents": true,
  "Name": "my-trail",
```

```
"TrailARN": "arn:aws:cloudtrail:us-east-2:123456789012:trail/my-trail",
"LogFileValidationEnabled": false,
"IsMultiRegionTrail": false,
"IsOrganizationTrail": false,
"S3BucketName": "my-bucket"
}
```

## Aktivieren und Deaktivieren der Protokollierung von globalen Serviceereignissen

Um einen Trail so zu ändern, dass er keine globalen Serviceereignisse protokolliert, verwenden Sie die Option `--no-include-global-service-events`.

```
aws cloudtrail update-trail --name my-trail --no-include-global-service-events
```

Um zu bestätigen, dass der Trail keine globalen Service-Ereignisse mehr protokolliert, zeigt das Element `IncludeGlobalServiceEvents` in der Ausgabe `false` an.

```
{
  "IncludeGlobalServiceEvents": false,
  "Name": "my-trail",
  "TrailARN": "arn:aws:cloudtrail:us-east-2:123456789012:trail/my-trail",
  "LogFileValidationEnabled": false,
  "IsMultiRegionTrail": false,
  "IsOrganizationTrail": false,
  "S3BucketName": "my-bucket"
}
```

Um einen Trail so zu ändern, dass er globale Serviceereignisse protokolliert, verwenden Sie die Option `--include-global-service-events`.

Trails für eine einzelne Region empfangen ab dem 22. November 2021 keine globalen Service-Ereignisse mehr, es sei denn, der Trail erscheint bereits in der Region USA Ost (Nord-Virginia), `us-east-1`. Um globale Service-Ereignisse weiter zu erfassen, aktualisieren Sie die Trail-Konfiguration auf einen multiregionalen Trail. Zum Beispiel aktualisiert dieser Befehl einen Trail für eine einzelne Region in USA Ost (Ohio), `us-east-2`, in einen multiregionalen Trail. Ersetzen Sie `myExistingSingleRegionTrailWithGSE` durch den entsprechenden Trail-Namen für Ihre Konfiguration.

```
aws cloudtrail --region us-east-2 update-trail --
name myExistingSingleRegionTrailWithGSE --is-multi-region-trail
```

Da globale Service-Ereignisse erst ab dem 22. November 2021 in der Region USA Ost (Nord-Virginia) verfügbar sind, können Sie auch einen Trail für eine einzelne Region erstellen, um globale Service-Ereignisse in der Region USA Ost (Nord-Virginia), us-east-1, zu abonnieren. Der folgende Befehl erstellt in us-east-1 einen Single-Region-Trail für Empfang CloudFront, IAM und Ereignisse: AWS STS

```
aws cloudtrail --region us-east-1 create-trail --include-global-service-events --name myTrail --s3-bucket-name DOC-EXAMPLE-BUCKET
```

### Aktivieren der Validierung von Protokolldateien

Um die Validierung von Protokolldateien für einen Trail zu aktivieren, verwenden Sie die `--enable-log-file-validation`-Option (Validierung von Protokolldateien aktivieren). Die Digest-Dateien für diesen Pfad werden im Amazon-S3-Bucket bereitgestellt.

```
aws cloudtrail update-trail --name my-trail --enable-log-file-validation
```

Um zu bestätigen, dass die Validierung der Protokolldatei aktiviert ist, zeigt das `LogFileValidationEnabled`-Element in der Ausgabe `true` an.

```
{
  "IncludeGlobalServiceEvents": true,
  "Name": "my-trail",
  "TrailARN": "arn:aws:cloudtrail:us-east-2:123456789012:trail/my-trail",
  "LogFileValidationEnabled": true,
  "IsMultiRegionTrail": false,
  "IsOrganizationTrail": false,
  "S3BucketName": "my-bucket"
}
```

### Deaktivieren der Validierung von Protokolldateien

Um die Validierung von Protokolldateien für einen Trail zu deaktivieren, verwenden Sie die `--no-enable-log-file-validation`-Option.

```
aws cloudtrail update-trail --name my-trail-name --no-enable-log-file-validation
```

Um zu bestätigen, dass die Validierung der Protokolldatei deaktiviert ist, zeigt das `LogFileValidationEnabled`-Element in der Ausgabe `false` an.

```
{
  "IncludeGlobalServiceEvents": true,
  "Name": "my-trail",
  "TrailARN": "arn:aws:cloudtrail:us-east-2:123456789012:trail/my-trail",
  "LogFileValidationEnabled": false,
  "IsMultiRegionTrail": false,
  "IsOrganizationTrail": false,
  "S3BucketName": "my-bucket"
}
```

Informationen zur Validierung von Protokolldateien mit dem finden Sie unter. [AWS CLI Überprüfen der Integrität der CloudTrail Protokolldatei mit dem AWS CLI](#)

## Verwaltung von Wanderwegen mit dem AWS CLI

Das AWS CLI beinhaltet mehrere andere Befehle, die dir helfen, deine Trails zu verwalten. Diese Befehle fügen Tags zu Trails hinzu, rufen den Trail-Status ab, starten und stoppen die Protokollierung für Trails und löschen Trails. Sie müssen diese Befehle in derselben AWS Region ausführen, in der der Trail erstellt wurde (in der Heimatregion). Denken Sie bei der Verwendung von daran AWS CLI, dass Ihre Befehle in der AWS Region ausgeführt werden, die für Ihr Profil konfiguriert ist. Wenn Sie die Befehle in einer anderen Region ausführen möchten, ändern Sie entweder die Standardregion für Ihr Profil, oder verwenden Sie den `--region`-Parameter mit dem Befehl.

### Themen

- [Hinzufügen eines oder mehrerer Tags zu einem Trail](#)
- [Auflisten von Tags für einen oder mehrere Trails](#)
- [Entfernen eines oder mehrerer Tags aus einem Trail](#)
- [Abruf von Trail-Einstellungen und des Status eines Trails](#)
- [Konfiguration von CloudTrail Insights-Ereignisselektoren](#)
- [Konfigurieren von Ereignisauswahlen](#)
- [Konfigurieren von fortschrittlichen Ereignisauswahlen](#)
- [Anhalten und Starten der Protokollierung für einen Trail](#)
- [Löschen eines Trails](#)

### Hinzufügen eines oder mehrerer Tags zu einem Trail

Führen Sie zum Hinzufügen eines oder mehrerer Tags zu einem Trail den Befehl `add-tags` aus.

Im folgenden Beispiel wird einem Tag mit dem Namen *Besitzer* und dem Wert *Mary* zu einem Trail mit dem ARN `arn:aws:cloudtrail:us-east-2:123456789012:trail/my-trail` in der Region USA Ost (Ohio) hinzugefügt.

```
aws cloudtrail add-tags --resource-id arn:aws:cloudtrail:us-east-2:123456789012:trail/my-trail --tags-list Key=Owner,Value=Mary --region us-east-2
```

Bei erfolgreicher Ausführung gibt dieser Befehl nichts zurück.

### Auflisten von Tags für einen oder mehrere Trails

Verwenden Sie zur Anzeige der mit einem oder mehreren vorhandenen Trails verbundenen Tags den `list-tags`-Befehl.

Das folgende Beispiel listet die Tags für *Trail1* und *Trail2* auf.

```
aws cloudtrail list-tags --resource-id-list arn:aws:cloudtrail:us-east-2:123456789012:trail/Trail1 arn:aws:cloudtrail:us-east-2:123456789012:trail/Trail2
```

Ist der Befehl erfolgreich, wird eine Ausgabe zurückgegeben, die wie folgt aussehen sollte.

```
{
  "ResourceTagList": [
    {
      "ResourceId": "arn:aws:cloudtrail:us-east-2:123456789012:trail/Trail1",
      "TagsList": [
        {
          "Value": "Alice",
          "Key": "Name"
        },
        {
          "Value": "Ohio",
          "Key": "Location"
        }
      ]
    },
    {
      "ResourceId": "arn:aws:cloudtrail:us-east-2:123456789012:trail/Trail2",
      "TagsList": [
        {
          "Value": "Bob",
```

```
        "Key": "Name"
      }
    ]
  }
}
```

## Entfernen eines oder mehrerer Tags aus einem Trail

Führen Sie zum Entfernen eines oder mehrerer Tags aus einem vorhandenen Trail den Befehl `remove-tags` aus.

Im folgenden Beispiel werden Tags mit den Namen *Location* und *Name* aus einem Trail mit dem ARN `arn:aws:cloudtrail:us-east-2:123456789012:trail/Trail1` in der Region USA Ost (Ohio) entfernt.

```
aws cloudtrail remove-tags --resource-id arn:aws:cloudtrail:us-
east-2:123456789012:trail/Trail1 --tags-list Key=Name Key=Location --region us-east-2
```

Bei erfolgreicher Ausführung gibt dieser Befehl nichts zurück.

## Abruf von Trail-Einstellungen und des Status eines Trails

Führen Sie den `describe-trails` Befehl aus, um Informationen über Wanderwege in einer AWS Region abzurufen. Das folgende Beispiel gibt Informationen zu in der Region USA Ost (Ohio) konfigurierten Trails aus.

```
aws cloudtrail describe-trails --region us-east-2
```

Wird der Befehl erfolgreich ausgeführt, wird Ihnen eine Ausgabe ähnlich der folgenden angezeigt.

```
{
  "trailList": [
    {
      "Name": "my-trail",
      "S3BucketName": "my-bucket",
      "S3KeyPrefix": "my-prefix",
      "IncludeGlobalServiceEvents": true,
      "IsMultiRegionTrail": true,
      "HomeRegion": "us-east-2"
      "TrailARN": "arn:aws:cloudtrail:us-east-2:123456789012:trail/my-trail",
    }
  ]
}
```



```
    "LogFileValidationEnabled": false,
    "HasCustomEventSelectors": false,
    "SnsTopicName": "my-topic",
    "IsOrganizationTrail": false,
  },
  {
    "Name": "my-special-trail",
    "S3BucketName": "another-bucket",
    "S3KeyPrefix": "example-prefix",
    "IncludeGlobalServiceEvents": false,
    "IsMultiRegionTrail": false,
    "HomeRegion": "us-east-2",
    "TrailARN": "arn:aws:cloudtrail:us-east-2:123456789012:trail/my-special-trail",
    "LogFileValidationEnabled": false,
    "HasCustomEventSelectors": true,
    "IsOrganizationTrail": false
  },
  {
    "Name": "my-org-trail",
    "S3BucketName": "my-bucket",
    "S3KeyPrefix": "my-prefix",
    "IncludeGlobalServiceEvents": true,
    "IsMultiRegionTrail": true,
    "HomeRegion": "us-east-1"
    "TrailARN": "arn:aws:cloudtrail:us-east-2:123456789012:trail/my-org-trail",
    "LogFileValidationEnabled": false,
    "HasCustomEventSelectors": false,
    "SnsTopicName": "my-topic",
    "IsOrganizationTrail": true
  }
]
}
```

Rufen Sie mit dem Befehl `get-trail` Einstellungsinformationen zu einem bestimmten Trail ab. Im folgenden Beispiel werden Einstellungsinformationen für einen Trail namens `my-trail` zurückgegeben.

```
aws cloudtrail get-trail - -name my-trail
```

Ist der Befehl erfolgreich, wird eine Ausgabe zurückgegeben, die wie folgt aussehen sollte.

```
{
```

```
"Trail": {
  "Name": "my-trail",
  "S3BucketName": "my-bucket",
  "S3KeyPrefix": "my-prefix",
  "IncludeGlobalServiceEvents": true,
  "IsMultiRegionTrail": true,
  "HomeRegion": "us-east-2"
  "TrailARN": "arn:aws:cloudtrail:us-east-2:123456789012:trail/my-trail",
  "LogFileValidationEnabled": false,
  "HasCustomEventSelectors": false,
  "SnsTopicName": "my-topic",
  "IsOrganizationTrail": false,
}
```

Führen Sie den Befehl `get-trail-status` aus, um den Status eines Trails abzurufen. Sie müssen diesen Befehl entweder von der AWS Region aus ausführen, in der er erstellt wurde (der Heimatregion), oder Sie müssen diese Region angeben, indem Sie den `--region` Parameter hinzufügen.

#### Note

Wenn es sich bei dem Trail um einen Organisations-Trail handelt und Sie ein Mitgliedskonto in der Organisation sind AWS Organizations, müssen Sie den vollständigen ARN dieses Trails angeben und nicht nur den Namen.

```
aws cloudtrail get-trail-status --name my-trail
```

Wird der Befehl erfolgreich ausgeführt, wird Ihnen eine Ausgabe ähnlich der folgenden angezeigt.

```
{
  "LatestDeliveryTime": 1441139757.497,
  "LatestDeliveryAttemptTime": "2015-09-01T20:35:57Z",
  "LatestNotificationAttemptSucceeded": "2015-09-01T20:35:57Z",
  "LatestDeliveryAttemptSucceeded": "2015-09-01T20:35:57Z",
  "IsLogging": true,
  "TimeLoggingStarted": "2015-09-01T00:54:02Z",
  "StartLoggingTime": 1441068842.76,
  "LatestDigestDeliveryTime": 1441140723.629,
  "LatestNotificationAttemptTime": "2015-09-01T20:35:57Z",
```

```
"TimeLoggingStopped": ""  
}
```

Neben den im vorherigen JSON-Code gezeigten Feldern, enthält der Status bei Vorliegen von Amazon-SNS- oder Amazon-S3-Fehlern die folgenden Felder:

- `LatestNotificationError`. Enthält den von Amazon SNS ausgegebenen Fehler, falls das Abonnieren eines Themas fehlgeschlagen ist.
- `LatestDeliveryError`. Enthält den von Amazon S3 ausgegebenen Fehler, wenn CloudTrail keine Protokolldatei an einen Bucket gesendet werden kann.

### Konfiguration von CloudTrail Insights-Ereignisselektoren

Aktivieren Sie Insights-Ereignisse für einen Trail, indem Sie den Befehl `put-insight-selectors` ausführen und `ApiCallRateInsight` und/oder `ApiErrorRateInsight` als Wert des Attributs `InsightType` angeben. Um für einen Trail die Einstellungen zur Insights-Auswahl anzuzeigen, führen Sie den Befehl `get-insight-selectors` aus. Sie müssen diesen Befehl entweder von der AWS Region aus ausführen, in der der Trail erstellt wurde (der Heimatregion), oder Sie müssen diese Region angeben, indem Sie dem Befehl den `--region` Parameter hinzufügen.

#### Note

Um Insights-Ereignisse für `ApiCallRateInsight` zu protokollieren, muss der Trail `write`-Verwaltungsereignisse protokollieren. Um Insights-Ereignisse für `ApiErrorRateInsight` zu protokollieren, muss der Trail `read`- oder `write`-Verwaltungsereignisse protokollieren.

### Beispiel-Trail zum Protokollieren von Insights-Ereignissen

Im folgenden Beispiel wird `put-insight-selectors` ein Insights-Ereignisselektor für einen Trail mit dem Namen `TrailName3` erstellt. Dadurch wird die Erfassung von Insights-Ereignissen für den Trail `TrailName3` aktiviert. Die Insights-Ereignisauswahl protokolliert sowohl `ApiErrorRateInsight`- als auch `ApiCallRateInsight`-Insights-Ereignistypen.

```
aws cloudtrail put-insight-selectors --trail-name TrailName3 --insight-selectors  
'[{"InsightType": "ApiCallRateInsight"}, {"InsightType": "ApiErrorRateInsight"}]'
```

Im Beispiel wird die Insights-Ereignisauswahl zurückgegeben, die für den Trail konfiguriert wurde.

```
{
  "InsightSelectors":
    [
      {
        "InsightType": "ApiErrorRateInsight"
      },
      {
        "InsightType": "ApiCallRateInsight"
      }
    ],
  "TrailARN": "arn:aws:cloudtrail:us-east-2:123456789012:trail/TrailName3"
}
```

### Beispiel: Sammlung von Insights-Ereignissen deaktivieren

Im folgenden Beispiel wird `put-insight-selectors` die Insights-Ereignisauswahl für einen Trail mit dem Namen *TrailName3* entfernt. *Durch das Löschen der JSON-Zeichenfolge der Insights-Selektoren wird die Insights-Ereigniserfassung für den TrailName3-Trail deaktiviert.*

```
aws cloudtrail put-insight-selectors --trail-name TrailName3 --insight-selectors '[]'
```

Im Beispiel wird die jetzt leere Insights-Ereignisauswahl zurückgegeben, die für den Trail konfiguriert wurde.

```
{
  "InsightSelectors": [ ],
  "TrailARN": "arn:aws:cloudtrail:us-east-2:123456789012:trail/TrailName3"
}
```

### Konfigurieren von Ereignisauswahlen

Um für einen Trail die Einstellungen zu den Ereignisauswahlen anzuzeigen, führen Sie den `get-event-selectors`-Befehl aus. Sie müssen diesen Befehl entweder von der AWS Region aus ausführen, in der er erstellt wurde (der Heimatregion), oder Sie müssen diese Region mithilfe des `--region` Parameters angeben.

```
aws cloudtrail get-event-selectors --trail-name TrailName
```

**Note**

Wenn es sich bei dem Trail um einen Organisations-Trail handelt und Sie ein Mitgliedskonto in der Organisation sind AWS Organizations, müssen Sie den vollständigen ARN dieses Trails angeben und nicht nur den Namen.

In dem folgenden Beispiel werden die Standardeinstellungen für eine Ereignisauswahl zu einem Trail zurückgegeben.

```
{
  "EventSelectors": [
    {
      "ExcludeManagementEventSources": [],
      "IncludeManagementEvents": true,
      "DataResources": [],
      "ReadWriteType": "All"
    }
  ],
  "TrailARN": "arn:aws:cloudtrail:us-east-2:123456789012:trail/TrailName"
}
```

Um eine Ereignisauswahl zu erstellen, führen Sie den Befehl `put-event-selectors` aus. Wenn Sie mit dem Trail Insights-Ereignisse protokollieren möchten, stellen Sie sicher, dass die Ereignisauswahl die Protokollierung der Insights-Typen aktiviert, für die Sie Ihren Trail konfigurieren möchten. Weitere Informationen zum Protokollieren von Insights-Ereignissen finden Sie unter [Protokollieren von Insights-Ereignissen](#).

Wenn in Ihrem Konto ein Ereignis eintritt, CloudTrail bewertet es die Konfiguration für Ihre Trails. Entspricht das Ereignis einer für den Trail festgelegten Ereignisauswahl, verarbeitet und protokolliert der Trail das Ereignis. Sie können bis zu 5 Ereignisauswahlen und bis zu 250 Datenressourcen für einen Trail konfigurieren. Weitere Informationen finden Sie unter [Protokollieren von Datenereignissen](#).

## Themen

- [Beispiel-Trail mit bestimmten Ereignisauswahlen](#)
- [Beispiel-Trail, für den alle Verwaltungs- und Datenereignisse protokolliert werden](#)
- [Beispiel für einen Trail, der keine Ereignisse protokolliert AWS Key Management Service](#)
- [Beispielpfad, der relevante Ereignisse mit geringem Volumen AWS Key Management Service protokolliert](#)

- [Beispiel-Trail, für den keine Amazon-RDS-Daten-API-Ereignisse protokolliert werden](#)

## Beispiel-Trail mit bestimmten Ereignisauswahlen

Das folgende Beispiel erstellt einen Event-Selector für einen Trail, der so benannt ist, *TrailName* dass er Verwaltungsereignisse mit Schreibschutz und Schreibschutz, Datenereignisse für zwei Amazon S3 S3-Bucket/Präfix-Kombinationen und Datenereignisse für eine einzelne Funktion mit dem Namen umfasst. AWS Lambda *hello-world-python-function*

```
aws cloudtrail put-event-selectors --trail-name TrailName --event-selectors
' [{"ReadWriteType": "All", "IncludeManagementEvents": true, "DataResources":
  [{"Type": "AWS::S3::Object", "Values": ["arn:aws:s3:::mybucket/
prefix", "arn:aws:s3:::mybucket2/prefix2"]}, {"Type": "AWS::Lambda::Function", "Values":
  ["arn:aws:lambda:us-west-2:999999999999:function:hello-world-python-function"]} ] ]'
```

Das Beispiel gibt die für den Trail konfigurierte Ereignisauswahl zurück.

```
{
  "EventSelectors": [
    {
      "ExcludeManagementEventSources": [],
      "IncludeManagementEvents": true,
      "DataResources": [
        {
          "Values": [
            "arn:aws:s3:::mybucket/prefix",
            "arn:aws:s3:::mybucket2/prefix2"
          ],
          "Type": "AWS::S3::Object"
        },
        {
          "Values": [
            "arn:aws:lambda:us-west-2:123456789012:function:hello-world-
python-function"
          ],
          "Type": "AWS::Lambda::Function"
        }
      ],
      "ReadWriteType": "All"
    }
  ],
  "TrailARN": "arn:aws:cloudtrail:us-east-2:123456789012:trail/TrailName"
}
```

```
}

```

Beispiel-Trail, für den alle Verwaltungs- und Datenereignisse protokolliert werden

Das folgende Beispiel erstellt einen Event-Selector für einen Trail mit dem Namen *TrailName2*, der alle Ereignisse, einschließlich Verwaltungsereignisse mit Schreibschutz und Schreibschutz, und alle Datenereignisse für alle Amazon S3 S3-Buckets, AWS Lambda Funktionen und Amazon DynamoDB-Tabellen im Konto umfasst. AWS Da dieses Beispiel grundlegende Event-Selektoren verwendet, kann es nicht die Protokollierung für S3-Ereignisse AWS Outposts, Amazon Managed Blockchain JSON-RPC-Aufrufe auf Ethereum-Knoten oder andere erweiterte Event-Selector-Ressourcentypen konfigurieren. Sie müssen erweiterte Ereigniserektoren verwenden, um Datenereignisse für diese Ressourcen zu protokollieren. Weitere Informationen finden Sie unter [Konfigurieren von fortschrittlichen Ereignisauswahlen](#).

#### Note

Wenn der Trail nur für eine Region gilt, werden nur Ereignisse in dieser Region protokolliert, auch wenn die Ereignisauswahlparameter alle Amazon-S3-Buckets und Lambda-Funktionen angeben. Ereignisauswahlen gelten nur für die Regionen, in denen der Trail erstellt wurde.

```
aws cloudtrail put-event-selectors --trail-name TrailName2 --event-selectors
' [{"ReadWriteType": "All", "IncludeManagementEvents": true, "DataResources":
[ {"Type": "AWS::S3::Object", "Values": ["arn:aws:s3:::"]}, {"Type":
"AWS::Lambda::Function", "Values": ["arn:aws:lambda"]}, {"Type":
"AWS::DynamoDB::Table", "Values": ["arn:aws:dynamodb"]} ] } ]'
```

Das Beispiel gibt die für den Trail konfigurierten Ereignisauswahlen zurück.

```
{
  "EventSelectors": [
    {
      "ExcludeManagementEventSources": [],
      "IncludeManagementEvents": true,
      "DataResources": [
        {
          "Values": [
            "arn:aws:s3:::"
          ],
        },
      ],
    },
  ],
}
```

```

        "Type": "AWS::S3::Object"
    },
    {
        "Values": [
            "arn:aws:lambda"
        ],
        "Type": "AWS::Lambda::Function"
    },
    {
        "Values": [
            "arn:aws:dynamodb"
        ],
        "Type": "AWS::DynamoDB::Table"
    }
],
"ReadWriteType": "All"
}
],
"TrailARN": "arn:aws:cloudtrail:us-east-2:123456789012:trail/TrailName2"
}

```

### Beispiel für einen Trail, der keine Ereignisse protokolliert AWS Key Management Service

Im folgenden Beispiel wird eine Ereignisauswahl für einen Trail erstellt, der so benannt ist *TrailName*, dass er Verwaltungsereignisse mit Schreibschutz und Lesezugriff, aber Ereignisse () ausschließt. AWS Key Management Service AWS KMS Da AWS KMS Ereignisse als Verwaltungsereignisse behandelt werden und es eine große Anzahl von Ereignissen geben kann, können sie erhebliche Auswirkungen auf Ihre CloudTrail Rechnung haben, wenn Sie mehr als einen Trail haben, der Verwaltungsereignisse erfasst. Der Benutzer in diesem Beispiel hat sich entschieden, AWS KMS -Ereignisse für jeden Trail – bis auf einen – auszuschließen. Fügen Sie Ihren Ereignisauswahlen zum Ausschließen einer Ereignisquelle das Element `ExcludeManagementEventSources` hinzu und geben Sie im Zeichenfolgenwert eine Ereignisquelle an.

Wenn Sie sich dafür entscheiden, Verwaltungsereignisse nicht zu protokollieren, werden AWS KMS Ereignisse nicht protokolliert, und Sie können die Einstellungen für die AWS KMS Ereignisprotokollierung nicht ändern.

Um wieder mit der Protokollierung von AWS KMS Ereignissen in einem Trail zu beginnen, übergeben Sie ein leeres Array als Wert von `ExcludeManagementEventSources`.



```
aws cloudtrail put-event-selectors --trail-name TrailName --event-selectors '[{"ReadWriteType": "All", "ExcludeManagementEventSources": ["kms.amazonaws.com"], "IncludeManagementEvents": true}]'
```

Im Beispiel wird die Ereignisauswahl zurückgegeben, die für den Trail konfiguriert ist.

```
{
  "EventSelectors": [
    {
      "ExcludeManagementEventSources": [ "kms.amazonaws.com" ],
      "IncludeManagementEvents": true,
      "DataResources": [],
      "ReadWriteType": "All"
    }
  ],
  "TrailARN": "arn:aws:cloudtrail:us-east-2:123456789012:trail/TrailName"
}
```

Um wieder mit der Protokollierung von AWS KMS Ereignissen in einem Trail zu beginnen, übergeben Sie ein leeres Array als Wert von `ExcludeManagementEventSources`, wie im folgenden Befehl gezeigt.

```
aws cloudtrail put-event-selectors --trail-name TrailName --event-selectors '[{"ReadWriteType": "All", "ExcludeManagementEventSources": [], "IncludeManagementEvents": true}]'
```

Beispielpfad, der relevante Ereignisse mit geringem Volumen AWS Key Management Service protokolliert

Im folgenden Beispiel wird eine Ereignisauswahl für einen Trail erstellt, der so benannt ist, dass er Verwaltungsereignisse und Ereignisse enthält *TrailName*, die nur Schreibzugriff haben. AWS KMS Da AWS KMS Ereignisse als Verwaltungsereignisse behandelt werden und es eine große Anzahl von Ereignissen geben kann, können sie erhebliche Auswirkungen auf Ihre CloudTrail Rechnung haben, wenn Sie mehr als einen Trail haben, der Verwaltungsereignisse erfasst. Der Benutzer in diesem Beispiel hat sich dafür entschieden, AWS KMS Write-Ereignisse einzubeziehen `Disable`, zu denen auch `Delete` und `GenerateDataKey` gehören, aber nicht mehr umfangreiche Aktionen wie `Encrypt`, `Decrypt`, und `GenerateDataKey` (diese werden jetzt als Lese-Ereignisse behandelt).

```
aws cloudtrail put-event-selectors --trail-name TrailName --event-selectors '[{"ReadWriteType": "WriteOnly", "ExcludeManagementEventSources": [], "IncludeManagementEvents": true}]'
```

Im Beispiel wird die Ereignisauswahl zurückgegeben, die für den Trail konfiguriert ist. Dadurch werden Verwaltungsereignisse, einschließlich Ereignisse, nur für Schreibvorgänge protokolliert. AWS KMS

```
{
  "EventSelectors": [
    {
      "ExcludeManagementEventSources": [],
      "IncludeManagementEvents": true,
      "DataResources": [],
      "ReadWriteType": "WriteOnly"
    }
  ],
  "TrailARN": "arn:aws:cloudtrail:us-east-2:123456789012:trail/TrailName"
}
```

Beispiel-Trail, für den keine Amazon-RDS-Daten-API-Ereignisse protokolliert werden

Das folgende Beispiel erstellt einen Event-Selector für einen Trail, der so benannt ist *TrailName*, dass er Verwaltungsereignisse mit Schreibschutz und Schreibschutz enthält, aber Amazon RDS Data API-Ereignisse ausschließt. Da Amazon RDS Data API-Ereignisse als Verwaltungsereignisse behandelt werden und es eine große Anzahl von Ereignissen geben kann, können sie erhebliche Auswirkungen auf Ihre CloudTrail Rechnung haben, wenn Sie mehr als einen Trail haben, der Verwaltungsereignisse erfasst. Der Benutzer in diesem Beispiel hat sich entschieden, Amazon-RDS-Daten-API-Ereignisse für jeden Trail – bis auf einen – auszuschließen. Fügen Sie Ihren Ereignisauswahlen zum Ausschließen einer Ereignisquelle das Element `ExcludeManagementEventSources` hinzu und geben Sie im Zeichenfolgenwert eine Amazon-RDS-Daten-API-Ereignisquelle an: `rdodata.amazonaws.com`.

Wenn Sie Verwaltungsereignisse nicht protokollieren möchten, werden Amazon-RDS-Daten-API-Ereignisse nicht protokolliert und Sie können die Einstellungen für die Ereignisprotokollierung nicht ändern.

Um wieder mit der Protokollierung von Amazon RDS Data API-Verwaltungsereignissen in einem Trail zu beginnen, übergeben Sie ein leeres Array als Wert von `ExcludeManagementEventSources`.

```
aws cloudtrail put-event-selectors --trail-name TrailName --event-selectors '[{"ReadWriteType": "All","ExcludeManagementEventSources":["rdsdata.amazonaws.com"],"IncludeManagementEvents": true}]'
```

Im Beispiel wird die Ereignisauswahl zurückgegeben, die für den Trail konfiguriert ist.

```
{
  "EventSelectors": [
    {
      "ExcludeManagementEventSources": [ "rdsdata.amazonaws.com" ],
      "IncludeManagementEvents": true,
      "DataResources": [],
      "ReadWriteType": "All"
    }
  ],
  "TrailARN": "arn:aws:cloudtrail:us-east-2:123456789012:trail/TrailName"
}
```

Um wieder mit der Protokollierung von Amazon RDS Data API-Verwaltungsereignissen in einem Trail zu beginnen, übergeben Sie ein leeres Array als Wert von `ExcludeManagementEventSources`, wie im folgenden Befehl gezeigt.

```
aws cloudtrail put-event-selectors --trail-name TrailName --event-selectors '[{"ReadWriteType": "All","ExcludeManagementEventSources": [],"IncludeManagementEvents": true}]'
```

## Konfigurieren von fortschrittlichen Ereignisauswahlen

Wenn Sie erweiterte Ereignisselektoren anstelle von einfachen Ereignisselektoren verwenden möchten, um Datenereignisse einzuschließen oder auszuschließen, verwenden Sie erweiterte Ereignisselektoren auf der Detailseite eines Trails. Mit erweiterten Ereignisselektoren können Sie Datenereignisse für mehr Ressourcentypen protokollieren als mit einfachen Ereignisselektoren. Grundlegende Selektoren protokollieren S3-Objektaktivitäten, Aktivitäten der AWS Lambda - Funktionsausführung und DynamoDB-Tabellen.

Erstellen Sie in Advanced Event Selectors einen Ausdruck, um Datenereignisse für bestimmte Ressourcentypen wie S3-Buckets, AWS Lambda Funktionen, DynamoDB-Tabellen, S3 Object Lambda-Zugriffspunkte, direkte Amazon EBS-APIs auf EBS-Snapshots, S3-Zugriffspunkte, DynamoDB-Streams, von Lake Formation erstellte Tabellen und mehr zu sammeln. AWS Glue

Weitere Informationen zu erweiterten Ereignisselectoren finden Sie unter [Konfigurieren von fortschrittlichen Ereignisauswahlen](#).

Um für einen Trail die Einstellungen zu den fortschrittlichen Ereignisauswahlen anzuzeigen, führen Sie den Befehl `get-event-selectors` aus. Sie müssen diesen Befehl entweder von der AWS Region aus ausführen, in der der Trail erstellt wurde (der Heimatregion), oder Sie müssen diese Region angeben, indem Sie den `--region` Parameter hinzufügen.

```
aws cloudtrail get-event-selectors --trail-name TrailName
```

#### Note

Wenn es sich bei dem Trail um einen Organisationspfad handelt und Sie mit einem Mitgliedskonto in der Organisation angemeldet sind AWS Organizations, müssen Sie den vollständigen ARN des Trails angeben und nicht nur den Namen.

Das folgende Beispiel gibt die Standardeinstellungen für erweiterte Ereignisselectoren für einen Trail zurück. Standardmäßig sind keine erweiterten Ereignisauswahlen für einen Trail konfiguriert.

```
{
  "AdvancedEventSelectors": [],
  "TrailARN": "arn:aws:cloudtrail:us-east-2:123456789012:trail/TrailName"
}
```

Um eine fortschrittliche Ereignisauswahl zu erstellen, führen Sie den Befehl `put-event-selectors` aus. Wenn in Ihrem Konto ein Datenereignis auftritt, wird die Konfiguration für Ihre Trails CloudTrail ausgewertet. Entspricht das Ereignis einer für den Trail festgelegten fortschrittlichen Ereignisauswahl, verarbeitet und protokolliert der Trail das Ereignis. Sie können bis zu 500 Bedingungen auf einem Trail konfigurieren, einschließlich aller Werte, die für alle erweiterten Ereignisselectoren auf Ihrem Trail angegeben sind. Weitere Informationen finden Sie unter [Protokollieren von Datenereignissen](#).

## Themen

- [Beispiel-Trail mit bestimmten fortschrittlichen Ereignisauswahlen](#)
- [Beispiel-Trail, der benutzerdefinierte erweiterte Event-Selektoren verwendet, um AWS Outposts Datenereignisse in Amazon S3 zu protokollieren](#)
- [Beispielpfad, der erweiterte Event-Selektoren verwendet, um Ereignisse auszuschließen AWS Key Management Service](#)

- [Beispielpfad, der erweiterte Event-Selektoren verwendet, um Amazon RDS Data API-Verwaltungsereignisse auszuschließen](#)

## Beispiel-Trail mit bestimmten fortschrittlichen Ereignisauswahlen

Das folgende Beispiel erstellt benutzerdefinierte erweiterte Event-Selektoren für einen Trail, der so benannt ist, *TrailName* dass er Lese- und Schreibverwaltungsereignisse (durch Weglassen des `readOnly` Selektors) `PutObject` und `DeleteObject` Datenereignisse für alle Amazon S3 S3-Bucket/Präfix-Kombinationen mit Ausnahme eines Buckets mit dem Namen `sample_bucket_name` und Datenereignisse für eine Funktion mit dem Namen enthält. `AWS Lambda MyLambdaFunction` Da es sich um benutzerdefinierte erweiterte Ereignisselektoren handelt, hat jeder Satz von Selektoren einen beschreibenden Namen. Beachten Sie, dass ein abschließender Schrägstrich Teil des ARN-Werts für S3 Buckets ist.

```
aws cloudtrail put-event-selectors --trail-name TrailName --advanced-event-selectors
'[
  {
    "Name": "Log readOnly and writeOnly management events",
    "FieldSelectors": [
      { "Field": "eventCategory", "Equals": ["Management"] }
    ]
  },
  {
    "Name": "Log PutObject and DeleteObject events for all but one bucket",
    "FieldSelectors": [
      { "Field": "eventCategory", "Equals": ["Data"] },
      { "Field": "resources.type", "Equals": ["AWS::S3::Object"] },
      { "Field": "eventName", "Equals": ["PutObject","DeleteObject"] },
      { "Field": "resources.ARN", "NotStartsWith":
["arn:aws:s3:::sample_bucket_name/"] }
    ]
  },
  {
    "Name": "Log data plane actions on MyLambdaFunction",
    "FieldSelectors": [
      { "Field": "eventCategory", "Equals": ["Data"] },
      { "Field": "resources.type", "Equals": ["AWS::Lambda::Function"] },
      { "Field": "resources.ARN", "Equals": ["arn:aws:lambda:us-
east-2:111122223333:function/MyLambdaFunction"] }
    ]
  }
]
```

```
]'
```

Das Beispiel gibt die für den Trail konfigurierten fortschrittlichen Ereignisauswahlen zurück.

```
{
  "AdvancedEventSelectors": [
    {
      "Name": "Log readOnly and writeOnly management events",
      "FieldSelectors": [
        {
          "Field": "eventCategory",
          "Equals": [ "Management" ]
        }
      ]
    },
    {
      "Name": "Log PutObject and DeleteObject events for all but one bucket",
      "FieldSelectors": [
        {
          "Field": "eventCategory",
          "Equals": [ "Data" ]
        },
        {
          "Field": "resources.type",
          "Equals": [ "AWS::S3::Object" ]
        },
        {
          "Field": "resources.ARN",
          "NotStartsWith": [ "arn:aws:s3:::sample_bucket_name/" ]
        }
      ]
    }
  ],
  {
    "Name": "Log data plane actions on MyLambdaFunction",
    "FieldSelectors": [
      {
        "Field": "eventCategory",
        "Equals": [ "Data" ]
      },
      {
        "Field": "resources.type",
        "Equals": [ "AWS::Lambda::Function" ]
      }
    ]
  }
}
```

```

    {
      "Field": "eventName",
      "Equals": [ "Invoke" ]
    },
    {
      "Field": "resources.ARN",
      "Equals": [ "arn:aws:lambda:us-east-2:111122223333:function/
MyLambdaFunction" ]
    }
  ]
},
"TrailARN": "arn:aws:cloudtrail:us-east-2:123456789012:trail/TrailName"
}

```

Beispiel-Trail, der benutzerdefinierte erweiterte Event-Selektoren verwendet, um AWS Outposts Datenergebnisse in Amazon S3 zu protokollieren

Das folgende Beispiel zeigt, wie Sie Ihren Trail so konfigurieren, dass er alle Datenergebnisse für alle Amazon S3 AWS Outposts S3-Objekte in Ihrem Außenposten enthält. In dieser Version ist der unterstützte Wert für S3 bei AWS Outposts Ereignissen für das `resources.type` `AWS::S3Outposts::Object` Feld.

```

aws cloudtrail put-event-selectors --trail-name TrailName --region region \
--advanced-event-selectors \
'[
  {
    "Name": "OutpostsEventSelector",
    "FieldSelectors": [
      { "Field": "eventCategory", "Equals": ["Data"] },
      { "Field": "resources.type", "Equals": ["AWS::S3Outposts::Object"] }
    ]
  }
]'

```

Der Befehl gibt die folgende Beispielausgabe zurück.

```

{
  "AdvancedEventSelectors": [
    {
      "Name": "OutpostsEventSelector",
      "FieldSelectors": [

```

```

        {
            "Field": "eventCategory",
            "Equals": [
                "Data"
            ]
        },
        {
            "Field": "resources.type",
            "Equals": [
                "AWS::S3Outposts::Object"
            ]
        }
    ]
},
"TrailARN": "arn:aws:cloudtrail:region:123456789012:trail/TrailName"
}

```

Beispielpfad, der erweiterte Event-Selektoren verwendet, um Ereignisse auszuschließen AWS Key Management Service

Im folgenden Beispiel wird eine erweiterte Ereignisauswahl für einen Trail erstellt, der so benannt ist, *TrailName* dass er Verwaltungsereignisse mit Schreibschutz und Schreibschutz (durch Weglassen des `readOnly` Selektors), aber Ereignisse ausschließt (`.`). AWS Key Management Service AWS KMS Da AWS KMS Ereignisse als Verwaltungsereignisse behandelt werden und es eine große Anzahl von Ereignissen geben kann, können sie erhebliche Auswirkungen auf Ihre CloudTrail Rechnung haben, wenn Sie mehr als einen Trail haben, der Verwaltungsereignisse erfasst.

Wenn Sie sich dafür entscheiden, Verwaltungsereignisse nicht zu protokollieren, werden AWS KMS Ereignisse nicht protokolliert, und Sie können die Einstellungen für die AWS KMS Ereignisprotokollierung nicht ändern.

Um wieder mit der Protokollierung von AWS KMS Ereignissen in einem Trail zu beginnen, entfernen Sie den `eventSource` Selektor und führen Sie den Befehl erneut aus.

```

aws cloudtrail put-event-selectors --trail-name TrailName \
--advanced-event-selectors '
[
{
    "Name": "Log all management events except KMS events",
    "FieldSelectors": [

```



```

    { "Field": "eventCategory", "Equals": ["Management"] },
    { "Field": "eventSource", "NotEquals": ["kms.amazonaws.com"] }
  ]
}
]'

```

Das Beispiel gibt die für den Trail konfigurierten fortschrittlichen Ereignisauswahlen zurück.

```

{
  "AdvancedEventSelectors": [
    {
      "Name": "Log all management events except KMS events",
      "FieldSelectors": [
        {
          "Field": "eventCategory",
          "Equals": [ "Management" ]
        },
        {
          "Field": "eventSource",
          "NotEquals": [ "kms.amazonaws.com" ]
        }
      ]
    }
  ],
  "TrailARN": "arn:aws:cloudtrail:us-east-2:123456789012:trail/TrailName"
}

```

Um die Protokollierung ausgeschlossener Ereignisse erneut in einen Trail zu starten, entfernen Sie den eventSource-Selektor, wie im folgenden Befehl gezeigt.

```

aws cloudtrail put-event-selectors --trail-name TrailName \
--advanced-event-selectors '
[
  {
    "Name": "Log all management events",
    "FieldSelectors": [
      { "Field": "eventCategory", "Equals": ["Management"] }
    ]
  }
]'

```

## Beispielpfad, der erweiterte Event-Selektoren verwendet, um Amazon RDS Data API-Verwaltungsereignisse auszuschließen

Im folgenden Beispiel wird ein erweiterter Event-Selektor für einen Trail erstellt, der so benannt ist *TrailName*, dass er Verwaltungsereignisse mit Schreibschutz und Schreibschutz (durch Weglassen des `readOnly` Selektors) einschließt, Amazon RDS Data API-Verwaltungsereignisse jedoch ausschließt. Um Amazon RDS Data API-Verwaltungsereignisse auszuschließen, geben Sie die Amazon RDS-Daten-API-Ereignisquelle im Zeichenfolgenwert für das `eventSource` Feld an: `rdodata.amazonaws.com`.

Wenn Sie sich dafür entscheiden, Verwaltungsereignisse nicht zu protokollieren, werden Amazon RDS Data API-Verwaltungsereignisse nicht protokolliert, und Sie können die Einstellungen für die Amazon RDS Data API-Ereignisprotokollierung nicht ändern.

Um wieder mit der Protokollierung von Amazon RDS Data API-Verwaltungsereignissen in einem Trail zu beginnen, entfernen Sie den `eventSource` Selektor und führen Sie den Befehl erneut aus.

```
aws cloudtrail put-event-selectors --trail-name TrailName \  
--advanced-event-selectors '  
[  
  {  
    "Name": "Log all management events except Amazon RDS Data API management events",  
    "FieldSelectors": [  
      { "Field": "eventCategory", "Equals": ["Management"] },  
      { "Field": "eventSource", "NotEquals": ["rdodata.amazonaws.com"] }  
    ]  
  }  
]
```

Das Beispiel gibt die für den Trail konfigurierten fortschrittlichen Ereignisauswahlen zurück.

```
{  
  "AdvancedEventSelectors": [  
    {  
      "Name": "Log all management events except Amazon RDS Data API management events",  
      "FieldSelectors": [  
        {  
          "Field": "eventCategory",  
          "Equals": [ "Management" ]  
        },  
        {
```

```
        "Field": "eventSource",
        "NotEquals": [ "rdsdata.amazonaws.com" ]
      }
    ]
  },
  "TrailARN": "arn:aws:cloudtrail:us-east-2:123456789012:trail/TrailName"
}
```

Um die Protokollierung ausgeschlossener Ereignisse erneut in einen Trail zu starten, entfernen Sie den eventSource-Selektor, wie im folgenden Befehl gezeigt.

```
aws cloudtrail put-event-selectors --trail-name TrailName \
--advanced-event-selectors '
[
  {
    "Name": "Log all management events",
    "FieldSelectors": [
      { "Field": "eventCategory", "Equals": ["Management"] }
    ]
  }
]
```

## Anhalten und Starten der Protokollierung für einen Trail

Die folgenden Befehle starten und beenden die CloudTrail Protokollierung.

```
aws cloudtrail start-logging --name awscloudtrail-example
```

```
aws cloudtrail stop-logging --name awscloudtrail-example
```

### Note

Führen Sie vor dem Löschen eines Buckets den Befehl `stop-logging` aus, um die Bereitstellung von Ereignissen im Bucket zu beenden. Wenn Sie die Protokollierung nicht beenden, wird CloudTrail versucht, Protokolldateien für einen begrenzten Zeitraum in einen Bucket mit demselben Namen zu übertragen.

Wenn Sie die Protokollierung beenden oder einen Trail löschen, ist CloudTrail Insights für diesen Trail deaktiviert.

## Löschen eines Trails

Wenn Sie CloudTrail Verwaltungsereignisse in Amazon Security Lake aktiviert haben, müssen Sie mindestens einen organisatorischen Pfad verwalten, der mehrere Regionen umfasst `read` und sowohl Verwaltungsereignisse als auch `write` Verwaltungsereignisse protokolliert. Sie können einen Trail nicht löschen, wenn er der einzige Trail ist, den Sie haben, der diese Anforderung erfüllt, es sei denn, Sie deaktivieren CloudTrail Verwaltungsereignisse in Security Lake.

Sie können einen Trail mit dem folgenden Befehl löschen. Sie können einen Trail nur in der Region löschen, in der er erstellt wurde (Home Region).

```
aws cloudtrail delete-trail --name awscloudtrail-example
```

Wenn Sie einen Trail löschen, löschen Sie nicht den Amazon-S3-Bucket oder das mit diesem verbundene Amazon-SNS-Thema. Verwenden Sie die Dienst-API AWS Management Console AWS CLI, oder, um diese Ressourcen separat zu löschen.

## Erstellen eines Trails für eine Organisation

Wenn Sie eine Organisation in erstellt haben AWS Organizations, können Sie einen Trail erstellen, der alle Ereignisse für alle AWS-Konten Mitglieder dieser Organisation protokolliert. Ein solcher Trail wird manchmal als Organisations-Trail bezeichnet.

Über das Verwaltungskonto einer Organisation können [delegierte Administratoren](#) für die Erstellung neuer Organisations-Trails oder die Verwaltung bestehender Organisations-Trails zugewiesen werden. Weitere Informationen zum Hinzufügen delegierter Administratoren finden Sie unter [Fügen Sie einen delegierten Administrator hinzu CloudTrail](#).

Das Verwaltungskonto der Organisation kann einen vorhandenen Trail im Konto eines delegierten Administrators bearbeiten und ihn auf eine Organisation anwenden, wodurch ein Organisations-Trail entsteht. Organisations-Trails protokollieren Ereignisse für das Verwaltungskonto und alle Mitgliedskonten in der Organisation. Weitere Informationen zu finden Sie AWS Organizations unter [Terminologie und Konzepte für Organizations](#).

### Note

Zum Erstellen eines Organisations-Trails müssen Sie sich mit dem Verwaltungskonto oder dem Konto eines delegierten Administrators einer Organisation anmelden. Sie müssen außerdem über [ausreichende Berechtigungen](#) für den Benutzer oder die Rolle im

Verwaltungs- oder delegierten Administratorkonto verfügen, um den Trail erstellen zu können. Wenn Sie nicht über ausreichende Berechtigungen verfügen, haben Sie nicht die Option, den Trail auf eine Organisation anzuwenden.

Bei allen mit der Konsole erstellten Organisationspfaden handelt es sich um regionsübergreifende Organisationspfade, in denen Ereignisse von Konten protokolliert werden, die AWS-Regionen in jedem Mitgliedskonto der Organisation [aktiviert](#) sind. Um Ereignisse in allen AWS Partitionen Ihrer Organisation zu protokollieren, erstellen Sie in jeder Partition einen regionsübergreifenden Organisationspfad. Sie können entweder einen Organisationspfad mit einer Region oder mit mehreren Regionen erstellen, indem Sie den verwenden. AWS CLI Wenn Sie einen Pfad mit nur einer Region erstellen, protokollieren Sie nur Aktivitäten in den Pfaden AWS-Region (auch als Heimatregion bezeichnet).

Obwohl die meisten Regionen standardmäßig für dich aktiviert AWS-Regionen sind AWS-Konto, musst du bestimmte Regionen (auch als Opt-in-Regionen bezeichnet) manuell aktivieren. Informationen darüber, welche Regionen standardmäßig aktiviert sind, finden Sie im AWS Account Management Referenzhandbuch unter [Überlegungen vor dem Aktivieren und Deaktivieren von Regionen](#). Eine Liste der CloudTrail unterstützten Regionen finden Sie unter [CloudTrail unterstützte Regionen](#).

Wenn Sie einen Organisationspfad erstellen, wird eine Kopie des Trails mit dem Namen, den Sie ihm geben, in den Mitgliedskonten Ihrer Organisation erstellt.

- Wenn sich der Organisationspfad auf eine einzelne Region bezieht und die Heimatregion des Trails keine OPT-Region ist, wird in jedem Mitgliedskonto eine Kopie des Trails in der Heimatregion des Organisationstrails erstellt.
- Wenn sich der Organisationspfad auf eine einzelne Region bezieht und die Heimatregion des Trails eine OPT-Region ist, wird eine Kopie des Trails in der Heimatregion des Organisationstrails in den Mitgliedskonten erstellt, die diese Region aktiviert haben.
- Wenn es sich bei dem Organisationspfad um mehrere Regionen handelt und die Heimatregion des Trails keine Region ist, in der sich der Weg angemeldet hat, wird in jedem Mitgliedskonto, das aktiviert AWS-Region ist, eine Kopie des Trails erstellt. Wenn ein Mitgliedskonto eine Opt-in-Region aktiviert, wird nach Abschluss der Aktivierung dieser Region eine Kopie des Multi-Region-Trails in der neu angemeldeten Region für das Mitgliedskonto erstellt.
- Wenn es sich bei dem Organisationspfad um einen Multi-Region-Trail handelt und die Heimatregion eine optionale Region ist, senden Mitgliedskonten keine Aktivitäten an den

Organisationspfad, es sei denn, sie entscheiden sich für den Ort, an AWS-Region dem der Multi-Region-Trail erstellt wurde. Wenn du beispielsweise einen Trail mit mehreren Regionen erstellst und die Region Europa (Spanien) als Heimatregion für den Trail auswählst, senden nur Mitgliedskonten, die die Region Europa (Spanien) für ihr Konto aktiviert haben, ihre Kontoaktivitäten an den Organisationspfad.

### Note

CloudTrail erstellt Organisationspfade in Mitgliedskonten, auch wenn eine Ressourcenvalidierung fehlschlägt. Zu den Beispielen für fehlgeschlagene Überprüfungen gehören:

- eine falsche Amazon S3 S3-Bucket-Richtlinie
- eine falsche Amazon SNS SNS-Themenrichtlinie
- Unfähigkeit, an eine CloudWatch Logs-Protokollgruppe zu liefern
- unzureichende Rechte zur Verschlüsselung mit einem KMS-Schlüssel

Ein Mitgliedskonto mit CloudTrail Berechtigungen kann alle Validierungsfehler für einen Organisationspfad anzeigen, indem es die Detailseite des Trails in der CloudTrail Konsole aufruft oder den AWS CLI [get-trail-status](#)Befehl ausführt.

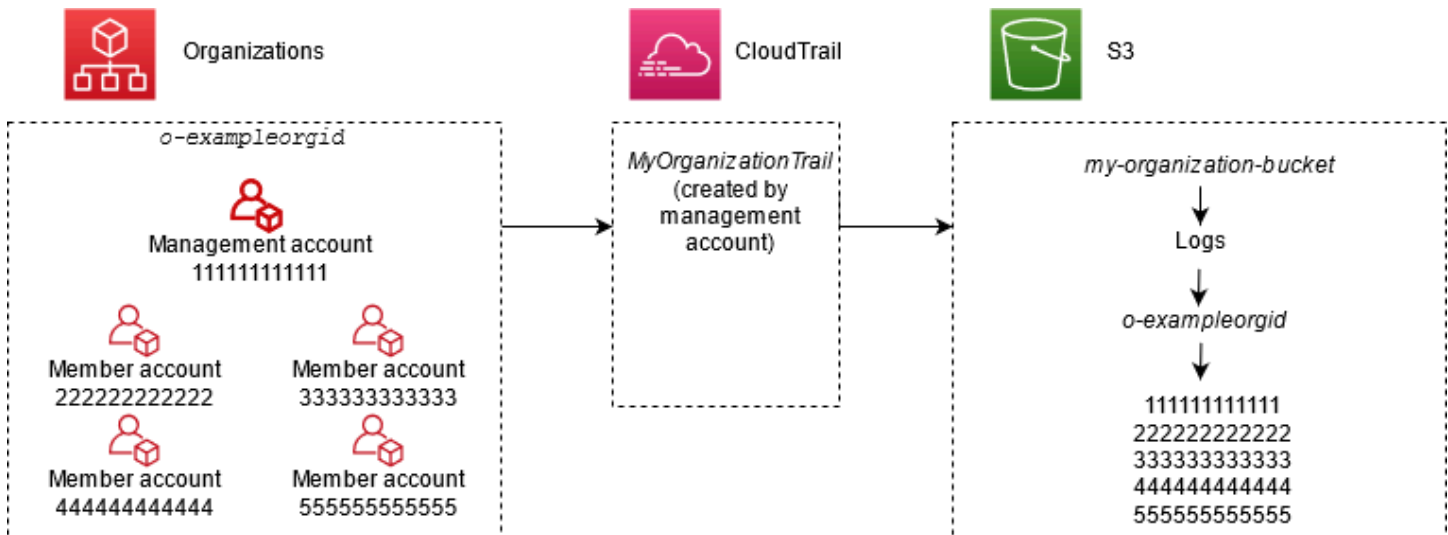
Benutzer mit CloudTrail Berechtigungen in Mitgliedskonten können Organisationspfade sehen AWS-Konten, wenn sie sich von ihrem Konto aus bei der AWS CloudTrail Konsole anmelden oder wenn sie AWS CLI Befehle wie `ausführendescribe-trails`. Benutzer mit Mitgliedskonten verfügen jedoch nicht über ausreichende Berechtigungen, um Organisationspfade zu löschen, die Anmeldung ein- oder auszuschalten, zu ändern, welche Arten von Ereignissen protokolliert werden, oder einen Organisationspfad auf andere Weise zu ändern.

Wenn Sie in der Konsole einen Organisationspfad erstellen oder wenn Sie ihn CloudTrail als vertrauenswürdigen Dienst in Organizations aktivieren, wird dadurch eine dienstverknüpfte Rolle erstellt, mit der Protokollierungsaufgaben in den Mitgliedskonten Ihrer Organisation ausgeführt werden können. Diese Rolle hat einen Namen und ist erforderlich `AWSServiceRoleForCloudTrail`, CloudTrail um Ereignisse für eine Organisation zu protokollieren. Wenn einer Organisation eine hinzugefügt AWS-Konto wird, werden der Organisationspfad und die mit dem Dienst verknüpfte Rolle hinzugefügt AWS-Konto, und die Protokollierung für dieses Konto wird automatisch im

Organisationspfad gestartet. Wenn ein aus einer Organisation entferntes AWS-Konto wird, werden der Organisationspfad und die mit dem Dienst verknüpfte Rolle aus der Organisation gelöscht. Das AWS-Konto, die nicht mehr Teil der Organisation ist. Allerdings bleiben diesem entfernten Konto zugehörige Protokolldateien, die vor der Entfernung des Kontos erstellt wurden, weiterhin in dem Amazon-S3-Bucket, in dem die Protokolldateien für den Trail gespeichert sind.

Wenn das Verwaltungskonto für eine AWS Organizations Organisation einen Organisationspfad erstellt, dann aber anschließend als Verwaltungskonto der Organisation entfernt wird, wird jeder mit diesem Konto erstellte Organisationspfad zu einem Nicht-Organisationspfad.

*Im folgenden Beispiel erstellt das Verwaltungskonto 111111111111 der Organisation einen Pfad, der nach der Organisation o-exampleorgid benannt ist. `MyOrganizationTrail`* Der Trail protokolliert Aktivitäten für alle Konten der Organisation im selben Amazon-S3-Bucket. Alle Konten in der Organisation können `MyOrganizationTrail` in ihrer Liste mit Pfaden angezeigt werden, aber Mitgliedskonten können den Organisationspfad nicht entfernen oder ändern. Nur über das Verwaltungskonto oder das Konto eines delegierten Administrators kann der Trail für die Organisation geändert oder gelöscht werden. Das Entfernen eines Mitgliedskontos aus einer Organisation kann nur über das Verwaltungskonto erfolgen. Ebenso hat standardmäßig nur das Verwaltungskonto Zugriff auf den Amazon S3 S3-Bucket `my-organization-bucket` für den Trail und die darin enthaltenen Protokolle. Die High-Level-Bucket-Struktur für Protokolldateien enthält einen nach der Organisations-ID benannten Ordner. In diesem Ordner befinden sich wiederum Unterordner, die nach den Konto-IDs aller Organisationskonten benannt sind. Ereignisse für jedes Mitgliedskonto werden in dem Ordner gespeichert, der der Mitgliedskonto-ID entspricht. Wenn das Mitgliedskonto 4444444444 aus der Organisation entfernt wird `MyOrganizationTrail` und die mit dem Service verknüpfte Rolle nicht mehr im AWS Konto 444444444444 erscheint und keine weiteren Ereignisse für dieses Konto im Organisationspfad protokolliert werden. Der Ordner 444444444444 verbleibt jedoch im Amazon-S3-Bucket, zusammen mit allen Protokollen, die vor dem Entfernen des Kontos aus der Organisation erstellt wurden.



In diesem Beispiel lautet der ARN des im Verwaltungskonto erstellten Trails `aws:cloudtrail:us-east-2:111111111111:trail/MyOrganizationTrail`. Dieser ARN bildet auch den ARN für den Trail in allen Mitgliedskonten.

Organisations-Trails sind regulären Trails in vielerlei Hinsicht ähnlich. Sie können mehrere Trails für Ihre Organisation erstellen und dann auswählen, ob Sie einen Organisations-Trail für alle Regionen oder eine einzelne Region anlegen möchten. Außerdem können Sie festlegen, welche Ereignistypen in Ihrem Organisations-Trail oder in anderen Trails protokolliert werden sollen. Es gibt jedoch einige Unterschiede. Wenn Sie beispielsweise in der Konsole einen Trail erstellen und auswählen, ob Datenereignisse für Amazon S3 S3-Buckets oder AWS Lambda Funktionen protokolliert werden sollen, werden in der CloudTrail Konsole nur die Ressourcen für das Verwaltungskonto aufgeführt. Sie können jedoch die ARNs für Ressourcen in Mitgliedskonten hinzufügen. Datenereignisse für Ressourcen angegebener Mitgliedskonten werden protokolliert, ohne dass der kontoübergreifende Zugriff auf diese Ressourcen manuell konfiguriert werden muss. Weitere Informationen zur Protokollierung von Verwaltungsereignissen, Insights-Ereignissen und Datenereignissen finden Sie unter [Protokollieren von Verwaltungsereignissen](#), [Protokollieren von Datenereignissen](#), und [Protokollieren von Insights-Ereignissen](#).

#### Note

In der Konsole erstellen Sie einen Trail mit mehreren Regionen. Dies ist eine empfohlene bewährte Methode. Durch das Protokollieren von Aktivitäten in allen Regionen Ihrer Umgebung AWS-Konto können Sie die Sicherheit Ihrer AWS Umgebung erhöhen. Um einen Trail für eine einzelne Region zu erstellen, [verwenden Sie die AWS CLI](#).



Wenn Sie Ereignisse im Ereignisverlauf für eine Organisation in anzeigen AWS Organizations, können Sie nur die Ereignisse der Organisation anzeigen, AWS-Konto mit der Sie angemeldet sind. Wenn Sie beispielsweise mit dem Verwaltungskonto der Organisation angemeldet sind, zeigt der Ereignisverlauf die Verwaltungsereignisse der letzten 90 Tage für das Verwaltungskonto an. Ereignisse des Organisationsmitgliedskontos werden im Ereignisverlauf für das Verwaltungskonto nicht angezeigt. Um Mitgliederkontoereignisse im Ereignisverlauf anzuzeigen, melden Sie sich mit dem Mitgliedskonto an.

Sie können andere AWS Dienste so konfigurieren, dass sie die in den CloudTrail Protokollen für ein Organisationsprotokoll gesammelten Ereignisdaten weiter analysieren und darauf reagieren, genauso wie Sie es für jeden anderen Trail tun würden. Beispielsweise können Sie die Daten eines Organisations-Trails mit Amazon Athena analysieren. Weitere Informationen finden Sie unter [AWS Serviceintegrationen mit Protokollen CloudTrail](#).

## Themen

- [Umstellung von Protokollen für Mitgliedskonten auf Organisationstrails](#)
- [Vorbereiten der Erstellung eines Trails für Ihre Organisation](#)
- [Vorbereiten der Erstellung eines Trails für Ihre Organisation in der Konsole](#)
- [Erstellen eines Trails für eine Organisation mit dem AWS Command Line Interface](#)
- [Fehlerbehebung](#)

## Umstellung von Protokollen für Mitgliedskonten auf Organisationstrails

Wenn Sie bereits CloudTrail Trails für einzelne Mitgliedskonten konfiguriert haben, aber zu einem Organisationspfad wechseln möchten, um Ereignisse in allen Konten zu protokollieren, möchten Sie nicht, dass Ereignisse verloren gehen, indem Sie die Trails einzelner Mitgliedskonten löschen, bevor Sie einen Organisationspfad erstellen. Allerdings entstehen bei zwei Trails aufgrund der zusätzlichen Kopie der Ereignisse, die an den Organisations-Trail geliefert werden höhere Kosten.

Zur Verwaltung der Kosten, ohne vor Beginn der Protokollzustellung beim Organisationspfad Ereignisse zu verlieren, sollten Sie sowohl die einzelnen Mitgliedskonto-Trails als auch den Organisations-Trail für bis zu einem Tag aufbewahren. Dadurch wird sichergestellt, dass der Organisations-Trail alle Ereignisse protokolliert und es entstehen nur für einen Tag doppelte Ereigniskosten. Nach dem ersten Tag können Sie die Anmeldung an einzelnen Mitgliedskonto-Trails beenden (oder diese löschen).

## Vorbereiten der Erstellung eines Trails für Ihre Organisation

Bevor Sie einen Trail für Ihre Organisation erstellen, müssen Sie sich vergewissern, dass das Verwaltungskonto oder das Konto eines delegierten Administrators Ihrer Organisation für die Trail-Erstellung richtig eingerichtet ist.

- In Ihrer Organisation müssen alle Funktionen aktiviert sein, bevor Sie einen Trail erstellen. Weitere Informationen finden Sie unter [Aktivieren aller Funktionen in der Organisation](#).
- Das Verwaltungskonto muss über die `AWSServiceRoleForOrganizations`-Rolle verfügen. Diese Rolle wird automatisch von Organizations erstellt, wenn Sie Ihre Organisation erstellen, und ist erforderlich, CloudTrail um Ereignisse für eine Organisation zu protokollieren. Weitere Informationen finden Sie unter [Organisationen und serviceverknüpfte Rollen](#).
- Der Benutzer oder die Rolle, der/die im Verwaltungskonto oder im Konto eines delegierten Administrators den Organisations-Trail erstellt, muss über ausreichende Berechtigungen zum Erstellen eines Organisations-Trails verfügen. Sie müssen mindestens die `AWSCloudTrail_FullAccess`-Richtlinie oder eine gleichwertige Richtlinie auf diese Rolle oder diesen Benutzer anwenden. Außerdem müssen Sie über ausreichende Berechtigungen in IAM und Organizations verfügen, um die serviceverknüpfte Rolle zu erstellen und den vertrauenswürdigen Zugriff zu aktivieren. Wenn Sie sich dafür entscheiden, mithilfe der CloudTrail Konsole einen neuen S3-Bucket für einen Organization Trail zu erstellen, Ihre Richtlinie muss auch Folgendes beinhalten `s3:PutEncryptionConfiguration` Aktion, da die serverseitige Verschlüsselung standardmäßig für den Bucket aktiviert ist. Die folgende Beispielrichtlinie zeigt die mindestens erforderlichen Berechtigungen.

### Note

Sie sollten die `AWSCloudTrail_FullAccess`Richtlinie nicht allgemein in Ihrem AWS-Konto Unternehmen anwenden. Stattdessen sollten Sie es aufgrund der hochsensiblen Natur der von gesammelten Informationen auf AWS-Konto Administratoren beschränken CloudTrail. Benutzer mit dieser Rolle haben die Möglichkeit, die sensibelsten und wichtigsten Auditing-Funktionen in ihren AWS-Konten zu deaktivieren oder zu konfigurieren. Aus diesem Grund sollte der Zugriff auf diese Richtlinie sorgfältig kontrolliert und überwacht werden.

```
{  
  "Version": "2012-10-17",  
  "Statement": [  
    {  
      "Action": "iam:CreateRole",  
      "Resource": "*",  
      "Effect": "Allow",  
      "Principal": "AWS" }  
    ]  
}
```

```

    {
      "Effect": "Allow",
      "Action": [
        "iam:GetRole",
        "organizations:EnableAWSServiceAccess",
        "organizations:ListAccounts",
        "iam:CreateServiceLinkedRole",
        "organizations:DisableAWSServiceAccess",
        "organizations:DescribeOrganization",
        "organizations:ListAWSServiceAccessForOrganization",
        "s3:PutEncryptionConfiguration"
      ],
      "Resource": "*"
    }
  ]
}

```

- Um die AWS CLI oder die CloudTrail APIs zur Erstellung eines Organization Trails zu verwenden, müssen Sie den vertrauenswürdigen Zugriff für CloudTrail in Organizations aktivieren und Sie müssen manuell einen Amazon S3 S3-Bucket mit einer Richtlinie erstellen, die die Protokollierung für einen Organization Trail ermöglicht. Weitere Informationen finden Sie unter [Erstellen eines Trails für eine Organisation mit dem AWS Command Line Interface](#).
- Um eine bestehende IAM-Rolle zu verwenden, um Amazon CloudWatch Logs die Überwachung eines Organisationstrails hinzuzufügen, müssen Sie die IAM-Rolle manuell ändern, um die Übermittlung von CloudWatch Protokollen für Mitgliedskonten an die CloudWatch Logs-Gruppe für das Verwaltungskonto zu ermöglichen, wie im folgenden Beispiel gezeigt.

#### Note

Sie müssen eine IAM-Rolle und eine CloudWatch Logs-Protokollgruppe verwenden, die in Ihrem eigenen Konto vorhanden sind. Sie können keine IAM-Rolle oder CloudWatch Logs-Protokollgruppe verwenden, die einem anderen Konto gehört.

```

{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Sid": "AWSCloudTrailCreateLogStream20141101",
      "Effect": "Allow",

```

```

        "Action": [
            "logs:CreateLogStream"
        ],
        "Resource": [
            "arn:aws:logs:us-east-2:111111111111:log-group:CloudTrail/
DefaultLogGroupTest:log-stream:111111111111_CloudTrail_us-east-2*",
            "arn:aws:logs:us-east-2:111111111111:log-group:CloudTrail/
DefaultLogGroupTest:log-stream:o-exampleorgid_*"
        ]
    },
    {
        "Sid": "AWSCloudTrailPutLogEvents20141101",
        "Effect": "Allow",
        "Action": [
            "logs:PutLogEvents"
        ],
        "Resource": [
            "arn:aws:logs:us-east-2:111111111111:log-group:CloudTrail/
DefaultLogGroupTest:log-stream:111111111111_CloudTrail_us-east-2*",
            "arn:aws:logs:us-east-2:111111111111:log-group:CloudTrail/
DefaultLogGroupTest:log-stream:o-exampleorgid_*"
        ]
    }
]
}

```

Sie können mehr darüber erfahren CloudTrail und Amazon CloudWatch loggt sich ein [Überwachung von CloudTrail Protokolldateien mit Amazon CloudWatch Logs](#). Darüber hinaus sollten Sie die Beschränkungen für CloudWatch Logs und die Preisgestaltung für den Service berücksichtigen, bevor Sie sich dafür entscheiden, das Erlebnis für einen Organisationstest zu aktivieren. Weitere Informationen finden Sie unter [CloudWatch Log-Limits](#) und [CloudWatchAmazon-Preise](#).

- Um Datenereignisse in Ihrem Organisations-Trail für bestimmte Ressourcen in Mitgliedskonten zu protokollieren, halten Sie eine Liste mit Amazon-Ressourcennamen (ARNs) für jede dieser Ressourcen bereit. Die Ressourcen des Mitgliedskontos werden nicht in der CloudTrail Konsole angezeigt, wenn Sie einen Trail erstellen. Sie können im Verwaltungskonto, für das die Erfassung von Datenereignissen unterstützt wird, nach Ressourcen suchen, z. B. S3-Buckets. Wenn Sie beim Erstellen oder Aktualisieren eines Organisations-Trails in der Befehlszeile bestimmte Mitgliedsressourcen hinzufügen möchten, benötigen Sie die ARNs für diese Ressourcen.

**Note**

Für die Protokollierung von Datenereignissen fallen zusätzliche Gebühren an. CloudTrail Die Preise finden Sie unter [AWS CloudTrail Preise](#).

Sie sollten auch in Betracht ziehen, zu überprüfen, wie viele Trails bereits im Verwaltungskonto und in den Mitgliedskonten existieren, bevor Sie einen Organisations-Trail erstellen. CloudTrail begrenzt die Anzahl der Wanderwege, die in jeder Region erstellt werden können. Sie können diesen Grenzwert in der Region, in der Sie den Organisations-Trail erstellen, im Verwaltungskonto nicht überschreiten. Beachten Sie jedoch, dass der Trail in den Mitgliedskonten auch dann erstellt wird, wenn für ein Mitgliedskonto die maximale Anzahl an Trails in einer Region erreicht ist. Während der erste Trail von Verwaltungsereignissen in jeder Region kostenlos ist, fallen für zusätzliche Trails Gebühren an. Zur Reduzierung der potenziellen Kosten eines Organisations-Trails sollten Sie alle nicht benötigten Trails im Verwaltungskonto und in Mitgliedskonten löschen. Weitere Informationen zur CloudTrail Preisgestaltung finden Sie unter [AWS CloudTrail Preise](#).

## Bewährte Sicherheitsmethoden in Organisations-Trails

Als bewährte Sicherheitsmethode empfehlen wir Ihnen, den `aws:SourceArn`-Bedingungsschlüssel zu Ressourcenrichtlinien (z. B. solche für S3-Buckets, KMS-Schlüssel oder SNS-Themen) hinzuzufügen, die Sie mit einem Organisations-Trail verwenden. Der Wert von `aws:SourceArn` ist der ARN des Organisations-Trails (oder ARNs, wenn Sie dieselbe Ressource für mehr als einen Trail verwenden, z. B. denselben S3-Bucket zum Speichern von Protokollen für mehr als einen Trail). Dies stellt sicher, dass die Ressource, z. B. ein S3-Bucket, nur Daten akzeptiert, die mit dem spezifischen Trail verknüpft sind. Der Trail-ARN muss die Konto-ID des Verwaltungskontos verwenden. Der folgende Richtlinienausschnitt zeigt ein Beispiel, in dem mehr als ein Trail die Ressource verwendet.

```
"Condition": {
  "StringEquals": {
    "aws:SourceArn": ["Trail_ARN_1", ..., "Trail_ARN_n"]
  }
}
```

Informationen zum Hinzufügen von Bedingungsschlüsseln zu Ressourcenrichtlinien finden Sie hier:

- [Amazon S3 S3-Bucket-Richtlinie für CloudTrail](#)
- [Konfigurieren Sie AWS KMS wichtige Richtlinien für CloudTrail](#)

- [Amazon SNS Themenrichtlinie für CloudTrail](#)

## Vorbereiten der Erstellung eines Trails für Ihre Organisation in der Konsole

Um einen Organisationspfad von der CloudTrail Konsole aus zu erstellen, müssen Sie sich bei der Konsole als Benutzer oder als Rolle im Verwaltungs- oder delegierten Administratorkonto anmelden, das über [ausreichende Berechtigungen](#) verfügt. Wenn Sie sich nicht mit dem Verwaltungs- oder delegierten Administratorkonto anmelden, wird Ihnen beim Erstellen oder Bearbeiten eines Trails von der Konsole aus die Option zum Anwenden CloudTrail eines Trails auf eine Organisation nicht angezeigt.

Sie können einen Organisations-Trail auf verschiedene Arten konfigurieren. Für Ihren Organisations-Trail können Sie beispielsweise die folgenden Einstellungen konfigurieren:


- Wenn Sie einen Trail in der Konsole anlegen, protokolliert der Trail standardmäßig alle AWS-Regionen in der [AWS -Partition](#), in der Sie arbeiten. Als bewährte Methode empfehlen wir dringend, Ereignisse in allen Regionen Ihrer AWS-Konto Region zu protokollieren. Um einen Trail für eine einzige Region zu erstellen, [verwenden Sie die AWS CLI](#).
- Geben Sie an, ob der Trail auf Ihre Organisation angewendet werden soll. Standardmäßig werden Trails nicht auf Organisationen angewendet. Sie müssen diese Option auswählen, um einen Organisations-Trail zu erstellen.
- Geben Sie an, welcher Amazon-S3-Bucket Protokolldateien für den Organisations-Trail empfangen soll. Sie können einen vorhandenen Amazon-S3-Bucket wählen oder speziell für den Organisations-Trail einen Bucket erstellen.
- Für Verwaltungs- und Datenereignisse können Sie angeben, ob Lesen, Schreiben oder alle Ereignisse protokolliert werden sollen. [CloudTrailInsights-Ereignisse](#) werden nur bei Verwaltungsereignissen protokolliert. Sie können Protokollierungsdatenereignisse für Ressourcen im Verwaltungskonto angeben, indem Sie sie aus den Listen in der Konsole auswählen und in Mitgliedskonten, wenn Sie die ARNs jeder Ressource angeben, für die Sie die Datenereignisprotokollierung aktivieren möchten. Weitere Informationen finden Sie unter [Datenereignisse](#).

Um einen Organisationspfad mit dem zu erstellen AWS Management Console

1. Melden Sie sich bei der an AWS Management Console und öffnen Sie die CloudTrail Konsole unter <https://console.aws.amazon.com/cloudtrail/>.

Sie müssen mit einer IAM-Identität im Verwaltungskonto oder im Konto eines delegierten Administrators mit [ausreichenden Berechtigungen](#) angemeldet sein, um einen Organisations-Trail zu erstellen.

2. Wählen Sie Trails und anschließend Create Trail (Trail erstellen).
3. Geben Sie auf der Seite Create Trail in Trail name einen Namen für den Trail ein. Weitere Informationen finden Sie unter [Benennungsanforderungen](#).
4. Wählen Sie Aktivieren für alle Konten in meiner Organisation aus. Diese Option wird nur angezeigt, wenn Sie sich mit einem Benutzer oder einer Rolle im Verwaltungskonto oder im Konto eines delegierten Administrators bei der Konsole anmelden. Zur Erstellung eines Organisations-Trails müssen dem Benutzer oder der Rolle [ausreichende Berechtigungen](#) zugewiesen sein.
5. Wählen Sie in Speicherort für Neuen S3 Bucket erstellen, um einen neuen Bucket zu erstellen. Wenn Sie einen Bucket erstellen, werden die erforderlichen Bucket-Richtlinien CloudTrail erstellt und angewendet.

 Note


Wenn Sie Vorhandenen S3 Bucket verwenden ausgewählt haben, geben Sie einen Bucket im Namen des Trail-Protokoll-Buckets an oder wählen Sie Durchsuchen, um einen Bucket auszuwählen. Sie können einen Bucket auswählen, der zu einem beliebigen Konto gehört. Die Bucket-Richtlinie muss jedoch die CloudTrail Schreibberechtigung für diesen Bucket gewähren. Informationen zur manuellen Bearbeitung der Bucket-Richtlinie finden Sie im Abschnitt [Amazon S3 S3-Bucket-Richtlinie für CloudTrail](#).

Um das Auffinden Ihrer Logs zu erleichtern, erstellen Sie in einem vorhandenen Bucket einen neuen Ordner (auch als Präfix bezeichnet), um Ihre CloudTrail Logs zu speichern. Geben Sie das Präfix in Präfix ein.

6. Wählen Sie unter Log file SSE-KMS encryption (SSE-KMS-Verschlüsselung der Protokolldatei) die Option Enabled (Aktiviert) aus, wenn Sie Ihre Protokolldateien mit der SSE-KMS-Verschlüsselung anstelle der SSE-S3-Verschlüsselung verschlüsseln möchten. Der Standard ist aktiviert. Wenn Sie die SSE-KMS-Verschlüsselung nicht aktivieren, werden die Protokolle mit der SSE-S3-Verschlüsselung verschlüsselt. Weitere Informationen zur SSE-KMS-Verschlüsselung finden Sie unter [Verwenden der serverseitigen Verschlüsselung mit AWS](#)

[Key Management Service \(SSE-KMS\)](#). Weitere Informationen zur SSE-S3-Verschlüsselung finden Sie unter [Verwenden der serverseitigen Verschlüsselung mit von Amazon S3 verwalteten Verschlüsselungsschlüsseln \(SSE-S3\)](#).

Wenn Sie die SSE-KMS-Verschlüsselung aktivieren, wählen Sie „Neu“ oder „Bestehend“. AWS KMS key Geben Sie AWS KMS unter Alias einen Alias im Format an. `alias/MyAliasName` Weitere Informationen finden Sie unter [Aktualisieren einer Ressource zur Verwendung des KMS-Schlüssels](#).

 Note

Sie können auch den ARN eines Schlüssels aus einem anderen Konto eingeben. Weitere Informationen finden Sie unter [Aktualisieren einer Ressource zur Verwendung des KMS-Schlüssels](#). Die Schlüsselrichtlinie muss die Verwendung des Schlüssels zum Verschlüsseln Ihrer Protokolldateien ermöglichen und den von Ihnen angegebenen Benutzern das Lesen von Protokolldateien in unverschlüsselter Form ermöglichen. CloudTrail Informationen zur manuellen Bearbeitung der Schlüsselrichtlinie finden Sie unter [Konfigurieren Sie AWS KMS wichtige Richtlinien für CloudTrail](#).

7. Konfigurieren Sie unter Zusätzliche Einstellungen Folgendes.
  - a. Wählen Sie für Protokolldateivalidierung Aktiviert, damit Ihrem S3 Bucket Protokoll-Digests übermittelt werden. Sie können die Digest-Dateien verwenden, um zu überprüfen, ob sich Ihre Protokolldateien nach CloudTrail der Übermittlung nicht geändert haben. Weitere Informationen finden Sie unter [Überprüfen der Integrität der CloudTrail Protokolldatei](#).
  - b. Wählen Sie für die Zustellung von SNS-Benachrichtigungen die Option Aktiviert aus, um jedes Mal benachrichtigt zu werden, wenn ein Protokoll an Ihren Bucket gesendet wird. CloudTrail speichert mehrere Ereignisse in einer Protokolldatei. SNS-Benachrichtigungen werden für jede Protokolldatei, nicht für jedes Ereignis gesendet. Weitere Informationen finden Sie unter [Konfiguration von Amazon SNS SNS-Benachrichtigungen für CloudTrail](#).


Wenn Sie SNS-Benachrichtigungen aktivieren, wählen Sie für Neues SNS-Thema erstellen die Option Neu aus, um ein Thema zu erstellen, oder wählen Sie Vorhanden aus, um ein vorhandenes Thema zu verwenden. Wenn Sie einen Trail erstellen, der für alle Regionen gilt, werden SNS-Benachrichtigungen für Protokolldateizustellungen aus allen Regionen an das von Ihnen erstellte einzelne SNS-Thema gesendet.



Wenn Sie Neu wählen, CloudTrail gibt Sie einen Namen für das neue Thema an, oder Sie können einen Namen eingeben. Wenn Sie Vorhanden wählen, wählen Sie ein SNS-Thema aus der Dropdown-Liste aus. Sie können auch den ARN eines Themas aus einer anderen Region oder aus einem Konto mit den entsprechenden Berechtigungen eingeben. Weitere Informationen finden Sie unter [Amazon SNS SNS-Themenrichtlinie für CloudTrail](#).


Wenn Sie ein Thema erstellen, müssen Sie das Thema abonnieren, um über die Zustellung von Protokolldateien benachrichtigt zu werden. Sie können das Abonnement von der Amazon-SNS-Konsole aus vornehmen. Aufgrund der Häufigkeit der Benachrichtigungen empfehlen wir, das Abonnement so zu konfigurieren, dass eine Amazon-SQS-Warteschlange zur programmgesteuerten Bearbeitung der Benachrichtigungen verwendet wird. Weitere Informationen finden Sie unter [Erste Schritte mit Amazon SNS](#) im Benutzerhandbuch für Amazon Simple Notification Service.

8. Optional können Sie konfigurieren, CloudTrail dass Protokolldateien an CloudWatch Protokolle gesendet werden, indem Sie in CloudWatch Protokollen die Option Aktiviert auswählen. Weitere Informationen finden Sie unter [Ereignisse an CloudWatch Logs senden](#).

 Note

Nur das Verwaltungskonto kann mithilfe der Konsole eine CloudWatch Protokollgruppe „Logs“ für einen Organization Trail konfigurieren. Der delegierte Administrator kann eine CloudWatch Logs-Protokollgruppe mithilfe der UpdateTrail API-Operationen AWS CLI oder CloudTrail CreateTrail oder konfigurieren.

- a. Wenn Sie die Integration mit CloudWatch Logs aktivieren, wählen Sie Neu, um eine neue Protokollgruppe zu erstellen, oder Existierend, um eine bestehende zu verwenden. Wenn Sie „Neu“ wählen CloudTrail, geben Sie einen Namen für die neue Protokollgruppe an, oder Sie können einen Namen eingeben.
- b. Wenn Sie Vorhanden wählen, wählen Sie eine Protokollgruppe aus der Dropdown-Liste aus.
- c. Wählen Sie Neu, um eine neue IAM-Rolle für Berechtigungen zum Senden von Protokollen an Logs zu CloudWatch erstellen. Wählen Sie Vorhanden, um eine vorhandene IAM-Rolle aus der Dropdown-Liste auszuwählen. Die Richtlinienanweisung für die neue oder vorhandene Rolle wird angezeigt, wenn Sie das Richtliniendokument erweitern. Weitere Informationen über diese Rolle finden Sie unter [Rollenrichtlinien-Dokument CloudTrail zur Verwendung von CloudWatch Logs zur Überwachung](#).

 Note

Beim Konfigurieren eines Trails können Sie einen S3-Bucket und ein Amazon-SNS-Thema auswählen, die zu einem anderen Konto gehören. Wenn Sie jedoch Ereignisse CloudTrail an eine CloudWatch Logs-Protokollgruppe übermitteln möchten, müssen Sie eine Protokollgruppe auswählen, die in Ihrem aktuellen Konto vorhanden ist.

9. Fügen Sie für Tags ein oder mehrere benutzerdefinierte Tags (Schlüssel-Wert-Paare) zu Ihrem Trail hinzu. Mithilfe von Tags können Sie sowohl Ihre CloudTrail Trails als auch die Amazon S3 S3-Buckets identifizieren, die CloudTrail Protokolldateien enthalten. Anschließend können Sie Ressourcengruppen für Ihre CloudTrail Ressourcen verwenden. Weitere Informationen finden Sie unter [AWS Resource Groups](#) und [Tags](#).
10. Wählen Sie auf der Seite Protokollereignisse auswählen die Ereignistypen aus, die Sie protokollieren möchten. Führen Sie unter Management events (Verwaltungsereignisse) die folgenden Schritte aus.
  - a. Wählen Sie für API-Aktivität aus, ob Ihr Trail Leseereignisse, Schreibereignisse oder beides protokollieren soll. Weitere Informationen finden Sie unter [Verwaltungsereignisse](#).
  - b. Wähle AWS KMS Ereignisse ausschließen, um Ereignisse aus deinem Trail herauszufiltern AWS Key Management Service (AWS KMS). Die Standardeinstellung besteht darin, alle AWS KMS -Ereignissen einzuschließen.


Die Option, AWS KMS Ereignisse zu protokollieren oder auszuschließen, ist nur verfügbar, wenn Sie Verwaltungsereignisse auf Ihrem Trail protokollieren. Wenn Sie sich dafür entscheiden, Verwaltungsereignisse nicht zu protokollieren, werden AWS KMS Ereignisse nicht protokolliert, und Sie können die Einstellungen für die AWS KMS Ereignisprotokollierung nicht ändern.

AWS KMS Aktionen wie EncryptDecrypt, und erzeugen GenerateDataKey in der Regel ein großes Volumen (mehr als 99%) von Ereignissen. Diese Aktionen werden nun als Leseereignisse protokolliert. Relevante AWS KMS Aktionen mit geringem Volumen wie DisableDelete, und ScheduleKey (die in der Regel weniger als 0,5% des AWS KMS Ereignisvolumens ausmachen) werden als Write-Ereignisse protokolliert.

Um Ereignisse mit hohem Volume wie Encrypt, Decrypt und GenerateDataKey auszuschließen, aber dennoch relevante Ereignisse wie Disable, Delete und


ScheduleKey zu protokollieren, wählen Sie Schreibverwaltungsereignisse protokollieren und deaktivieren Sie das Kontrollkästchen für AWS KMS -Ereignisse ausschließen.

- c. Klicken Sie auf Amazon-RDS-Daten-API ausschließen zum Filtern von Ereignissen der Amazon-Relational-Database-Service-Daten-API aus Ihrem Trail. Die Standardeinstellung besteht darin, alle Amazon-RDS-Daten-API-Ereignisse einzubeziehen. Weitere Informationen über die Amazon-RDS-Daten-API finden Sie unter [Protokollieren von Daten-API-Aufrufen mit AWS CloudTrail](#) im Amazon-RDS-Benutzerhandbuch für Aurora.
11. Zum Protokollieren von Datenereignissen wählen Sie Datenereignisse aus. Für die Protokollierung von Datenereignissen fallen zusätzliche Gebühren an. Weitere Informationen finden Sie unter [AWS CloudTrail -Preisgestaltung](#).

12.  **Important**

Die Schritte 12 bis 16 betreffen die Konfiguration von Datenereignissen mithilfe erweiterter Ereignisauswahlen, was die Standardeinstellung ist. Mithilfe erweiterter Ereignisauswahlen können Sie mehr [Datenereignistypen](#) konfigurieren und genau steuern, welche Datenereignisse in Ihrem Trail erfasst werden. Wenn Sie sich für die Verwendung grundlegender Ereignisauswahlen entschieden haben, führen Sie die Schritte unter [Konfigurieren von Datenereigniseinstellungen mithilfe grundlegender Ereignisauswahlen](#) aus und fahren Sie anschließend mit Schritt 17 dieses Verfahrens fort.

Wählen Sie für Datenereignistyp den Ressourcentyp aus, für den Sie Datenereignisse protokollieren möchten. Weitere Informationen zu den verfügbaren Datenereignistypen finden Sie unter [Datenereignisse](#).

 **Note**

Um Datenereignisse für von Lake Formation erstellte AWS Glue Tabellen zu protokollieren, wählen Sie Lake Formation.

13. Wählen Sie eine Protokollauswahlvorlage aus. CloudTrail enthält vordefinierte Vorlagen, die alle Datenereignisse für den Ressourcentyp protokollieren. Um eine benutzerdefinierte Protokoll-Selektorvorlage zu erstellen, wählen Sie Benutzerdefiniert aus.

 Note

Wenn Sie eine vordefinierte Vorlage für S3-Buckets auswählen, wird die Protokollierung von Datenereignissen für alle Buckets aktiviert, die sich derzeit in Ihrem AWS Konto befinden, sowie für alle Buckets, die Sie nach Abschluss der Erstellung des Trails erstellen. Es ermöglicht auch die Protokollierung von Datenereignisaktivitäten, die von einer beliebigen IAM-Identität in Ihrem AWS Konto ausgeführt werden, selbst wenn diese Aktivität in einem Bucket ausgeführt wird, der zu einem anderen Konto gehört. AWS Wenn der Trail nur für eine Region gilt, aktiviert die Auswahl einer vordefinierten Vorlage, die alle S3 Buckets protokolliert, die Datenereignisprotokollierung für alle Buckets in derselben Region wie Ihr Trail und alle Buckets, die Sie später in dieser Region erstellen. Es werden keine Protokollereignisse für Amazon-S3-Buckets in anderen Regionen in Ihrem AWS -Konto protokolliert.

Wenn Sie einen Trail für alle Regionen erstellen, aktiviert die Auswahl einer vordefinierten Vorlage für Lambda-Funktionen die Datenereignisprotokollierung für alle Funktionen, die sich derzeit in Ihrem AWS Konto befinden, sowie für alle Lambda-Funktionen, die Sie möglicherweise in einer beliebigen Region erstellen, nachdem Sie den Trail erstellt haben. Wenn Sie einen Trail für eine einzelne Region erstellen (mithilfe von AWS CLI), aktiviert diese Auswahl die Datenereignisprotokollierung für alle Funktionen, die sich derzeit in dieser Region in Ihrem AWS Konto befinden, sowie für alle Lambda-Funktionen, die Sie möglicherweise in dieser Region erstellen, nachdem Sie den Trail erstellt haben. Es wird keine Datenereignisprotokollierung für Lambda-Funktionen aktiviert, die in anderen Regionen erstellt wurden.


Das Protokollieren von Datenereignissen für alle Funktionen ermöglicht auch die Protokollierung von Datenereignisaktivitäten, die von einer beliebigen IAM-Identität in Ihrem AWS Konto ausgeführt werden, selbst wenn diese Aktivität für eine Funktion ausgeführt wird, die zu einem anderen AWS Konto gehört.

14. (Optional) Geben Sie unter Selektorname einen Namen ein, um Ihre Auswahl zu identifizieren. Der Selektorname ist ein optionaler, beschreibender Name für eine erweiterte Ereignisauswahl, z. B. „Datenereignisse nur für zwei S3-Buckets protokollieren“. Der Name des Selektors wird als Name in der erweiterten Ereignisauswahl aufgeführt und ist sichtbar, wenn Sie die JSON-Ansicht erweitern.
15. Erstellen Sie in den erweiterten Ereignisselektoren einen Ausdruck für die spezifischen Ressourcen, für die Sie Datenereignisse protokollieren möchten. Sie können diesen Schritt überspringen, wenn Sie eine vordefinierte Protokollvorlage verwenden.

a. Wählen Sie aus den folgenden Feldern.

- **readOnly**- readOnly kann auf den Wert oder gesetzt werden. true false  
Schreibgeschützte Datenereignisse sind Ereignisse, die den Zustand einer Ressource nicht ändern, z. B. Get\*- oder Describe\*-Ereignisse. Schreibereignisse fügen Ressourcen, Attribute oder Artefakte hinzu, ändern oder löschen sie, wie z. B. Put\*-, Delete\*- oder Write\*-Ereignisse. Um sowohl read- als auch write-Ereignisse zu protokollieren, fügen Sie keinen readOnly-Selektor hinzu.
- **eventName** – eventName kann einen beliebigen Operator verwenden. Sie können damit jedes Datenereignis, für das protokolliert wurde, ein- oder ausschließen CloudTrail, z. B. PutBucketPutItem, oderGetSnapshotBlock.
- **resources.ARN**- Sie können jeden Operator mit verwendenresources.ARN, aber wenn Sie equals oder ungleich verwenden, muss der Wert genau dem ARN einer gültigen Ressource des Typs entsprechen, den Sie in der Vorlage als Wert von resources.type angegeben haben.

In der folgenden Tabelle wird das gültige ARN-Format für alle resources.type-Werte aufgeführt.

 Note

Sie können das resources.ARN Feld nicht verwenden, um Ressourcentypen zu filtern, die keine ARNs haben.

resources.type	resources.ARN
AWS::DynamoDB::Table <sup>1</sup>	arn:partition :dynamodb : region:account_ID :table/table_name
AWS::Lambda::Function	arn:partition :lambda:region:account_ID :function: function_name

resources.type	resources.ARN
AWS::S3::Object <sup>2</sup>	<pre>arn:partition :s3::bucket_name / arn:partition :s3::bucket_name /object_or_file_name /</pre>
AWS::AppConfig::Configuration	<pre>arn:partition :appconfi g: region:account_ID :applicat ion/ application_ID /environm ent/ environment_ID /configur ation/ configuration_profile_ID</pre>
AWS::B2BI::Transformer	<pre>arn:partition :b2bi:region:account_I D :transformer/ transformer_ID</pre>
AWS::Bedrock::AgentAlias	<pre>arn:partition :bedrock: region:account_ID :agent-al ias/ agent_ID/alias_ID</pre>
AWS::Bedrock::KnowledgeBase	<pre>arn:partition :bedrock: region:account_ID :knowledge- base/knowledge_base_ID</pre>
AWS::Cassandra::Table	<pre>arn:partition :cassandr a: region:account_ID :keyspace / keyspace_name /table/table_name</pre>
AWS::CloudFront::KeyValueStore	<pre>arn:partition :cloudfro nt: region:account_ID :key-value- store/KVS_name</pre>
AWS::CloudTrail::Channel	<pre>arn:partition :cloudtra il: region:account_ID :channel/ channel_UUID</pre>

resources.type	resources.ARN
AWS::CodeWhisperer::Customization	arn: <i>partition</i> :codewhisperer: <i>region:account_ID</i> :customization/ <i>customization_ID</i>
AWS::CodeWhisperer::Profile	arn: <i>partition</i> :codewhisperer: <i>region:account_ID</i> :profile/ <i>profile_ID</i>
AWS::Cognito::IdentityPool	arn: <i>partition</i> :cognito-identity: <i>region:account_ID</i> :identitypool/ <i>identity_pool_ID</i>
AWS::DynamoDB::Stream	arn: <i>partition</i> :dynamodb: <i>region:account_ID</i> :table/ <i>table_name</i> /stream/ <i>date_time</i>
AWS::EC2::Snapshot	arn: <i>partition</i> :ec2: <i>region</i> ::snapshot/ <i>snapshot_ID</i>
AWS::EMRWALES::Workspace	arn: <i>partition</i> :emrwal: <i>region:account_ID</i> :workspace/ <i>workspace_name</i>
AWS::FinSpace::Environment	arn: <i>partition</i> :finspace: <i>region:account_ID</i> :environment/ <i>environment_ID</i>
AWS::Glue::Table	arn: <i>partition</i> :glue: <i>region:account_ID</i> :table/ <i>database_name</i> / <i>table_name</i>
AWS::GreengrassV2::ComponentVersion	arn: <i>partition</i> :greengrass: <i>region:account_ID</i> :components/ <i>component_name</i>

resources.type	resources.ARN
AWS::GreengrassV2::Deployment	<pre>arn:partition :greengrass: region:account_ID :deployments/ deployment_ID</pre>
AWS::GuardDuty::Detector	<pre>arn:partition :guardduty: region:account_ID :detector/ detector_ID</pre>
AWS::IoT::Certificate	<pre>arn:partition :iot:region:account_ID :cert/certificate_ID</pre>
AWS::IoT::Thing	<pre>arn:partition :iot:region:account_ID :thing/thing_ID</pre>
AWS::IoTSiteWise::Asset	<pre>arn:partition :iotsitewise: region:account_ID :asset/asset_ID</pre>
AWS::IoTSiteWise::TimeSeries	<pre>arn:partition :iotsitewise: region:account_ID :timeseries/ timeseries_ID</pre>
AWS::IoT TwinMaker::Entity	<pre>arn:partition :iottwinmaker: region:account_ID :workspace/ workspace_ID /entity/entity_ID</pre>
AWS::IoT TwinMaker::Workspace	<pre>arn:partition :iottwinmaker: region:account_ID :workspace/ workspace_ID</pre>



resources.type	resources.ARN
AWS::KendraRanking::ExecutionPlan	<pre>arn:<i>partition</i> :kendra-ranking: <i>region</i>:<i>account_ID</i> :rescore-execution-plan/ <i>rescore_execution_plan_ID</i></pre>
AWS::Kinesis::Stream	<pre>arn:<i>partition</i> :kinesis: <i>region</i>:<i>account_ID</i> :stream/<i>stream_name</i></pre>
AWS::Kinesis::StreamConsumer	<pre>arn:<i>partition</i> :kinesis: <i>region</i>:<i>account_ID</i> :<i>stream_type</i> /<i>stream_name</i> /consumer/ <i>consumer_name</i> :<i>consumer_creation_timestamp</i></pre>
AWS::KinesisVideo::Stream	<pre>arn:<i>partition</i> :kinesisvideo: <i>region</i>:<i>account_ID</i> :stream/<i>stream_name</i> /<i>creation_time</i></pre>
AWS::ManagedBlockchain::Network	<pre>arn:<i>partition</i> :managedblockchain:::networks/ <i>network_name</i></pre>
AWS::ManagedBlockchain::Node	<pre>arn:<i>partition</i> :managedblockchain: <i>region</i>:<i>account_ID</i> :nodes/<i>node_ID</i></pre>
AWS::MedicalImaging::Datastore	<pre>arn:<i>partition</i> :medical-imaging: <i>region</i>:<i>account_ID</i> :datastore/<i>data_store_ID</i></pre>
AWS::NeptuneGraph::Graph	<pre>arn:<i>partition</i> :neptune-graph: <i>region</i>:<i>account_ID</i> :graph/<i>graph_ID</i></pre>

resources.type	resources.ARN
AWS::PCACConnectorAD::Connector	<pre>arn:partition :pca-connector- ad: region:account_ID :connecto r/ connector_ID</pre>
AWS::QApps:QApp	<pre>arn:partition :qapps:region:account_I D :application/ application_UUID / qapp/qapp_UUID</pre>
AWS::QBusiness::Application	<pre>arn:partition :qbusines s: region:account_ID :applicat ion/ application_ID</pre>
AWS::QBusiness::DataSource	<pre>arn:partition :qbusines s: region:account_ID :applicat ion/ application_ID /index/index_ID/ data-source/ datasource_ID</pre>
AWS::QBusiness::Index	<pre>arn:partition :qbusines s: region:account_ID :applicat ion/ application_ID /index/index_ID</pre>
AWS::QBusiness::WebExperience	<pre>arn:partition :qbusines s: region:account_ID :applicat ion/ application_ID /web-expe rience/ web_experienc_ID</pre>
AWS::RDS::DBCluster	<pre>arn:partition :rds:region:account_I D :cluster/ cluster_name</pre>
AWS::S3::AccessPoint <sup>3</sup>	<pre>arn:partition :s3:region:account_I D :accesspoint/ access_point_name</pre>

resources.type	resources.ARN
AWS::S3ObjectLambda::AccessPoint	<pre>arn:<i>partition</i> :s3-object-lambda:   <i>region</i>:<i>account_ID</i> :accesspoint/ <i>access_point_name</i></pre>
AWS::S3Outposts::Object	<pre>arn:<i>partition</i> :s3-outposts: <i>region</i>:<i>account_ID</i> :<i>object_path</i></pre>
AWS::SageMaker::Endpoint	<pre>arn:<i>partition</i> :sagemaker:   r: <i>region</i>:<i>account_ID</i> :endpoint/ <i>endpoint_name</i></pre>
AWS::SageMaker::ExperimentTrialComponent	<pre>arn:<i>partition</i> :sagemaker:   r: <i>region</i>:<i>account_ID</i> :experiment-trial-component/ <i>experiment_trial_component_name</i></pre>
AWS::SageMaker::FeatureGroup	<pre>arn:<i>partition</i> :sagemaker:   r: <i>region</i>:<i>account_ID</i> :feature-group/ <i>feature_group_name</i></pre>
AWS::SCN::Instance	<pre>arn:<i>partition</i> :scn:<i>region</i>:<i>account_ID</i> :instance/ <i>instance_ID</i></pre>
AWS::ServiceDiscovery::Namespace	<pre>arn:<i>partition</i> :servicediscovery:   <i>region</i>:<i>account_ID</i> :namespace/ <i>namespace_ID</i></pre>
AWS::ServiceDiscovery::Service	<pre>arn:<i>partition</i> :servicediscovery:   <i>region</i>:<i>account_ID</i> :service/ <i>service_ID</i></pre>

resources.type	resources.ARN
AWS::SNS::PlatformEndpoint	<pre>arn:<i>partition</i> :sns:region:account_ID :endpoint/ endpoint_type /endpoint_name /endpoint_ID</pre>
AWS::SNS::Topic	<pre>arn:<i>partition</i> :sns:region:account_ID :topic_name</pre>
AWS::SQS::Queue	<pre>arn:<i>partition</i> :sqs:region:account_ID :queue_name</pre>
AWS::SSM::ManagedNode	<p>Der ARN muss in einem der folgenden Formate vorliegen:</p> <ul style="list-style-type: none"> <li>• arn:<i>partition</i> :ssm:region:account_ID :managed-instance/ <i>instance_ID</i></li> <li>• arn:<i>partition</i> :ec2:region:account_ID :instance / <i>instance_ID</i></li> </ul>
AWS::SSMMessages::ControlChannel	<pre>arn:<i>partition</i> :ssmmessages: region:account_ID :control-channel/ control_channel_ID</pre>
AWS::StepFunctions::StateMachine	<p>Der ARN muss in einem der folgenden Formate vorliegen:</p> <ul style="list-style-type: none"> <li>• arn:<i>partition</i> :states:region:account_ID :stateMachine: stateMachine_name</li> <li>• arn:<i>partition</i> :states:region:account_ID :stateMachine: stateMachine_name /label_name</li> </ul>

resources.type	resources.ARN
AWS::SWF::Domain	arn: <i>partition</i> :swf: <i>region</i> : <i>account_ID</i> :/ domain/ <i>domain_name</i>
AWS::ThinClient::Device	arn: <i>partition</i> :thinclie nt: <i>region</i> : <i>account_ID</i> :device/ <i>device_ID</i>
AWS::ThinClient::Environment	arn: <i>partition</i> :thinclie nt: <i>region</i> : <i>account_ID</i> :environm ent/ <i>environment_ID</i>
AWS::Timestream::Database	arn: <i>partition</i> :timestre am: <i>region</i> : <i>account_ID</i> :database / <i>database_name</i>
AWS::Timestream::Table	arn: <i>partition</i> :timestre am: <i>region</i> : <i>account_ID</i> :database / <i>database_name</i> /table/ <i>table_name</i>
AWS::VerifiedPermissions::PolicyStore	arn: <i>partition</i> :verifiedpermissio ns: <i>region</i> : <i>account_ID</i> :policy-s tore/ <i>policy_store_ID</i>

<sup>1</sup> Bei Tabellen mit aktivierten Streams enthält das `resources`-Feld im Datenereignis sowohl `AWS::DynamoDB::Stream` als auch `AWS::DynamoDB::Table`. Wenn Sie `AWS::DynamoDB::Table` als `resources.type` angeben, werden standardmäßig sowohl DynamoDB-Tabellen- als auch DynamoDB-Stream-Ereignisse protokolliert. Um [Streams-Ereignisse](#) auszuschließen, fügen Sie dem `eventName` Feld einen Filter hinzu.

<sup>2</sup> Um alle Datenereignisse für alle Objekte in einem bestimmten S3-Bucket zu protokollieren, verwenden Sie den `StartsWith`-Operator und geben Sie nur die Bucket-ARN als übereinstimmenden Wert an. Der abschließende Schrägstrich ist beabsichtigt; schließen Sie ihn nicht aus.

<sup>3</sup> Um Ereignisse zu allen Objekten in einem S3-Zugangspunkt zu protokollieren, empfehlen wir, nur die Zugangspunkt-ARN zu verwenden, den Objektpfad nicht einzuschließen und die `StartsWith`- oder `NotStartsWith`-Operatoren oder zu verwenden.

Weitere Informationen zu den ARN-Formaten von Datenereignisressourcen finden Sie unter [Actions, resources, and condition keys](#) (Aktionen, Ressourcen und Bedingungsschlüssel) im AWS Identity and Access Management -Benutzerhandbuch.

- b. Wählen Sie für jedes Feld + Bedingung aus, um beliebig viele Bedingungen hinzuzufügen, bis zu maximal 500 angegebene Werte für alle Bedingungen. Um beispielsweise Datenereignisse für zwei S3-Buckets von Datenereignissen auszuschließen, die in Ihrem Trail protokolliert werden, können Sie das Feld auf `Resources.ARN` festlegen, den Operator für `beginnt nicht mit` festlegen und dann entweder einen S3-Bucket-ARN einfügen oder nach den S3-Buckets suchen, für die Sie keine Ereignisse protokollieren möchten.

Um den zweiten S3-Bucket hinzuzufügen, wählen Sie + Bedingung und wiederholen Sie dann die vorherige Anweisung, indem Sie den ARN für einen anderen Bucket einfügen oder nach einem anderen Bucket suchen.

#### Note

Sie können maximal 500 Werte für alle Selektoren auf einem Trail haben. Dies schließt Arrays mit mehreren Werten für einen Selektor wie `eventName` ein. Wenn Sie einzelne Werte für alle Selektoren haben, können Sie einem Selektor maximal 500 Bedingungen hinzufügen.

Wenn Sie mehr als 15.000 Lambda-Funktionen in Ihrem Konto haben, können Sie beim Erstellen eines Trails nicht alle Funktionen in der CloudTrail Konsole anzeigen oder auswählen. Sie können jedoch alle Funktionen mit einer vordefinierten Selektorvorlage protokollieren, auch wenn sie nicht angezeigt werden. Wenn Sie Datenereignisse für bestimmte Funktionen protokollieren möchten, können Sie eine Funktion manuell hinzufügen, wenn Sie deren ARN kennen. Sie können die Erstellung des Trails auch in der Konsole abschließen und dann den Befehl `AWS CLI` und den `put-event-selectors` Befehl verwenden, um die Datenereignisprotokollierung für bestimmte Lambda-Funktionen zu konfigurieren.

Weitere Informationen finden Sie unter [Verwaltung von Wanderwegen mit dem AWS CLI](#).

- c. Wählen Sie + Feld, um bei Bedarf zusätzliche Felder hinzuzufügen. Um Fehler zu vermeiden, legen Sie keine widersprüchlichen oder doppelten Werte für Felder fest. Geben Sie beispielsweise nicht an, dass ein ARN in einem Selektor einem Wert entspricht, und geben Sie dann an, dass der ARN in einem anderen Selektor nicht dem gleichen Wert entspricht.
16. Um einen weiteren Datentyp hinzuzufügen, für den Datenereignisse protokolliert werden sollen, wählen Sie Datenereignistyp hinzufügen. Wiederholen Sie die Schritte 12 bis zu diesem Schritt, um erweiterte Ereignisselectoren für den Datenereignistyp zu konfigurieren.
17. Wählen Sie Insights-Ereignisse, wenn Ihr Trail CloudTrail Insights-Ereignisse protokollieren soll.

Wählen Sie unter Ereignistyp Insights-Ereignisse aus. Wählen Sie in Insights-Ereignisse API-Aufruftrate und/oder API-Fehlerrate aus. Sie müssen Schreib-Verwaltungsereignisse protokollieren, um Insights-Ereignisse für die API-Aufruftrate zu protokollieren. Sie müssen Lese- und Schreib-Verwaltungsereignisse protokollieren, um Insights-Ereignisse für die API-Fehlerrate zu protokollieren.

CloudTrail Insights analysiert Verwaltungsereignisse auf ungewöhnliche Aktivitäten und protokolliert Ereignisse, wenn Anomalien festgestellt werden. Standardmäßig werden für Trails keine Insights-Ereignisse protokolliert. Weitere Informationen zu Insights-Ereignissen erhalten Sie unter [Protokollieren von Insights-Ereignissen](#). Für die Protokollierung von Insights-Ereignissen fallen zusätzliche Gebühren an. [Preise finden Sie unter CloudTrail AWS CloudTrail Preisgestaltung](#).

Insights-Ereignisse werden in einen anderen Ordner übertragen, /CloudTrail-Insight der nach demselben S3-Bucket benannt ist, der auf der Seite mit den Trail-Details im Bereich Speicherort angegeben ist. CloudTrail erstellt das neue Präfix für Sie. Wenn beispielsweise Ihr aktueller S3-Ziel-Bucket den Namen S3bucketName/AWSLogs/CloudTrail/ hat, lautet der Name mit dem Präfix als Zusatz S3bucketName/AWSLogs/CloudTrail-Insight/.

18. Wenn Sie die Auswahl der zu protokollierenden Ereignistypen abgeschlossen haben, wählen Sie Weiter aus.
19. Überprüfen Sie auf der Seite Prüfen und erstellen Ihre Auswahl. Wählen Sie Bearbeiten in einem Abschnitt, um die in diesem Abschnitt angezeigten Trail-Einstellungen zu ändern. Wenn Sie bereit sind, den Trail zu erstellen, wählen Sie Trail erstellen.

20. Der neue Trail wird auf der Seite Trails angezeigt. Es kann bis zu 24 Stunden dauern, bis ein Organisations-Trail in allen Regionen und in allen Mitgliedskonten erstellt wird. Auf der Seite Trails werden die Trails in Ihrem Konto aus allen Regionen angezeigt. Veröffentlicht in etwa 5 Minuten CloudTrail Protokolldateien, in denen die in Ihrer Organisation getätigten AWS API-Aufrufe aufgeführt sind. Sie können die Protokolldateien in dem von Ihnen angegebenen Amazon-S3-Bucket anzeigen.

#### Note

Es ist nicht möglich, einen Trail nach dem Erstellen umzubenennen. Stattdessen können Sie den Trail löschen und einen neuen erstellen.

## Nächste Schritte

Nach der Trail-Erstellung können Sie zu dem Trail zurückkehren, um Änderungen vorzunehmen:

- Ändern Sie die Konfiguration Ihres Trails, indem Sie ihn bearbeiten. Weitere Informationen finden Sie unter [Aktualisieren eines Trails](#).
- Konfigurieren Sie den Amazon-S3-Bucket bei Bedarf so, dass bestimmte Benutzer in Mitgliedskonten die Protokolldateien für die Organisation lesen können. Weitere Informationen finden Sie unter [CloudTrail Protokolldateien zwischen AWS Konten teilen](#).
- Konfigurieren Sie CloudTrail das Senden von Protokolldateien an CloudWatch Logs. Weitere Informationen finden Sie unter [Ereignisse an CloudWatch Logs senden](#) und [das Element CloudWatch Protokolle](#) unter [Vorbereiten der Erstellung eines Trails für Ihre Organisation](#).

#### Note

Nur das Verwaltungskonto kann eine Protokollgruppe „CloudWatch Logs“ für einen Organization Trail konfigurieren.

- Erstellen Sie eine Tabelle zur Ausführung einer Abfrage in Amazon Athena, um die AWS -Service-Aktivitäten zu analysieren. Weitere Informationen finden Sie unter [Erstellen einer Tabelle für CloudTrail Protokolle in der CloudTrail Konsole](#) im [Amazon Athena Athena-Benutzerhandbuch](#).
- Fügen Sie benutzerdefinierte Tags (Schlüssel-Wert-Paare) zum Trail hinzu.
- Kehren Sie zur Seite Trails zurück und wählen Sie Create trail (Trail erstellen), um einen anderen Trail zu erstellen.



**Note**

Beim Konfigurieren eines Trails können Sie einen Amazon-S3-Bucket und ein SNS-Thema auswählen, die zu einem anderen Konto gehören. Wenn Sie jedoch Ereignisse CloudTrail an eine CloudWatch Logs-Protokollgruppe übermitteln möchten, müssen Sie eine Protokollgruppe auswählen, die in Ihrem aktuellen Konto vorhanden ist.

## Erstellen eines Trails für eine Organisation mit dem AWS Command Line Interface

Sie können mit der AWS CLI einen Organisations-Trail erstellen. Das AWS CLI wird regelmäßig mit zusätzlichen Funktionen und Befehlen aktualisiert. Um den Erfolg sicherzustellen, stellen Sie sicher, dass Sie eine aktuelle Version installiert oder auf eine aktuelle AWS CLI Version aktualisiert haben, bevor Sie beginnen.

**Note**

Die Beispiele in diesem Abschnitt gelten speziell für das Erstellen und Aktualisieren von Organisations-Trails. Beispiele für die Verwendung von AWS CLI zur Verwaltung von Pfaden finden Sie unter [Verwaltung von Wanderwegen mit dem AWS CLI](#) und [Konfiguration der CloudWatch Protokollüberwachung mit dem AWS CLI](#). Wenn Sie einen Organisationspfad mit dem erstellen oder aktualisieren AWS CLI, müssen Sie ein AWS CLI Profil im Verwaltungskonto oder ein delegiertes Administratorkonto mit ausreichenden Berechtigungen verwenden. Wenn Sie einen Organisations-Trail in einen Nicht-Organisations-Trail umwandeln, müssen Sie das Verwaltungskonto der Organisation verwenden. Sie müssen den für einen Organisationstrail verwendeten Amazon-S3-Bucket mit ausreichenden Berechtigungen konfigurieren.

## Erstellen oder Aktualisieren eines Amazon-S3-Buckets zum Speichern der Protokolldateien für einen Organisations-Trail

Sie müssen einen Amazon-S3-Bucket für den Empfang der Protokolldateien für einen Organisationstrail angeben. Dieser Bucket muss über eine Richtlinie verfügen, die es CloudTrail ermöglicht, die Protokolldateien für die Organisation in den Bucket zu übernehmen.

Im Folgenden finden Sie eine Beispielrichtlinie für einen Amazon S3 S3-Bucket mit dem Namen *myOrganizationBucket*, der dem Verwaltungskonto der Organisation gehört. Ersetzen Sie *Region myOrganizationBucket*, *ManagementAccountID*, *TrailName* und *OrganizationId* durch die Werte für Ihre Organisation

Diese Bucket-Richtlinie besteht aus drei Anweisungen:

- Die erste Anweisung ermöglicht CloudTrail den Aufruf der Amazon S3 GetBucketAcl S3-Aktion im Amazon S3 S3-Bucket.
- Die zweite Anweisung ermöglicht die Protokollierung des Ereignisses für den Fall, dass der Trail von einem Organisations-Trail zu einem kontospezifischen Trail geändert wird.
- Die dritte Anweisung ermöglicht die Protokollierung eines Organisations-Trails.

Die Beispielrichtlinie enthält einen `aws:SourceArn`-Bedingungsschlüssel für die Richtlinie von Amazon-S3-Bucket. Der globale IAM-Bedingungsschlüssel `aws:SourceArn` trägt dazu bei, dass nur für einen oder mehrere bestimmte Pfade in den S3-Bucket CloudTrail geschrieben wird. In einem Organisations-Trail muss der Wert von `aws:SourceArn` ein Trail-ARN sein, der im Besitz des Verwaltungskontos ist und die Verwaltungskonto-ID verwendet.

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Sid": "AWSCloudTrailAclCheck20150319",
      "Effect": "Allow",
      "Principal": {
        "Service": [
          "cloudtrail.amazonaws.com"
        ]
      },
      "Action": "s3:GetBucketAcl",
      "Resource": "arn:aws:s3:::myOrganizationBucket",
      "Condition": {
        "StringEquals": {
          "aws:SourceArn":
            "arn:aws:cloudtrail:region:managementAccountID:trail/trailName"
        }
      }
    },
    {
```

```

    "Sid": "AWSCloudTrailWrite20150319",
    "Effect": "Allow",
    "Principal": {
      "Service": [
        "cloudtrail.amazonaws.com"
      ]
    },
    "Action": "s3:PutObject",
    "Resource": "arn:aws:s3:::myOrganizationBucket/AWSLogs/managementAccountID/
*",
    "Condition": {
      "StringEquals": {
        "s3:x-amz-acl": "bucket-owner-full-control",
        "aws:SourceArn":
"arn:aws:cloudtrail:region:managementAccountID:trail/trailName"
      }
    }
  },
  {
    "Sid": "AWSCloudTrailOrganizationWrite20150319",
    "Effect": "Allow",
    "Principal": {
      "Service": [
        "cloudtrail.amazonaws.com"
      ]
    },
    "Action": "s3:PutObject",
    "Resource": "arn:aws:s3:::myOrganizationBucket/AWSLogs/o-organizationID/*",
    "Condition": {
      "StringEquals": {
        "s3:x-amz-acl": "bucket-owner-full-control",
        "aws:SourceArn":
"arn:aws:cloudtrail:region:managementAccountID:trail/trailName"
      }
    }
  }
]
}

```

Diese Beispielrichtlinie sieht nicht vor, dass beliebige Benutzer über Mitgliedskonten auf die für die Organisation erstellten Protokolldateien zugreifen können. Standardmäßig ist der Zugriff auf die Protokolldateien der Organisation nur über das Verwaltungskonto möglich. Weitere Informationen

dazu, wie Sie IAM-Benutzern in Mitgliedskonten den Lesezugriff auf den Amazon-S3-Bucket gewähren, finden Sie unter [CloudTrail Protokolldateien zwischen AWS Konten teilen](#).

## Aktivierung CloudTrail als vertrauenswürdiger Dienst in AWS Organizations

Sie müssen zunächst in Organizations alle Funktionen aktivieren, bevor Sie einen Organisations-Trail erstellen können. Weitere Informationen finden Sie unter [Aktivieren aller Funktionen in der Organisation](#). Alternativ führen Sie anhand eines Profils mit ausreichenden Berechtigungen im Verwaltungskonto den folgenden Befehl aus:

```
aws organizations enable-all-features
```

Nachdem Sie alle Funktionen aktiviert haben, müssen Sie Organizations so konfigurieren, dass es sich um einen vertrauenswürdigen Dienst handelt. CloudTrail

Um die vertrauenswürdige Dienstbeziehung zwischen AWS Organizations und herzustellen CloudTrail, öffnen Sie ein Terminal oder eine Befehlszeile und verwenden Sie ein Profil im Verwaltungskonto. Führen Sie den Befehl `aws organizations enable-aws-service-access` wie im folgenden Beispiel beschrieben aus.

```
aws organizations enable-aws-service-access --service-principal  
cloudtrail.amazonaws.com
```

## Verwendung von „create-trail“

Erstellen eines für alle Regionen geltenden Organisations-Trails

Zum Erstellen eines für alle Regionen geltenden Organisations-Trails verwenden Sie die Optionen `--is-organization-trail` und `--is-multi-region-trail`.

### Note

Wenn Sie einen Organisationspfad mit dem erstellen AWS CLI, müssen Sie ein AWS CLI Profil im Verwaltungskonto oder ein delegiertes Administratorkonto mit ausreichenden Berechtigungen verwenden.

Im folgenden Beispiel wird ein Organisations-Trail angelegt, der Protokolle aus allen Regionen an einen vorhandenen Bucket mit dem Namen *my-bucket* übermittelt:

```
aws cloudtrail create-trail --name my-trail --s3-bucket-name my-bucket --is-organization-trail --is-multi-region-trail
```

Die Parameter `IsOrganizationTrail` und `IsMultiRegionTrail` in der Ausgabe sind auf `true` festgelegt, um zu bestätigen, dass Ihr Trail in allen Regionen vorhanden ist:

```
{
  "IncludeGlobalServiceEvents": true,
  "Name": "my-trail",
  "TrailARN": "arn:aws:cloudtrail:us-east-2:123456789012:trail/my-trail",
  "LogFileValidationEnabled": false,
  "IsMultiRegionTrail": true,
  "IsOrganizationTrail": true,
  "S3BucketName": "my-bucket"
}
```

#### Note

Führen Sie den Befehl `start-logging` aus, um die Protokollierung für den Trail zu starten. Weitere Informationen finden Sie unter [Anhalten und Starten der Protokollierung für einen Trail](#).

## Erstellen eines Organisations-Trails als Trail für eine einzelne Region

Mit dem folgenden Befehl wird ein Organisationspfad erstellt, der nur Ereignisse in einem einzigen Pfad protokolliert AWS-Region, der auch als Einzelregionspfad bezeichnet wird. Die AWS Region, in der Ereignisse protokolliert werden, ist die Region, die im Konfigurationsprofil für angegeben ist. AWS CLI

```
aws cloudtrail create-trail --name my-trail --s3-bucket-name my-bucket --is-organization-trail
```

Weitere Informationen finden Sie unter [Benennungsanforderungen](#).

Beispielausgabe:

```
{
  "IncludeGlobalServiceEvents": true,
  "Name": "my-trail",
```

```
"TrailARN": "arn:aws:cloudtrail:us-east-2:123456789012:trail/my-trail",
"LogFileValidationEnabled": false,
"IsMultiRegionTrail": false,
"IsOrganizationTrail": true,
"S3BucketName": "my-bucket"
}
```

Standardmäßig erstellt der Befehl `create-trail` einen Trail für eine einzelne Region, der die Validierung von Protokolldateien nicht aktiviert.

#### Note

Führen Sie den Befehl `start-logging` aus, um die Protokollierung für den Trail zu starten.

## update-trail ausführen, um einen Organisations-Trail zu aktualisieren

Sie können mit dem Befehl `update-trail` die Konfigurationseinstellungen eines Organisations-Trails ändern oder einen vorhandenen Trail für ein einzelnes AWS -Konto auf eine gesamte Organisation anwenden. Beachten Sie, dass Sie den Befehl `update-trail` nur in der Region ausführen können, in der der Trail erstellt wurde.

#### Note

Wenn Sie das AWS CLI oder eines der AWS SDKs verwenden, um einen Trail zu aktualisieren, stellen Sie sicher, dass die Bucket-Richtlinie des Trails aktiviert ist up-to-date. Weitere Informationen finden Sie unter [Erstellen eines Trails für eine Organisation mit dem AWS Command Line Interface](#).

Wenn Sie einen Organisationspfad mit dem aktualisieren AWS CLI, müssen Sie ein AWS CLI Profil im Verwaltungskonto oder im delegierten Administratorkonto mit ausreichenden Berechtigungen verwenden. Wenn Sie einen Organisations-Trail in ein Nicht-Organisations-Trail umwandeln möchten, müssen Sie das Verwaltungskonto der Organisation verwenden, da dieses Konto der Besitzer aller Organisationsressourcen ist.

CloudTrail aktualisiert die Organisationspfade in Mitgliedskonten, auch wenn eine Ressourcenvalidierung fehlschlägt. Zu den Beispielen für fehlgeschlagene Überprüfungen gehören:

- eine falsche Amazon S3 S3-Bucket-Richtlinie
- eine falsche Amazon SNS SNS-Themenrichtlinie

- Unfähigkeit, an eine CloudWatch Logs-Protokollgruppe zu liefern
- unzureichende Rechte zur Verschlüsselung mit einem KMS-Schlüssel

Ein Mitgliedskonto mit CloudTrail Berechtigungen kann alle Validierungsfehler für einen Organisationspfad anzeigen, indem es die Detailseite des Trails in der CloudTrail Konsole aufruft oder den AWS CLI [get-trail-status](#) Befehl ausführt.

## Anwenden eines vorhandenen Trails auf eine Organisation

Um einen vorhandenen Trail so zu ändern, dass er auch für eine Organisation und nicht für ein einzelnes AWS Konto gilt, fügen Sie die `--is-organization-trail` Option hinzu, wie im folgenden Beispiel gezeigt.

### Note

Verwenden Sie das Verwaltungskonto, um einen vorhandenen Nicht-Organisations-Trail in einen Organisations-Trail umzuwandeln.

```
aws cloudtrail update-trail --name my-trail --is-organization-trail
```

Um zu bestätigen, dass der Trail jetzt für die Organisation gilt, hat der `IsOrganizationTrail`-Parameter in der Ausgabe den Wert `true`.

```
{
  "IncludeGlobalServiceEvents": true,
  "Name": "my-trail",
  "TrailARN": "arn:aws:cloudtrail:us-east-2:123456789012:trail/my-trail",
  "LogFileValidationEnabled": false,
  "IsMultiRegionTrail": true,
  "IsOrganizationTrail": true,
  "S3BucketName": "my-bucket"
}
```

Im vorherigen Beispiel wurde der Trail so konfiguriert, dass er für alle Regionen gilt (`"IsMultiRegionTrail": true`). Ein Trail, der nur für eine einzelne Region gilt, würde in der Ausgabe den Wert `"IsMultiRegionTrail": false` anzeigen.

Umwandeln eines für eine Region geltenden Organisations-Trails, damit er für alle Regionen gilt

Um einen vorhandenen Organisations-Trail so zu ändern, dass er für alle Regionen gilt, fügen Sie die Option `--is-multi-region-trail` wie im folgenden Beispiel gezeigt hinzu.

```
aws cloudtrail update-trail --name my-trail --is-multi-region-trail
```

Um zu bestätigen, dass der Trail jetzt für alle Regionen gilt, hat der `IsMultiRegionTrail`-Parameter in der Ausgabe den Wert `true`.

```
{
  "IncludeGlobalServiceEvents": true,
  "Name": "my-trail",
  "TrailARN": "arn:aws:cloudtrail:us-east-2:123456789012:trail/my-trail",
  "LogFileValidationEnabled": false,
  "IsMultiRegionTrail": true,
  "IsOrganizationTrail": true,
  "S3BucketName": "my-bucket"
}
```

## Fehlerbehebung

Dieser Abschnitt enthält Informationen zur Behebung von Problemen mit einem Organization Trail.

Themen

- [CloudTrail übermittelt keine Ereignisse](#)
- [CloudTrail sendet keine Amazon SNS SNS-Benachrichtigungen für ein Mitgliedskonto in einer Organisation](#)

### CloudTrail übermittelt keine Ereignisse

Wenn CloudTrail keine CloudTrail Protokolldateien an den Amazon S3-Bucket gesendet werden

Prüfen Sie, ob ein Problem mit dem S3-Bucket vorliegt.

- Überprüfe von der CloudTrail Konsole aus die Detailseite des Trails. Wenn es ein Problem mit dem S3-Bucket gibt, enthält die Detailseite eine Warnung, dass die Lieferung an den S3-Bucket fehlgeschlagen ist.



- Führen Sie von AWS CLI der aus den [get-trail-status](#)Befehl aus. Wenn ein Fehler auftritt, enthält die Befehlsausgabe das LatestDeliveryError Feld, das alle Amazon S3 S3-Fehler anzeigt, die beim Versuch, Protokolldateien an den angegebenen Bucket zu liefern, CloudTrail aufgetreten sind. Dieser Fehler tritt nur auf, wenn ein Problem mit dem Ziel-S3-Bucket vorliegt, und tritt nicht bei Anfragen auf, bei denen das Timeout auftritt. Um das Problem zu beheben, korrigieren Sie die Bucket-Richtlinie, sodass in den Bucket geschrieben werden CloudTrail kann, oder erstellen Sie einen neuen Bucket und rufen Sie dann auf, `update-trail` um den neuen Bucket anzugeben. Informationen zur Organisations-Bucket-Richtlinie finden [Sie unter Erstellen oder Aktualisieren eines Amazon S3 S3-Buckets, der zum Speichern der Protokolldateien für einen Organisation-Trail verwendet](#) werden soll.

Wenn CloudTrail es sich nicht um die Übermittlung von Protokollen an CloudWatch Logs handelt

Prüfen Sie, ob ein Problem mit der Konfiguration der Rollenrichtlinie „ CloudWatch Logs“ vorliegt.

- Überprüfe von der CloudTrail Konsole aus die Detailseite des Trails. Wenn es ein Problem mit den CloudWatch Protokollen gibt, enthält die Detailseite eine Warnung, die darauf hinweist, dass die Übertragung der CloudWatch Protokolle fehlgeschlagen ist.
- Führen Sie von AWS CLI der aus den [get-trail-status](#)Befehl aus. Wenn ein Fehler auftritt, enthält die Befehlsausgabe das LatestCloudWatchLogsDeliveryError Feld, in dem alle CloudWatch Logs-Fehler angezeigt werden, die beim Versuch, Logs an Logs zu CloudWatch übermitteln, CloudTrail aufgetreten sind. Korrigieren Sie die Rollenrichtlinie „ CloudWatch Logs“, um das Problem zu beheben. Informationen zur Rollenrichtlinie „ CloudWatch Logs“ finden Sie unter [Rollenrichtlinien-Dokument CloudTrail zur Verwendung von CloudWatch Logs zur Überwachung](#).

Wenn Sie in einem Organisationspfad keine Aktivitäten für ein Mitgliedskonto sehen

Wenn du in einem Organisationspfad keine Aktivitäten für ein Mitgliedskonto siehst, überprüfe Folgendes:

- Schau in der Heimatregion des Trails nach, ob es sich um eine Region handelt, in der du dich anmelden kannst

Obwohl die meisten Regionen standardmäßig für deine aktiviert AWS-Regionen sind AWS-Konto, musst du bestimmte Regionen (auch als Opt-in-Regionen bezeichnet) manuell aktivieren. Informationen darüber, welche Regionen standardmäßig aktiviert sind, finden Sie im AWS Account Management Referenzhandbuch unter [Überlegungen vor dem Aktivieren und Deaktivieren von](#)

[Regionen](#). Eine Liste der CloudTrail unterstützten Regionen finden Sie unter [CloudTrail unterstützte Regionen](#).

Wenn es sich bei dem Organization Trail um einen Multi-Region-Trail handelt und es sich bei der Heimatregion um eine Opt-in-Region handelt, senden Mitgliedskonten keine Aktivitäten an den Organisationspfad, es sei denn, sie entscheiden sich für den AWS-Region Ort, an dem der Multi-Region-Trail erstellt wurde. Wenn du beispielsweise einen Trail mit mehreren Regionen erstellst und die Region Europa (Spanien) als Heimatregion für den Trail auswählst, senden nur Mitgliedskonten, die die Region Europa (Spanien) für ihr Konto aktiviert haben, ihre Kontoaktivitäten an den Organisationspfad. Um das Problem zu lösen, aktivieren Sie die Opt-in-Region in jedem Mitgliedskonto Ihrer Organisation. Informationen zur Aktivierung einer Opt-in-Region finden Sie im AWS Account Management Referenzhandbuch unter [Aktivieren oder Deaktivieren einer Region in Ihrer Organisation](#).

- Prüfen Sie, ob die ressourcenbasierte Richtlinie der Organisation mit der servicebezogenen Rollenrichtlinie kollidiert CloudTrail

CloudTrail verwendet die mit dem Dienst verknüpfte Rolle, die zur Unterstützung von Organisationstrails benannt [AWSServiceRoleForCloudTrail](#) ist. Diese dienstbezogene Rolle ermöglicht CloudTrail das Ausführen von Aktionen an Unternehmensressourcen, wie z. `organizations:DescribeOrganization` Wenn die ressourcenbasierte Richtlinie der Organisation eine Aktion ablehnt, die in der Richtlinie für dienstbezogene Rollen zulässig ist, CloudTrail kann die Aktion nicht ausgeführt werden, obwohl sie in der Richtlinie für dienstbezogene Rollen zulässig ist. Um das Problem zu lösen, korrigieren Sie die ressourcenbasierte Richtlinie der Organisation, sodass Aktionen nicht verweigert werden, die in der dienstbezogenen Rollenrichtlinie zulässig sind.

## CloudTrail sendet keine Amazon SNS SNS-Benachrichtigungen für ein Mitgliedskonto in einer Organisation

Wenn ein Mitgliedskonto mit einem AWS Organizations Organisations-Trail keine Amazon SNS SNS-Benachrichtigungen sendet, liegt möglicherweise ein Problem mit der Konfiguration der SNS-Themenrichtlinie vor. CloudTrail erstellt Organisationstrails in Mitgliedskonten, auch wenn eine Ressourcenvalidierung fehlschlägt. Beispielsweise enthält das SNS-Thema des Organisationstrails nicht alle Mitgliedskonto-IDs. Wenn die SNS-Themenrichtlinie falsch ist, tritt ein Autorisierungsfehler auf.

Um zu überprüfen, ob die SNS-Themenrichtlinie eines Trails einen Autorisierungsfehler aufweist:

- Überprüfen Sie die CloudTrail Konsole auf die Detailseite des Trails. Wenn die Autorisierung fehlschlägt, enthält die Detailseite eine Warnung `SNS authorization failed` und weist darauf hin, dass die SNS-Themenrichtlinie repariert werden muss.
- Führen Sie von der AWS CLI aus den [get-trail-status](#) Befehl aus. Wenn die Autorisierung fehlschlägt, enthält die Befehlsausgabe das `LastNotificationError` Feld mit dem Wert `AuthorizationError`. Korrigieren Sie die Amazon SNS SNS-Themenrichtlinie, um das Problem zu beheben. Informationen zur Amazon SNS SNS-Themenrichtlinie finden Sie unter [Amazon SNS SNS-Themenrichtlinie für CloudTrail](#).

Weitere Informationen zu SNS-Themen und deren Abonnement finden Sie unter [Erste Schritte mit Amazon SNS im Amazon Simple Notification Service Developer Guide](#).

## CloudTrail Insights-Ereignisse für Wanderwege anzeigen

Nachdem Sie CloudTrail Insights on a Trail aktiviert haben, können Sie sich Insights-Ereignisse von bis zu 90 Tagen über die CloudTrail Konsole oder das ansehen AWS CLI. In diesem Abschnitt wird beschrieben, wie Sie eine Datei mit Insights-Ereignissen anzeigen, nachschlagen und herunterladen. Informationen zur Verwendung der `LookupEvents` API zum Abrufen von Informationen aus CloudTrail Ereignissen finden Sie in der [AWS CloudTrail API-Referenz](#). Weitere Informationen zu CloudTrail Insights finden Sie [Protokollieren von Insights-Ereignissen](#) in diesem Handbuch.

Informationen zum Erstellen eines Trails finden Sie unter [Erstellen eines Trails](#) und [CloudTrail Logdateien abrufen und einsehen](#).

### Note

Um Insights-Ereignisse anhand des API-Aufrufvolumens zu protokollieren, muss der Trail `write`-Verwaltungsereignisse protokollieren. Um Insights-Ereignisse anhand der API-Fehlerrate zu protokollieren, muss der Trail `read`- oder `write`-Verwaltungsereignisse protokollieren.

### Themen

- [CloudTrail Insights-Ereignisse für Trails in der CloudTrail Konsole anzeigen](#)
- [CloudTrail Insights-Ereignisse für Trails anzeigen mit dem AWS CLI](#)

## CloudTrail Insights-Ereignisse für Trails in der CloudTrail Konsole anzeigen

Nachdem Sie CloudTrail Insights-Ereignisse auf einem Trail aktiviert haben, generiert CloudTrail When ungewöhnliche API- oder Fehlerratenaktivitäten, CloudTrail generiert Insights-Ereignisse und zeigt sie auf den Seiten Dashboard und Insights in der an AWS Management Console. Sie können die Insights-Ereignisse in der Konsole anzeigen und die Fehlerbehebung für die ungewöhnlichen Aktivitäten durchführen. In der Konsole werden die letzten 90 Tage der Insights-Ereignisse angezeigt. Sie können Insights-Ereignisse auch mithilfe der AWS CloudTrail Konsole herunterladen. Sie können Ereignisse mithilfe der AWS SDKs oder programmgesteuert nachschlagen. AWS Command Line Interface Weitere Informationen zu CloudTrail Insights-Ereignissen finden Sie [Protokollieren von Insights-Ereignissen](#) in diesem Handbuch.

### Note

Um Insights-Ereignisse anhand des API-Aufruf-Volumens zu protokollieren, muss der Trail `write`-Verwaltungsereignisse protokollieren. Um Insights-Ereignisse auf der API-Fehlerrate zu protokollieren, muss der Trail `read`- oder `write`-Verwaltungsereignisse protokollieren.

Nachdem Insights-Ereignisse protokolliert wurden, werden die sie 90 Tage lang auf der Seite Insights angezeigt. Sie können Ereignisse nicht manuell von der Seite Insights löschen. Da Sie [einen Trail erstellen](#) müssen, bevor Sie CloudTrail Insights aktivieren können, können Sie Insights-Ereignisse, die in Ihrem Trail protokolliert wurden, anzeigen, solange Sie sie in dem S3-Bucket speichern, der in Ihren Trail-Einstellungen konfiguriert ist.

Überwachen Sie mit Amazon CloudWatch Logs Ihre Traillogs und lassen Sie sich benachrichtigen, wenn bestimmte Insights-Ereignisse auftreten. Weitere Informationen finden Sie unter [Überwachung von CloudTrail Protokolldateien mit Amazon CloudWatch Logs](#).

So zeigen Sie Insights-Ereignisse an

CloudTrail Insights-Ereignisse müssen auf Ihrem Trail aktiviert sein, damit Insights-Ereignisse in der Konsole angezeigt werden. Wenn ungewöhnliche Aktivitäten festgestellt werden, kann es bis CloudTrail zu 36 Stunden dauern, bis die ersten Insights-Ereignisse angezeigt werden.

1. Melden Sie sich bei der an AWS Management Console und öffnen Sie die CloudTrail Konsole unter <https://console.aws.amazon.com/cloudtrail/home/>.

2. Wählen Sie im Navigationsbereich die Option Dashboard aus, um die fünf letzten Insights-Ereignisse anzuzeigen, oder Insights, um alle Insights-Ereignisse anzuzeigen, die in den letzten 90 Tagen unter Ihrem Konto protokolliert wurden.

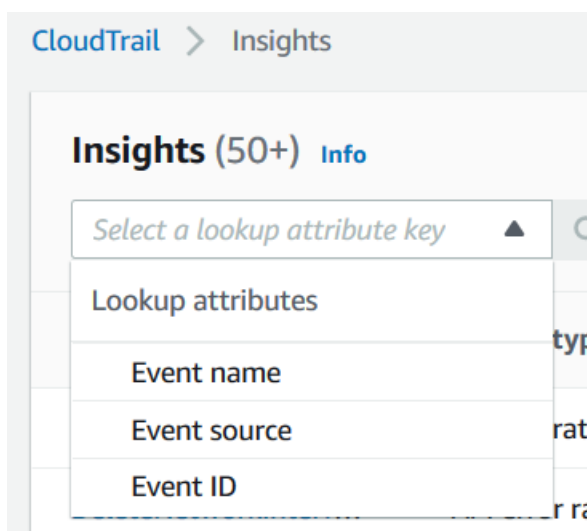
Auf der Seite Insights können Sie Insights-Ereignisse nach bestimmten Kriterien filtern, z. B. nach API-Ereignisquelle, Ereignisname und Ereignis-ID, und die angezeigten Ereignisse auf einen bestimmten Zeitraum beschränken. Weitere Informationen zum Filtern von Insights-Ereignissen erhalten Sie unter [Filtern von Insights-Ereignissen](#).

## Inhalt

- [Filtern von Insights-Ereignissen](#)
- [Details zu Insights-Ereignissen anzeigen](#)
- [Zoomen, Schwenken und Herunterladen des Diagramms](#)
- [Ändern der Einstellungen für die Zeitspanne des Diagramms](#)
- [Herunterladen von Insights-Ereignissen](#)

## Filtern von Insights-Ereignissen

Standardmäßig werden Ereignisse unter Insights in umgekehrter chronologischer Reihenfolge angezeigt. Die neuesten Insights-Ereignisse, sortiert nach Startzeit des Ereignisses, werden oben angezeigt. In der folgenden Liste werden die verfügbaren Attribute beschrieben. Sie können nach den ersten drei Attributen filtern: Ereignisname, Ereignisquelle und Ereignis-ID.



## Ereignisname

Der Name des Ereignisses, in der Regel die AWS API, auf der ungewöhnliche Aktivitäten aufgezeichnet wurden.

## Insight-Typ

Der Typ des CloudTrail Insights-Ereignisses, bei dem es sich entweder um die API-Aufrufrate oder die API-Fehlerrate handelt. Der Insight-Typ API-Aufrufrate analysiert schreibgeschützte Verwaltungs-API-Aufrufe, die pro Minute im Vergleich zu einem Baseline-API-Aufrufvolumen aggregiert werden. Der Insights-Typ API-Fehlerrate analysiert Verwaltungs-API-Aufrufe, die zu Fehlercodes führen. Der Fehler wird angezeigt, wenn der API-Aufruf fehlschlägt.

## Ereignisquelle

Der AWS Dienst, an den die Anfrage gestellt wurde, z. B. `iam.amazonaws.com` oder `s3.amazonaws.com`. Sie können eine Liste von Ereignisquellen durchblättern, nachdem Sie den Filter Event source ausgewählt haben.

## Ereignis-ID

Die ID des Insights-Ereignisses. Ereignis-IDs werden nicht in der Tabelle auf der Seite Insights angezeigt, aber es handelt sich um ein Attribut, nach dem Sie Insights-Ereignisse filtern können. Die Ereignis-IDs von Verwaltungsereignissen, die zum Generieren von Insights-Ereignisse analysiert werden, unterscheiden sich von den Ereignis-IDs von Insights-Ereignisse.

## Startzeit des Ereignisses

Der Zeitpunkt des Beginns eines Insights-Ereignisses, gemessen ab der ersten Minute, in der ungewöhnliche Aktivitäten aufgezeichnet wurden. Dieses Attribut wird in der Insights-Tabelle angezeigt, aber Sie können nicht nach der Startzeit des Ereignisses in der Konsole filtern.

## Baseline-Durchschnitt

Das normale Muster der API-Aufruf- oder Fehlerraten-Aktivität. Der Baseline-Durchschnitt wird in den sieben Tagen vor Beginn eines Insights-Ereignisses berechnet. Der Wert der Basisdauer — der Zeitraum, in dem die normale Aktivität anhand von APIs CloudTrail analysiert wird — beträgt zwar ungefähr sieben Tage, CloudTrail rundet die Basisdauer jedoch auf eine ganze Ganzzahl ab, sodass die genaue Basisdauer variieren kann.

## Insight-Durchschnitt

Die durchschnittliche Anzahl von Aufrufen einer API oder die durchschnittliche Anzahl eines bestimmten Fehlers, der bei Aufrufen einer API zurückgegeben wurde und das Insights-Ereignis ausgelöst hat. Der CloudTrail Insights-Durchschnitt für das Startereignis ist die Häufigkeit der

Ereignisse, die das Insights-Ereignis ausgelöst haben. Normalerweise ist dies die erste Minute mit ungewöhnlichen Aktivitäten. Der Insight-Durchschnitt für das Endereignis ist die Rate von Vorkommen für die Dauer der ungewöhnlichen Aktivität zwischen dem Insights-Start- und -Endereignis.

## Ratenänderung

Die Differenz zwischen dem Wert von Baseline-Durchschnitt und Insight-Durchschnitt, gemessen als Prozentsatz. Beispiel: Wenn der Baseline-Durchschnitt eines AccessDenied-Fehlervorkommens 1,0 und der Insight-Durchschnitt 3,0 beträgt, liegt eine Ratenänderung von 300 % vor. Für eine Ratenänderung für einen Insight-Durchschnitt, der einen Baseline-Durchschnitt übersteigt, wird neben dem Wert ein Nach-oben-Pfeil angezeigt. Wenn das Insights-Ereignis protokolliert wurde, weil die Aktivität unter dem Baseline-Durchschnitt liegt, wird für Ratenänderung ein Nach-unten-Pfeil neben dem Prozentsatz angezeigt.

Wurden für das gewählte Attribut oder die gewählte Zeit keine Ereignisse protokolliert, bleibt die Ergebnisliste leer. Neben dem Filter für den Zeitraum können Sie nur noch einen Attribut-Filter anwenden. Wenn Sie einen anderen Attributfilter auswählen, wird der angegebene Zeitbereich beibehalten.

In den folgenden Schritten wird beschrieben, wie Sie nach einem Attribut filtern.

So filtern Sie nach einem Attribut

1. Um die Ergebnisse nach einem Attribut zu filtern, wählen Sie ein Nachschlageattribut aus dem Dropdown-Menü aus und geben oder wählen Sie dann einen Wert in das Feld Nachschlagewert eingeben aus.
2. Um einen Attributfilter zu entfernen, klicken Sie auf das X rechts vom Feld für den Attributfilter.

In den folgenden Schritten wird beschrieben, wie Sie nach einem Start- und Enddatum und nach Uhrzeit filtern.

Nach einem Start- und Enddatum und Uhrzeit filtern

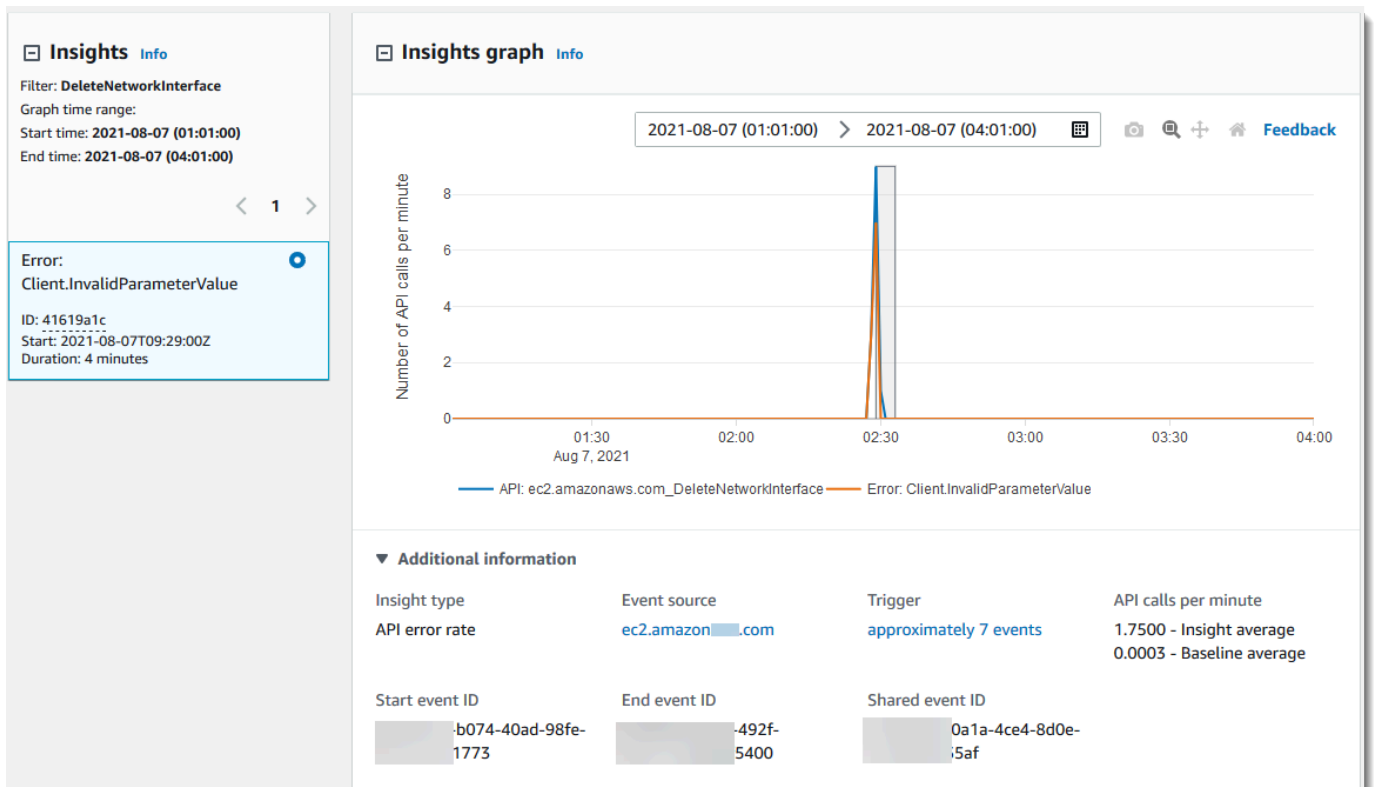
1. Um den Zeitraum für die Ereignisse, die Sie anzeigen möchten, einzugrenzen, wählen Sie einen Zeitraum in der Zeitspannenleiste oben in der Tabelle aus. Voreingestellte Zeitbereiche umfassen 30 Minuten, 1 Stunde, 3 Stunden oder 12 Stunden. Um einen benutzerdefinierten Zeitraum anzugeben, wählen Sie Benutzerdefiniert aus.

2. Wählen Sie eine der folgenden Registerkarten.
  - Absolut – Hier können Sie eine bestimmte Zeit wählen. Fahren Sie mit dem nächsten Schritt fort.
  - Relativ zum ausgewählten Ereignis – Standardmäßig ausgewählt. Hier können Sie einen Zeitraum relativ zur Startzeit eines Insights-Ereignisses auswählen. Fahren Sie mit Schritt 4 fort.
3. Gehen Sie wie folgt vor, um einen absoluten Zeitbereich festzulegen.
  - a. Wählen Sie auf der Registerkarte Absolut den Tag aus, an dem der Zeitraum beginnen soll. Geben Sie eine Startzeit am ausgewählten Tag ein. Um ein Datum manuell einzugeben, geben Sie das Datum im Format yyyy/mm/dd ein. Die Start- und Endzeiten verwenden ein 24-Stunden-Format und die Werte müssen das Format hh:mm:ss haben. Um beispielsweise eine Startzeit von 18.30 Uhr anzugeben, geben Sie **18:30:00** ein.
  - b. Wählen Sie ein Enddatum für den Bereich im Kalender aus oder geben Sie ein Enddatum und eine Endzeit unterhalb des Kalenders an. Wählen Sie Anwenden aus.
4. Gehen Sie wie folgt vor, um einen Relativ zum ausgewählten Ereigniszeitbereich festzulegen.
  - a. Wählen Sie einen voreingestellten Zeitraum relativ zur Startzeit von Insights-Ereignissen. Voreingestellte Werte sind in Minuten, Stunden, Tagen oder Wochen verfügbar. Die maximale relative Zeitspanne beträgt 12 Wochen.
  - b. Passen Sie bei Bedarf den voreingestellten Wert in den Feldern unterhalb der Voreinstellungen an. Wählen Sie Löschen, um Ihre Änderungen bei Bedarf zurückzusetzen. Wenn Sie die gewünschte relative Zeit eingestellt haben, wählen Sie Anwenden.
5. Wählen Sie unter Bis den Tag aus und geben Sie die Uhrzeit an, die als Endzeitpunkt des Zeitraums verwendet werden soll. Wählen Sie Apply (Anwenden) aus.
6. Um Zeitraumfilter zu entfernen, klicken Sie auf das Kalendersymbol rechts vom Feld Zeitraum und wählen anschließend Entfernen.

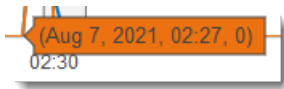
## Details zu Insights-Ereignissen anzeigen

1. Wählen Sie ein Insights-Ereignis in der Ergebnisliste aus, um die Details dazu anzuzeigen. Auf der Seite mit den Details eines Insights-Ereignisses wird ein Diagramm mit der Zeitachse der ungewöhnlichen Aktivitäten angezeigt.





2. Bewegen Sie den Mauszeiger über die hervorgehobenen Bänder, um die Startzeit und Dauer jedes Insights-Ereignisses im Diagramm anzuzeigen.



Die folgenden Informationen werden im Bereich Zusätzliche Informationen des Diagramms angezeigt:

- Insight-Typ. Dies kann API-Aufrufrate oder API-Fehlerrate sein.
- Auslöser. Dies ist ein Link zur Registerkarte Cloudtrail-Ereignisse, auf der die Verwaltungsereignisse aufgelistet sind, die analysiert wurden, um festzustellen, dass ungewöhnliche Aktivitäten aufgetreten sind.
- API-Aufrufe pro Minute
  - Baseline-Durchschnitt – Die typische Rate von Vorkommen pro Minute für diese API, für die das Insights-Ereignis protokolliert wurde, gemessen in ungefähr den letzten sieben Tagen in einer bestimmten Region in Ihrem Konto.
  - Insight-Durchschnitt: Die Rate der Vorkommen pro Minute für diese API, von der das Insights-Ereignis ausgelöst wurde. Der CloudTrail Insights-Durchschnitt für das Startereignis

ist die Rate der Aufrufe oder Fehler pro Minute auf der API, die das Insights-Ereignis ausgelöst haben. Normalerweise ist dies die erste Minute mit ungewöhnlichen Aktivitäten. Der Insights-Durchschnitt für das Endereignis ist die Rate von API-Aufrufen oder -Fehlern pro Minute für die Dauer der ungewöhnlichen Aktivitäten zwischen dem Insights-Start- und -Endereignis.

- Ereignisquelle. Der AWS Service-Endpunkt, auf dem die ungewöhnliche Anzahl von API-Aufrufen oder Fehlern protokolliert wurde. Im vorherigen Image ist die Quelle `ec2.amazonaws.com`, der Service-Endpunkt für Amazon EC2.
  - Ereignis-IDs.
    - Startereignis-ID – Die ID des Insights-Ereignisses, das zu Beginn der ungewöhnlichen Aktivitäten protokolliert wurde.
    - Endereignis-ID – Die ID des Insights-Ereignisses, das am Ende der ungewöhnlichen Aktivitäten protokolliert wurde.
    - Gemeinsame Ereignis-ID — Bei Insights-Ereignissen ist die Shared Event ID eine GUID, die von CloudTrail Insights generiert wird, um ein Start- und Endpaar von Insights-Ereignissen eindeutig zu identifizieren. Die Gemeinsame Ereignis-ID ist für das Insights-Start- und -Endereignis gleich und dient zum Erstellen einer Korrelation zwischen den beiden Ereignissen, um ungewöhnliche Aktivitäten eindeutig identifizieren zu können.
3. Wählen Sie die Registerkarte Namensnennungen aus, um Informationen zu den Benutzeridentitäten, Benutzeragenten und zu API-Fehlerrate-Insights-Ereignissen und Fehlercodes anzuzeigen, die mit ungewöhnlichen und grundlegenden Aktivitäten korreliert sind. In Tabellen auf der Registerkarte Attributionen werden maximal fünf Benutzeridentitäten, fünf Benutzeragenten und fünf Fehlercodes angezeigt, sortiert nach dem Durchschnitt der Aktivitätsanzahl in absteigender Reihenfolge vom höchsten zum niedrigsten Wert. Weitere Informationen zur Registerkarte Attributionen finden Sie unter [Registerkarte Attributionen](#) und [CloudTrail insightDetailsElement „Einblicke“](#) in diesem Leitfaden.
  4. Sehen Sie sich auf der Registerkarte CloudTrail Ereignisse verwandte Ereignisse an, die CloudTrail analysiert wurden, um festzustellen, dass ungewöhnliche Aktivitäten aufgetreten sind. Standardmäßig wird bereits ein Filter für den Namen des Insights-Ereignisses angewendet. Dies ist auch der Name der zugehörigen API. Auf der Registerkarte CloudTrail Ereignisse werden CloudTrail Verwaltungsereignisse im Zusammenhang mit der Betreff-API angezeigt, die zwischen der Startzeit (minus eine Minute) und der Endzeit (plus eine Minute) des Insights-Ereignisses aufgetreten sind.

Wenn Sie andere Insights-Ereignisse im Diagramm auswählen, ändern sich die in der CloudTrail Ereignistabelle angezeigten Ereignisse. Mit diesen Ereignissen können Sie eine eingehendere Analyse durchführen, um die wahrscheinliche Ursache eines Insights-Ereignisses und die Gründe für die ungewöhnlichen API-Aktivitäten zu ermitteln.

Um alle CloudTrail Ereignisse anzuzeigen, die während der Dauer des Insights-Ereignisses protokolliert wurden, und nicht nur die Ereignisse für die zugehörige API, schalten Sie den Filter aus.

5. Wählen Sie die Registerkarte Insights-Ereignisdatensatz, um die Insights-Start- und Endereignisse im JSON-Format anzuzeigen.
6. Wenn Sie die verknüpfte Ereignisquelle auswählen, kehren Sie zur Seite Insights zurück, die nach dieser Ereignisquelle gefiltert ist.

## Zoomen, Schwenken und Herunterladen des Diagramms

Sie können das Diagramm auf der Detailseite des Insights-Ereignisses zoomen, schwenken und dessen Achsen zurücksetzen, indem Sie die Symbolleiste oben rechts verwenden.

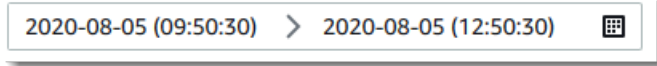


Von links nach rechts haben die Befehlsschaltflächen des Diagramms die folgenden Funktionen:

- Plot als PNG herunterladen: Laden Sie das Diagrammbild herunter, das auf der Detailseite angezeigt wird, und speichern Sie es im PNG-Format.
- Zoomen: Ziehen Sie mit dem Mauszeiger ein Kästchen auf, um einen Bereich des Diagramms auszuwählen, den Sie vergrößern und detaillierter anzeigen möchten.
- Schwenken: Verschieben Sie das Diagramm, um daneben angeordnete Datumsangaben oder Uhrzeiten anzuzeigen.
- Achsen zurücksetzen: Setzen Sie die Diagrammachsen wieder in den Originalzustand zurück. Hierbei werden die Zoom- und Schwenkeinstellungen gelöscht.

## Ändern der Einstellungen für die Zeitspanne des Diagramms

Sie können die Zeitspanne – die ausgewählte Dauer der auf der x-Achse angezeigten Ereignisse – ändern, die im Diagramm angezeigt wird, indem Sie eine Einstellung in der oberen rechten Ecke des Diagramms auswählen.



Die im Diagramm angezeigte Standardzeitspanne hängt von der Dauer des ausgewählten Insights-Ereignisses ab.

Dauer des Insights-Ereignisses	Standardzeitspanne
Weniger als 4 Stunden	3 h (drei Stunden)
Zwischen 4 und 12 Stunden	12 h(12 Stunden)
Zwischen 12 und 24 Stunden	1 T (ein Tag)
Zwischen 24 und 72 Stunden	3 T (drei Tage)
Länger als 72 Stunden	1 W (eine Woche)

Sie können Voreinstellungen von fünf Minuten, 30 Minuten, einer Stunde, drei Stunden, 12 Stunden oder Benutzerdefiniert auswählen. Im folgenden Image werden Zeiträume angezeigt, die relativ zum ausgewählten Ereignis sind, die Sie in den Einstellungen unter Benutzerdefiniert auswählen können. Relative Zeiträume sind ungefähre Zeiträume, die den Beginn und das Ende des ausgewählten Insights-Ereignisses umgeben, das auf einer Seite mit Details zu Insights-Ereignissen angezeigt wird.

**Absolute**
**Relative to selected event**
Local time zone ▼

**Minutes**

<input type="text" value="5"/>	<input type="text" value="10"/>	<input type="text" value="15"/>	<input type="text" value="30"/>	<input type="text" value="45"/>
--------------------------------	---------------------------------	---------------------------------	---------------------------------	---------------------------------

**Hours**

<input type="text" value="1"/>	<input type="text" value="2"/>	<input type="text" value="3"/>	<input type="text" value="6"/>	<input type="text" value="8"/>	<input type="text" value="12"/>
--------------------------------	--------------------------------	--------------------------------	--------------------------------	--------------------------------	---------------------------------

**Days**

<input type="text" value="1"/>	<input type="text" value="2"/>	<input type="text" value="3"/>	<input type="text" value="4"/>	<input type="text" value="5"/>	<input type="text" value="6"/>
--------------------------------	--------------------------------	--------------------------------	--------------------------------	--------------------------------	--------------------------------

**Weeks**

<input type="text" value="1"/>	<input type="text" value="2"/>	<input type="text" value="3"/>	<input type="text" value="4"/>
--------------------------------	--------------------------------	--------------------------------	--------------------------------

Um eine ausgewählte Voreinstellung anzupassen, geben Sie in den Feldern unter den Voreinstellungen eine Zahl und eine Zeiteinheit an.

Wählen Sie die Registerkarte **Absolute** aus, um ein genaues Datum und einen Zeitraum anzugeben. Wenn Sie einen absoluten Datums- und Zeitbereich festlegen, sind Start- und Endzeiten erforderlich. Informationen zum Einstellen der Uhrzeit finden Sie unter [the section called “Filtern von Insights-Ereignissen”](#) in diesem Thema.

**Absolute**
**Relative to selected event**
Local time zone ▼

<
**August 2020**
>

Su	Mo	Tu	We	Th	Fr	Sa
						1
2	3	4	5	6	7	8
9	10	11	12	13	14	15
16	17	18	19	20	21	22
23	24	25	26	27	28	29
30	31					

Su	Mo	Tu	We	Th	Fr	Sa
		1	2	3	4	5
6	7	8	9	10	11	12
13	14	15	16	17	18	19
20	21	22	23	24	25	26
27	28	29	30			

## Herunterladen von Insights-Ereignissen

Sie können einen aufgezeichneten Verlauf von Insights-Ereignissen als Datei im CSV- oder JSON-Format herunterladen. Verwenden Sie Filter und Zeitbereiche zur Reduzierung der Größe der Datei, die Sie herunterladen.

### Note

CloudTrail Ereignisverlaufsdateien sind Datendateien, die Informationen (wie Ressourcennamen) enthalten, die von einzelnen Benutzern konfiguriert werden können. Einige Daten können potenziell als Befehle in Programmen verwendet werden, um diese Daten zu lesen und zu analysieren (CSV-Injektion). Wenn CloudTrail Ereignisse beispielsweise als CSV exportiert und in ein Tabellenkalkulationsprogramm importiert werden, warnt Sie dieses Programm möglicherweise vor Sicherheitsbedenken. Die bewährte Sicherheitsmethode besteht darin, Links oder Makros aus heruntergeladenen Dateien mit Ereignisverläufen zu deaktivieren.

1. Geben Sie den Filter und Zeitraum für die Ereignisse an, die Sie herunterladen möchten. Sie können beispielsweise den Ereignisnamen `StartInstances` und einen Zeitrahmen für die letzten drei Tage Aktivität angeben.
2. Wählen Sie Ereignisse herunterladen und dann CSV herunterladen oder JSON herunterladen aus. Sie werden aufgefordert, einen Speicherort für die Datei auszuwählen.

### Note

Ihr Download kann einige Zeit in Anspruch nehmen. Verwenden Sie für schnellere Ergebnisse einen detaillierteren Filter oder einen kürzeren Zeitbereich, um die Ergebnisse einzuschränken, bevor Sie den Download-Vorgang starten.

3. Wenn der Download abgeschlossen ist, öffnen Sie die Datei, um die Ereignisse anzuzeigen, die Sie angegeben haben.
4. Um Ihren Download abbrechen, wählen Sie Download abbrechen. Wenn Sie einen Download abbrechen, bevor er abgeschlossen ist, enthält eine CSV- oder JSON-Datei auf Ihrem lokalen Computer möglicherweise nur einen Teil Ihrer Ereignisse.

## CloudTrail Insights-Ereignisse für Trails anzeigen mit dem AWS CLI

Sie können CloudTrail Insights-Ereignisse der letzten 90 Tage nachschlagen, indem Sie den `aws cloudtrail lookup-events` Befehl ausführen. Der Befehl `lookup-events` hat die folgenden Optionen:

- `--end-time`
- `--event-category`
- `--max-results`
- `--start-time`
- `--lookup-attributes`
- `--next-token`
- `--generate-cli-skeleton`
- `--cli-input-json`

Allgemeine Informationen zur Verwendung von AWS Command Line Interface finden Sie im [AWS Command Line Interface Benutzerhandbuch](#).

### Inhalt

- [Voraussetzungen](#)
- [Nutzen der Befehlszeilenhilfe](#)
- [Suchen nach Insights-Ereignissen](#)
- [Angaben der Anzahl von zurückzugebenden Insights-Ereignissen](#)
- [Suchen nach Insights-Ereignissen nach Zeitraum](#)
- [Suchen nach Insights-Ereignissen nach Attribut](#)
  - [Beispiele für die Attributsuche](#)
- [Angabe der nächsten Ergebnisseite](#)
- [Abrufen der JSON-Eingabe aus einer Datei](#)
- [Ausgabefelder der Suche](#)

### Voraussetzungen

- Um AWS CLI Befehle ausführen zu können, müssen Sie den installieren AWS CLI. Weitere Informationen finden Sie unter [Erste Schritte mit dem AWS CLI](#).

- Stellen Sie sicher, dass Ihre AWS CLI Version höher als 1.6.6 ist. Sie können die CLI-Version verifizieren, indem Sie `aws --version` in der Befehlszeile ausführen.
- Verwenden Sie den `aws configure` Befehl, um das Konto, die Region und das Standardausgabeformat für eine AWS CLI Sitzung festzulegen. Weitere Informationen finden Sie unter [Konfigurieren der AWS -Befehlszeilenschnittstelle](#).
- Um Insights-Ereignisse anhand des API-Aufruf-Volumens zu protokollieren, muss der Trail `write`-Verwaltungsereignisse protokollieren. Um Insights-Ereignisse auf der API-Fehlerrate zu protokollieren, muss der Trail `read`- oder `write`-Verwaltungsereignisse protokollieren.

### Note

Bei den CloudTrail AWS CLI Befehlen wird zwischen Groß- und Kleinschreibung unterschieden.

## Nutzen der Befehlszeilenhilfe

Geben Sie den folgenden Befehl ein, wenn Sie die Befehlszeilenhilfe zu `lookup-events` anzeigen möchten.

```
aws cloudtrail lookup-events help
```

## Suchen nach Insights-Ereignissen

Um die zehn neuesten Insights-Ereignisse anzuzeigen, geben Sie den folgenden Befehl ein.

```
aws cloudtrail lookup-events --event-category insight
```

Ein zurückgegebenes Ereignis sieht in etwa wie folgt aus:

```
{
  "NextToken": "kb0t5L1Ze+
+mErCebpy2TgaMgmDvF1kYGFcH64JSjIbZfjsuvrSqq66b5YGssKutDYIyII4lrP4IDbeQdi0bkp9YA1ju3oXd12juEXAMP
  "Events": [
    {
      "eventVersion": "1.07",
      "eventTime": "2019-10-15T21:13:00Z",
      "awsRegion": "us-east-1",
      "eventID": "EXAMPLE-9b6f-45f8-bc6b-9b41c052ebc7",
```



```

"eventType": "AwsCloudTrailInsight",
"recipientAccountId": "123456789012",
"sharedEventID": "EXAMPLE8-02b2-4e93-9aab-08ed47ea5fd3",
"insightDetails": {
"state": "Start",
"eventSource": "autoscaling.amazonaws.com",
"eventName": "CompleteLifecycleAction",
"insightType": "ApiCallRateInsight",
"insightContext": {
"statistics": {
"baseline": {
"average": 0.0000882145
},
"insight": {
"average": 0.6
},
"insightDuration": 5,
"baselineDuration": 11336
},
"attributions": [
{
"attribute": "userIdentityArn",
"insight": [
{
"value": "arn:aws:sts::012345678901:assumed-role/
CodeDeployRole1",
"average": 0.2
},
{
"value": "arn:aws:sts::012345678901:assumed-role/
CodeDeployRole2",
"average": 0.2
},
{
"value": "arn:aws:sts::012345678901:assumed-role/
CodeDeployRole3",
"average": 0.2
}
],
"baseline": [
{
"value": "arn:aws:sts::012345678901:assumed-role/
CodeDeployRole1",
"average": 0.0000882145

```

```
    }
  ]
},
{
  "attribute": "userAgent",
  "insight": [
    {
      "value": "codedeploy.amazonaws.com",
      "average": 0.6
    }
  ],
  "baseline": [
    {
      "value": "codedeploy.amazonaws.com",
      "average": 0.0000882145
    }
  ]
},
{
  "attribute": "errorCode",
  "insight": [
    {
      "value": "null",
      "average": 0.6
    }
  ],
  "baseline": [
    {
      "value": "null",
      "average": 0.0000882145
    }
  ]
}
],
}
},
"eventCategory": "Insight"
},
{
  "eventVersion": "1.07",
  "eventTime": "2019-10-15T21:14:00Z",
  "awsRegion": "us-east-1",
  "eventID": "EXAMPLEc-9eac-4af6-8e07-26a5ae8786a5",
  "eventType": "AwsCloudTrailInsight",
```

```
"recipientAccountId": "123456789012",
"sharedEventID": "EXAMPLE8-02b2-4e93-9aab-08ed47ea5fd3",
"insightDetails": {
  "state": "End",
  "eventSource": "autoscaling.amazonaws.com",
  "eventName": "CompleteLifecycleAction",
  "insightType": "ApiCallRateInsight",
  "insightContext": {
    "statistics": {
      "baseline": {
        "average": 0.0000882145
      },
      "insight": {
        "average": 0.6
      },
      "insightDuration": 5,
      "baselineDuration": 11336
    },
    "attributions": [
      {
        "attribute": "userIdentityArn",
        "insight": [
          {
            "value": "arn:aws:sts::012345678901:assumed-role/
CodeDeployRole1",
            "average": 0.2
          },
          {
            "value": "arn:aws:sts::012345678901:assumed-role/
CodeDeployRole2",
            "average": 0.2
          },
          {
            "value": "arn:aws:sts::012345678901:assumed-role/
CodeDeployRole3",
            "average": 0.2
          }
        ],
        "baseline": [
          {
            "value": "arn:aws:sts::012345678901:assumed-role/
CodeDeployRole1",
            "average": 0.0000882145
          }
        ]
      }
    ]
  }
}
```

```
    ]
  },
  {
    "attribute": "userAgent",
    "insight": [
      {
        "value": "codedeploy.amazonaws.com",
        "average": 0.6
      }
    ],
    "baseline": [
      {
        "value": "codedeploy.amazonaws.com",
        "average": 0.0000882145
      }
    ]
  },
  {
    "attribute": "errorCode",
    "insight": [
      {
        "value": "null",
        "average": 0.6
      }
    ],
    "baseline": [
      {
        "value": "null",
        "average": 0.0000882145
      }
    ]
  }
]
}
"eventCategory": "Insight"
}
```

Eine Erläuterung der suchbezogenen Felder in der Ausgabe finden Sie im Abschnitt [Ausgabefelder der Suche](#) in diesem Thema. Eine Erläuterung der Felder im Insights-Ereignis erhalten Sie unter [CloudTrail Inhalt aufzeichnen](#).

## Angeben der Anzahl von zurückzugebenden Insights-Ereignissen

Geben Sie den folgenden Befehl ein, um die Anzahl von zurückzugebenden Ereignissen anzugeben.

```
aws cloudtrail lookup-events --event-category insight --max-results <integer>
```

Der Standardwert für *<integer>* ist 10, falls nichts anderes angegeben ist. Mögliche Werte: 1 bis 50. Im folgenden Beispiel wird ein Ergebnis zurückgegeben.

```
aws cloudtrail lookup-events --event-category insight --max-results 1
```

## Suchen nach Insights-Ereignissen nach Zeitraum

Für die Suche sind die Insights-Ereignisse der letzten 90 Tage verfügbar. Geben Sie den folgenden Befehl ein, um einen Zeitraum anzugeben.

```
aws cloudtrail lookup-events --event-category insight --start-time <timestamp> --end-time <timestamp>
```

`--start-time <timestamp>` gibt in UTC an, dass nur Insights-Ereignisse, die nach oder zum angegebenen Zeitpunkt eintreten, zurückgegeben werden. Falls die angegebene Anfangszeit nach der angegebenen Endzeit liegt, wird ein Fehler zurückgegeben.

`--end-time <timestamp>` gibt in UTC an, dass nur Insights-Ereignisse, die vor oder zum angegebenen Zeitpunkt eintreten, zurückgegeben werden. Falls die angegebene Endzeit vor der angegebenen Anfangszeit liegt, wird ein Fehler zurückgegeben.

Standardmäßige Anfangszeit ist das früheste Datum, an dem innerhalb der letzten 90 Tage Daten verfügbar sind. Standardmäßige Endzeit ist der Zeitpunkt des Ereignisses, das zu dem der aktuellen Zeit am nächsten liegenden Zeitpunkt eingetreten ist.

Alle Zeitstempel werden in UTC angezeigt.

## Suchen nach Insights-Ereignissen nach Attribut

Geben Sie zum Filtern nach einem Attribut den folgenden Befehl ein.

```
aws cloudtrail lookup-events --event-category insight --lookup-attributes  
AttributeKey=<attribute>,AttributeValue=<string>
```

Sie können für jeden `lookup-events`-Befehl nur ein Paar angeben, das aus dem Attributsschlüssel und dem zugehörigen Wert besteht. Im Folgenden sind die gültigen Werte von Insights-Ereignissen für `AttributeKey` angegeben. Bei den Wertnamen muss die Groß- und Kleinschreibung beachtet werden.

- `EventId`
- `EventName`
- `EventSource`

Die maximale Länge für die `AttributeValue` beträgt 2000 Zeichen. Die folgenden Zeichen (`'_'`, `"`, `,`, `\"`) gelten als zwei Zeichen im Verhältnis zur Obergrenze von 2000 Zeichen.

### Beispiele für die Attributsuche

Der folgende Beispielbefehl gibt die Insights-Ereignisse mit dem `EventName`-Wert `PutRule` zurück.

```
aws cloudtrail lookup-events --event-category insight --lookup-attributes
  AttributeKey=EventName, AttributeValue=PutRule
```

Der folgende Beispielbefehl gibt die Insights-Ereignisse mit dem `EventId`-Wert `b5cc8c40-12ba-4d08-a8d9-2bceb9a3e002` zurück.

```
aws cloudtrail lookup-events --event-category insight --lookup-attributes
  AttributeKey=EventId, AttributeValue=b5cc8c40-12ba-4d08-a8d9-2bceb9a3e002
```

Der folgende Beispielbefehl gibt die Insights-Ereignisse mit dem `EventSource`-Wert `iam.amazonaws.com` zurück.

```
aws cloudtrail lookup-events --event-category insight --lookup-attributes
  AttributeKey=EventSource, AttributeValue=iam.amazonaws.com
```

### Angabe der nächsten Ergebnisseite

Um die nächste Seite mit Ergebnissen des Befehls `lookup-events` abzurufen, geben Sie den folgenden Befehl ein.

```
aws cloudtrail lookup-events --event-category insight <same parameters as previous
  command> --next-token=<token>
```

Bei diesem Befehl wird der Wert für `<token>` aus dem ersten Feld der Ausgabe des vorherigen Befehls entnommen.

Wenn Sie `--next-token` in einem Befehl verwenden, müssen Sie dieselben Parameter wie im vorherigen Befehl verwenden. Angenommen, Sie führen den unten angegebenen Befehl aus.

```
aws cloudtrail lookup-events --event-category insight --lookup-attributes
  AttributeKey=EventName, AttributeValue=PutRule
```

Um die nächste Seite mit Ergebnissen abzurufen, würde Ihr nächster Befehl wie folgt aussehen.

```
aws cloudtrail lookup-events --event-category insight --lookup-attributes
  AttributeKey=EventName,AttributeValue=PutRule --next-token=EXAMPLEZe+
+mErCebpy2TgaMgmDvF1kYGFch64JSjIbZfjsuvrSqq66b5YGssKutDYIyII4lrP4IDbeQdi0bKp9YA1ju3oXd12juEXAMP
```

## Abrufen der JSON-Eingabe aus einer Datei

AWS CLI Für einige AWS Dienste gibt es zwei Parameter, `--generate-cli-skeleton` mit denen Sie eine JSON-Vorlage generieren können, die Sie ändern und als Eingabe für den `--cli-input-json` Parameter verwenden können. `--cli-input-json` In diesem Abschnitt wird die Verwendung dieser Parameter mit `aws cloudtrail lookup-events` beschrieben. Weitere Informationen finden Sie unter [AWS CLI Skelette und Eingabedateien](#).

So suchen Sie Insights-Ereignisse durch Abrufen der JSON-Eingabe aus einer Datei

1. Erstellen Sie eine Eingabevorlage für die Verwendung mit `lookup-events` und leiten Sie dazu die `--generate-cli-skeleton`-Ausgabe in eine Datei um, wie im folgenden Beispiel dargestellt.


```
aws cloudtrail lookup-events --event-category insight --generate-cli-skeleton >
  LookupEvents.txt
```

Die generierte Vorlagendatei (in diesem Fall `LookupEvents.txt`) sieht wie folgt aus.

```
{
  "LookupAttributes": [
    {
      "AttributeKey": "",
```

```
        "AttributeValue": ""
      }
    ],
    "StartTime": null,
    "EndTime": null,
    "MaxResults": 0,
    "NextToken": ""
  }
```

2. Ändern Sie die JSON-Daten in einem Texteditor nach Bedarf. Die JSON-Eingabe darf nur angegebene Werte umfassen.

 **Wichtig**


Die Vorlage kann erst verwendet werden, nachdem alle leeren Werte oder Nullwerte daraus entfernt wurden.

Im folgenden Beispiel sind ein Zeitraum und die maximale Anzahl der zurückzugebenden Ergebnisse angegeben.

```
{
  "StartTime": "2023-11-01",
  "EndTime": "2023-12-12",
  "MaxResults": 10
}
```

3. Verwenden Sie die Syntax `--cli-input-json file://<filename>`, wie im folgenden Beispiel dargestellt, um die bearbeitete Datei als Eingabe zu verwenden.

```
aws cloudtrail lookup-events --event-category insight --cli-input-json file://
LookupEvents.txt
```

 **Note**

Sie können in derselben Befehlszeile wie `--cli-input-json` weitere Argumente verwenden.



## Ausgabefelder der Suche

### Ereignisse

Eine Liste der Suchereignisse basierend auf dem angegebenen Suchattribut und Zeitbereich. Die Ereignisliste ist nach Zeit sortiert, das neueste Ereignis ist zuerst aufgeführt. Jeder Eintrag enthält Informationen über die Suchanfrage und eine Zeichenfolgendarstellung des abgerufenen CloudTrail Ereignisses.

Die folgenden Einträge beschreiben die Felder in den einzelnen Suchereignissen.

### CloudTrailEvent

Eine JSON-Zeichenfolge, die eine Objektdarstellung des zurückgegebenen Ereignisses enthält. Weitere Informationen zu den einzelnen zurückgegebenen Elementen finden Sie im Abschnitt [Datensatzinhalte](#).

### EventId

Eine Zeichenfolge, die die GUID des zurückgegebenen Ereignisses enthält.

### EventName

Eine Zeichenfolge, die den Namen des zurückgegebenen Ereignisses enthält.

### EventSource

Der AWS Dienst, an den die Anfrage gestellt wurde.

### EventTime

Datum und Uhrzeit des Ereignisses im UNIX-Zeitformat.

### Ressourcen

Eine Liste der Ressourcen, auf die von dem zurückgegebenen Ereignis verwiesen wird. In jedem Ressourceneintrag ist ein Ressourcentyp und ein Ressourcenname angegeben.

### ResourceName

Eine Zeichenfolge, die den Namen der Ressource enthält, auf die von dem Ereignis verwiesen wird.

### ResourceType

Eine Zeichenfolge, die den Typ einer Ressource enthält, auf die von dem Ereignis verwiesen wird. Wenn der Ressourcentyp nicht ermittelt werden kann, wird Null zurückgegeben.

## Username

Eine Zeichenfolge, die den Benutzernamen des Kontos für das zurückgegebene Ereignis enthält.

## NextToken

Eine Zeichenfolge zum Abrufen der nächsten Ergebnisseite eines vorherigen `lookup-events`-Befehls. Um das Token verwenden zu können, müssen die Parameter mit den Parametern im ursprünglichen Befehl übereinstimmen. Wenn es in der Ausgabe keinen `NextToken`-Eintrag gibt, sind keine weiteren Ergebnisse vorhanden, die zurückgegeben werden können.

Weitere Informationen zu CloudTrail Insights-Ereignissen finden Sie [Protokollieren von Insights-Ereignissen](#) in diesem Handbuch.

## Trailereignisse nach CloudTrail Lake kopieren

Sie können vorhandene Trail-Ereignisse in einen CloudTrail Lake Event Data Store kopieren, um eine point-in-time Momentaufnahme der im Trail protokollierten Ereignisse zu erstellen. Das Kopieren von Trail-Ereignissen beeinträchtigt nicht die Fähigkeit des Trails, Ereignisse zu protokollieren, und verändert den Trail in keiner Weise.

Sie können Trail-Ereignisse in einen vorhandenen, für CloudTrail Ereignisse konfigurierten Event-Datenspeicher kopieren, oder Sie können einen neuen CloudTrail Event-Datenspeicher erstellen und bei der Erstellung des Event-Datenspeichers die Option Trail-Ereignisse kopieren auswählen. Weitere Informationen zum Kopieren von Trail-Ereignissen in einen bestehenden Ereignisdatenspeicher finden Sie unter [Kopieren Sie Trail-Ereignisse mithilfe der Konsole in einen vorhandenen Ereignisdatenspeicher CloudTrail](#). Weitere Informationen zum Erstellen eines neuen Ereignisdatenspeichers finden Sie unter [Erstellen Sie mit der Konsole einen Ereignisdatenspeicher für CloudTrail Ereignisse](#).

Wenn Sie Trail-Ereignisse in einen CloudTrail Lake-Event-Datenspeicher kopieren, können Sie Abfragen für die kopierten Ereignisse ausführen. CloudTrail Lake-Abfragen bieten eine umfassendere und besser anpassbare Ansicht von Ereignissen als einfache Schlüssel- und Werte-Suchen in der Ereignishistorie oder bei laufenden `LookupEvents` Ereignissen. Weitere Informationen zu CloudTrail Lake finden Sie unter [Mit AWS CloudTrail Lake arbeiten](#).

Wenn Sie Trail-Ereignisse in den Ereignisdatenspeicher einer Organisation kopieren, müssen Sie das Verwaltungskonto der Organisation verwenden. Trail-Ereignisse lassen sich nicht mit dem Konto eines delegierten Administrators einer Organisation kopieren.

CloudTrail Für Datenspeicher mit Ereignissen in Lake fallen Gebühren an. Beim Erstellen eines Ereignisdatenspeichers wählen Sie die [Preisoption](#) aus, die für den Ereignisdatenspeicher genutzt werden soll. Die Preisoption bestimmt die Kosten für die Erfassung und Speicherung von Ereignissen sowie die standardmäßige und maximale Aufbewahrungsdauer für den Ereignisdatenspeicher. Informationen zur CloudTrail Preisgestaltung und Verwaltung der Lake-Kosten finden Sie unter [AWS CloudTrail Preise](#) und [Verwaltung der CloudTrail Seekosten](#).

Wenn Sie Trail-Ereignisse in einen CloudTrail Lake-Ereignisdatenspeicher kopieren, fallen Gebühren an, die auf der Menge der unkomprimierten Daten basieren, die der Ereignisdatenspeicher aufnimmt.

Wenn Sie Trail-Ereignisse nach CloudTrail Lake kopieren, werden die im komprimierten CloudTrail GZIP-Format gespeicherten Protokolle entpackt und anschließend die in den Protokollen enthaltenen Ereignisse in Ihren Ereignisdatenspeicher kopiert. Die Größe der unkomprimierten Daten könnte größer sein als die tatsächliche S3-Speichergröße. Um eine allgemeine Schätzung der Größe der unkomprimierten Daten zu erhalten, können Sie die Größe der Protokolle im S3-Bucket mit 10 multiplizieren.

Sie können die Kosten senken, indem Sie einen engeren Zeitraum für die kopierten Ereignisse angeben. Wenn Sie planen, den Ereignisdatenspeicher nur zum Abfragen Ihrer kopierten Ereignisse zu verwenden, können Sie die Ereignisaufnahme deaktivieren, um zu vermeiden, dass für zukünftige Ereignisse Gebühren anfallen. Weitere Informationen finden Sie unter [AWS CloudTrail -Preise](#) und [Verwaltung der CloudTrail Seekosten](#).

## Szenarien

In der folgenden Tabelle werden einige gängige Szenarien für das Kopieren von Trail-Ereignissen beschrieben. Außerdem wird beschrieben, wie Sie die einzelnen Szenarien mithilfe der Konsole ausführen.

Szenario	Wie erreiche ich das in der Konsole?
Analysieren Sie historische Trail-Ereignisse in CloudTrail Lake und fragen Sie sie ab, ohne neue Ereignisse zu übernehmen	Erstellen Sie einen <a href="#">neuen Ereignisdatenspeicher</a> und wählen Sie im Rahmen der Erstellung des Ereignisdatenspeichers die Option Trail-Ereignisse kopieren aus. Deaktivieren Sie beim Erstellen des Ereignisdatenspeichers die Option Ereignisse aufnehmen (Schritt 15 des Verfahrens), um sicherzustellen, dass der Ereignisdatenspeicher nur die Verlaufsereignisse für Ihren Trail und keine zukünftigen Ereignisse enthält.

Szenario	Wie erreiche ich das in der Konsole?
Ersetzen Sie Ihren vorhandenen Trail durch einen CloudTrail Lake Event Data Store	<p>Erstellen Sie einen Ereignisdatenspeicher mit den gleichen Ereignisselektoren wie bei Ihrem Trail, um sicherzustellen, dass der Ereignisdatenspeicher die gleiche Ereignisabdeckung hat wie Ihr Trail.</p> <p>Um zu vermeiden, dass Ereignisse zwischen dem Quell-Trail und dem Zielereignisdatenspeicher dupliziert werden, wählen Sie einen Zeitraum für die kopierten Ereignisse aus, der vor der Erstellung des Ereignisdatenspeichers liegt.</p> <p>Nachdem Ihr Ereignisdatenspeicher erstellt wurde, können Sie die Protokollierung für den Trail deaktivieren, um zusätzliche Gebühren zu vermeiden.</p>

## Themen

- [Überlegungen zum Kopieren von Trail-Ereignissen](#)
- [Erforderliche Berechtigungen zum Kopieren von Trail-Ereignissen](#)
- [Kopieren Sie Trail-Ereignisse mithilfe der Konsole in einen vorhandenen Ereignisdatenspeicher CloudTrail](#)

## Überlegungen zum Kopieren von Trail-Ereignissen

Berücksichtigen Sie beim Kopieren von Trail-Ereignissen die folgenden Faktoren.

- CloudTrail verwendet beim Kopieren von Trail-Ereignissen den [GetObject](#)-S3-API-Vorgang, um die Trail-Ereignisse im S3-Quell-Bucket abzurufen. Es gibt einige archivierte Speicherklassen von S3, wie S3 Glacier Flexible Retrieval, S3 Glacier Deep Archive, S3 Outposts und S3 Intelligent-Tiering Deep Archive, auf die mithilfe von `GetObject` nicht zugegriffen werden kann. Um in diesen archivierten Speicherklassen gespeicherte Trail-Ereignisse zu kopieren, müssen Sie zunächst eine Kopie mithilfe des S3-Vorgangs `RestoreObject` wiederherstellen. Informationen zum Wiederherstellen archivierter Objekte finden Sie unter [Wiederherstellen archivierter Objekte](#) im Benutzerhandbuch von Amazon S3.

- Wenn Sie Trail-Ereignisse in einen Event-Datenspeicher CloudTrail kopieren, werden alle Trail-Ereignisse unabhängig von der Konfiguration der Ereignistypen des Ziel-Event-Datenspeichers, den erweiterten Event-Selektoren oder AWS-Region kopiert.
- Bevor Sie Trail-Ereignisse in einen vorhandenen Ereignisdatenspeicher kopieren, stellen Sie sicher, dass die Preisoption und der Aufbewahrungszeitraum des Ereignisdatenspeichers für Ihren Anwendungsfall entsprechend konfiguriert sind.
  - Preisoption: Die Preisoption bestimmt die Kosten für die Erfassung und Speicherung von Ereignissen. Weitere Informationen zu Preisoptionen und Details finden Sie unter [AWS CloudTrail -Preise](#) und [Preisoptionen für den Ereignisdatenspeicher](#).
  - Aufbewahrungszeitraum: Der Aufbewahrungszeitraum bestimmt, wie lange Ereignisdaten im Ereignisdatenspeicher aufbewahrt werden. CloudTrail kopiert nur Ereignisse, die eventTime innerhalb der Aufbewahrungsfrist des Veranstaltungsdatspeichers liegen. Um den geeigneten Aufbewahrungszeitraum zu ermitteln, nehmen Sie die Summe aus dem ältesten Ereignis, das Sie kopieren möchten, in Tagen und der Anzahl der Tage, an denen Sie die Ereignisse im Ereignisdatenspeicher speichern möchten (Aufbewahrungszeitraum = *oldest-event-in-days* + *number-days-to-retain*). Wenn das älteste Ereignis, das Sie kopieren, beispielsweise 45 Tage alt ist und Sie die Ereignisse weitere 45 Tage im Ereignisdatenspeicher aufbewahren möchten, würden Sie die Aufbewahrungsdauer auf 90 Tage festlegen.
- Wenn Sie Trail-Ereignisse zur Untersuchung in einen Ereignisdatenspeicher kopieren und keine zukünftigen Ereignisse aufnehmen möchten, können Sie die Aufnahme in den Ereignisdatenspeicher beenden. Deaktivieren Sie beim Erstellen des Ereignisdatenspeichers die Option Ereignisse aufnehmen (Schritt 15 des [Verfahrens](#)), um sicherzustellen, dass der Ereignisdatenspeicher nur die Verlaufereignisse für Ihren Trail und keine zukünftigen Ereignisse enthält.
- Deaktivieren Sie vor dem Kopieren von Trailer-Eignissen alle Zugriffssteuerungslisten (ACL), die an den S3-Quell-Bucket angehängt sind, und aktualisieren Sie die S3-Bucket-Richtlinie für den Zielereignisdatspeicher. Weitere Informationen zum Aktualisieren der S3-Bucket-Richtlinie finden Sie unter [Amazon-S3-Bucket-Richtlinie für das Kopieren von Trail-Ereignissen](#). Weitere Informationen zum Deaktivieren von ACLs finden Sie unter [Steuern des Eigentums an Objekten und Deaktivieren von ACLs für Ihren Bucket](#).
- CloudTrail kopiert nur Trail-Ereignisse aus Gzip-komprimierten Protokolldateien, die sich im S3-Quell-Bucket befinden. CloudTrail kopiert keine Trail-Ereignisse aus unkomprimierten Protokolldateien oder Protokolldateien, die in einem anderen Format als Gzip komprimiert wurden.

- Um zu vermeiden, dass Ereignisse zwischen dem Quell-Trail und dem Zielereignisdatenspeicher dupliziert werden, wählen Sie einen Zeitraum für die kopierten Ereignisse aus, der vor der Erstellung des Ereignisdatenspeichers liegt.
- Standardmäßig werden CloudTrail nur CloudTrail Ereignisse kopiert, die im CloudTrail Präfix des S3-Buckets und die Präfixe innerhalb des CloudTrail Präfixes enthalten sind, und überprüft keine Präfixe für andere Dienste. AWS Wenn Sie CloudTrail Ereignisse kopieren möchten, die in einem anderen Präfix enthalten sind, müssen Sie das Präfix beim Kopieren von Trail-Ereignissen auswählen.
- Um Trail-Ereignisse in den Ereignisdatenspeicher einer Organisation zu kopieren, müssen Sie das Verwaltungskonto der Organisation verwenden. Über das Konto eines delegierten Administrators lassen sich Trail-Ereignisse nicht in den Ereignisdatenspeicher einer Organisation kopieren.

## Erforderliche Berechtigungen zum Kopieren von Trail-Ereignissen

Stellen Sie vor dem Kopieren von Trail-Ereignissen sicher, dass Sie über alle erforderlichen Berechtigungen für Ihre IAM-Rolle verfügen. Sie müssen die IAM-Rollenberechtigungen nur aktualisieren, wenn Sie eine vorhandene IAM-Rolle zum Kopieren von Trail-Ereignissen auswählen. Wenn Sie sich dafür entscheiden, eine neue IAM-Rolle zu erstellen, CloudTrail stellt alle erforderlichen Berechtigungen für die Rolle bereit.

Wenn der S3-Quell-Bucket einen KMS-Schlüssel für die Datenverschlüsselung verwendet, stellen Sie sicher, dass die KMS-Schlüsselrichtlinie das Entschlüsseln von Daten im Bucket zulässt CloudTrail . Wenn der S3-Quell-Bucket mehrere KMS-Schlüssel verwendet, müssen Sie die Richtlinien für jeden Schlüssel aktualisieren, damit CloudTrail die Daten im Bucket entschlüsselt werden können.

### Themen

- [IAM-Berechtigungen zum Kopieren von Trail-Ereignissen](#)
- [Amazon-S3-Bucket-Richtlinie für das Kopieren von Trail-Ereignissen](#)
- [KMS-Schlüsselrichtlinie zum Entschlüsseln von Daten im S3-Quell-Bucket](#)

## IAM-Berechtigungen zum Kopieren von Trail-Ereignissen

Beim Kopieren von Trail-Ereignissen haben Sie die Möglichkeit, eine neue IAM-Rolle zu erstellen oder eine vorhandene IAM-Rolle zu verwenden. Wenn Sie eine neue IAM-Rolle auswählen, CloudTrail wird eine IAM-Rolle mit den erforderlichen Berechtigungen erstellt, sodass keine weiteren Maßnahmen Ihrerseits erforderlich sind.

Wenn Sie sich für eine bestehende Rolle entscheiden, stellen Sie sicher, dass die Richtlinien der IAM-Rolle das Kopieren von Trail-Ereignissen aus dem S3-Quell-Bucket zulassen CloudTrail . Dieser Abschnitt enthält Beispiele für die erforderlichen IAM-Rollenberechtigungen und Vertrauensrichtlinien.

Das folgende Beispiel enthält die Berechtigungsrichtlinie, die es ermöglicht, Trail-Ereignisse aus dem S3-Quell-Bucket CloudTrail zu kopieren. Ersetzen Sie *myBucketNameMyAccountID*, *Region*, *Präfix* und *eventDataStoreId* durch die entsprechenden Werte für Ihre Konfiguration. Die *MyAccountID* ist die für CloudTrail Lake verwendete AWS Konto-ID, die möglicherweise nicht mit der AWS Konto-ID für den S3-Bucket identisch ist.

Ersetzen Sie *key-region*, *keyAccountID* und *keyID* durch die Werte für den KMS-Schlüssel, der zur Verschlüsselung des S3-Quell-Buckets verwendet wird. Sie können die *AWSCloudTrailImportKeyAccess*-Anweisung weglassen, wenn der S3-Quell-Bucket keinen KMS-Schlüssel für die Verschlüsselung verwendet.

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Sid": "AWSCloudTrailImportBucketAccess",
      "Effect": "Allow",
      "Action": ["s3:ListBucket", "s3:GetBucketAcl"],
      "Resource": [
        "arn:aws:s3:::myBucketName"
      ],
      "Condition": {
        "StringEquals": {
          "aws:SourceAccount": "myAccountID",
          "aws:SourceArn":
            "arn:aws:cloudtrail:region:myAccountID:eventdataStore/eventDataStoreId"
        }
      }
    },
    {
      "Sid": "AWSCloudTrailImportObjectAccess",
      "Effect": "Allow",
      "Action": ["s3:GetObject"],
      "Resource": [
        "arn:aws:s3:::myBucketName/prefix",
        "arn:aws:s3:::myBucketName/prefix/*"
      ],
      "Condition": {
```

```

    "StringEquals": {
      "aws:SourceAccount": "myAccountID",
      "aws:SourceArn":
"arn:aws:cloudtrail:region:myAccountID:eventdataStore/eventDataStoreId"
    }
  },
  {
    "Sid": "AWSCloudTrailImportKeyAccess",
    "Effect": "Allow",
    "Action": ["kms:GenerateDataKey", "kms:Decrypt"],
    "Resource": [
      "arn:aws:kms:key-region:keyAccountID:key/keyID"
    ]
  }
]
}

```

Das folgende Beispiel enthält die IAM-Vertrauensrichtlinie, die es ermöglicht, eine IAM-Rolle anzunehmen, CloudTrail um Trail-Ereignisse aus dem S3-Quell-Bucket zu kopieren. *Ersetzen Sie MyAccountID, Region und eventDataStore Id durch die entsprechenden Werte für Ihre Konfiguration.* Die *MyAccountID* ist die für CloudTrail Lake verwendete AWS Konto-ID, die möglicherweise nicht mit der AWS Konto-ID für den S3-Bucket identisch ist.

```

{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Principal": {
        "Service": "cloudtrail.amazonaws.com"
      },
      "Action": "sts:AssumeRole",
      "Condition": {
        "StringEquals": {
          "aws:SourceAccount": "myAccountID",
          "aws:SourceArn":
"arn:aws:cloudtrail:region:myAccountID:eventdataStore/eventDataStoreId"
        }
      }
    }
  ]
}

```



## Amazon-S3-Bucket-Richtlinie für das Kopieren von Trail-Ereignissen

Standardmäßig werden Amazon-S3-Buckets und -Objekte als privat eingestuft. Nur der Ressourcenbesitzer (das AWS -Konto, das den Bucket erstellt hat) kann auf den Bucket und die darin enthaltenen Objekte zugreifen. Der Ressourcenbesitzer kann anderen Ressourcen und Benutzern Zugriffsberechtigungen gewähren, indem er eine Zugriffsrichtlinie schreibt.

Bevor Sie Trail-Ereignisse kopieren, müssen Sie die S3-Bucket-Richtlinie aktualisieren, damit CloudTrail Trail-Ereignisse aus dem Bucket kopiert werden können.

Sie können der S3-Bucket-Richtlinie die folgende Anweisung hinzufügen, um diese Berechtigungen zu gewähren. Ersetzen *roleArn* und *myBucketName* durch die entsprechenden Werte für Ihre Konfiguration.

```
{
  "Sid": "AWSCloudTrailImportBucketAccess",
  "Effect": "Allow",
  "Action": [
    "s3:ListBucket",
    "s3:GetBucketAcl",
    "s3:GetObject"
  ],
  "Principal": {
    "AWS": "roleArn"
  },
  "Resource": [
    "arn:aws:s3:::myBucketName",
    "arn:aws:s3:::myBucketName/*"
  ]
},
```

## KMS-Schlüsselrichtlinie zum Entschlüsseln von Daten im S3-Quell-Bucket

Wenn der Quell-S3-Bucket einen KMS-Schlüssel für die Datenverschlüsselung verwendet, stellen Sie sicher, dass die KMS-Schlüsselrichtlinie über die `kms:Decrypt` erforderlichen `kms:GenerateDataKey` Berechtigungen verfügt CloudTrail , um Trail-Ereignisse aus einem

S3-Bucket mit aktivierter SSE-KMS-Verschlüsselung zu kopieren. Wenn Ihr S3-Quell-Bucket mehrere KMS-Schlüssel verwendet, müssen Sie die Richtlinien jedes Schlüssels aktualisieren. Durch die Aktualisierung der KMS-Schlüsselrichtlinie können CloudTrail Daten im S3-Quell-Bucket entschlüsselt, Validierungsprüfungen durchgeführt werden, um sicherzustellen, dass Ereignisse den CloudTrail Standards entsprechen, und Ereignisse in den CloudTrail Lake-Ereignisdatenspeicher kopiert werden.

Das folgende Beispiel enthält die KMS-Schlüsselrichtlinie, mit der die Daten im CloudTrail S3-Quell-Bucket entschlüsselt werden können. *Ersetzen Sie RoleARN myBucketName, MyAccountID, Region und eventDataStore Id durch die entsprechenden Werte für Ihre Konfiguration.* Die *myAccountID* ist die für CloudTrail Lake verwendete AWS Konto-ID, die möglicherweise nicht mit der AWS Konto-ID für den S3-Bucket identisch ist.

```
{
  "Sid": "AWSCloudTrailImportDecrypt",
  "Effect": "Allow",
  "Action": [
    "kms:Decrypt",
    "kms:GenerateDataKey"
  ],
  "Principal": {
    "AWS": "roleArn"
  },
  "Resource": "*",
  "Condition": {
    "StringLike": {
      "kms:EncryptionContext:aws:s3:arn": "arn:aws:s3:::myBucketName/*"
    },
    "StringEquals": {
      "aws:SourceAccount": "myAccountID",
      "aws:SourceArn":
        "arn:aws:cloudtrail:region:myAccountID:eventdataStore/eventDataStoreId"
    }
  }
}
```

## Kopieren Sie Trail-Ereignisse mithilfe der Konsole in einen vorhandenen Ereignisdatenspeicher CloudTrail

Gehen Sie wie folgt vor, um Trail-Ereignisse in einen bestehenden Ereignisdatenspeicher zu kopieren. Weitere Informationen zum Erstellen eines neuen Ereignisdatenspeichers finden Sie unter [Erstellen Sie mit der Konsole einen Ereignisdatenspeicher für CloudTrail Ereignisse](#).

### Note

Bevor Sie Trail-Ereignisse in einen vorhandenen Ereignisdatenspeicher kopieren, stellen Sie sicher, dass die Preisoption und der Aufbewahrungszeitraum des Ereignisdatenspeichers für Ihren Anwendungsfall entsprechend konfiguriert sind.

- **Preisoption:** Die Preisoption bestimmt die Kosten für die Erfassung und Speicherung von Ereignissen. Weitere Informationen zu Preisoptionen und Details finden Sie unter [AWS CloudTrail -Preise](#) und [Preisoptionen für den Ereignisdatenspeicher](#).
- **Aufbewahrungszeitraum:** Der Aufbewahrungszeitraum bestimmt, wie lange Ereignisdaten im Ereignisdatenspeicher aufbewahrt werden. CloudTrail kopiert nur Ereignisse, die eventTime innerhalb der Aufbewahrungsfrist des Veranstaltungsdatspeichers liegen. Um den geeigneten Aufbewahrungszeitraum zu ermitteln, nehmen Sie die Summe aus dem ältesten Ereignis, das Sie kopieren möchten, in Tagen und der Anzahl der Tage, an denen Sie die Ereignisse im Ereignisdatenspeicher speichern möchten (Aufbewahrungszeitraum = *oldest-event-in-days* + *number-days-to-retain*). Wenn das älteste Ereignis, das Sie kopieren, beispielsweise 45 Tage alt ist und Sie die Ereignisse weitere 45 Tage im Ereignisdatenspeicher aufbewahren möchten, würden Sie die Aufbewahrungsdauer auf 90 Tage festlegen.

So kopieren Sie Trail-Ereignisse in einen Ereignisdatenspeicher

1. Melden Sie sich bei der an AWS Management Console und öffnen Sie die CloudTrail Konsole unter <https://console.aws.amazon.com/cloudtrail/>.
2. Wählen Sie im linken Navigationsbereich der CloudTrail Konsole Trails aus.
3. Wählen Sie auf der Trails-Seite den Pfad aus und wählen Sie dann Copy events to Lake (Ereignisse nach Lake kopieren). Wenn der S3-Quell-Bucket für den Trail einen KMS-Schlüssel für die Datenverschlüsselung verwendet, stellen Sie sicher, dass die KMS-Schlüsselrichtlinie das Entschlüsseln von Daten im Bucket zulässt CloudTrail . Wenn der S3-Quell-Bucket mehrere

KMS-Schlüssel verwendet, müssen Sie die Richtlinien für jeden Schlüssel aktualisieren, damit CloudTrail die Daten im Bucket entschlüsselt werden können. Weitere Informationen zum Aktualisieren der KMS-Schlüssel-Richtlinie finden Sie unter [KMS-Schlüsselrichtlinie zum Entschlüsseln von Daten im S3-Quell-Bucket](#).

4. (Optional) Standardmäßig werden CloudTrail nur CloudTrail Ereignisse kopiert, die im CloudTrail Präfix des S3-Buckets und die Präfixe innerhalb des CloudTrail Präfixes enthalten sind, und überprüft keine Präfixe für andere Dienste. AWS Wenn Sie CloudTrail Ereignisse kopieren möchten, die in einem anderen Präfix enthalten sind, wählen Sie S3-URI eingeben und dann S3 durchsuchen, um zum Präfix zu navigieren.


Die S3-Bucket-Richtlinie muss CloudTrail Zugriff auf Copy-Trail-Ereignisse gewähren. Weitere Informationen zum Aktualisieren der S3-Bucket-Richtlinie finden Sie unter [Amazon-S3-Bucket-Richtlinie für das Kopieren von Trail-Ereignissen](#).

5. Wählen Sie unter Geben Sie einen Zeitraum für Ereignisse an den Zeitraum aus, in dem die Ereignisse kopiert werden sollen. CloudTrail überprüft das Präfix und den Namen der Protokolldatei, um sicherzustellen, dass der Name ein Datum zwischen dem ausgewählten Start- und Enddatum enthält, bevor versucht wird, Trail-Ereignisse zu kopieren. Sie können einen Relative range (Relativen Bereich) oder einen Absolute range (Absoluten Bereich) wählen. Um zu vermeiden, dass Ereignisse zwischen dem Quell-Trail und dem Zielergebnisdatenspeicher dupliziert werden, wählen Sie einen Zeitraum aus, der vor der Erstellung des Ereignisdatenspeichers liegt.

#### Note

CloudTrail kopiert nur Trail-Ereignisse, die eventTime innerhalb der Aufbewahrungsfrist des Event-Datenspeichers liegen. Wenn die Aufbewahrungsfrist eines Event-Datenspeichers beispielsweise 90 Tage beträgt, CloudTrail werden keine Trail-Ereignisse kopiert, die eventTime älter als 90 Tage sind.

- Wenn Sie Relativer Bereich wählen, können Sie wählen, ob Ereignisse kopiert werden sollen, die in den letzten 6 Monaten, 1 Jahr, 2 Jahren, 7 Jahren oder in einem benutzerdefinierten Bereich protokolliert wurden. CloudTrail kopiert die Ereignisse, die innerhalb des ausgewählten Zeitraums protokolliert wurden.
- Wenn Sie „Absoluter Bereich“ wählen, können Sie ein bestimmtes Start- und Enddatum wählen. CloudTrail kopiert die Ereignisse, die zwischen dem ausgewählten Start- und Enddatum aufgetreten sind.

6. Wählen Sie für Delivery location (Zustellungsort) den Zielereignisdatenspeicher aus der Dropdown-Liste aus.
  7. Wählen Sie für Permissions (Berechtigungen) unter den folgenden IAM-Rollenoptionen aus. Wenn Sie eine vorhandene IAM-Rolle auswählen, stellen Sie sicher, dass die IAM-Rollenrichtlinie die erforderlichen Berechtigungen bereitstellt. Weitere Informationen zum Aktualisieren der IAM-Rollenberechtigungen finden Sie unter [IAM-Berechtigungen zum Kopieren von Trail-Ereignissen](#).
    - Wählen Sie Create a new role (recommended) (Erstellen Sie eine neue Rolle (empfohlen)), um eine neue IAM-Rolle zu erstellen. Geben Sie für Enter IAM role name (IAM-Rollennamen eingeben) einen Namen für die Rolle ein. CloudTrail erstellt automatisch die erforderlichen Berechtigungen für diese neue Rolle.
    - Wählen Sie Eine benutzerdefinierte IAM-Rolle verwenden ARN aus, um eine benutzerdefinierte IAM-Rolle zu verwenden, die nicht aufgeführt ist. Geben Sie für Enter IAM role ARN (IAM-Rollen-ARN eingeben) den IAM-ARN ein.
    - Wählen Sie eine vorhandene IAM-Rolle aus der Drop-down-Liste aus.
  8. Wählen Sie Copy events (Kopieren von Ereignissen).
  9. Sie werden aufgefordert, das Kopieren zu bestätigen. Sobald Sie bereit sind zu bestätigen, wählen Sie Copy trail events to Lake (Trail-Ereignisse nach Lake kopieren) aus und dann wählen Sie Copy events (Ereignisse kopieren).
  10. Auf der Seite Copy details (Kopieren von Details) können Sie den Kopierstatus anzeigen und eventuelle Fehler überprüfen. Wenn eine Trail-Ereignis-Kopie abgeschlossen ist, wird der Copy status (Kopierstatus) entweder auf Completed (Abgeschlossen) festgelegt, wenn keine Fehler aufgetreten sind, oder auf Failed (Fehlgeschlagen), wenn Fehler aufgetreten sind.
-  **Note**

Details, die auf der Detailseite der Ereigniskopie angezeigt werden, sind nicht in Echtzeit. Die tatsächlichen Werte für Details wie Kopierte Präfixe können höher sein als die, die auf der Seite angezeigt werden. CloudTrail aktualisiert die Details im Verlauf der Ereigniskopie schrittweise.
11. Wenn der Copy status (Kopierstatus) Failed (Fehlgeschlagen) lautet, beheben Sie alle Fehler, die unter Copy failures (Kopierfehler) angezeigt werden, und wählen Sie dann Retry copy (Kopie wiederholen) aus. Wenn Sie erneut versuchen, eine Kopie zu erstellen, CloudTrail wird der Kopiervorgang an der Stelle fortgesetzt, an der der Fehler aufgetreten ist.

Weitere Informationen zum Anzeigen der Details eines Trail-Ereignisses finden Sie unter [Details zur Ereigniskopie](#).

## CloudTrail Logdateien abrufen und einsehen

Nachdem Sie einen Trail so eingerichtet haben, dass die gewünschten Protokolldateien erfasst werden, müssen Sie die Protokolldateien finden und die darin enthaltenen Informationen interpretieren können.

CloudTrail übermittelt Ihre Protokolldateien an einen Amazon S3 S3-Bucket, den Sie bei der Erstellung des Trails angeben. CloudTrail übermittelt Protokolle in der Regel innerhalb von durchschnittlich etwa 5 Minuten nach einem API-Aufruf. Diese Zeit ist nicht garantiert. Weitere Informationen finden Sie unter [AWS CloudTrail Service Level Agreement](#). Normalerweise werden Insights-Ereignisse in Ihrem Bucket innerhalb von 30 Minuten mit ungewöhnlichen Aktivitäten in Ihrem Bucket angezeigt. Nachdem Sie Insights-Ereignisse zum ersten Mal aktiviert haben, kann es bis zu 36 Stunden dauern, bis nach der Erkennung von ungewöhnlichen Aktivitäten die ersten Insights-Ereignisse erscheinen.

### Note

Wenn Sie Ihren Trail falsch konfigurieren (z. B. wenn der S3-Bucket nicht erreichbar ist), CloudTrail wird versucht, die Protokolldateien 30 Tage lang erneut in Ihren S3-Bucket zu übertragen. Für diese attempted-to-deliver Ereignisse fallen Standardgebühren an. CloudTrail Um Gebühren für einen falsch konfigurierten Trail zu vermeiden, müssen Sie den Trail löschen.

### Themen

- [Finden Sie Ihre Protokolldateien CloudTrail](#)
- [Deine CloudTrail Logdateien herunterladen](#)

## Finden Sie Ihre Protokolldateien CloudTrail

CloudTrail veröffentlicht Protokolldateien in Ihrem S3-Bucket in einem GZIP-Archiv. In diesem S3-Bucket hat die Protokolldatei einen formatierten Namen, der die folgenden Elemente enthält:

- Der Bucket-Name, den Sie bei der Erstellung des Trails angegeben haben (zu finden auf der Trails-Seite der CloudTrail Konsole)
- Das (optionale) Präfix, das Sie beim Erstellen des Trails angegeben haben
- Die Zeichenfolge "AWSLogs"
- Die Kontonummer
- Die Zeichenfolge "CloudTrail"
- Eine Regions-ID, z. B. "us-west-1"
- Das Jahr, in dem die Protokolldatei veröffentlicht wurde, im Format YYYY
- Den Monat, in dem die Protokolldatei veröffentlicht wurde, im Format MM
- Den Tag, an dem die Protokolldatei veröffentlicht wurde, im Format DD
- Eine alphanumerische Zeichenfolge, anhand derer sich die Datei von anderen Dateien zu demselben Zeitraum unterscheidet

Das folgende Beispiel zeigt einen vollständigen Protokolldatei-Objektnamen:

```
bucket_name/prefix_name/AWSLogs/Account ID/  
CloudTrail/region/YYYY/MM/DD/file_name.json.gz
```

#### Note

Bei Organisationstrails enthält der Objektname der Protokolldatei im S3-Bucket die ID der Organisationseinheit im Pfad, und zwar wie folgt:

```
bucket_name/prefix_name/AWSLogs/O-ID/Account ID/  
CloudTrail/Region/YYYY/MM/DD/file_name.json.gz
```

Zum Abrufen einer Protokolldatei können Sie die Amazon-S3-Konsole, die Amazon-S3-Befehlszeilenschnittstelle (CLI) oder die API verwenden.

Suchen Sie Protokolldateien mit der Amazon-S3-Konsole wie folgt

1. Öffnen Sie die Amazon S3-Konsole.
2. Wählen Sie den Bucket aus, den Sie angegeben haben.
3. Navigieren Sie durch die Objekthierarchie, bis Sie die gewünschte Protokolldatei finden.

Alle Protokolldateien haben eine GZ-Erweiterung.

Sie navigieren dabei durch eine Objekthierarchie, die dem folgenden Beispiel ähnelt; Bucket-Name, Konto-ID, Region und Datum sind jedoch anders.

```
All Buckets
  Bucket_Name
    AWSLogs
      123456789012
        CloudTrail
          us-west-1
            2014
              06
                20
```

Eine Protokolldatei für die obige Objekthierarchie sieht wie folgt aus:

```
123456789012_CloudTrail_us-west-1_20140620T1255ZHdkvFTX0A3Vnhbc.json.gz
```

#### Note

In seltenen Fällen kann es vorkommen, dass Sie Protokolldateien erhalten, die eines oder mehrere doppelte Ereignisse enthalten. In den meisten Fällen haben doppelte Ereignisse dieselbe eventID. Weitere Informationen zum Feld eventID finden Sie unter [CloudTrail Inhalt aufzeichnen](#).

## Deine CloudTrail Logdateien herunterladen

Protokolldateien haben das Format JSON. Wenn Sie ein Add-On für die Anzeige von JSON installiert haben, können Sie die Dateien direkt in Ihrem Browser anzeigen. Doppelklicken Sie auf den Namen der Protokolldatei im Bucket, um ein neues Browserfenster oder eine neue Registerkarte zu öffnen. Die JSON-Datei wird in einem lesbaren Format angezeigt.




CloudTrail Protokolldateien sind Amazon S3 S3-Objekte. Sie können die Amazon S3 S3-Konsole, die AWS Command Line Interface (CLI) oder die Amazon S3 S3-API verwenden, um Protokolldateien abzurufen.

Weitere Informationen finden Sie in der [Amazon S3 S3-Objektübersicht](#) im Amazon Simple Storage Service-Benutzerhandbuch.

Im folgenden Verfahren wird beschrieben, wie Sie eine Protokolldatei mit der AWS Management Console herunterladen.

So laden Sie eine Protokolldatei herunter und lesen sie

1. Öffnen Sie die Amazon-S3-Konsole unter <https://console.aws.amazon.com/s3/>.
2. Wählen Sie den Bucket und die Protokolldatei, die Sie herunterladen möchten.
3. Wählen Sie Download oder Download as und befolgen Sie die Anweisungen, um die Datei zu speichern. Hierdurch wird die Datei in einem komprimierten Format gespeichert.


 Note

Einige Browser, wie beispielsweise Chrome, extrahieren die Protokolldatei automatisch für Sie. Wenn Ihr Browser dies unterstützt, fahren Sie mit Schritt 5 fort.

4. Verwenden Sie ein Produkt wie [7-Zip](#), um die Protokolldatei zu extrahieren.
5. Öffnen Sie die Protokolldatei in einem Texteditor wie Notepad++.

Weitere Informationen über die Ereignis-Felder, die in einem Protokolldateieintrag angezeigt werden können, finden Sie unter [CloudTrail Inhalt aufzeichnen](#).

AWS arbeitet mit externen Spezialisten für Protokollierung und Analyse zusammen, um Lösungen bereitzustellen, die CloudTrail Ergebnisse verwenden. Weitere Informationen finden Sie unter [AWS CloudTrail Partner](#).

 Note

Sie können den Ereignisverlauf auch verwenden, um Ereignisse im Zusammenhang mit dem Erstellen, Aktualisieren und Löschen von API-Aktivitäten während der letzten 90 Tage nachzuschlagen.

Weitere Informationen finden Sie unter [Mit dem CloudTrail Eventverlauf arbeiten](#).

## Konfiguration von Amazon SNS SNS-Benachrichtigungen für CloudTrail

Sie können benachrichtigt werden, wenn neue Protokolldateien in Ihrem Amazon S3 S3-Bucket CloudTrail veröffentlicht werden. Sie verwalten Benachrichtigungen mit dem Amazon Simple Notification Service (Amazon SNS).

Benachrichtigungen sind optional. Wenn Sie Benachrichtigungen wünschen, konfigurieren Sie so CloudTrail, dass Aktualisierungsinformationen an ein Amazon SNS SNS-Thema gesendet werden, wenn eine neue Protokolldatei gesendet wurde. Um diese Benachrichtigungen zu erhalten, verwenden Sie Amazon SNS zum Abonnieren des Themas. Als Subscriber erhalten Sie Aktualisierungen, die an eine Amazon-Simple-Queue-Service-Warteschlange (Amazon SQS) gesendet wurden. So können Sie diese Benachrichtigungen programmgesteuert verarbeiten.

Themen

- [Konfiguration für CloudTrail das Senden von Benachrichtigungen](#)

### Konfiguration für CloudTrail das Senden von Benachrichtigungen

Sie können einen Trail für die Verwendung eines Amazon-SNS-Themas konfigurieren. Sie können die CloudTrail Konsole oder den [aws cloudtrail create-trail](#) CLI-Befehl verwenden, um das Thema zu erstellen. CloudTrail erstellt das Amazon SNS SNS-Thema für Sie und fügt eine entsprechende Richtlinie hinzu, sodass Sie CloudTrail berechtigt sind, zu diesem Thema zu veröffentlichen.

Wenn Sie einen SNS-Themennamen vergeben, muss der Name folgende Anforderungen erfüllen:

- Er muss zwischen 1 und 256 Zeichen lang sein.
- Er muss ASCII-Buchstaben mit Groß- und Kleinschreibung, Zahlen, Unterstriche oder Bindestriche enthalten.

Beim Konfigurieren von Benachrichtigungen für einen Trail, der auf alle Regionen angewendet wird, werden Benachrichtigungen von allen Regionen an das Amazon-SNS-Thema gesendet, das Sie festlegen. Wenn Sie einen oder mehrere regionsspezifische Trails eingerichtet haben, müssen Sie für jede Region ein eigenes Thema erstellen und jedes einzeln abonnieren.

Um Benachrichtigungen zu erhalten, abonnieren Sie das Amazon SNS SNS-Thema oder die Themen, die CloudTrail verwendet werden. Nutzen Sie hierfür die [Amazon-SNS-Konsole](#) oder [Amazon-SNS-CLI-Befehle](#). Weitere Informationen finden Sie unter [Amazon SNS-Thema abonnieren](#) im Amazon Simple Notification Service-Entwicklerhandbuch.

### Note

CloudTrail sendet eine Benachrichtigung, wenn Protokolldateien in den Amazon S3 S3-Bucket geschrieben werden. Bei einem aktiven Konto kann eine große Anzahl an Benachrichtigungen entstehen. Wenn Sie Benachrichtigungen per E-Mail oder SMS abonniert haben, erhalten Sie möglicherweise eine große Menge an Nachrichten. Wir empfehlen, die Benachrichtigung per Amazon Simple Queue Service (Amazon SQS) zu abonnieren, damit Sie Benachrichtigungen programmgesteuert verarbeiten können. Weitere Informationen finden Sie unter Tutorial: [Abonnieren einer Amazon-SQS-Warteschlange zu einem Amazon-SNS-Thema \(Konsole\)](#) im Amazon-Simple-Queue-Service-Entwicklerhandbuch.

Die Amazon-SNS-Benachrichtigung besteht aus einem JSON-Objekt mit einem Message-Feld. Im Feld Message ist der vollständige Pfad zur Protokolldatei angegeben, wie im folgenden Beispiel dargestellt:

```
{
  "s3Bucket": "your-bucket-name", "s3objectKey": ["AWSLogs/123456789012/
CloudTrail/us-east-2/2013/12/13/123456789012_CloudTrail_us-
west-2_20131213T1920Z_LnPgDQnpkSKEspV.json.gz"]
}
```

Wenn mehrere Protokolldateien an den Amazon-S3-Bucket übermittelt werden, beinhaltet eine Benachrichtigung u. U. mehrere Protokolle, wie im folgenden Beispiel dargestellt:

```
{
  "s3Bucket": "your-bucket-name",
  "s3objectKey": [
    "AWSLogs/123456789012/CloudTrail/us-
east-2/2016/08/11/123456789012_CloudTrail_us-
east-2_20160811T2215Z_kpaMYavMQA9Ahp7L.json.gz",
    "AWSLogs/123456789012/CloudTrail/us-
east-2/2016/08/11/123456789012_CloudTrail_us-
east-2_20160811T2210Z_zqDkyQv3TK8ZdLr0.json.gz",
  ]
}
```

```
"AWSLogs/123456789012/CloudTrail/us-
east-2/2016/08/11/123456789012_CloudTrail_us-
east-2_20160811T2205Z_jaMVRa6JfdLCJYHP.json.gz"
]
}
```

Wenn Sie Benachrichtigungen per E-Mail erhalten, besteht der E-Mail-Text aus dem Inhalt des Feldes `Message`. Informationen zur JSON-Struktur finden Sie unter [Warteschlangen von Fanout zu Amazon SQS](#) im Amazon Simple Notification Service Developer Guide. Nur das `Message` Feld zeigt Informationen. CloudTrail Die anderen Felder enthalten Informationen aus dem Amazon-SNS-Service.

Wenn Sie mit der CloudTrail API einen Trail erstellen, können Sie ein vorhandenes Amazon SNS SNS-Thema angeben, CloudTrail an das Sie Benachrichtigungen mit den [UpdateTrail](#) Oder-Vorgängen [CreateTrail](#) senden möchten. Sie müssen sicherstellen, dass das Thema existiert und dass es über Berechtigungen verfügt, die das Senden von Benachrichtigungen CloudTrail an dieses Thema ermöglichen. Siehe [Amazon SNS SNS-Themenrichtlinie für CloudTrail](#).

## Weitere Ressourcen

Weitere Informationen zu Amazon-SNS-Themen und zum Abonnieren von diesen finden Sie im [Entwicklerhandbuch zu Amazon Simple Notification Service](#).

## Tipps zum Verwalten von Trails

- Ab dem 12. April 2019 sind Pfade nur dort sichtbar, AWS-Regionen wo sie Ereignisse protokollieren. Wenn Sie einen Trail erstellen, der alle Ereignisse protokolliert AWS-Regionen, wird er in der Konsole AWS-Regionen in allen Bereichen der [AWS Partition](#) angezeigt, in der Sie arbeiten. Wenn Sie einen Trail erstellen, der nur Ereignisse in einer einzigen Datei protokolliert AWS-Region, können Sie ihn nur in dieser Datei anzeigen und verwalten AWS-Region.
- Wählen Sie zum Bearbeiten eines Trails aus der Liste dessen Namen aus.
- Konfigurieren Sie mindestens einen Trail, der für alle Regionen gilt, sodass Sie Protokolldateien aus allen Regionen der AWS Partition erhalten, in der Sie arbeiten.
- Zum Protokollieren von Ereignissen einer bestimmten Region und zum Übermitteln von Protokolldateien an einen S3-Bucket in derselben Region können Sie den Trail aktualisieren, um ihn auf eine einzelne Region anzuwenden. Das ist hilfreich, wenn Sie Ihre Protokolldateien trennen möchten. Möglicherweise möchten Sie, dass Benutzer ihre eigenen Logs in bestimmten Regionen verwalten, oder Sie möchten CloudWatch Log-Alarmer nach Regionen trennen.

- Wenn Sie Ereignisse von mehreren AWS Konten in einem Trail protokollieren möchten, sollten Sie in Erwägung ziehen, zunächst eine Organisation in AWS Organizations und dann einen Organisations-Trail zu erstellen.
- Bei der Erstellung mehrerer Trails fallen zusätzliche Kosten an. Weitere Informationen zu Preisen erhalten Sie unter [AWS CloudTrail – Preise](#).

## Verwaltung der CloudTrail Trailkosten

Als bewährte Methode empfehlen wir die Nutzung von AWS Services und Tools, die Ihnen bei der CloudTrail Kostenkontrolle helfen können. Sie können CloudTrail Trails auch so konfigurieren und verwalten, dass Sie die benötigten Daten erfassen und gleichzeitig kostengünstig bleiben. Weitere Informationen zur CloudTrail Preisgestaltung finden Sie unter [AWS CloudTrail Preise](#).

### Tools zur Kostenverwaltung

AWS Budgets, eine Funktion von AWS Billing and Cost Management, ermöglicht es Ihnen, benutzerdefinierte Budgets festzulegen, die Sie benachrichtigen, wenn Ihre Kosten oder Nutzung Ihren budgetierten Betrag überschreiten (oder voraussichtlich überschreiten werden).

Wenn Sie mehrere Pläne erstellen, empfiehlt es sich, mithilfe CloudTrail von AWS Budgets ein Budget für zu erstellen, das Ihnen dabei helfen kann, Ihre CloudTrail Ausgaben zu verfolgen. Kostenbasierte Budgets tragen dazu bei, das Bewusstsein dafür zu schärfen, wie viel Ihnen für Ihre CloudTrail Nutzung in Rechnung gestellt werden könnte. [Budgetwarnungen](#) benachrichtigen Sie, wenn Ihre Rechnung einen von Ihnen definierten Schwellenwert erreicht. Wenn Sie eine Budget-Warnung erhalten, können Sie Änderungen vor dem Ende des Abrechnungszeitraums vornehmen, um Ihre Kosten zu verwalten.

Nachdem Sie [ein Budget erstellt](#) haben, können Sie AWS Cost Explorer damit sehen, wie sich Ihre CloudTrail Kosten auf Ihre AWS Gesamtrechnung auswirken. Im AWS Cost Explorer können Sie nach dem Hinzufügen CloudTrail zum Servicefilter Ihre historischen CloudTrail Ausgaben mit denen Ihrer aktuellen Ausgaben month-to-date (MTD) vergleichen, sowohl nach Region als auch nach Konto. Mit dieser Funktion können Sie unerwartete Kosten in Ihren monatlichen CloudTrail Ausgaben überwachen und erkennen. Zusätzliche Funktionen im Cost Explorer ermöglichen es Ihnen, die CloudTrail Ausgaben mit den monatlichen Ausgaben auf der jeweiligen Ressourcenebene zu vergleichen und so Informationen darüber zu erhalten, was zu Kostenerhöhungen oder -senkungen in Ihrer Rechnung führen könnte.

**Note**

Sie können zwar Markierungen auf CloudTrail Wanderwege anwenden, können aber derzeit AWS Billing keine Markierungen, die auf Wanderwege angewendet wurden, für die Kostenzuweisung verwenden. Cost Explorer kann Kosten für CloudTrail Lake Event Data Stores und für den CloudTrail Service als Ganzes anzeigen.

Um mit AWS Budgets zu beginnen [AWS Billing and Cost Management](#), öffnen Sie das Fenster und wählen Sie dann in der linken Navigationsleiste Budgets aus. Wir empfehlen, bei der Erstellung eines Budgets Budgetwarnungen zu konfigurieren, um die CloudTrail Ausgaben nachzuverfolgen. Weitere Informationen zur Verwendung von AWS Budgets finden Sie unter [Kosten verwalten mit AWS Budgets](#) und [Bewährte Methoden für AWS Budgets](#).

## Trail-Konfiguration

CloudTrail bietet Flexibilität bei der Konfiguration von Trails in Ihrem Konto. Einige Entscheidungen, die Sie während des Einrichtungsprozesses treffen, setzen voraus, dass Sie die Auswirkungen auf Ihre CloudTrail Rechnung verstehen. Im Folgenden finden Sie Beispiele dafür, wie sich die Konfiguration von Pfaden auf Ihre CloudTrail Rechnung auswirken kann.

### Erstellen mehrerer Trails

Das erste Exemplar der Management-Veranstaltungen in jeder Region wird kostenlos zugestellt. Wenn Ihr Konto beispielsweise zwei Trails für eine einzelne Region, einen Trail in us-east-1 und einen weiteren Trail in hatus-west-2, fallen keine CloudTrail Gebühren an, da es in jeder Region nur ein Traillogging-Event gibt. Wenn dein Konto jedoch über einen Trail mit mehreren Regionen und einen zusätzlichen Trail mit einer einzelnen Region verfügt, fallen für den Trail mit einer Region Gebühren an, da der Trail mit mehreren Regionen bereits Ereignisse in jeder Region protokolliert.

Wenn du mehr Trails erstellst, die dieselben Managementereignisse an andere Ziele übertragen, fallen für diese nachfolgenden Lieferungen Kosten an. CloudTrail Sie können dies tun, um es verschiedenen Benutzergruppen (z. B. Entwickler, Sicherheitspersonal und IT-Prüfer) zu ermöglichen, ihre eigenen Kopien der Protokolldateien zu erhalten. Bei Datenereignissen fallen für alle Lieferungen CloudTrail Kosten an, auch für die erste.

Wenn Sie weitere Trails erstellen, ist es besonders wichtig, sich mit Ihren Protokollen vertraut zu machen und die Arten und Volumes von Ereignissen zu verstehen, die von Ressourcen in Ihrem

Konto generiert werden. Auf diese Weise können Sie das Volume der Ereignisse vorhersehen, die mit einem Konto verknüpft sind, und Trail-Kosten planen. Beispielsweise kann die Verwendung von AWS KMS-managed serverseitiger Verschlüsselung (SSE-KMS) für Ihre S3-Buckets zu einer großen Anzahl von Verwaltungsereignissen in führen. AWS KMS CloudTrail Größere Volumes von Ereignissen über mehrere Trails hinweg können sich ebenfalls auf die Kosten auswirken.

Um die Anzahl der Ereignisse zu begrenzen, die in Ihrem Trail protokolliert werden, können Sie Amazon RDS Data API-Ereignisse AWS KMS herausfiltern, indem Sie AWS KMS Ereignisse ausschließen oder Amazon RDS Data API-Ereignisse ausschließen auf den Seiten Trail erstellen oder Trail aktualisieren auswählen. Wenn Sie grundlegende Ereignisselectoren verwenden, können Sie nur Verwaltungsereignisse filtern. Sie können jedoch erweiterte Ereignisselectoren verwenden, um sowohl Verwaltungs- als auch Datenereignisse zu filtern. Sie können erweiterte Ereignisselectoren verwenden, um Datenereignisse auf der Grundlage der Felder `resources.type`, `eventName`, `resources.ARN` und `readOnly` einzuschließen oder auszuschließen, sodass Sie nur die Datenereignisse protokollieren, die Sie interessieren. Weitere Informationen zum Konfigurieren dieser Felder finden Sie unter [AdvancedFieldSelector](#). Weitere Informationen zum Erstellen und Aktualisieren eines Trails finden Sie unter [Erstellen eines Trails](#) oder [Aktualisieren eines Trails](#) in diesem Handbuch.

## AWS Organizations

Wenn Sie einen Organisations-Trail mit einrichten CloudTrail, CloudTrail repliziert den Trail auf jedes Mitgliedskonto innerhalb Ihrer Organisation. Der neue Trail wird zusätzlich zu den vorhandenen Trails in Mitgliedskonten erstellt. Stellen Sie sicher, dass die Konfiguration Ihres Organisations-Trails der gewünschten Trail-Konfiguration für alle Konten innerhalb einer Organisation entspricht, da die Konfiguration des Organisations-Trails in allen Konten übernommen wird.

Da Organizations einen Trail in jedem Mitgliedskonto erstellt, sammelt ein einzelnes Mitgliedskonto, das einen zusätzlichen Trail erstellt, um dieselben Verwaltungsereignisse wie der Organizations-Trail zu sammeln, eine zweite Kopie der Ereignisse. Das Konto wird für die zweite Kopie belastet. Wenn ein Konto über einen multiregionalen Trail verfügt und einen zweiten Trail in einer einzelnen Region erstellt, um dieselben Verwaltungsereignisse wie der multiregionale Trail zu erfassen, übermittelt der Trail in der einzelnen Region eine zweite Kopie der Ereignisse. Für die zweite Kopie fallen Gebühren an.

Weitere Informationen finden Sie auch unter

- [AWS CloudTrail – Preise](#)
- [Verwalten Sie Ihre Kosten mit AWS Budgets](#)
- [Erste Schritte mit Cost Explorer](#)
- [Vorbereiten der Erstellung eines Trails für Ihre Organisation](#)

## Benennungsanforderungen

Dieser Abschnitt enthält Informationen zu den Benennungsanforderungen für CloudTrail Ressourcen, Amazon S3 S3-Buckets und KMS-Schlüssel.

Themen

- [CloudTrail Anforderungen an die Benennung von Ressourcen](#)
- [Anforderungen zu Namen für Amazon-S3-Buckets](#)
- [AWS KMS Anforderungen an die Aliasbenennung](#)

### CloudTrail Anforderungen an die Benennung von Ressourcen

CloudTrail Ressourcennamen müssen die folgenden Anforderungen erfüllen:

- Sie dürfen nur ASCII-Buchstaben (a-z, A-Z), Ziffern (0-9), Punkte (.), Unterstriche (\_) oder Bindestriche (-) enthalten.
- Am Anfang und Ende des Namens sollte ein Buchstabe oder eine Zahl stehen.
- Der Name sollte 3 bis 128 Zeichen umfassen.
- Verwenden Sie keine nebeneinander stehenden Punkte, Unterstriche oder Bindestriche. Namen wie z. B. mein\_ Namespace oder mein-\ Namespace sind ungültig.
- Geben Sie den Namen nicht im IP-Adressformat ein (z. B. 192.168.5.4).

### Anforderungen zu Namen für Amazon-S3-Buckets

Der Amazon S3 S3-Bucket, den Sie zum Speichern von CloudTrail Protokolldateien verwenden, muss einen Namen haben, der den Benennungsanforderungen für Regionen entspricht, die nicht dem US-Standard entsprechen. Amazon S3 definiert einen Bucket-Namen als eine oder mehrere



Bezeichnungen, die durch Punkte getrennt sind. Eine vollständige Liste der Benennungsregeln finden Sie unter [Benennungsregeln für Buckets](#) im Benutzerhandbuch zu Amazon Simple Storage Service.

Dies ist eine Auswahl der Regeln:

- Der Bucket-Name muss eine Länge von 3 bis 63 Zeichen aufweisen und darf nur Kleinbuchstaben, Zahlen, Punkte und Gedankenstriche enthalten.
- Jedes Kennzeichen im Bucket-Namen muss mit einem Kleinbuchstaben oder einer Zahl beginnen.
- Der Bucket-Name darf keine Unterstriche enthalten, nicht mit einem Gedankenstrich enden und nicht mehrere aufeinanderfolgende Punkte bzw. benachbarte Gedankenstriche und Punkte aufweisen.
- Der Bucket-Name darf nicht wie eine IP-Adresse formatiert sein (198.51.100.24).

#### Warning

Da Ihr Bucket in S3 als URL verwendet werden kann, die öffentlich zugänglich ist, muss der Bucket-Name weltweit einmalig sein. Wenn ein anderes Konto bereits einen Bucket mit dem von Ihnen gewählten Namen erstellt hat, müssen Sie einen anderen Namen verwenden. Weitere Informationen finden Sie unter [Bucket-Einschränkungen und -Limits](#) im Benutzerhandbuch zu Amazon Simple Storage Service.

## AWS KMS Anforderungen an die Aliasbenennung

Wenn Sie einen erstellen AWS KMS key, können Sie einen Alias wählen, um ihn zu identifizieren. Sie könnten beispielsweise den Alias „KMS- CloudTrail -us-west-2“ wählen, um die Logs für einen bestimmten Trail zu verschlüsseln.

Der Alias muss die folgenden Anforderungen erfüllen:

- Zwischen 1 und 256 Zeichen, inklusive
- Enthält alphanumerische Zeichen (A-Z, a-z, 0-9), Bindestriche (-), Schrägstriche (/) und Unterstriche (\_)
- Darf nicht mit aws beginnen

Weitere Informationen finden Sie unter [Erstellen von Schlüsseln](#) im AWS Key Management Service - Entwicklerhandbuch.

## Erstellen von mehreren Trails

Sie können CloudTrail Protokolldateien verwenden, um Betriebs- oder Sicherheitsprobleme in Ihrem AWS Konto zu beheben. Sie können Trails für unterschiedliche Benutzer erstellen, die ihre eigenen Trails generieren und verwalten können. Sie können Trails zur Übermittlung von Protokolldateien an separate oder freigegebene S3-Buckets konfigurieren.

### Note

Die jeweils erste Kopie der Verwaltungsereignisse AWS-Region für ein Konto ist kostenlos. Wenn Sie mehrere Trails erstellen, die dieselben Management-Ereignisse an andere Ziele übertragen, fallen für diese nachfolgenden Lieferungen CloudTrail Kosten an. Weitere Informationen zu den CloudTrail Kosten finden Sie unter [AWS CloudTrail Preise](#) und [Verwaltung der CloudTrail Trailkosten](#).

Beispielsweise sind folgende Benutzer vorhanden:

- Ein Sicherheitsadministrator erstellt einen Trail in der Region Europa (Irland) und konfiguriert die KMS-Protokolldateiverschlüsselung. Der Trail übermittelt die Protokolldateien an einen S3 Bucket in der Region Europa (Irland).
- Ein IT-Auditor erstellt einen Trail in der Region Europa (Irland) und konfiguriert die Integritätsprüfung der Protokolldatei, um sicherzustellen, dass sich die Protokolldateien seit ihrer Übermittlung nicht geändert haben. CloudTrail Der Trail ist so konfiguriert, dass die Protokolldateien an einen S3 Bucket in der Region bereitgestellt werden
- Ein Entwickler erstellt einen Trail in der Region Europa (Frankfurt) und konfiguriert CloudWatch Alarme so, dass er Benachrichtigungen für bestimmte API-Aktivitäten erhält. Der Trail nutzt denselben S3-Bucket wie der Trail mit der konfigurierten Integritätsvalidierung von Protokolldateien.
- Ein anderer Entwickler erstellt einen Trail in der Region Europa (Frankfurt) und konfiguriert SNS. Die Protokolldateien werden in einem separaten S3 Bucket in der Region Europa (Frankfurt) bereitgestellt.

Die folgende Abbildung veranschaulicht dieses Beispiel.



### Note

Sie können bis zu fünf Trails pro AWS-Region Route erstellen. Ein Pfad mit mehreren Regionen zählt als ein Weg pro Region.

Sie können Berechtigungen auf Ressourcenebene verwenden, um die Fähigkeit eines Benutzers zu verwalten, bestimmte Operationen auszuführen. CloudTrail

Sie können beispielsweise einem Benutzer die Berechtigung zum Anzeigen von Trail-Aktivitäten erteilen, ihm aber das Starten oder Beenden der Protokollierung für einen Trail verweigern. Einem anderen Benutzer hingegen können Sie umfassende Berechtigungen zum Erstellen und Löschen von Trails erteilen. Auf diese Weise können Sie Ihre Trails und den Benutzerzugriff präzise steuern.

Weitere Informationen zu Berechtigungen auf Ressourcenebene finden Sie unter [Beispiele: Erstellen und Anwenden von Richtlinien bei Aktionen für bestimmte Trails](#).

Weitere Informationen zu mehreren Wanderwegen finden Sie in den [CloudTrail häufig gestellten Fragen](#).

## Benutzerberechtigungen für CloudTrail Trails kontrollieren

AWS CloudTrail lässt sich in AWS Identity and Access Management (IAM) integrieren, sodass Sie den Zugriff auf CloudTrail und andere benötigte AWS Ressourcen kontrollieren können. CloudTrail Beispiele für diese Ressourcen umfassen Amazon-S3-Buckets und Themen von Amazon Simple Notification Service (Amazon SNS). Mit IAM können Sie steuern, welche AWS Benutzer CloudTrail Trails erstellen, konfigurieren oder löschen, die Protokollierung starten und beenden und auf die Buckets zugreifen können, die Protokollinformationen enthalten. Weitere Informationen hierzu finden Sie unter [Identity and Access Management für AWS CloudTrail](#).

Die folgenden Themen helfen Ihnen, Berechtigungen, Richtlinien und CloudTrail Sicherheit zu verstehen:

- [Erteilen von Berechtigungen für die CloudTrail Verwaltung](#)
- [Benennungsregeln für Amazon-S3-Buckets](#)
- [Amazon S3 S3-Bucket-Richtlinie für CloudTrail](#)
- Ein Beispiel für eine Bucket-Richtlinie für einen Organisations-Trail in [Erstellen eines Trails für eine Organisation mit dem AWS Command Line Interface](#).
- [Amazon SNS SNS-Themenrichtlinie für CloudTrail](#)
- [CloudTrail Logdateien mit AWS KMS Schlüsseln verschlüsseln \(SSE-KMS\)](#)
- [Erforderliche Berechtigungen zum Kopieren von Trail-Ereignissen](#)
- [Erforderliche Berechtigungen zum Zuweisen delegierter Administratoren](#)
- [In CloudTrail der Konsole erstellte Standard-KMS-Schlüsselrichtlinie](#)
- [Erteilen Sie die Berechtigung zum Anzeigen von AWS Config Informationen auf der Konsole CloudTrail](#)
- [CloudTrail Protokolldateien zwischen AWS Konten teilen](#)
- [Erforderliche Berechtigungen für die Erstellung eines Organisations-Trails](#)
- [Verwenden einer bereits vorhandenen IAM-Rolle, um Amazon Logs die Überwachung eines Organisationstrails hinzuzufügen CloudWatch](#)

# Verwendung AWS CloudTrail mit VPC-Endpunkten mit Schnittstelle

Wenn Sie Amazon Virtual Private Cloud (Amazon VPC) zum Hosten Ihrer AWS Ressourcen verwenden, können Sie eine private Verbindung zwischen Ihrer VPC und herstellen. AWS CloudTrail Sie können diese Verbindung verwenden, CloudTrail um mit Ihren Ressourcen auf Ihrer VPC zu kommunizieren, ohne das öffentliche Internet nutzen zu müssen.

Amazon VPC ist ein AWS Service, mit dem Sie AWS Ressourcen in einem von Ihnen definierten virtuellen Netzwerk starten können. Mit einer VPC haben Sie die Kontrolle über Ihre Netzwerkeinstellungen, wie IP-Adressbereich, Subnetze, Routing-Tabellen und Netzwerk-Gateways. Bei VPC-Endpunkten wird das Routing zwischen der VPC und den AWS Diensten vom AWS Netzwerk abgewickelt, und Sie können IAM-Richtlinien verwenden, um den Zugriff auf Dienstressourcen zu steuern.

Um Ihre VPC zu verbinden CloudTrail, definieren Sie einen VPC-Schnittstellen-Endpunkt für. CloudTrail Ein Schnittstellenendpunkt ist eine elastic network interface mit einer privaten IP-Adresse, die als Einstiegspunkt für Datenverkehr dient, der für einen unterstützten AWS Dienst bestimmt ist. Der Endpunkt bietet zuverlässige, skalierbare Konnektivität, CloudTrail ohne dass ein Internet-Gateway, eine NAT-Instanz (Network Address Translation) oder eine VPN-Verbindung erforderlich sind. Weitere Informationen finden Sie unter [Was ist Amazon VPC](#) im Benutzerhandbuch zu Amazon VPC.

Schnittstelle, auf der VPC-Endpunkte basieren AWS PrivateLink, eine AWS Technologie, die private Kommunikation zwischen AWS Diensten über eine elastic network interface mit privaten IP-Adressen ermöglicht. Weitere Informationen finden Sie unter [AWS PrivateLink](#)

Die folgenden Schritte sind für Benutzer von Amazon VPC vorgesehen. Weitere Informationen finden Sie unter [Erste Schritte mit Amazon VPC](#) im Amazon-VPC-Benutzerhandbuch.

## Verfügbarkeit

CloudTrail unterstützt derzeit VPC-Endpunkte in den folgenden Regionen: AWS

- US East (Ohio)
- USA Ost (Nord-Virginia)
- USA West (Nordkalifornien)
- USA West (Oregon)
- Africa (Cape Town)

- Asien-Pazifik (Hongkong)
- Asien-Pazifik (Hyderabad)
- Asien-Pazifik (Jakarta)
- Asien-Pazifik (Melbourne)
- Asien-Pazifik (Mumbai)
- Asia Pacific (Osaka)
- Asia Pacific (Seoul)
- Asien-Pazifik (Singapur)
- Asien-Pazifik (Sydney)
- Asien-Pazifik (Tokio)
- Canada (Central)
- Kanada West (Calgary)
- Europe (Frankfurt)
- Europa (Irland)
- Europa (London)
- Europa (Milan)
- Europa (Paris)
- Europa (Spain)
- Europa (Stockholm)
- Europa (Zürich)
- Israel (Tel Aviv)
- Naher Osten (Bahrain)
- Naher Osten (VAE)
- Südamerika (São Paulo)
- AWS GovCloud (US-Ost)
- AWS GovCloud (US-West)

## Erstellen Sie einen VPC-Endpunkt für CloudTrail

Um mit der Verwendung CloudTrail mit Ihrer VPC zu beginnen, erstellen Sie einen VPC-Schnittstellen-Endpunkt für. CloudTrail Weitere Informationen finden Sie unter [Zugreifen und](#)

[AWS-Service Verwenden eines VPC-Endpunkts mit einer Schnittstelle](#) im Amazon VPC-Benutzerhandbuch.

Sie müssen die Einstellungen für nicht ändern. CloudTrail CloudTrail ruft andere auf, die entweder öffentliche Endpunkte oder VPC-Endpunkte mit privater Schnittstelle AWS-Services verwenden, je nachdem, welche verwendet werden.

## Gemeinsam genutzte Subnetze

Ein CloudTrail VPC-Endpunkt kann wie jeder andere VPC-Endpunkt nur von einem Besitzerkonto im gemeinsam genutzten Subnetz erstellt werden. Ein Teilnehmerkonto kann jedoch CloudTrail VPC-Endpunkte in Subnetzen verwenden, die mit dem Teilnehmerkonto gemeinsam genutzt werden. Weitere Informationen zur Freigabe von Amazon-VPC-Subnetzen finden Sie unter [Freigeben Ihrer VPC für andere Konten](#) im Benutzerhandbuch von Amazon VPC.

## AWS-Konto Sperrung und Wege

AWS CloudTrail überwacht und zeichnet kontinuierlich Ereignisse im Zusammenhang mit Kontoaktivitäten auf, die von einem beliebigen Benutzer, einer Rolle oder AWS-Service für einen generiert wurden AWS-Konto. Benutzer können einen CloudTrail Trail erstellen, um eine Kopie dieser Ereignisse in einem S3-Bucket zu erhalten, den sie besitzen.

CloudTrail ist ein grundlegender Sicherheitsdienst, weshalb von Benutzern erstellte Trails weiterhin existieren und Ereignisse auslösen, auch wenn ein AWS-Konto System geschlossen wurde, es sei denn, ein Benutzer löscht die Trails AWS-Konto vor dem Schließen ausdrücklich. Dieses Verhalten gilt auch für Organisationspfade, die vom Verwaltungskonto oder vom delegierten Administrator erstellt werden, sowie für Organisationspfade mit mehreren Regionen, die dann in den Mitgliedskonten der Organisation erstellt werden. Dadurch wird sichergestellt, dass, wenn ein Benutzer ein geschlossenes Konto erneut öffnet, dieser Benutzer über eine ununterbrochene Aufzeichnung der Kontoaktivitäten verfügt. Es bietet Benutzern auch Einblick in alle endgültigen Kontoaktivitäten, einschließlich der Löschung und Beendigung verbleibender Kontoressourcen und -services.

Benutzer haben die Möglichkeit, Trails zu löschen, bevor sie ihre Trails schließen AWS-Konto, oder sich an uns zu wenden, [AWS Supportum](#) das Löschen von Trails zu beantragen, nachdem sie geschlossen AWS-Konto wurden.

Weitere Informationen zum Schließen eines AWS-Konto finden Sie unter [Schließen eines AWS-Konto](#).

 Note

Wenn die Überprüfung der CloudTrail Protokolldatei aktiviert ist, erhalten Benutzer weiterhin stündlich Übersichtsdateien, die angeben, ob CloudTrail Protokolle erstellt wurden oder nicht. CloudTrail Lake-Event-Datenspeicher, CloudTrail Lake-Kanäle für Integrationen, CloudTrail serviceverknüpfte Kanäle und Ressourcen, die für Trails erstellt wurden (z. B. Amazon CloudWatch Logs-Protokollgruppen und Amazon S3 S3-Buckets, die im geschlossenen Konto vorhanden sind), folgen dem AWS Standardverhalten für die Kontoschließung und werden nach Ablauf des Zeitraums nach der Schließung (in der Regel 90 Tage) dauerhaft gelöscht.



# CloudTrail Einstellungen konfigurieren

Sie können die Einstellungsseite auf der CloudTrail Konsole verwenden, um CloudTrail Einstellungen zu konfigurieren und zu überprüfen.

So greifen Sie auf die Einstellungsseite zu

1. Melden Sie sich bei der an AWS Management Console und öffnen Sie die CloudTrail Konsole unter <https://console.aws.amazon.com/cloudtrail/>.
2. Wählen Sie im linken Navigationsbereich der CloudTrail Konsole Einstellungen aus.
3. Überprüfen und aktualisieren Sie die Einstellungen nach Bedarf.

Die folgenden Einstellungen sind verfügbar:

- [Delegierte Organisationsadministratoren](#) — Wenn Sie über eine AWS Organizations Organisation verfügen, können Sie CloudTrail delegierte Administratoren anzeigen, delegierte Administratoren hinzufügen (maximal drei) und delegierte Administratoren entfernen. Nur das Verwaltungskonto der Organisation kann delegierte Administratoren hinzufügen oder entfernen.

Mit dem Verwaltungskonto der Organisation kann jedem Konto innerhalb der Organisation die Rolle eines CloudTrail delegierten Administrators zugewiesen werden, der im Namen der Organisation die Trails und die Ereignisdatenspeicher der Organisation verwaltet.

- [Serviceverknüpfte Kanäle](#)— Sie können alle mit Diensten verknüpften Kanäle einsehen, die für Ihr Konto erstellt wurden.

AWS-Services kann einen serviceverknüpften Kanal einrichten, um CloudTrail Ereignisse in Ihrem Namen zu empfangen. Der AWS Dienst, der den serviceverknüpften Kanal erstellt, konfiguriert erweiterte Ereignisauswahlmöglichkeiten für den Kanal und gibt an, ob der Kanal für alle AWS-Regionen oder für einen einzelnen Kanal gilt. AWS-Region

## Delegierte Administratoren einer Organisation

Wenn Sie die Software CloudTrail zusammen mit einer AWS Organizations Organisation verwenden, können Sie jedem Konto innerhalb der Organisation die Rolle eines CloudTrail delegierten Administrators zuweisen, der die Trails und Event-Datenspeicher der Organisation im Namen der Organisation verwaltet. Ein delegierter Administrator ist ein Mitgliedskonto in einer Organisation, das

dieselben Verwaltungsaufgaben (sofern nicht anders [angegeben](#)) ausführen kann CloudTrail wie das Verwaltungskonto.

Wenn Sie einen delegierten Administrator auswählen, verfügt das betreffende Mitgliedskonto über Administratorberechtigungen für alle Trails und Ereignisdatenspeicher in der Organisation. Das Hinzufügen eines delegierten Administrators hat keine Auswirkungen auf die Verwaltung oder Ausführung der Trails oder Ereignisdatenspeicher der Organisation.

Wenn Sie zum ersten Mal einen delegierten Administrator in der CloudTrail Konsole oder mithilfe der CloudTrail API AWS CLI oder hinzufügen, wird CloudTrail geprüft, ob das Verwaltungskonto der Organisation eine dienstbezogene Rolle hat. Wenn das Verwaltungskonto keine dienstbezogene Rolle hat, CloudTrail erstellt es die dienstverknüpfte Rolle für das Verwaltungskonto. Weitere Informationen zu serviceverknüpften Rollen finden Sie unter [Verwenden von serviceverknüpften Rollen für AWS CloudTrail](#).

#### Note

Wenn Sie einen delegierten Administrator mithilfe der AWS Organizations CLI- oder API-Operation hinzufügen, wird die dienstverknüpfte Rolle nicht erstellt, wenn sie nicht existiert. Die dienstverknüpfte Rolle wird nur erstellt, wenn Sie vom Verwaltungskonto aus einen direkten Anruf an den CloudTrail Service tätigen, z. B. wenn Sie einen delegierten Administrator hinzufügen oder mithilfe der CloudTrail Konsole oder API einen Organization Trail- oder Event-Datenspeicher erstellen. AWS CLI CloudTrail

Beachten Sie die folgenden Faktoren, die definieren, wie der delegierte Administrator arbeitet. CloudTrail

Das Verwaltungskonto bleibt Eigentümer aller CloudTrail Organisationsressourcen, die der delegierte Administrator erstellt.

Das Verwaltungskonto der Organisation bleibt der Besitzer aller CloudTrail Organisationsressourcen, die der delegierte Administrator erstellt, wie z. B. Pfade und Ereignisdatenspeicher. Das sorgt für Kontinuität in der Organisation, falls der delegierte Administrator wechselt.

Durch das Entfernen eines delegierten Administratorkontos werden keine vom Administrator erstellten CloudTrail Organisationsressourcen gelöscht.

Organisationspfade und Ereignisdatenspeicher, die vom delegierten Administrator erstellt wurden, werden nicht gelöscht, wenn Sie den delegierten Administrator entfernen, da das Verwaltungskonto immer als Besitzer der CloudTrail Organisationsressourcen fungiert, unabhängig davon, ob sie vom delegierten Administrator oder vom Verwaltungskonto erstellt wurden.

Eine Organisation kann maximal drei CloudTrail delegierte Administratoren haben.

Sie können maximal drei CloudTrail delegierte Administratoren pro Organisation haben. Weitere Informationen zum Entfernen delegierter Administratoren finden Sie unter [Entfernen Sie einen CloudTrail delegierten Administrator](#).

Die folgende Tabelle zeigt die Funktionen des Verwaltungskontos, der delegierten Administratorkonten und der Konten, die Mitglieder der AWS Organizations Organisation sind.

Funktionen	Verwaltungskonto	Delegiertes Administratorkonto	Mitgliedskonten
Delegierte Administratorkonten hinzufügen/entfernen	Ja	Nein	Nein
Organisations-Trail erstellen	Ja	Ja <sup>1</sup>	Nein
Liste der Organisations-Trails ansehen	Ja	Ja	Ja
Organisations-Trails aktualisieren	Ja	Ja <sup>1, 2</sup>	Nein
Organisations-Trails löschen	Ja	Ja	Nein
Erstellen Sie einen Organisationsereignisdatenspeicher für CloudTrail Ereignisse oder AWS Config Konfigurationselemente.	Ja	Ja	Nein

Funktionen	Verwaltungskonto	Delegiertes Administratorkonto	Mitgliedskonten
Insights im Ereignisdatenspeicher einer Organisation aktivieren	Ja	Nein	Nein
Ereignisdatenspeicher einer Organisation aktualisieren	Ja	Ja <sup>2</sup>	Nein
Lake-Abfrageverbund im Ereignisdatenspeicher einer Organisation aktivieren <sup>3</sup>	Ja	Ja	Nein
Lake-Abfrageverbund im Ereignisdatenspeicher einer Organisation deaktivieren	Ja	Ja	Nein
Ereignisdatenspeicher einer Organisation löschen	Ja	Ja	Nein
Trail-Ereignisse in den Ereignisdatenspeicher einer Organisation kopieren	Ja	Nein	Nein
Abfragen in Ereignisdatenspeichern einer Organisation ausführen	Ja	Ja	Nein
Lake-Dashboard für den Ereignisdatenspeicher einer Organisation ansehen	Ja	Ja	Nein

<sup>1</sup> Der delegierte Administrator kann eine CloudWatch Logs-Protokollgruppe nur mithilfe der `UpdateTrail` API-Operationen `AWS CLI` oder `CloudTrail CreateTrail` oder konfigurieren. Sowohl die CloudWatch Logs-Log-Gruppe als auch die Log-Rolle müssen im aufrufenden Konto vorhanden sein.

<sup>2</sup> Nur das Verwaltungskonto kann einen Pfad- oder Ereignisdatenspeicher einer Organisation in einen Trail- oder Ereignisdatenspeicher auf Kontoebene oder einen Protokoll- oder Ereignisdatenspeicher auf Kontoebene in einen Pfad- oder Ereignisdatenspeicher für Organisationen konvertieren. Diese Aktionen sind für den delegierten Administrator nicht zulässig, da Trails und Ereignisdatenspeicher von Organisationen nur im Verwaltungskonto vorhanden sind. Wenn ein Trail- oder Event-Datenspeicher einer Organisation in einen Trail- oder Event-Datenspeicher auf Kontoebene konvertiert wird, hat nur das Verwaltungskonto Zugriff auf den Trail- oder Event-Datenspeicher.

<sup>3</sup> Nur ein einziges delegiertes Administratorkonto oder das Verwaltungskonto können den Verbund für den Ereignisdatenspeicher einer Organisation aktivieren. Andere delegierte Administratorkonten können mithilfe des [Lake-Formation-Datenfreigabefeatures](#) Informationen abfragen und austauschen. Jedes delegierte Administratorkonto sowie das Verwaltungskonto der Organisation können den Verbund deaktivieren.

## Themen

- [Erforderliche Berechtigungen zum Zuweisen delegierter Administratoren](#)
- [Fügen Sie einen delegierten Administrator hinzu CloudTrail](#)
- [Entfernen Sie einen CloudTrail delegierten Administrator](#)

## Erforderliche Berechtigungen zum Zuweisen delegierter Administratoren

Wenn Sie einen CloudTrail delegierten Administrator zuweisen, müssen Sie über die Berechtigungen zum Hinzufügen und Entfernen des delegierten Administrators sowie über bestimmte AWS Organizations API-Aktionen und IAM-Berechtigungen verfügen CloudTrail, die in der folgenden Richtlinienerklärung aufgeführt sind.

Sie können die folgende Anweisung am Ende einer vorhandenen IAM-Richtlinie hinzufügen, um diese Berechtigungen zu erteilen:

```
{
  "Sid": "Permissions",
  "Effect": "Allow",
  "Action": [
    "cloudtrail:RegisterOrganizationDelegatedAdmin",
    "cloudtrail:DeregisterOrganizationDelegatedAdmin",
    "organizations:RegisterDelegatedAdministrator",
    "organizations:DeregisterDelegatedAdministrator",
    "organizations:ListAWSServiceAccessForOrganization",
    "iam:CreateServiceLinkedRole",
```

```
    "iam:GetRole"  
  ],  
  "Resource": "*" }  
}
```

## Fügen Sie einen delegierten Administrator hinzu CloudTrail

Sie können einen delegierten Administrator hinzufügen, um die CloudTrail Ressourcen einer Organisation zu verwalten, wie z. B. Datenspeicher und Datenspeicher für Ereignisse.

Sie können einen CloudTrail delegierten Administrator für Ihre AWS Organisation über die CloudTrail Konsole oder die hinzufügen. AWS CLI

Bevor Sie einen delegierten Administrator hinzufügen, sollten Sie sicherstellen, dass dieser ein Konto in Ihrer Organisation hat und Sie mit dem Verwaltungskonto für Ihre Organisation angemeldet sind. Informationen zum Erstellen eines neuen AWS Kontos für Ihre Organisation finden Sie unter [AWS Konto in Ihrer Organisation erstellen](#). Informationen dazu, wie Sie ein vorhandenes AWS Konto zu Ihrer Organisation einladen können, finden Sie unter [Ein AWS Konto zum Beitritt zu Ihrer Organisation einladen](#).

### CloudTrail console

Das folgende Verfahren zeigt Ihnen, wie Sie mithilfe der CloudTrail Konsole einen CloudTrail delegierten Administrator hinzufügen.

1. Melden Sie sich bei der an AWS Management Console und öffnen Sie die CloudTrail Konsole unter <https://console.aws.amazon.com/cloudtrail/>.
2. Wählen Sie im linken Navigationsbereich der CloudTrail Konsole Einstellungen aus.
3. Wählen Sie im Bereich Organization delegated administrators (Delegierte Administratoren der Organisation) die Option Register administrator (Administrator registrieren) aus.
4. Geben Sie die zwölfstellige AWS Konto-ID des Kontos ein, das Sie als CloudTrail delegierten Administrator für die Trails und Event-Datenspeicher der Organisation zuweisen möchten.
5. Wählen Sie Register administrator (Administrator registrieren) aus.

### AWS CLI

Im folgenden Beispiel wird ein CloudTrail delegierter Administrator hinzugefügt.

```
aws cloudtrail register-organization-delegated-admin
```

```
--member-account-id="memberAccountId"
```

Dieser Befehl erzeugt keine Ausgabe, wenn er erfolgreich ist.

## Entfernen Sie einen CloudTrail delegierten Administrator

Sie können einen CloudTrail delegierten Administrator mithilfe der CloudTrail Konsole oder der AWS CLI entfernen.

### CloudTrail console

Das folgende Verfahren zeigt Ihnen, wie Sie einen CloudTrail delegierten Administrator mithilfe der CloudTrail Konsole entfernen.

1. Melden Sie sich bei der an AWS Management Console und öffnen Sie die CloudTrail Konsole unter <https://console.aws.amazon.com/cloudtrail/>.
2. Wählen Sie im linken Navigationsbereich der CloudTrail Konsole Einstellungen aus.
3. Wählen Sie im Bereich Organization delegated administrators (Delegierte Administratoren der Organisation) den delegierten Administrator aus, den Sie entfernen möchten.
4. Wählen Sie Remove administrator (Administrator entfernen) aus.
5. Bestätigen Sie, dass Sie den delegierten Administrator entfernen möchten, und wählen Sie dann Remove administrator (Administrator entfernen) aus.

### AWS CLI

Mit dem folgenden Befehl wird ein CloudTrail delegierter Administrator entfernt.

```
aws cloudtrail deregister-organization-delegated-admin  
--delegated-admin-account-id="delegatedAdminAccountId"
```

Dieser Befehl erzeugt keine Ausgabe, wenn er erfolgreich ist.

## Serviceverknüpfte Kanäle

AWS Dienste können einen mit Diensten verknüpften Kanal einrichten, über den CloudTrail Ereignisse in Ihrem Namen empfangen werden. Der AWS Dienst, der den serviceverknüpften Kanal

erstellt, konfiguriert erweiterte Ereignisauswahlmöglichkeiten für den Kanal und gibt an, ob der Kanal für alle AWS-Regionen oder für einen einzelnen Kanal gilt. AWS-Region

## Themen

- [Anzeigen von serviceverknüpften Kanälen mithilfe der Konsole](#)
- [Mit dem Dienst verknüpfte Kanäle anzeigen AWS CLI](#)

## Anzeigen von serviceverknüpften Kanälen mithilfe der Konsole

Mithilfe der CloudTrail Konsole können Sie Informationen zu allen CloudTrail serviceverknüpften Kanälen anzeigen, die von Diensten erstellt wurden. AWS Die Tabelle ist leer, wenn Ihr Konto keine serviceverknüpften Kanäle hat.

Gehen Sie wie folgt vor, um Informationen über einen serviceverknüpften Kanal anzuzeigen.

1. Wählen Sie im linken Navigationsbereich der CloudTrail Konsole Einstellungen aus.
2. Wählen Sie unter Serviceverknüpfte Kanäle einen serviceverknüpften Kanal aus, um dessen Details einzusehen.
3. Überprüfen Sie auf der Detailseite die konfigurierten Einstellungen für den serviceverknüpften Kanal.

Auf der Detailseite können Sie die folgenden Informationen anzeigen:

- Kanalname – Der vollständige Name des Kanals. Das Kanalnamenformat `aws-service-channel/AWS_service_name/slc AWS_service_name` steht dabei für den Namen des AWS Dienstes, der den Kanal verwaltet.
- Kanal-ARN – Der ARN des Kanals, den Sie in einer API-Anforderung verwenden können, um Details über den Kanal zu erhalten.
- Alle Regionen – Der Wert ist Yes, wenn der Kanal für alle AWS-Regionen konfiguriert ist.
- AWS service — Der Name des AWS Dienstes, der den Kanal verwaltet.
- Verwaltungsereignisse – Zeigt alle für den Kanal konfigurierten Verwaltungsereignisse an.
- Datenereignisse – Zeigt alle für den Kanal konfigurierten Datenereignisse an.



## Mit dem Dienst verknüpfte Kanäle anzeigen AWS CLI

Mithilfe von können Sie Informationen zu allen CloudTrail dienstverknüpften Kanälen anzeigen, die von Diensten erstellt AWS wurden. AWS CLI

Themen

- [Holen Sie sich einen CloudTrail dienstverknüpften Kanal](#)
- [Listet alle mit Diensten CloudTrail verknüpften Kanäle auf](#)
- [AWS Serviceereignisse auf Kanälen, die mit Diensten verknüpft sind](#)

### Holen Sie sich einen CloudTrail dienstverknüpften Kanal

Der folgende AWS CLI Beispielbefehl gibt Informationen über einen bestimmten mit einem CloudTrail Dienst verknüpften Kanal zurück, einschließlich des Namens des AWS Zieldienstes, aller für den Kanal konfigurierten erweiterten Selektoren und der Angabe, ob der Kanal für alle Regionen oder eine einzelne Region gilt.

Sie müssen einen ARN oder das ID-Suffix eines ARNs für `--channel` angeben.

```
aws cloudtrail get-channel --channel EXAMPLE-ee54-4813-92d5-999aeEXAMPLE
```

Nachfolgend finden Sie eine Beispielantwort. In diesem Beispiel `AWS_service_name` steht er für den Namen des AWS Dienstes, der den Kanal erstellt hat.

```
{
  "ChannelArn": "arn:aws:cloudtrail:us-east-1:111122223333:channel/EXAMPLE-ee54-4813-92d5-999aeEXAMPLE",
  "Name": "aws-service-channel/AWS_service_name/slc",
  "Source": "CloudTrail",
  "SourceConfig": {
    "ApplyToAllRegions": false,
    "AdvancedEventSelectors": [
      {
        "Name": "Management Events Only",
        "FieldSelectors": [
          {
            "Field": "eventCategory",
            "Equals": [
```

```

        "Management"
      ]
    }
  ]
},
"Destinations": [
  {
    "Type": "AWS_SERVICE",
    "Location": "AWS_service_name"
  }
]
}

```

## Listet alle mit Diensten CloudTrail verknüpften Kanäle auf

Der folgende AWS CLI Beispielbefehl gibt Informationen zu allen CloudTrail serviceverknüpften Kanälen zurück, die in Ihrem Namen erstellt wurden. Optionale Parameter umfassen `--max-results`, um eine maximale Anzahl von Ergebnissen anzugeben, die der Befehl auf einer einzelnen Seite zurückgeben soll. Wenn es mehr Ergebnisse als den von Ihnen angegebenen `--max-results`-Wert gibt, führen Sie den Befehl `NextToken` erneut aus und fügen den zurückgegebenen Wert hinzu, um die nächste Seite mit Ergebnissen zu erhalten.

```
aws cloudtrail list-channels
```

Nachfolgend finden Sie eine Beispielantwort. In diesem Beispiel `AWS_service_name` steht er für den Namen des AWS Dienstes, der den Kanal erstellt hat.

```

{
  "Channels": [
    {
      "ChannelArn": "arn:aws:cloudtrail:us-east-1:111122223333:channel/EXAMPLE-ee54-4813-92d5-999aeEXAMPLE",
      "Name": "aws-service-channel/AWS_service_name/slc"
    }
  ]
}

```

## AWS Serviceereignisse auf Kanälen, die mit Diensten verknüpft sind

Der AWS Dienst, der den mit dem Dienst verbundenen Kanal verwaltet, kann Aktionen auf dem mit dem Dienst verbundenen Kanal einleiten (z. B. einen mit dem Dienst verbundenen Kanal erstellen oder aktualisieren). CloudTrail protokolliert diese Aktionen als [AWS Dienstereignisse](#) und übermittelt diese Ereignisse an den Ereignisverlauf sowie an alle aktiven Protokolle und Ereignisdatenspeicher, die für Verwaltungsereignisse konfiguriert sind. Für diese Ereignisse lautet das eventType-Feld `AwsServiceEvent`.

Im Folgenden finden Sie ein Beispiel für einen Protokolleintrag für ein AWS Dienstereignis zur Erstellung eines mit einem Dienst verknüpften Kanals.

```
{
  "eventVersion": "1.08",
  "userIdentity": {
    "accountId": "111122223333",
    "invokedBy": "AWS Internal"
  },
  "eventTime": "2022-08-18T17:11:22Z",
  "eventSource": "cloudtrail.amazonaws.com",
  "eventName": "CreateServiceLinkedChannel",
  "awsRegion": "us-east-1",
  "sourceIPAddress": "AWS Internal",
  "userAgent": "AWS Internal",
  "requestParameters": null,
  "responseElements": null,
  "requestID": "564f004c-EXAMPLE",
  "eventID": "234f004b-EXAMPLE",
  "readOnly": false,
  "resources": [
    {
      "accountId": "184434908391",
      "type": "AWS::CloudTrail::Channel",
      "ARN": "arn:aws:cloudtrail:us-east-1:111122223333:channel/7944f0ec-EXAMPLE"
    }
  ],
  "eventType": "AwsServiceEvent",
  "managementEvent": true,
  "recipientAccountId": "111122223333",
  "eventCategory": "Management"
}
```

# CloudTrail Ereignisse verstehen

Ein Ereignis in CloudTrail ist die Aufzeichnung einer Aktivität in einem AWS Konto. Bei dieser Aktivität kann es sich um eine Aktion handeln, die von einer IAM-Identität oder einem Dienst ausgeführt wird, der von überwacht werden kann. CloudTrail CloudTrail Ereignisse bieten einen Verlauf der API- und Nicht-API-Kontoaktivitäten, die mithilfe von AWS SDKs AWS Management Console, Befehlszeilentools und anderen Programmen durchgeführt wurden. AWS-Services

CloudTrail Protokolldateien sind kein geordneter Stack-Trace der öffentlichen API-Aufrufe, sodass Ereignisse nicht in einer bestimmten Reihenfolge angezeigt werden.

Es gibt drei Arten von CloudTrail Ereignissen:

- [Verwaltungsereignisse](#)
- [Datenereignisse](#)
- [Insights-Ereignisse](#)

Standardmäßig protokollieren Trails und Ereignisdatenspeicher Verwaltungsereignisse, aber keine Daten- oder Insights-Ereignisse.

Alle Ereignistypen verwenden ein CloudTrail JSON-Protokollformat. Das Protokoll enthält Informationen zu Anforderungen von Ressourcen in Ihrem Konto, z. B. wer die Anforderung gestellt hat, welche Services verwendet, welche Aktionen ausgeführt und welche Parameter für die Aktion eingesetzt wurden. Die Ereignisdaten sind in einem Records-Array enthalten.

Hinweise zu Feldern für CloudTrail Ereignisdatensätze finden Sie unter [CloudTrail Inhalt aufzeichnen](#).

## Verwaltungsereignisse

Verwaltungsereignisse enthalten Informationen über Verwaltungsvorgänge, die mit Ressourcen in Ihrem AWS Konto ausgeführt werden. Sie werden auch als Vorgänge auf Steuerebene bezeichnet. Beispiele für Verwaltungsereignisse:

- Konfiguration der Sicherheit (z. B. AWS Identity and Access Management AttachRolePolicy API-Operationen).
- Registrieren von Geräten (z. B. CreateDefaultVpc-API-Operationen von Amazon EC2).

- Konfigurieren von Regeln für die Datenweiterleitung (z. B. CreateSubnet-API-Operationen von Amazon EC2).
- Einrichtung der Protokollierung (z. B. AWS CloudTrail CreateTrail API-Operationen).

Verwaltungsereignisse können auch andere als API-Ereignisse einschließen, die in Ihrem Konto auftreten. Wenn sich beispielsweise ein Benutzer bei Ihrem Konto CloudTrail anmeldet, wird das ConsoleLogin Ereignis protokolliert. Weitere Informationen finden Sie unter [Nicht-API-Ereignisse, erfasst von CloudTrail](#). Eine Liste der Verwaltungsereignisse, die für AWS Dienste CloudTrail protokolliert werden, finden Sie unter [CloudTrail unterstützte Dienste und Integrationen](#).

Das folgende Beispiel zeigt einen einzelnen Protokolldatensatz eines Verwaltungsereignisses. In diesem Fall Mary\_Major führte ein IAM-Benutzer mit dem Namen den aws cloudtrail start-logging Befehl aus, um die CloudTrail [StartLogging](#)Aktion zum Starten des Protokollierungsprozesses in einem Pfad mit dem Namen myTrail aufzurufen.

```
{
  "eventVersion": "1.09",
  "userIdentity": {
    "type": "IAMUser",
    "principalId": "EXAMPLE6E4XEGITWATV6R",
    "arn": "arn:aws:iam::123456789012:user/Mary_Major",
    "accountId": "123456789012",
    "accessKeyId": "AKIAIOSFODNN7EXAMPLE",
    "userName": "Mary_Major",
    "sessionContext": {
      "attributes": {
        "creationDate": "2023-07-19T21:11:57Z",
        "mfaAuthenticated": "false"
      }
    }
  },
  "eventTime": "2023-07-19T21:33:41Z",
  "eventSource": "cloudtrail.amazonaws.com",
  "eventName": "StartLogging",
  "awsRegion": "us-east-1",
  "sourceIPAddress": "192.0.2.0",
  "userAgent": "aws-cli/2.13.5 Python/3.11.4 Linux/4.14.255-314-253.539.amzn2.x86_64
exec-env/CloudShell exe/x86_64.amzn.2 prompt/off command/cloudtrail.start-logging",
  "requestParameters": {
    "name": "myTrail"
  },
}
```

```
"responseElements": null,
"requestID": "9d478fc1-4f10-490f-a26b-EXAMPLE0e932",
"eventID": "eae87c48-d421-4626-94f5-EXAMPLEEac994",
"readOnly": false,
"eventType": "AwsApiCall",
"managementEvent": true,
"recipientAccountId": "123456789012",
"eventCategory": "Management",
"tlsDetails": {
  "tlsVersion": "TLSv1.2",
  "cipherSuite": "ECDHE-RSA-AES128-GCM-SHA256",
  "clientProvidedHostHeader": "cloudtrail.us-east-1.amazonaws.com"
},
"sessionCredentialFromConsole": "true"
}
```

Im nächsten Beispiel hat ein IAM-Benutzer mit dem Namen Paulo\_Santos den Befehl `aws cloudtrail start-event-data-store-ingestion` ausgeführt, um die Aktion [StartEventDataStoreIngestion](#) aufzurufen und die Aufnahme in einen Ereignisdatenspeicher zu starten.

```
{
  "eventVersion": "1.09",
  "userIdentity": {
    "type": "IAMUser",
    "principalId": "EXAMPLEPHCNW5EQV7NA54",
    "arn": "arn:aws:iam::123456789012:user/Paulo_Santos",
    "accountId": "123456789012",
    "accessKeyId": "(AKIAIOSFODNN7EXAMPLE",
    "userName": "Paulo_Santos",
    "sessionContext": {
      "attributes": {
        "creationDate": "2023-07-21T21:55:30Z",
        "mfaAuthenticated": "false"
      }
    }
  },
  "eventTime": "2023-07-21T21:57:28Z",
  "eventSource": "cloudtrail.amazonaws.com",
  "eventName": "StartEventDataStoreIngestion",
  "awsRegion": "us-east-1",
  "sourceIPAddress": "192.0.2.0",
}
```

```
"userAgent": "aws-cli/2.13.1 Python/3.11.4 Linux/4.14.255-314-253.539.amzn2.x86_64
exec-env/CloudShell exe/x86_64.amzn.2 prompt/off command/cloudtrail.start-event-data-
store-ingestion",
  "requestParameters": {
    "eventDataStore": "arn:aws:cloudtrail:us-
east-1:123456789012:eventdatastore/2a8f2138-0caa-46c8-a194-EXAMPLE87d41"
  },
  "responseElements": null,
  "requestID": "f62a3494-ba4e-49ee-8e27-EXAMPLE4253f",
  "eventID": "d97ca7e2-04fe-45b4-882d-EXAMPLEa9b2c",
  "readOnly": false,
  "eventType": "AwsApiCall",
  "managementEvent": true,
  "recipientAccountId": "123456789012",
  "eventCategory": "Management",
  "tlsDetails": {
    "tlsVersion": "TLSv1.2",
    "cipherSuite": "ECDHE-RSA-AES128-GCM-SHA256",
    "clientProvidedHostHeader": "cloudtrail.us-east-1.amazonaws.com"
  },
  "sessionCredentialFromConsole": "true"
}
```

## Datenergebnisse

Datenergebnisse liefern Informationen zu Ressourcenoperationen, die für oder innerhalb einer Ressource ausgeführt wurden. Sie werden auch als Vorgänge auf Datenebene bezeichnet. Datenergebnisse sind oft Aktivitäten mit hohem Volume.

Beispiele für Datenergebnisse:

- [Amazon S3 S3-API-Aktivität auf Objektebene](#) (z. B., `GetObjectDeleteObject`, und `PutObject` API-Operationen) für Objekte in S3-Buckets.
- AWS Lambda Aktivität zur Ausführung von Funktionen (die `Invoke` API).
- CloudTrail [PutAuditEvents](#) Aktivität auf einem [CloudTrail Lake-Kanal](#), der verwendet wird, um Ereignisse von außen zu protokollieren AWS.
- [Publish](#)- und [PublishBatch](#)-API-Operationen von Amazon SNS zu Themen.


In der folgenden Tabelle sind die Datenergebnistypen aufgeführt, die für Trails und Ereignisdatenspeicher verfügbar sind. In der Spalte Datenergebnistyp (Konsole) wird die

entsprechende Auswahl in der Konsole angezeigt. In der Wertspalte `resources.type` wird der `resources.type` Wert angezeigt, den Sie angeben würden, um Datenereignisse dieses Typs mithilfe der APIs oder in Ihren Trail- oder Event-Datenspeicher aufzunehmen. AWS CLI CloudTrail

Für Trails können Sie einfache oder erweiterte Event-Selektoren verwenden, um Datenereignisse für Amazon S3 S3-Objekte, Lambda-Funktionen und DynamoDB-Tabellen zu protokollieren (in den ersten drei Zeilen der Tabelle dargestellt). Sie können nur erweiterte Ereignisselektoren verwenden, um die in den verbleibenden Zeilen angezeigten Datenereignistypen zu protokollieren.

Für Ereignisdatenspeicher können Sie nur erweiterte Ereignisselektoren verwenden, um Datenereignisse einzubeziehen.

AWS-Service	Beschreibung	Typ des Datenereignisses (Konsole)	<code>resources.type</code> -Wert
Amazon-DynamoDB	<a href="#">Amazon DynamoDB DynamoDB-API-Aktivität auf Artikelebene</a> für Tabellen (z. B., <code>PutItemDeleteItem</code> , und <code>UpdateItem</code> API-Operationen).	DynamoDB	<code>AWS::DynamoDB::Table</code>

 **Note**

Bei Tabellen mit aktivierten Streams enthält das `resources`-Feld im Datenereignis sowohl `AWS::DynamoDB::Stream` als auch




AWS-Service	Beschreibung	Typ des Dateneignisses (Konsole)	resources.type-Wert
	<p>AWS::DynamoDB::Table .</p> <p>Wenn Sie AWS::DynamoDB::Table als resources.type angeben, werden standardmäßig sowohl DynamoDB-Tabellen als auch DynamoDB-Stream-Ereignisse protokolliert. Um <a href="#">Streams-Ereignisse</a> auszuschließen, fügen Sie dem Feld einen Filter hinzu.</p> <p>eventName</p>		


AWS-Service	Beschreibung	Typ des Datenereignisses (Konsole)	resources.type-Wert
AWS Lambda	AWS Lambda Aktivität zur Funktionsausführung (die Invoke API).	Lambda	AWS::Lambda::Function
Amazon S3	<a href="#">Amazon S3 S3-API-Aktivität auf Objektebene</a> (z. B., GetObject , DeleteObject , und PutObject API-Operationen) für Objekte in S3-Buckets.	S3	AWS::S3::Object
AWS AppConfig	<a href="#">AWS AppConfig API-Aktivität</a> für Konfigurationsvorgänge wie Aufrufe von und. StartConfigurationSession GetLatestConfiguration	AWS AppConfig	AWS::AppConfig::Configuration


AWS-Service	Beschreibung	Typ des Dateneignisses (Konsole)	resources.type-Wert
AWS B2B-Datenaustausch	B2B-Datenaustausch-API-Aktivität für Transformer-Operationen wie Aufrufe von <code>GetTransformerJob</code> und <code>StartTransformerJob</code> .	B2B-Datenaustausch	<code>AWS::B2BI::Transformer</code>
Amazon Bedrock	<a href="#">Amazon-Bedrock-API-Aktivität</a> auf einem Agent-Alias.	Bedrock-Agent-Alias	<code>AWS::Bedrock::AgentAlias</code>
	<a href="#">Amazon-Bedrock-API-Aktivität</a> auf einer Wissensdatenbank.	Bedrock-Wissensdatenbank	<code>AWS::Bedrock::KnowledgeBase</code>
Amazon CloudFront	CloudFront API-Aktivität auf einem <a href="#">KeyValueStore</a> .	CloudFront KeyValueStore	<code>AWS::CloudFront::KeyValueStore</code>
AWS Cloud Map	<a href="#">AWS Cloud Map API-Aktivität</a> in einem <a href="#">Namespace</a> .	AWS Cloud Map Namespace	<code>AWS::ServiceDiscovery::Namespace</code>
	<a href="#">AWS Cloud Map API-Aktivität</a> für einen <a href="#">Dienst</a> .	AWS Cloud Map Service nicht zulässig	<code>AWS::ServiceDiscovery::Service</code>

AWS-Service	Beschreibung	Typ des Datenereignisses (Konsole)	resources.type-Wert
AWS CloudTrail	CloudTrail <a href="#">PutAuditEvents</a> Aktivität auf einem <a href="#">CloudTrail Lake-Kanal</a> , der verwendet wird, um Ereignisse von außen zu protokollieren AWS.	CloudTrail Kanal	AWS::CloudTrail::Channel
Amazon CodeWhisperer	CodeWhisperer Amazon-API-Aktivität bei einer Anpassung.	CodeWhisperer Anpassung	AWS::CodeWhisperer::Customization
	CodeWhisperer Amazon-API-Aktivität in einem Profil.	CodeWhisperer	AWS::CodeWhisperer::Profile
Amazon Cognito	API-Aktivität von Amazon Cognito in Amazon-Cognito- <a href="#">Identitätspools</a> .	Cognito-Identitätspools	AWS::Cognito::IdentityPool
Amazon-DynamoDB	API-Aktivitäten von <a href="#">Amazon DynamoDB</a> in Streams.	DynamoDB-Streams	AWS::DynamoDB::Stream

AWS-Service	Beschreibung	Typ des Dateneignisses (Konsole)	resources.type-Wert
Amazon Elastic Block Store	Direkte APIs von <a href="#">Amazon Elastic Block Store (EBS)</a> wie PutSnapshotBlock , GetSnapshotBlock und ListChangedBlocks in Amazon-EBS-Snapshots.	Amazon EBS Direct-APIs	AWS::EC2::Snapshot
Amazon EMR	API-Aktivität von Amazon EMR in einem Write-Ahead-Log-Workspace.	EMR-Write-Ahead-Log-Workspace	AWS::EMRWAAL::Workspace
Amazon FinSpace	API-Aktivitäten von <a href="#">Amazon FinSpace</a> in Umgebungen.	FinSpace	AWS::FinSpace::Environment

AWS-Service	Beschreibung	Typ des Dateneignisses (Konsole)	resources.type-Wert
AWS Glue	<p>AWS Glue API-Aktivität für Tabellen, die von Lake Formation erstellt wurden.</p> <div data-bbox="354 590 673 1785" style="border: 1px solid #add8e6; border-radius: 10px; padding: 10px;"><p> <b>Note</b></p><p>AWS Glue Dateneignisse für Tabellen werden derzeit nur in den folgenden Regionen unterstützt:</p><ul style="list-style-type: none"><li>• USA Ost (Nord-Virginia)</li><li>• USA Ost (Ohio)</li><li>• USA West (Oregon)</li><li>• Europa (Irland)</li><li>• Region Asien-Pazifik (Tokio)</li></ul></div>	Lake Formation	AWS::Glue::Table

AWS-Service	Beschreibung	Typ des Datenereignisses (Konsole)	resources.type-Wert
Amazon GuardDuty	GuardDuty Amazon-API-Aktivität für einen <a href="#">Detektor</a> .	GuardDuty Detektor	AWS::GuardDuty::Detector
AWS HealthImaging	AWS HealthImaging API-Aktivität in Datenspeichern.	Datenspeicher für medizinische Bildgebung	AWS::MedicalImaging::Datastore
AWS IoT	<a href="#">AWS IoT API-Aktivität</a> für <a href="#">Zertifikate</a> .	IoT-Zertifikat	AWS::IoT::Certificate
	<a href="#">AWS IoT API-Aktivität</a> für <a href="#">Dinge</a> .	IoT-Sache	AWS::IoT::Thing
AWS IoT Greengrass Version 2	<a href="#">Greengrass-API-Aktivität</a> von einem Greengrass-Core-Gerät auf einer Komponentenversion.  <div data-bbox="354 1297 672 1801" style="border: 1px solid #00a0e3; border-radius: 10px; padding: 10px; background-color: #e6f2ff;"> <p> <b>Note</b></p> <p>Greengrass protokolliert keine Ereignisse, bei denen der Zugriff verweigert wurde.</p> </div>	IoT Greengrass-Komponentenversion	AWS::GreengrassV2::ComponentVersion

AWS-Service	Beschreibung	Typ des Datenereignisses (Konsole)	resources.type-Wert
	<p><a href="#">Greengrass-API-Aktivität</a> von einem Greengrass-Core-Gerät in einer Bereitstellung.</p> <div style="border: 1px solid #0070C0; border-radius: 10px; padding: 10px; margin-top: 10px;"> <p> <b>Note</b></p> <p>Greengrass protokolliert keine Ereignisse, bei denen der Zugriff verweigert wurde.</p> </div>	Einsatz von IoT Greengrass	AWS::GreengrassV2::Deployment
AWS IoT SiteWise	<a href="#">SiteWise IoT-API-Aktivität</a> für <a href="#">Anlagen</a> .	SiteWise IoT-Anlage	AWS::IoTSiteWise::Asset
	<a href="#">SiteWise IoT-API-Aktivität</a> in <a href="#">Zeitreihen</a> .	SiteWise IoT-Zeitreihen	AWS::IoTSiteWise::TimeSeries
AWS IoT TwinMaker	TwinMaker IoT-API-Aktivität für eine <a href="#">Entität</a> .	TwinMaker IoT-Entität	AWS::IoTTwinMaker::Entity
	TwinMaker IoT-API-Aktivität in einem <a href="#">Workspace</a> .	TwinMaker IoT-Arbeitsplatz	AWS::IoTTwinMaker::Workspace



AWS-Service	Beschreibung	Typ des Datenereignisses (Konsole)	resources.type-Wert
Amazon Kendra Intelligent Ranking	API-Aktivität von Amazon Kendra Intelligent Rankin für <a href="#">Rescore-Ausführung spläne</a> .	Kendra-Rangliste	AWS::KendraRanking::ExecutionPlan
Amazon Keyspaces (für Apache Cassandra)	<a href="#">Amazon Keyspaces-API-Aktivität</a> in einer Tabelle.	Cassandra-Tabelle	AWS::Cassandra::Table
Amazon-Kinesis-Data-Streams	Kinesis Data Streams API-Aktivität in <a href="#">Streams</a> .	Kinesis-Stream	AWS::Kinesis::Stream
	Kinesis Data Streams API-Aktivität auf <a href="#">Stream-Verbrauchern</a> .	Kinesis Stream-Verbraucher	AWS::Kinesis::StreamConsumer
Amazon Kinesis Video Streams	Kinesis Video Streams Streams-API-Aktivitäten in Videostreams, z. B. Aufrufe von GetMedia undPutMedia.	Kinesis-Videostream	AWS::KinesisVideo::Stream
Amazon Managed Blockchain	API-Aktivität von Amazon Managed Blockchain in einem Netzwerk.	Managed-Blockchain-Netzwerk	AWS::ManagedBlockchain::Network

AWS-Service	Beschreibung	Typ des Datenereignisses (Konsole)	resources.type-Wert
	JSON-RPC-Aufrufe von <a href="#">Amazon Managed Blockchain</a> in Ethereum-Knoten, zum Beispiel <code>eth_getBalance</code> oder <code>eth_getBlockByNumber</code> .	Managed Blockchain	<code>AWS::ManagedBlockchain::Node</code>
Amazon-Neptune-Graph	Daten-API-Aktivitäten in einem Neptune-Graph, zum Beispiel Abfragen, Algorithmen oder Vektorsuche.	Neptun-Graph	<code>AWS::NeptuneGraph::Graph</code>
AWS Private CA	AWS Private CA Konnektor für Active Directory-API-Aktivitäten.	AWS Private CA Konnektor für Active Directory	<code>AWS::PCAConnectorAD::Connector</code>
Amazon Q Apps	Daten-API-Aktivität auf <a href="#">Amazon Q Apps</a> .	Amazon Q Apps	<code>AWS::QApps:QApp</code>
Amazon Q Business	<a href="#">Amazon-Q-Business-API-Aktivität</a> auf einer Anwendung.	Amazon-Q-Business-Anwendung	<code>AWS::QBusiness::Application</code>
	<a href="#">Amazon-Q-Business-API-Aktivität</a> auf einer Datenquelle.	Amazon-Q-Business-Datenquelle	<code>AWS::QBusiness::DataSource</code>

AWS-Service	Beschreibung	Typ des Dateneignisses (Konsole)	resources.type-Wert
	<a href="#">Amazon-Q-Business-API-Aktivität</a> auf einem Index.	Amazon-Q-Business-Index	AWS::QBusiness::Index
	<a href="#">Amazon-Q-Business-API-Aktivität</a> auf einem Weberlebnis.	Amazon-Q-Business-Weberlebnis	AWS::QBusiness::WebExperience
Amazon RDS	<a href="#">Amazon RDS-API-Aktivität</a> in einem DB-Cluster.	RDS-Daten-API — DB-Cluster	AWS::RDS::DBCluster
Amazon S3	<a href="#">Amazon S3 S3-API-Aktivität</a> auf Access Points.	S3-Zugangspunkt	AWS::S3::AccessPoint
	<a href="#">API-Aktivitäten für Amazon S3 Object Lambda Access Points</a> , z. B. Aufrufe von CompleteMultipartUpload undGetObject .	S3 Objekt Lambda	AWS::S3ObjectLambda::AccessPoint
Amazon S3 in Outposts	API-Aktivität auf Objektebene auf <a href="#">Amazon S3 on Outposts</a> .	S3-Outposts	AWS::S3Outposts::Object

AWS-Service	Beschreibung	Typ des Datenereignisses (Konsole)	resources.type-Wert
Amazon SageMaker	SageMaker <a href="#">InvokeEndpointWithResponseStream</a> Amazon-Aktivitäten auf Endpunkten.	SageMaker Endpunkt	AWS::SageMaker::Endpoint
	SageMaker Amazon-API-Aktivität in Feature-Stores.	SageMaker feature store	AWS::SageMaker::FeatureGroup
	SageMaker Amazon-API-Aktivität für <a href="#">Versuchskomponente</a> .	SageMaker Metriken, Experiment, Versuchskomponente	AWS::SageMaker::ExperimentTrialComponent
Amazon SNS	<a href="#">Publish</a> -API-Operationen von Amazon SNS auf Plattformendpunkten.	SNS-Plattformendpunkt	AWS::SNS::PlatformEndpoint
	<a href="#">Publish</a> - und <a href="#">PublishBatch</a> - API-Operationen von Amazon SNS zu Themen.	SNS-Thema	AWS::SNS::Topic
Amazon SQS	<a href="#">Amazon-SQS-API-Aktivität</a> auf Nachrichten.	SQS	AWS::SQS::Queue

AWS-Service	Beschreibung	Typ des Datenereignisses (Konsole)	resources.type-Wert
AWS Step Functions	<a href="#">API-Aktivität von Step Functions</a> auf einer Zustandsmaschine.	Step-Functions-Zustandsautomat	AWS::StepFunctions::StateMachine
AWS Supply Chain	AWS Supply Chain API-Aktivität auf einer Instanz.	Lieferkette	AWS::SCN::Instance
Amazon SWF	<a href="#">Amazon SWF SWF-API-Aktivität</a> auf <a href="#">Domains</a> .	SWF-Domäne	AWS::SWF::Domain
AWS Systems Manager	<a href="#">Systems Manager Manager-API-Aktivität</a> auf Kontrollkanälen.	Systems Manager	AWS::SSMMessages::ControlChannel
	<a href="#">Systems Manager Manager-API-Aktivität</a> auf verwalteten Knoten.	Von Systems Manager verwalteter Knoten	AWS::SSM::ManagedNode
Amazon Timestream	<a href="#">Query</a> -API-Aktivität von Amazon Timestream in Datenbanken.	Timestream-Datenbank	AWS::Timestream::Database
	<a href="#">Query</a> -API-Aktivität von Amazon Timestream in Tabellen.	Timestream-Tabelle	AWS::Timestream::Table

AWS-Service	Beschreibung	Typ des Datenereignisses (Konsole)	resources.type-Wert
Amazon Verified Permissions	API-Aktivität von Amazon Verified Permissions in einem Richtlinienpeicher.	Amazon Verified Permissions	AWS::VerifiedPermissions::PolicyStore
Amazon WorkSpaces Thin Client	WorkSpaces Thin Client-API-Aktivität auf einem Gerät.	Thin-Client-Gerät	AWS::ThinClient::Device
	WorkSpaces Thin Client-API-Aktivität in einer Umgebung.	Thin-Client-Umgebung	AWS::ThinClient::Environment
AWS X-Ray	<a href="#">X-Ray-API-Aktivität auf Spuren</a> .	Röntgenspur	AWS::XRay::Trace

Datenereignisse werden standardmäßig nicht protokolliert, wenn Sie einen Trail oder einen Ereignisdatenspeicher erstellen. Um CloudTrail Datenereignisse aufzuzeichnen, müssen Sie explizit die unterstützten Ressourcen oder Ressourcentypen hinzufügen, für die Sie Aktivitäten erfassen möchten. Weitere Informationen finden Sie unter [Erstellen eines Trails](#) und [Erstellen Sie mit der Konsole einen Ereignisdatenspeicher für CloudTrail Ereignisse](#).

Für die Protokollierung von Datenereignissen fallen zusätzliche Gebühren an. CloudTrail Preise finden Sie unter [AWS CloudTrail Preisgestaltung](#).

Das folgende Beispiel zeigt einen einzelnen Protokolleintrag eines Datenereignisses für die Amazon SNS Publish SNS-Aktion.

```
{
  "eventVersion": "1.09",
  "userIdentity": {
    "type": "AssumedRole",
    "principalId": "EX_PRINCIPAL_ID",
    "arn": "arn:aws:iam::123456789012:user/Bob",
```

```
    "accountId": "123456789012",
    "accessKeyId": "AKIAIOSFODNN7EXAMPLE",
    "sessionContext": {
      "sessionIssuer": {
        "type": "Role",
        "principalId": "AKIAIOSFODNN7EXAMPLE",
        "arn": "arn:aws:iam::123456789012:role/Admin",
        "accountId": "123456789012",
        "userName": "ExampleUser"
      },
      "attributes": {
        "creationDate": "2023-08-21T16:44:05Z",
        "mfaAuthenticated": "false"
      }
    }
  },
  "eventTime": "2023-08-21T16:48:37Z",
  "eventSource": "sns.amazonaws.com",
  "eventName": "Publish",
  "awsRegion": "us-east-1",
  "sourceIPAddress": "192.0.2.0",
  "userAgent": "aws-cli/1.29.16 md/Botocore#1.31.16 ua/2.0 os/
linux#5.4.250-173.369.amzn2int.x86_64 md/arch#x86_64 lang/python#3.8.17 md/
pyimpl#CPython cfg/retry-mode#legacy botocore/1.31.16",
  "requestParameters": {
    "topicArn": "arn:aws:sns:us-east-1:123456789012:ExampleSNSTopic",
    "message": "HIDDEN_DUE_TO_SECURITY_REASONS",
    "subject": "HIDDEN_DUE_TO_SECURITY_REASONS",
    "messageStructure": "json",
    "messageAttributes": "HIDDEN_DUE_TO_SECURITY_REASONS"
  },
  "responseElements": {
    "messageId": "0787cd1e-d92b-521c-a8b4-90434e8ef840"
  },
  "requestID": "0a8ab208-11bf-5e01-bd2d-ef55861b545d",
  "eventID": "bb3496d4-5252-4660-9c28-3c6aebdb21c0",
  "readOnly": false,
  "resources": [{
    "accountId": "123456789012",
    "type": "AWS::SNS::Topic",
    "ARN": "arn:aws:sns:us-east-1:123456789012:ExampleSNSTopic"
  }],
  "eventType": "AwsApiCall",
  "managementEvent": false,
```

```

"recipientAccountId": "123456789012",
"eventCategory": "Data",
"tlsDetails": {
  "tlsVersion": "TLSv1.2",
  "cipherSuite": "ECDHE-RSA-AES128-GCM-SHA256",
  "clientProvidedHostHeader": "sns.us-east-1.amazonaws.com"
}
}

```

Das nächste Beispiel zeigt einen einzelnen Protokolleintrag eines Datenereignisses für die Amazon Cognito GetCredentialsForIdentity Cognito-Aktion.

```

{
  "eventVersion": "1.08",
  "userIdentity": {
    "type": "Unknown"
  },
  "eventTime": "2023-01-19T16:55:08Z",
  "eventSource": "cognito-identity.amazonaws.com",
  "eventName": "GetCredentialsForIdentity",
  "awsRegion": "us-east-1",
  "sourceIPAddress": "192.0.2.4",
  "userAgent": "aws-cli/2.7.25 Python/3.9.11 Darwin/21.6.0 exe/x86_64 prompt/off
command/cognito-identity.get-credentials-for-identity",
  "requestParameters": {
    "logins": {
      "cognito-idp.us-east-1.amazonaws.com/us-east-1_aaaaaaaaa":
"HIDDEN_DUE_TO_SECURITY_REASONS"
    },
    "identityId": "us-east-1:1cf667a2-49a6-454b-9e45-23199EXAMPLE"
  },
  "responseElements": {
    "credentials": {
      "accessKeyId": "ASIAIOSFODNN7EXAMPLE",
      "sessionToken": "aAaAaAaAaAaAab1111111111111111EXAMPLE",
      "expiration": "Jan 19, 2023 5:55:08 PM"
    },
    "identityId": "us-east-1:1cf667a2-49a6-454b-9e45-23199EXAMPLE"
  },
  "requestID": "659dfc23-7c4e-4e7c-858a-1abce884d645",
  "eventID": "6ad1c766-5a41-4b28-b5ca-e223ccb00f0d",
  "readOnly": false,
  "resources": [{

```



```
    "accountId": "111122223333",
    "type": "AWS::Cognito::IdentityPool",
    "ARN": "arn:aws:cognito-identity:us-east-1:111122223333:identitypool/us-
east-1:2dg778b3-50b7-565c-0f56-34200EXAMPLE"
  }],
  "eventType": "AwsApiCall",
  "managementEvent": false,
  "recipientAccountId": "111122223333",
  "eventCategory": "Data"
}
```

## Einblicke und Ereignisse

CloudTrail Insights-Ereignisse erfassen ungewöhnliche API-Aufruf- oder Fehlerquoten in Ihrem AWS Konto, indem sie die CloudTrail Verwaltungsaktivitäten analysieren. Insights-Ereignisse stellen relevante Informationen bereit, z. B. die zugehörige API, den Fehlercode, die Vorfalzeit und Statistiken, die Ihnen helfen, ungewöhnliche Aktivitäten zu verstehen und darauf zu reagieren. Im Gegensatz zu anderen Arten von Ereignissen, die in einem CloudTrail Trail- oder Event-Datenspeicher erfasst werden, werden Insights-Ereignisse nur protokolliert, wenn Änderungen in der API-Nutzung Ihres Kontos oder bei der Protokollierung der Fehlerquote CloudTrail festgestellt werden, die sich erheblich von den typischen Nutzungsmustern des Kontos unterscheiden.

Beispiele für Aktivitäten, bei denen ggf. Insights-Ereignisse generiert werden, sind:

- Für Ihr Konto werden pro Minute normalerweise nicht mehr als 20 `deleteBucket`-API-Aufrufe vom Typ Amazon S3 protokolliert, aber unter Ihrem Konto werden nun durchschnittlich 100 `deleteBucket`-API-Aufrufe pro Minute protokolliert. Ein Insights-Ereignis wird zu Beginn der ungewöhnlichen Aktivitäten protokolliert und ein anderes Insights-Ereignis wird protokolliert, um das Ende der ungewöhnlichen Aktivitäten zu markieren.
- Für Ihr Konto werden pro Minute normalerweise 20 Aufrufe der Amazon-`EC2-AuthorizeSecurityGroupIngress`-API protokolliert, aber unter Ihrem Konto werden nun keine Aufrufe von `AuthorizeSecurityGroupIngress` mehr protokolliert. Ein Insights-Ereignis wird zu Beginn der ungewöhnlichen Aktivitäten protokolliert und zehn Minuten später, nachdem die ungewöhnlichen Aktivitäten nicht mehr auftreten, wird ein anderes Insights-Ereignis protokolliert, um das Ende der ungewöhnlichen Aktivitäten zu markieren.
- Ihr Konto protokolliert normalerweise weniger als einen `AccessDeniedException`-Fehler in einem Zeitraum von sieben Tagen in der AWS Identity and Access Management -API, `DeleteInstanceProfile`. Ihr Konto beginnt mit der Protokollierung von durchschnittlich 12

AccessDeniedException-Fehlern pro Minute für den DeleteInstanceProfile-API-Aufruf. Ein Insights-Ereignis wird zu Beginn der ungewöhnlichen Fehlerraten-Aktivitäten protokolliert und ein anderes Insights-Ereignis wird protokolliert, um das Ende der ungewöhnlichen Aktivitäten zu markieren.

Diese Beispiele dienen nur zur Veranschaulichung. Ihre Ergebnisse können je nach Anwendungsfall abweichen.

Um CloudTrail Insights-Ereignisse zu protokollieren, müssen Sie Insights-Ereignisse in einem neuen oder vorhandenen Trail- oder Event-Datenspeicher explizit aktivieren. Weitere Informationen zum Erstellen eines Trails finden Sie unter [Erstellen eines Trails](#). Weitere Informationen zum Erstellen eines Ereignisdatenspeichers finden Sie unter [Erstellen Sie mit der Konsole einen Ereignisdatenspeicher für CloudTrail Insights-Ereignisse](#).

Für Insights-Ereignisse fallen zusätzliche Gebühren an. Wenn Sie Insights sowohl für Trails als auch für Ereignisdatenspeicher aktivieren, wird Ihnen eine separate Gebühr in Rechnung gestellt. Weitere Informationen finden Sie unter [AWS CloudTrail -Preisgestaltung](#).

In CloudTrail Insights werden zwei Ereignisse protokolliert, die auf ungewöhnliche Aktivitäten hinweisen: ein Startereignis und ein Endereignis. Im folgenden Beispiel wird ein einzelner Protokolldatensatz mit einem Insights-Ereignis veranschaulicht, das aufgetreten ist, als CompleteLifecycleAction für die Application-Auto-Scaling-API ungewöhnlich häufig aufgerufen wurde. Bei Insights-Ereignissen hat eventCategory den Wert Insight. Mit einem insightDetails-Block werden Ereignisstatus, Quelle, Name, Insights-Typ und Kontext, einschließlich Statistiken und Attributionen, identifiziert. Weitere Informationen zum insightDetails-Block finden Sie unter [CloudTrail insightDetailsElement „Einblicke“](#).

```
{
  "eventVersion": "1.08",
  "eventTime": "2023-07-10T01:42:00Z",
  "awsRegion": "us-east-1",
  "eventID": "55ed45c5-0b0c-4228-9fe5-EXAMPLEc3f4d",
  "eventType": "AwsCloudTrailInsight",
  "recipientAccountId": "123456789012",
  "sharedEventID": "979c82fe-14d4-4e4c-aa01-EXAMPLE3acee",
  "insightDetails": {
    "state": "Start",
    "eventSource": "autoscaling.amazonaws.com",
    "eventName": "CompleteLifecycleAction",
    "insightType": "ApiCallRateInsight",
```

```

    "insightContext": {
      "statistics": {
        "baseline": {
          "average": 9.82222E-5
        },
        "insight": {
          "average": 5.0
        },
        "insightDuration": 1,
        "baselineDuration": 10181
      },
      "attributions": [{
        "attribute": "userIdentityArn",
        "insight": [{
          "value": "arn:aws:sts::123456789012:assumed-role/
CodeDeployRole1",
          "average": 5.0
        }, {
          "value": "arn:aws:sts::123456789012:assumed-role/
CodeDeployRole2",
          "average": 5.0
        }, {
          "value": "arn:aws:sts::123456789012:assumed-role/
CodeDeployRole3",
          "average": 5.0
        }
      ]],
      "baseline": [{
        "value": "arn:aws:sts::123456789012:assumed-role/
CodeDeployRole1",
        "average": 9.82222E-5
      }
    ], {
      "attribute": "userAgent",
      "insight": [{
        "value": "codedeploy.amazonaws.com",
        "average": 5.0
      }
    ]],
      "baseline": [{
        "value": "codedeploy.amazonaws.com",
        "average": 9.82222E-5
      }
    ]
  }, {
    "attribute": "errorCode",
    "insight": [{

```

```
        "value": "null",
        "average": 5.0
      }],
      "baseline": [{
        "value": "null",
        "average": 9.82222E-5
      }]
    }
  },
  "eventCategory": "Insight"
}
```

## Protokollieren von Verwaltungsereignissen

Standardmäßig protokollieren Trails und Ereignisdatenspeicher Verwaltungsereignisse und enthalten keine Datenereignisse oder Insights-Ereignisse.

Für Daten- bzw. Insights-Ereignisse fallen zusätzliche Gebühren an. Weitere Informationen finden Sie unter [AWS CloudTrail -Preisgestaltung](#).

### Inhalt

- [Verwaltungsereignisse](#)
  - [Protokollieren von Verwaltungsereignissen mit AWS Management Console](#)
- [Lesen und Schreiben von Ereignissen](#)
- [Protokollieren von Ereignissen mit der AWS Command Line Interface](#)
  - [Beispiel: Protokollieren von Verwaltungsereignissen für Trails](#)
    - [Beispiele: Protokollierung von Verwaltungsereignissen für Trails mithilfe erweiterter Event-Selektoren](#)
    - [Beispiele: Protokollierung von Verwaltungsereignissen für Trails mithilfe einfacher Event-Selektoren](#)
  - [Beispiele: Protokollieren von Verwaltungsereignissen für Ereignisdatenspeicher](#)
- [Protokollieren von Ereignissen mit AWS -SDKs](#)
- [Ereignisse an Amazon CloudWatch Logs senden](#)

## Verwaltungsereignisse

Verwaltungsereignisse bieten Einblick in Verwaltungsvorgänge, die mit Ressourcen in Ihrem AWS Konto ausgeführt werden. Sie werden auch als Vorgänge auf Steuerebene bezeichnet. Beispiele für Verwaltungsereignisse:

- Konfigurieren von Sicherheit (z. B. AttachRolePolicy-API-Operationen von IAM)
- Registrieren von Geräten (z. B. CreateDefaultVpc-API-Operationen von Amazon EC2)
- Konfigurieren von Regeln für die Datenweiterleitung (z. B. CreateSubnet-API-Operationen von Amazon EC2)
- Einrichtung der Protokollierung (z. B. AWS CloudTrail CreateTrail API-Operationen)

Verwaltungsereignisse können auch andere als API-Ereignisse einschließen, die in Ihrem Konto auftreten. Wenn sich beispielsweise ein Benutzer bei Ihrem Konto anmeldet, wird das ConsoleLogin Ereignis CloudTrail protokolliert. Weitere Informationen finden Sie unter [Nicht-API-Ereignisse, erfasst von CloudTrail](#).

Standardmäßig sind Trails und Ereignisdatenspeicher so konfiguriert, dass sie Verwaltungsereignisse protokollieren.

### Note

Die Funktion „CloudTrail Ereignisverlauf“ unterstützt nur Verwaltungsereignisse. Sie können keine Amazon RDS Data API-Ereignisse aus dem Event-Verlauf ausschließen AWS KMS . Einstellungen, die Sie auf einen Trail- oder Event-Datenspeicher anwenden, gelten nicht für den Event-Verlauf. Weitere Informationen finden Sie unter [Mit dem CloudTrail Eventverlauf arbeiten](#).

## Protokollieren von Verwaltungsereignissen mit AWS Management Console

1. Melden Sie sich bei der an AWS Management Console und öffnen Sie die CloudTrail Konsole unter <https://console.aws.amazon.com/cloudtrail/>.
2. Um einen Trail zu aktualisieren, öffne die Trail-Seite der CloudTrail Konsole und wähle den Namen des Trails aus.

Um einen Ereignisdatenspeicher zu aktualisieren, öffnen Sie in der CloudTrail Konsole die Seite mit den Ereignisdatenspeichern und wählen Sie den Namen des Ereignisdatenspeichers aus.

3. Wählen Sie für Management-Ereignisse Bearbeiten aus.

- Wählen Sie aus, ob Ihr Trail oder Ereignisdatenspeicher Leseereignisse, Schreibereignisse oder beides protokollieren soll.
- Wählen Sie **AWS KMS Ereignisse ausschließen**, um Ereignisse aus Ihrem Trail- oder Event-Datenspeicher herauszufiltern **AWS Key Management Service (AWS KMS)**. Die Standardeinstellung ist, alle AWS KMS Ereignisse einzubeziehen.

Die Option zum Protokollieren oder Ausschließen von AWS KMS Ereignissen ist nur verfügbar, wenn Sie Verwaltungsereignisse in Ihrem Trail- oder Ereignisdatenspeicher protokollieren. Wenn Sie sich dafür entscheiden, Verwaltungsereignisse nicht zu protokollieren, werden AWS KMS Ereignisse nicht protokolliert, und Sie können die Einstellungen für die AWS KMS Ereignisprotokollierung nicht ändern.

AWS KMS Aktionen wie **EncryptDecrypt**, und erzeugen **GenerateDataKey** in der Regel ein großes Volumen (mehr als 99%) von Ereignissen. Diese Aktionen werden nun als Leseereignisse protokolliert. Relevante AWS KMS Aktionen mit geringem Volumen wie **DisableDelete**, und **ScheduleKey** (die in der Regel weniger als 0,5% des AWS KMS Ereignisvolumens ausmachen) werden als Write-Ereignisse protokolliert.

Wenn Sie Ereignisse mit hohem Volumen wie **Encrypt**, und ausschließen möchten **DecryptGenerateDataKey**, aber dennoch relevante Ereignisse wie, **Delete** und protokollieren möchten **DisableScheduleKey**, wählen Sie die Option **Schreibverwaltungsereignisse protokollieren** und deaktivieren Sie das Kontrollkästchen für Ereignisse ausschließen. **AWS KMS**

- Klicken Sie auf **Amazon-RDS-Daten-API-Ereignisse ausschließen** zum Filtern von Daten-API-Ereignissen von Amazon Relational Database Service aus Ihrem Trail oder Ereignisdatenspeicher. Die Standardeinstellung besteht darin, alle Amazon-RDS-Daten-API-Ereignisse einzubeziehen. Weitere Informationen über die Amazon-RDS-Daten-API finden Sie unter [Protokollieren von Daten-API-Aufrufen mit AWS CloudTrail](#) im Amazon-RDS-Benutzerhandbuch für Aurora.

4. Klicken Sie auf **Änderungen speichern**, wenn Sie fertig sind.

## Lesen und Schreiben von Ereignissen

Wenn Sie Ihren Trail oder Ereignisdatenspeicher für das Protokollieren von Verwaltungsereignissen konfigurieren, können Sie festlegen, ob Nur-Lesen-Ereignisse, Nur-Schreiben-Ereignisse oder beides protokolliert werden sollen.

- Read (Lesen)

Schreibgeschützte Ereignisse umfassen API-Operationen, die Ihre Ressourcen lesen, aber keine Änderungen vornehmen. Schreibgeschützte Ereignisse enthalten beispielsweise die API-Operationen Amazon EC2 `DescribeSecurityGroups` und `DescribeSubnets`. Diese Operationen geben nur Informationen über die Amazon-EC2-Ressourcen zurück und ändern nicht die Konfigurationen.

- Write (Schreiben)

Nur-Schreiben-Ereignisse enthalten API-Operationen, die (möglicherweise) Ihre Ressourcen ändern. Die API-Operationen Amazon EC2 `RunInstances` und `TerminateInstances` ändern beispielsweise Ihre Instances.

Beispiel: protokollieren von Lese- und Schreibereignissen für separate Trails

Das folgende Beispiel zeigt, wie Sie Trails konfigurieren können, um die Protokollaktivität für ein Konto in separate S3-Buckets aufzuteilen: ein Bucket empfängt schreibgeschützte Ereignisse und ein zweiter Bucket empfängt schreibgeschützte Ereignisse.

1. Sie erstellen einen Pfad und wählen einen S3-Bucket namens `read-only-bucket` für den Empfang von Protokolldateien aus. Anschließend aktualisieren Sie den Trail, um anzugeben, dass Sie Lese-Verwaltungsereignisse haben möchten.
2. Sie erstellen einen zweiten Trail und wählen einen S3-Bucket namens `write-only-bucket` aus, der die Protokolldateien aufnehmen soll. Anschließend aktualisieren Sie den Trail, um anzugeben, dass Sie Verwaltungsereignisse vom Typ Schreiben protokollieren möchten.
3. Die API-Operationen Amazon EC2 `DescribeInstances` und `TerminateInstances` werden in Ihrem Konto ausgeführt.
4. Der `DescribeInstances`-API-Vorgang ist ein schreibgeschütztes Ereignis und entspricht den Einstellungen für den ersten Trail. Der Trail protokolliert das Ereignis und liefert es an den `read-only-bucket`.

- Die `TerminateInstances`-API-Operation ist ein Nur-Schreiben-Ereignis und stimmt mit den Einstellungen für den zweiten Trail überein. Der Trail protokolliert das Ereignis und liefert es an den `write-only-bucket`.

## Protokollieren von Ereignissen mit der AWS Command Line Interface

Sie können Ihre Trails oder Ereignisdatenspeicher so konfigurieren, dass Verwaltungsereignisse mit AWS CLI protokolliert werden.

### Themen

- [Beispiel: Protokollieren von Verwaltungsereignissen für Trails](#)
- [Beispiele: Protokollieren von Verwaltungsereignissen für Ereignisdatenspeicher](#)

### Beispiel: Protokollieren von Verwaltungsereignissen für Trails

Führen Sie den Befehl `get-event-selectors` aus, um anzuzeigen, ob Ihr Trail Verwaltungsereignisse protokolliert.

```
aws cloudtrail get-event-selectors --trail-name TrailName
```

Das folgende Beispiel gibt die Standardeinstellungen für einen Trail zurück. Standardmäßig protokollieren Trails alle Verwaltungsereignisse, Ereignisse aller Ereignisquellen und keine Datenereignisse.

```
{
  "TrailARN": "arn:aws:cloudtrail:us-east-1:111122223333:trail/TrailName",
  "AdvancedEventSelectors": [
    {
      "Name": "Management events selector",
      "FieldSelectors": [
        {
          "Field": "eventCategory",
          "Equals": [
            "Management"
          ]
        }
      ]
    }
  ]
}
```



```
}
```

Sie können entweder einfache oder erweiterte Ereignisauswahlfunktionen verwenden, um Verwaltungsereignisse zu protokollieren. Sie können nicht sowohl Ereignisauswahlen als auch erweiterte Ereignisauswahlen auf einen Trail anwenden. Wenn Sie erweiterte Ereignisselektoren auf einen Trail anwenden, werden alle vorhandenen grundlegenden Ereignisselektoren überschrieben. Die folgenden Abschnitte enthalten Beispiele für die Protokollierung von Verwaltungsereignissen mithilfe erweiterter Ereignisselektoren und einfacher Ereignisselektoren.

## Themen

- [Beispiele: Protokollierung von Verwaltungsereignissen für Trails mithilfe erweiterter Event-Selektoren](#)
- [Beispiele: Protokollierung von Verwaltungsereignissen für Trails mithilfe einfacher Event-Selektoren](#)

## Beispiele: Protokollierung von Verwaltungsereignissen für Trails mithilfe erweiterter Event-Selektoren

Im folgenden Beispiel wird eine erweiterte Ereignisauswahl für einen Trail erstellt, der so benannt ist, *TrailName* dass er Verwaltungsereignisse mit Schreibschutz und Schreibzugriff (durch Weglassen des `readOnly` Selektors), aber Ereignisse ausschließt (`eventSource`). AWS Key Management Service AWS KMS Da AWS KMS Ereignisse als Verwaltungsereignisse behandelt werden und es eine große Anzahl von Ereignissen geben kann, können sie erhebliche Auswirkungen auf Ihre CloudTrail Rechnung haben, wenn Sie mehr als einen Trail haben, der Verwaltungsereignisse erfasst.

Wenn Sie sich dafür entscheiden, Verwaltungsereignisse nicht zu protokollieren, werden AWS KMS Ereignisse nicht protokolliert, und Sie können die Einstellungen für die AWS KMS Ereignisprotokollierung nicht ändern.

Um wieder mit der Protokollierung von AWS KMS Ereignissen in einem Trail zu beginnen, entfernen Sie die `eventSource` Auswahl und führen Sie den Befehl erneut aus.

```
aws cloudtrail put-event-selectors --trail-name TrailName \  
--advanced-event-selectors '  
[  
  {  
    "Name": "Log all management events except KMS events",  
    "FieldSelectors": [  
      { "Field": "eventCategory", "Equals": ["Management"] },  
      { "Field": "eventSource", "NotEquals": ["kms.amazonaws.com"] }  
    ]  
  }  
]
```

```
}
]'
```

Das Beispiel gibt die für den Trail konfigurierten fortschrittlichen Ereignisauswahlen zurück.

```
{
  "AdvancedEventSelectors": [
    {
      "Name": "Log all management events except KMS events",
      "FieldSelectors": [
        {
          "Field": "eventCategory",
          "Equals": [ "Management" ]
        },
        {
          "Field": "eventSource",
          "NotEquals": [ "kms.amazonaws.com" ]
        }
      ]
    }
  ],
  "TrailARN": "arn:aws:cloudtrail:us-east-2:123456789012:trail/TrailName"
}
```

Um die Protokollierung ausgeschlossener Ereignisse erneut in einen Trail zu starten, entfernen Sie den eventSource-Selektor, wie im folgenden Befehl gezeigt.

```
aws cloudtrail put-event-selectors --trail-name TrailName \
--advanced-event-selectors '
[
  {
    "Name": "Log all management events",
    "FieldSelectors": [
      { "Field": "eventCategory", "Equals": ["Management"] }
    ]
  }
]'
```

Im nächsten Beispiel wird ein erweiterter Event-Selektor für einen Trail erstellt, der so benannt ist *TrailName*, dass er Verwaltungsereignisse mit Schreibschutz und Schreibschutz (durch Weglassen des readOnly Selektors) einschließt, Amazon RDS Data API-Verwaltungsereignisse jedoch ausschließt. Um Amazon RDS Data API-Verwaltungsereignisse auszuschließen, geben

Sie die Amazon RDS-Daten-API-Ereignisquelle im Zeichenfolgenwert für das eventSource Feld an:rdsdata.amazonaws.com.

Wenn Sie sich dafür entscheiden, Verwaltungsereignisse nicht zu protokollieren, werden Amazon RDS Data API-Verwaltungsereignisse nicht protokolliert, und Sie können die Einstellungen für die Amazon RDS Data API-Ereignisprotokollierung nicht ändern.

Um wieder mit der Protokollierung von Amazon RDS Data API-Verwaltungsereignissen in einem Trail zu beginnen, entfernen Sie den eventSource Selektor und führen Sie den Befehl erneut aus.

```
aws cloudtrail put-event-selectors --trail-name TrailName \  
--advanced-event-selectors '  
[  
  {  
    "Name": "Log all management events except Amazon RDS Data API management events",  
    "FieldSelectors": [  
      { "Field": "eventCategory", "Equals": ["Management"] },  
      { "Field": "eventSource", "NotEquals": ["rdsdata.amazonaws.com"] }  
    ]  
  }  
]
```

Das Beispiel gibt die für den Trail konfigurierten fortschrittlichen Ereignisauswahlen zurück.


```
{  
  "AdvancedEventSelectors": [  
    {  
      "Name": "Log all management events except Amazon RDS Data API management events",  
      "FieldSelectors": [  
        {  
          "Field": "eventCategory",  
          "Equals": [ "Management" ]  
        },  
        {  
          "Field": "eventSource",  
          "NotEquals": [ "rdsdata.amazonaws.com" ]  
        }  
      ]  
    }  
  ],  
  "TrailARN": "arn:aws:cloudtrail:us-east-2:123456789012:trail/TrailName"  
}
```

Um die Protokollierung ausgeschlossener Ereignisse erneut in einen Trail zu starten, entfernen Sie den `eventSource`-Selektor, wie im folgenden Befehl gezeigt.

```
aws cloudtrail put-event-selectors --trail-name TrailName \  
--advanced-event-selectors '  
[  
  {  
    "Name": "Log all management events",  
    "FieldSelectors": [  
      { "Field": "eventCategory", "Equals": ["Management"] }  
    ]  
  }  
]'
```

Beispiele: Protokollierung von Verwaltungsereignissen für Trails mithilfe einfacher Event-Selektoren

Führen Sie den Befehl `put-event-selectors` aus, um Ihren Trail für die Protokollierung von Verwaltungsereignissen zu konfigurieren. Im folgenden Beispiel wird gezeigt, wie Sie den Trail so konfigurieren, dass alle Verwaltungsereignisse für zwei S3-Objekte eingeschlossen werden. Sie können zwischen 1 und 5 Ereignisselectoren für einen Trail angeben. Sie können zwischen 1 und 250 Datenressourcen für einen Trail festlegen.

 Note

Die maximale Anzahl der S3-Datenressourcen beträgt 250, unabhängig von der Anzahl der Ereignisauswahlen.

```
aws cloudtrail put-event-selectors --trail-name TrailName --event-selectors  
'[{"ReadWriteType": "All", "IncludeManagementEvents": true, "DataResources":  
[{"Type": "AWS::S3::Object", "Values": ["arn:aws:s3:::mybucket/prefix",  
"arn:aws:s3:::mybucket2/prefix2"]} ]]'
```

Das folgende Beispiel gibt die für den Trail konfigurierte Ereignisauswahl zurück.

```
{  
  "TrailARN": "arn:aws:cloudtrail:us-east-1:111122223333:trail/TrailName",  
  "EventSelectors": [  
    {  
      "ReadWriteType": "All",
```

```

    "IncludeManagementEvents": true,
    "DataResources": [
      {
        "Type": "AWS::S3::Object",
        "Values": [
          "arn:aws:s3:::mybucket/prefix",
          "arn:aws:s3:::mybucket2/prefix2",
        ]
      }
    ],
    "ExcludeManagementEventSources": []
  }
]
}

```

Um Ereignisse AWS Key Management Service (AWS KMS) aus den Protokollen eines Trails auszuschließen, führen Sie den `put-event-selectors` Befehl aus und fügen Sie das Attribut `ExcludeManagementEventSources` mit dem Wert `kms.amazonaws.com` hinzu. Im folgenden Beispiel wird eine Ereignisauswahl für einen Trail erstellt, der so benannt ist, *TrailName* dass er Verwaltungsereignisse mit Schreibschutz und Schreibschutz enthält, Ereignisse jedoch ausschließt. AWS KMS Da eine große Anzahl von Ereignissen generiert werden AWS KMS kann, möchte der Benutzer in diesem Beispiel möglicherweise Ereignisse einschränken, um die Kosten eines Trails zu senken.

```

aws cloudtrail put-event-selectors --trail-name TrailName --event-selectors '[{"ReadWriteType": "All","ExcludeManagementEventSources": ["kms.amazonaws.com"],"IncludeManagementEvents": true}]'

```

Das Beispiel gibt die für den Trail konfigurierte Ereignisauswahl zurück.

```

{
  "TrailARN": "arn:aws:cloudtrail:us-east-1:111122223333:trail/TrailName",
  "EventSelectors": [
    {
      "ReadWriteType": "All",
      "IncludeManagementEvents": true,
      "DataResources": [],
      "ExcludeManagementEventSources": [
        "kms.amazonaws.com"
      ]
    }
  ]
}

```

```
]
}
```

Um Verwaltungsereignisse der Amazon RDS Data API aus den Protokollen eines Trails auszuschließen, führen Sie den `put-event-selectors` Befehl aus und fügen Sie das Attribut `ExcludeManagementEventSources` mit dem Wert `hzrdsdata.amazonaws.com`. Das folgende Beispiel erstellt einen Event-Selector für einen Trail, der so benannt ist, *TrailName* dass er Verwaltungsereignisse mit Schreibschutz und Schreibschutz enthält, aber Amazon RDS Data API-Verwaltungsereignisse ausschließt. Da die Amazon RDS Data API eine große Anzahl von Verwaltungsereignissen generieren kann, möchte der Benutzer in diesem Beispiel möglicherweise Ereignisse einschränken, um die Kosten eines Trails zu verwalten.

```
{
  "TrailARN": "arn:aws:cloudtrail:us-east-1:111122223333:trail/TrailName",
  "EventSelectors": [
    {
      "ReadWriteType": "All",
      "IncludeManagementEvents": true,
      "DataResources": [],
      "ExcludeManagementEventSources": [
        "rdsdata.amazonaws.com"
      ]
    }
  ]
}
```

Um wieder mit der Protokollierung AWS KMS oder von Amazon RDS Data API-Verwaltungsereignissen in einem Trail zu beginnen, übergeben Sie eine leere Zeichenfolge als Wert von `ExcludeManagementEventSources`, wie im folgenden Befehl gezeigt.

```
aws cloudtrail put-event-selectors --trail-name TrailName --event-
selectors '[{"ReadWriteType": "All","ExcludeManagementEventSources":
[],"IncludeManagementEvents": true}]'
```

Um relevante AWS KMS Ereignisse in einem Trail wie `Delete` und zu protokollieren `DisableScheduleKey`, aber umfangreiche AWS KMS Ereignisse wie, und auszuschließen `Encrypt DecryptGenerateDataKey`, protokollieren Sie Verwaltungsereignisse nur mit Schreibzugriff und behalten Sie die Standardeinstellung zum Protokollieren von AWS KMS Ereignissen bei, wie im folgenden Beispiel gezeigt.

```
aws cloudtrail put-event-selectors --trail-name TrailName --event-  
selectors '[{"ReadWriteType": "WriteOnly", "ExcludeManagementEventSources":  
[], "IncludeManagementEvents": true}]'
```

## Beispiele: Protokollieren von Verwaltungsereignissen für Ereignisdatenspeicher

Führen Sie den Befehl „get-event-data-store“ aus, um zu überprüfen, ob Ihr Ereignisdatenspeicher Verwaltungsereignisse enthält.

```
aws cloudtrail get-event-data-store  
--event-data-store arn:aws:cloudtrail:us-east-1:12345678910:eventdatastore/EXAMPLE-  
f852-4e8f-8bd1-bcf6cEXAMPLE
```

Nachfolgend finden Sie eine Beispielantwort. Die Erstellung und die letzten aktualisierten Zeiten sind im timestamp-Format.

```
{  
  "EventDataStoreArn": "arn:aws:cloudtrail:us-east-1:12345678910:eventdatastore/  
EXAMPLE-f852-4e8f-8bd1-bcf6cEXAMPLE",  
  "Name": "myManagementEvents",  
  "Status": "ENABLED",  
  "AdvancedEventSelectors": [  
    {  
      "Name": "Management events selector",  
      "FieldSelectors": [  
        {  
          "Field": "eventCategory",  
          "Equals": [  
            "Management"  
          ]  
        }  
      ]  
    }  
  ],  
  "MultiRegionEnabled": true,  
  "OrganizationEnabled": false,  
  "BillingMode": "FIXED_RETENTION_PRICING",  
  "RetentionPeriod": 2557,  
  "TerminationProtectionEnabled": true,  
  "CreatedTimestamp": "2023-02-04T15:56:27.418000+00:00",  
  "UpdatedTimestamp": "2023-02-04T15:56:27.544000+00:00"
```

```
}
```

Um einen Ereignisdatenspeicher zu erstellen, der alle Verwaltungsereignisse enthält, führen Sie den Befehl „create-event-data-store“ aus. Sie müssen keine erweiterten Ereignisselektoren angeben, um alle Verwaltungsereignisse einzubeziehen.

```
aws cloudtrail create-event-data-store
--name my-event-data-store
--retention-period 90\
```

Nachfolgend finden Sie eine Beispielantwort.

```
{
  "EventDataStoreArn": "arn:aws:cloudtrail:us-east-1:12345678910:eventdatastore/
EXAMPLE-f852-4e8f-8bd1-bcf6cEXAMPLE",
  "Name": "my-event-data-store",
  "Status": "CREATED",
  "AdvancedEventSelectors": [
    {
      "Name": "Default management events",
      "FieldSelectors": [
        {
          "Field": "eventCategory",
          "Equals": [
            "Management"
          ]
        }
      ]
    }
  ],
  "MultiRegionEnabled": true,
  "OrganizationEnabled": false,
  "BillingMode": "EXTENDABLE_RETENTION_PRICING",
  "RetentionPeriod": 90,
  "TerminationProtectionEnabled": true,
  "CreatedTimestamp": "2023-11-13T16:41:57.224000+00:00",
  "UpdatedTimestamp": "2023-11-13T16:41:57.357000+00:00"
}
```

Um einen Ereignisdatenspeicher zu erstellen, der Ereignisse AWS Key Management Service (AWS KMS) ausschließt, führen Sie den create-event-data-store Befehl aus und geben Sie an, dass eventSource der Wert ungleich ist. kms . amazonaws . com Im folgenden Beispiel wird ein



Ereignisdatenspeicher erstellt, der Verwaltungsereignisse mit Schreibschutz und Schreibschutz enthält, Ereignisse jedoch ausschließt. AWS KMS

```
aws cloudtrail create-event-data-store --name event-data-store-name --retention-period
90 --advanced-event-selectors '[
  {
    "Name": "Management events selector",
    "FieldSelectors": [
      {"Field": "eventCategory", "Equals": ["Management"]},
      {"Field": "eventSource", "NotEquals": ["kms.amazonaws.com"]}
    ]
  }
]'
```

Nachfolgend finden Sie eine Beispielantwort.

```
{
  "EventDataStoreArn": "arn:aws:cloudtrail:us-east-1:12345678910:eventdatastore/
EXAMPLE-f852-4e8f-8bd1-bcf6cEXAMPLE",
  "Name": "event-data-store-name",
  "Status": "CREATED",
  "AdvancedEventSelectors": [
    {
      "Name": "Management events selector",
      "FieldSelectors": [
        {
          "Field": "eventCategory",
          "Equals": [
            "Management"
          ]
        },
        {
          "Field": "eventSource",
          "NotEquals": [
            "kms.amazonaws.com"
          ]
        }
      ]
    }
  ],
  "MultiRegionEnabled": true,
  "OrganizationEnabled": false,
  "BillingMode": "EXTENDABLE_RETENTION_PRICING",
```

```

    "RetentionPeriod": 90,
    "TerminationProtectionEnabled": true,
    "CreatedTimestamp": "2023-11-13T17:02:02.067000+00:00",
    "UpdatedTimestamp": "2023-11-13T17:02:02.241000+00:00"
  }

```

Um einen Ereignisdatenspeicher zu erstellen, der Verwaltungsereignisse der Amazon RDS Data API ausschließt, führen Sie den `create-event-data-store` Befehl aus und geben Sie an, dass `eventSource` dies ungleich `rdpdata.amazonaws.com` ist. Im folgenden Beispiel wird ein Ereignisdatenspeicher erstellt, bei dem Verwaltungsereignisse vom Typ „Nur Lesen“ und „Nur Schreiben“ ein- aber Daten-API-Ereignisse von Amazon RDS ausgeschlossen werden.

```

aws cloudtrail create-event-data-store --name event-data-store-name --retention-period
90 --advanced-event-selectors '[
  {
    "Name": "Management events selector",
    "FieldSelectors": [
      {"Field": "eventCategory", "Equals": ["Management"]},
      {"Field": "eventSource", "NotEquals": ["rdpdata.amazonaws.com"]}
    ]
  }
]'

```

Nachfolgend finden Sie eine Beispielantwort.

```

{
  "EventDataStoreArn": "arn:aws:cloudtrail:us-east-1:12345678910:eventdatastore/
EXAMPLE-f852-4e8f-8bd1-bcf6cEXAMPLE",
  "Name": "my-event-data-store",
  "Status": "CREATED",
  "AdvancedEventSelectors": [
    {
      "Name": "Management events selector",
      "FieldSelectors": [
        {
          "Field": "eventCategory",
          "Equals": [
            "Management"
          ]
        },
        {
          "Field": "eventSource",

```

```
        "NotEquals": [
            "rdsdata.amazonaws.com"
        ]
    }
]
},
"MultiRegionEnabled": true,
"OrganizationEnabled": false,
"BillingMode": "EXTENDABLE_RETENTION_PRICING",
"RetentionPeriod": 90,
"TerminationProtectionEnabled": true,
"CreatedTimestamp": "2023-11-13T17:02:02.067000+00:00",
"UpdatedTimestamp": "2023-11-13T17:02:02.241000+00:00"
}
```

## Protokollieren von Ereignissen mit AWS -SDKs

Verwenden Sie den [GetEventSelectors](#) Vorgang, um festzustellen, ob Ihr Trail Verwaltungsereignisse für einen Trail protokolliert. Sie können Ihre Trails so konfigurieren, dass sie Verwaltungsereignisse während des [PutEventSelectors](#) Vorgangs protokollieren. Weitere Informationen finden Sie in der [AWS CloudTrail -API-Referenz](#).

Führen Sie den [GetEventDataStore](#) Vorgang aus, um festzustellen, ob Ihr Ereignisdatenspeicher Verwaltungsereignisse enthält. Sie können Ihre Ereignisdatenspeicher so konfigurieren, dass sie Verwaltungsereignisse enthalten, indem Sie die [UpdateEventDataStore](#) Operationen [CreateEventDataStore](#) oder ausführen. Weitere Informationen finden Sie unter [Erstellen, aktualisieren und verwalten Sie Ereignisdatenspeicher mit dem AWS CLI](#) und der [AWS CloudTrail -API-Referenz](#).

## Ereignisse an Amazon CloudWatch Logs senden

CloudTrail unterstützt bei Trails das Senden von Daten und Verwaltungsereignissen an CloudWatch Logs. Wenn Sie Ihren Trail so konfigurieren, dass Ereignisse an Ihre CloudWatch Log-Protokollgruppe CloudTrail gesendet werden, werden nur die Ereignisse gesendet, die Sie in Ihrem Trail angegeben haben. Wenn Sie Ihren Trail beispielsweise so konfigurieren, dass er nur Verwaltungsereignisse protokolliert, übermittelt Ihr Trail Verwaltungsereignisse nur an Ihre CloudWatch Logs-Protokollgruppe. Weitere Informationen finden Sie unter [Überwachung von CloudTrail Protokolldateien mit Amazon CloudWatch Logs](#).

# Protokollieren von Datenereignissen

In diesem Abschnitt wird beschrieben, wie Datenereignisse mithilfe der [CloudTrail Konsole](#) und protokolliert [AWS CLI](#) werden.

Standardmäßig werden Datenereignisse nicht von Trails und Ereignisdatenspeichern protokolliert. Für Datenereignisse werden zusätzliche Gebühren fällig. Weitere Informationen finden Sie unter [AWS CloudTrail -Preisgestaltung](#).

Datenereignisse bieten Einblicke in die Ressourcenvorgänge, die für oder innerhalb einer Ressource ausgeführt wurden. Sie werden auch als Vorgänge auf der Datenebene bezeichnet. Datenereignisse sind oft Aktivitäten mit hohem Volume.

Beispiele für Datenereignisse:

- [Amazon S3 S3-API-Aktivität auf Objektebene](#) (z. B., `GetObjectDeleteObject`, und `PutObject` API-Operationen) für Objekte in S3-Buckets.
- AWS Lambda Aktivität zur Ausführung von Funktionen (die `Invoke` API).
- CloudTrail [PutAuditEvents](#) Aktivität auf einem [CloudTrail Lake-Kanal](#), der verwendet wird, um Ereignisse von außen zu protokollieren AWS.
- [Publish](#)- und [PublishBatch](#)-API-Operationen von Amazon SNS zu Themen.

Sie können erweiterte Event-Selektoren verwenden, um detaillierte Selektoren zu erstellen, die Ihnen helfen, die Kosten zu kontrollieren, indem sie nur die spezifischen Ereignisse protokollieren, die für Ihre Anwendungsfälle von Interesse sind. Sie können beispielsweise erweiterte Event-Selektoren verwenden, um bestimmte API-Aufrufe zu protokollieren, indem Sie dem Feld einen Filter hinzufügen. `eventName` Weitere Informationen finden Sie unter [Filtern von Datenereignissen mithilfe erweiterter Ereignisselectoren](#).

## Note

Die Ereignisse, die von Ihren Trails protokolliert werden, sind bei Amazon verfügbar EventBridge. Wenn Sie beispielsweise für den Trail festlegen, dass er Datenereignisse für S3-Objekte, aber keine Verwaltungsereignisse protokolliert, verarbeitet und protokolliert Ihr Trail nur Datenereignisse für die angegebenen S3-Objekte. Die Datenereignisse für diese S3-Objekte sind in Amazon verfügbar EventBridge. Weitere Informationen finden Sie unter [Events from AWS services](#) im EventBridge Amazon-Benutzerhandbuch.

## Inhalt


- [Datenergebnisse](#)
  - [Beispiele: Protokollieren von Datenergebnissen für Amazon-S3-Objekte](#)
  - [Protokollierung von Datenergebnissen für S3-Objekte in anderen AWS Konten](#)
- [Schreibgeschützte Ereignisse und Nur-Schreiben-Ereignisse](#)
- [Protokollierung von Datenergebnissen mit dem AWS Management Console](#)
- [Protokollieren von Datenergebnissen mit dem AWS Command Line Interface](#)
- [Protokollierung von Datenergebnissen für Trails mit dem AWS CLI](#)
  - [Protokollieren von Ereignissen mithilfe erweiterter Ereignisselektoren](#)
  - [Protokollieren Sie alle Amazon S3 S3-Ereignisse für einen Amazon S3 S3-Bucket mithilfe erweiterter Event-Selektoren](#)
  - [Protokollieren von Amazon S3 bei AWS Outposts -Ereignissen mithilfe erweiterter Ereignisselektoren](#)
  - [Protokollieren von Ereignissen mithilfe grundlegender Ereignisselektoren](#)
- [Protokollieren von Datenergebnissen für Ereignisdatenspeicher mit dem AWS CLI](#)
  - [Einschließen aller Amazon-S3-Ereignisse für einen Bucket](#)
  - [Einschließen von Amazon S3 in AWS Outposts -Ereignissen](#)
- [Filtern von Datenergebnissen mithilfe erweiterter Ereignisselektoren](#)
  - [Filterung von Datenergebnissen nach eventName](#)
    - [Filtern von Datenergebnissen mithilfe der eventNameAWS Management Console](#)
    - [Filtern von Datenergebnissen eventName mithilfe von AWS CLI](#)
  - [Filtern von Datenergebnissen nach resources.ARN](#)
    - [Filtern von Datenergebnissen resources.ARN mithilfe von AWS Management Console](#)
    - [Filtern von Datenergebnissen resources.ARN mithilfe von AWS CLI](#)
- [Datenergebnisse nach readOnly Wert filtern](#)
  - [Filtern von Datenergebnissen nach readOnly Wert mithilfe des AWS Management Console](#)
  - [Filtern von Datenergebnissen nach readOnly Wert mithilfe der AWS CLI](#)
- [Protokollieren von Datenergebnissen für AWS Config -Compliance](#)
- [Protokollieren von Datenergebnissen mit den SDKs AWS](#)

## Datenereignisse

In der folgenden Tabelle sind die Datenereignistypen aufgeführt, die für Trails und Ereignisdatenspeicher verfügbar sind. In der Spalte Datenereignistyp (Konsole) wird die entsprechende Auswahl in der Konsole angezeigt. Die Wertspalte `resources.type` zeigt den `resources.type` Wert, den Sie angeben würden, um Datenereignisse dieses Typs mithilfe der APIs oder in Ihren Trail- oder Event-Datenspeicher aufzunehmen. AWS CLI CloudTrail

Für Trails können Sie einfache oder erweiterte Event-Selektoren verwenden, um Datenereignisse für Amazon S3 S3-Objekte, Lambda-Funktionen und DynamoDB-Tabellen zu protokollieren (in den ersten drei Zeilen der Tabelle dargestellt). Sie können nur erweiterte Ereignisselektoren verwenden, um die in den verbleibenden Zeilen angezeigten Datenereignistypen zu protokollieren.

Für Ereignisdatenspeicher können Sie nur erweiterte Ereignisselektoren verwenden, um Datenereignisse einzubeziehen.

AWS-Service	Beschreibung	Typ des Datenereignisses (Konsole)	resources.type-Wert
Amazon-DynamoDB	<p><a href="#">Amazon DynamoDB DynamoDB-API-Aktivität auf Artikelebene</a> für Tabellen (z. B., <code>PutItemDeleteItem</code>, und <code>UpdateItem</code> API-Operationen).</p> <div data-bbox="354 1465 673 1885" style="border: 1px solid #0070C0; border-radius: 10px; padding: 10px; margin-top: 10px;"> <p> <b>Note</b></p> <p>Bei Tabellen mit aktivierten Streams enthält das <code>resources</code>-Feld im Datenereignis</p> </div>	DynamoDB	<code>AWS::DynamoDB::Table</code>

AWS-Service	Beschreibung	Typ des Dateneignisses (Konsole)	resources.type-Wert
	<p>gnis sowohl            AWS::Dyna            moDB::Str            eam als auch            AWS::Dyna            moDB::Tab            le .            Wenn Sie            AWS::Dyna            moDB::Tab            le als            resources            .type            angeben,            werden            standardm            äßig sowohl            DynamoDB-            Tabellen-            als auch            DynamoDB-            Stream-Er            eignisse            protokolliert.            Um <a href="#">Streams-            Ereignisse</a>            auszuschl            ießen, fügen            Sie dem            Feld einen</p>		


AWS-Service	Beschreibung	Typ des Datenereignisses (Konsole)	resources.type-Wert
	<div style="border: 1px solid #add8e6; border-radius: 10px; padding: 5px; width: fit-content; margin: auto;">           Filter hinzu. eventName         </div>		
AWS Lambda	AWS Lambda Aktivität zur Funktionsausführung (die Invoke API).	Lambda	AWS::Lambda::Function
Amazon S3	<a href="#">Amazon S3 S3-API-Aktivität auf Objektebene</a> (z. B., GetObject , DeleteObject , und PutObject API-Operationen) für Objekte in S3-Buckets.	S3	AWS::S3::Object
AWS AppConfig	<a href="#">AWS AppConfig API-Aktivität</a> für Konfigurationsvorgänge wie Aufrufe von und. StartConfigurationSession GetLatestConfiguration	AWS AppConfig	AWS::AppConfig::Configuration





AWS-Service	Beschreibung	Typ des Dateneignisses (Konsole)	resources.type-Wert
AWS B2B-Datenaustausch	B2B-Datenaustausch-API-Aktivität für Transformer-Operationen wie Aufrufe von <code>GetTransformerJob</code> und <code>StartTransformerJob</code> .	B2B-Datenaustausch	<code>AWS::B2BI::Transformer</code>
Amazon Bedrock	<a href="#">Amazon-Bedrock-API-Aktivität</a> auf einem Agent-Alias.	Bedrock-Agent-Alias	<code>AWS::Bedrock::AgentAlias</code>
	<a href="#">Amazon-Bedrock-API-Aktivität</a> auf einer Wissensdatenbank.	Bedrock-Wissensdatenbank	<code>AWS::Bedrock::KnowledgeBase</code>
Amazon CloudFront	CloudFront API-Aktivität auf einem <a href="#">KeyValueStore</a> .	CloudFront KeyValueStore	<code>AWS::CloudFront::KeyValueStore</code>
AWS Cloud Map	<a href="#">AWS Cloud Map API-Aktivität</a> in einem <a href="#">Namespace</a> .	AWS Cloud Map Namespace	<code>AWS::ServiceDiscovery::Namespace</code>
	<a href="#">AWS Cloud Map API-Aktivität</a> für einen <a href="#">Dienst</a> .	AWS Cloud Map Service nicht zulässig	<code>AWS::ServiceDiscovery::Service</code>

AWS-Service	Beschreibung	Typ des Datenereignisses (Konsole)	resources.type-Wert
AWS CloudTrail	CloudTrail <a href="#">PutAuditEvents</a> Aktivität auf einem <a href="#">CloudTrail Lake-Kanal</a> , der verwendet wird, um Ereignisse von außen zu protokollieren AWS.	CloudTrail Kanal	AWS::CloudTrail::Channel
Amazon CodeWhisperer	CodeWhisperer Amazon-API-Aktivität bei einer Anpassung.	CodeWhisperer Anpassung	AWS::CodeWhisperer::Customization
	CodeWhisperer Amazon-API-Aktivität in einem Profil.	CodeWhisperer	AWS::CodeWhisperer::Profile
Amazon Cognito	API-Aktivität von Amazon Cognito in Amazon-Cognito- <a href="#">Identitätspools</a> .	Cognito-Identitätspools	AWS::Cognito::IdentityPool
Amazon-DynamoDB	API-Aktivitäten von <a href="#">Amazon DynamoDB</a> in Streams.	DynamoDB-Streams	AWS::DynamoDB::Stream

AWS-Service	Beschreibung	Typ des Datenereignisses (Konsole)	resources.type-Wert
Amazon Elastic Block Store	Direkte APIs von <a href="#">Amazon Elastic Block Store (EBS)</a> wie PutSnapshotBlock , GetSnapshotBlock und ListChangedBlocks in Amazon-EBS-Snapshots.	Amazon EBS Direct-APIs	AWS::EC2::Snapshot
Amazon EMR	API-Aktivität von Amazon EMR in einem Write-Ahead-Log-Workspace.	EMR-Write-Ahead-Log-Workspace	AWS::EMRWAAL::Workspace
Amazon FinSpace	API-Aktivitäten von <a href="#">Amazon FinSpace</a> in Umgebungen.	FinSpace	AWS::FinSpace::Environment

AWS-Service	Beschreibung	Typ des Dateneignisses (Konsole)	resources.type-Wert
AWS Glue	<p>AWS Glue API-Aktivität für Tabellen, die von Lake Formation erstellt wurden.</p> <div data-bbox="354 590 673 1785" style="border: 1px solid #add8e6; border-radius: 10px; padding: 10px;"><p> <b>Note</b></p><p>AWS Glue Dateneignisse für Tabellen werden derzeit nur in den folgenden Regionen unterstützt:</p><ul style="list-style-type: none"><li>• USA Ost (Nord-Virginia)</li><li>• USA Ost (Ohio)</li><li>• USA West (Oregon)</li><li>• Europa (Irland)</li><li>• Region Asien-Pazifik (Tokio)</li></ul></div>	Lake Formation	AWS::Glue::Table

AWS-Service	Beschreibung	Typ des Datenereignisses (Konsole)	resources.type-Wert
Amazon GuardDuty	GuardDuty Amazon-API-Aktivität für einen <a href="#">Detektor</a> .	GuardDuty Detektor	AWS::GuardDuty::Detector
AWS HealthImaging	AWS HealthImaging API-Aktivität in Datenspeichern.	Datenspeicher für medizinische Bildgebung	AWS::MedicalImaging::Datastore
AWS IoT	<a href="#">AWS IoT API-Aktivität</a> für <a href="#">Zertifikate</a> .	IoT-Zertifikat	AWS::IoT::Certificate
	<a href="#">AWS IoT API-Aktivität</a> für <a href="#">Dinge</a> .	IoT-Sache	AWS::IoT::Thing
AWS IoT Greengrass Version 2	<a href="#">Greengrass-API-Aktivität</a> von einem Greengrass-Core-Gerät auf einer Komponentenversion.  <div data-bbox="354 1297 672 1801" style="border: 1px solid #00a0e3; border-radius: 10px; padding: 10px; background-color: #e6f2ff;"> <p> <b>Note</b></p> <p>Greengrass protokolliert keine Ereignisse, bei denen der Zugriff verweigert wurde.</p> </div>	IoT Greengrass-Komponentenversion	AWS::GreengrassV2::ComponentVersion

AWS-Service	Beschreibung	Typ des Datenereignisses (Konsole)	resources.type-Wert
	<p><a href="#">Greengrass-API-Aktivität</a> von einem Greengrass-Core-Gerät in einer Bereitstellung.</p> <div style="border: 1px solid #0070C0; border-radius: 10px; padding: 10px; margin-top: 10px;"> <p> <b>Note</b></p> <p>Greengrass protokolliert keine Ereignisse, bei denen der Zugriff verweigert wurde.</p> </div>	Einsatz von IoT Greengrass	AWS::GreengrassV2::Deployment
AWS IoT SiteWise	<a href="#">SiteWise IoT-API-Aktivität</a> für <a href="#">Anlagen</a> .	SiteWise IoT-Anlage	AWS::IoTSiteWise::Asset
	<a href="#">SiteWise IoT-API-Aktivität</a> in <a href="#">Zeitreihen</a> .	SiteWise IoT-Zeitreihen	AWS::IoTSiteWise::TimeSeries
AWS IoT TwinMaker	TwinMaker IoT-API-Aktivität für eine <a href="#">Entität</a> .	TwinMaker IoT-Entität	AWS::IoTTwinMaker::Entity
	TwinMaker IoT-API-Aktivität in einem <a href="#">Workspace</a> .	TwinMaker IoT-Arbeitsplatz	AWS::IoTTwinMaker::Workspace

AWS-Service	Beschreibung	Typ des Datenereignisses (Konsole)	resources.type-Wert
Amazon Kendra Intelligent Ranking	API-Aktivität von Amazon Kendra Intelligent Rankin für <a href="#">Rescore-Ausführungspläne</a> .	Kendra-Rangliste	AWS::KendraRanking::ExecutionPlan
Amazon Keyspaces (für Apache Cassandra)	<a href="#">Amazon Keyspaces-API-Aktivität</a> in einer Tabelle.	Cassandra-Tabelle	AWS::Cassandra::Table
Amazon-Kinesis-Data-Streams	Kinesis Data Streams Streams-API-Aktivität in <a href="#">Streams</a> .	Kinesis-Stream	AWS::Kinesis::Stream
	Kinesis Data Streams Streams-API-Aktivität auf <a href="#">Stream-Verbrauchern</a> .	Kinesis Stream Consumer	AWS::Kinesis::StreamConsumer
Amazon Kinesis Video Streams	Kinesis Video Streams Streams-API-Aktivitäten in Videostreams, z. B. Aufrufe von GetMedia undPutMedia.	Kinesis-VideoStream	AWS::KinesisVideo::Stream
Amazon Managed Blockchain	API-Aktivität von Amazon Managed Blockchain in einem Netzwerk.	Managed-Blockchain-Netzwerk	AWS::ManagedBlockchain::Network

AWS-Service	Beschreibung	Typ des Datenereignisses (Konsole)	resources.type-Wert
	JSON-RPC-Aufrufe von <a href="#">Amazon Managed Blockchain</a> in Ethereum-Knoten, zum Beispiel <code>eth_getBalance</code> oder <code>eth_getBlockByNumber</code> .	Managed Blockchain	<code>AWS::ManagedBlockchain::Node</code>
Amazon-Neptune-Graph	Daten-API-Aktivitäten in einem Neptune-Graph, zum Beispiel Abfragen, Algorithmen oder Vektorsuche.	Neptun-Graph	<code>AWS::NeptuneGraph::Graph</code>
AWS Private CA	AWS Private CA Konnektor für Active Directory-API-Aktivitäten.	AWS Private CA Konnektor für Active Directory	<code>AWS::PCACConnectorAD::Connector</code>
Amazon Q Apps	Daten-API-Aktivität auf <a href="#">Amazon Q Apps</a> .	Amazon Q Apps	<code>AWS::QApps:QApp</code>
Amazon Q Business	<a href="#">Amazon-Q-Business-API-Aktivität</a> auf einer Anwendung.	Amazon-Q-Business-Anwendung	<code>AWS::QBusiness::Application</code>
	<a href="#">Amazon-Q-Business-API-Aktivität</a> auf einer Datenquelle.	Amazon-Q-Business-Datenquelle	<code>AWS::QBusiness::DataSource</code>



AWS-Service	Beschreibung	Typ des Dateneignisses (Konsole)	resources.type-Wert
	<a href="#">Amazon-Q-Business-API-Aktivität</a> auf einem Index.	Amazon-Q-Business-Index	AWS::QBusiness::Index
	<a href="#">Amazon-Q-Business-API-Aktivität</a> auf einem Weberlebnis.	Amazon-Q-Business-Weberlebnis	AWS::QBusiness::WebExperience
Amazon RDS	<a href="#">Amazon RDS-API-Aktivität</a> in einem DB-Cluster.	RDS-Daten-API — DB-Cluster	AWS::RDS::DBCluster
Amazon S3	<a href="#">Amazon S3 S3-API-Aktivität</a> auf Access Points.	S3-Zugangspunkt	AWS::S3::AccessPoint
	<a href="#">API-Aktivitäten für Amazon S3 Object Lambda Access Points</a> , z. B. Aufrufe von CompleteMultipartUpload undGetObject .	S3 Objekt Lambda	AWS::S3ObjectLambda::AccessPoint
Amazon S3 in Outposts	API-Aktivität auf Objektebene auf <a href="#">Amazon S3 on Outposts</a> .	S3-Outposts	AWS::S3Outposts::Object

AWS-Service	Beschreibung	Typ des Datenereignisses (Konsole)	resources.type-Wert
Amazon SageMaker	SageMaker <a href="#">InvokeEndpointWithResponseStream</a> Amazon-Aktivitäten auf Endpunkten.	SageMaker Endpunkt	AWS::SageMaker::Endpoint
	SageMaker Amazon-API-Aktivität in Feature-Stores.	SageMaker feature store	AWS::SageMaker::FeatureGroup
	SageMaker Amazon-API-Aktivität für <a href="#">Komponenten von Versuchsversuchen</a> .	SageMaker Metriken, Experiment, Versuchskomponente	AWS::SageMaker::ExperimentTrialComponent
Amazon SNS	<a href="#">Publish</a> -API-Operationen von Amazon SNS auf Plattformendpunkten.	SNS-Plattformendpunkt	AWS::SNS::PlatformEndpoint
	<a href="#">Publish</a> - und <a href="#">PublishBatch</a> - API-Operationen von Amazon SNS zu Themen.	SNS-Thema	AWS::SNS::Topic
Amazon SQS	<a href="#">Amazon-SQS-API-Aktivität</a> auf Nachrichten.	SQS	AWS::SQS::Queue

AWS-Service	Beschreibung	Typ des Datenereignisses (Konsole)	resources.type-Wert
AWS Step Functions	<a href="#">API-Aktivität von Step Functions</a> auf einer Zustandsmaschine.	Step-Functions-Zustandsautomat	AWS::StepFunctions::StateMachine
AWS Supply Chain	AWS Supply Chain API-Aktivität auf einer Instanz.	Lieferkette	AWS::SCN::Instance
Amazon SWF	<a href="#">Amazon SWF SWF-API-Aktivität</a> auf <a href="#">Domains</a> .	SWF-Domäne	AWS::SWF::Domain
AWS Systems Manager	<a href="#">Systems Manager Manager-API-Aktivität</a> auf Kontrollkanälen.	Systems Manager	AWS::SSMMessages::ControlChannel
	<a href="#">Systems Manager Manager-API-Aktivität</a> auf verwalteten Knoten.	Von Systems Manager verwalteter Knoten	AWS::SSM::ManagedNode
Amazon Timestream	<a href="#">Query</a> -API-Aktivität von Amazon Timestream in Datenbanken.	Timestream-Datenbank	AWS::Timestream::Database
	<a href="#">Query</a> -API-Aktivität von Amazon Timestream in Tabellen.	Timestream-Tabelle	AWS::Timestream::Table

AWS-Service	Beschreibung	Typ des Datenereignisses (Konsole)	resources.type-Wert
Amazon Verified Permissions	API-Aktivität von Amazon Verified Permissions in einem Richtlinienpeicher.	Amazon Verified Permissions	AWS::VerifiedPermissions::PolicyStore
Amazon WorkSpaces Thin Client	WorkSpaces Thin Client-API-Aktivität auf einem Gerät.	Thin-Client-Gerät	AWS::ThinClient::Device
	WorkSpaces Thin Client-API-Aktivität in einer Umgebung.	Thin-Client-Umgebung	AWS::ThinClient::Environment
AWS X-Ray	<a href="#">X-Ray-API-Aktivität auf Spuren</a> .	Röntgenspur	AWS::XRay::Trace

Um CloudTrail Datenereignisse aufzuzeichnen, müssen Sie jeden Ressourcentyp, für den Sie Aktivitäten erfassen möchten, explizit hinzufügen. Weitere Informationen finden Sie unter [Erstellen eines Trails](#) und [Erstellen Sie mit der Konsole einen Ereignisdatenspeicher für CloudTrail Ereignisse](#).

In einem Trail oder einem Ereignisspeicher mit einer Region können Sie Datenereignisse nur für Ressourcen protokollieren, auf die Sie in dieser Region zugreifen können. Obwohl S3-Buckets global sind, sind AWS Lambda Funktionen und DynamoDB-Tabellen regional.

Für die Protokollierung von Datenereignissen fallen zusätzliche Gebühren an. CloudTrail [Die Preise finden Sie unter Preise.AWS CloudTrail](#)

## Beispiele: Protokollieren von Datenereignissen für Amazon-S3-Objekte

Protokollierung von Datenereignissen für alle S3-Objekte in einem S3-Bucket

Das folgende Beispiel zeigt, wie die Protokollierung funktioniert, wenn Sie die Protokollierung aller Datenereignisse für einen S3-Bucket namens *bucket-1* konfigurieren. In diesem Beispiel

hat der CloudTrail Benutzer ein leeres Präfix und die Option angegeben, sowohl Lese - als auch Schreibdatenereignisse zu protokollieren.

1. Ein Benutzer lädt ein Objekt auf bucket-1 hoch.
2. Der PutObject-API-Vorgang ist eine Amazon-S3-API auf Objektebene. Es wird als Datenereignis in aufgezeichnet CloudTrail. Da der CloudTrail Benutzer einen S3-Bucket mit einem leeren Präfix angegeben hat, werden Ereignisse, die für jedes Objekt in diesem Bucket auftreten, protokolliert. Der Trail oder der Ereignisdatenspeicher verarbeitet und protokolliert das Ereignis.
3. Ein weiterer Benutzer lädt ein Objekt auf bucket-2 hoch.
4. Der PutObject-API-Vorgang ist an einem Objekt in einem S3-Bucket aufgetreten, das nicht für den Trail oder den Ereignisdatenspeicher angegeben wurde. Der Trail- oder Ereignisdatenspeicher protokolliert das Ereignis nicht.

### Protokollierung von Datenereignissen für bestimmte S3-Objekte

Das folgende Beispiel zeigt, wie die Protokollierung funktioniert, wenn Sie einen Trail oder Ereignisdatenspeicher so konfigurieren, dass Ereignisse für bestimmte S3-Objekte protokolliert werden. In diesem Beispiel hat der CloudTrail Benutzer einen S3-Bucket namens *bucket-3* mit dem Präfix *my-images* und der Option angegeben, nur Write-Data-Ereignisse zu protokollieren.

1. Ein Benutzer löscht im Bucket ein Objekt, das mit dem my-images-Präfix beginnt, beispielsweise `arn:aws:s3:::bucket-3/my-images/example.jpg`.
2. Der DeleteObject-API-Vorgang ist eine Amazon-S3-API auf Objektebene. Es wird als Write-Data-Ereignis in aufgezeichnet. CloudTrail Das Ereignis ist bei einem Objekt eingetreten, das mit dem in dem Trail oder Ereignisdatenspeicher angegebenen S3-Bucket und Präfix übereinstimmt. Der Trail oder der Ereignisdatenspeicher verarbeitet und protokolliert das Ereignis.
3. Ein weiterer Benutzer löscht im S3-Bucket ein Objekt mit einem anderen Präfix, beispielsweise `arn:aws:s3:::bucket-3/my-videos/example.avi`.
4. Das Ereignis ist bei einem Objekt aufgetreten, das nicht mit dem in Ihrem Trail oder Ereignisdatenspeicher angegebenen Präfix übereinstimmt. Der Trail- oder Ereignisdatenspeicher protokolliert das Ereignis nicht.
5. Ein Benutzer ruft den GetObject-API-Vorgang für das Objekt auf, `arn:aws:s3:::bucket-3/my-images/example.jpg`.
6. Das Ereignis ist in einem Bucket und einem Präfix aufgetreten, die im Trail oder dem Ereignisdatenspeicher angegeben sind, aber bei GetObject handelt es sich um eine Amazon-

S3-API auf Objektebene mit Lesefunktion. Es wird als Datenleseereignis in aufgezeichnet CloudTrail, und der Trail- oder Ereignisdatenspeicher ist nicht für die Protokollierung von Leseereignissen konfiguriert. Der Trail- oder Ereignisdatenspeicher protokolliert das Ereignis nicht.

#### Note

Wenn Sie für Trails Datenereignisse für bestimmte Amazon-S3-Buckets protokollieren, wird empfohlen, keinen Amazon-S3-Bucket für die Protokollierung von Datenereignissen zu verwenden, um Protokolldateien zu empfangen, die Sie im Abschnitt für Datenereignisse angegeben haben. Wenn Sie denselben Amazon-S3-Bucket verwenden, protokolliert Ihr Trail jedes Mal ein Datenereignis, wenn die Protokolldateien an Ihren Amazon-S3-Bucket übergeben werden. Bei den Protokolldateien handelt es sich um aggregierte Ereignisse, die in regelmäßigen Abständen geliefert werden. Es handelt sich also nicht um ein 1:1-Verhältnis von Ereignis zu Protokolldatei; das Ereignis wird in der nächsten Protokolldatei aufgezeichnet. Wenn beispielsweise Protokolle CloudTrail übermittelt werden, tritt das PutObject Ereignis im S3-Bucket auf. Wenn der S3-Bucket auch im Abschnitt Datenereignisse angegeben ist, verarbeitet und protokolliert der Trail das PutObject-Ereignis als Datenereignis. Diese Aktion ist ein weiteres PutObject-Ereignis, und die Spur verarbeitet und protokolliert das Ereignis erneut.

Um die Protokollierung von Datenereignissen für den Amazon S3 S3-Bucket zu vermeiden, in dem Sie Protokolldateien erhalten, wenn Sie einen Trail zur Protokollierung aller Amazon S3 S3-Datenereignisse in Ihrem AWS Konto konfigurieren, sollten Sie die Übertragung von Protokolldateien an einen Amazon S3 S3-Bucket konfigurieren, der zu einem anderen AWS Konto gehört. Weitere Informationen finden Sie unter [Empfangen von CloudTrail Protokolldateien von mehreren Konten](#).

## Protokollierung von Datenereignissen für S3-Objekte in anderen AWS Konten

Wenn Sie Ihren Trail so konfigurieren, dass Datenereignisse protokolliert werden, können Sie auch S3-Objekte angeben, die zu anderen AWS Konten gehören. Wenn ein Ereignis für ein bestimmtes Objekt eintritt, wird CloudTrail ausgewertet, ob das Ereignis mit irgendwelchen Pfaden in den einzelnen Konten übereinstimmt. Wenn das Ereignis mit den Einstellungen für ein Trail übereinstimmt, verarbeitet und protokolliert den Trail das Ereignis für dieses Konto. Im Allgemeinen können sowohl API-Aufrufer als auch Ressourcenbesitzer Ereignisse empfangen.

Wenn Sie Eigentümer eines S3-Objekts sind und es in Ihrem Trail angeben, protokolliert Ihr Trail Ereignisse, die auf dem Objekt in Ihrem Konto auftreten. Da das Objekt Ihnen gehört, protokolliert der Trail auch Ereignisse, wenn andere Konten das Objekt aufrufen.

Wenn Sie ein S3-Objekt in Ihrem Trail angeben und das Objekt ist einem anderen Konto zugeordnet, protokolliert der Trail nur Ereignisse, die auf diesem Objekt in Ihrem Konto auftreten. Ereignisse, die in anderen Konten auftreten, werden von Ihrem Trail nicht protokolliert.

Beispiel: Protokollieren von Datenereignissen für ein Amazon-S3-Objekt für zwei AWS -Konten

Das folgende Beispiel zeigt, wie zwei AWS Konten so konfiguriert werden CloudTrail , dass sie Ereignisse für dasselbe S3-Objekt protokollieren.

1. In Ihrem Konto möchten Sie, dass Ihr Trail Datenereignisse für alle Objekte in Ihrem S3-Bucket namens `owner-bucket` protokolliert. Sie konfigurieren den Trail, indem Sie den S3-Bucket mit einem leeren Objektpräfix angeben.
2. Bob hat ein separates Konto, das auf den S3-Bucket zugreifen kann. Bob möchte auch Datenereignisse für alle Objekte im selben S3-Bucket protokollieren. Für sein Trail konfiguriert er sein Trail und gibt denselben S3-Bucket mit einem leeren Objektpräfix an.
3. Bob lädt mit dem `PutObject`-API-Vorgang ein Objekt in den S3-Bucket hoch.
4. Dieses Ereignis ist in seinem Konto aufgetreten und stimmt mit den Trail-Einstellungen überein. Bobs Trail verarbeitet und protokolliert das Ereignis.
5. Da der S3-Bucket Ihnen zugeordnet ist und das Ereignis mit den Einstellungen für Ihren Trail übereinstimmt, verarbeitet und protokolliert Ihr Trail das Ereignis ebenfalls. Da es jetzt zwei Kopien des Ereignisses gibt (eine ist in Bobs Spur und eine in Ihrer Datenbank protokolliert), CloudTrail fallen Gebühren für zwei Kopien des Datenereignisses an.
6. Sie laden ein Objekt in den S3-Bucket hoch.
7. Dieses Ereignis tritt in Ihrem Konto auf und entspricht den Einstellungen für Ihren Pfad. Ihr Trail verarbeitet und protokolliert das Ereignis.
8. Da das Ereignis nicht in Bobs Konto eingetreten ist und ihm der S3-Bucket nicht gehört, protokolliert Bobs Trail das Ereignis nicht. CloudTrail berechnet nur eine Kopie dieses Datenereignisses.

Beispiel: Protokollierung von Datenereignissen für alle Buckets, einschließlich eines S3-Buckets, der von zwei AWS Konten genutzt wird

Das folgende Beispiel zeigt das Protokollierungsverhalten, wenn „Alle S3-Buckets in Ihrem Konto auswählen“ für Trails aktiviert ist, die Datenereignisse in einem AWS Konto erfassen.

1. Ihr Trail soll in Ihrem Konto Datenereignisse für alle S3-Buckets protokollieren. Sie konfigurieren den Trail, indem Sie Lese-Ereignisse, Schreib-Ereignisse oder beides für Alle aktuellen und zukünftigen S3 Buckets in Datenereignisse auswählen.
2. Bob hat ein separates Konto, das Zugriff auf einen S3-Bucket in Ihrem Konto erhalten hat. Er möchte Datenereignisse für den Bucket protokollieren, auf den er Zugriff hat. Er konfiguriert seinen Trail so, dass er Datenereignisse für alle S3-Buckets erhält.
3. Bob lädt mit dem PutObject-API-Vorgang ein Objekt in den S3-Bucket hoch.
4. Dieses Ereignis ist in seinem Konto aufgetreten und stimmt mit den Trail-Einstellungen überein. Bobs Trail verarbeitet und protokolliert das Ereignis.
5. Da Sie Eigentümer des S3-Buckets sind und das Ereignis den Einstellungen für Ihren Trail entspricht, verarbeitet und protokolliert Ihr Trail das Ereignis ebenfalls. Da es jetzt zwei Kopien des Ereignisses gibt (eine ist in Bobs Trail angemeldet und eine in Ihrem Konto), wird für jedes Konto eine Kopie des Datenereignisses CloudTrail berechnet.
6. Sie laden ein Objekt in den S3-Bucket hoch.
7. Dieses Ereignis tritt in Ihrem Konto auf und entspricht den Einstellungen für Ihren Pfad. Ihr Trail verarbeitet und protokolliert das Ereignis.
8. Da das Ereignis nicht in Bobs Konto eingetreten ist und ihm der S3-Bucket nicht gehört, protokolliert Bobs Trail das Ereignis nicht. CloudTrail Gebühren für nur eine Kopie dieses Datenereignisses in Ihrem Konto.
9. Ein dritter Benutzer, Mary, hat Zugriff auf den S3-Bucket und führt einen GetObject-Vorgang auf dem Bucket aus. Sie hat eine Spur konfiguriert, um Datenereignisse auf allen S3-Buckets in ihrem Konto zu protokollieren. Da sie die API-Aufruferin ist, CloudTrail protokolliert sie ein Datenereignis. Obwohl Bob Zugriff auf den Bucket hat, ist er nicht der Eigentümer der Ressource, so dass diesmal kein Bucket in seinem Trail protokolliert wird. Als Eigentümerin der Ressource erhalten Sie in Ihrem Trail ein Ereignis über den GetObject Vorgang, den Mary aufgerufen hat. CloudTrailbelastet Ihr Konto und Marys Konto mit jeder Kopie des Datenereignisses: eine Kopie in Marys Spur und eine in Ihrer.



## Schreibgeschützte Ereignisse und Nur-Schreiben-Ereignisse

Wenn Sie Ihren Trail oder Ereignisdatenspeicher so konfigurieren, dass er Daten und Verwaltungsereignisse protokolliert, können Sie angeben, ob Sie Nur-Lesen-Ereignisse, Nur-Schreiben-Ereignisse oder beides wünschen.

- Read (Lesen)

Schreib-Ereignisse umfassen API-Operationen, die Ihre Ressourcen lesen, aber keine Änderungen vornehmen. Schreibgeschützte Ereignisse enthalten beispielsweise die API-Operationen Amazon EC2 `DescribeSecurityGroups` und `DescribeSubnets`. Diese Operationen geben nur Informationen über die Amazon-EC2-Ressourcen zurück und ändern nicht die Konfigurationen.

- Write (Schreiben)

Schreib-Ereignisse enthalten API-Operationen, die (möglicherweise) Ihre Ressourcen ändern. Die API-Operationen Amazon EC2 `RunInstances` und `TerminateInstances` ändern beispielsweise Ihre Instances.

Beispiel: protokollieren von Lese- und Schreibereignissen für separate Trails

Das folgende Beispiel zeigt, wie Sie Trails konfigurieren können, um die Protokollaktivität für ein Konto in separate S3-Buckets aufzuteilen: ein Bucket empfängt schreibgeschützte Ereignisse und ein zweiter Bucket empfängt schreiben geschützte Ereignisse.

1. Sie erstellen einen Pfad und wählen einen S3-Bucket namens `read-only-bucket` für den Empfang von Protokolldateien aus. Anschließend aktualisieren Sie den Trail, um anzugeben, dass Sie Schreib-Verwaltungs- und Datenereignisse protokollieren möchten.
2. Sie erstellen einen zweiten Trail und wählen einen S3-Bucket namens `write-only-bucket` aus, der die Protokolldateien aufnehmen soll. Anschließend aktualisieren Sie den Trail, um anzugeben, dass Sie Verwaltungs- und Datenereignisse vom Typ Schreiben protokollieren möchten.
3. Die API-Operationen Amazon EC2 `DescribeInstances` und `TerminateInstances` werden in Ihrem Konto ausgeführt.
4. Der `DescribeInstances`-API-Vorgang ist ein schreibgeschütztes Ereignis und entspricht den Einstellungen für den ersten Trail. Der Trail protokolliert das Ereignis und liefert es an den `read-only-bucket`.

5. Die `TerminateInstances`-API-Operation ist ein Nur-Schreiben-Ereignis und stimmt mit den Einstellungen für den zweiten Trail überein. Der Trail protokolliert das Ereignis und liefert es an den `write-only-bucket`.

## Protokollierung von Datenereignissen mit dem AWS Management Console

In den folgenden Verfahren wird beschrieben, wie Sie einen vorhandenen Ereignisdatenspeicher oder Trail aktualisieren, um Datenereignisse mit der AWS Management Console zu protokollieren. Weitere Informationen zum Erstellen eines Ereignisdatenspeichers zum Speichern von Protokolldatenereignissen finden Sie unter [Erstellen Sie mit der Konsole einen Ereignisdatenspeicher für CloudTrail Ereignisse](#). Weitere Informationen zum Erstellen eines Trails zum Protokollieren von Datenereignissen finden Sie unter [Erstellen eines Trails in der Konsole](#).

Bei Trails unterscheiden sich die Schritte zum Protokollieren von Datenereignissen je nachdem, ob Sie erweiterte oder einfache Event-Selektoren verwenden. Sie können Datenereignisse für alle Datenereignisarten mithilfe erweiterter Event-Selektoren protokollieren. Wenn Sie jedoch einfache Event-Selektoren verwenden, sind Sie auf die Protokollierung von Datenereignissen für Amazon S3 S3-Buckets und Bucket-Objekte, AWS Lambda Funktionen und Amazon DynamoDB-Tabellen beschränkt.

### Aktualisierung eines vorhandenen Ereignisdatenspeichers zur Protokollierung von Datenereignissen in AWS Management Console

Verwenden Sie das folgende Verfahren, um einen vorhandenen Ereignisdatenspeicher zu aktualisieren und Datenereignisse zu protokollieren. Weitere Informationen zur Verwendung erweiterter Ereignisselektoren finden Sie unter [Filtern von Datenereignissen mithilfe erweiterter Ereignisselektoren](#) diesem Thema.

1. Melden Sie sich unter <https://console.aws.amazon.com/cloudtrail/> bei der an AWS Management Console und öffnen Sie die CloudTrail Konsole.
2. Wählen Sie im Navigationsbereich unter Lake Ereignisdatenspeicher aus.
3. Wählen Sie auf der Seite Ereignisdatenspeicher den Ereignisdatenspeicher aus, den Sie aktualisieren möchten.


#### Note

Sie können Datenereignisse nur in Ereignisdatenspeichern aktivieren, die CloudTrail Ereignisse enthalten. Sie können keine Datenereignisse in CloudTrail

Ereignisdatenspeichern für AWS Config Konfigurationselemente, CloudTrail Insights-Ereignisse oder AWS Nichtereignisse aktivieren.

4. Wählen Sie auf der Detailseite unter Datenereignisse die Option Bearbeiten aus.
5. Wenn Sie noch keine Datenereignisse protokollieren, aktivieren Sie das Kontrollkästchen Datenereignisse.
6. Wählen Sie für Datenereignistyp den Ressourcentyp aus, für den Sie Datenereignisse protokollieren möchten.
7. Wählen Sie eine Protokollauswahlvorlage aus. CloudTrail enthält vordefinierte Vorlagen, die alle Datenereignisse für den Ressourcentyp protokollieren. Um eine benutzerdefinierte Protokoll-Selektorvorlage zu erstellen, wählen Sie Benutzerdefiniert aus.
8. (Optional) Geben Sie unter Selektornamen einen Namen ein, um Ihre Auswahl zu identifizieren. Der Selektornamen ist ein optionaler, beschreibender Name für eine erweiterte Ereignisauswahl, z. B. „Datenereignisse nur für zwei S3-Buckets protokollieren“. Der Name des Selektors wird als Name in der erweiterten Ereignisauswahl aufgeführt und ist sichtbar, wenn Sie die JSON-Ansicht erweitern.
9. Erstellen Sie in den erweiterten Ereignisselektoren einen Ausdruck für die spezifischen Ressourcen, für die Sie Datenereignisse protokollieren möchten. Sie können diesen Schritt überspringen, wenn Sie eine vordefinierte Protokollvorlage verwenden.
  - a. Wählen Sie aus den folgenden Feldern.
    - **readOnly**- `readOnly` kann auf den Wert **true** oder **false** gesetzt werden. Schreibgeschützte Datenereignisse sind Ereignisse, die den Zustand einer Ressource nicht ändern, z. B. `Get*`- oder `Describe*`-Ereignisse. Schreibereignisse fügen Ressourcen, Attribute oder Artefakte hinzu, ändern oder löschen sie, wie z. B. `Put*`-, `Delete*`- oder `Write*`-Ereignisse. Um sowohl `read`- als auch `write`-Ereignisse zu protokollieren, fügen Sie keinen `readOnly`-Selektor hinzu.
    - **eventName** – `eventName` kann einen beliebigen Operator verwenden. Sie können damit jedes Datenereignis, für das protokolliert wurde, ein- oder ausschließen CloudTrail, z. B. `PutBucketGetItem`, oder `GetSnapshotBlock`.
    - **resources.ARN**- Sie können jeden Operator mit `resources.ARN` verwenden, aber wenn Sie `equals` oder `unequal` verwenden, muss der Wert genau dem ARN einer gültigen Ressource des Typs entsprechen, den Sie in der Vorlage als Wert von `resources.type` angegeben haben.

In der folgenden Tabelle wird das gültige ARN-Format für alle `resources.type`-Werte aufgeführt.

 Note

Sie können das `resources.ARN` Feld nicht verwenden, um Ressourcentypen zu filtern, die keine ARNs haben.

resources.type	resources.ARN
AWS::DynamoDB::Table <sup>1</sup>	arn: <i>partition</i> :dynamodb : <i>region:account_ID</i> :table/ <i>table_name</i>
AWS::Lambda::Function	arn: <i>partition</i> :lambda: <i>region:account_ID</i> :function: <i>function_name</i>
AWS::S3::Object <sup>2</sup>	arn: <i>partition</i> :s3::: <i>bucket_name</i> / arn: <i>partition</i> :s3::: <i>bucket_name</i> / <i>object_or_file_name</i> /
AWS::AppConfig::Configuration	arn: <i>partition</i> :appconfi g: <i>region:account_ID</i> :applicat ion/ <i>application_ID</i> /environm ent/ <i>environment_ID</i> /configur ation/ <i>configuration_profile_ID</i>
AWS::B2BI::Transformer	arn: <i>partition</i> :b2bi: <i>region:account_ID</i> :transformer/ <i>transformer_ID</i>
AWS::Bedrock::AgentAlias	arn: <i>partition</i> :bedrock: <i>region:account_ID</i> :agent-al ias/ <i>agent_ID/alias_ID</i>

resources.type	resources.ARN
AWS::Bedrock::KnowledgeBase	<pre>arn:<i>partition</i> :bedrock:   <i>region</i>:<i>account_ID</i> :knowledge- base/<i>knowledge_base_ID</i></pre>
AWS::Cassandra::Table	<pre>arn:<i>partition</i> :cassandr a: <i>region</i>:<i>account_ID</i> :keyspace / <i>keyspace_name</i> /table/<i>table_name</i></pre>
AWS::CloudFront::KeyValueStore	<pre>arn:<i>partition</i> :cloudfro nt: <i>region</i>:<i>account_ID</i> :key-value- store/<i>KVS_name</i></pre>
AWS::CloudTrail::Channel	<pre>arn:<i>partition</i> :cloudtra il: <i>region</i>:<i>account_ID</i> :channel/ <i>channel_UUID</i></pre>
AWS::CodeWhisperer::Customization	<pre>arn:<i>partition</i> :codewhis perer: <i>region</i>:<i>account_ID</i> :customiz ation/ <i>customization_ID</i></pre>
AWS::CodeWhisperer::Profile	<pre>arn:<i>partition</i> :codewhis perer: <i>region</i>:<i>account_ID</i> :profile/ <i>profile_ID</i></pre>
AWS::Cognito::IdentityPool	<pre>arn:<i>partition</i> :cognito-identity:   <i>region</i>:<i>account_ID</i> :identity pool/ <i>identity_pool_ID</i></pre>
AWS::DynamoDB::Stream	<pre>arn:<i>partition</i> :dynamodb : <i>region</i>:<i>account_ID</i> :table/<i>table_name</i> / stream/<i>date_time</i></pre>

resources.type	resources.ARN
AWS::EC2::Snapshot	arn: <i>partition</i> :ec2: <i>region</i> ::snapshot/ <i>snapshot_ID</i>
AWS::EMRWALES::Workspace	arn: <i>partition</i> :emrwal: <i>region</i> : <i>account_ID</i> :workspace/ <i>workspace_name</i>
AWS::FinSpace::Environment	arn: <i>partition</i> :finspace : <i>region</i> : <i>account_ID</i> :environment/ <i>environment_ID</i>
AWS::Glue::Table	arn: <i>partition</i> :glue: <i>region</i> : <i>account_ID</i> :table/ <i>database_name</i> / <i>table_name</i>
AWS::GreengrassV2::ComponentVersion	arn: <i>partition</i> :greengrass : <i>region</i> : <i>account_ID</i> :components/ <i>component_name</i>
AWS::GreengrassV2::Deployment	arn: <i>partition</i> :greengrass : <i>region</i> : <i>account_ID</i> :deployments/ <i>deployment_ID</i>
AWS::GuardDuty::Detector	arn: <i>partition</i> :guardduty : <i>region</i> : <i>account_ID</i> :detector / <i>detector_ID</i>
AWS::IoT::Certificate	arn: <i>partition</i> :iot: <i>region</i> : <i>account_ID</i> :cert/ <i>certificate_ID</i>
AWS::IoT::Thing	arn: <i>partition</i> :iot: <i>region</i> : <i>account_ID</i> :thing/ <i>thing_ID</i>

resources.type	resources.ARN
AWS::IoTSiteWise::Asset	arn: <i>partition</i> :iotsitew ise: <i>region:account_ID</i> :asset/ <i>asset_ID</i>
AWS::IoTSiteWise::TimeSeries	arn: <i>partition</i> :iotsitew ise: <i>region:account_ID</i> :timeseri es/ <i>timeseries_ID</i>
AWS::IoTTwinMaker::Entity	arn: <i>partition</i> :iottwinm aker: <i>region:account_ID</i> :workspac e/ <i>workspace_ID</i> /entity/ <i>entity_ID</i>
AWS::IoTTwinMaker::Workspace	arn: <i>partition</i> :iottwinm aker: <i>region:account_ID</i> :workspac e/ <i>workspace_ID</i>
AWS::KendraRanking::ExecutionPlan	arn: <i>partition</i> :kendra-r anking: <i>region:account_ID</i> :rescore- execution-plan/ <i>rescore_execution_</i> <i>plan_ID</i>
AWS::Kinesis::Stream	arn: <i>partition</i> :kinesis: <i>region:account_ID</i> :stream/ <i>stream_name</i>
AWS::Kinesis::StreamConsumer	arn: <i>partition</i> :kinesis: <i>region:account_ID</i> :stream_ <i>ty</i> <i>pe</i> / <i>stream_name</i> /consumer/ <i>consumer_</i> <i>name</i> : <i>consumer_creation_timestamp</i>
AWS::KinesisVideo::Stream	arn: <i>partition</i> :kinesisv ideo: <i>region:account_I</i> <i>D</i> :stream/ <i>stream_name</i> / <i>creation_time</i>

resources.type	resources.ARN
AWS::ManagedBlockchain::Network	arn: <i>partition</i> :managedblockchain :::networks/ <i>network_name</i>
AWS::ManagedBlockchain::Node	arn: <i>partition</i> :managedblockchain : <i>region:account_ID</i> :nodes/ <i>node_ID</i>
AWS::MedicalImaging::Datastore	arn: <i>partition</i> :medical- imaging: <i>region:account_ID</i> :datastor e/ <i>data_store_ID</i>
AWS::NeptuneGraph::Graph	arn: <i>partition</i> :neptune- graph: <i>region:account_I</i> <i>D</i> :graph/ <i>graph_ID</i>
AWS::PCACConnectorAD::Connector	arn: <i>partition</i> :pca-connector- ad: <i>region:account_ID</i> :connecto r/ <i>connector_ID</i>
AWS::QApps:QApp	arn: <i>partition</i> :qapps: <i>region:account_I</i> <i>D</i> :application/ <i>application_UUID</i> / qapp/ <i>qapp_UUID</i>
AWS::QBusiness::Application	arn: <i>partition</i> :qbusines s: <i>region:account_ID</i> :applicat ion/ <i>application_ID</i>
AWS::QBusiness::DataSource	arn: <i>partition</i> :qbusines s: <i>region:account_ID</i> :applicat ion/ <i>application_ID</i> /index/ <i>index_ID</i> / data-source/ <i>datasource_ID</i>



resources.type	resources.ARN
AWS::QBusiness::Index	<pre>arn:partition :qbusines s: region:account_ID :applicat ion/ application_ID /index/index_ID</pre>
AWS::QBusiness::WebExperience	<pre>arn:partition :qbusines s: region:account_ID :applicat ion/ application_ID /web-expe rience/ web_experienc_ID</pre>
AWS::RDS::DBCluster	<pre>arn:partition :rds:region:account_I D :cluster/ cluster_name</pre>
AWS::S3::AccessPoint <sup>3</sup>	<pre>arn:partition :s3:region:account_I D :accesspoint/ access_point_name</pre>
AWS::S3ObjectLambda::AccessPoint	<pre>arn:partition :s3-object-lambda: region:account_ID :accesspo int/ access_point_name</pre>
AWS::S3Outposts::Object	<pre>arn:partition :s3-outpo sts: region:account_ID :object_path</pre>
AWS::SageMaker::Endpoint	<pre>arn:partition :sagemake r: region:account_ID :endpoint / endpoint_name</pre>
AWS::SageMaker::ExperimentTrialComponent	<pre>arn:partition :sagemake r: region:account_ID :experiment- trial-component/ experiment_trial_c omponent_name</pre>

resources.type	resources.ARN
AWS::SageMaker::FeatureGroup	<code>arn:partition:sagemake r: region:account_ID :feature- group/ feature_group_name</code>
AWS::SCN::Instance	<code>arn:partition :scn:region:account_I D :instance/ instance_ID</code>
AWS::ServiceDiscovery::Namespace	<code>arn:partition :servicediscovery: region:account_ID :namespac e/ namespace_ID</code>
AWS::ServiceDiscovery::Service	<code>arn:partition :servicediscovery: region:account_ID :service/ service_I D</code>
AWS::SNS::PlatformEndpoint	<code>arn:partition :sns:region:account_I D :endpoint/ endpoint_type /endpoint_ name /endpoint_ID</code>
AWS::SNS::Topic	<code>arn:partition :sns:region:account_I D :topic_name</code>
AWS::SQS::Queue	<code>arn:partition :sqs:region:account_I D :queue_name</code>

resources.type	resources.ARN
AWS::SSM::ManagedNode	<p>Der ARN muss in einem der folgenden Formate vorliegen:</p> <ul style="list-style-type: none"> <li>• <code>arn:<i>partition</i>:ssm:<i>region</i>:<i>account_ID</i>:managed-instance/<i>instance_ID</i></code></li> <li>• <code>arn:<i>partition</i>:ec2:<i>region</i>:<i>account_ID</i>:instance/<i>instance_ID</i></code></li> </ul>
AWS::SSMMessages::ControlChannel	<pre>arn:<i>partition</i>:ssmmessages:<i>region</i>:<i>account_ID</i>:control-channel/<i>control_channel_ID</i></pre>
AWS::StepFunctions::StateMachine	<p>Der ARN muss in einem der folgenden Formate vorliegen:</p> <ul style="list-style-type: none"> <li>• <code>arn:<i>partition</i>:states:<i>region</i>:<i>account_ID</i>:stateMachine:<i>stateMachine_name</i></code></li> <li>• <code>arn:<i>partition</i>:states:<i>region</i>:<i>account_ID</i>:stateMachine:<i>stateMachine_name</i>/<i>label_name</i></code></li> </ul>
AWS::SWF::Domain	<pre>arn:<i>partition</i>:swf:<i>region</i>:<i>account_ID</i>:domain/<i>domain_name</i></pre>
AWS::ThinClient::Device	<pre>arn:<i>partition</i>:thinclient:<i>region</i>:<i>account_ID</i>:device/<i>device_ID</i></pre>

resources.type	resources.ARN
AWS::ThinClient::Environment	arn: <i>partition</i> :thinclient: <i>region</i> : <i>account_ID</i> :environment/ <i>environment_ID</i>
AWS::Timestream::Database	arn: <i>partition</i> :timestream: <i>region</i> : <i>account_ID</i> :database/ <i>database_name</i>
AWS::Timestream::Table	arn: <i>partition</i> :timestream: <i>region</i> : <i>account_ID</i> :database/ <i>database_name</i> /table/ <i>table_name</i>
AWS::VerifiedPermissions::PolicyStore	arn: <i>partition</i> :verifiedpermissions: <i>region</i> : <i>account_ID</i> :policy-store/ <i>policy_store_ID</i>

<sup>1</sup> Bei Tabellen mit aktivierten Streams enthält das resources-Feld im Datenereignis sowohl AWS::DynamoDB::Stream als auch AWS::DynamoDB::Table. Wenn Sie AWS::DynamoDB::Table als resources.type angeben, werden standardmäßig sowohl DynamoDB-Tabellen- als auch DynamoDB-Stream-Ereignisse protokolliert. Um [Streams-Ereignisse](#) auszuschließen, fügen Sie dem eventName Feld einen Filter hinzu.


<sup>2</sup> Um alle Datenereignisse für alle Objekte in einem bestimmten S3-Bucket zu protokollieren, verwenden Sie den StartsWith-Operator und geben Sie nur die Bucket-ARN als übereinstimmenden Wert an. Der abschließende Schrägstrich ist beabsichtigt; schließen Sie ihn nicht aus.

<sup>3</sup> Um Ereignisse zu allen Objekten in einem S3-Zugangspunkt zu protokollieren, empfehlen wir, nur die Zugangspunkt-ARN zu verwenden, den Objektpfad nicht einzuschließen und die StartsWith- oder NotStartsWith-Operatoren oder zu verwenden.

Weitere Informationen zu den ARN-Formaten von Datenereignisressourcen finden Sie unter [Actions, resources, and condition keys](#) (Aktionen, Ressourcen und Bedingungsschlüssel) im AWS Identity and Access Management -Benutzerhandbuch.

- b. Wählen Sie für jedes Feld + Bedingung aus, um beliebig viele Bedingungen hinzuzufügen, bis zu maximal 500 angegebene Werte für alle Bedingungen. Um beispielsweise Datenereignisse für zwei S3-Buckets von Datenereignissen auszuschließen, die in Ihrem Ereignisdatenspeicher protokolliert werden, können Sie das Feld auf Resources.ARN festlegen, den Operator für beginnt nicht mit festlegen und dann entweder einen S3-Bucket-ARN einfügen oder nach den S3-Buckets suchen, für die Sie keine Ereignisse protokollieren möchten.

Um den zweiten S3-Bucket hinzuzufügen, wählen Sie + Bedingung und wiederholen Sie dann die vorherige Anweisung, indem Sie den ARN für einen anderen Bucket einfügen oder nach einem anderen Bucket suchen.

 Note

Sie können maximal 500 Werte für alle Selektoren in einem Ereignisdatenspeicher haben. Dies schließt Arrays mit mehreren Werten für einen Selektor wie eventName ein. Wenn Sie einzelne Werte für alle Selektoren haben, können Sie einem Selektor maximal 500 Bedingungen hinzufügen.

- c. Wählen Sie + Feld, um bei Bedarf zusätzliche Felder hinzuzufügen. Um Fehler zu vermeiden, legen Sie keine widersprüchlichen oder doppelten Werte für Felder fest. Geben Sie beispielsweise nicht an, dass ein ARN in einem Selektor einem Wert entspricht, und geben Sie dann an, dass der ARN in einem anderen Selektor nicht dem gleichen Wert entspricht.
10. Um einen weiteren Datentyp hinzuzufügen, für den Datenereignisse protokolliert werden sollen, wählen Sie Datenereignistyp hinzufügen. Wiederholen Sie die 6 Schritte bis zu diesem Schritt, um erweiterte Ereignisselektoren für den Datenereignistyp zu konfigurieren.
  11. Nachdem Sie Ihre Auswahl überprüft und bestätigt haben, wählen Sie Änderungen speichern aus.

## Aktualisierung eines vorhandenen Pfads zur Protokollierung von Datenereignissen mit erweiterten Event-Selektoren im AWS Management Console

Wenn Ihr Trail erweiterte Event-Selektoren verwendet AWS Management Console, können Sie aus vordefinierten Vorlagen wählen, die alle Datenereignisse auf einer ausgewählten Ressource protokollieren. Nachdem Sie eine Protokol- Selektorvorlage ausgewählt haben, können Sie die Vorlage so anpassen, dass sie nur die Datenereignisse enthält, die Sie am meisten sehen möchten. Weitere Informationen zur Verwendung erweiterter Event-Selektoren finden Sie unter [Filtern von Datenereignissen mithilfe erweiterter Ereignisselectoren](#) diesem Thema.

1. Wählen Sie auf den Seiten Dashboard oder Trails der CloudTrail Konsole den Trail aus, den Sie aktualisieren möchten.
2. Wählen Sie auf der Detailseite unter Datenereignisse die Option Bearbeiten aus.
3. Wenn Sie noch keine Datenereignisse protokollieren, aktivieren Sie das Kontrollkästchen Datenereignisse.
4. Wählen Sie für Datenereignistyp den Ressourcentyp aus, für den Sie Datenereignisse protokollieren möchten.
5. Wählen Sie eine Protokollauswahlvorlage aus. CloudTrail enthält vordefinierte Vorlagen, die alle Datenereignisse für den Ressourcentyp protokollieren. Um eine benutzerdefinierte Protokoll-Selektorvorlage zu erstellen, wählen Sie Benutzerdefiniert aus.

### Note

Wenn Sie eine vordefinierte Vorlage für S3-Buckets auswählen, wird die Protokollierung von Datenereignissen für alle Buckets aktiviert, die sich derzeit in Ihrem AWS Konto befinden, sowie für alle Buckets, die Sie nach Abschluss der Erstellung des Trails erstellen. Es ermöglicht auch die Protokollierung der Datenereignisaktivitäten, die von einem beliebigen Benutzer oder einer Rolle in Ihrem AWS Konto ausgeführt werden, selbst wenn diese Aktivität in einem Bucket ausgeführt wird, der zu einem anderen Konto gehört. AWS

Wenn der Trail nur für eine Region gilt, aktiviert die Auswahl einer vordefinierten Vorlage, die alle S3 Buckets protokolliert, die Datenereignisprotokollierung für alle Buckets in derselben Region wie Ihr Trail und alle Buckets, die Sie später in dieser Region erstellen. Es werden keine Datenereignisse für Amazon S3 S3-Buckets in anderen Regionen in Ihrem AWS Konto protokolliert.

Wenn Sie einen Trail für alle Regionen erstellen, aktiviert die Auswahl einer vordefinierten Vorlage für Lambda-Funktionen die Datenereignisprotokollierung


für alle Funktionen, die sich derzeit in Ihrem AWS Konto befinden, sowie für alle Lambda-Funktionen, die Sie möglicherweise in einer beliebigen Region erstellen, nachdem Sie den Trail erstellt haben. Wenn Sie einen Trail für eine einzelne Region erstellen (bei Pfaden ist dies nur mit der möglich AWS CLI), aktiviert diese Auswahl die Datenereignisprotokollierung für alle Funktionen, die sich derzeit in dieser Region in Ihrem AWS Konto befinden, sowie für alle Lambda-Funktionen, die Sie möglicherweise in dieser Region erstellen, nachdem Sie den Trail erstellt haben. Es wird keine Datenereignisprotokollierung für Lambda-Funktionen aktiviert, die in anderen Regionen erstellt wurden.

Das Protokollieren von Datenereignissen für alle Funktionen ermöglicht auch die Protokollierung von Datenereignisaktivitäten, die von einem beliebigen Benutzer oder einer Rolle in Ihrem AWS Konto ausgeführt werden, selbst wenn diese Aktivität für eine Funktion ausgeführt wird, die zu einem anderen AWS Konto gehört.

6. (Optional) Geben Sie unter Selektornamen einen Namen ein, um Ihre Auswahl zu identifizieren. Der Selektornamen ist ein optionaler, beschreibender Name für eine erweiterte Ereignisauswahl, z. B. „Datenereignisse nur für zwei S3-Buckets protokollieren“. Der Name des Selektors wird als Name in der erweiterten Ereignisauswahl aufgeführt und ist sichtbar, wenn Sie die JSON-Ansicht erweitern.
7. Erstellen Sie in den erweiterten Ereignisselektoren einen Ausdruck für die spezifischen Ressourcen, für die Sie Datenereignisse protokollieren möchten. Sie können diesen Schritt überspringen, wenn Sie eine vordefinierte Protokollvorlage verwenden.
  - a. Wählen Sie aus den folgenden Feldern.
    - **readOnly**- `readOnly` kann auf den Wert **true** oder **false** gesetzt werden. Schreibgeschützte Datenereignisse sind Ereignisse, die den Zustand einer Ressource nicht ändern, z. B. `Get*`- oder `Describe*`-Ereignisse. Schreibereignisse fügen Ressourcen, Attribute oder Artefakte hinzu, ändern oder löschen sie, wie z. B. `Put*`-, `Delete*`- oder `Write*`-Ereignisse. Um sowohl `read`- als auch `write`-Ereignisse zu protokollieren, fügen Sie keinen `readOnly`-Selektor hinzu.
    - **eventName** – `eventName` kann einen beliebigen Operator verwenden. Sie können damit jedes Datenereignis, für das protokolliert wurde, ein- oder ausschließen CloudTrail, z. B. `PutBucketGetItem`, oder `GetSnapshotBlock`.
    - **resources.ARN**- Sie können jeden Operator mit verwenden `resources.ARN`, aber wenn Sie `equals` oder `ungleich` verwenden, muss der Wert genau dem ARN einer gültigen

Ressource des Typs entsprechen, den Sie in der Vorlage als Wert von `resources.type` angegeben haben.

In der folgenden Tabelle wird das gültige ARN-Format für alle `resources.type`-Werte aufgeführt.

 Note

Sie können das `resources.ARN` Feld nicht verwenden, um Ressourcentypen zu filtern, die keine ARNs haben.

resources.type	resources.ARN
AWS::DynamoDB::Table <sup>1</sup>	arn: <i>partition</i> :dynamodb : <i>region</i> : <i>account_ID</i> :table/ <i>table_name</i>
AWS::Lambda::Function	arn: <i>partition</i> :lambda: <i>region</i> : <i>account_ID</i> : <i>function</i> : <i>function_name</i>
AWS::S3::Object <sup>2</sup>	arn: <i>partition</i> :s3:: <i>bucket_name</i> / arn: <i>partition</i> :s3:: <i>bucket_name</i> / <i>object_or_file_name</i> /
AWS::AppConfig::Configuration	arn: <i>partition</i> :appconfi g: <i>region</i> : <i>account_ID</i> :applicat ion/ <i>application_ID</i> /environm ent/ <i>environment_ID</i> /configur ation/ <i>configuration_profile_ID</i>
AWS::B2BI::Transformer	arn: <i>partition</i> :b2bi: <i>region</i> : <i>account_ID</i> : <i>transformer</i> / <i>transformer_ID</i>



resources.type	resources.ARN
AWS::Bedrock::AgentAlias	<pre>arn:<i>partition</i> :bedrock:   <i>region</i>:<i>account_ID</i> :agent-alias/   <i>agent_ID</i>/<i>alias_ID</i></pre>
AWS::Bedrock::KnowledgeBase	<pre>arn:<i>partition</i> :bedrock:   <i>region</i>:<i>account_ID</i> :knowledge-base/   <i>knowledge_base_ID</i></pre>
AWS::Cassandra::Table	<pre>arn:<i>partition</i> :cassandra:   <i>region</i>:<i>account_ID</i> :keyspace/   <i>keyspace_name</i> /table/<i>table_name</i></pre>
AWS::CloudFront::KeyValueStore	<pre>arn:<i>partition</i> :cloudfront:   <i>region</i>:<i>account_ID</i> :key-value-store/   <i>KVS_name</i></pre>
AWS::CloudTrail::Channel	<pre>arn:<i>partition</i> :cloudtrail:   <i>region</i>:<i>account_ID</i> :channel/   <i>channel_UUID</i></pre>
AWS::CodeWhisperer::Customization	<pre>arn:<i>partition</i> :codewhisperer:   <i>region</i>:<i>account_ID</i> :customization/   <i>customization_ID</i></pre>
AWS::CodeWhisperer::Profile	<pre>arn:<i>partition</i> :codewhisperer:   <i>region</i>:<i>account_ID</i> :profile/   <i>profile_ID</i></pre>
AWS::Cognito::IdentityPool	<pre>arn:<i>partition</i> :cognito-identity:   <i>region</i>:<i>account_ID</i> :identity-pool/   <i>identity_pool_ID</i></pre>

resources.type	resources.ARN
AWS::DynamoDB::Stream	arn: <i>partition</i> :dynamodb : <i>region:account_ID</i> :table/ <i>table_name</i> / stream/ <i>date_time</i>
AWS::EC2::Snapshot	arn: <i>partition</i> :ec2: <i>region</i> ::snapsho t/ <i>snapshot_ID</i>
AWS::EMRWALES::Workspace	arn: <i>partition</i> :emrwal: <i>region:account_I</i> <i>D</i> :workspace/ <i>workspace_name</i>
AWS::FinSpace::Environment	arn: <i>partition</i> :finspace : <i>region:account_ID</i> :environm ent/ <i>environment_ID</i>
AWS::Glue::Table	arn: <i>partition</i> :glue: <i>region:account_I</i> <i>D</i> :table/ <i>database_name</i> / <i>table_name</i>
AWS::GreengrassV2::ComponentVersion	arn: <i>partition</i> :greengra ss: <i>region:account_ID</i> :componen ts/ <i>component_name</i>
AWS::GreengrassV2::Deployment	arn: <i>partition</i> :greengra ss: <i>region:account_ID</i> :deployme nts/ <i>deployment_ID</i>
AWS::GuardDuty::Detector	arn: <i>partition</i> :guarddut y: <i>region:account_ID</i> :detector / <i>detector_ID</i>
AWS::IoT::Certificate	arn: <i>partition</i> :iot: <i>region:account_I</i> <i>D</i> :cert/ <i>certificate_ID</i>

resources.type	resources.ARN
AWS::IoT::Thing	<code>arn:partition :iot:region:account_ID :thing/thing_ID</code>
AWS::IoTSiteWise::Asset	<code>arn:partition :iotsitewise: region:account_ID :asset/asset_ID</code>
AWS::IoTSiteWise::TimeSeries	<code>arn:partition :iotsitewise: region:account_ID :timeseries/ timeseries_ID</code>
AWS::IoTTwinMaker::Entity	<code>arn:partition :iottwinmaker: region:account_ID :workspace/ workspace_ID /entity/entity_ID</code>
AWS::IoTTwinMaker::Workspace	<code>arn:partition :iottwinmaker: region:account_ID :workspace/ workspace_ID</code>
AWS::KendraRanking::ExecutionPlan	<code>arn:partition :kendra-ranking: region:account_ID :rescore-execution-plan/ rescore_execution_plan_ID</code>
AWS::Kinesis::Stream	<code>arn:partition :kinesis: region:account_ID :stream/stream_name</code>
AWS::Kinesis::StreamConsumer	<code>arn:partition :kinesis: region:account_ID :stream_type /stream_name /consumer/ consumer_name :consumer_creation_timestamp</code>

resources.type	resources.ARN
AWS::KinesisVideo::Stream	<pre>arn:partition:kinesisvideo:region:account_ID:stream/stream_name/creation_time</pre>
AWS::ManagedBlockchain::Network	<pre>arn:partition:managedblockchain::networks/network_name</pre>
AWS::ManagedBlockchain::Node	<pre>arn:partition:managedblockchain:region:account_ID:nodes/node_ID</pre>
AWS::MedicalImaging::Datastore	<pre>arn:partition:medical-imaging:region:account_ID:datastore/data_store_ID</pre>
AWS::NeptuneGraph::Graph	<pre>arn:partition:neptune-graph:region:account_ID:graph/graph_ID</pre>
AWS::PCACConnectorAD::Connector	<pre>arn:partition:pca-connector-ad:region:account_ID:connector/connector_ID</pre>
AWS::QApps:QApp	<pre>arn:partition:qapps:region:account_ID:application/application_UUID/qapp/qapp_UUID</pre>
AWS::QBusiness::Application	<pre>arn:partition:qbusiness:region:account_ID:application/application_ID</pre>

resources.type	resources.ARN
AWS::QBusiness::DataSource	<pre>arn:partition :qbusines s: region:account_ID :applicat ion/ application_ID /index/index_ID/ data-source/ datasource_ID</pre>
AWS::QBusiness::Index	<pre>arn:partition :qbusines s: region:account_ID :applicat ion/ application_ID /index/index_ID</pre>
AWS::QBusiness::WebExperience	<pre>arn:partition :qbusines s: region:account_ID :applicat ion/ application_ID /web-expe rience/ web_experienc_ID</pre>
AWS::RDS::DBCluster	<pre>arn:partition :rds:region:account_I D :cluster/ cluster_name</pre>
AWS::S3::AccessPoint <sup>3</sup>	<pre>arn:partition :s3:region:account_I D :accesspoint/ access_point_name</pre>
AWS::S3ObjectLambda::AccessPoint	<pre>arn:partition :s3-object-lambda: region:account_ID :accesspo int/ access_point_name</pre>
AWS::S3Outposts::Object	<pre>arn:partition :s3-outpo sts: region:account_ID :object_path</pre>
AWS::SageMaker::Endpoint	<pre>arn:partition :sagemake r: region:account_ID :endpoint / endpoint_name</pre>

resources.type	resources.ARN
AWS::SageMaker::ExperimentTrialComponent	<pre>arn:partition:sagemake r: region:account_ID :experiment- trial-component/ experiment_trial_c omponent_name</pre>
AWS::SageMaker::FeatureGroup	<pre>arn:partition:sagemake r: region:account_ID :feature- group/ feature_group_name</pre>
AWS::SCN::Instance	<pre>arn:partition:scn:region:account_I D :instance/ instance_ID</pre>
AWS::ServiceDiscovery::Namespace	<pre>arn:partition:servicediscovery: region:account_ID :namespac e/ namespace_ID</pre>
AWS::ServiceDiscovery::Service	<pre>arn:partition:servicediscovery: region:account_ID :service/ service_I D</pre>
AWS::SNS::PlatformEndpoint	<pre>arn:partition:sns:region:account_I D :endpoint/ endpoint_type /endpoint_ name /endpoint_ID</pre>
AWS::SNS::Topic	<pre>arn:partition:sns:region:account_I D :topic_name</pre>
AWS::SQS::Queue	<pre>arn:partition:sqs:region:account_I D :queue_name</pre>

resources.type	resources.ARN
AWS::SSM::ManagedNode	<p>Der ARN muss in einem der folgenden Formate vorliegen:</p> <ul style="list-style-type: none"> <li>arn:<i>partition</i> :ssm:<i>region</i>:<i>account_ID</i> :managed-instance/ <i>instance_ID</i></li> <li>arn:<i>partition</i> :ec2:<i>region</i>:<i>account_ID</i> :instance / <i>instance_ID</i></li> </ul>
AWS::SSMMessages::ControlChannel	<pre>arn:<i>partition</i> :ssmmessages:<i>region</i>:<i>account_ID</i> :control-channel/ <i>control_channel_ID</i></pre>
AWS::StepFunctions::StateMachine	<p>Der ARN muss in einem der folgenden Formate vorliegen:</p> <ul style="list-style-type: none"> <li>arn:<i>partition</i> :states:<i>region</i>:<i>account_ID</i> :stateMachine: <i>stateMachine_name</i></li> <li>arn:<i>partition</i> :states:<i>region</i>:<i>account_ID</i> :stateMachine: <i>stateMachine_name</i> /<i>label_name</i></li> </ul>
AWS::SWF::Domain	<pre>arn:<i>partition</i> :swf:<i>region</i>:<i>account_ID</i> :domain/ <i>domain_name</i></pre>
AWS::ThinClient::Device	<pre>arn:<i>partition</i> :thinclient:<i>region</i>:<i>account_ID</i> :device/<i>device_ID</i></pre>

resources.type	resources.ARN
AWS::ThinClient::Environment	arn: <i>partition</i> :thinclient: <i>region</i> : <i>account_ID</i> :environment/ <i>environment_ID</i>
AWS::Timestream::Database	arn: <i>partition</i> :timestream: <i>region</i> : <i>account_ID</i> :database/ <i>database_name</i>
AWS::Timestream::Table	arn: <i>partition</i> :timestream: <i>region</i> : <i>account_ID</i> :database/ <i>database_name</i> /table/ <i>table_name</i>
AWS::VerifiedPermissions::PolicyStore	arn: <i>partition</i> :verifiedpermissions: <i>region</i> : <i>account_ID</i> :policy-store/ <i>policy_store_ID</i>

<sup>1</sup> Bei Tabellen mit aktivierten Streams enthält das resources-Feld im Datenereignis sowohl AWS::DynamoDB::Stream als auch AWS::DynamoDB::Table. Wenn Sie AWS::DynamoDB::Table als resources.type angeben, werden standardmäßig sowohl DynamoDB-Tabellen- als auch DynamoDB-Stream-Ereignisse protokolliert. Um [Streams-Ereignisse](#) auszuschließen, fügen Sie dem eventName Feld einen Filter hinzu.

<sup>2</sup> Um alle Datenereignisse für alle Objekte in einem bestimmten S3-Bucket zu protokollieren, verwenden Sie den StartsWith-Operator und geben Sie nur die Bucket-ARN als übereinstimmenden Wert an. Der abschließende Schrägstrich ist beabsichtigt; schließen Sie ihn nicht aus.


<sup>3</sup> Um Ereignisse zu allen Objekten in einem S3-Zugangspunkt zu protokollieren, empfehlen wir, nur die Zugangspunkt-ARN zu verwenden, den Objektpfad nicht einzuschließen und die StartsWith- oder NotStartsWith-Operatoren oder zu verwenden.



Weitere Informationen zu den ARN-Formaten von Datenereignisressourcen finden Sie unter [Actions, resources, and condition keys](#) (Aktionen, Ressourcen und Bedingungsschlüssel) im AWS Identity and Access Management -Benutzerhandbuch.

- b. Wählen Sie für jedes Feld + Bedingung aus, um beliebig viele Bedingungen hinzuzufügen, bis zu maximal 500 angegebene Werte für alle Bedingungen. Um beispielsweise Datenereignisse für zwei S3-Buckets von Datenereignissen auszuschließen, die in Ihrem Trail protokolliert werden, können Sie das Feld auf Resources.ARN festlegen, den Operator für beginnt nicht mit festlegen und dann entweder einen S3-Bucket-ARN einfügen oder nach den S3-Buckets suchen, für die Sie keine Ereignisse protokollieren möchten.

Um den zweiten S3-Bucket hinzuzufügen, wählen Sie + Bedingung und wiederholen Sie dann die vorherige Anweisung, indem Sie den ARN für einen anderen Bucket einfügen oder nach einem anderen Bucket suchen.

 Note


Sie können maximal 500 Werte für alle Selektoren auf einem Trail haben. Dies schließt Arrays mit mehreren Werten für einen Selektor wie eventName ein. Wenn Sie einzelne Werte für alle Selektoren haben, können Sie einem Selektor maximal 500 Bedingungen hinzufügen.

- c. Wählen Sie + Feld, um bei Bedarf zusätzliche Felder hinzuzufügen. Um Fehler zu vermeiden, legen Sie keine widersprüchlichen oder doppelten Werte für Felder fest. Geben Sie beispielsweise nicht an, dass ein ARN in einem Selektor einem Wert entspricht, und geben Sie dann an, dass der ARN in einem anderen Selektor nicht dem gleichen Wert entspricht.
8. Um einen weiteren Datentyp hinzuzufügen, für den Datenereignisse protokolliert werden sollen, wählen Sie Datenereignistyp hinzufügen. Wiederholen Sie die Schritte 4 bis zu diesem Schritt, um erweiterte Ereignisselektoren für den Datenereignistyp zu konfigurieren.
  9. Nachdem Sie Ihre Auswahl überprüft und bestätigt haben, wählen Sie Änderungen speichern aus.

Aktualisieren Sie einen vorhandenen Trail, um Datenereignisse mit grundlegenden Event-Selektoren in der AWS Management Console


Verwenden Sie das folgende Verfahren, um einen vorhandenen Trail zu aktualisieren und Datenereignisse mit grundlegenden Ereignisselektoren zu protokollieren.

1. Melden Sie sich bei der an AWS Management Console und öffnen Sie die CloudTrail Konsole unter <https://console.aws.amazon.com/cloudtrail/>.
2. Öffnen Sie die Trails-Seite der CloudTrail Konsole und wählen Sie den Namen des Trails aus.

 Note

Sie können zwar einen vorhandenen Trail bearbeiten, um Datenereignisse zu protokollieren, doch es ist eine bewährte Methode, einen separaten Trail speziell für das Protokollieren von Datenereignissen zu erstellen.

3. Wählen Sie für Datenereignisse Bearbeiten aus.
4. Für Amazon-S3-Buckets:
  - a. Wählen Sie für Daten-Ereignisquelle S3 aus.
  - b. Sie können wählen, ob Sie alle aktuellen und zukünftigen S3 Buckets protokollieren oder einzelne Buckets oder Funktionen angeben möchten. Standardmäßig werden Datenereignisse für alle aktuellen und zukünftigen S3 Buckets protokolliert.

 Note

Wenn Sie die Standardoption Alle aktuellen und future S3-Buckets beibehalten, wird die Datenereignisprotokollierung für alle Buckets aktiviert, die sich derzeit in Ihrem AWS Konto befinden, sowie für alle Buckets, die Sie nach Abschluss der Erstellung des Trails erstellen. Es ermöglicht auch die Protokollierung der Datenereignisaktivitäten, die von einem beliebigen Benutzer oder einer Rolle in Ihrem AWS Konto ausgeführt werden, selbst wenn diese Aktivität in einem Bucket ausgeführt wird, der zu einem anderen Konto gehört. AWS

Wenn Sie einen Trail für eine einzelne Region erstellen (mithilfe von AWS CLI), aktivieren Sie durch Auswahl der Option Alle S3-Buckets in Ihrem Konto auswählen die Datenereignisprotokollierung für alle Buckets in derselben Region wie Ihr Trail und für alle Buckets, die Sie später in dieser Region erstellen. Es werden keine

Datenereignisse für Amazon S3 S3-Buckets in anderen Regionen in Ihrem AWS Konto protokolliert.

- c. Wenn Sie die Standardeinstellung Alle aktuellen und zukünftigen S3 Buckets beibehalten, können Sie Leseereignisse, Schreibereignisse oder beides protokollieren.
- d. Um einzelne Buckets auszuwählen, leeren Sie die Kontrollkästchen Lesen und Schreiben für Alle aktuellen und zukünftigen S3 Buckets. Suchen Sie unter Individuelle Bucket-Auswahl nach einem Bucket, in dem Datenereignisse protokolliert werden sollen. Um bestimmte Buckets zu suchen, geben Sie ein Bucket-Präfix für den gewünschten Bucket ein. Sie können in diesem Fenster mehrere Buckets auswählen. Wählen Sie Bucket hinzufügen, um Datenereignisse für weitere Buckets zu protokollieren. Wählen Sie, ob Sie Read (Lesen)-Ereignisse wie `GetObject`, Write (Schreiben)-Ereignisse wie `PutObject` oder Ereignisse beider Typen protokolliert werden sollen.

Diese Einstellung hat Vorrang vor individuellen Einstellungen, die Sie für einzelne Buckets konfigurieren. Wenn Sie beispielsweise die Protokollierung von Lese-Ereignissen für alle S3-Buckets festlegen und dann einen bestimmten Bucket für die Protokollierung von Datenereignissen hinzufügen, ist für den hinzugefügten Bucket bereits Lesen ausgewählt. Sie können die Auswahl nicht löschen. Sie können die Option nur für Write (Schreiben) konfigurieren.

Um einen Bucket aus der Protokollierung zu entfernen, wählen Sie X aus.

5. Um einen weiteren Datentyp hinzuzufügen, für den Datenereignisse protokolliert werden sollen, wählen Sie Datenereignistyp hinzufügen.
6. Für Lambda-Funktionen:
  - a. Wählen Sie für Daten-Ereignisquelle Lambda aus.
  - b. Wählen Sie in der Lambda-Funktion Alle Regionen aus, um alle Lambda-Funktionen zu protokollieren, oder Eingabefunktion als ARN, um Datenereignisse für eine bestimmte Funktion zu protokollieren.

Um Datenereignisse für alle Lambda-Funktionen in Ihrem AWS -Konto zu protokollieren, wählen Sie Log all current and future functions (Alle aktuellen und zukünftigen Funktionen protokollieren). Diese Einstellung hat Vorrang vor individuellen Einstellungen, die Sie für einzelne Funktionen vornehmen. Alle Funktionen werden protokolliert, auch wenn nicht alle Funktionen angezeigt werden.

**Note**

Wenn Sie einen Trail für alle Regionen erstellen, wird durch diese Auswahl die Datenereignisprotokollierung für alle Funktionen aktiviert, die sich derzeit in Ihrem AWS -Konto befinden, sowie für alle Lambda-Funktionen, die Sie ggf. in einer Region erstellen, nachdem Sie den Trail erstellt haben. Wenn Sie einen Trail für eine einzelne Region erstellen (mithilfe von AWS CLI), aktiviert diese Auswahl die Datenereignisprotokollierung für alle Funktionen, die sich derzeit in dieser Region in Ihrem AWS Konto befinden, sowie für alle Lambda-Funktionen, die Sie möglicherweise in dieser Region erstellen, nachdem Sie den Trail erstellt haben. Es wird keine Datenereignisprotokollierung für Lambda-Funktionen aktiviert, die in anderen Regionen erstellt wurden.

Das Protokollieren von Datenereignissen für alle Funktionen ermöglicht auch die Protokollierung von Datenereignisaktivitäten, die von einem beliebigen Benutzer oder einer Rolle in Ihrem AWS Konto ausgeführt werden, selbst wenn diese Aktivität für eine Funktion ausgeführt wird, die zu einem anderen AWS Konto gehört.

- c. Wenn Sie Eingabefunktion als ARN wählen, geben Sie den ARN einer Lambda-Funktion ein.

**Note**

Wenn Sie mehr als 15.000 Lambda-Funktionen in Ihrem Konto haben, können Sie beim Erstellen eines Trails nicht alle Funktionen in der CloudTrail Konsole anzeigen oder auswählen. Sie können weiterhin die Option wählen, alle Funktionen zu protokollieren, auch wenn sie nicht angezeigt werden. Wenn Sie Datenereignisse für bestimmte Funktionen protokollieren möchten, können Sie eine Funktion manuell hinzufügen, wenn Sie deren ARN kennen. Sie können die Erstellung des Trails auch in der Konsole abschließen und dann den Befehl AWS CLI und den `put-event-selectors` Befehl verwenden, um die Datenereignisprotokollierung für bestimmte Lambda-Funktionen zu konfigurieren. Weitere Informationen finden Sie unter [Verwaltung von Wanderwegen mit dem AWS CLI](#).

7. Um einen weiteren Datentyp hinzuzufügen, für den Datenereignisse protokolliert werden sollen, wählen Sie Datenereignistyp hinzufügen.
8. Für DynamoDB-Tabellen:
  - a. Wählen Sie für Daten-Ereignisquelle DynamoDB aus.

- b. Wählen Sie unter DynamoDB table selection (DynamoDB-Tabellenauswahl) die Option Browse (Durchsuchen), um eine Tabelle auszuwählen, oder fügen Sie den ARN einer DynamoDB-Tabelle ein, auf die Sie Zugriff haben. Ein DynamoDB-Tabellen-ARN verwendet das folgende Format:

```
arn:partition:dynamodb:region:account_ID:table/table_name
```

Um eine weitere Tabelle hinzuzufügen, wählen Sie Add row (Zeile hinzufügen) und suchen Sie nach einer Tabelle oder fügen Sie den ARN einer Tabelle ein, auf die Sie Zugriff haben.

9. Wählen Sie Änderungen speichern aus.

## Protokollieren von Datenereignissen mit dem AWS Command Line Interface

Sie können Ihre Trails oder Ereignisdatenspeicher so konfigurieren, dass Datenereignisse per AWS CLI protokolliert werden.

### Themen

- [Protokollierung von Datenereignissen für Trails mit dem AWS CLI](#)
- [Protokollieren von Datenereignissen für Ereignisdatenspeicher mit dem AWS CLI](#)

## Protokollierung von Datenereignissen für Trails mit dem AWS CLI

Sie können Ihre Trails so konfigurieren, dass Verwaltungs- und Datenereignisse mit AWS CLI protokolliert werden.

### Note

- Beachten Sie, dass Sie Gebühren anfallen, wenn Ihr Konto mehr als eine Kopie von Verwaltungsereignissen protokolliert. Für die Protokollierung von Datenereignissen fällt immer eine Gebühr an. Weitere Informationen finden Sie unter [Preise zu AWS CloudTrail](#).
- Sie können entweder erweiterte Ereignisselectoren oder einfache Ereignisselectoren verwenden, aber nicht beide. Wenn Sie erweiterte Ereignisselectoren auf einen Trail anwenden, werden alle vorhandenen grundlegenden Ereignisselectoren überschrieben.
- Wenn Ihr Trail grundlegende Ereignisselectoren verwendet, können Sie nur die folgenden Ressourcentypen protokollieren:

- `AWS::DynamoDB::Table`
- `AWS::Lambda::Function`
- `AWS::S3::Object`

Um zusätzliche Ressourcentypen zu protokollieren, müssen Sie erweiterte Ereignisselectoren verwenden. Um einen Trail in erweiterte Ereignisselectoren umzuwandeln, führen Sie den Befehl `get-event-selectors` aus, um die aktuellen Ereignisselectoren zu bestätigen, und konfigurieren Sie dann die erweiterten Ereignisselectoren so, dass sie der Abdeckung der vorherigen Ereignisselectoren entsprechen. Fügen Sie dann Selectoren für alle Ressourcentypen hinzu, für die Sie Datenereignisse protokollieren möchten.

- Mithilfe erweiterter Ereignisselectoren können Sie nach dem Wert der Felder `eventName`, `resources.ARN` und `readOnly` filtern, sodass Sie nur die Datenereignisse protokollieren, die für Sie von Interesse sind. Weitere Informationen zur Konfiguration dieser Felder finden Sie [AdvancedFieldSelector](#) in der AWS CloudTrail API-Referenz und [Filtern von Datenereignissen mithilfe erweiterter Ereignisselectoren](#) in diesem Thema.

Führen Sie den Befehl [get-event-selectors](#) aus, um anzuzeigen, ob Ihr Trail Verwaltungs- und Datenereignisse protokolliert.

```
aws cloudtrail get-event-selectors --trail-name TrailName
```

Der Befehl gibt die Event-Selectoren für den Trail zurück.

## Themen

- [Protokollieren von Ereignissen mithilfe erweiterter Ereignisselectoren](#)
- [Protokollieren Sie alle Amazon S3 S3-Ereignisse für einen Amazon S3 S3-Bucket mithilfe erweiterter Event-Selectoren](#)
- [Protokollieren von Amazon S3 bei AWS Outposts -Ereignissen mithilfe erweiterter Ereignisselectoren](#)
- [Protokollieren von Ereignissen mithilfe grundlegender Ereignisselectoren](#)

## Protokollieren von Ereignissen mithilfe erweiterter Ereignisselektoren

### Note

Wenn Sie erweiterte Ereignisselektoren auf einen Trail anwenden, werden alle vorhandenen grundlegenden Ereignisselektoren überschrieben. Bevor Sie die erweiterten Ereignisselektoren konfigurieren, führen Sie den Befehl `get-event-selectors` aus, um die aktuellen Ereignisselektoren zu bestätigen. Anschließend konfigurieren Sie die erweiterten Ereignisselektoren so, dass sie der Abdeckung der vorherigen Ereignisselektoren entsprechen, und fügen dann Selektoren für zusätzliche Datenereignisse hinzu, die Sie protokollieren möchten.

Das folgende Beispiel erstellt benutzerdefinierte erweiterte Event-Selektoren für einen Trail, der so benannt ist, *TrailName* dass er Lese- und Schreibverwaltungsereignisse (durch Weglassen des `readOnly` Selektors) `PutObject` und `DeleteObject` Datenereignisse für alle Amazon S3 S3-Bucket/Präfix-Kombinationen mit Ausnahme eines Buckets mit dem Namen `sample_bucket_name` und Datenereignisse für eine Funktion mit dem Namen `MyLambdaFunction` enthält. Da es sich um benutzerdefinierte erweiterte Ereignisselektoren handelt, hat jeder Satz von Selektoren einen beschreibenden Namen. Beachten Sie, dass ein abschließender Schrägstrich Teil des ARN-Werts für S3 Buckets ist.

```
aws cloudtrail put-event-selectors --trail-name TrailName --advanced-event-selectors
'[
  {
    "Name": "Log readOnly and writeOnly management events",
    "FieldSelectors": [
      { "Field": "eventCategory", "Equals": ["Management"] }
    ]
  },
  {
    "Name": "Log PutObject and DeleteObject events for all but one bucket",
    "FieldSelectors": [
      { "Field": "eventCategory", "Equals": ["Data"] },
      { "Field": "resources.type", "Equals": ["AWS::S3::Object"] },
      { "Field": "eventName", "Equals": ["PutObject","DeleteObject"] },
      { "Field": "resources.ARN", "NotStartsWith":
["arn:aws:s3:::sample_bucket_name/"] }
    ]
  },
]
```

```
{
  "Name": "Log data plane actions on MyLambdaFunction",
  "FieldSelectors": [
    { "Field": "eventCategory", "Equals": ["Data"] },
    { "Field": "resources.type", "Equals": ["AWS::Lambda::Function"] },
    { "Field": "resources.ARN", "Equals": ["arn:aws:lambda:us-
east-2:111122223333:function/MyLambdaFunction"] }
  ]
}
]'
```

Das Beispiel gibt die für den Trail konfigurierten fortschrittlichen Ereignisauswahlen zurück.

```
{
  "AdvancedEventSelectors": [
    {
      "Name": "Log readOnly and writeOnly management events",
      "FieldSelectors": [
        {
          "Field": "eventCategory",
          "Equals": [ "Management" ]
        }
      ]
    },
    {
      "Name": "Log PutObject and DeleteObject events for all but one bucket",
      "FieldSelectors": [
        {
          "Field": "eventCategory",
          "Equals": [ "Data" ]
        },
        {
          "Field": "resources.type",
          "Equals": [ "AWS::S3::Object" ]
        },
        {
          "Field": "resources.ARN",
          "NotStartsWith": [ "arn:aws:s3:::sample_bucket_name/" ]
        }
      ]
    }
  ],
  {
    "Name": "Log data plane actions on MyLambdaFunction",
```



```
    "FieldSelectors": [
      {
        "Field": "eventCategory",
        "Equals": [ "Data" ]
      },
      {
        "Field": "resources.type",
        "Equals": [ "AWS::Lambda::Function" ]
      },
      {
        "Field": "eventName",
        "Equals": [ "Invoke" ]
      },
      {
        "Field": "resources.ARN",
        "Equals": [ "arn:aws:lambda:us-east-2:111122223333:function/
MyLambdaFunction" ]
      }
    ]
  },
  "TrailARN": "arn:aws:cloudtrail:us-east-2:123456789012:trail/TrailName"
}
```

Protokollieren Sie alle Amazon S3 S3-Ereignisse für einen Amazon S3 S3-Bucket mithilfe erweiterter Event-Selektoren

#### Note

Wenn Sie erweiterte Ereignisselectoren auf einen Trail anwenden, werden alle vorhandenen grundlegenden Ereignisselectoren überschrieben.

Das folgende Beispiel zeigt, wie Sie Ihren Trail so konfigurieren, dass alle Datenereignisse für alle Amazon-S3-Objekte in einem bestimmten S3 Bucket enthalten sind. Der Wert für S3-Ereignisse für das `resources.type`-Feld ist `AWS::S3::Object`. Da sich die ARN-Werte für S3-Objekte und S3 Buckets geringfügig unterscheiden, müssen Sie den `StartsWith`-Operator für `resources.ARN` hinzufügen, um alle Ereignisse zu erfassen.

```
aws cloudtrail put-event-selectors --trail-name TrailName --region region \  
--advanced-event-selectors \  

```

```
'[
  {
    "Name": "S3EventSelector",
    "FieldSelectors": [
      { "Field": "eventCategory", "Equals": ["Data"] },
      { "Field": "resources.type", "Equals": ["AWS::S3::Object"] },
      { "Field": "resources.ARN", "StartsWith":
["arn:partition:s3:::bucket_name/"] }
    ]
  }
]
```

Der Befehl gibt die folgende Beispielausgabe zurück.

```
{
  "TrailARN": "arn:aws:cloudtrail:region:account_ID:trail/TrailName",
  "AdvancedEventSelectors": [
    {
      "Name": "S3EventSelector",
      "FieldSelectors": [
        {
          "Field": "eventCategory",
          "Equals": [
            "Data"
          ]
        },
        {
          "Field": "resources.type",
          "Equals": [
            "AWS::S3::Object"
          ]
        },
        {
          "Field": "resources.ARN",
          "StartsWith": [
            "arn:partition:s3:::bucket_name/"
          ]
        }
      ]
    }
  ]
}
```

## Protokollieren von Amazon S3 bei AWS Outposts -Ereignissen mithilfe erweiterter Ereignisselektoren

 Note

Wenn Sie erweiterte Ereignisselektoren auf einen Trail anwenden, werden alle vorhandenen grundlegenden Ereignisselektoren überschrieben.

Das folgende Beispiel zeigt, wie Sie Ihren Trail so konfigurieren, dass alle Datenereignisse für alle Amazon S3 on Outposts-Objekte in Ihrem Outpost enthalten sind.

```
aws cloudtrail put-event-selectors --trail-name TrailName --region region \  
--advanced-event-selectors \  
'[  
  {  
    "Name": "OutpostsEventSelector",  
    "FieldSelectors": [  
      { "Field": "eventCategory", "Equals": ["Data"] },  
      { "Field": "resources.type", "Equals": ["AWS::S3Outposts::Object"] }  
    ]  
  }  
]
```

Der Befehl gibt die folgende Beispielausgabe zurück.

```
{  
  "TrailARN": "arn:aws:cloudtrail:region:account_ID:trail/TrailName",  
  "AdvancedEventSelectors": [  
    {  
      "Name": "OutpostsEventSelector",  
      "FieldSelectors": [  
        {  
          "Field": "eventCategory",  
          "Equals": [  
            "Data"  
          ]  
        },  
        {  
          "Field": "resources.type",  
          "Equals": [  
            "AWS::S3Outposts::Object"  
          ]  
        }  
      ]  
    }  
  ]  
}
```

```

    ]
  }
}

```

## Protokollieren von Ereignissen mithilfe grundlegender Ereignisselektoren

Das Folgende ist ein Beispielergebnis des `get-event-selectors`-Befehls, das grundlegende Ereignisselektoren zeigt. Wenn Sie einen Trail mithilfe von erstellen AWS CLI, protokolliert ein Trail standardmäßig alle Verwaltungsereignisse. Standardmäßig protokollieren die Trails keine Datenereignisse.

```

{
  "TrailARN": "arn:aws:cloudtrail:us-east-2:123456789012:trail/TrailName",
  "EventSelectors": [
    {
      "IncludeManagementEvents": true,
      "DataResources": [],
      "ReadWriteType": "All"
    }
  ]
}

```

Führen Sie den Befehl [put-event-selectors](#) aus, um Ihren Trail für die Protokollierung von Verwaltungs- und Datenereignissen zu konfigurieren.

Das folgende Beispiel zeigt, wie Sie grundlegende Ereignisselektoren verwenden, um Ihren Trail so zu konfigurieren, dass er alle Verwaltungs- und Datenereignisse für die S3-Objekte in zwei S3-Bucket-Präfixen enthält. Sie können zwischen 1 und 5 Ereignisselektoren für einen Trail angeben. Sie können zwischen 1 und 250 Datenressourcen für einen Trail festlegen.

### Note

Die maximale Anzahl von S3-Datenressourcen beträgt 250, wenn Sie Datenereignisse mithilfe einfacher Ereignisselektoren begrenzen.

```

aws cloudtrail put-event-selectors --trail-name TrailName --event-selectors
'[{ "ReadWriteType": "All", "IncludeManagementEvents":true, "DataResources":

```

```
[{ "Type": "AWS::S3::Object", "Values": ["arn:aws:s3:::mybucket/prefix",  
"arn:aws:s3:::mybucket2/prefix2"] }] ]'
```

Der Befehl gibt die Ereigniselektoren zurück, die für den Trail konfiguriert sind.

```
{  
  "TrailARN": "arn:aws:cloudtrail:us-east-2:123456789012:trail/TrailName",  
  "EventSelectors": [  
    {  
      "IncludeManagementEvents": true,  
      "DataResources": [  
        {  
          "Values": [  
            "arn:aws:s3:::mybucket/prefix",  
            "arn:aws:s3:::mybucket2/prefix2",  
          ],  
          "Type": "AWS::S3::Object"  
        }  
      ],  
      "ReadWriteType": "All"  
    }  
  ]  
}
```

## Protokollieren von Datenereignissen für Ereignisdatenspeicher mit dem AWS CLI

Sie können Ihre Ereignisdatenspeicher so konfigurieren, dass Datenereignisse per AWS CLI protokolliert werden. Verwenden Sie den Befehl [create-event-data-store](#), um einen neuen Ereignisdatenspeicher zum Protokollieren von Datenereignissen zu erstellen. Verwenden Sie den Befehl [update-event-data-store](#), um die erweiterten Ereigniselektoren für einen vorhandenen Ereignisdatenspeicher zu aktualisieren.

Führen Sie den Befehl [get-event-data-store](#) aus, um zu überprüfen, ob Ihr Ereignisdatenspeicher Datenereignisse enthält.

```
aws cloudtrail get-event-data-store --event-data-store EventDataStoreARN
```

Der Befehl gibt die Einstellungen für den Ereignisdatenspeicher zurück.

```
{  
  "EventDataStoreArn": "arn:aws:cloudtrail:us-east-1:111122223333:eventdatastore/  
EXAMPLE492-301f-4053-ac5e-EXAMPLE6441aa",
```

```
"Name": "ebs-data-events",
>Status": "ENABLED",
>AdvancedEventSelectors": [
>  {
>    "Name": "Log all EBS direct APIs on EBS snapshots",
>    "FieldSelectors": [
>      {
>        "Field": "eventCategory",
>        "Equals": [
>          "Data"
>        ]
>      },
>      {
>        "Field": "resources.type",
>        "Equals": [
>          "AWS::EC2::Snapshot"
>        ]
>      }
>    ]
>  }
> ],
>MultiRegionEnabled": true,
>OrganizationEnabled": false,
>BillingMode": "EXTENDABLE_RETENTION_PRICING",
>RetentionPeriod": 366,
>TerminationProtectionEnabled": true,
>CreatedTimestamp": "2023-11-04T15:57:33.701000+00:00",
>UpdatedTimestamp": "2023-11-20T20:37:34.228000+00:00"
}
```

## Themen

- [Einschließen aller Amazon-S3-Ereignisse für einen Bucket](#)
- [Einschließen von Amazon S3 in AWS Outposts -Ereignissen](#)

### Einschließen aller Amazon-S3-Ereignisse für einen Bucket

Das folgende Beispiel zeigt, wie Sie Ihren Ereignisdatenspeicher so konfigurieren, dass alle Datenereignisse für alle Amazon-S3-Objekte in einem bestimmten S3-Bucket enthalten sind. Der Wert für S3-Ereignisse für das `resources.type`-Feld ist `AWS::S3::Object`. Da sich die ARN-Werte für S3-Objekte und S3 Buckets geringfügig unterscheiden, müssen Sie den `StartsWith`-Operator für `resources.ARN` hinzufügen, um alle Ereignisse zu erfassen.

```
aws cloudtrail create-event-data-store --name "EventDataStoreName" --multi-region-
enabled \
--advanced-event-selectors \
'[
  {
    "Name": "S3EventSelector",
    "FieldSelectors": [
      { "Field": "eventCategory", "Equals": ["Data"] },
      { "Field": "resources.type", "Equals": ["AWS::S3::Object"] },
      { "Field": "resources.ARN", "StartsWith":
["arn:partition:s3:::bucket_name/"] }
    ]
  }
]'
```

Der Befehl gibt die folgende Beispielausgabe zurück.

```
{
  "EventDataStoreArn": "arn:aws:cloudtrail:us-east-1:111122223333:eventdatastore/
EXAMPLE492-301f-4053-ac5e-EXAMPLE441aa",
  "Name": "EventDataStoreName",
  "Status": "ENABLED",
  "AdvancedEventSelectors": [
    {
      "Name": "S3EventSelector",
      "FieldSelectors": [
        {
          "Field": "eventCategory",
          "Equals": [
            "Data"
          ]
        },
        {
          "Field": "resources.ARN",
          "StartsWith": [
            "arn:partition:s3:::bucket_name/"
          ]
        },
        {
          "Field": "resources.type",
          "Equals": [
            "AWS::S3::Object"
          ]
        }
      ]
    }
  ]
}
```

```

    }
  ]
}
],
"MultiRegionEnabled": true,
"OrganizationEnabled": false,
"BillingMode": "EXTENDABLE_RETENTION_PRICING",
"RetentionPeriod": 366,
"TerminationProtectionEnabled": true,
"CreatedTimestamp": "2023-11-04T15:57:33.701000+00:00",
"UpdatedTimestamp": "2023-11-20T20:49:21.766000+00:00"
}

```

## Einschließen von Amazon S3 in AWS Outposts -Ereignissen

Das folgende Beispiel zeigt, wie Sie Ihren Ereignisdatenspeicher so konfigurieren, dass alle Datenereignisse für alle Objekte von Amazon S3 on Outposts in Ihrem Outpost enthalten sind.

```

aws cloudtrail create-event-data-store --name EventDataStoreName \
--advanced-event-selectors \
'[
  {
    "Name": "OutpostsEventSelector",
    "FieldSelectors": [
      { "Field": "eventCategory", "Equals": ["Data"] },
      { "Field": "resources.type", "Equals": ["AWS::S3outposts::Object"] }
    ]
  }
]'

```

Der Befehl gibt die folgende Beispielausgabe zurück.

```

{
  "EventDataStoreArn": "arn:aws:cloudtrail:us-east-1:111122223333:eventdatastore/
EXAMPLEb4a8-99b1-4ec2-9258-EXAMPLEc890",
  "Name": "EventDataStoreName",
  "Status": "CREATED",
  "AdvancedEventSelectors": [
    {
      "Name": "OutpostsEventSelector",
      "FieldSelectors": [
        {
          "Field": "eventCategory",

```



```

        "Equals": [
            "Data"
        ]
    },
    {
        "Field": "resources.type",
        "Equals": [
            "AWS::S3outposts::Object"
        ]
    }
]
}
],
"MultiRegionEnabled": true,
"OrganizationEnabled": false,
"BillingMode": "EXTENDABLE_RETENTION_PRICING",
"RetentionPeriod": 366,
"TerminationProtectionEnabled": true,
"CreatedTimestamp": "2023-02-20T21:00:17.673000+00:00",
"UpdatedTimestamp": "2023-02-20T21:00:17.820000+00:00"
}

```

## Filtern von Datenereignissen mithilfe erweiterter Ereignisselektoren

In diesem Abschnitt wird beschrieben, wie Sie erweiterte Ereignisselektoren verwenden können, um detaillierte Selektoren zu erstellen, die Ihnen helfen, die Kosten zu kontrollieren, indem nur die spezifischen Datenereignisse protokolliert werden, die für Sie von Interesse sind.

Beispielsweise:

- Sie können bestimmte API-Aufrufe ein- oder ausschließen, indem Sie dem Feld einen Filter hinzufügen. `eventName`
- Sie können die Protokollierung für bestimmte Ressourcen ein- oder ausschließen, indem Sie dem `resources.ARN` Feld einen Filter hinzufügen. Wenn Sie beispielsweise S3-Datenereignisse protokollieren, könnten Sie die Protokollierung für den S3-Bucket für Ihren Trail ausschließen.
- Sie können wählen, ob nur Schreibereignisse oder schreibgeschützte Ereignisse protokolliert werden sollen, indem Sie dem Feld einen Filter hinzufügen. `readOnly`

Die folgende Tabelle enthält zusätzliche Informationen zu den konfigurierbaren Feldern für erweiterte Ereignisselektoren.

Feld	Erforderlich	Gültige Operatoren	Beschreibung
<b>eventCategory</b>	Ja	Equals	Dieses Feld ist so eingestellt, dass Data Datenergebnisse protokolliert werden.
<b>resources.type</b>	Ja	Equals	Dieses Feld wird verwendet, um den Ressourcentyp auszuwählen, für den Sie Datenergebnisse protokollieren möchten. Die Tabelle mit <a href="#">Datenergebnissen</a> zeigt die möglichen Werte.
<b>readOnly</b>	Nein	Equals	Dies ist ein optionales Feld, das verwendet wird, um Datenergebnisse basierend auf dem readOnly Wert ein- oder auszuschließen. Der Wert true protokolliert nur Leseereignisse. Der Wert false protokolliert nur Schreiberereignisse. Wenn Sie dieses Feld nicht hinzufügen, werden sowohl Lese- als auch Schreiberereignisse CloudTrail protokolliert.
<b>eventName</b>	Nein	Any	<p>Dies ist ein optionales Feld, das verwendet wird, um jedes Datenergebnis, bei dem protokolliert wurde, ein- oder herauszufiltern CloudTrail, z. B. PutBucket oder. GetSnapshotBlock</p> <p>Wenn Sie den verwenden AWS CLI, können Sie mehrere Werte angeben, indem Sie jeden Wert durch ein Komma trennen.</p> <p>Wenn Sie die Konsole verwenden, können Sie mehrere Werte angeben, indem Sie für jeden Wert, nach dem eventName Sie filtern möchten, eine Bedingung erstellen.</p>

Feld	Erforderlich	Gültige Operatoren	Beschreibung
<b>resources.ARN</b>	Nein	Any	<p>Dies ist ein optionales Feld, das verwendet wird, um Datenereignisse für eine bestimmte Ressource auszuschließen oder einzuschließen, indem Sie die angeben <code>resources.ARN</code>. Sie können jeden Operator mit verwenden <code>resources.ARN</code>, aber wenn Sie <code>Equals</code> oder verwenden <code>NotEquals</code>, muss der Wert genau dem ARN einer gültigen Ressource für die von <code>resources.type</code> Ihnen angegebene Ressource entsprechen.</p> <p>Wenn Sie den verwenden AWS CLI, können Sie mehrere Werte angeben, indem Sie jeden Wert durch ein Komma trennen.</p> <p>Wenn Sie die Konsole verwenden, können Sie mehrere Werte angeben, indem Sie für jeden Wert, nach dem <code>resources.ARN</code> Sie filtern möchten, eine Bedingung erstellen.</p>

Um Datenereignisse mithilfe der CloudTrail Konsole zu protokollieren, wählen Sie die Option Datenereignisse und dann den gewünschten Datenereignistyp aus, wenn Sie einen Trail- oder Event-Datenspeicher erstellen oder aktualisieren. In der Tabelle mit [Datenereignissen](#) werden die möglichen Datenereignistypen aufgeführt, die Sie auf der CloudTrail Konsole auswählen können.

### Data events Info

Data events show information about the resource operations performed on or within a resource. [Additional charges apply](#)

ⓘ **Advanced event selectors are enabled**
Switch to basic event selectors

Use the following fields for fine-grained control over the data events captured by your trail.

**▼ Data event: SNS topic** Remove

**Data event type**  
Choose the source of data events to log.

SNS topic
▼

**Log selector template**

Log all events
▼

**Selector name - optional**

Log all data events on SNS topics

1,000 character limit

**► JSON view**

Add data event type

Um Datenereignisse mit dem zu protokollieren AWS CLI, konfigurieren Sie den `--advanced-event-selector` Parameter so, dass er `eventCategory` gleich `Data` und der `resources.type` Wert gleich dem Ressourcentypwert ist, für den Sie Datenereignisse protokollieren möchten. In der Tabelle mit [Datenereignissen](#) sind die verfügbaren Ressourcentypen aufgeführt.

Wenn Sie beispielsweise Datenereignisse für alle Cognito Identity-Pools protokollieren möchten, konfigurieren Sie den `--advanced-event-selectors` Parameter so, dass er wie folgt aussieht:

```
--advanced-event-selectors '[
  {
    "Name": "Log Cognito data events on Identity pools",
    "FieldSelectors": [
      { "Field": "eventCategory", "Equals": ["Data"] },
      { "Field": "resources.type", "Equals": ["AWS::Cognito::IdentityPool"] }
    ]
  }
]'
```

Im vorherigen Beispiel werden alle Cognito-Datenereignisse in Identitätspools protokolliert. Sie können die erweiterten Ereignisauswahlen weiter verfeinern, um nach den `resources.ARN` FelderneventName, und zu `filterReadOnly`, um bestimmte Ereignisse von Interesse zu protokollieren oder Ereignisse auszuschließen, die nicht von Interesse sind.

Sie können erweiterte Ereignisauswahlen konfigurieren, um Datenereignisse auf der Grundlage mehrerer Bedingungen zu filtern. Sie können beispielsweise erweiterte Event-Selektoren so konfigurieren, dass sie alle Amazon S3 PutObject - und DeleteObject API-Aufrufe protokollieren, aber die Ereignisprotokollierung für einen bestimmten S3-Bucket ausschließen, wie im folgenden Beispiel gezeigt.

```
--advanced-event-selectors
'[
  {
    "Name": "Log PutObject and DeleteObject events for all but one bucket",
    "FieldSelectors": [
      { "Field": "eventCategory", "Equals": ["Data"] },
      { "Field": "resources.type", "Equals": ["AWS::S3::Object"] },
      { "Field": "eventName", "Equals": ["PutObject","DeleteObject"] },
      { "Field": "resources.ARN", "NotStartsWith":
["arn:aws:s3:::sample_bucket_name/"] }
    ]
  }
]'
```

Sie können erweiterte Event-Selektoren verwenden, um sowohl Verwaltungs- als auch Datenereignisse zu protokollieren. Um Datenereignisse für mehrere Ressourcentypen zu protokollieren, fügen Sie für jeden Ressourcentyp, für den Sie Datenereignisse protokollieren möchten, eine Feldauswahlweisung hinzu.

#### Note

Für Trails können entweder einfache oder erweiterte Event-Selektoren verwendet werden, aber nicht beide. Wenn Sie erweiterte Ereignisselektoren auf einen Trail anwenden, werden alle vorhandenen grundlegenden Ereignisselektoren überschrieben.

## Themen

- [Filterung von Datenereignissen nach eventName](#)
- [Filtern von Datenereignissen nach resources.ARN](#)
- [Datenereignisse nach readOnly Wert filtern](#)

## Filterung von Datenereignissen nach **eventName**

Mithilfe erweiterter Event-Selektoren können Sie Ereignisse basierend auf dem Wert des `eventName` Felds ein- oder ausschließen. Das Filtern nach `eventName` kann helfen, die Kosten zu kontrollieren, da Sie vermeiden, dass Kosten entstehen, wenn AWS-Service Sie Datenereignisse protokollieren, um Unterstützung für neue Daten-APIs hinzuzufügen.

Sie können einen beliebigen Operator für das `eventName` Feld verwenden. Sie können ihn verwenden, um jedes Datenereignis, bei dem protokolliert wurde, ein- oder herauszufiltern CloudTrail, z. B. `PutBucket` oder `GetSnapshotBlock`

### Themen

- [Filtern von Datenereignissen mithilfe der `eventName`AWS Management Console](#)
- [Filtern von Datenereignissen `eventName` mithilfe von AWS CLI](#)

### Filtern von Datenereignissen mithilfe der **eventName**AWS Management Console

Gehen Sie wie folgt vor, um das `eventName` Feld mithilfe der CloudTrail Konsole zu filtern.

1. Folgen Sie den Schritten im Verfahren zum [Erstellen von Pfaden](#) oder folgen Sie den Schritten im Verfahren zum [Erstellen eines Ereignisdatenspeichers](#).
2. Wenn Sie den Schritten zum Erstellen des Trail- oder Event-Datenspeichers folgen, treffen Sie die folgenden Auswahlen:
  - a. Wählen Sie Datenereignisse aus.
  - b. Wählen Sie den Datenereignistyp, für den Sie Datenereignisse protokollieren möchten.
  - c. Wählen Sie für die Protokollauswahlvorlage die Option Benutzerdefiniert aus.
  - d. (Optional) Geben Sie unter Selektorname einen Namen ein, um Ihre Auswahl zu identifizieren. Der Selektorname ist ein optionaler, beschreibender Name für eine erweiterte Ereignisauswahl, z. B. „Datenereignisse nur für zwei S3-Buckets protokollieren“. Der Name des Selektors wird als Name in der erweiterten Ereignisauswahl aufgeführt und ist sichtbar, wenn Sie die JSON-Ansicht erweitern.
  - e. Gehen Sie unter Erweiterte Event-Selektoren wie folgt vor, um nach folgenden Kriterien zu filtern: `eventName`
    - i. Wählen Sie für Feld die Option `eventName` aus.

- ii. Wählen Sie für Operator den Bedingungsoperator aus. In diesem Beispiel wählen wir Equals, weil wir einen bestimmten API-Aufruf protokollieren möchten.
- iii. Geben Sie unter Value den Namen des Ereignisses ein, nach dem Sie filtern möchten.
- iv. Um nach einem anderen zu filtern eventName, wählen Sie + Bedingung.

**Data events** [Info](#)  
Data events show information about the resource operations performed on or within a resource.

▼ Data event: S3 Remove

**Data event type**  
Choose the source of data events to log.  
S3

**Log selector template**  
Custom

**Selector name - optional**  
Log S3 PutObject and DeleteObject API calls  
1,000 character limit

**Collect events**  
Log all events, or choose a template to log specific, filtered events to your trail. You can edit templates later.

**Advanced event selectors** [Info](#)  
Log or exclude events from specific resources.

Field	Operator	Value	
eventName	equals	PutObject	×
OR			
eventName	equals	DeleteObject	×

+ Field      + Condition

► JSON view

[Add data event type](#)

- f. Wählen Sie +Feld, um Filter für andere Felder hinzuzufügen.

## Filtern von Datenereignissen **eventName** mithilfe von AWS CLI

Mithilfe von können Sie nach dem eventName Feld filtern, um bestimmte Ereignisse ein- oder auszuschließen. AWS CLI

Im folgenden Beispiel werden S3-Datenereignisse in einem Trail protokolliert. Sie --advanced-event-selectors sind so konfiguriert, dass sie nur Datenereignisse für die DeleteObject API-Aufrufe GetObjectPutObject, und protokollieren.

```
aws cloudtrail put-event-selectors \
--trail-name trailName \
```

```
--advanced-event-selectors '[
  {
    "Name": "Log GetObject, PutObject and DeleteObject S3 data events",
    "FieldSelectors": [
      { "Field": "eventCategory", "Equals": ["Data"] },
      { "Field": "resources.type", "Equals": ["AWS::S3::Object"] },
      { "Field": "eventName", "Equals": ["GetObject","PutObject","DeleteObject"] }
    ]
  }
]'
```

Im nächsten Beispiel wird ein neuer Ereignisdatenspeicher erstellt, der Datenereignisse für EBS Direct-APIs protokolliert, ListChangedBlocks API-Aufrufe jedoch ausschließt. Sie können den [update-event-data-store](#) Befehl verwenden, um einen vorhandenen Ereignisdatenspeicher zu aktualisieren.

```
aws cloudtrail create-event-data-store \
--name "eventDataStoreName"
--advanced-event-selectors '[
  {
    "Name": "Log all EBS Direct API data events except ListChangedBlocks",
    "FieldSelectors": [
      { "Field": "eventCategory", "Equals": ["Data"] },
      { "Field": "resources.type", "Equals": ["AWS::EC2::Snapshot"] },
      { "Field": "eventName", "NotEquals": ["ListChangedBlocks"] }
    ]
  }
]'
```

## Filtern von Datenereignissen nach **resources.ARN**

Mithilfe erweiterter Event-Selektoren können Sie nach dem Wert des `resources.ARN` Felds filtern.

Sie können jeden Operator mit `resources.ARN` verwenden, aber wenn Sie `Equals` oder `NotEquals` verwenden, muss der Wert genau dem ARN einer gültigen Ressource für den von Ihnen angegebenen `resources.type` Wert entsprechen. Um alle Datenereignisse für alle Objekte in einem bestimmten S3-Bucket zu protokollieren, verwenden Sie den `StartsWith`-Operator und geben nur den Bucket-ARN als übereinstimmenden Wert an.

In der folgenden Tabelle wird das gültige ARN-Format für alle `resources.type`-Werte aufgeführt.



**Note**

Sie können das `resources.ARN` Feld nicht verwenden, um Ressourcentypen zu filtern, die keine ARNs haben.

resources.type	resources.ARN
AWS::DynamoDB::Table <sup>1</sup>	<code>arn:partition:dynamodb: :region:account_ID:table/table_name</code>
AWS::Lambda::Function	<code>arn:partition:lambda:region:account_I D:function: function_name</code>
AWS::S3::Object <sup>2</sup>	<code>arn:partition:s3::bucket_name / arn:partition:s3::bucket_na me /object_or_file_name /</code>
AWS::AppConfig::Configuration	<code>arn:partition:appconfi g: region:account_ID :applicat ion/ application_ID /environm ent/ environment_ID /configur ation/ configuration_profile_ID</code>
AWS::B2BI::Transformer	<code>arn:partition:b2bi:region:account_I D:transformer/ transformer_ID</code>
AWS::Bedrock::AgentAlias	<code>arn:partition:bedrock: region:account_ID :agent-al ias/ agent_ID/alias_ID</code>
AWS::Bedrock::KnowledgeBase	<code>arn:partition:bedrock: region:account_ID :knowledge- base/knowledge_base_ID</code>

resources.type	resources.ARN
AWS::Cassandra::Table	<pre>arn:partition :cassandr a: region:account_ID :keyspace / keyspace_name /table/table_name</pre>
AWS::CloudFront::KeyValueStore	<pre>arn:partition :cloudfro nt: region:account_ID :key-value- store/KVS_name</pre>
AWS::CloudTrail::Channel	<pre>arn:partition :cloudtra il: region:account_ID :channel/ channel_UUID</pre>
AWS::CodeWhisperer::Customization	<pre>arn:partition :codewhis perer: region:account_ID :customiz ation/ customization_ID</pre>
AWS::CodeWhisperer::Profile	<pre>arn:partition :codewhis perer: region:account_ID :profile/ profile_ID</pre>
AWS::Cognito::IdentityPool	<pre>arn:partition :cognito-identity: region:account_ID :identity pool/ identity_pool_ID</pre>
AWS::DynamoDB::Stream	<pre>arn:partition :dynamodb : region:account_ID :table/table_name / stream/date_time</pre>
AWS::EC2::Snapshot	<pre>arn:partition :ec2:region::snapsho t/ snapshot_ID</pre>

resources.type	resources.ARN
AWS::EMRWAL::Workspace	arn: <i>partition</i> :emrwal: <i>region</i> : <i>account_ID</i> :workspace/ <i>workspace_name</i>
AWS::FinSpace::Environment	arn: <i>partition</i> :finspace : <i>region</i> : <i>account_ID</i> :environment/ <i>environment_ID</i>
AWS::Glue::Table	arn: <i>partition</i> :glue: <i>region</i> : <i>account_ID</i> :table/ <i>database_name</i> / <i>table_name</i>
AWS::GreengrassV2::ComponentVersion	arn: <i>partition</i> :greengrass: <i>region</i> : <i>account_ID</i> :components/ <i>component_name</i>
AWS::GreengrassV2::Deployment	arn: <i>partition</i> :greengrass: <i>region</i> : <i>account_ID</i> :deployments/ <i>deployment_ID</i>
AWS::GuardDuty::Detector	arn: <i>partition</i> :guardduty: <i>region</i> : <i>account_ID</i> :detector / <i>detector_ID</i>
AWS::IoT::Certificate	arn: <i>partition</i> :iot: <i>region</i> : <i>account_ID</i> :cert/ <i>certificate_ID</i>
AWS::IoT::Thing	arn: <i>partition</i> :iot: <i>region</i> : <i>account_ID</i> :thing/ <i>thing_ID</i>
AWS::IoTSiteWise::Asset	arn: <i>partition</i> :iotsitewise: <i>region</i> : <i>account_ID</i> :asset/ <i>asset_ID</i>

resources.type	resources.ARN
AWS::IoTSiteWise::TimeSeries	<pre>arn:<i>partition</i> :iotsitew ise: <i>region:account_ID</i> :timeseri es/ <i>timeseries_ID</i></pre>
AWS::IoTTwinMaker::Entity	<pre>arn:<i>partition</i> :iottwinm aker: <i>region:account_ID</i> :workspac e/ <i>workspace_ID</i> /entity/<i>entity_ID</i></pre>
AWS::IoTTwinMaker::Workspace	<pre>arn:<i>partition</i> :iottwinm aker: <i>region:account_ID</i> :workspac e/ <i>workspace_ID</i></pre>
AWS::KendraRanking::ExecutionPlan	<pre>arn:<i>partition</i> :kendra-r anking: <i>region:account_ID</i> :rescore- execution-plan/ <i>rescore_execution_ plan_ID</i></pre>
AWS::Kinesis::Stream	<pre>arn:<i>partition</i> :kinesis: <i>region:account_ID</i> :stream/<i>stream_name</i></pre>
AWS::Kinesis::StreamConsumer	<pre>arn:<i>partition</i> :kinesis: <i>region:account_ID</i> :stream_ty pe /<i>stream_name</i> /consumer/ <i>consumer_ name</i> :<i>consumer_creation_timestamp</i></pre>
AWS::KinesisVideo::Stream	<pre>arn:<i>partition</i> :kinesisv ideo: <i>region:account_I D</i> :stream/<i>stream_name</i> /<i>creation_time</i></pre>
AWS::ManagedBlockchain::Network	<pre>arn:<i>partition</i> :managedblockchain :::networks/ <i>network_name</i></pre>

resources.type	resources.ARN
AWS::ManagedBlockchain::Node	arn: <i>partition</i> :managedblockchain : <i>region</i> : <i>account_ID</i> :nodes/ <i>node_ID</i>
AWS::MedicalImaging::Datastore	arn: <i>partition</i> :medical-imaging: <i>region</i> : <i>account_ID</i> :datastore/ <i>data_store_ID</i>
AWS::NeptuneGraph::Graph	arn: <i>partition</i> :neptune-graph: <i>region</i> : <i>account_ID</i> :graph/ <i>graph_ID</i>
AWS::PCAConectorAD::Connector	arn: <i>partition</i> :pca-connector-ad: <i>region</i> : <i>account_ID</i> :connector/ <i>connector_ID</i>
AWS::QApps:QApp	arn: <i>partition</i> :qapps: <i>region</i> : <i>account_ID</i> :application/ <i>application_UUID</i> /qapp/ <i>qapp_UUID</i>
AWS::QBusiness::Application	arn: <i>partition</i> :qbusines s: <i>region</i> : <i>account_ID</i> :application/ <i>application_ID</i>
AWS::QBusiness::DataSource	arn: <i>partition</i> :qbusines s: <i>region</i> : <i>account_ID</i> :application/ <i>application_ID</i> /index/ <i>index_ID</i> /data-source/ <i>datasource_ID</i>
AWS::QBusiness::Index	arn: <i>partition</i> :qbusines s: <i>region</i> : <i>account_ID</i> :application/ <i>application_ID</i> /index/ <i>index_ID</i>

resources.type	resources.ARN
AWS::QBusiness::WebExperience	arn: <i>partition</i> :qbusines s: <i>region:account_ID</i> :applicat ion/ <i>application_ID</i> /web-expe rience/ <i>web_experienc_ID</i>
AWS::RDS::DBCluster	arn: <i>partition</i> :rds: <i>region:account_I D</i> :cluster/ <i>cluster_name</i>
AWS::S3::AccessPoint <sup>3</sup>	arn: <i>partition</i> :s3: <i>region:account_I D</i> :accesspoint/ <i>access_point_name</i>
AWS::S3ObjectLambda::AccessPoint	arn: <i>partition</i> :s3-object-lambda: <i>region:account_ID</i> :accesspo int/ <i>access_point_name</i>
AWS::S3Outposts::Object	arn: <i>partition</i> :s3-outpo sts: <i>region:account_ID</i> :object_path
AWS::SageMaker::Endpoint	arn: <i>partition</i> :sagemake r: <i>region:account_ID</i> :endpoint / <i>endpoint_name</i>
AWS::SageMaker::ExperimentT rialComponent	arn: <i>partition</i> :sagemake r: <i>region:account_ID</i> :experiment- trial-component/ <i>experiment_trial_c omponent_name</i>
AWS::SageMaker::FeatureGroup	arn: <i>partition</i> :sagemake r: <i>region:account_ID</i> :feature- group/ <i>feature_group_name</i>

resources.type	resources.ARN
AWS::SCN::Instance	<pre>arn:partition :scn:region:account_ID :instance/ instance_ID</pre>
AWS::ServiceDiscovery::Namespace	<pre>arn:partition :servicediscovery:region:account_ID :namespace/ namespace_ID</pre>
AWS::ServiceDiscovery::Service	<pre>arn:partition :servicediscovery:region:account_ID :service/ service_ID</pre>
AWS::SNS::PlatformEndpoint	<pre>arn:partition :sns:region:account_ID :endpoint/ endpoint_type /endpoint_name /endpoint_ID</pre>
AWS::SNS::Topic	<pre>arn:partition :sns:region:account_ID :topic_name</pre>
AWS::SQS::Queue	<pre>arn:partition :sqs:region:account_ID :queue_name</pre>
AWS::SSM::ManagedNode	<p>Der ARN muss in einem der folgenden Formate vorliegen:</p> <ul style="list-style-type: none"> <li>• <code>arn:partition :ssm:region:account_ID :managed-instance/ instance_ID</code></li> <li>• <code>arn:partition :ec2:region:account_ID :instance / instance_ID</code></li> </ul>

resources.type	resources.ARN
AWS::SSMMessages::ControlChannel	<pre>arn:partition :ssmmessage: region:account_ID :control- channel/ control_channel_ID</pre>
AWS::StepFunctions::StateMachine	<p>Der ARN muss in einem der folgenden Formate vorliegen:</p> <ul style="list-style-type: none"> <li>• arn:partition :states:region:account_ID :stateMachine: stateMachine_name</li> <li>• arn:partition :states:region:account_ID :stateMachine: stateMachine_name /label_name</li> </ul>
AWS::SWF::Domain	<pre>arn:partition :swf:region:account_ID :/ domain/ domain_name</pre>
AWS::ThinClient::Device	<pre>arn:partition :thinclient: region:account_ID :device/device_ID</pre>
AWS::ThinClient::Environment	<pre>arn:partition :thinclient: region:account_ID :environment/ environment_ID</pre>
AWS::Timestream::Database	<pre>arn:partition :timestream: region:account_ID :database / database_name</pre>



resources.type	resources.ARN
AWS::Timestream::Table	arn: <i>partition</i> :timestream: am: <i>region:account_ID</i> :database / <i>database_name</i> /table/ <i>table_name</i>
AWS::VerifiedPermissions::PolicyStore	arn: <i>partition</i> :verifiedpermissions: ns: <i>region:account_ID</i> :policy-store/ <i>policy_store_ID</i>

<sup>1</sup> Bei Tabellen mit aktivierten Streams enthält das `resources`-Feld im Datenereignis sowohl `AWS::DynamoDB::Stream` als auch `AWS::DynamoDB::Table`. Wenn Sie `AWS::DynamoDB::Table` als `resources.type` angeben, werden standardmäßig sowohl DynamoDB-Tabellen- als auch DynamoDB-Stream-Ereignisse protokolliert. Um [Streams-Ereignisse](#) auszuschließen, fügen Sie dem `eventName` Feld einen Filter hinzu.

<sup>2</sup> Um alle Datenereignisse für alle Objekte in einem bestimmten S3-Bucket zu protokollieren, verwenden Sie den `StartsWith`-Operator und geben Sie nur die Bucket-ARN als übereinstimmenden Wert an. Der abschließende Schrägstrich ist beabsichtigt; schließen Sie ihn nicht aus.

<sup>3</sup> Um Ereignisse zu allen Objekten in einem S3-Zugangspunkt zu protokollieren, empfehlen wir, nur die Zugangspunkt-ARN zu verwenden, den Objektpfad nicht einzuschließen und die `StartsWith`- oder `NotStartsWith`-Operatoren oder zu verwenden.

## Themen

- [Filtern von Datenereignissen resources.ARN mithilfe von AWS Management Console](#)
- [Filtern von Datenereignissen resources.ARN mithilfe von AWS CLI](#)

## Filtern von Datenereignissen **resources.ARN** mithilfe von AWS Management Console

Gehen Sie wie folgt vor, um das `resources.ARN` Feld mithilfe der CloudTrail Konsole zu filtern.

1. Folgen Sie den Schritten im Verfahren zum [Erstellen von Pfaden](#) oder folgen Sie den Schritten im Verfahren zum [Erstellen eines Ereignisdatenspeichers](#).

2. Wenn Sie den Schritten zum Erstellen des Trail- oder Event-Datenspeichers folgen, treffen Sie die folgenden Auswahlen:
  - a. Wählen Sie Datenereignisse aus.
  - b. Wählen Sie den Datenereignistyp, für den Sie Datenereignisse protokollieren möchten.
  - c. Wählen Sie für die Protokollauswahlvorlage die Option Benutzerdefiniert aus.
  - d. (Optional) Geben Sie unter Selektorname einen Namen ein, um Ihre Auswahl zu identifizieren. Der Selektorname ist ein optionaler, beschreibender Name für eine erweiterte Ereignisauswahl, z. B. „Datenereignisse nur für zwei S3-Buckets protokollieren“. Der Name des Selektors wird als Name in der erweiterten Ereignisauswahl aufgeführt und ist sichtbar, wenn Sie die JSON-Ansicht erweitern.
  - e. Gehen Sie unter Erweiterte Event-Selektoren wie folgt vor, um nach folgenden Kriterien zu filtern: `resources.ARN`
    - i. Wählen Sie für Feld `resources.ARN` aus.
    - ii. Wählen Sie unter Operator den Bedingungsoperator aus. In diesem Beispiel wählen wir `starts with`, weil wir Datenereignisse für einen bestimmten S3-Bucket protokollieren möchten.
    - iii. Geben Sie unter Value den ARN für Ihren Ressourcentyp ein (z. B. `arn:aws:s3:::bucket-name`).
    - iv. Um einen anderen zu filtern, wählen Sie + Bedingung. **`resources.ARN`**

**Data events** [Info](#)  
Data events show information about the resource operations performed on or within a resource.

▼ **Data event: S3** Remove

**Data event type**  
Choose the source of data events to log.  
S3

**Log selector template**  
Custom

**Selector name - optional**  
Log S3 data events for a specific bucket  
1,000 character limit

**Collect events**  
Log all events, or choose a template to log specific, filtered events to your trail. You can edit templates later.

**Advanced event selectors** [Info](#)  
Log or exclude events from specific resources.

Field	Operator	Value
resources.ARN	starts with	arn:aws:s3:::bucket-name

+ Field      + Condition

► **JSON view**

Add data event type

f. Wählen Sie +Feld, um Filter für andere Felder hinzuzufügen.

## Filtern von Datenereignissen **resources.ARN** mithilfe von AWS CLI

Mithilfe von können Sie nach dem `resources.ARN` Feld filtern AWS CLI, um Ereignisse für einen bestimmten ARN zu protokollieren oder die Protokollierung für einen bestimmten ARN auszuschließen.

Das folgende Beispiel zeigt, wie Sie Ihren Trail so konfigurieren, dass alle Datenereignisse für alle Amazon-S3-Objekte in einem bestimmten S3 Bucket enthalten sind. Der Wert für S3-Ereignisse für das `resources.type`-Feld ist `AWS::S3::Object`. Da sich die ARN-Werte für S3-Objekte und S3 Buckets geringfügig unterscheiden, müssen Sie den `StartsWith`-Operator für `resources.ARN` hinzufügen, um alle Ereignisse zu erfassen.

```
aws cloudtrail put-event-selectors \
--trail-name TrailName \
--region region \
--advanced-event-selectors \
'[
```

```
{
  "Name": "S3EventSelector",
  "FieldSelectors": [
    { "Field": "eventCategory", "Equals": ["Data"] },
    { "Field": "resources.type", "Equals": ["AWS::S3::Object"] },
    { "Field": "resources.ARN", "StartsWith":
["arn:aws:s3:::bucket_name/"] }
  ]
}
```

## Datenereignisse nach **readOnly** Wert filtern

Mithilfe erweiterter Event-Selektoren können Sie basierend auf dem Wert des `readOnly` Felds filtern.

Sie können den `Equals` Operator nur mit dem `readOnly` Feld verwenden. Sie können den `readOnly` Wert auf `true` oder `false` setzen. Wenn Sie dieses Feld nicht hinzufügen, werden sowohl Lese- als auch Schreibereignisse CloudTrail protokolliert. Ein Wert von `true` protokolliert nur Leseereignisse. Der Wert `false` protokolliert nur Schreibereignisse.

### Themen

- [Filtern von Datenereignissen nach readOnly Wert mithilfe des AWS Management Console](#)
- [Filtern von Datenereignissen nach readOnly Wert mithilfe der AWS CLI](#)

### Filtern von Datenereignissen nach **readOnly** Wert mithilfe des AWS Management Console

Gehen Sie wie folgt vor, um das `readOnly` Feld mithilfe der CloudTrail Konsole zu filtern.

1. Folgen Sie den Schritten im Verfahren zum [Erstellen von Pfaden](#) oder folgen Sie den Schritten im Verfahren zum [Erstellen eines Ereignisdatenspeichers](#).
2. Wenn Sie den Schritten zum Erstellen des Trail- oder Event-Datenspeichers folgen, treffen Sie die folgenden Auswahlen:
  - a. Wählen Sie Datenereignisse aus.
  - b. Wählen Sie den Datenereignistyp, für den Sie Datenereignisse protokollieren möchten.
  - c. Wählen Sie unter Log Selector Template die passende Vorlage für Ihren Anwendungsfall aus.

**Data events** [Info](#)  
Data events show information about the resource operations performed on or within a resource.

▼ **Data event: SNS topic** Remove

**Data event type**  
Choose the source of data events to log.

SNS topic ▼

**Log selector template**

Log all events ▲

Log all events ✓

Log readOnly events

Log writeOnly events

Custom

JSON view

Add data event type

Wenn Sie dies planen	Wählen Sie diese Log-Selector-Vorlage
Protokollieren Sie nur Leseereignisse und wenden Sie keine anderen Filter an (z. B. auf den <code>resources.ARN</code> Wert).	Nur ReadOnly-Ereignisse protokollieren
Nur Schreibereignisse protokollieren und keine anderen Filter anwenden (z. B. auf den <code>resources.ARN</code> Wert).	Loggen Sie WriteOnly-Ereignisse

Wenn Sie dies planen	Wählen Sie diese Log-Selector-Vorlage
<p>Filtern Sie nach dem <code>readOnly</code> Wert und wenden Sie zusätzliche Filter an (z. B. auf den <code>resources.ARN</code> Wert).</p>	<p>Custom (Benutzerdefiniert)</p> <p>Gehen Sie unter Erweiterte Event-Selektoren wie folgt vor, um nach dem <code>readOnly</code> Wert zu filtern:</p> <p>Um Schreibereignisse zu protokollieren</p> <ol style="list-style-type: none"><li>Wählen Sie für Feld die Option <code>readOnly</code> aus.</li><li>Wählen Sie für Operator die Option <code>Equals</code> aus.</li><li>Geben Sie für Wert <b>false</b> ein.</li><li>Wählen Sie <code>+Feld</code>, um Filter für andere Felder hinzuzufügen.</li></ol> <p>Um Leseereignisse zu protokollieren</p> <ol style="list-style-type: none"><li>Wählen Sie für Feld die Option <code>readOnly</code> aus.</li><li>Wählen Sie für Operator die Option <code>Equals</code> aus.</li><li>Geben Sie für Wert <b>true</b> ein.</li><li>Wählen Sie <code>+Feld</code>, um Filter für andere Felder hinzuzufügen.</li></ol>

## Filtern von Datenereignissen nach **readOnly** Wert mithilfe der AWS CLI

Mit dem AWS CLI können Sie nach dem `readOnly` Feld filtern.

Sie können den `Equals` Operator nur mit dem `readOnly` Feld verwenden. Sie können den `readOnly` Wert auf `true` oder `false` setzen. Wenn Sie dieses Feld nicht hinzufügen, werden sowohl Lese- als auch Schreibereignisse CloudTrail protokolliert. Ein Wert von `true` protokolliert nur Leseereignisse. Der Wert `false` protokolliert nur Schreibereignisse.

Das folgende Beispiel zeigt, wie Sie Ihren Trail so konfigurieren, dass schreibgeschützte Datenereignisse für alle Amazon S3 S3-Objekte protokolliert werden.

```
aws cloudtrail put-event-selectors \  
--trail-name TrailName \  
--region region \  
--advanced-event-selectors '[  
  {  
    "Name": "Log read-only S3 data events",  
    "FieldSelectors": [  
      { "Field": "eventCategory", "Equals": ["Data"] },  
      { "Field": "resources.type", "Equals": ["AWS::S3::Object"] },  
      { "Field": "readOnly", "Equals": ["true"] }  
    ]  
  }  
]'
```

Im nächsten Beispiel wird ein neuer Ereignisdatenspeicher erstellt, der nur schreibgeschützte Datenereignisse für EBS Direct-APIs protokolliert. Sie können den [update-event-data-store](#) Befehl verwenden, um einen vorhandenen Ereignisdatenspeicher zu aktualisieren.

```
aws cloudtrail create-event-data-store \  
--name "eventDataStoreName" \  
--advanced-event-selectors \  
'[  
  {  
    "Name": "Log write-only EBS Direct API data events",  
    "FieldSelectors": [  
      { "Field": "eventCategory", "Equals": ["Data"] },  
      { "Field": "resources.type", "Equals": ["AWS::EC2::Snapshot"] },  
      { "Field": "readOnly", "Equals": ["false"] }  
    ]  
  }  
]'
```

## Protokollieren von Datenereignissen für AWS Config -Compliance

Wenn Sie AWS Config Conformance Packs verwenden, um Ihr Unternehmen bei der Einhaltung formalisierter Standards zu unterstützen, wie sie beispielsweise vom Federal Risk and Authorization Management Program (FedRAMP) oder vom National Institute of Standards and Technology (NIST) gefordert werden, erfordern Konformitätspakete für Compliance-Frameworks in der Regel,

dass Sie mindestens Datenereignisse für Amazon S3 S3-Buckets protokollieren. Compliance-Pakete für Compliance-Frameworks enthalten eine [verwaltete Regel](#) namens [cloudtrail-s3-dataevents-enabled](#), die die S3-Datenereignisprotokollierung in Ihrem Konto überprüft. Viele Compliance-Pakete, die nicht mit Compliance-Frameworks verknüpft sind, erfordern auch die S3-Datenereignisprotokollierung. Im Folgenden finden Sie Beispiele für Konformitätspakete, die diese Regel enthalten.

- [Bewährte betriebliche Verfahren für die AWS Sicherheitssäule eines Well-Architected Frameworks](#)
- [Betriebliche bewährte Methoden für FDA Titel 21 CFR Teil 11](#)
- [Betriebliche bewährte Methoden für FFIEC](#)
- [Betriebliche bewährte Methoden für FedRAMP \(Moderat\)](#)
- [Betriebliche bewährte Methoden für die HIPAA-Sicherheit](#)
- [Betriebliche bewährte Methoden für K-ISMS](#)
- [Betriebliche bewährte Methoden für die Protokollierung](#)

Eine vollständige Liste der in verfügbaren Muster-Conformance Packs finden Sie im AWS Config Developer Guide unter [Conformance Pack-Beispielvorlagen](#).AWS Config

## Protokollieren von Datenereignissen mit den SDKs AWS

Führen Sie den [GetEventSelectors](#)Vorgang aus, um festzustellen, ob Ihr Trail Datenereignisse protokolliert. Sie können Ihre Trails so konfigurieren, dass Datenereignisse protokolliert werden, indem Sie den [PutEventSelectors](#)Vorgang ausführen. Weitere Informationen finden Sie in der [AWS CloudTrail -API-Referenz](#).

Führen Sie den [GetEventDataStore](#)Vorgang aus, um festzustellen, ob Ihr Ereignisdatenspeicher Datenereignisse protokolliert. Sie können Ihre Ereignisdatenspeicher so konfigurieren, dass sie Datenereignisse enthalten, indem Sie die [UpdateEventDataStore](#)Operationen [CreateEventDataStore](#)oder ausführen und erweiterte Ereigniselektoren angeben. Weitere Informationen finden Sie unter [Erstellen, aktualisieren und verwalten Sie Ereignisdatenspeicher mit dem AWS CLI](#) und der [AWS CloudTrail -API-Referenz](#).

## Ereignisse an Amazon CloudWatch Logs senden

CloudTrail unterstützt das Senden von Datenereignissen an CloudWatch Logs. Wenn Sie Ihren Trail so konfigurieren, dass Ereignisse an Ihre CloudWatch Logs-Protokollgruppe CloudTrail gesendet



werden, werden nur die Ereignisse gesendet, die Sie in Ihrem Trail angegeben haben. Wenn Sie Ihren Trail beispielsweise so konfigurieren, dass er nur Datenereignisse protokolliert, übermittelt Ihr Trail Datenereignisse nur an Ihre CloudWatch Logs-Protokollgruppe. Weitere Informationen finden Sie unter [Überwachung von CloudTrail Protokolldateien mit Amazon CloudWatch Logs](#).

## Protokollieren von Insights-Ereignissen

AWS CloudTrail Insights helfen AWS Benutzern, ungewöhnliche Aktivitäten im Zusammenhang mit API-Aufrufen und API-Fehlerraten zu identifizieren und darauf zu reagieren, indem CloudTrail Verwaltungsereignisse kontinuierlich analysiert werden. CloudTrail Insights analysiert Ihre normalen Muster des API-Aufrufvolumens und der API-Fehlerraten, auch Basiswerte genannt, und generiert Insights-Ereignisse, wenn das Aufrufvolumen oder die Fehlerraten außerhalb der normalen Muster liegen. Insights-Ereignisse zum API-Aufrufvolumen werden für `write`-Verwaltungs-APIs und Insights-Ereignisse zur API-Fehlerrate für `read`- und `write`-Verwaltungs-APIs generiert.

### Note

Um Insights-Ereignisse auf dem API-Aufrufvolumen zu protokollieren, muss der Trail- oder Ereignisdatenspeicher `write`-Verwaltungsereignisse protokollieren. Um Insights-Ereignisse auf der API-Fehlerrate zu protokollieren, muss der Trail oder Ereignisdatenspeicher `read`- oder `write`-Verwaltungsereignisse protokollieren.

CloudTrail Insights analysiert Managementereignisse, die in einer einzelnen Region und nicht weltweit auftreten. Ein CloudTrail Insights-Ereignis wird in derselben Region generiert, in der auch die zugehörigen Managementereignisse generiert werden.

Für Insights-Ereignisse fallen zusätzliche Gebühren an. Wenn Sie Insights sowohl für Trails als auch für Ereignisdatenspeicher aktivieren, wird Ihnen eine separate Gebühr in Rechnung gestellt. Weitere Informationen finden Sie unter [AWS CloudTrail -Preisgestaltung](#).

### Inhalt

- [Grundlegendes zur Insights-Ereignisbereitstellung](#)
- [Protokollieren von Insights-Ereignissen mit dem AWS Management Console](#)
  - [CloudTrail Insights-Ereignisse auf einem vorhandenen Trail aktivieren](#)
  - [Aktivierung von CloudTrail Insights-Ereignissen in einem vorhandenen Ereignisdatenspeicher](#)
- [Protokollieren von Insights-Ereignissen mit dem AWS Command Line Interface](#)

- [Protokollieren von Insights-Ereignissen für einen Trail mit dem AWS CLI](#)
- [Protokollieren von Insights-Ereignissen für einen Ereignisdatenspeicher mit dem AWS CLI](#)
- [Ereignisse mit den AWS SDKs protokollieren](#)
- [Zusätzliche Informationen für Trails](#)
  - [Anzeigen von Insights-Ereignissen für Trails in der Konsole](#)
    - [Spalte filtern](#)
    - [Registerkarte Insights-Diagramm](#)
    - [Registerkarte Attributionen](#)
      - [Baseline-Durchschnitt und Insights Durchschnitt](#)
    - [CloudTrail Registerkarte „Ereignisse“](#)
    - [Registerkarte Insights-Ereignisdatensatz](#)
  - [Trail-Ereignisse an Amazon CloudWatch Logs senden](#)

## Grundlegendes zur Insights-Ereignisbereitstellung

Im Gegensatz zu anderen Arten von Ereignissen, die CloudTrail erfasst werden, werden Insights-Ereignisse nur protokolliert, wenn Änderungen in der API-Nutzung Ihres Kontos CloudTrail festgestellt werden, die sich erheblich von den typischen Nutzungsmustern des Kontos unterscheiden.

Wo Ereignisse CloudTrail übermittelt werden und wie lange es dauert, bis Insights-Ereignisse empfangen werden, unterscheidet sich je nach Trail- und Ereignisdatenspeicher.

### Insights-Ereignisse für Trails bereitstellen

Wenn du Insights-Ereignisse auf einem Trail aktiviert hast und ungewöhnliche Aktivitäten CloudTrail feststellst, werden CloudTrail Insights-Ereignisse an den `/CloudTrail-Insight` Ordner im ausgewählten S3-Ziel-Bucket für deinen Trail gesendet. Nachdem Sie CloudTrail Insights zum ersten Mal auf einem Trail aktiviert haben, kann es bis zu 36 Stunden dauern, CloudTrail bis das erste Insights-Ereignis übermittelt wird, wenn ungewöhnliche Aktivitäten erkannt werden.

Wenn Sie die Protokollierung von Insights-Ereignissen in einem Trail deaktivieren und dann wieder aktivieren oder die Protokollierung für CloudTrail einen Trail beenden und neu starten, kann es bis zu 36 Stunden dauern, bis die Bereitstellung von Insights-Ereignissen wieder aufgenommen wird, wenn ungewöhnliche Aktivitäten festgestellt werden.

### Insights-Ereignisse für Ereignisdatenspeicher bereitstellen

Wenn Sie Insights-Ereignisse in einem Quell-Eventdatenspeicher aktiviert haben, CloudTrail werden Insights-Ereignisse an den Ziel-Ereignisdatspeicher übermittelt. Nachdem Sie CloudTrail Insights zum ersten Mal im Quell-Eventdatenspeicher aktiviert haben, kann es bis zu 7 Tage dauern, CloudTrail bis das erste Insights-Ereignis an den Ziel-Ereignisdatspeicher übermittelt wird, falls ungewöhnliche Aktivitäten festgestellt werden.

Wenn Sie die Protokollierung von Insights-Ereignissen in einem Quellereignisdatspeicher deaktivieren und dann Insights-Ereignisse erneut aktivieren oder die Ereignisaufnahme in einem Quellereignisdatspeicher beenden und neu starten, kann es bis zu 7 Tage dauern, CloudTrail bis die Übermittlung von Insights-Ereignissen wieder aufgenommen wird, wenn ungewöhnliche Aktivitäten festgestellt werden. Für die Aufnahme von Insights-Ereignissen in Lake fallen zusätzliche Gebühren an. CloudTrail Wenn Sie Insights sowohl für Trails als auch für Ereignisdatspeicher aktivieren, wird Ihnen eine separate Gebühr in Rechnung gestellt. Informationen zur CloudTrail Preisgestaltung finden Sie unter [AWS CloudTrail Preise](#).

## Protokollieren von Insights-Ereignissen mit dem AWS Management Console

Sie können Insights-Ereignisse in einem Trail- oder Ereignisdatspeicher mithilfe der Konsole aktivieren.

### Themen

- [CloudTrail Insights-Ereignisse auf einem vorhandenen Trail aktivieren](#)
- [Aktivierung von CloudTrail Insights-Ereignissen in einem vorhandenen Ereignisdatspeicher](#)

### CloudTrail Insights-Ereignisse auf einem vorhandenen Trail aktivieren

Gehen Sie wie folgt vor, um CloudTrail Insights-Ereignisse auf einem vorhandenen Trail zu aktivieren. Standardmäßig sind Insights-Ereignisse nicht aktiviert.

1. Öffnen Sie im linken Navigationsbereich der CloudTrail Konsole die Seite Trails und wählen Sie einen Trailnamen aus.
2. Wählen Sie unter Insights-Ereignisse Bearbeiten aus.

#### Note

Für die Protokollierung von Insights-Ereignissen fallen zusätzliche Gebühren an. CloudTrail Preise finden Sie unter [AWS CloudTrail Preise](#).

3. Wählen Sie unter Ereignistyp Insights-Ereignisse.
4. Wählen Sie in Insights-Ereignisse unter Insights-Typen API-Aufruftrate und/oder API-Fehlerrate aus. Ihr Trail muss Schreibverwaltungsereignisse protokollieren, um Insights-Ereignisse für die API-Aufruftrate zu protokollieren. Ihr Trail muss Lese- und Schreib-Verwaltungsereignisse protokollieren, um Insights-Ereignisse für die API-Fehlerrate zu protokollieren.
5. Wählen Sie Änderungen speichern aus, um Ihre Änderungen zu speichern.

Es kann bis zu 36 Stunden dauern, CloudTrail bis die ersten Insights-Ereignisse gemeldet werden, wenn ungewöhnliche Aktivitäten festgestellt werden.

## Aktivierung von CloudTrail Insights-Ereignissen in einem vorhandenen Ereignisdatenspeicher

Gehen Sie wie folgt vor, um CloudTrail Insights-Ereignisse in einem vorhandenen Ereignisdatenspeicher zu aktivieren. Standardmäßig sind Insights-Ereignisse nicht aktiviert.

Für die Aufnahme von Insights-Veranstaltungen in CloudTrail Lake fallen zusätzliche Gebühren an. Wenn Sie Insights sowohl für Trails als auch für Ereignisdatenspeicher aktivieren, wird Ihnen eine separate Gebühr in Rechnung gestellt. Informationen zur CloudTrail Preisgestaltung finden Sie unter [AWS CloudTrail Preise](#).

### Note

Sie können CloudTrail Insights-Ereignisse nur für Ereignisdatenspeicher aktivieren, die CloudTrail Verwaltungsereignisse enthalten. Sie können CloudTrail Insights-Ereignisse nicht für andere Typen von Ereignisdatenspeichern aktivieren.

1. Wählen Sie im linken Navigationsbereich der CloudTrail Konsole unter Lake die Option Event Data Stores aus.
2. Wählen Sie den Namen des Ereignisdatenspeichers aus.
3. Wählen Sie für Verwaltungsereignisse Bearbeiten aus.
4. Wählen Sie Insights aktivieren aus.
5. Wählen Sie den Ziel-Eventdatenspeicher aus, in den Insights-Ereignisse übertragen CloudTrail werden sollen. Der Zielereignisdatenspeicher erfasst Insights-Ereignisse auf

der Grundlage der Verwaltungsereignisaktivität in diesem Ereignisdatenspeicher. Weitere Informationen zum Erstellen des Zielereignisdatenspeichers finden Sie unter [Erstellen eines Zielereignisdatenspeichers, der Insights-Ereignisse protokolliert](#).

- Wählen Sie unter Insights-Typen auswählen API-Aufruftrate, API-Fehlerrate oder beides aus. Der Ereignisdatenspeicher muss Schreib-Verwaltungsereignisse protokollieren, um Insights-Ereignisse für die API-Aufruftrate zu protokollieren. Der Ereignisdatenspeicher muss Lese- und Schreib-Verwaltungsereignisse protokollieren, um Insights-Ereignisse für die API-Fehlerrate zu protokollieren.
- Wählen Sie Änderungen speichern aus, um Ihre Änderungen zu speichern.

Es kann bis zu 7 Tage dauern, CloudTrail bis die ersten Insights-Ereignisse zugestellt werden, wenn ungewöhnliche Aktivitäten festgestellt werden.

## Protokollieren von Insights-Ereignissen mit dem AWS Command Line Interface

Sie können Ihre Trails und Ereignisdatenspeicher so konfigurieren, dass Insights-Ereignisse per AWS CLI protokolliert werden.

### Note

Um Insights-Ereignisse auf dem API-Aufrufvolumen zu protokollieren, muss der Trail- oder Ereignisdatenspeicher `write`-Verwaltungsereignisse protokollieren. Um Insights-Ereignisse auf der API-Fehlerrate zu protokollieren, muss der Trail oder Ereignisdatenspeicher `read`- oder `write`-Verwaltungsereignisse protokollieren.

### Themen

- [Protokollieren von Insights-Ereignissen für einen Trail mit dem AWS CLI](#)
- [Protokollieren von Insights-Ereignissen für einen Ereignisdatenspeicher mit dem AWS CLI](#)

## Protokollieren von Insights-Ereignissen für einen Trail mit dem AWS CLI

Führen Sie den Befehl `get-insight-selectors` aus, um anzuzeigen, ob Ihr Trail Insights-Ereignisse protokolliert.

```
aws cloudtrail get-insight-selectors --trail-name TrailName
```

Das folgende Ergebnis enthält die Standardeinstellungen für einen Trail. Standardmäßig werden für Trails keine Insights-Ereignisse protokolliert. Der Attributwert `InsightType` ist leer, und es wird keine Auswahl für Insights-Ereignisse angezeigt, weil die Erfassung von Insights-Ereignissen nicht aktiviert ist.

Wenn Sie keine Insights-Selektoren hinzufügen, gibt der `get-insight-selectors` Befehl die folgende Fehlermeldung zurück: „Beim Aufrufen der `GetInsightSelectors` Operation ist ein Fehler aufgetreten (`InsightNotEnabledException`): Beim *Namen* des Trails ist Insights nicht aktiviert. Edit the trail settings to enable Insights, and then try the operation again.“

```
{
  "InsightSelectors": [ ],
  "TrailARN": "arn:aws:cloudtrail:us-east-1:123456789012:trail/TrailName"
}
```

Führen Sie den Befehl `put-insight-selectors` aus, um Ihren Trail für die Protokollierung von Insights-Ereignissen zu konfigurieren. Im folgenden Beispiel wird veranschaulicht, wie Sie Ihren Trail für Insights-Ereignisse konfigurieren. Insights-Selektor-Werte können `ApiCallRateInsight` und/oder `ApiErrorRateInsight` sein.

```
aws cloudtrail put-insight-selectors --trail-name TrailName --insight-selectors
' [{"InsightType": "ApiCallRateInsight"}, {"InsightType": "ApiErrorRateInsight"} ]'
```

Das folgende Ergebnis enthält die Auswahl für Insights-Ereignisse, die für den Trail konfiguriert wurde.

```
{
  "InsightSelectors":
    [
      {
        "InsightType": "ApiErrorRateInsight"
      },
      {
        "InsightType": "ApiCallRateInsight"
      }
    ],
  "TrailARN": "arn:aws:cloudtrail:us-east-1:123456789012:trail/TrailName"
}
```

```
}
```

## Protokollieren von Insights-Ereignissen für einen Ereignisdatenspeicher mit dem AWS CLI

Um Insights in einem Ereignisdatenspeicher zu aktivieren, benötigen Sie einen Quellereignisdatenspeicher, der Verwaltungsereignisse protokolliert, und einen Zielereignisdatenspeicher, der Insights-Ereignisse protokolliert.

Führen Sie den Befehl `get-insight-selectors` aus, um zu überprüfen, ob Insights-Ereignisse in einem Ereignisdatenspeicher aktiviert sind.

```
aws cloudtrail get-insight-selectors --event-data-store arn:aws:cloudtrail:us-east-1:123456789012:eventdatastore/EXAMPLE-f852-4e8f-8bd1-bcf6cEXAMPLE
```

Führen Sie den Befehl `get-event-data-store` aus, um zu überprüfen, ob Insights-Ereignisse oder Verwaltungsereignisse in einem Ereignisdatenspeicher aktiviert sind.

```
aws cloudtrail get-event-data-store --event-data-store arn:aws:cloudtrail:us-east-1:123456789012:eventdatastore/EXAMPLE-d483-5c7d-4ac2-adb5dEXAMPLE
```

Das folgende Verfahren zeigt, wie Sie die Ziel- und Quellereignisdatenspeicher erstellen und anschließend Insights-Ereignisse aktivieren.

1. Führen Sie den Befehl [aws cloudtrail create-event-data-store](#) aus, um einen Zielereignisdatenspeicher zu erstellen, der Insights-Ereignisse sammelt. Der Wert für `eventCategory` muss `Insight` sein. *retention-period-days* Ersetzen Sie es durch die Anzahl der Tage, an denen Sie Ereignisse in Ihrem Ereignisdatenspeicher speichern möchten.

Wenn Sie mit dem Verwaltungskonto für eine AWS Organizations Organisation angemeldet sind, geben Sie den `--organization-enabled` Parameter an, wenn Sie Ihrem [delegierten Administrator](#) Zugriff auf den Ereignisdatenspeicher gewähren möchten.

```
aws cloudtrail create-event-data-store \  
--name insights-event-data-store \  
--no-multi-region-enabled \  
--retention-period retention-period-days \  
--advanced-event-selectors '[  
  {  
    "Name": "Select Insights events",
```

```

    "FieldSelectors": [
      { "Field": "eventCategory", "Equals": ["Insight"] }
    ]
  }
]'

```

Nachfolgend finden Sie eine Beispielantwort.

```

{
  "Name": "insights-event-data-store",
  "ARN": "arn:aws:cloudtrail:us-east-1:111122223333:eventdatastore/
EXAMPLEf852-4e8f-8bd1-bcf6cEXAMPLE",
  "AdvancedEventSelectors": [
    {
      "Name": "Select Insights events",
      "FieldSelectors": [
        {
          "Field": "eventCategory",
          "Equals": [
            "Insight"
          ]
        }
      ]
    }
  ],
  "MultiRegionEnabled": false,
  "OrganizationEnabled": false,
  "BillingMode": "EXTENDABLE_RETENTION_PRICING",
  "RetentionPeriod": "90",
  "TerminationProtectionEnabled": true,
  "CreatedTimestamp": "2023-11-08T15:22:33.578000+00:00",
  "UpdatedTimestamp": "2023-11-08T15:22:33.714000+00:00"
}

```

Sie verwenden die ARN (oder das ID-Suffix des ARN) aus der Antwort als Wert für den Parameter `--insights-destination` in Schritt 3.

- Um einen Quellereignisdatenspeicher zu erstellen, der Verwaltungsereignisse protokolliert, führen Sie den Befehl [aws cloudtrail create-event-data-store](#) aus. Standardmäßig protokollieren Ereignisdatenquellen alle Verwaltungsereignisse. Sie müssen keine erweiterten Ereigniselektoren angeben, um alle Verwaltungsereignisse zu protokollieren. *retention-*



*period-days* Ersetzen Sie ihn durch die Anzahl der Tage, an denen Sie Ereignisse in Ihrem Ereignisdatenspeicher speichern möchten. Wenn Sie einen Datenspeicher für Organisationsereignisse erstellen, fügen Sie den Parameter `--organization-enabled` hinzu.

```
aws cloudtrail create-event-data-store --name source-event-data-store --retention-period retention-period-days
```

Nachfolgend finden Sie eine Beispielantwort.

```
{
  "EventDataStoreArn": "arn:aws:cloudtrail:us-east-1:111122223333:eventdatastore/EXAMPLE9952-4ab9-49c0-b788-f4f3EXAMPLE",
  "Name": "source-event-data-store",
  "Status": "CREATED",
  "AdvancedEventSelectors": [
    {
      "Name": "Default management events",
      "FieldSelectors": [
        {
          "Field": "eventCategory",
          "Equals": [
            "Management"
          ]
        }
      ]
    }
  ],
  "MultiRegionEnabled": true,
  "OrganizationEnabled": false,
  "BillingMode": "EXTENDABLE_RETENTION_PRICING",
  "RetentionPeriod": 90,
  "TerminationProtectionEnabled": true,
  "CreatedTimestamp": "2023-11-08T15:25:35.578000+00:00",
  "UpdatedTimestamp": "2023-11-08T15:25:35.714000+00:00"
}
```

Sie verwenden die ARN (oder das ID-Suffix des ARN) aus der Antwort als Wert für den Parameter `--event-data-store` in Schritt 3.

3. Führen Sie den Befehl [put-insight-selectors](#) aus, um Insights-Ereignisse zu aktivieren. Insights-Selektorwerte können `ApiCallRateInsight` und/oder `ApiErrorRateInsight` sein. Geben Sie für den Parameter `--event-data-store` den ARN (oder das ID-Suffix der ARN) des

Quellereignisdatenspeichers an, der Verwaltungsereignisse protokolliert und Insights aktiviert. Geben Sie für den Parameter `--insights-destination` den ARN (oder das ID-Suffix des ARN) des Zielereignisdatenspeichers an, der Insights-Ereignisse protokolliert.

```
aws cloudtrail put-insight-selectors --event-data-store arn:aws:cloudtrail:us-east-1:111122223333:eventdatastore/EXAMPLE9952-4ab9-49c0-b788-f4f3EXAMPLE --insights-destination arn:aws:cloudtrail:us-east-1:111122223333:eventdatastore/EXAMPLEf852-4e8f-8bd1-bcf6cEXAMPLE --insight-selectors '[{"InsightType": "ApiCallRateInsight"}, {"InsightType": "ApiErrorRateInsight"}]'
```

Das folgende Ergebnis zeigt den Insights-Ereignisselektor, der für den Ereignisdatenspeicher konfiguriert wurde.

```
{
  "EventDataStoreARN": "arn:aws:cloudtrail:us-east-1:111122223333:eventdatastore/EXAMPLE9952-4ab9-49c0-b788-f4f3EXAMPLE",
  "InsightsDestination": "arn:aws:cloudtrail:us-east-1:111122223333:eventdatastore/EXAMPLEf852-4e8f-8bd1-bcf6cEXAMPLE",
  "InsightSelectors":
    [
      {
        "InsightType": "ApiErrorRateInsight"
      },
      {
        "InsightType": "ApiCallRateInsight"
      }
    ]
}
```

Nachdem Sie CloudTrail Insights zum ersten Mal in einem Ereignisdatenspeicher aktiviert haben, kann es bis zu 7 Tage dauern, CloudTrail bis das erste Insights-Ereignis übermittelt wird, wenn ungewöhnliche Aktivitäten festgestellt werden.

CloudTrail Insights analysiert Verwaltungsereignisse, die in einer einzelnen Region und nicht global auftreten. Ein CloudTrail Insights-Ereignis wird in derselben Region generiert, in der auch die zugehörigen Managementereignisse generiert werden.

CloudTrail Analysiert bei einem Datenspeicher für Organisationsereignisse Verwaltungsereignisse aus den Konten der einzelnen Mitglieder, anstatt die Aggregation aller Verwaltungsereignisse für die Organisation zu analysieren.

Für die Aufnahme von Insights-Veranstaltungen in Lake fallen zusätzliche Gebühren an CloudTrail . Wenn Sie Insights sowohl für Trails als auch für Ereignisdatenspeicher aktivieren, wird Ihnen eine separate Gebühr in Rechnung gestellt. Informationen zur CloudTrail Preisgestaltung finden Sie unter [AWS CloudTrail Preise](#).

## Ereignisse mit den AWS SDKs protokollieren

Führen Sie den [GetInsightSelectors](#)Vorgang aus, um festzustellen, ob Ihr Trail- oder Event-Datenspeicher Insights-Ereignisse aktiviert. Sie können Ihre Datenspeicher für Pfade oder Ereignisse so konfigurieren, dass Insights-Ereignisse während des [PutInsightSelectors](#)Vorgangs aktiviert werden. Weitere Informationen finden Sie in der [AWS CloudTrail -API-Referenz](#).

## Zusätzliche Informationen für Trails

Dieser Abschnitt enthält zusätzliche Informationen, die sich speziell auf Trails beziehen. In diesem Abschnitt wird beschrieben, wie Sie Ereignisse für Ihre abonnierten Trails auf der Insights-Seite in der CloudTrail Konsole anzeigen können und wie Sie diese Ereignisse optional zur Überwachung an CloudWatch Logs senden können.

### Themen

- [Anzeigen von Insights-Ereignissen für Trails in der Konsole](#)
- [Trail-Ereignisse an Amazon CloudWatch Logs senden](#)

## Anzeigen von Insights-Ereignissen für Trails in der Konsole

Bei Trails können Sie auch auf der Insights-Seite in der CloudTrail Konsole auf Insights-Ereignisse zugreifen und diese einsehen. Weitere Informationen zum Aufrufen und Anzeigen von Insights-Ereignissen in der Konsole und mithilfe von finden Sie [CloudTrail Insights-Ereignisse für Wanderwege anzeigen](#) in diesem Handbuch. AWS CLI

Das folgende Bild zeigt ein Beispiel für Insights-Ereignisse für einen Trail. Sie öffnen die Detailseiten für ein Insights-Ereignis, indem Sie auf der Seite Dashboard oder Insights den Namen eines Insights-Ereignisses auswählen.

Wenn Sie CloudTrail Insights in einem Trail deaktivieren oder die Protokollierung bei einem Trail beenden (wodurch CloudTrail Insights deaktiviert wird), werden möglicherweise Insights-Ereignisse in Ihrem Ziel-S3-Bucket gespeichert oder auf der Insights-Seite der Konsole angezeigt. Dabei handelt es sich um das Datum, zu dem Sie Insights früher aktiviert hatten.

## Spalte filtern

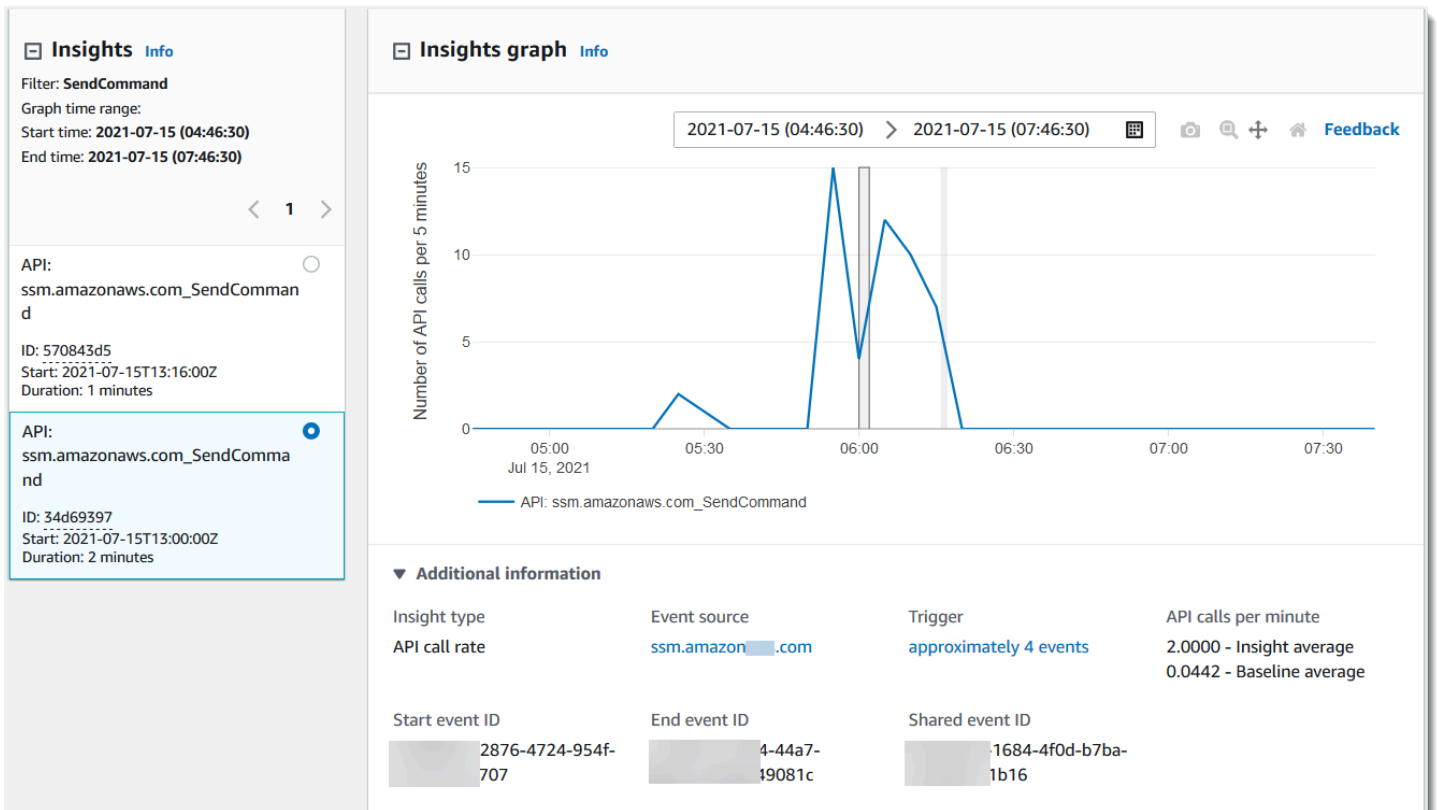
In der Spalte auf der linken Seite sind Insights-Ereignisse aufgeführt, die sich auf die Subjekt-API beziehen und den gleichen Typ von Insights-Ereignis aufweisen. In der Spalte können Sie das Ereignis „Insights“ auswählen, zu dem Sie weitere Informationen wünschen. Wenn Sie in dieser Spalte ein Ereignis auswählen, wird das Ereignis in der Grafik auf der Registerkarte Insights-Diagramm hervorgehoben. CloudTrail wendet standardmäßig einen Filter an, der die auf der Registerkarte „Ereignisse“ angezeigten Ereignisse auf CloudTrail-Ereignisse beschränkt, die sich auf die spezifische API beziehen, die während des Zeitraums ungewöhnlicher Aktivitäten aufgerufen wurde, der das Insights-Ereignis ausgelöst hat. Um alle CloudTrail-Ereignisse anzuzeigen, die während des Zeitraums ungewöhnlicher Aktivitäten aufgerufen wurden, einschließlich Ereignissen, die nichts mit dem Insights-Ereignis zu tun haben, schalten Sie den Filter aus.

## Registerkarte Insights-Diagramm

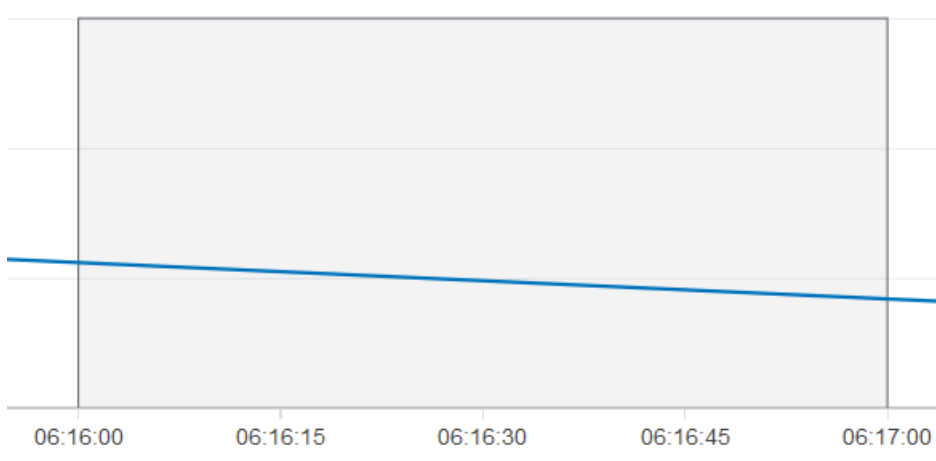
Auf der Registerkarte Insights-Diagramm zeigt die Detailseite für ein Insights-Ereignis ein Diagramm des API-Aufrufvolumens oder der Fehlerrate an, das bzw. die über einen bestimmten Zeitraum vor und nach der Protokollierung eines oder mehrerer Insights-Ereignisse aufgetreten ist. In der Grafik sind Insights-Ereignisse durch vertikale Balken gekennzeichnet und die Breite des Balkens gibt die Start- und Endzeit des Insights-Ereignisses an.

In diesem Beispiel zeigt ein vertikales hervorgehobenes Band ungewöhnlich viele AWS Systems Manager SendCommand API-Aufrufe in einem Konto. Im hervorgehobenen Bereich wurde ein Insights-Ereignis CloudTrail protokolliert, als die ungewöhnliche Aktivität erkannt wurde, da die Anzahl der Aufrufe über den Basisdurchschnitt des Kontos von 0,0442 Aufrufen pro Minute gestiegen ist. SendCommand Das Insights-Ereignis zeichnete auf, dass in einem Zeitraum von fünf Minuten zwischen 5:50 und 5:55 Uhr 15 SendCommand-Aufrufe getätigt wurden. Dies sind pro Minute ca. 2 API-Aufrufe mehr, als für das Konto erwartet werden. In diesem Beispiel beträgt die Zeitspanne des Diagramms drei Stunden: 4:30 Uhr PDT am 15. Juli 2021 bis 7:30 Uhr PDT am 15. Juli 2021. Dieses Ereignis startet um 6:00 Uhr PDT am 15. Juli 2021 und endet zwei Minuten später. Ein endendes Insights-Ereignis, das nicht hervorgehoben ist, zeigt, dass die ungewöhnliche Aktivität gegen 6:16 Uhr endete.

Die Baseline wird in den sieben Tagen vor Beginn eines Insights-Ereignisses berechnet. Der Wert der Basisdauer — der Zeitraum, in dem normale Aktivitäten auf CloudTrail APIs analysiert werden — beträgt zwar ungefähr sieben Tage, CloudTrail rundet die Basisdauer jedoch auf eine ganze Ganzzahl auf, sodass die genaue Basisdauer variieren kann.



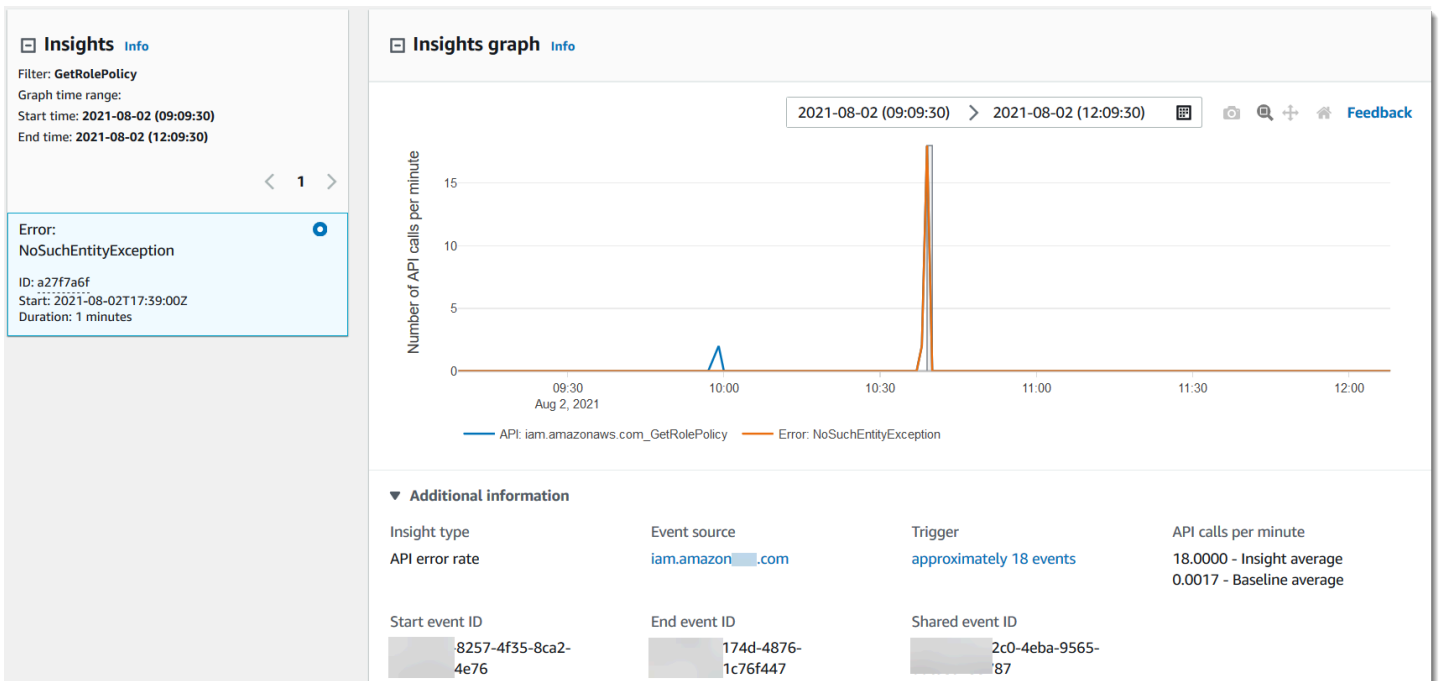
Sie können den Zoom-Befehl in der Symbolleiste verwenden, um das endende Insights-Ereignis zu vergrößern und die Start- und Endzeit anzuzeigen. Wenn Sie in diesem Beispiel Zoom wählen und dann den Zoom-Cursor eine sehr kurze Strecke über eine Kante des hervorgehobenen Insights-Ereignisses ziehen, wird das Insights-Ereignis erweitert und es werden mehr Zeitachsendetails angezeigt.



Um CloudTrail Ereignisse anzuzeigen, die analysiert wurden, um ungewöhnliche Aktivitäten zu ermitteln, öffnen Sie den Tab CloudTrail Ereignisse. In diesem Beispiel CloudTrail wurden 12 Ereignisse analysiert, von denen vier das Insights-Ereignis ausgelöst haben.

Event name	Event time	User name	Event source	Resource type	Resource name
SendCommand	July 15, 2021, 06:01:01 (UTC-07...	i-0db2a4	ssm.amazonaws.com	-	-
SendCommand	July 15, 2021, 06:00:39 (UTC-07...	i-0db2a4	ssm.amazonaws.com	-	-
SendCommand	July 15, 2021, 06:00:08 (UTC-07...	i-0da014	ssm.amazonaws.com	-	-
SendCommand	July 15, 2021, 06:00:04 (UTC-07...	i-0b442a	ssm.amazonaws.com	-	-
SendCommand	July 15, 2021, 05:59:57 (UTC-07...	i-0db2a4	ssm.amazonaws.com	-	-
SendCommand	July 15, 2021, 05:59:46 (UTC-07...	i-0da014	ssm.amazonaws.com	-	-
SendCommand	July 15, 2021, 05:59:43 (UTC-07...	i-0b0ba5	ssm.amazonaws.com	-	-
SendCommand	July 15, 2021, 05:59:42 (UTC-07...	i-0b442a	ssm.amazonaws.com	-	-
SendCommand	July 15, 2021, 05:59:14 (UTC-07...	i-0db2a4	ssm.amazonaws.com	-	-
SendCommand	July 15, 2021, 05:59:11 (UTC-07...	i-0b0ba5	ssm.amazonaws.com	-	-
SendCommand	July 15, 2021, 05:59:04 (UTC-07...	i-0da014	ssm.amazonaws.com	-	-
SendCommand	July 15, 2021, 05:59:00 (UTC-07...	i-0b442a	ssm.amazonaws.com	-	-

Das folgende Bild zeigt eine Registerkarte mit einem Insights-Diagramm für ein API-Fehlerrate-Insights-Ereignis. Der hervorgehobene Bereich zeigt, dass ein Insights-Ereignis protokolliert wurde, da Vorkommen des NoSuchEntityException-Fehlers für den GetRolePolicy-IAM-API-Aufruf den Baseline-Durchschnitt von 0,0017 NoSuchEntityException-Fehlern pro Minute bei diesem API-Aufruf überschritten haben: Während des Insight-Zeitraums sind durchschnittlich 18 Fehler pro Minute aufgetreten. Die Anzahl der CloudTrail Ereignisse, die das Insights-Ereignis ausgelöst haben, entspricht in diesem Beispiel dem Insights-Durchschnitt von 18 NoSuchEntityException Fehlern pro Minute. Im Gegensatz zu einem API-Aufruf-Diagramm zeigt die API-Fehlerrate zwei Linien in kontrastierenden Farben: eine Linie, die Aufrufe an die IAM-API GetRolePolicy misst, die zu einer ungewöhnlichen Anzahl von Fehlern führten, und eine Linie, die den Fehler misst, für den ungewöhnliche Aktivitäten protokolliert wurden, NoSuchEntityException.



## Registerkarte Attributionen

Auf der Registerkarte Attributionen werden die folgenden Informationen zu einem Insights-Ereignis angezeigt. Die Informationen auf der Registerkarte Attributionen können Ihnen helfen, die Ursachen und Quellen von Insights-Aktivitäten zu ermitteln. Erweitern Sie die obersten Baseline-Bereiche, um die Benutzeridentität, den Benutzeragenten und die Fehlercode-Aktivität in normalen Zeiträumen mit denen zu vergleichen, die während der Insights-Aktivität zugeordnet werden. In Top-Baseline-Benutzeridentitäts-ARNs, Top-Baseline-Benutzeragenten und Top-Baseline-Fehlercodes wird nur der Baseline-Durchschnitt angezeigt – der historische Durchschnitt der Ereignisse für die API, die von der Benutzeridentität oder dem Benutzeragenten protokolliert werden oder die in etwa sieben Tagen vor der Startzeit des Insights-Ereignisses zum Fehlercode führen.

Insights graph			
Attributions <span>New</span>			
CloudTrail events			
Insights event record			
<b>Top user identity ARNs during Insights event</b> <a href="#">Info</a>			
User identity ARN	Insight average	Baseline average	
1 arn:aws:sts::[REDACTED]:assumed-role/AWSServiceRoleForApplicationAutoScaling_DynamoDBTable/AutoScaling-ManageAlarms	3.0000 (100.000%)	0.0523 (100.000%)	
<b>Average API calls during Insights event</b>	<b>3.0000</b>	<b>0.0523</b>	
▶ Top baseline user identity ARNs			
<b>Top user agents during Insights event</b> <a href="#">Info</a>			
User agent	Insight average	Baseline average	
1 dynamodb.application-autoscaling.amazonaws.com	3.0000 (100.000%)	0.0523 (100.000%)	
<b>Average API calls during Insights event</b>	<b>3.0000</b>	<b>0.0523</b>	
▶ Top baseline user agents			
<b>Top error codes during Insights event</b> <a href="#">Info</a>			
Error code	Insight average	Baseline average	
1 None	3.0000 (100.000%)	0.0523 (100.000%)	
<b>Average API calls during Insights event</b>	<b>3.0000</b>	<b>0.0523</b>	
▶ Top baseline error codes			

Auf der Registerkarte Attributionen werden nur Top-Benutzeridentitäts-ARNs und Top-Benutzeragenten für ein Fehlerrate-Insights-Ereignis angezeigt, wie im folgenden Image dargestellt. Top-Fehlercodes sind für Fehlerrate-Insights-Ereignisse nicht erforderlich.



Attributions			
CloudTrail events			
Insights event record			
<b>Top user identity ARNs during Insights event</b> <a href="#">Info</a>			
	User identity ARN	Insight average	Baseline average
1	[REDACTED]	1.7500 (100.000%)	0.0037 (100.000%)
<b>Average API calls during Insights event</b>		<b>1.7500</b>	<b>0.0037</b>
▶ Top baseline user identity ARNs			
<b>Top user agents during Insights event</b> <a href="#">Info</a>			
	User agent	Insight average	Baseline average
1	[REDACTED]	1.7500 (100.000%)	0.0012 (33.333%)
<b>Average API calls during Insights event</b>		<b>1.7500</b>	<b>0.0037</b>
▶ Top baseline user agents			

- ARNs mit den häufigsten Benutzeridentitäten — In dieser Tabelle sind die fünf wichtigsten AWS Benutzer oder IAM-Rollen (Benutzeridentitäten) aufgeführt, die in den ungewöhnlichen Aktivitäts- und Basiszeiträumen zu API-Aufrufen beigetragen haben, in absteigender Reihenfolge nach der durchschnittlichen Anzahl der eingereichten API-Aufrufe. Der Prozentsatz der Durchschnittswerte als Summe der Aktivität, die zu der ungewöhnlichen Aktivität beigetragen hat, wird in Klammern angezeigt. Wenn mehr als fünf Benutzeridentitäts-ARNs zu der ungewöhnlichen Aktivität beigetragen haben, wird ihre Aktivität in der Zeile Sonstige zusammengefasst.
- Top-Benutzeragenten — In dieser Tabelle sind die fünf wichtigsten AWS Tools aufgeführt, mit denen die Benutzeridentität in den ungewöhnlichen Aktivitäts- und Basiszeiträumen zu API-Aufrufen beigetragen hat, in absteigender Reihenfolge nach der durchschnittlichen Anzahl der bereitgestellten API-Aufrufe. Zu diesen Tools gehören die AWS Management Console AWS CLI, oder die SDKs AWS . Beispiel: Ein User-Agent mit dem Namen `ec2.amazonaws.com` gibt an, dass die Amazon-EC2-Konsole zu den Tools gehörte, die zum Aufrufen der API verwendet wurden. Der Prozentsatz der Durchschnittswerte als Summe der Aktivität, die zu der ungewöhnlichen Aktivität beigetragen hat, wird in Klammern angezeigt. Wenn mehr als fünf Benutzeragenten zu der ungewöhnlichen Aktivität beigetragen haben, wird ihre Aktivität in der Zeile Sonstige zusammengefasst.

- Top-Fehlercodes – Werden nur für Insights-Ereignisse für API-Aufrufen angezeigt. Diese Tabelle zeigt bis zu fünf der häufigsten Fehlercodes, die bei API-Aufrufen während der ungewöhnlichen Aktivitäts- und Baseline-Zeiträume aufgetreten sind, in absteigender Reihenfolge von der größten zur kleinsten Anzahl von API-Aufrufen. Der Prozentsatz der Durchschnittswerte als Summe der Aktivität, die zu der ungewöhnlichen Aktivität beigetragen hat, wird in Klammern angezeigt. Wenn während der ungewöhnlichen oder grundlegenden Aktivität mehr als fünf Fehlercodes aufgetreten sind, wird ihre Aktivität in der Zeile Sonstige zusammengefasst.

Ein Wert von None als einer der fünf häufigsten Fehlercodewerte bedeutet, dass ein erheblicher Prozentsatz der Aufrufe, die zum Insights-Ereignis beigetragen haben, nicht zu Fehlern geführt hat. Wenn der Fehlercodewert x ist None und keine anderen Fehlercodes in der Tabelle vorhanden sind, sind die Werte in den Spalten Insight-Durchschnitt und Baseline-Durchschnitt dieselben wie für das Insights-Ereignis insgesamt. Sie können diese Werte auch in der Legende für Insight-Durchschnitt und Baseline-Durchschnitt auf der Registerkarte Insights-Diagramm unter API-Aufrufe pro Minute anzeigen.

## Baseline-Durchschnitt und Insights Durchschnitt

Baseline-Durchschnitt und Insights-Durchschnitt werden für Top-Benutzeridentitäten, Top-Benutzeragenten und Top-Fehlercodes angezeigt.

- Baseline-Durchschnitt – Die typische Rate von Vorkommen pro Minute für diese API, für die das Insights-Ereignis protokolliert wurde, gemessen in ungefähr den letzten sieben Tagen in einer bestimmten Region in Ihrem Konto.
- Insights-Durchschnitt – Die Rate von API-Aufrufen oder -Fehlern, von denen das Insights-Ereignis ausgelöst wurde. Der CloudTrail Insights-Durchschnitt für das Startereignis ist die Rate der Aufrufe oder Fehler pro Minute auf der API, die das Insights-Ereignis ausgelöst haben. Normalerweise ist dies die erste Minute mit ungewöhnlichen Aktivitäten. Der Insights-Durchschnitt für das Endereignis ist die Rate von API-Aufrufen oder -Fehlern pro Minute für die Dauer der ungewöhnlichen Aktivitäten zwischen dem Insights-Start- und -Endereignis.

## CloudTrail Registerkarte „Ereignisse“

Sehen Sie sich auf der Registerkarte CloudTrail Ereignisse verwandte Ereignisse an, die CloudTrail analysiert wurden, um festzustellen, ob ungewöhnliche Aktivitäten aufgetreten sind. Standardmäßig wird bereits ein Filter für den Namen des Insights-Ereignisses angewendet. Dies ist auch der Name der zugehörigen API. Um alle CloudTrail Ereignisse anzuzeigen, die während des Zeitraums

ungewöhnlicher Aktivitäten protokolliert wurden, deaktivieren Sie die Option Nur Ereignisse für das ausgewählte Insights-Ereignis anzeigen. Auf der Registerkarte „CloudTrail Ereignisse“ werden CloudTrail Verwaltungsereignisse im Zusammenhang mit der Betreff-API angezeigt, die zwischen der Start- und Endzeit des Insights-Ereignisses aufgetreten sind. Mit diesen Ereignissen können Sie eine eingehendere Analyse durchführen, um die wahrscheinliche Ursache eines Insights-Ereignisses und die Gründe für die ungewöhnliche API- und Fehlerraten-Aktivität zu ermitteln.

## Registerkarte Insights-Ereignisdatensatz

Wie jedes CloudTrail Ereignis ist ein CloudTrail Insights-Ereignis ein Datensatz im JSON-Format. Die Registerkarte Insights-Ereignisdatensatz zeigt die JSON-Struktur und den Inhalt der Insights-Start- und -Endereignisse an, die manchmal auch als Ereignis-Nutzlast bezeichnet werden. Weitere Informationen zu den Feldern und Inhalten des Insights-Ereignisdatensatzes finden Sie unter [Datensatzfelder von Insights-Ereignissen](#) und [CloudTrail insightDetailsElement „Einblicke“](#) in diesem Handbuch.

## Trail-Ereignisse an Amazon CloudWatch Logs senden

CloudTrail unterstützt das Senden von Insights-Ereignissen für Trails an CloudWatch Logs. Wenn Sie Ihren Trail so konfigurieren, dass Insights-Ereignisse an Ihre CloudWatch Logs-Protokollgruppe gesendet werden, sendet CloudTrail Insights nur die Ereignisse, die Sie in Ihrem Trail angeben. Wenn Sie Ihren Trail beispielsweise so konfigurieren, dass er Verwaltungs- und Insights-Ereignisse protokolliert, übermittelt Ihr Trail Verwaltungs- und Insights-Ereignisse an Ihre CloudWatch Logs-Protokollgruppe. Weitere Informationen finden Sie unter [Überwachung von CloudTrail Protokolldateien mit Amazon CloudWatch Logs](#).

## CloudTrail Inhalt aufzeichnen

Der Hauptteil des Datensatzes enthält Felder, mit deren Hilfe Sie die angeforderte Aktion bestimmen können sowie wann und wo die Anforderung gestellt wurde. Wenn der Wert von `Optional True` lautet, ist das Feld nur vorhanden, wenn es für den Service, die API oder den Ereignistyp gilt. Der optionale Wert `False` bedeutet, dass das Feld entweder immer vorhanden ist oder dass seine Präsenz nicht vom Service, der API oder dem Ereignistyp abhängt. Ein Beispiel ist `responseElements`, das in Ereignissen für Aktionen vorhanden ist, die Änderungen vornehmen (Erstellungs-, Aktualisierungs- oder Löschungsaktionen).

CloudTrail kürzt ein Feld, wenn der Inhalt des Felds die maximale Feldgröße überschreitet. Wenn ein Feld gekürzt wird, ist `omitted` mit einem Wert `true` vorhanden.

## eventTime

Das Datum und die Uhrzeit, zu der die Anforderung abgeschlossen wurde, in koordinierter Weltzeit (UTC). Der Zeitstempel eines Ereignisses stammt vom lokalen Host, der den Service-API-Endpunkt bereitstellt, auf dem der API-Aufruf erfolgte. Beispielsweise würde ein CreateBucket API-Ereignis, das in der Region USA West (Oregon) ausgeführt wird, seinen Zeitstempel von der Uhrzeit auf einem AWS Host erhalten, auf dem der Amazon S3 S3-Endpunkt ausgeführt wird `s3.us-west-2.amazonaws.com`. Im Allgemeinen verwenden AWS Dienste das Network Time Protocol (NTP), um ihre Systemuhren zu synchronisieren.

Seit: 1.0

Optional: False

## eventVersion

Die Version des Protokollereignisformats. Die aktuelle Version ist 1.10.

Der Wert `eventVersion` ist eine Haupt- und eine Nebenversion in der Form *major\_version.minor\_version*. Sie können beispielsweise einen `eventVersion`-Wert von `1.09` haben, wobei 1 die Hauptversion und 09 die Nebenversion ist.

CloudTrail erhöht die Hauptversion, wenn eine Änderung an der Ereignisstruktur vorgenommen wird, die nicht abwärtskompatibel ist. Dazu gehört das Entfernen eines bereits vorhandenen JSON-Felds oder das Ändern der Darstellung des Feldinhalts (z. B. eines Datumsformats). CloudTrail erhöht die Nebenversion, wenn der Ereignisstruktur durch eine Änderung neue Felder hinzugefügt werden. Dies kann der Fall sein, wenn neue Informationen für einige oder alle vorhandenen Ereignisse verfügbar sind oder wenn neue Informationen nur für neue Ereignistypen verfügbar sind. Anwendungen können neue Felder ignorieren, um weiter kompatibel mit neuen Nebenversionen der Ereignisstruktur zu sein.

Wenn neue Ereignistypen CloudTrail eingeführt werden, die Struktur des Ereignisses aber ansonsten unverändert bleibt, ändert sich die Eventversion nicht.

Um sicherzustellen, dass Ihre Anwendungen die Ereignisstruktur analysieren können, empfehlen wir Ihnen, einen Gleichheitsvergleich der Hauptversionsnummer durchzuführen. Um sicherzugehen, dass Felder vorhanden sind, die von Ihrer Anwendung erwartet werden, empfehlen wir außerdem, für die Nebenversion einen `greater-than-or-equal-to`-Vergleich durchzuführen. Es gibt keine führenden Nullen in der Nebenversion. Sie können sowohl *major\_version* als auch *minor\_version* als Zahlen interpretieren und Vergleichsoperationen durchführen.

Seit: 1.0

Optional: False

### **userIdentity**

Informationen über die IAM-Identität, die eine Anforderung erstellt hat. Weitere Informationen finden Sie unter [CloudTrail Element „userIdentity“](#).

Seit: 1.0

Optional: False

### **eventSource**

Der Service, bei dem die Anforderung gestellt wurde. Dieser Name ist normalerweise eine Kurzform des Servicenamens ohne Leerzeichen plus `.amazonaws.com`. Beispielsweise:

- AWS CloudFormation ist `cloudformation.amazonaws.com`.
- Amazon EC2 ist `ec2.amazonaws.com`.
- Amazon Simple Workflow Service ist `swf.amazonaws.com`.

Zu dieser Konvention gibt es einige Ausnahmen. Zum Beispiel CloudWatch ist das `eventSource` für `Amazonmonitoring.amazonaws.com`.

Seit: 1.0

Optional: False

### **eventName**

Die angeforderte Aktion, die eine der Aktionen in der API für diesen Service ist.

Seit: 1.0

Optional: False

### **awsRegion**

Die AWS-Region, an die die Anfrage gestellt wurde, z. `us-east-2` B. Siehe [CloudTrail unterstützte Regionen](#).

Seit: 1.0

Optional: False

## sourceIPAddress

Die IP-Adresse, von der die Anforderung erfolgt ist. Bei Aktionen, die von der Servicekonsole ausgehen, ist die gemeldete Adresse die der zugrunde liegenden Kundenressource, nicht die des Konsolen-Webserverns. Für Dienste in AWS wird nur der DNS-Name angezeigt.

### Note

Bei aus AWS stammenden Ereignissen ist der Inhalt dieses Felds in der Regel `AWS Internal/#`, wobei `#` eine Zahl ist, die für interne Zwecke verwendet wird.

Seit: 1.0

Optional: False

## userAgent

Der Agent, über den die Anfrage gestellt wurde, z. B. der AWS Management Console, ein AWS Dienst, die AWS SDKs oder der AWS CLI. Dieses Feld hat eine maximale Größe von 1 KB; Inhalte, die diesen Grenzwert überschreiten, werden abgeschnitten. Es folgen Beispielwerte:

- `lambda.amazonaws.com` – Die Anforderung wurde mit AWS Lambda erstellt.
- `aws-sdk-java` – Die Anforderung wurde mit AWS SDK for Java erstellt.
- `aws-sdk-ruby` – Die Anforderung wurde mit AWS SDK for Ruby erstellt.
- `aws-cli/1.3.23 Python/2.7.6 Linux/2.6.18-164.el5`— Die Anfrage wurde mit dem auf Linux AWS CLI installierten System gestellt.

### Note

Für Ereignisse, die von AWS, wenn CloudTrail weiß, wer den Aufruf AWS-Service getätigt hat, ausgelöst wurden, ist dieses Feld die Ereignisquelle des aufrufenden Dienstes (zum Beispieler `c2.amazonaws.com`). Andernfalls ist dieses Feld eine Zahl `AWS Internal/#`, `#` die für interne Zwecke verwendet wird.

Seit: 1.0

Optional: Wahr

## **errorCode**

Der AWS Dienstfehler, wenn die Anfrage einen Fehler zurückgibt. Ein Beispiel, das dieses Feld zeigt, finden Sie unter [Beispiel für ein Protokoll mit Fehlercode und Fehlermeldung](#). Dieses Feld hat eine maximale Größe von 1 KB; Inhalte, die diesen Grenzwert überschreiten, werden abgeschnitten.

Seit: 1.0

Optional: Wahr

## **errorMessage**

Die Beschreibung des Fehlers, sofern die Anforderung einen Fehler zurückgegeben hat. Diese Nachricht enthält Meldungen zu Autorisierungsfehlern. CloudTrail erfasst die vom Dienst bei der Ausnahmebehandlung protokollierte Nachricht. Ein Beispiel finden Sie unter [Beispiel für ein Protokoll mit Fehlercode und Fehlermeldung](#). Dieses Feld hat eine maximale Größe von 1 KB; Inhalte, die diesen Grenzwert überschreiten, werden abgeschnitten.

### Note

Einige AWS Dienste stellen die Felder `errorCode` und `errorMessage` als Felder der obersten Ebene für das Ereignis bereit. Andere AWS -Services stellen Fehlerinformationen im Rahmen von `responseElements` bereit.

Seit: 1.0

Optional: Wahr

## **requestParameters**

Die Parameter, die mit der Anforderung gesendet wurden, sofern zutreffend. Diese Parameter sind in der API-Referenzdokumentation für den entsprechenden AWS Dienst dokumentiert. Dieses Feld hat eine maximale Größe von 100 KB; Inhalte, die diesen Grenzwert überschreiten, werden abgeschnitten.

Seit: 1.0

Optional: False

## **responseElements**

Die Antwortelemente, falls vorhanden, für Aktionen, die Änderungen vornehmen (Aktionen erstellen, aktualisieren oder löschen). Wenn die Aktion gibt keine Antwortelemente zurück, dieses Feld schonnull. Wenn eine Aktion ändert den Status nicht (z. B. eine Anforderung, Objekte abzurufen oder aufzulisten), dieses Element wird weggelassen. Die Antwortelemente für Aktionen sind in der API-Referenz dokumentiert Dokumentation für die entsprechenden AWS-Service. Dieses Feld hat eine maximale Größe von 100 KB; Inhalte, die diese Grenze überschreiten, werden gekürzt.

Der `responseElements` Wert hilft Ihnen dabei, eine Anfrage nachzuverfolgen mit AWS Support. Sowohl als `x-amz-request-id` auch `x-amz-id-2` enthalten Informationen, die Ihnen helfen, eine Anfrage nachzuverfolgen AWS Support. Diese Werte sind dieselben wie diejenigen, die der Dienst in der Antwort auf die Anfrage zurückgibt initiiert die Ereignisse, sodass Sie sie verwenden können, um das Ereignis dem zuzuordnen Anfrage.

Seit: 1.0

Optional: False

## **additionalEventData**

Zusätzliche Daten zu dem Ereignis, die nicht Teil der Anforderung oder Antwort waren. Dieses Feld hat eine maximale Größe von 28 KB; Inhalte, die diesen Grenzwert überschreiten, werden abgeschnitten.

Seit: 1.0

Optional: Wahr

## **requestID**

Der Wert, anhand dessen die Anforderung identifiziert wird. Der aufgerufene Service generiert diesen Wert. Dieses Feld hat eine maximale Größe von 1 KB; Inhalte, die diesen Grenzwert überschreiten, werden abgeschnitten.



Seit: 1.01

Optional: Wahr

## eventID

GUID, generiert von CloudTrail , um jedes Ereignis eindeutig zu identifizieren. Sie können diesen Wert verwenden, um ein einzelnes Ereignis zu identifizieren. Beispiel: Sie können die ID als Primärschlüssel zum Abrufen von Protokolldaten aus einer durchsuchbaren Datenbank verwenden.

Seit: 1.01

Optional: False

## eventType

Identifiziert den Typ des Ereignisses, das den Ereignisdatensatz generiert hat. Dabei kann es sich um einen der folgenden Werte handeln:

- `AwsApiCall` – Eine API wurde aufgerufen.
- [AwsServiceEvent](#) – Der Service hat ein Ereignis mit Bezug zu Ihrem Trail generiert. Beispiel: Dies kann auftreten, wenn ein anderes Konto einen Aufruf mit einer Ressource getätigt hat, deren Eigentümer Sie sind.
- `AwsConsoleAction` – In der Konsole wurde eine Aktion ausgeführt, die kein API-Aufruf war.
- [AwsConsoleSignIn](#)— Ein Benutzer in Ihrem Konto (root, IAM, Federated, SAML oder SwitchRole) hat sich bei dem angemeldet. AWS Management Console
- [AwsCloudTrailInsight](#)— Wenn Insights-Ereignisse aktiviert sind, werden Insights-Ereignisse CloudTrail generiert, wenn ungewöhnliche betriebliche Aktivitäten wie Spitzenwerte bei der Ressourcenbereitstellung oder Ausbrüche von (IAM-) Aktionen CloudTrail erkannt werden. AWS Identity and Access Management

`AwsCloudTrailInsight`-Ereignisse verwenden nicht die folgenden Felder:

- `eventName`
- `eventSource`
- `sourceIPAddress`
- `userAgent`

- `userIdentity`

Seit: 1.02

Optional: False

## **apiVersion**

Identifiziert die API-Version, die dem Wert `AwsApiCall` `eventType` zugeordnet ist.

Seit: 1.01

Optional: Wahr

## **managementEvent**

Ein boolescher Wert, der angibt, ob es sich bei dem Ereignis um ein Verwaltungsereignis handelt. `managementEvent` wird in einem Ereignisdatensatz angezeigt, wenn `eventVersion` 1.06 oder höher und der Ereignistyp einer der folgenden ist:

- `AwsApiCall`
- `AwsConsoleAction`
- `AwsConsoleSignIn`
- `AwsServiceEvent`

Seit: 1.06

Optional: Wahr

## **readOnly**

Gibt an, ob es sich um einen schreibgeschützten Vorgang handelt. Dabei kann es sich um einen der folgenden Werte handeln:

- `true` – Der Vorgang ist schreibgeschützt (z. B. `DescribeTrails`).
- `false` – Der Vorgang ist lesegeschützt (z. B. `DeleteTrail`).

Seit: 1.01

Optional: Wahr

## resources

Eine Liste der Ressourcen, auf die bei dem Ereignis zugegriffen wurde. Das Feld kann die folgenden Informationen enthalten:

- Ressourcen-ARNs
- Konto-ID des Ressourceneigentümers
- Ressourcentyp-ID im folgenden Format: `AWS::aws-service-name::data-type-name`

Wenn beispielsweise ein AssumeRole-Ereignis protokolliert wird, kann das Feld `resources` wie folgt angezeigt werden:

- ARN: `arn:aws:iam::123456789012:role/myRole`
- Konto-ID: 123456789012
- Ressourcentyp-ID: `AWS::IAM::Role`

Logs mit dem `resources` Feld finden Sie beispielsweise unter [AWS STS API-Ereignis in CloudTrail Protokolldatei im IAM-Benutzerhandbuch](#) oder [Protokollierung von AWS KMS API-Aufrufen](#) im Entwicklerhandbuch.AWS Key Management Service

Seit: 1.01

Optional: Wahr

## recipientAccountId

Repräsentiert die Konto-ID, die das Ereignis empfangen hat. Die `recipientAccountId` kann von der [CloudTrail Element „userIdentity“](#) `accountId` abweichen. Dies kann bei kontoübergreifendem Ressourcenzugriff vorkommen. Wenn beispielsweise ein KMS-Schlüssel, auch als [AWS KMS key](#) bezeichnet, von einem separaten Konto verwendet wurde, um die [Verschlüsselungs-API](#) aufzurufen, sind die Werte `accountId` und `recipientAccountId` für das Ereignis, das an das Konto gesendet wird, von dem der Aufruf stammt, dieselben, aber die Werte für das Ereignis, das an das Konto übermittelt werden, das Eigentümer des KMS-Schlüssel ist, weichen ab.

Seit: 1.02

Optional: Wahr

## serviceEventDetails

Identifiziert das Serviceereignis, einschließlich des Auslösers des Ereignisses und des Ergebnisses. Weitere Informationen finden Sie unter [AWS Serviceereignisse](#). Dieses Feld hat eine maximale Größe von 100 KB; Inhalte, die diesen Grenzwert überschreiten, werden abgeschnitten.

Seit: 1.05

Optional: Wahr

## sharedEventID

GUID, generiert von CloudTrail, um CloudTrail Ereignisse aus derselben AWS Aktion, die an verschiedene AWS Konten gesendet wurde, eindeutig zu identifizieren.

Wenn ein Konto beispielsweise ein Konto verwendet, [AWS KMS key](#) das zu einem anderen Konto gehört, erhalten das Konto, das den KMS-Schlüssel verwendet hat, und das Konto, das den KMS-Schlüssel besitzt, separate CloudTrail Ereignisse für dieselbe Aktion. Jedes CloudTrail Ereignis, das für diese AWS Aktion bereitgestellt wird, hat dasselbe `sharedEventID`, hat aber auch ein eindeutiges `eventID` und `recipientAccountID`.

Weitere Informationen finden Sie unter [Beispiel für die sharedEventID](#).

### Note

Das `sharedEventID` Feld ist nur vorhanden, wenn CloudTrail Ereignisse an mehrere Konten übermittelt werden. Wenn der Anrufer und der Besitzer dasselbe AWS Konto haben, wird nur ein Ereignis CloudTrail gesendet und das `sharedEventID` Feld ist nicht vorhanden.

Seit: 1.03

Optional: Wahr

## vpcEndpointId

Identifiziert den VPC-Endpunkt, von dem aus Anforderungen aus einer VPC an einen anderen AWS -Service getätigt wurden, z. B. Amazon S3.

Seit: 1.04

Optional: Wahr

## eventCategory

Zeigt die Ereigniskategorie an. Das eventCategory wird in [LookupEvents](#)Aufrufen für Management- und Insights-Veranstaltungen verwendet.

- Bei Verwaltungsereignissen lautet der Wert Management.
- Bei Datenereignissen lautet der Wert Data.
- Bei Insights-Ereignissen lautet der Wert Insight.

Seit: 1.07

Optional: False

## addendum

Wenn eine Ereigniszustellung verzögert wurde oder zusätzliche Informationen zu einem vorhandenen Ereignis verfügbar werden, nachdem das Ereignis protokolliert wurde, zeigt ein Zusatzfeld Informationen darüber an, warum das Ereignis verzögert wurde. Wenn Informationen zu einem bestehenden Ereignis fehlten, enthält das Nachtragsfeld die fehlenden Informationen und einen Grund für das Fehlen. Die Inhalte sind folgende.

- **reason** – Der Grund, dass das Ereignis oder einige seiner Inhalte fehlten. Werte können einer der folgenden sein.
  - **DELIVERY\_DELAY**— Es gab eine Verzögerung bei der Lieferung von Ereignissen. Dies kann durch hohen Netzwerkverkehr, Verbindungsprobleme oder ein CloudTrail Serviceproblem verursacht werden.
  - **UPDATED\_DATA** – Ein Feld im Ereignisdatensatz fehlte oder hatte einen falschen Wert.
  - **SERVICE\_OUTAGE**— Ein Dienst, der Ereignisse protokolliert, CloudTrail hatte einen Ausfall und konnte keine Ereignisse protokollieren. CloudTrail Dies ist außergewöhnlich selten.
- **updatedFields** – Die Ereignisdatensatzfelder, die durch das Addendum aktualisiert werden. Dies wird nur angegeben, wenn der Grund UPDATED\_DATA ist.
- **originalRequestID** – Die ursprüngliche eindeutige ID der Anfrage. Dies wird nur angegeben, wenn der Grund UPDATED\_DATA ist.
- **originalEventID** – Die ursprüngliche Ereignis-ID. Dies wird nur angegeben, wenn der Grund UPDATED\_DATA ist.

Seit: 1.08

Optional: Wahr

### **sessionCredentialFromConsole**

Zeigt an, ob ein Ereignis aus einer AWS Management Console Sitzung stammt oder nicht. Dieses Feld wird nur angezeigt, wenn der Wert `true` ist, was bedeutet, dass der Client, der für den API-Aufruf verwendet wurde, entweder ein Proxy oder ein externer Client war. Wenn ein Proxy-Client verwendet wurde, wird das `tlsDetails`-Ereignisfeld nicht angezeigt.

Seit: 1.08

Optional: Wahr

### **edgeDeviceDetails**

Zeigt Informationen zu Edge-Geräten an, die Ziele einer Anforderung sind. Derzeit enthalten [S3 Outposts](#)-Gerät ereignisse dieses Feld. Dieses Feld hat eine maximale Größe von 28 KB; Inhalte, die diesen Grenzwert überschreiten, werden abgeschnitten.

Seit: 1.08

Optional: Wahr

### **tlsDetails**

Zeigt Informationen über die TLS-Version (Transport Layer Security), die Cipher Suites und den vollqualifizierten Domännennamen (FQDN) des vom Client bereitgestellten Hostnamens an, der im Service-API-Aufruf verwendet wird. Dabei handelt es sich in der Regel um den FQDN des Dienstendpunkts. CloudTrail protokolliert weiterhin teilweise TLS-Details, wenn die erwarteten Informationen fehlen oder leer sind. Wenn beispielsweise die TLS-Version und die Cipher Suite vorhanden sind, der `HOST` Header jedoch leer ist, werden die verfügbaren TLS-Details dennoch im CloudTrail Ereignis protokolliert.

- **tlsVersion** – Die TLS-Version einer Anfrage.
- **cipherSuite** – Die Verschlüsselungssuite (Kombination der verwendeten Sicherheitsalgorithmen) einer Anfrage.
- **clientProvidedHostHeader** – Der vom Client bereitgestellte Hostname, der im Service-API-Aufruf verwendet wird, der normalerweise der FQDN des Serviceendpunkts ist.

#### Note

Es gibt Fälle, in denen das Feld `tlsDetails` in einem Ereignisdatensatz nicht vorhanden ist.

- Das `tlsDetails` Feld ist nicht vorhanden, wenn der API-Aufruf von einem in AWS-Service Ihrem Namen getätigt wurde. Das Feld `invokedBy` im `userIdentity`-Element identifiziert den AWS-Service, der den API-Aufruf ausgeführt hat.
- Wenn `sessionCredentialFromConsole` mit dem Wert „Wahr“ vorliegt, ist `tlsDetails` nur dann in einem Ereignisdatensatz vorhanden, wenn ein externer Client für den API-Aufruf verwendet wurde.

Seit: 1.08

Optional: Wahr

## Datensatzfelder von Insights-Ereignissen

Unten sind die Attribute aufgeführt, die in der JSON-Struktur eines Insights-Ereignisses angezeigt werden und sich von den Attributen eines Verwaltungs- oder Datenereignisses unterscheiden.

### **sharedEventId**

A `sharedEventID` für CloudTrail Insights-Ereignisse unterscheidet sich von den CloudTrail Ereignissen `sharedEventID` für die Verwaltung und die Datentypen. Bei Insights-Ereignissen `sharedEventID` ist eine GUID, die von CloudTrail Insights generiert wird, um ein Insights-Ereignis eindeutig zu identifizieren. `sharedEventID` ist bei Insights-Start- und Endereignissen üblich und hilft dabei, beide Ereignisse miteinander zu verbinden, um ungewöhnliche Aktivitäten eindeutig zu identifizieren. Sie können sich die `sharedEventID` als allgemeine ID für Insights-Ereignisse vorstellen.

Seit: 1.07

Optional: False

### **insightDetails**

Nur Insights-Ereignisse. Zeigt Informationen zu den zugrunde liegenden Triggern eines Insights-Ereignisses an, z. B. Ereignisquelle, Benutzeragent, Statistiken, API-Name und ob es sich bei dem Ereignis um den Beginn oder das Ende des Insights-Ereignisses handelt. Weitere Informationen über den Inhalt des Blocks `insightDetails` finden Sie unter [CloudTrail insightDetailsElement „Einblicke“](#).

Seit: 1.07

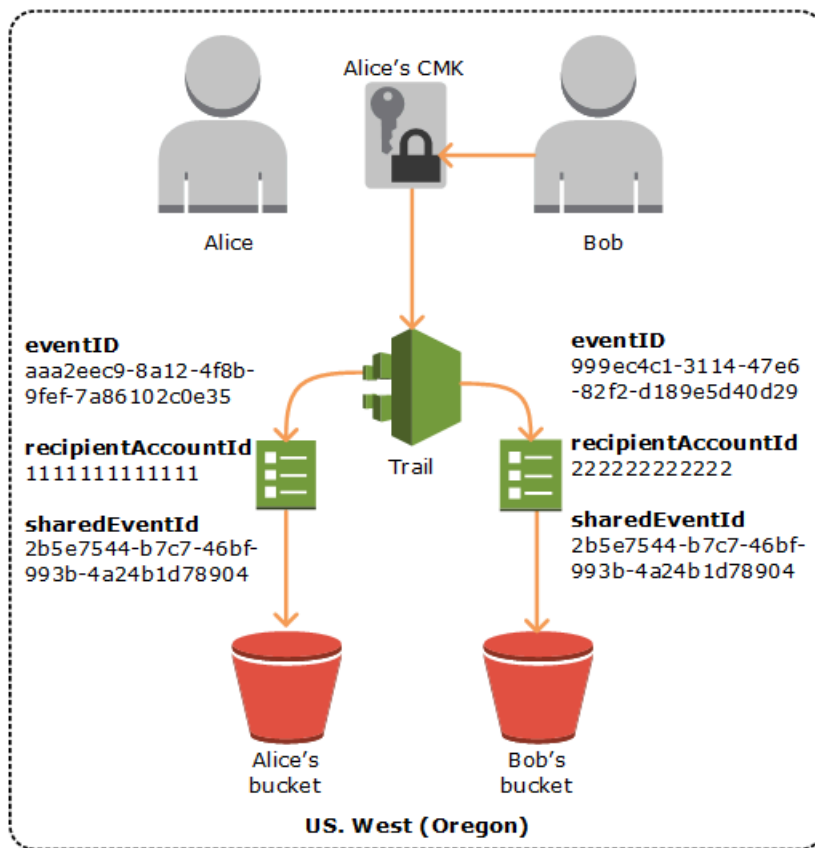
Optional: False

## Beispiel für die sharedEventID

Im folgenden Beispiel wird beschrieben, wie CloudTrail zwei Ereignisse für dieselbe Aktion ausgelöst werden:

1. Alice hat ein AWS Konto (111111111111) und erstellt ein AWS KMS key Sie ist der Eigentümer des KMS-Schlüssels.
2. Bob hat AWS ein Konto (222222222222). Alice weist Bob die Berechtigung zur Verwendung des KMS-Schlüssel zu.
3. Jedes Konto verfügt über einen Trail und einen separaten Bucket.
4. Bob verwendet den KMS-Schlüssel, um die Encrypt-API aufzurufen.
5. CloudTrail sendet zwei separate Ereignisse.
  - Ein Ereignis wird an Bob gesendet. Das Ereignis zeigt, dass er den KMS-Schlüssel verwendet hat.
  - Ein Ereignis wird an Alice gesendet. Das Ereignis zeigt, dass Bob den KMS-Schlüssel verwendet hat.
  - Die Ereignisse haben dieselbe sharedEventID, aber eventID und recipientAccountID sind eindeutig.





## Geteilte Ereignis-IDs in CloudTrail Insights

A sharedEventID für CloudTrail Insights-Ereignisse unterscheidet sich von den CloudTrail Ereignissen sharedEventID für die Verwaltung und die Datentypen. Bei Insights-Ereignissen sharedEventID ist eine GUID, die von CloudTrail Insights generiert wird, um ein Start- und Endpaar von Insights-Ereignissen eindeutig zu identifizieren. sharedEventID ist zwischen dem Start- und dem Endereignis von Insights üblich und hilft dabei, eine Korrelation zwischen beiden Ereignissen herzustellen, um ungewöhnliche Aktivitäten eindeutig zu identifizieren.

Sie können sich die sharedEventID als allgemeine ID für Insights-Ereignisse vorstellen.

## CloudTrail Element „userIdentity“

AWS Identity and Access Management (IAM) bietet verschiedene Arten von Identitäten. Das userIdentity-Element enthält Details über die Art der für die Abfrage genutzten IAM-Identität und dazu, welche Anmeldeinformationen verwendet wurden. Wenn temporäre Anmeldeinformationen verwendet wurden, zeigt das Element, wie die Anmeldeinformationen erhalten wurden.

### Inhalt

- [Beispiele](#)
- [Felder](#)
- [Werte für AWS STS APIs mit SAML und Web-Identitätsverbund](#)
- [AWS STS Quellidentität](#)

## Beispiele

### **userIdentity** mit IAM-Benutzeranmeldeinformationen

Das folgende Beispiel zeigt das `userIdentity`-Element einer einfachen Anforderung mit den Anmeldeinformationen des IAM-Benutzers namens Alice.

```
"userIdentity": {
  "type": "IAMUser",
  "principalId": "AIDAJ45Q7YFFAREXAMPLE",
  "arn": "arn:aws:iam::123456789012:user/Alice",
  "accountId": "123456789012",
  "accessKeyId": "",
  "userName": "Alice"
}
```

### **userIdentity** mit temporären Sicherheitsanmeldeinformationen

Das folgende Beispiel zeigt ein `userIdentity`-Element für eine Anforderung mit temporären Sicherheitsanmeldeinformationen, die durch Annahme einer IAM-Rolle erhalten wurden. Das Element enthält weitere Informationen über die Rolle, die angenommen wurde, um Anmeldeinformationen zu erhalten.

```
"userIdentity": {
  "type": "AssumedRole",
  "principalId": "AROAI DPPEZS35WEXAMPLE:AssumedRoleSessionName",
  "arn": "arn:aws:sts::123456789012:assumed-role/RoleToBeAssumed/MySessionName",
  "accountId": "123456789012",
  "accessKeyId": "",
  "sessionContext": {
    "attributes": {
      "mfaAuthenticated": "false",
      "creationDate": "20131102T010628Z"
    }
  },
}
```

```
    "sessionIssuer": {
      "type": "Role",
      "principalId": "AROAIIDPPEZS35WEXAMPLE",
      "arn": "arn:aws:iam::123456789012:role/RoleToBeAssumed",
      "accountId": "123456789012",
      "userName": "RoleToBeAssumed"
    }
  }
}
```

**userIdentity** für eine Anforderung, die im Namen eines IAM-Identity-Center-Benutzers erstellt wurde

Das folgende Beispiel zeigt ein `userIdentity`-Element für eine Anforderung, die im Namen eines IAM-Identity-Center-Benutzers erstellt wurde.

```
"userIdentity": {
  "type": "IdentityCenterUser",
  "accountId": "123456789012",
  "onBehalfOf": {
    "userId": "544894e8-80c1-707f-60e3-3ba6510dfac1",
    "identityStoreArn": "arn:aws:identitystore::123456789012:identitystore/d-9067642ac7"
  },
  "credentialId": "EXAMPLEVHULjJdTUdPJfofVa1sufHDoj7aYc0YcxFV1lWR_Whr1fEXAMPLE"
}
```

## Felder

Die folgenden Felder können in einem `userIdentity` Element erscheinen.

### **type**

Die Art der Identität. Die folgenden Werte sind möglich:

- **Root**— Die Anfrage wurde mit Ihren AWS-Konto Anmeldeinformationen gestellt. Wenn der `userIdentity`-Typ `Root` lautet und Sie einen Alias für das Konto festlegen, enthält das Feld `userName` den Konto-Alias. Weitere Informationen finden Sie unter [Ihre AWS-Konto -ID und der zugehörige Alias](#).
- **IAMUser** – Die Anforderung wurde mit den Anmeldeinformationen eines IAM-Benutzers erstellt.
- **AssumedRole** – Die Anforderung wurde mit temporären Sicherheitsanmeldeinformationen erstellt, die mit einer Rolle durch einen Aufruf der AWS Security Token Service (AWS STS)

[AssumeRole](#) API erhalten wurden. Dies kann [Rollen für Amazon EC2](#) und kontoübergreifenden API-Zugriff beinhalten.

- `Role` – Die Anforderung wurde mit einer dauerhaften IAM-Identität, die über bestimmte Berechtigungen verfügt, erstellt. Der Aussteller der Rollensitzungen ist immer die Rolle. Weitere Informationen zu Rollen finden Sie unter [Begriffe und Konzepte zu Rollen](#) im IAM-Benutzerhandbuch.
- `FederatedUser`— Die Anfrage wurde mit temporären Sicherheitsanmeldedaten gestellt, die durch einen API-Aufruf abgerufen wurden. AWS STS [GetFederationToken](#) Das `sessionIssuer`-Element gibt an, wenn die API mit Root oder IAM-Benutzer-Anmeldeinformationen aufgerufen wurde.

Weitere Informationen zu temporären Anmeldeinformationen finden Sie unter [Temporäre Sicherheitsanmeldeinformationen](#) im IAM-Benutzerhandbuch.

- `Directory` – Die Anforderung wurde an einen Directory Service gestellt und der Typ ist unbekannt. Zu den Verzeichnisdiensten gehören: Amazon WorkDocs und Amazon QuickSight.
- `AWSAccount`— Die Anfrage wurde von einem anderen gestellt AWS-Konto
- `AWSService`— Die Anfrage wurde von einem gestellt AWS-Konto , der einem gehört AWS-Service. AWS Elastic Beanstalk Nimmt beispielsweise eine IAM-Rolle in Ihrem Konto an, um in Ihrem Namen andere AWS-Services Personen anzurufen.
- `IdentityCenterUser`: Die Anforderung wurde im Namen eines IAM-Identity-Center-Benutzers erstellt.
- `Unknown`— Die Anfrage wurde mit einem Identitätstyp gestellt, der nicht bestimmt CloudTrail werden kann.

Optional: False

`AWSAccount` und `AWSService` werden in den Protokollen für `type` angezeigt, wenn ein kontoübergreifender Zugriff über eine IAM-Rolle erfolgt, die Sie besitzen.

Beispiel: von einem anderen AWS -Konto initiiertes kontoübergreifendes Zugriff

1. Sie besitzen eine IAM-Rolle in Ihrem Konto.
2. Ein anderes AWS Konto wechselt zu dieser Rolle, um die Rolle für Ihr Konto zu übernehmen.
3. Da Sie die IAM-Rolle besitzen, erhalten Sie ein Protokoll, aus dem hervorgeht, dass das andere Konto die Rolle übernommen hat. Der `type` ist `AWSAccount`. Ein Beispiel für einen Protokolleintrag finden Sie unter [AWS STS API-Ereignis in der CloudTrail Protokolldatei](#).

Beispiel: Kontoübergreifender Zugriff, der von einem AWS Dienst initiiert wurde


1. Sie besitzen eine IAM-Rolle in Ihrem Konto.
2. Ein AWS Konto, das einem AWS Dienst gehört, übernimmt diese Rolle.
3. Da Sie die IAM-Rolle besitzen, erhalten Sie ein Protokoll, aus dem hervorgeht, dass der AWS -Service die Rolle angenommen hat. Das type ist AWSService.

## userName

Der Anzeigename der Identität, von der der Aufruf stammt. Der angezeigte Wert userName basiert auf dem in type angegebenen Wert. Die folgende Tabelle zeigt das Verhältnis zwischen type und userName:

type	userName	Beschreibung
Root (kein Alias festgelegt)	Nicht vorhanden	Wenn Sie keinen Alias für Ihren eingerichtet haben AWS-Konto, wird das userName Feld nicht angezeigt. Weitere Informationen zu Kontoaliasnamen finden Sie unter <a href="#">Ihre AWS-Konto ID und ihr Alias</a> . Beachten Sie bitte, dass das Feld userName niemals den Wert Root enthält, da es sich bei Root um einen Identitätstyp und nicht um einen Benutzernamen handelt.
Root (Stamm) (kein Alias festgelegt)	Konto-Alias	Weitere Informationen zu AWS-Konto Aliasnamen findest du unter <a href="#">Deine AWS-Konto ID und ihr Alias</a> .
IAMUser	Der Benutzername des IAM-Benutzers	
AssumedRole	Nicht vorhanden	Im Fall des Typs AssumedRole finden Sie das Feld userName in sessionContext als Teil des <a href="#">sessionIssuer</a> -Elements. Einen Beispieleintrag finden Sie unter <a href="#">Beispiele</a> .

type	userName	Beschreibung
Role	Benutzerdefiniert	Die Abschnitte <code>sessionContext</code> und <code>sessionIssuer</code> enthalten Informationen über die Identität, die die Sitzung für die Rolle erstellt hat.
FederatedUser	Nicht vorhanden	Die Abschnitte <code>sessionContext</code> und <code>sessionIssuer</code> enthalten Informationen über die Identität, die die Sitzung für den Verbundbenutzer erstellt hat.
Directory	Kann vorhanden sein	Der Wert kann beispielsweise der <a href="#">Kontoalias</a> oder die E-Mail-Adresse der zugehörigen <a href="#">AWS-Konto-ID</a> sein.
AWSservice	Nicht vorhanden	
AWSAccount	Nicht vorhanden	
IdentityCenterUser	Nicht vorhanden	Der Abschnitt <code>onBehalfOf</code> enthält Informationen zur ID des IAM-Identity-Center-Benutzers und zum Identitätsspeicher-ARN, für den der Aufruf durchgeführt wurde. Weitere Informationen zu IAM Identity Center finden Sie im <a href="#">Benutzerhandbuch von AWS IAM Identity Center</a> .
Unknown	Kann vorhanden sein	Der Wert kann beispielsweise der <a href="#">Kontoalias</a> oder die E-Mail-Adresse der zugehörigen <a href="#">AWS-Konto-ID</a> sein.

 Note

Das `userName`-Feld enthält die Zeichenfolge, `HIDDEN_DUE_TO_SECURITY_REASONS`, wenn das aufgezeichnete Ereignis einen Konsole-Anmeldefehler durch Eingabe eines

falschen Benutzernamens angibt. CloudTrail zeichnet den Inhalt in diesem Fall nicht auf, da der Text vertrauliche Informationen enthalten könnte, wie in den folgenden Beispielen:

- Ein Benutzer gibt versehentlich ein Passwort im Feld für den Benutzernamen ein.
- Ein Benutzer klickt auf den Link für die Anmeldeseite eines AWS Kontos, gibt dann aber die Kontonummer für ein anderes Konto ein.
- Ein Benutzer gibt versehentlich den Kontonamen eines persönlichen E-Mail-Kontos, eine Bank-Anmelde-ID oder eine andere private ID ein.

Optional: Wahr

### **principalId**

Eine eindeutige ID für die Entität, von der der Aufruf stammt. Bei Abfragen mit temporären Sicherheitsanmeldeinformationen enthält dieser Wert den Sitzungsnamen, der an `AssumeRole`, `AssumeRoleWithWebIdentity` übergeben wurde, oder den `GetFederationToken` API-Aufruf.

Optional: Wahr

### **arn**

Der Amazon-Ressourcenname (ARN) des Prinzipals, von dem der Aufruf stammt. Der letzte Abschnitt des ARN enthält den Benutzer oder die Rolle, von dem/der der Aufruf stammt.

Optional: Wahr

### **accountId**

Das Konto, das die Entität besitzt, die die Berechtigungen für die Anforderung erteilte. Wenn die Anforderung mittels temporärer Sicherheitsanmeldeinformationen erfolgte, ist dies das Konto mit dem IAM-Benutzer oder der Rolle, der bzw. die verwendet wurde, um die Anmeldeinformationen abzurufen.

Wenn die Anforderung mit einem für IAM Identity Center autorisierten Zugriffstoken erstellt wurde, ist dies das Konto, zu dem die IAM-Identity-Center-Instance gehört.

Optional: Wahr

### **accessKeyId**

Die -Zugriffsschlüssel-ID, die zum Signieren der Abfrage verwendet wurde. Erfolgte die Abfrage mittels temporärer Sicherheitsanmeldeinformationen, ist dies die Zugriffsschlüssel-ID der

temporären Anmeldeinformationen. Aus Sicherheitsgründen ist `accessKeyId` möglicherweise nicht vorhanden oder wird als leere Zeichenfolge angezeigt.

Optional: Wahr

## **sessionContext**

Erfolgte die Anforderung mittels temporärer Sicherheitsanmeldeinformationen, stellt `sessionContext` die Informationen über die Sitzung bereit, die für diese Anmeldeinformationen erstellt wurde. Sitzungen werden erstellt, wenn eine API aufgerufen wird, die temporäre Anmeldeinformationen zurückgibt. Sitzungen werden auch erstellt, wenn Benutzer in der Konsole arbeiten und Anforderungen mit APIs erstellen, die eine [Multifaktor-Authentifizierung](#) umfassen. Dieses Element hat die folgenden Attribute:

- `creationDate` – Das Datum und die Uhrzeit, zu dem/der die temporären Sicherheitsanmeldeinformationen ausgestellt wurden. Dargestellt in ISO 8601 grundlegende Notation.
- `mfaAuthenticated`: Der Wert ist `true`, wenn der Root-Benutzer oder der IAM-Benutzer, dessen Anmeldeinformationen für die Anforderung verwendet wurden, auch über ein MFA-Gerät authentifiziert wurde. Anderenfalls lautet der Wert `false`.
- `sourceIdentity` – Weitere Informationen finden Sie unter [AWS STS Quellidentität](#) in diesem Thema. Das Feld `sourceIdentity` tritt in Ereignissen auf, wenn Benutzer eine IAM-Rolle annehmen, um eine Aktion auszuführen. `sourceIdentity` identifiziert die ursprüngliche Benutzeridentität, die die Anforderung erstellt, unabhängig davon, ob es sich bei der Identität um einen IAM-Benutzer, eine IAM-Rolle, einen Benutzer, der über einen SAML-basierten Verbund authentifiziert wurde, oder einen Benutzer handelt, der über einen OpenID Connect (OIDC)-konformen Web-Identitätsverbund authentifiziert wurde. Weitere Informationen AWS STS zur Konfiguration der Erfassung von Quellidentitätsinformationen finden Sie im IAM-Benutzerhandbuch unter [Überwachen und Steuern von Aktionen, die mit übernommenen Rollen ergriffen wurden](#).
- `ec2RoleDelivery` – Der Wert ist `1.0`, wenn die Anmeldeinformationen von Amazon EC2 Instance Metadata Service Version 1 (IMDSv1) bereitgestellt wurden. Der Wert ist `2.0`, wenn die Anmeldeinformationen mithilfe des neuen IMDS-Schemas bereitgestellt wurden.

AWS Die vom Amazon EC2 Instance Metadata Service (IMDS) bereitgestellten Anmeldeinformationen beinhalten einen `ec2: RoleDelivery` IAM-Kontextschlüssel. Dieser Kontextschlüssel macht es einfach, die Verwendung des neuen Schemas auf `resource-by-resource` Or-Basis zu erzwingen, indem der Kontextschlüssel als Bedingung in IAM-Richtlinien, Ressourcenrichtlinien `service-by-service` oder Service-Kontrollrichtlinien verwendet wird.



AWS Organizations Weitere Informationen dazu finden Sie unter [Instance-Metadaten und Benutzerdaten](#) im Amazon-EC2-Benutzerhandbuch für Linux-Instances.

Optional: Wahr

### **invokedBy**

Der Name desjenigen AWS-Service, der die Anfrage gestellt hat, wenn eine Anfrage von einem AWS-Service wie Amazon EC2 Auto Scaling oder AWS Elastic Beanstalk gestellt wird. Dieses Feld ist nur vorhanden, wenn eine Anfrage von einem AWS-Service gestellt wird. Dazu gehören Anfragen von Diensten, die Forward Access Sessions (FAS), AWS-Service Principals, dienstverknüpfte Rollen oder von einem verwendete Servicerollen verwenden. AWS-Service

Optional: Wahr

### **sessionIssuer**

Erfolgte die Anforderung mittels temporärer Sicherheitsanmeldeinformationen, gibt `sessionIssuer` Auskunft darüber, wie die Anmeldeinformationen abgerufen wurden. Wurden die temporären Sicherheitsanmeldeinformationen beispielsweise durch Annahme einer Rolle abgerufen, gibt dieses Element Auskunft über die entsprechende Rolle. Wurden die Anmeldeinformationen mit Root- oder IAM-Benutzer-Anmeldeinformationen abgerufen, um AWS STS `GetFederationToken` aufzurufen, stellt das Element Informationen zum Root-Konto oder IAM-Benutzer bereit. Dieses Element hat die folgenden Attribute:

- `type` – Die Quelle der temporären Sicherheitsanmeldeinformationen wie z. B. `Root` (Stamm), `IAMUser` (IAM-Benutzer) oder `Role` (Rolle).
- `userName` – Der Anzeigename des Benutzers oder der Rolle, die die Sitzung erstellt hat. Der angezeigte Wert ist vom `sessionIssuer`-Identitäts-type abhängig. Die folgende Tabelle zeigt das Verhältnis zwischen `sessionIssuer type` und `userName`:

<b>sessionIssuer - Typ</b>	<b>userName</b>	Beschreibung
Root (kein Alias festgelegt)	Nicht vorhanden	Wenn Sie für das Konto keinen Alias festgelegt haben, wird das <code>userName</code> -Feld nicht angezeigt. Weitere Informationen zu AWS-Konto Aliasnamen finden Sie unter <a href="#">Ihre AWS-Konto ID</a> und ihr Alias. Beachten Sie bitte, dass das Feld <code>userName</code> niemals den Wert <code>Root</code> enthält, da

<b>sessionIssuer</b> - Typ	<b>userName</b>	Beschreibung
		es sich bei Root um einen Identitätstyp und nicht um einen Benutzernamen handelt.
Root (Stamm) (kein Alias festgelegt)	Konto-Alias	Weitere Informationen zu AWS-Konto Aliasnamen findest du unter <a href="#">Deine AWS Konto-ID und ihr Alias</a> .
IAMUser	Der Benutzername des IAM-Benutzers	Dies gilt auch, wenn ein verbundener Benutzer eine Sitzung verwendet, die von einem IAMUser erstellt wurde.
Role	Rollenname	Eine Rolle, AWS-Service die von einem IAM-Benutzer oder einem Verbundbenutzer mit Web-Identität in einer Rollensitzung übernommen wurde.

- **principalId**: Die interne ID der Entität, die verwendet wurde, um die Anmeldeinformationen abzurufen.
- **arn** – Der ARN der Quelle (Konto, IAM-Benutzer oder Rolle), der verwendet wurde, um die temporären Sicherheitsanmeldeinformationen zu erhalten.
- **accountId** – Das Konto, das die Entität besitzt, die verwendet wurde, um die Anmeldeinformationen zu erhalten.

Optional: Wahr

## **onBehalfOf**

Wenn die Anforderung von einem IAM-Identity-Center-Aufrufer erstellt wurde, stellt **onBehalfOf** Informationen zur ID des IAM-Identity-Center-Benutzers und zum Identitätsspeicher-ARN bereit, für den der Aufruf getätigt wurde. Dieses Element hat die folgenden Attribute:

- **userId**: Die ID des IAM-Identity-Center-Benutzers, in dessen Namen der Aufruf getätigt wurde.
- **identityStoreArn**: Die ID des IAM-Identity-Center-Identitätsspeichers, in dessen Namen der Aufruf getätigt wurde.

Optional: Wahr

## credentialId

Die Anmeldeinformationen-ID für die Anforderung. Dies wird nur festgelegt, wenn der Aufrufer ein Bearer-Token verwendet, z. B. ein für IAM Identity Center autorisiertes Zugriffstoken.

Optional: Wahr

## webIdFederationData

Erfolgte die Anforderung mittels temporärer Anmeldeinformationen, die durch einen [Web-Identitätsverbund](#) abgerufen wurden, führt `webIdFederationData` Informationen zum Identitätsanbieter auf.

Dieses Element hat die folgenden Attribute:

- `federatedProvider` – Der Prinzipal-Name des Identitätsanbieters (z. B. `www.amazon.com` für Login with Amazon oder `accounts.google.com` für Google).
- `attributes` – Die Anwendungs-ID und Benutzer-ID, wie sie vom Anbieter gemeldet wurden (z. B. `www.amazon.com:app_id` und `www.amazon.com:user_id` für Login with Amazon).

### Note

Das Weglassen dieses Felds oder das Vorhandensein dieses Felds mit einem leeren Wert bedeutet, dass keine Informationen über den Identitätsanbieter vorliegen.

Optional: Wahr

## Werte für AWS STS APIs mit SAML und Web-Identitätsverbund

AWS CloudTrail unterstützt Logging AWS Security Token Service (AWS STS) -API-Aufrufe, die mit Security Assertion Markup Language (SAML) und Web Identity Federation getätigt wurden. Wenn ein Benutzer die [AssumeRoleWithWebIdentity](#) APIs [AssumeRoleWithSAML](#) aufruft, CloudTrail zeichnet er den Anruf auf und übermittelt das Ereignis an Ihren Amazon S3 S3-Bucket.

Das `userIdentity`-Element für diese APIs enthält die folgenden Werte:

### type

Den Identitätstyp.

- `SAMLUser` – Die Abfrage erfolgte mit SAML-Zusicherung.

- `WebIdentityUser` – Die Abfrage erfolgte über einen Web-Identitätsverbundanbieter.

## **principalId**

Eine eindeutige ID für die Entität, von der der Aufruf stammt.

- Bei einem `SAMLUser` ist dies eine Kombination aus `saml:namequalifier` und `saml:sub`-Schlüsseln.
- Bei einem `WebIdentityUser` ist dies eine Kombination aus dem Aussteller, Anwendungs-ID und Benutzer-ID.

## **userName**

Der Name der Identität, über die der Aufruf getätigt wurde.

- Bei einem `SAMLUser` ist dies der `saml:sub`-Schlüssel.
- Bei einem `WebIdentityUser` ist dies die Benutzer-ID.

## **identityProvider**

Der Prinzipal-Name des externen Identitätsanbieters. Dieses Feld wird nur bei `SAMLUser` oder `WebIdentityUser`-Typen angezeigt.

- Bei einem `SAMLUser` ist dies der `saml:namequalifier`-Schlüssel für die SAML-Zusicherung.
- Bei einem `WebIdentityUser` ist dies der Aussteller-Name des Web-Identitätsverbundanbieters. Hierbei kann es sich um einen Anbieter, den Sie konfiguriert haben, handeln wie z .B.:
  - `cognito-identity.amazon.com` für Amazon Cognito
  - `www.amazon.com` für Login with Amazon
  - `accounts.google.com` für Google
  - `graph.facebook.com` für Facebook

Nachstehend finden Sie ein Beispiel eines `userIdentity`-Elements (Benutzeridentität) für die `AssumeRoleWithWebIdentity`-Aktion (Übernahme einer Rolle mit der Web-Identität).

```
"userIdentity": {
  "type": "WebIdentityUser",
  "principalId": "accounts.google.com:application-id.apps.googleusercontent.com:user-id",
  "userName": "user-id",
```

```
"identityProvider": "accounts.google.com"  
}
```

Logs darüber, wie das `userIdentity` Element angezeigt wird `SAMLUser` und welche `WebIdentityUser` Typen es gibt, finden Sie unter [Protokollieren von IAM- und AWS STS API-Aufrufen mit AWS CloudTrail](#).

## AWS STS Quellidentität

Ein IAM-Administrator kann so konfigurieren AWS Security Token Service , dass Benutzer ihre Identität angeben müssen, wenn sie temporäre Anmeldeinformationen verwenden, um Rollen zu übernehmen. Das Feld `sourceIdentity` tritt in Ereignissen auf, wenn Benutzer eine IAM-Rolle annehmen oder Aktionen mit der angenommenen Rolle ausführen.

Das `sourceIdentity`-Feld identifiziert die ursprüngliche Benutzeridentität, die die Anforderung stellt, unabhängig davon, ob es sich bei der Identität dieses Benutzers um einen IAM-Benutzer, eine IAM-Rolle, einen Benutzer, der mit einem SAML-basierten Verbund authentifiziert wurde, oder einen Benutzer handelt, der mit einem OpenID-Connect-(OIDC)-konformen Web-Identitätsverbund authentifiziert wurde. Nach der Konfiguration durch den IAM-Administrator werden AWS STS `sourceIdentity` Informationen zu den folgenden Ereignissen und Orten im Ereignisdatensatz CloudTrail protokolliert:

- Die AWS STS `AssumeRole`, oder `AssumeRoleWithWebIdentity` - Aufrufe `AssumeRoleWithSAML`, die eine Benutzeridentität tätigt, wenn sie eine Rolle übernimmt. `sourceIdentity` befindet sich im `requestParameters` Block der AWS STS Aufrufe.
- Die `AssumeRoleWithWebIdentity` Aufrufe AWS STS `AssumeRole`, oder `AssumeRoleWithSAML`, die eine Benutzeridentität tätigt, wenn sie eine Rolle verwendet, um eine andere Rolle anzunehmen. Dies wird als [Rollenverkettung](#) bezeichnet. `sourceIdentity` befindet sich im `requestParameters` Block der AWS STS Aufrufe.
- Die AWS Service-API ruft auf, die die Benutzeridentität ausgibt, während sie eine Rolle annimmt und die temporären Anmeldeinformationen verwendet, die von zugewiesen wurden AWS STS. In Service-API-Ereignissen befindet sich `sourceIdentity` im `sessionContext`-Block. Wenn beispielsweise eine Benutzeridentität einen neuen S3 Bucket erstellt, kommt `sourceIdentity` im `sessionContext`-Block des `CreateBucket`-Ereignisses vor.

Weitere Informationen AWS STS zur Konfiguration der Erfassung von Quellidentitätsinformationen finden Sie im IAM-Benutzerhandbuch unter [Überwachen und Steuern von Aktionen, die mit](#)

[übernommenen Rollen ergriffen wurden](#). Weitere Informationen zu AWS STS Ereignissen, die protokolliert werden CloudTrail, finden Sie AWS CloudTrail im [IAM-Benutzerhandbuch unter Protokollieren von IAM- und AWS STS API-Aufrufen mit](#).

Im Folgenden finden Sie Beispielausschnitte von Ereignissen, die das `sourceIdentity`-Feld anzeigen.

### Beispiel Abschnitt **requestParameters**

Im folgenden Beispiel-Event-Snippet stellt ein Benutzer eine AWS STS AssumeRole Anfrage und legt eine Quellidentität fest, hier dargestellt durch *source-identity-value-set*. Der Benutzer übernimmt eine Rolle, die durch die Rollen-ARN `arn:aws:iam::123456789012:role/Assumed_Role` repräsentiert wird. Das `sourceIdentity`-Feld befindet sich im `requestParameters`-Block des Ereignisses.

```
"eventVersion": "1.05",
  "userIdentity": {
    "type": "AWSAccount",
    "principalId": "AIDAJ45Q7YFFAREXAMPLE",
    "accountId": "123456789012"
  },
  "eventTime": "2020-04-02T18:20:53Z",
  "eventSource": "sts.amazonaws.com",
  "eventName": "AssumeRole",
  "awsRegion": "us-east-1",
  "sourceIPAddress": "203.0.113.64",
  "userAgent": "aws-cli/1.16.96 Python/3.6.0 Windows/10 botocore/1.12.86",
  "requestParameters": {
    "roleArn": "arn:aws:iam::123456789012:role/Assumed_Role",
    "roleSessionName": "Test1",
    "sourceIdentity": "source-identity-value-set",
  },
```

### Beispiel Abschnitt **responseElements**

Im folgenden Beispiel-Event-Snippet stellt ein Benutzer eine AWS STS AssumeRole Anfrage zur Übernahme einer Rolle mit dem Namen und legt eine `Developer_Role` Quellidentität fest. Admin Der Benutzer übernimmt eine Rolle, die durch die Rollen-ARN `arn:aws:iam::111122223333:role/Developer_Role` repräsentiert wird. Das `sourceIdentity`-Feld befindet sich in den `requestParameters`- und `responseElements`-Blöcken des Ereignisses. Die temporären Anmeldeinformationen, die zum Annehmen der

Rolle verwendet wurden, die Zeichenfolge des Sitzungstokens und die ID der angenommenen Rolle, der Sitzungsname und der Sitzungs-ARN werden zusammen mit der Quellidentität im `responseElements`-Block angezeigt.

```

"requestParameters": {
  "roleArn": "arn:aws:iam::111122223333:role/Developer_Role",
  "roleSessionName": "Session_Name",
  "sourceIdentity": "Admin"
},
"responseElements": {
  "credentials": {
    "accessKeyId": "ASIAIOSFODNN7EXAMPLE",
    "expiration": "Jan 22, 2021 12:46:28 AM",
    "sessionToken": "XXYYaz...
                    EXAMPLE_SESSION_TOKEN
                    XXyYaZAz"
  },
  "assumedRoleUser": {
    "assumedRoleId": "AR0ACKCEVSQ6C2EXAMPLE:Session_Name",
    "arn": "arn:aws:sts::111122223333:assumed-role/Developer_Role/Session_Name"
  },
  "sourceIdentity": "Admin"
}
...

```

### Beispiel Abschnitt `sessionContext`

Im folgenden Beispiel-Event-Snippet nimmt ein Benutzer eine Rolle an, die `DevRole` zum Aufrufen einer Service-API benannt ist. AWS Der Benutzer legt eine Quellidentität fest, hier dargestellt durch *`source-identity-value-set`*. Das `sourceIdentity`-Feld befindet sich im `sessionContext`-Block, innerhalb des `userIdentity`-Blocks des Ereignisses.

```

{
  "eventVersion": "1.08",
  "userIdentity": {
    "type": "AssumedRole",
    "principalId": "AR0AJ45Q7YFFAREXAMPLE: Dev1",
    "arn": "arn:aws:sts: : 123456789012: assumed-role/DevRole/Dev1",
    "accountId": "123456789012",
    "accessKeyId": "ASIAIOSFODNN7EXAMPLE",
    "sessionContext": {
      "sessionIssuer": {

```

```
    "type": "Role",
    "principalId": "AR0AJ45Q7YFFAREXAMPLE",
    "arn": "arn: aws: iam: : 123456789012: role/DevRole",
    "accountId": "123456789012",
    "userName": "DevRole"
  },
  "webIdFederationData": {},
  "attributes": {
    "mfaAuthenticated": "false",
    "creationDate": "2021-02-21T23: 46: 28Z"
  },
  "sourceIdentity": "source-identity-value-set"
}
}
```

## CloudTrail **insightDetails**Element „Einblicke“

AWS CloudTrail Insights-Ereignisdatensätze enthalten Felder, die sich in ihrer JSON-Struktur, die manchmal auch als Payload bezeichnet wird, von anderen CloudTrail Ereignissen unterscheiden. Ein CloudTrail Insights-Ereignisdatensatz umfasst einen `insightDetails` Block, der Informationen über die zugrunde liegenden Auslöser eines Insights-Ereignisses enthält, wie z. B. die Ereignisquelle, Benutzeridentitäten, Benutzeragenten, historische Durchschnittswerte oder Basislinien, Statistiken, den API-Namen und ob das Ereignis der Beginn oder das Ende des Insights-Ereignisses ist. Der `insightDetails`-Block enthält die folgenden Informationen.

- **state** – Ob das Ereignis das Start- oder End-Insights-Ereignis ist. Dabei kann es sich um den Wert `Start` oder `End` handeln.

Seit: 1.07

Optional: False

- **eventSource**— Der AWS Service-Endpunkt, der die Quelle der ungewöhnlichen Aktivität war, z. B. `ec2.amazonaws.com`

Seit: 1.07

Optional: False

- **eventName** – Der Name des Insights-Ereignisses, normalerweise der Name der API, die die Quelle der ungewöhnlichen Aktivität war.



Seit: 1.07

Optional: False

- **insightType** – Der Typ des Insights-Ereignisses. Dabei kann es sich um den Wert `ApiCallRateInsight`, `ApiErrorRateInsight` oder beide Werte handeln.

Seit: 1.07

Optional: False

- **insightContext** -

Informationen zu den AWS Tools (als Benutzeragenten bezeichnet), zu IAM-Benutzern und -Rollen (als Benutzeridentitäten bezeichnet) sowie zu den Fehlercodes im Zusammenhang mit den Ereignissen, die zur Generierung des Insights-Ereignisses CloudTrail analysiert wurden. Dieses Element enthält auch Statistiken, die zeigen, wie die ungewöhnliche Aktivität in einem Insights-Ereignis im Vergleich zum Ausgangswert oder der normalen Aktivität abschneidet.

Seit: 1.07

Optional: False

- **statistics** – Enthält Daten über den Ausgangswert oder die typische durchschnittliche Rate der Aufrufe oder Fehler der Subject-API durch ein Konto, gemessen während des Ausgangszeitraums, die durchschnittliche Rate der Aufrufe oder Fehler, die das Insights-Ereignis in der ersten Minute des Insights-Ereignisses ausgelöst haben, die Dauer des Insights-Ereignisses in Minuten und die Dauer des Ausgangswert-Messzeitraums in Minuten.

Seit: 1.07

Optional: False

- **baseline** – Die durchschnittliche Anzahl von API-Aufrufen oder -Fehlern pro Minute während der Ausgangswert-Dauer der Themen-API des Insights-Ereignisses für das Konto, berechnet über die sieben Tage vor dem Start des Insights-Ereignisses.

Seit: 1.07

Optional: False

- **insight** -

Für ein beginnendes Insights-Ereignis ist dieser Wert die durchschnittliche Anzahl von API-Aufrufen oder -Fehlern pro Minute während des Starts der ungewöhnlichen Aktivität. Für ein endendes Insights-Ereignis ist dieser Wert die durchschnittliche Anzahl von API-Aufrufen oder -Fehlern pro Minute über die Dauer der ungewöhnlichen Aktivität.

Seit: 1.07

Optional: False

- **insightDuration** – Die Dauer eines Insights-Ereignisses in Minuten (der Zeitraum vom Beginn bis zum Ende einer ungewöhnlichen Aktivität in der betreffenden API). `insightDuration` tritt sowohl beim Starten als auch beim Beenden von Insights-Ereignissen auf.

Seit: 1.07

Optional: False

- **baselineDuration** – Die Dauer des Baseline-Zeitraums (in Minuten) (der Zeitraum, in dem die normale Aktivität an der betreffenden API gemessen wird). `baselineDuration` sind mindestens die sieben Tage (10 080 Minuten) vor einem Insights-Ereignis. Dieses Feld kommt sowohl in beginnenden als auch in beendenden Insights-Ereignissen vor. Der Endzeitpunkt der `baselineDuration`-Messung ist immer der Beginn eines Insights-Ereignisses.

Seit: 1.07

Optional: False

- **attributions** – Dieser Block enthält Informationen zu den Benutzeridentitäten, Benutzeragenten und Fehlercodes, die mit ungewöhnlichen und grundlegenden Aktivitäten korreliert sind. In einem Insights-Ereignis-`attributions`-Block werden maximal fünf Benutzeridentitäten, fünf Benutzeragenten und fünf Fehlercodes erfasst, sortiert nach dem Durchschnitt der Aktivitätsanzahl in absteigender Reihenfolge vom höchsten zum niedrigsten Wert.

Seit: 1.07

Optional: Wahr

- **attribute** – Enthält den Attributtyp. Werte können Folgende sein: `userIdentityArn`, `userAgent` oder `errorCode`.

- **userIdentityArn**— Ein Block, in dem die fünf wichtigsten AWS Benutzer oder IAM-Rollen angezeigt werden, die in den ungewöhnlichen Aktivitäts- und Basiszeiträumen zu API-Aufrufen oder Fehlern beigetragen haben. Siehe auch `userIdentity` in [CloudTrail Inhalt aufzeichnen](#).

Seit: 1.07

Optional: False

- **insight** – Ein Block, der in absteigender Reihenfolge von der größten bis zur kleinsten Anzahl von API-Aufrufen bis zu den fünf häufigsten Benutzeridentitäts-ARNs anzeigt, die zu den API-Aufrufen während des ungewöhnlichen Aktivitätszeitraums beigetragen haben. Es zeigt auch die durchschnittliche Anzahl von API-Aufrufen an, die von den Benutzeridentitäten während des ungewöhnlichen Aktivitätszeitraums getätigt wurden.

Seit: 1.07

Optional: False

- **value** – Der ARN einer der fünf häufigsten Benutzeridentitäten, die zu den API-Aufrufen während des ungewöhnlichen Aktivitätszeitraums beigetragen haben.

Seit: 1.07

Optional: False

- **average** – Die Anzahl der API-Aufrufe oder -Fehler pro Minute während des ungewöhnlichen Aktivitätszeitraums für die Benutzeridentität im `value`-Feld.

Seit: 1.07

Optional: False

- **baseline** – Ein Block, der bis zu den fünf wichtigsten Benutzeridentitäts-ARNs anzeigt, die am meisten zu den API-Aufrufen oder -Fehlern während des normalen Aktivitätszeitraums beigetragen haben. Es zeigt auch die durchschnittliche Anzahl von API-Aufrufen oder -Fehlern an, die von den Benutzeridentitäten während des normalen Aktivitätszeitraums protokolliert wurden.

Seit: 1.07

Optional: False

- **value** – Der ARN einer der fünf häufigsten Benutzeridentitäten, die zu den API-Aufrufen oder -Fehlern während des normalen Aktivitätszeitraums beigetragen haben.

Seit: 1.07

Optional: False

- **average** – Der historische Durchschnitt der API-Aufrufe oder -Fehler pro Minute während der sieben Tage vor der Startzeit der Insights-Aktivität für den Benutzeridentitäten im `value`-Feld.

Seit: 1.07

Optional: False

- **userAgent** – Ein Block, in dem die fünf wichtigsten AWS Tools angezeigt werden, mit denen die Benutzeridentität in den ungewöhnlichen Aktivitäts- und Basiszeiträumen zu API-Aufrufen beigetragen hat. Zu diesen Tools gehören die AWS Management Console AWS CLI, oder die AWS SDKs. Siehe auch `userAgent` in [CloudTrail Inhalt aufzeichnen](#).

Seit: 1.07

Optional: False

- **insight** – Ein Block, der in absteigender Reihenfolge von der größten bis zur kleinsten Anzahl von API-Aufrufen bis zu den fünf häufigsten Benutzeragenten anzeigt, die zu den API-Aufrufen während des ungewöhnlichen Aktivitätszeitraums beigetragen haben. Es zeigt auch die durchschnittliche Anzahl der API-Aufrufe oder -Fehler an, die von den Benutzeragenten während des ungewöhnlichen Aktivitätszeitraums protokolliert wurden.

Seit: 1.07

Optional: False

- **value** – Einer der fünf häufigsten Benutzeragenten, der zu den API-Aufrufen während des ungewöhnlichen Aktivitätszeitraums beigetragen hat.

Seit: 1.07

Optional: False

- **average** – Die Anzahl der API-Aufrufe oder protokollierten Fehler pro Minute während des ungewöhnlichen Aktivitätszeitraums für den Benutzeragenten im `value`-Feld.

Seit: 1.07

Optional: False

- **baseline** – Ein Block, der bis zu den fünf wichtigsten Benutzeragenten anzeigt, die am meisten zu den API-Aufrufen während des normalen Aktivitätszeitraums beigetragen haben. Es zeigt auch die durchschnittliche Anzahl der API-Aufrufe oder -Fehler an, die von den Benutzeragenten während des normalen Aktivitätszeitraums protokolliert wurden.

Seit: 1.07

Optional: False

- **value** – Einer der fünf häufigsten Benutzeragenten, der zu den API-Aufrufen oder protokollierten Fehlern während des normalen Aktivitätszeitraums beigetragen hat.

Seit: 1.07

Optional: False

- **average** – Der historische Durchschnitt der API-Aufrufe oder -Fehler pro Minute während der sieben Tage vor der Startzeit der Insights-Aktivität für den Benutzeragenten im `value`-Feld.

Seit: 1.07

Optional: False

- **errorCode** – Ein Block, der die fünf häufigsten Fehlercodes anzeigt, die bei API-Aufrufen während der ungewöhnlichen Aktivitäts- und Baseline-Zeiträume aufgetreten sind, in absteigender Reihenfolge von der größten zur kleinsten Anzahl von API-Aufrufen. Siehe auch `errorCode` in [CloudTrail Inhalt aufzeichnen](#).

Seit: 1.07

Optional: False

- **insight** – Ein Block, der bis zu den fünf häufigsten Fehlercodes anzeigt, die bei den API-Aufrufen während des ungewöhnlichen Aktivitätszeitraums aufgetreten sind, in absteigender Reihenfolge von der größten Anzahl der zugeordneten API-Aufrufe zur kleinsten. Es zeigt auch die durchschnittliche Anzahl von API-Aufrufen an, bei denen die Fehler während des ungewöhnlichen Aktivitätszeitraums aufgetreten sind.

Seit: 1.07

Optional: False

- **value** – Einer der fünf häufigsten Fehlercodes, die bei den API-Aufrufen während des ungewöhnlichen Aktivitätszeitraums aufgetreten sind, z. B. `AccessDeniedException`.

Wenn keiner der Aufrufe, die das Insights-Ereignis ausgelöst haben, zu Fehlern geführt hat, ist dieser Wert `null`.

Seit: 1.07

Optional: False

- **average** – Die Anzahl der API-Aufrufe pro Minute während des ungewöhnlichen Aktivitätszeitraums für den Fehlercode im `value`-Feld.

Wenn der Fehlercodewert `null` ist und keine anderen Fehlercodes im `insight`-Block vorhanden sind, ist der Wert von `average` der gleiche wie im `statistics`-Block für das Insights-Ereignis insgesamt.

Seit: 1.07

Optional: False

- **baseline** – Ein Block, der bis zu den fünf häufigsten Fehlercodes anzeigt, die bei den API-Aufrufen während des normalen Aktivitätszeitraums aufgetreten sind. Es zeigt auch die durchschnittliche Anzahl der API-Aufrufe an, die von den Benutzeragenten während des normalen Aktivitätszeitraums getätigt wurden.

Seit: 1.07

Optional: False

- **value** – Einer der fünf häufigsten Fehlercodes, die bei den API-Aufrufen während des normalen Aktivitätszeitraums aufgetreten sind, z. B. `AccessDeniedException`.

Seit: 1.07

Optional: False

- **average** – Der historische Durchschnitt der API-Aufrufe oder -Fehler pro Minute während der sieben Tage vor der Startzeit der Insights-Aktivität für den Fehlercode im `value`-Feld.

Seit: 1.07

Optional: False

## Beispiel-**insightDetails**-Block

Im Folgenden finden Sie ein Beispiel für einen Insights-Ereignis-`insightDetails`-Block für ein Insights-Ereignis, das auftrat, wenn die `Application-Auto-Scaling-API CompleteLifecycleAction` ungewöhnlich oft aufgerufen wurde. Ein Beispiel für ein vollständiges Insights-Ereignis finden Sie unter [Einblicke und Ereignisse](#).

Dieses Beispiel stammt aus einem beginnenden Insights-Ereignis, das durch `"state": "Start"` angezeigt wird. Die wichtigsten Benutzeridentitäten, die die mit dem Insights-Ereignis verknüpften APIs aufgerufen haben, `CodeDeployRole1`, `CodeDeployRole2` und `CodeDeployRole3`, werden im `attributions`-Block zusammen mit ihren durchschnittlichen API-Aufrufzahlen für dieses Insights-Ereignis und der Ausgangswert für die `CodeDeployRole1`-Rolle angezeigt. Der `attributions` Block zeigt auch, dass der Benutzeragent `codedeploy.amazonaws.com`, d. h. die wichtigsten Benutzeridentitäten, die AWS CodeDeploy Konsole verwendet haben, um die API-Aufrufe auszuführen.

Da den Ereignissen, die analysiert wurden, um das Insights-Ereignis zu generieren, keine Fehlercodes zugeordnet sind (der Wert ist `null`), entspricht der `insight`-Durchschnitt für den Fehlercode dem gesamten `insight`-Durchschnitt für das gesamte Insights-Ereignis, der im `statistics`-Block angezeigt wird.

```
"insightDetails": {
  "state": "Start",
  "eventSource": "autoscaling.amazonaws.com",
  "eventName": "CompleteLifecycleAction",
  "insightType": "ApiCallRateInsight",
  "insightContext": {
    "statistics": {
      "baseline": {
        "average": 0.0000882145
      }
    }
  },
}
```

```
    "insight": {
      "average": 0.6
    },
    "insightDuration": 5,
    "baselineDuration": 11336
  },
  "attributions": [
    {
      "attribute": "userIdentityArn",
      "insight": [
        {
          "value": "arn:aws:sts::012345678901:assumed-role/
CodeDeployRole1",
          "average": 0.2
        },
        {
          "value": "arn:aws:sts::012345678901:assumed-role/
CodeDeployRole2",
          "average": 0.2
        },
        {
          "value": "arn:aws:sts::012345678901:assumed-role/
CodeDeployRole3",
          "average": 0.2
        }
      ],
      "baseline": [
        {
          "value": "arn:aws:sts::012345678901:assumed-role/
CodeDeployRole1",
          "average": 0.0000882145
        }
      ]
    },
    {
      "attribute": "userAgent",
      "insight": [
        {
          "value": "codedeploy.amazonaws.com",
          "average": 0.6
        }
      ],
      "baseline": [
        {
```



```
        "value": "codedeploy.amazonaws.com",
        "average": 0.0000882145
      }
    ],
  },
  {
    "attribute": "errorCode",
    "insight": [
      {
        "value": "null",
        "average": 0.6
      }
    ],
    "baseline": [
      {
        "value": "null",
        "average": 0.0000882145
      }
    ]
  }
]
}
```

## Nicht-API-Ereignisse, erfasst von CloudTrail

CloudTrail erfasst neben der Protokollierung von AWS API-Aufrufen auch andere verwandte Ereignisse, die sich auf die Sicherheit oder die Einhaltung von Vorschriften auf Ihr AWS Konto auswirken könnten oder die Ihnen bei der Behebung betrieblicher Probleme helfen könnten.

### Themen

- [AWS Serviceereignisse](#)
- [AWS Management Console Anmeldeereignisse](#)

## AWS Serviceereignisse

CloudTrail unterstützt die Protokollierung von Nicht-API-Dienstereignissen. Diese Ereignisse werden von AWS Diensten erzeugt, aber nicht direkt durch eine Anfrage an eine öffentliche AWS API ausgelöst. Für diese Ereignisse lautet das `eventType`-Feld `AwsServiceEvent`.

Im Folgenden finden Sie ein Beispielszenario für ein AWS Serviceereignis, bei dem ein vom Kunden verwalteter Schlüssel automatisch eingewechselt wird AWS Key Management Service (AWS KMS). Weitere Informationen zum Rotieren der KMS-Schlüssel finden Sie unter [Rotieren von KMS-Kundenmasterschlüsseln](#).

```
{
  "eventVersion": "1.05",
  "userIdentity": {
    "accountId": "123456789012",
    "invokedBy": "AWS Internal"
  },
  "eventTime": "2019-06-02T00:06:08Z",
  "eventSource": "kms.amazonaws.com",
  "eventName": "RotateKey",
  "awsRegion": "us-east-2",
  "sourceIPAddress": "AWS Internal",
  "userAgent": "AWS Internal",
  "requestParameters": null,
  "responseElements": null,
  "eventID": "234f004b-EXAMPLE",
  "readOnly": false,
  "resources": [
    {
      "ARN": "arn:aws:kms:us-east-2:123456789012:key/7944f0ec-EXAMPLE",
      "accountId": "123456789012",
      "type": "AWS::KMS::Key"
    }
  ],
  "eventType": "AwsServiceEvent",
  "recipientAccountId": "123456789012",
  "serviceEventDetails": {
    "keyId": "7944f0ec-EXAMPLE"
  }
}
```

## AWS Management Console Anmeldeereignisse

CloudTrail protokolliert Versuche AWS Management Console, sich in den AWS Diskussionsforen und im AWS Support Center anzumelden. Alle Anmeldeereignisse für IAM-Benutzer und Root-Benutzer sowie alle Anmeldeereignisse von Verbundbenutzern generieren Datensätze in Protokolldateien. CloudTrail Weitere Informationen zum Suchen und Anzeigen von Protokollen finden Sie unter [Finden Sie Ihre Protokolldateien CloudTrail](#) und [Deine CloudTrail Logdateien herunterladen](#).

**Note**

Die in einem ConsoleLogin Ereignis aufgezeichnete Region hängt vom Benutzertyp und davon ab, ob Sie einen globalen oder regionalen Endpunkt für die Anmeldung verwenden.

- Wenn Sie sich als Root-Benutzer anmelden, CloudTrail zeichnet das Ereignis in us-east-1 auf.
- Wenn Sie sich mit einem IAM-Benutzer anmelden und den globalen Endpunkt verwenden, CloudTrail zeichnet die Region des ConsoleLogin Ereignisses wie folgt auf:
  - Wenn ein Konto-Alias-Cookie im Browser vorhanden ist, wird das ConsoleLogin Ereignis in einer der folgenden Regionen CloudTrail aufgezeichnet: us-east-2, eu-north-1 oder ap-southeast-2. Das liegt daran, dass der Konsolen-Proxy den Benutzer auf der Grundlage der Latenz vom Anmeldeort des Benutzers umleitet.
  - Wenn im Browser kein Konto-Alias-Cookie vorhanden ist, wird das ConsoleLogin Ereignis in us-east-1 CloudTrail aufgezeichnet. Das liegt daran, dass der Konsolen-Proxy zur globalen Anmeldung zurückleitet.
- Wenn Sie sich mit einem IAM-Benutzer anmelden und einen [regionalen Endpunkt](#) verwenden, CloudTrail zeichnet das ConsoleLogin Ereignis in der entsprechenden Region für den Endpunkt auf. Weitere Informationen zu AWS-Anmeldung Endpunkten finden Sie unter [AWS-Anmeldung Endpunkte und Kontingente](#).

## Themen

- [Beispielhafte Ereignisdatensätze für IAM-Benutzer](#)
- [Beispiel-Ereignisdatensätze für Stamm-Benutzer](#)
- [Beispielhafte Ereignisdatensätze für Verbundbenutzer](#)

## Beispielhafte Ereignisdatensätze für IAM-Benutzer

Die folgenden Beispiele zeigen Ereignisdatensätze für mehrere IAM-Benutzeranmeldeszenarien.

## Themen

- [IAM-Benutzer, erfolgreiche Anmeldung ohne MFA](#)
- [IAM-Benutzer, erfolgreiche Anmeldung mit MFA](#)
- [IAM-Benutzer, erfolglose Anmeldung](#)

- [IAM-Benutzer, Anmeldeprozess überprüft auf MFA \(einzelner MFA-Gerätetyp\)](#)
- [IAM-Benutzer, Anmeldeprozess überprüft auf MFA \(mehrere MFA-Gerätetypen\)](#)

## IAM-Benutzer, erfolgreiche Anmeldung ohne MFA

Der folgende Datensatz zeigt, dass sich ein Benutzer mit dem Namen Anaya erfolgreich bei der angemeldet hat, AWS Management Console ohne die Multi-Faktor-Authentifizierung (MFA) zu verwenden.

```
{
  "eventVersion": "1.08",
  "userIdentity": {
    "type": "IAMUser",
    "principalId": "EXAMPLE6E4XEGITWATV6R",
    "arn": "arn:aws:iam::999999999999:user/Anaya",
    "accountId": "999999999999",
    "userName": "Anaya"
  },
  "eventTime": "2023-07-19T21:44:40Z",
  "eventSource": "signin.amazonaws.com",
  "eventName": "ConsoleLogin",
  "awsRegion": "us-east-1",
  "sourceIPAddress": "192.0.2.0",
  "userAgent": "Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:102.0) Gecko/20100101
Firefox/102.0",
  "requestParameters": null,
  "responseElements": {
    "ConsoleLogin": "Success"
  },
  "additionalEventData": {
    "LoginTo": "https://console.aws.amazon.com/console/home?hashArgs=
%23&isauthcode=true&state=hashArgsFromTB_us-east-1_examplee9aba7f8",
    "MobileVersion": "No",
    "MFAUsed": "No"
  },
  "eventID": "e1bf1000-86a4-4a78-81d7-EXAMPLE83102",
  "readOnly": false,
  "eventType": "AwsConsoleSignIn",
  "managementEvent": true,
  "recipientAccountId": "999999999999",
  "eventCategory": "Management",
  "tlsDetails": {
```

```

    "tlsVersion": "TLSv1.3",
    "cipherSuite": "TLS_AES_128_GCM_SHA256",
    "clientProvidedHostHeader": "us-east-1.signin.aws.amazon.com"
  }
}

```

## IAM-Benutzer, erfolgreiche Anmeldung mit MFA

Der folgende Datensatz zeigt, dass sich ein IAM-Benutzer AWS Management Console mit dem Namen „Multi-Factor Authentication“ (MFA) Anaya erfolgreich bei der Multi-Factor Authentication (MFA) angemeldet hat.

```

{
  "eventVersion": "1.08",
  "userIdentity": {
    "type": "IAMUser",
    "principalId": "EXAMPLE6E4XEGITWATV6R",
    "arn": "arn:aws:iam::999999999999:user/Anaya",
    "accountId": "999999999999",
    "userName": "Anaya"
  },
  "eventTime": "2023-07-19T22:01:30Z",
  "eventSource": "signin.amazonaws.com",
  "eventName": "ConsoleLogin",
  "awsRegion": "us-east-1",
  "sourceIPAddress": "192.0.2.0",
  "userAgent": "Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:102.0) Gecko/20100101 Firefox/102.0",
  "requestParameters": null,
  "responseElements": {
    "ConsoleLogin": "Success"
  },
  "additionalEventData": {
    "LoginTo": "https://console.aws.amazon.com/console/home?hashArgs=%23&isauthcode=true&state=hashArgsFromTB_us-east-1_examplebde32f3c9",
    "MobileVersion": "No",
    "MFAIdentifier": "arn:aws:iam::999999999999:mfa/mfa-device",
    "MFAUsed": "Yes"
  },
  "eventID": "e1f76697-5beb-46e8-9cfc-EXAMPLEbde31",
  "readOnly": false,
  "eventType": "AwsConsoleSignIn",
  "managementEvent": true,

```

```
"recipientAccountId": "999999999999",
"eventCategory": "Management",
"tlsDetails": {
  "tlsVersion": "TLSv1.3",
  "cipherSuite": "TLS_AES_128_GCM_SHA256",
  "clientProvidedHostHeader": "us-east-1.signin.aws.amazon.com"
}
}
```

## IAM-Benutzer, erfolgreiche Anmeldung

Der folgende Datensatz zeigt die erfolgreiche Anmeldung eines IAM-Benutzers mit dem Namen Paulo.

```
{
  "eventVersion": "1.08",
  "userIdentity": {
    "type": "IAMUser",
    "principalId": "EXAMPLE6E4XEGITWATV6R",
    "accountId": "123456789012",
    "accessKeyId": "",
    "userName": "Paulo"
  },
  "eventTime": "2023-07-19T22:01:20Z",
  "eventSource": "signin.amazonaws.com",
  "eventName": "ConsoleLogin",
  "awsRegion": "us-east-1",
  "sourceIPAddress": "192.0.2.0",
  "userAgent": "Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:102.0) Gecko/20100101
Firefox/102.0",
  "errorMessage": "Failed authentication",
  "requestParameters": null,
  "responseElements": {
    "ConsoleLogin": "Failure"
  },
  "additionalEventData": {
    "LoginTo": "https://console.aws.amazon.com/console/home?hashArgs=
%23&isauthcode=true&state=hashArgsFromTB_us-east-1_examplebde32f3c9",
    "MobileVersion": "No",
    "MFAUsed": "Yes"
  },
  "eventID": "66c97220-2b7d-43b6-a7a0-EXAMPLEbae9c",
  "readOnly": false,
  "eventType": "AwsConsoleSignIn",
  "managementEvent": true,
```

```
"recipientAccountId": "123456789012",
"eventCategory": "Management",
"tlsDetails": {
  "tlsVersion": "TLSv1.3",
  "cipherSuite": "TLS_AES_128_GCM_SHA256",
  "clientProvidedHostHeader": "us-east-1.signin.aws.amazon.com"
}
}
```

## IAM-Benutzer, Anmeldeprozess überprüft auf MFA (einzelner MFA-Gerätetyp)

Das folgende Beispiel zeigt, dass der Anmeldeprozess überprüft, ob für einen IAM-Benutzer während der Anmeldung Multi-Faktor-Authentifizierung (MFA) erforderlich ist. In diesem Beispiel hat `mfaType` den Wert `U2F MFA`. Das weist darauf hin, dass der IAM-Benutzer ein einzelnes MFA-Gerät oder mehrere MFA-Geräte desselben Typs aktiviert hat (`U2F MFA`).

```
{
  "eventVersion": "1.08",
  "userIdentity": {
    "type": "IAMUser",
    "principalId": "EXAMPLE6E4XEGITWATV6R",
    "accountId": "123456789012",
    "accessKeyId": "",
    "userName": "Alice"
  },
  "eventTime": "2023-07-19T22:01:26Z",
  "eventSource": "signin.amazonaws.com",
  "eventName": "CheckMfa",
  "awsRegion": "us-east-1",
  "sourceIPAddress": "192.0.2.0",
  "userAgent": "Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:102.0) Gecko/20100101
Firefox/102.0",
  "requestParameters": null,
  "responseElements": {
    "CheckMfa": "Success"
  },
  "additionalEventData": {
    "MfaType": "Virtual MFA"
  },
  "eventID": "7d8a0746-b2e7-44f5-9917-EXAMPLEfb77c",
  "readOnly": false,
  "eventType": "AwsConsoleSignIn",
  "managementEvent": true,
```

```
"recipientAccountId": "123456789012",
"eventCategory": "Management",
"tlsDetails": {
  "tlsVersion": "TLSv1.3",
  "cipherSuite": "TLS_AES_128_GCM_SHA256",
  "clientProvidedHostHeader": "us-east-1.signin.aws.amazon.com"
}
}
```

## IAM-Benutzer, Anmeldeprozess überprüft auf MFA (mehrere MFA-Gerätetypen)

Das folgende Beispiel zeigt, dass der Anmeldeprozess überprüft, ob für einen IAM-Benutzer während der Anmeldung Multi-Faktor-Authentifizierung (MFA) erforderlich ist. In diesem Beispiel lautet der Wert von `mfaType` `Multiple MFA Devices`. Das weist darauf hin, dass der IAM-Benutzer mehrere MFA-Gerätetypen aktiviert hat.

```
{
  "eventVersion": "1.08",
  "userIdentity": {
    "type": "IAMUser",
    "principalId": "EXAMPLE6E4XEGITWATV6R",
    "accountId": "123456789012",
    "accessKeyId": "",
    "userName": "Mary"
  },
  "eventTime": "2023-07-19T23:10:09Z",
  "eventSource": "signin.amazonaws.com",
  "eventName": "CheckMfa",
  "awsRegion": "us-east-1",
  "sourceIPAddress": "192.0.2.0",
  "userAgent": "Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:102.0) Gecko/20100101
Firefox/102.0",
  "requestParameters": null,
  "responseElements": {
    "CheckMfa": "Success"
  },
  "additionalEventData": {
    "MfaType": "Multiple MFA Devices"
  },
  "eventID": "19bd1a1c-76b1-4806-9d8f-EXAMPLE02a96",
  "readOnly": false,
  "eventType": "AwsConsoleSignIn",
  "managementEvent": true,
```



```
"recipientAccountId": "123456789012",
"eventCategory": "Management",
"tlsDetails": {
  "tlsVersion": "TLSv1.3",
  "cipherSuite": "TLS_AES_128_GCM_SHA256",
  "clientProvidedHostHeader": "signin.aws.amazon.com"
}
}
```

## Beispiel-Ereignisdatensätze für Stamm-Benutzer

Die folgenden Beispiele stellen Ereignisdatensätze für mehrereroot-Szenarien für die Benutzeranmeldung. Wenn Sie sich mit dem Root-Benutzer anmelden, CloudTrail zeichnet das ConsoleLogin Ereignis in us-east-1 auf.

### Themen

- [Root-Benutzer, erfolgreiche Anmeldung ohne MFA](#)
- [Root-Benutzer, erfolgreiche Anmeldung mit MFA](#)
- [Nicht erfolgreiche Anmeldungen für Stammbenutzer](#)
- [Stammbenutzer, MFA geändert](#)
- [Stamm-Benutzer, Kennwort geändert](#)

### Root-Benutzer, erfolgreiche Anmeldung ohne MFA

Das folgende Beispiel zeigt das Ereignis einer erfolgreichen Anmeldung für einen Root-Benutzer, der keine Multi-Faktor-Authentifizierung (MFA) verwendet.

```
{
  "eventVersion": "1.08",
  "userIdentity": {
    "type": "Root",
    "principalId": "111122223333",
    "arn": "arn:aws:iam::111122223333:root",
    "accountId": "111122223333",
    "accessKeyId": ""
  },
  "eventTime": "2023-07-12T13:35:31Z",
  "eventSource": "signin.amazonaws.com",
  "eventName": "ConsoleLogin",
  "awsRegion": "us-east-1",
```

```
"sourceIPAddress": "192.0.2.0",
"userAgent": "Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML,
like Gecko) Chrome/114.0.0.0 Safari/537.36",
"requestParameters": null,
"responseElements": {
  "ConsoleLogin": "Success"
},
"additionalEventData": {
  "LoginTo": "https://console.aws.amazon.com/console/home?hashArgs=
%23&isauthcode=true&nc2=h_ct&src=header-signin&state=hashArgsFromTB_ap-
southeast-2_example80afacd389",
  "MobileVersion": "No",
  "MFAUsed": "No"
},
"eventID": "4217cc13-7328-4820-a90c-EXAMPLE8002e6",
"readOnly": false,
"eventType": "AwsConsoleSignIn",
"managementEvent": true,
"recipientAccountId": "111122223333",
"eventCategory": "Management",
"tlsDetails": {
  "tlsVersion": "TLSv1.3",
  "cipherSuite": "TLS_AES_128_GCM_SHA256",
  "clientProvidedHostHeader": "signin.aws.amazon.com"
}
}
```

## Root-Benutzer, erfolgreiche Anmeldung mit MFA

Das folgende Beispiel zeigt das Ereignis einer erfolgreichen Anmeldung für einen Root-Benutzer, der die Multi-Faktor-Authentifizierung (MFA) verwendet.

```
{
  "eventVersion": "1.08",
  "userIdentity": {
    "type": "Root",
    "principalId": "444455556666",
    "arn": "arn:aws:iam::444455556666:root",
    "accountId": "444455556666",
    "accessKeyId": ""
  },
  "eventTime": "2023-07-13T03:04:43Z",
  "eventSource": "signin.amazonaws.com",
```

```
"eventName": "ConsoleLogin",
"awsRegion": "us-east-1",
"sourceIPAddress": "192.0.2.0",
"userAgent": "Mozilla/5.0 (X11; Linux x86_64) AppleWebKit/537.36 (KHTML, like
Gecko) Chrome/114.0.0.0 Safari/537.36",
"requestParameters": null,
"responseElements": {
  "ConsoleLogin": "Success"
},
"additionalEventData": {
  "LoginTo": "https://ap-southeast-1.console.aws.amazon.com/ec2/home?region=ap-
southeast-1&state=hashArgs%23Instances%3Av%3D3%3B%24case%3Dtags%3Atrue%255C%2Cclient
%3Afalse%3B%24regex%3Dtags%3Afalse%255C%2Cclient%3Afalse&isauthcode=true",
  "MobileVersion": "No",
  "MFAIdentifier": "arn:aws:iam::444455556666:mfa/root-account-mfa-device",
  "MFAUsed": "Yes"
},
"eventID": "e0176723-ea76-4275-83a3-EXAMPLEf03fb",
"readOnly": false,
"eventType": "AwsConsoleSignIn",
"managementEvent": true,
"recipientAccountId": "444455556666",
"eventCategory": "Management",
"tlsDetails": {
  "tlsVersion": "TLSv1.3",
  "cipherSuite": "TLS_AES_128_GCM_SHA256",
  "clientProvidedHostHeader": "signin.aws.amazon.com"
}
}
```

## Nicht erfolgreiche Anmeldungen für Stammbenutzer

Das folgende Beispiel zeigt das Ereignis einer nicht erfolgreichen Anmeldung für einen Stamm-Benutzer, der keine MFA verwendet.

```
{
  "eventVersion": "1.08",
  "userIdentity": {
    "type": "Root",
    "principalId": "123456789012",
    "arn": "arn:aws:iam::123456789012:root",
    "accountId": "123456789012",
    "accessKeyId": ""
  }
}
```

```
    },
    "eventTime": "2023-07-16T04:33:40Z",
    "eventSource": "signin.amazonaws.com",
    "eventName": "ConsoleLogin",
    "awsRegion": "us-east-1",
    "sourceIPAddress": "192.0.2.0",
    "userAgent": "Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML,
like Gecko) Chrome/111.0.0.0 Safari/537.36",
    "errorMessage": "Failed authentication",
    "requestParameters": null,
    "responseElements": {
      "ConsoleLogin": "Failure"
    },
    },
    "additionalEventData": {
      "LoginTo": "https://us-east-1.console.aws.amazon.com/billing/home?region=us-
east-1&state=hashArgs%23%2Faccount&isauthcode=true",
      "MobileVersion": "No",
      "MFAUsed": "No"
    },
    },
    "eventID": "f28d4329-5050-480b-8de0-EXAMPLE07329",
    "readOnly": false,
    "eventType": "AwsConsoleSignIn",
    "managementEvent": true,
    "recipientAccountId": "123456789012",
    "eventCategory": "Management",
    "tlsDetails": {
      "tlsVersion": "TLSv1.3",
      "cipherSuite": "TLS_AES_128_GCM_SHA256",
      "clientProvidedHostHeader": "signin.aws.amazon.com"
    }
  }
}
```

## Stammbenutzer, MFA geändert

Das folgende Beispiel zeigt ein Beispiel für einen Stamm-Benutzer, der Einstellungen für Multi-Faktor-Authentifizierung (MFA) ändert.

```
{
  "eventVersion": "1.08",
  "userIdentity": {
    "type": "Root",
    "principalId": "111122223333",
    "arn": "arn:aws:iam::111122223333:root",
```

```
"accountId": "111122223333",
"accessKeyId": "EXAMPLE4XX3IEV4PFQTH",
"userName": "AWS ROOT USER",
"sessionContext": {
  "sessionIssuer": {},
  "webIdFederationData": {},
  "attributes": {
    "creationDate": "2023-07-15T03:51:12Z",
    "mfaAuthenticated": "false"
  }
}
},
"eventTime": "2023-07-15T04:37:08Z",
"eventSource": "iam.amazonaws.com",
"eventName": "EnableMFADevice",
"awsRegion": "us-east-1",
"sourceIPAddress": "192.0.2.0",
"userAgent": "Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML,
like Gecko) Chrome/111.0.0.0 Safari/537.36",
"requestParameters": {
  "userName": "AWS ROOT USER",
  "serialNumber": "arn:aws:iam::111122223333:mfa/root-account-mfa-device"
},
"responseElements": null,
"requestID": "9b45cd4c-a598-41e7-9170-EXAMPLE535f0",
"eventID": "b4f18d55-d36f-49a0-afcb-EXAMPLEc026b",
"readOnly": false,
"eventType": "AwsApiCall",
"managementEvent": true,
"recipientAccountId": "111122223333",
"eventCategory": "Management",
"sessionCredentialFromConsole": "true"
}
```

## Stamm-Benutzer, Kennwort geändert

Im Folgenden wird ein Beispiereignis für einen Stamm-Benutzer gezeigt, der sein Kennwort ändert.

```
{
  "eventVersion": "1.08",
  "userIdentity": {
    "type": "Root",
    "principalId": "444455556666",
    "arn": "arn:aws:iam::444455556666:root",
```

```
    "accountId": "444455556666",
    "accessKeyId": "EXAMPLEA0TKEG44KPW5P",
    "sessionContext": {
      "sessionIssuer": {},
      "webIdFederationData": {},
      "attributes": {
        "creationDate": "2022-11-25T13:01:14Z",
        "mfaAuthenticated": "false"
      }
    }
  },
  "eventTime": "2022-11-25T13:01:14Z",
  "eventSource": "iam.amazonaws.com",
  "eventName": "ChangePassword",
  "awsRegion": "us-east-1",
  "sourceIPAddress": "192.0.2.0",
  "userAgent": "Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML,
like Gecko) Chrome/111.0.0.0 Safari/537.36",
  "requestParameters": null,
  "responseElements": null,
  "requestID": "c64254c2-e4ff-49c0-900e-EXAMPLE9e6d2",
  "eventID": "d059176c-4f4d-4a9e-b8d7-EXAMPLE2b7b3",
  "readOnly": false,
  "eventType": "AwsApiCall",
  "managementEvent": true,
  "recipientAccountId": "444455556666",
  "eventCategory": "Management"
}
```

## Beispielhafte Ereignisdatensätze für Verbundbenutzer

Die folgenden Beispiele zeigen Ereignisdatensätze für Verbundbenutzer. Verbundbenutzer erhalten temporäre Sicherheitsanmeldedaten, um über eine Anfrage auf AWS Ressourcen zugreifen zu können. [AssumeRole](#)

Nachstehend finden Sie ein Beispielereignis für eine Verbundverschlüsselungsanforderung. Die ursprüngliche Zugriffsschlüssel-ID wird im `accessKeyId`-Feld des `userIdentity`-Elements angegeben. Das `accessKeyId`-Feld in `responseElements` enthält eine neue Zugriffsschlüssel-ID, wenn die angeforderte `sessionDuration` in der Verschlüsselungsanforderung übergeben wird. Anderenfalls enthält es den Wert der ursprünglichen Zugriffsschlüssel-ID.

```
{
```

```
"eventVersion": "1.08",
"userIdentity": {
  "type": "AssumedRole",
  "principalId": "EXAMPLEUU4MH70YK5ZCOA:JohnDoe",
  "arn": "arn:aws:sts::123456789012:assumed-role/roleName/JohnDoe",
  "accountId": "123456789012",
  "accessKeyId": "originalAccessKeyID",
  "sessionContext": {
    "sessionIssuer": {
      "type": "Role",
      "principalId": "EXAMPLEUU4MH70YK5ZCOA",
      "arn": "arn:aws:iam::123456789012:role/roleName",
      "accountId": "123456789012",
      "userName": "roleName"
    },
    "webIdFederationData": {},
    "attributes": {
      "creationDate": "2023-09-25T21:30:39Z",
      "mfaAuthenticated": "false"
    }
  }
},
"eventTime": "2023-09-25T21:30:39Z",
"eventSource": "signin.amazonaws.com",
"eventName": "GetSigninToken",
"awsRegion": "us-east-1",
"sourceIPAddress": "192.0.2.0",
"userAgent": "Java/1.8.0_382",
"requestParameters": null,
"responseElements": {
  "credentials": {
    "accessKeyId": "accessKeyID"
  },
  "GetSigninToken": "Success"
},
"additionalEventData": {
  "MobileVersion": "No",
  "MFAUsed": "No"
},
"eventID": "1d66615b-a417-40da-a38e-EXAMPLE8c89b",
"readOnly": false,
"eventType": "AwsConsoleSignIn",
"managementEvent": true,
"recipientAccountId": "123456789012",
```

```

"eventCategory": "Management",
"tlsDetails": {
  "tlsVersion": "TLSv1.3",
  "cipherSuite": "TLS_AES_128_GCM_SHA256",
  "clientProvidedHostHeader": "us-east-1.signin.aws.amazon.com"
}
}

```

Das folgende Beispiel zeigt das Ereignis einer erfolgreichen Anmeldung für einen Verbundbenutzer, der keine Multi-Faktor-Authentifizierung (MFA) verwendet.

```

{
  "eventVersion": "1.08",
  "userIdentity": {
    "type": "AssumedRole",
    "principalId": "EXAMPLEPHCNW7ZCASLJOH:JohnDoe",
    "arn": "arn:aws:sts::123456789012:assumed-role/RoLeName/JohnDoe",
    "accountId": "123456789012",
    "accessKeyId": "AKIAIOSFODNN7EXAMPLE",
    "sessionContext": {
      "sessionIssuer": {
        "type": "Role",
        "principalId": "EXAMPLEPHCNW7ZCASLJOH",
        "arn": "arn:aws:iam::123456789012:role/RoLeName",
        "accountId": "123456789012",
        "userName": "RoLeName"
      },
      "webIdFederationData": {},
      "attributes": {
        "creationDate": "2023-09-22T16:15:47Z",
        "mfaAuthenticated": "false"
      }
    }
  },
  "eventTime": "2023-09-22T16:15:47Z",
  "eventSource": "signin.amazonaws.com",
  "eventName": "ConsoleLogin",
  "awsRegion": "us-east-1",
  "sourceIPAddress": "192.0.2.0",
  "userAgent": "Mozilla/5.0 (Macintosh; Intel Mac OS X 10_15_7) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/116.0.0.0 Safari/537.36",
  "requestParameters": null,
  "responseElements": {

```



```
    "ConsoleLogin": "Success"
  },
  "additionalEventData": {
    "MobileVersion": "No",
    "MFAUsed": "No"
  },
  "eventID": "b73f1ec6-c064-4cd3-ba83-EXAMPLE441d7",
  "readOnly": false,
  "eventType": "AwsConsoleSignIn",
  "managementEvent": true,
  "recipientAccountId": "123456789012",
  "eventCategory": "Management",
  "tlsDetails": {
    "tlsVersion": "TLSv1.3",
    "cipherSuite": "TLS_AES_128_GCM_SHA256",
    "clientProvidedHostHeader": "us-east-1.signin.aws.amazon.com"
  }
}
```

# Mit CloudTrail Protokolldateien arbeiten

Sie können komplexere Aufgaben mit Ihren CloudTrail Dateien ausführen.

- Erstellen Sie mehrere Trails pro Region.
- Überwachen CloudTrail Sie Protokolldateien, indem Sie sie an CloudWatch Logs senden.
- Sie können Protokolldateien zwischen Konten freigeben.
- Verwenden Sie die AWS CloudTrail Processing Library, um Anwendungen zur Protokollverarbeitung in Java zu schreiben.
- Überprüfen Sie Ihre Protokolldateien, um sicherzustellen, dass sie sich nach der Lieferung von nicht geändert haben CloudTrail.

Wenn in deinem Konto ein Ereignis eintritt, wird CloudTrail geprüft, ob das Ereignis den Einstellungen für deine Trails entspricht. Nur Ereignisse, die Ihren Trail-Einstellungen entsprechen, werden an Ihren Amazon S3 S3-Bucket und Ihre Amazon CloudWatch Logs-Protokollgruppe übermittelt.

Sie können mehrere Trails unterschiedlich konfigurieren, sodass die Trails nur die von Ihnen angegebenen Ereignisse protokollieren. So kann beispielsweise ein Trail so konfiguriert werden, dass nur schreibgeschützte Daten- und Verwaltungsereignisse protokolliert werden. So werden alle schreibgeschützten Ereignisse an einen S3-Bucket übermittelt. Ein weiterer Trail kann so konfiguriert werden, dass nur Daten- und Verwaltungsereignisse vom Typ Nur-Schreiben protokolliert werden, sodass alle Nur-Schreiben-Ereignisse an einen separaten S3-Bucket übermittelt werden.

Sie können Ihre Trails auch so konfigurieren, dass nur ein Trail-Protokoll verwendet wird und alle Verwaltungsereignisse an einen S3-Bucket übermittelt werden. Ein anderer Trail kann dann so eingerichtet werden, dass alle Datenereignisse protokolliert und an einen anderen S3-Bucket geliefert werden.

Sie können Ihre Trails konfigurieren, um Folgendes zu protokollieren:

- [Datenereignisse](#): Diese Ereignisse bieten Einblicke in die Ressourcenoperationen, die für oder innerhalb einer Ressource ausgeführt wurden. Sie werden auch als Vorgänge auf Datenebene bezeichnet.
- [Verwaltungsereignisse](#): Verwaltungsereignisse bieten Einblick in Verwaltungsvorgänge, die mit Ressourcen in Ihrem AWS Konto ausgeführt werden. Sie werden auch als Vorgänge auf Steuerebene bezeichnet. Verwaltungsereignisse können auch andere als API-Ereignisse

einschließen, die in Ihrem Konto auftreten. Wenn sich beispielsweise ein Benutzer bei Ihrem Konto anmeldet, wird das `ConsoleLogin` Ereignis CloudTrail protokolliert. Weitere Informationen finden Sie unter [Nicht-API-Ereignisse, erfasst von CloudTrail](#).

- [Insights-Ereignisse](#): In Insights-Ereignissen werden ungewöhnliche Aktivitäten erfasst, die für Ihr Konto erkannt werden. Wenn Sie Insights-Ereignisse aktiviert haben und CloudTrail ungewöhnliche Aktivitäten feststellen, werden Insights-Ereignisse im Ziel-S3-Bucket für Ihren Trail protokolliert, jedoch in einem anderen Ordner. Sie können auch die Art des Insights-Ereignisses und den Zeitraum des Vorfalls sehen, wenn Sie Insights-Ereignisse auf der CloudTrail Konsole aufrufen. Im Gegensatz zu anderen Arten von Ereignissen, die in einem CloudTrail Trail erfasst werden, werden Insights-Ereignisse nur protokolliert, wenn Änderungen in der API-Nutzung Ihres Kontos CloudTrail festgestellt werden, die sich erheblich von den typischen Nutzungsmustern des Kontos unterscheiden.

Insights-Ereignisse werden nur für Verwaltungs-APIs generiert. Weitere Informationen finden Sie unter [Protokollieren von Insights-Ereignissen](#).

#### Note

CloudTrail übermittelt Protokolle in der Regel innerhalb von durchschnittlich etwa 5 Minuten nach einem API-Aufruf. Diese Zeit ist nicht garantiert. Weitere Informationen finden Sie unter [AWS CloudTrail Service Level Agreement](#).

Wenn Sie Ihren Trail falsch konfigurieren (z. B. wenn der S3-Bucket nicht erreichbar ist), CloudTrail wird versucht, die Protokolldateien 30 Tage lang erneut in Ihren S3-Bucket zu übertragen. Für diese attempted-to-deliver Ereignisse fallen Standardgebühren an. CloudTrail Um Gebühren für einen falsch konfigurierten Trail zu vermeiden, müssen Sie den Trail löschen.

## Themen

- [Empfangen von CloudTrail Protokolldateien aus mehreren Regionen](#)
- [Verwaltung der Datenkonsistenz in CloudTrail](#)
- [Überwachung von CloudTrail Protokolldateien mit Amazon CloudWatch Logs](#)
- [Empfangen von CloudTrail Protokolldateien von mehreren Konten](#)
- [CloudTrail Protokolldateien zwischen AWS Konten teilen](#)
- [Überprüfen der Integrität der CloudTrail Protokolldatei](#)

- [CloudTrail Beispiele für Protokolldateien](#)
- [Verwendung der CloudTrail Processing Library](#)

## Empfangen von CloudTrail Protokolldateien aus mehreren Regionen

Sie können so konfigurieren CloudTrail, dass Protokolldateien aus mehreren Regionen für ein einzelnes Konto in einen einzigen S3-Bucket übertragen werden. Sie haben beispielsweise einen Trail in der Region USA West (Oregon), der für die Übermittlung von Protokolldateien an einen S3-Bucket konfiguriert ist, und eine CloudWatch Logs-Protokollgruppe. Wenn Sie einen bestehenden Trail mit einer einzelnen Region so ändern, dass er alle Regionen CloudTrail protokolliert, werden Ereignisse aus allen Regionen protokolliert, die sich in einer einzigen AWS Partition Ihres Kontos befinden. CloudTrail übermittelt Protokolldateien an denselben S3-Bucket und dieselbe CloudWatch Logs-Protokollgruppe. Solange er über Schreibberechtigungen für einen S3-Bucket CloudTrail verfügt, muss sich der Bucket für einen Trail mit mehreren Regionen nicht in der Heimatregion des Trails befinden.

Um Ereignisse in allen Regionen auf allen AWS Partitionen Ihres Kontos zu protokollieren, erstellen Sie in jeder Partition einen Trail mit mehreren Regionen.

In der Konsole erstellen Sie standardmäßig einen Trail, der Ereignisse in allen AWS-Regionen in der [AWS -Partition](#) in der Sie arbeiten, protokolliert. Dies ist eine empfohlene bewährte Methode. Um Ereignisse in einer einzelnen Region zu protokollieren (nicht empfohlen), [verwenden Sie AWS CLI](#). Um einen vorhandenen Trail für eine einzelne Region für die Anmeldung in allen Regionen zu konfigurieren, müssen Sie AWS CLI verwenden.

Um einen vorhandenen Trail so zu ändern, dass er für alle Regionen gilt, fügen Sie dem Befehl [update-trail](#) die Option `--is-multi-region-trail` hinzu.

```
aws cloudtrail update-trail --name my-trail --is-multi-region-trail
```

Um zu bestätigen, dass der Trail nun für alle Regionen gilt, zeigt das `IsMultiRegionTrail`-Element in der Ausgabe `true` an.

```
{
  "IncludeGlobalServiceEvents": true,
  "Name": "my-trail",
  "TrailARN": "arn:aws:cloudtrail:us-east-2:123456789012:trail/my-trail",
```

```
"LogFileValidationEnabled": false,  
"IsMultiRegionTrail": true,  
"IsOrganizationTrail": false,  
"S3BucketName": "my-bucket"  
}
```

### Note

Wenn eine neue Region in der [awsPartition](#) gestartet CloudTrail wird, wird automatisch ein Trail für Sie in der neuen Region mit denselben Einstellungen wie Ihr ursprünglicher Trail erstellt.

Weitere Informationen finden Sie in den folgenden Ressourcen:

- [Mit CloudTrail Trails arbeiten](#)
- [CloudTrail Häufig gestellte Fragen](#)

## Verwaltung der Datenkonsistenz in CloudTrail

CloudTrail verwendet ein verteiltes Rechenmodell, das als [letztendliche Konsistenz](#) bezeichnet wird. Jede Änderung, die Sie an Ihrer CloudTrail Konfiguration (oder anderen AWS Diensten) vornehmen, einschließlich der Tags, die in der [attributebasierten Zugriffskontrolle \(ABAC\)](#) verwendet werden, dauert einige Zeit, bis sie von allen möglichen Endpunkten aus sichtbar ist. Ein Teil der Verzögerung ist auf die Zeit zurückzuführen, die benötigt wird, um die Daten von Server zu Server, von Replikationszone zu Replikationszone und von Region zu Region auf der ganzen Welt zu senden. CloudTrail verwendet auch Caching, um die Leistung zu verbessern, aber in einigen Fällen kann dies zu mehr Zeit führen. Die Änderung ist möglicherweise erst sichtbar, wenn die Zeit für die vorher zwischengespeicherten Daten abgelaufen ist.

Sie müssen Ihre Anwendungen unter Berücksichtigung dieser potenziellen Verzögerungen konzipieren. Stellen Sie sicher, dass sie wie erwartet funktionieren, und zwar auch dann, wenn eine Änderung an einem Speicherort nicht sofort an einem anderen sichtbar ist. Zu diesen Änderungen gehören das Erstellen oder Aktualisieren von Trails oder Ereignisdatenspeichern, das Aktualisieren von Ereignisselektoren und das Starten oder Beenden der Protokollierung. Wenn Sie einen Trail- oder Event-Datenspeicher erstellen oder aktualisieren, CloudTrail übermittelt Logs auf der Grundlage der letzten bekannten Konfiguration an den S3-Bucket oder den Ereignisdatenspeicher, bis die Änderungen auf alle Speicherorte übertragen werden.

Weitere Informationen darüber, wie sich dies auf andere auswirkt AWS-Services, finden Sie in den folgenden Ressourcen:

- Amazon DynamoDB: [Wie lautet das Konsistenzmodell von Amazon DynamoDB?](#) im DynamoDB – Häufig gestellte Fragen und [Lesekonsistenz](#) im Entwicklerleitfaden für Amazon DynamoDB.
- Amazon EC2: [Letztendliche Konsistenz](#) in der API-Referenz zu Amazon Elastic Compute Cloud.
- Amazon EMR: [Sicherstellung der Konsistenz bei der Verwendung von Amazon S3 und Amazon Elastic MapReduce für ETL-Workflows](#) im AWS Big Data-Blog.
- AWS Identity and Access Management (IAM): [Änderungen, die ich vornehme, sind nicht immer sofort im IAM-Benutzerhandbuch sichtbar](#).
- Amazon Redshift: [Verwalten der Datenkonsistenz](#) im Entwicklerhandbuch für Amazon-Redshift-Datenbanken.
- Amazon S3: [Amazon-S3-Datenkonsistenzmodell](#) im Benutzerhandbuch für Amazon Simple Storage Service

## Überwachung von CloudTrail Protokolldateien mit Amazon CloudWatch Logs

Sie können CloudWatch Logs so konfigurieren CloudTrail , dass Ihre Trail-Logs überwacht werden und Sie benachrichtigt werden, wenn bestimmte Aktivitäten auftreten.

1. Konfigurieren Sie Ihren Trail so, dass Protokollereignisse an CloudWatch Logs gesendet werden.
2. Definieren Sie Metrikfilter für CloudWatch Logs, um Log-Ereignisse nach Übereinstimmungen in Begriffen, Ausdrücken oder Werten auszuwerten. Sie können beispielsweise eine Überprüfung auf ConsoleLogin-Ereignisse vornehmen.
3. Weisen Sie den CloudWatch Metrikfiltern Metriken zu.
4. Erstellen Sie CloudWatch Alarme, die gemäß den von Ihnen angegebenen Schwellenwerten und Zeiträumen ausgelöst werden. Sie können Alarme so konfigurieren, dass bei Alarmauslösung Benachrichtigungen gesendet werden, damit Sie Maßnahmen ergreifen können.
5. Sie können auch so konfigurieren CloudWatch , dass als Reaktion auf einen Alarm automatisch eine Aktion ausgeführt wird.

Es gelten die Standardpreise für Amazon CloudWatch und Amazon CloudWatch Logs. Weitere Informationen finden Sie unter [CloudWatch Amazon-Preise](#).

Weitere Informationen zu den Regionen, in denen Sie Ihre Trails so konfigurieren können, dass Logs an CloudWatch Logs gesendet werden, finden Sie unter [Amazon CloudWatch Logs Regions and Quotas](#) in der AWS Allgemeinen Referenz.

## Themen

- [Ereignisse an CloudWatch Logs senden](#)
- [CloudWatch Alarme für CloudTrail Ereignisse erstellen: Beispiele](#)
- [Das Senden CloudTrail von Ereignissen an CloudWatch Logs beenden](#)
- [CloudWatch Benennung von Protokollgruppen und Protokollströmen für CloudTrail](#)
- [Rollenrichtlinien-Dokument CloudTrail zur Verwendung von CloudWatch Logs zur Überwachung](#)

## Ereignisse an CloudWatch Logs senden

Wenn du deinen Trail so konfigurierst, dass er Ereignisse an CloudWatch Logs CloudTrail sendet, werden nur die Ereignisse gesendet, die deinen Trail-Einstellungen entsprechen. Wenn du deinen Trail beispielsweise so konfigurierst, dass nur Datenereignisse protokolliert werden, sendet dein Trail nur Datenereignisse an deine CloudWatch Logs-Protokollgruppe. CloudTrail unterstützt das Senden von Daten, Erkenntnissen und Verwaltungsereignissen an CloudWatch Logs. Weitere Informationen finden Sie unter [Mit CloudTrail Protokolldateien arbeiten](#).

### Note

Nur das Verwaltungskonto kann mithilfe der Konsole eine CloudWatch Logs-Protokollgruppe für einen Organisations-Trail konfigurieren. Der delegierte Administrator kann eine CloudWatch Logs-Protokollgruppe mithilfe der UpdateTrail API-Operationen AWS CLI oder CloudTrail CreateTrail oder konfigurieren.

Um Ereignisse an eine CloudWatch Logs-Protokollgruppe zu senden:

- Stellen Sie sicher, dass Sie über ausreichende Berechtigungen zum Erstellen oder Angeben einer IAM-Rolle verfügen. Weitere Informationen finden Sie unter [Erteilen der Berechtigung zum Anzeigen und Konfigurieren von Amazon CloudWatch Logs-Informationen auf der CloudTrail Konsole](#).
- Wenn Sie die CloudWatch Logs-Protokollgruppe mithilfe von konfigurieren AWS CLI, stellen Sie sicher, dass Sie über ausreichende Berechtigungen verfügen, um in der von Ihnen angegebenen

Protokollgruppe einen CloudWatch Logs-Log-Stream zu erstellen und CloudTrail Ereignisse an diesen Log-Stream zu übermitteln. Weitere Informationen finden Sie unter [Erstellen eines Richtliniendokuments](#).

- Erstellen Sie einen neuen Trail oder wählen Sie einen vorhandenen aus. Weitere Informationen finden Sie unter [Erstellen und Aktualisieren eines Trails mit der Konsole](#).
- Erstellen Sie eine Protokollgruppe oder wählen Sie eine vorhandene aus.
- Geben Sie eine IAM-Rolle an. Wenn Sie eine vorhandene IAM-Rolle für einen Organisations-Trail ändern, müssen Sie die Richtlinie manuell aktualisieren, damit die Protokollierung für den Organisations-Trail aktiv wird. Weitere Informationen finden Sie [in diesem Richtlinienbeispiel](#) und unter [Erstellen eines Trails für eine Organisation](#).
- Fügen Sie eine Rollenrichtlinie hinzu oder verwenden Sie die Standardwerte.

## Inhalt

- [Konfiguration der CloudWatch Protokollüberwachung mit der Konsole](#)
  - [Erstellen einer Protokollgruppe oder Auswählen einer vorhandenen Protokollgruppe](#)
  - [Auswählen einer IAM-Rolle](#)
  - [Ereignisse in der CloudWatch Konsole anzeigen](#)
- [Konfiguration der CloudWatch Protokollüberwachung mit dem AWS CLI](#)
  - [Erstellen einer Protokollgruppe](#)
  - [Erstellen einer Rolle](#)
  - [Erstellen eines Richtliniendokuments](#)
  - [Aktualisieren des Trails](#)
- [Einschränkung](#)

## Konfiguration der CloudWatch Protokollüberwachung mit der Konsole

Sie können das verwenden AWS Management Console , um Ihren Trail so zu konfigurieren, dass Ereignisse zur Überwachung an CloudWatch Logs gesendet werden.


### Erstellen einer Protokollgruppe oder Auswählen einer vorhandenen Protokollgruppe

CloudTrail verwendet eine CloudWatch Logs-Protokollgruppe als Übermittlungsendpunkt für Protokollereignisse. Sie können eine Protokollgruppe erstellen oder eine vorhandene auswählen.




Erstellen oder spezifizieren Sie eine Protokollgruppe für einen vorhandenen Trail wie folgt:

1. Stellen Sie sicher, dass Sie sich mit einem Administratorbenutzer oder einer Administratorrolle mit ausreichenden Rechten anmelden, um die CloudWatch Logs-Integration zu konfigurieren. Weitere Informationen finden Sie unter [Erteilen der Berechtigung zum Anzeigen und Konfigurieren von Amazon CloudWatch Logs-Informationen auf der CloudTrail Konsole](#).

 Note

Nur das Verwaltungskonto kann mithilfe der Konsole eine CloudWatch Logs-Protokollgruppe für einen Organisationstrail konfigurieren. Der delegierte Administrator kann eine CloudWatch Logs-Protokollgruppe mithilfe der UpdateTrail API-Operationen AWS CLI oder CloudTrail CreateTrail oder konfigurieren.


2. Öffnen Sie die CloudTrail Konsole unter <https://console.aws.amazon.com/cloudtrail/>.
3. Wählen Sie den Trail-Namen aus. Wenn Sie einen für alle Regionen geltenden Trail auswählen, werden Sie zu der Region weitergeleitet, in der dieser Trail erstellt wurde. Sie können eine Protokollgruppe erstellen oder eine vorhandene Protokollgruppe in derselben Region auswählen, in der sich der Trail befindet.

 Note

Ein Trail, der für alle Regionen gilt, sendet Protokolldateien aus allen Regionen an die von Ihnen angegebene CloudWatch Logs-Protokollgruppe.

4. Wählen Sie unter CloudWatch Logs die Option Bearbeiten aus.
5. Wählen Sie für CloudWatch Protokolle die Option Aktiviert aus.
6. Wählen Sie unter Protokollgruppenname die Option Neu aus, um eine neue Protokollgruppe zu erstellen, oder Bestehend, um eine bestehende Gruppe zu verwenden. Wenn Sie Neu wählen, CloudTrail gibt Sie einen Namen für die neue Protokollgruppe an, oder Sie können einen Namen eingeben. Weitere Informationen zur Namensgebung finden Sie unter [CloudWatch Benennung von Protokollgruppen und Protokolldatenströmen für CloudTrail](#).
7. Wenn Sie Vorhanden wählen, wählen Sie eine Protokollgruppe aus der Dropdown-Liste aus.
8. Wählen Sie unter Rollename die Option Neu aus, um eine neue IAM-Rolle für Berechtigungen zum Senden von Protokollen an Logs zu CloudWatch erstellen. Wählen Sie Vorhanden, um eine vorhandene IAM-Rolle aus der Dropdown-Liste auszuwählen. Die Richtlinienanweisung für die neue oder vorhandene Rolle wird angezeigt, wenn Sie das Richtliniendokument erweitern.

Weitere Informationen über diese Rolle finden Sie unter [Rollenrichtlinien-Dokument CloudTrail zur Verwendung von CloudWatch Logs zur Überwachung](#).

 Note

Beim Konfigurieren eines Trails können Sie einen S3 Bucket und ein SNS-Thema auswählen, die zu einem anderen Konto gehören. Wenn Sie jedoch Ereignisse CloudTrail an eine CloudWatch Logs-Protokollgruppe übermitteln möchten, müssen Sie eine Protokollgruppe auswählen, die in Ihrem aktuellen Konto vorhanden ist.


9. Wählen Sie Änderungen speichern aus.

### Auswählen einer IAM-Rolle

Sie können eine Rolle angeben, von der CloudTrail die Übermittlung von Ereignissen an den Protokollstream übernommen werden soll.

So wählen Sie eine Rolle aus:

1. Standardmäßig ist `CloudTrail_CloudWatchLogs_Role` ausgewählt. Die Standardrollenrichtlinie verfügt über die erforderlichen Berechtigungen, um einen CloudWatch Log-Log-Stream in einer von Ihnen angegebenen Protokollgruppe zu erstellen und CloudTrail Ereignisse an diesen Log-Stream zu übermitteln.

 Note

Wenn Sie diese Rolle für eine Protokollgruppe eines Organisations-Trails verwenden möchten, müssen Sie die Richtlinie nach dem Erstellen der Rolle manuell ändern. Weitere Informationen finden Sie [in diesem Richtlinienbeispiel](#) und unter [Erstellen eines Trails für eine Organisation](#).

- a. Rufen Sie die AWS Identity and Access Management Konsole unter <https://console.aws.amazon.com/iam/> auf, um die Rolle zu überprüfen.
- b. Wählen Sie Rollen und dann die CloudWatchLogsRolle CloudTrail \_\_ aus.
- c. Erweitern Sie auf der Registerkarte Berechtigungen die Richtlinie, um ihren Inhalt anzuzeigen.

2. Sie können eine andere Rolle angeben, müssen jedoch die erforderliche Rollenrichtlinie an die bestehende Rolle anhängen, wenn Sie sie zum Senden von Ereignissen an CloudWatch Logs verwenden möchten. Weitere Informationen finden Sie unter [Rollenrichtlinien-Dokument CloudTrail zur Verwendung von CloudWatch Logs zur Überwachung](#).

## Ereignisse in der CloudWatch Konsole anzeigen

Nachdem Sie Ihren Trail so konfiguriert haben, dass Ereignisse an Ihre Protokollgruppe CloudWatch Logs gesendet werden, können Sie die Ereignisse in der CloudWatch Konsole anzeigen. CloudTrail übermittelt Ereignisse in der Regel innerhalb von durchschnittlich etwa 5 Minuten nach einem API-Aufruf an Ihre Protokollgruppe. Diese Zeit ist nicht garantiert. Weitere Informationen finden Sie unter [AWS CloudTrail Service Level Agreement](#).

### Um Ereignisse in der CloudWatch Konsole anzuzeigen

1. Öffnen Sie die CloudWatch Konsole unter <https://console.aws.amazon.com/cloudwatch/>.
2. Wählen Sie im linken Navigationsbereich unter Protokolle die Option Protokollgruppen aus.
3. Wählen Sie die Protokollgruppe aus, die Sie für den Trail angegeben haben.
4. Wählen Sie den Protokollstream aus, den Sie anzeigen möchten.
5. Wählen Sie ein vom Trail protokolliertes Ereignis aus, um Details dazu aufzurufen.

#### Note

In der Spalte Zeit (UTC) in der CloudWatch Konsole wird angezeigt, wann das Ereignis an Ihre Protokollgruppe übermittelt wurde. Die tatsächliche Uhrzeit, bis zu der das Ereignis protokolliert wurde CloudTrail, finden Sie in dem `eventTime` Feld.

## Konfiguration der CloudWatch Protokollüberwachung mit dem AWS CLI

Sie können das AWS CLI zur Konfiguration verwenden, CloudTrail um Ereignisse zur Überwachung an CloudWatch Logs zu senden.

## Erstellen einer Protokollgruppe

1. Wenn Sie noch keine Protokollgruppe haben, erstellen Sie mit dem `create-log-group` Befehl CloudWatch Logs eine Logs-Protokollgruppe als Übermittlungsendpunkt für Protokollereignisse. CloudWatch

```
aws logs create-log-group --log-group-name name
```

Im folgenden Beispiel wird eine Protokollgruppe mit dem Namen `CloudTrail/logs` erstellt:

```
aws logs create-log-group --log-group-name CloudTrail/logs
```

2. Rufen Sie den ARN (Amazon Resource Name) der Protokollgruppe ab.

```
aws logs describe-log-groups
```

## Erstellen einer Rolle

Erstellen Sie eine Rolle CloudTrail, die es ihr ermöglicht, Ereignisse an die Protokollgruppe CloudWatch Logs zu senden. Der IAM-Befehl `create-role` benötigt zwei Parameter, nämlich einen Rollennamen und einen Dateipfad, um das Dokument mit der Rollenrichtlinie im JSON-Format verwenden zu können. Das von Ihnen verwendete Richtliniendokument gewährt `AssumeRole` Berechtigungen für CloudTrail. Über den Befehl `create-role` wird die Rolle mit den erforderlichen Berechtigungen generiert.

Zum Erstellen der JSON-Datei, die das Richtliniendokument enthält, öffnen Sie einen Texteditor und speichern den folgenden Richtlinieninhalt in einer Datei mit dem Namen `assume_role_policy_document.json`.

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Sid": "",
      "Effect": "Allow",
      "Principal": {
        "Service": "cloudtrail.amazonaws.com"
      },
      "Action": "sts:AssumeRole"
    }
  ]
}
```

```
}  
]  
}
```

Führen Sie den folgenden Befehl aus, um die Rolle mit den AssumeRole Berechtigungen für zu erstellen CloudTrail.

```
aws iam create-role --role-name role_name --assume-role-policy-document file://<path to  
assume_role_policy_document>.json
```

Notieren Sie sich nach der Ausführung des Befehls den Rollen-ARN in der Ausgabe.

### Erstellen eines Richtliniendokuments

Erstellen Sie das folgende Rollenrichtlinien-Dokument für CloudTrail. Dieses Dokument gewährt CloudTrail die erforderlichen Berechtigungen, um einen CloudWatch Log-Log-Stream in der von Ihnen angegebenen Protokollgruppe zu erstellen und CloudTrail Ereignisse an diesen Log-Stream zu übermitteln.

```
{  
  "Version": "2012-10-17",  
  "Statement": [  
    {  
      "Sid": "AWSCloudTrailCreateLogStream2014110",  
      "Effect": "Allow",  
      "Action": [  
        "logs:CreateLogStream"  
      ],  
      "Resource": [  
        "arn:aws:logs:region:accountID:log-group:log_group_name:log-  
stream:accountID_CloudTrail_region*"      ]  
    },  
    {  
      "Sid": "AWSCloudTrailPutLogEvents20141101",  
      "Effect": "Allow",  
      "Action": [  
        "logs:PutLogEvents"  
      ],  
      "Resource": [  

```

```

        "arn:aws:logs:region:accountID:log-group:log_group_name:log-
stream:accountID_CloudTrail_region*"
    ]
}
]
}

```

Speichern Sie das Richtliniendokument in einer Datei mit dem Namen `role-policy-document.json`.

Wenn Sie eine Richtlinie erstellen, die auch für Organisations-Trails verwendet werden soll, müssen Sie sie etwas anders konfigurieren. Die folgende Richtlinie gewährt beispielsweise CloudTrail die erforderlichen Berechtigungen, um einen CloudWatch Logs-Log-Stream in der von Ihnen angegebenen Protokollgruppe zu erstellen und CloudTrail Ereignisse an diesen Log-Stream zu übermitteln, und zwar sowohl für Pfade im AWS Konto 111111111111 als auch für Organisationspfade, die im Konto 111111111111 erstellt wurden und auf die AWS Organizations Organisation mit der ID *o-exampleorgid* angewendet werden:

```

{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Sid": "AWSCloudTrailCreateLogStream20141101",
      "Effect": "Allow",
      "Action": [
        "logs:CreateLogStream"
      ],
      "Resource": [
        "arn:aws:logs:us-east-2:111111111111:log-group:CloudTrail/
DefaultLogGroupTest:log-stream:111111111111_CloudTrail_us-east-2*",
        "arn:aws:logs:us-east-2:111111111111:log-group:CloudTrail/
DefaultLogGroupTest:log-stream:o-exampleorgid_*"
      ]
    },
    {
      "Sid": "AWSCloudTrailPutLogEvents20141101",
      "Effect": "Allow",
      "Action": [
        "logs:PutLogEvents"
      ],
      "Resource": [

```

```
        "arn:aws:logs:us-east-2:111111111111:log-group:CloudTrail/
DefaultLogGroupTest:log-stream:111111111111_CloudTrail_us-east-2*",
        "arn:aws:logs:us-east-2:111111111111:log-group:CloudTrail/
DefaultLogGroupTest:log-stream:o-exampleorgid_*"
    ]
}
]
```

Weitere Informationen zu Organisations-Trails finden Sie unter [Erstellen eines Trails für eine Organisation](#).

Führen Sie den folgenden Befehl aus, damit die Richtlinie für die Rolle gilt.

```
aws iam put-role-policy --role-name role_name --policy-name cloudtrail-policy --policy-
document file://<path to role-policy-document>.json
```

## Aktualisieren des Trails

Aktualisieren Sie den Trail mithilfe des Befehls mit den Protokollgruppen- und Rolleninformationen.

CloudTrail update-trail

```
aws cloudtrail update-trail --name trail_name --cloud-watch-logs-log-group-
arn log_group_arn --cloud-watch-logs-role-arn role_arn
```

Weitere Informationen zu den AWS CLI Befehlen finden Sie in der [AWS CloudTrail Befehlszeilenreferenz](#).

## Einschränkung

CloudWatch In den Protokollen ist EventBridge jeweils [eine maximale Ereignisgröße von 256 KB zulässig](#). Obwohl die meisten Dienstereignisse eine maximale Größe von 256 KB haben, haben einige Dienste immer noch größere Ereignisse. CloudTrail sendet diese Ereignisse nicht an CloudWatch Logs oder EventBridge.

Ab der CloudTrail Ereignisversion 1.05 haben Ereignisse eine maximale Größe von 256 KB. Dies soll dazu beitragen, die Ausnutzung durch böswillige Akteure zu verhindern und die Nutzung von Ereignissen durch andere AWS Dienste wie CloudWatch Logs und EventBridge zu ermöglichen.

# CloudWatch Alarme für CloudTrail Ereignisse erstellen: Beispiele

In diesem Thema wird beschrieben, wie Alarme für CloudTrail Ereignisse konfiguriert werden, und es enthält Beispiele.

## Themen

- [Voraussetzungen](#)
- [Einen Metrikfilter und einen Alarm erstellen](#)
- [Beispiel: Änderungen an der Sicherheitsgruppenkonfiguration](#)
- [Beispiele für AWS Management Console fehlgeschlagene Anmeldevorgänge](#)
- [Beispiel: Änderungen an der IAM-Richtlinie](#)
- [Benachrichtigungen für CloudWatch Logs-Alarme konfigurieren](#)

## Voraussetzungen

Bevor Sie die Beispiele in diesem Thema verwenden können, müssen Sie:

- Einen Trail mit der Konsole oder CLI erstellen.
- Erstellen Sie eine Protokollgruppe, die Sie beim Erstellen eines Trails durchführen können. Weitere Informationen zum Erstellen eines Trails finden Sie unter [Erstellen eines Trails](#).
- Geben Sie eine IAM-Rolle an, oder erstellen Sie eine, CloudTrail die die Berechtigungen zum Erstellen eines CloudWatch Log-Log-Streams in der von Ihnen angegebenen Protokollgruppe und zum Übermitteln von CloudTrail Ereignissen an diesen Log-Stream gewährt. Die standardmäßige `CloudTrail_CloudWatchLogs_Role` führt dies für Sie aus.

Weitere Informationen finden Sie unter [Ereignisse an CloudWatch Logs senden](#). Die Beispiele in diesem Abschnitt werden in der Amazon CloudWatch Logs-Konsole ausgeführt. Weitere Informationen zum Erstellen von Metrikfiltern und Alarmen finden Sie unter [Metriken aus Protokollereignissen mithilfe von Filtern erstellen](#) und [CloudWatch Amazon-Alarme verwenden](#) im CloudWatch Amazon-Benutzerhandbuch.

## Einen Metrikfilter und einen Alarm erstellen

Um einen Alarm zu erstellen, müssen Sie zuerst einen Metrikfilter erstellen und dann basierend auf diesem Filter einen Alarm konfigurieren. Die Verfahren werden für alle Beispiele gezeigt. Weitere Informationen zur Syntax für Metrikfilter und Muster für CloudTrail Protokollereignisse finden Sie



in den JSON-bezogenen Abschnitten von [Filter- und Mustersyntax](#) im Amazon CloudWatch Logs-Benutzerhandbuch.

## Beispiel: Änderungen an der Sicherheitsgruppenkonfiguration

Gehen Sie wie folgt vor, um einen CloudWatch Amazon-Alarm zu erstellen, der ausgelöst wird, wenn Konfigurationsänderungen an Sicherheitsgruppen vorgenommen werden.

### Einen Metrikfilter erstellen

1. Öffnen Sie die CloudWatch Konsole unter <https://console.aws.amazon.com/cloudwatch/>.
2. Wählen Sie im Navigationsbereich unter Protokolle die Option Protokollgruppen aus.
3. Wählen Sie in der Liste von Protokollgruppen die Protokollgruppe aus, die Sie für Ihren Trail erstellt haben.
4. Wählen Sie im Menü Metrikfilter oder Aktionen die Option Metrikfilter erstellen aus.
5. Geben Sie auf der Seite Muster definieren unter Filtermuster erstellen Folgendes für Filtermuster ein.

```
{ ($.eventName = AuthorizeSecurityGroupIngress) || ($.eventName = AuthorizeSecurityGroupEgress) || ($.eventName = RevokeSecurityGroupIngress) || ($.eventName = RevokeSecurityGroupEgress) || ($.eventName = CreateSecurityGroup) || ($.eventName = DeleteSecurityGroup) }
```

6. Behalten Sie in Testmuster die Standardeinstellungen bei. Wählen Sie Weiter aus.
7. Geben Sie auf der Seite Metrik zuweisen für Filtername den Wert **SecurityGroupEvents** ein.
8. Aktivieren Sie unter Metrikdetails die Option Neu erstellen und geben Sie dann für Namespace der Metrik den Wert **CloudTrailMetrics** ein.
9. Geben Sie für Metrikname den Wert **SecurityGroupEventCount** ein.
10. Geben Sie für Metrikwert den Wert **1** ein.
11. Lassen Sie den Standardwert leer.
12. Wählen Sie Weiter aus.
13. Überprüfen Sie auf der Seite Prüfen und erstellen Ihre Auswahl. Wählen Sie Metrikfilter erstellen, um den Filter zu erstellen, oder wählen Sie Bearbeiten, um zurückzugehen und Werte zu ändern.

## Alarm erstellen

Nachdem Sie den Metrikfilter erstellt haben, wird die Seite mit den Details zur CloudWatch Log-Log-Gruppe für Ihre CloudTrail Trail-Log-Gruppe geöffnet. Gehen Sie folgendermaßen vor, um einen Alarm zu erstellen.

1. Suchen Sie auf der Registerkarte Metrikfilter den in [the section called “Einen Metrikfilter erstellen”](#) erstellten Metrikfilter. Aktivieren Sie das Kontrollkästchen für den Metrikfilter. Wählen Sie in der Leiste Metrikfilter die Option Alarm erstellen aus.
2. Geben Sie unter Metrik und Bedingungen festlegen Folgendes ein:
  - a. Bei Diagramm wird die Linie basierend auf anderen Einstellungen, die Sie beim Erstellen Ihres Alarms vornehmen, auf **1** gesetzt.
  - b. Behalten Sie für Metrikname den aktuellen Metriknamen **SecurityGroupEventCount** bei.
  - c. Behalten Sie für Statistik den Standardwert **Sum** bei.
  - d. Behalten Sie für Zeitraum den Standardwert **5 minutes** bei.
  - e. Wählen Sie unter Bedingungen unter Schwellenwerttyp die Option Statisch aus.
  - f. Wählen Sie Größer/Gleich für Immer wenn ***metric\_name*** ist.
  - g. Geben Sie als Schwellenwert **1** ein.
  - h. Übernehmen Sie unter Zusätzliche Konfiguration die Standardeinstellungen. Wählen Sie Weiter aus.
3. Wählen Sie auf der Seite Aktionen konfigurieren die Option Benachrichtigung und dann Bei Alarm aus. Dies bedeutet, dass die Aktion ausgeführt wird, wenn der Schwellenwert von 1 Änderungsereignis innerhalb von 5 Minuten überschritten SecurityGroupEventCount wird und sich der Alarmstatus befindet.
  - a. Wählen Sie unter Benachrichtigung an folgendes SNS-Thema senden die Option Neues Thema erstellen aus.
  - b. Geben Sie **SecurityGroupChanges\_CloudWatch\_Alarms\_Topic** als Namen des neuen Amazon-SNS-Themas ein.
  - c. Geben Sie unter E-Mail-Endpunkte, die die Benachrichtigung erhalten, die E-Mail-Adressen der Benutzer ein, die Benachrichtigungen erhalten sollen, wenn dieser Alarm ausgelöst wird. Trennen Sie E-Mail-Adressen durch Kommas.

Jeder E-Mail-Empfänger erhält eine E-Mail, in der er bestätigen muss, dass er das Amazon-SNS-Thema abonniert haben möchten.

- d. Wählen Sie Thema erstellen aus.
4. Überspringen Sie in diesem Beispiel die anderen Aktionstypen. Wählen Sie Weiter.
5. Geben Sie auf der Seite Name und Beschreibung hinzufügen einen Anzeigenamen für den Alarm und eine Beschreibung ein. Geben Sie in diesem Beispiel **Security group configuration changes** für den Namen und **Raises alarms if security group configuration changes occur** für die Beschreibung ein. Wählen Sie Weiter aus.
6. Überprüfen Sie auf der Seite Vorschau anzeigen und erstellen Ihre Auswahl. Wählen Sie Bearbeiten, um Änderungen vorzunehmen, oder wählen Sie Alarm erstellen, um den Alarm zu erstellen.

Nachdem Sie den Alarm erstellt haben, CloudWatch wird die Seite Alarme geöffnet. In der Spalte Aktionen des Alarms wird Bestätigung ausstehend angezeigt, bis alle E-Mail-Empfänger zum Thema SNS bestätigt haben, dass sie SNS-Benachrichtigungen abonnieren möchten.

## Beispiele für AWS Management Console fehlgeschlagene Anmeldevorgänge

Gehen Sie wie folgt vor, um einen CloudWatch Amazon-Alarm zu erstellen, der ausgelöst wird, wenn innerhalb eines Zeitraums von fünf Minuten drei oder mehr AWS Management Console Anmeldefehler auftreten.

### Einen Metrikfilter erstellen

1. Öffnen Sie die CloudWatch Konsole unter <https://console.aws.amazon.com/cloudwatch/>.
2. Wählen Sie im Navigationsbereich unter Protokolle die Option Protokollgruppen aus.
3. Wählen Sie in der Liste von Protokollgruppen die Protokollgruppe aus, die Sie für Ihren Trail erstellt haben.
4. Wählen Sie im Menü Metrikfilter oder Aktionen die Option Metrikfilter erstellen aus.
5. Geben Sie auf der Seite Muster definieren unter Filtermuster erstellen Folgendes für Filtermuster ein.

```
{ ($.eventName = ConsoleLogin) && ($.errorMessage = "Failed authentication") }
```

6. Behalten Sie in Testmuster die Standardeinstellungen bei. Wählen Sie Weiter aus.
7. Geben Sie auf der Seite Metrik zuweisen für Filtername den Wert **ConsoleSignInFailures** ein.

8. Aktivieren Sie unter Metrikdetails die Option Neu erstellen und geben Sie dann für Namespace der Metrik den Wert **CloudTrailMetrics** ein.
9. Geben Sie für Metrikname den Wert **ConsoleSigninFailureCount** ein.
10. Geben Sie für Metrikwert den Wert **1** ein.
11. Lassen Sie den Standardwert leer.
12. Wählen Sie Weiter aus.
13. Überprüfen Sie auf der Seite Prüfen und erstellen Ihre Auswahl. Wählen Sie Metrikfilter erstellen, um den Filter zu erstellen, oder wählen Sie Bearbeiten, um zurückzugehen und Werte zu ändern.

## Alarm erstellen

Nachdem Sie den Metrikfilter erstellt haben, wird die Seite mit den Details zur CloudWatch Log-Log-Gruppe für Ihre CloudTrail Trail-Log-Gruppe geöffnet. Gehen Sie folgendermaßen vor, um einen Alarm zu erstellen.

1. Suchen Sie auf der Registerkarte Metrikfilter den in [the section called “Einen Metrikfilter erstellen”](#) erstellten Metrikfilter. Aktivieren Sie das Kontrollkästchen für den Metrikfilter. Wählen Sie in der Leiste Metrikfilter die Option Alarm erstellen aus.
2. Geben Sie auf der Seite Alarm erstellen unter Metrik und Bedingungen angeben Folgendes ein.
  - a. Bei Diagramm, wird die Linie basierend auf anderen Einstellungen, die Sie beim Erstellen Ihres Alarms vornehmen, auf **3** gesetzt.
  - b. Behalten Sie für Metrikname den aktuellen Metriknamen **ConsoleSigninFailureCount** bei.
  - c. Behalten Sie für Statistik den Standardwert **Sum** bei.
  - d. Behalten Sie für Zeitraum den Standardwert **5 minutes** bei.
  - e. Wählen Sie unter Bedingungen unter Schwellenwerttyp die Option Statisch aus.
  - f. Wählen Sie Größer/Gleich für Immer wenn ***metric\_name*** ist.
  - g. Geben Sie als Schwellenwert **3** ein.
  - h. Übernehmen Sie unter Zusätzliche Konfiguration die Standardeinstellungen. Wählen Sie Weiter aus.
3. Wählen Sie auf der Seite Aktionen konfigurieren für Benachrichtigung die Option Bei Alarm aus. Dies bedeutet, dass die Aktion ausgeführt wird, wenn der Schwellenwert von 3

Änderungsereignissen innerhalb von 5 Minuten überschritten `ConsoleSignInFailureCount` wird und sich im Alarmzustand befindet.

- a. Wählen Sie unter Benachrichtigung an folgendes SNS-Thema senden die Option Neues Thema erstellen aus.
- b. Geben Sie **ConsoleSignInFailures\_CloudWatch\_Alarms\_Topic** als Namen des neuen Amazon-SNS-Themas ein.
- c. Geben Sie unter E-Mail-Endpunkte, die die Benachrichtigung erhalten, die E-Mail-Adressen der Benutzer ein, die Benachrichtigungen erhalten sollen, wenn dieser Alarm ausgelöst wird. Trennen Sie E-Mail-Adressen durch Kommas.

Jeder E-Mail-Empfänger erhält eine E-Mail, in der er bestätigen muss, dass er das Amazon-SNS-Thema abonniert haben möchten.

- d. Wählen Sie Thema erstellen aus.
4. Überspringen Sie in diesem Beispiel die anderen Aktionstypen. Wählen Sie Weiter.
  5. Geben Sie auf der Seite Name und Beschreibung hinzufügen einen Anzeigenamen für den Alarm und eine Beschreibung ein. Geben Sie in diesem Beispiel **Console sign-in failures** für den Namen und **Raises alarms if more than 3 console sign-in failures occur in 5 minutes** für die Beschreibung ein. Wählen Sie Weiter aus.
  6. Überprüfen Sie auf der Seite Vorschau anzeigen und erstellen Ihre Auswahl. Wählen Sie Bearbeiten, um Änderungen vorzunehmen, oder wählen Sie Alarm erstellen, um den Alarm zu erstellen.

Nachdem Sie den Alarm erstellt haben, CloudWatch wird die Seite Alarme geöffnet. In der Spalte Aktionen des Alarms wird Bestätigung ausstehend angezeigt, bis alle E-Mail-Empfänger zum Thema SNS bestätigt haben, dass sie SNS-Benachrichtigungen abonnieren möchten.

## Beispiel: Änderungen an der IAM-Richtlinie

Gehen Sie wie folgt vor, um einen CloudWatch Amazon-Alarm zu erstellen, der ausgelöst wird, wenn ein API-Aufruf zur Änderung einer IAM-Richtlinie erfolgt.

### Einen Metrikfilter erstellen

1. Öffnen Sie die CloudWatch Konsole unter <https://console.aws.amazon.com/cloudwatch/>.
2. Wählen Sie im Navigationsbereich Protokolle aus.

3. Wählen Sie in der Liste von Protokollgruppen die Protokollgruppe aus, die Sie für Ihren Trail erstellt haben.
4. Wählen Sie Aktionen und dann Metrikfilter erstellen.
5. Geben Sie auf der Seite Muster definieren unter Filtermuster erstellen Folgendes für Filtermuster ein.

```
{ ($.eventName=DeleteGroupPolicy)||($.eventName=DeleteRolePolicy)||
 ($.eventName=DeleteUserPolicy)||($.eventName=PutGroupPolicy)||
 ($.eventName=PutRolePolicy)||($.eventName=PutUserPolicy)||
 ($.eventName=CreatePolicy)||($.eventName=DeletePolicy)||
 ($.eventName=CreatePolicyVersion)||($.eventName=DeletePolicyVersion)||
 ($.eventName=AttachRolePolicy)||($.eventName=DetachRolePolicy)||
 ($.eventName=AttachUserPolicy)||($.eventName=DetachUserPolicy)||
 ($.eventName=AttachGroupPolicy)||($.eventName=DetachGroupPolicy)}
```

6. Behalten Sie in Testmuster die Standardeinstellungen bei. Wählen Sie Weiter aus.
7. Geben Sie auf der Seite Metrik zuweisen für Filtername den Wert **IAMPolicyChanges** ein.
8. Aktivieren Sie unter Metrikdetails die Option Neu erstellen und geben Sie dann für Namespace der Metrik den Wert **CloudTrailMetrics** ein.
9. Geben Sie für Metrikname den Wert **IAMPolicyEventCount** ein.
10. Geben Sie für Metrikwert den Wert **1** ein.
11. Lassen Sie den Standardwert leer.
12. Wählen Sie Weiter aus.
13. Überprüfen Sie auf der Seite Prüfen und erstellen Ihre Auswahl. Wählen Sie Metrikfilter erstellen, um den Filter zu erstellen, oder wählen Sie Bearbeiten, um zurückzugehen und Werte zu ändern.

## Alarm erstellen

Nachdem Sie den Metrikfilter erstellt haben, wird die Seite mit den Details zur CloudWatch Log-Log-Gruppe für Ihre CloudTrail Trail-Log-Gruppe geöffnet. Gehen Sie folgendermaßen vor, um einen Alarm zu erstellen.

1. Suchen Sie auf der Registerkarte Metrikfilter den in [the section called “Einen Metrikfilter erstellen”](#) erstellten Metrikfilter. Aktivieren Sie das Kontrollkästchen für den Metrikfilter. Wählen Sie in der Leiste Metrikfilter die Option Alarm erstellen aus.
2. Geben Sie auf der Seite Alarm erstellen unter Metrik und Bedingungen angeben Folgendes ein.

- a. Bei Diagramm, wird die Linie basierend auf anderen Einstellungen, die Sie beim Erstellen Ihres Alarms vornehmen, auf **1** gesetzt.
  - b. Behalten Sie für Metrikname den aktuellen Metriknamen **IAMPolicyEventCount** bei.
  - c. Behalten Sie für Statistik den Standardwert **Sum** bei.
  - d. Behalten Sie für Zeitraum den Standardwert **5 minutes** bei.
  - e. Wählen Sie unter Bedingungen unter Schwellenwerttyp die Option Statisch aus.
  - f. Wählen Sie Größer/Gleich für Immer wenn *metric\_name* ist.
  - g. Geben Sie als Schwellenwert **1** ein.
  - h. Übernehmen Sie unter Zusätzliche Konfiguration die Standardeinstellungen. Wählen Sie Weiter aus.
  - i.
3. Wählen Sie auf der Seite Aktionen konfigurieren für Benachrichtigung die Option Bei Alarm aus. Dies bedeutet, dass die Aktion ausgeführt wird, wenn der Schwellenwert von 1 Änderungsereignis innerhalb von 5 Minuten überschritten wird und IAM PolicyEventCount sich im Alarmstatus befindet.
    - a. Wählen Sie unter Benachrichtigung an folgendes SNS-Thema senden die Option Neues Thema erstellen aus.
    - b. Geben Sie **IAM\_Policy\_Changes\_CloudWatch\_Alarms\_Topic** als Namen des neuen Amazon-SNS-Themas ein.
    - c. Geben Sie unter E-Mail-Endpunkte, die die Benachrichtigung erhalten, die E-Mail-Adressen der Benutzer ein, die Benachrichtigungen erhalten sollen, wenn dieser Alarm ausgelöst wird. Trennen Sie E-Mail-Adressen durch Kommas.

Jeder E-Mail-Empfänger erhält eine E-Mail, in der er bestätigen muss, dass er das Amazon-SNS-Thema abonniert haben möchten.
    - d. Wählen Sie Thema erstellen aus.
  4. Überspringen Sie in diesem Beispiel die anderen Aktionstypen. Wählen Sie Weiter.
  5. Geben Sie auf der Seite Name und Beschreibung hinzufügen einen Anzeigenamen für den Alarm und eine Beschreibung ein. Geben Sie in diesem Beispiel **IAM Policy Changes** für den Namen und **Raises alarms if IAM policy changes occur** für die Beschreibung ein. Wählen Sie Weiter aus.

- Überprüfen Sie auf der Seite Vorschau anzeigen und erstellen Ihre Auswahl. Wählen Sie Bearbeiten, um Änderungen vorzunehmen, oder wählen Sie Alarm erstellen, um den Alarm zu erstellen.

Nachdem Sie den Alarm erstellt haben, CloudWatch wird die Seite Alarme geöffnet. In der Spalte Aktionen des Alarms wird Bestätigung ausstehend angezeigt, bis alle E-Mail-Empfänger zum Thema SNS bestätigt haben, dass sie SNS-Benachrichtigungen abonnieren möchten.

## Benachrichtigungen für CloudWatch Logs-Alarme konfigurieren

Sie können CloudWatch Logs so konfigurieren, dass eine Benachrichtigung gesendet wird, wenn ein Alarm ausgelöst wird. CloudTrail Auf diese Weise können Sie schnell auf kritische Betriebsereignisse reagieren, die in CloudTrail Ereignissen erfasst und in CloudWatch Protokollen erkannt werden. CloudWatch verwendet Amazon Simple Notification Service (SNS) zum Senden von E-Mails. Weitere Informationen finden Sie im CloudWatch Benutzerhandbuch unter [Amazon SNS SNS-Benachrichtigungen einrichten](#).

## Das Senden CloudTrail von Ereignissen an CloudWatch Logs beenden

Sie können das Senden von AWS CloudTrail Ereignissen an Amazon CloudWatch Logs beenden, indem Sie einen Trail aktualisieren, um die CloudWatch Logs-Einstellungen zu deaktivieren.

### Beenden Sie das Senden von Ereignissen an CloudWatch Logs (Konsole)

Um das Senden von CloudTrail Ereignissen an CloudWatch Logs zu beenden

- Melden Sie sich bei der an AWS Management Console und öffnen Sie die CloudTrail Konsole unter <https://console.aws.amazon.com/cloudtrail/>.
- Wählen Sie im Navigationsbereich Trails aus.
- Wählen Sie den Namen des Trails, für den Sie die CloudWatch Logs-Integration deaktivieren möchten.
- Wählen Sie unter CloudWatch Logs die Option Bearbeiten aus.
- Deaktivieren Sie das Kontrollkästchen Enabled (Aktiviert).
- Wählen Sie Änderungen speichern aus.



## Beenden Sie das Senden von Ereignissen an CloudWatch Logs (CLI)

Sie können die Protokollgruppe CloudWatch Logs als Übermittlungsendpunkt entfernen, indem [update-trail](#) Sie den Befehl ausführen. Mit dem folgenden Befehl werden die Protokollgruppe und die Rolle aus der Trail-Konfiguration gelöscht, indem die Werte für die Protokollgruppe ARN und die CloudWatch Protokollrolle ARN durch leere Werte ersetzt werden.

```
aws cloudtrail update-trail --name trail_name --cloud-watch-logs-log-group-arn="" --cloud-watch-logs-role-arn=""
```

## CloudWatch Benennung von Protokollgruppen und Protokolldatenströmen für CloudTrail

Amazon CloudWatch zeigt die Protokollgruppe, die Sie für CloudTrail Ereignisse erstellt haben, zusammen mit allen anderen Protokollgruppen an, die Sie in einer Region haben. Sie sollten einen Protokollgruppennamen verwenden, der es Ihnen ermöglicht, die Gruppe leicht von anderen zu unterscheiden. z. B. **CloudTrail/logs**.

Befolgen Sie die folgenden Richtlinien, wenn Sie eine Protokollgruppe benennen:

- Die Namen der Protokollgruppen müssen innerhalb einer Region für ein AWS-Konto eindeutig sein.
- Protokollgruppennamen können zwischen 1 und 512 Zeichen lang sein.
- Protokollgruppennamen bestehen aus den folgenden Zeichen: a–z, A–Z, 0–9, „\_“ (Unterstrich), „-“ (Bindestrich), „/“ (Schrägstrich), „.“ (Punkt) und „#“ (Raute).

*Wenn der Log-Stream für die Log-Gruppe CloudTrail erstellt wird, benennt es den Log-Stream nach dem folgenden Format: Account\_ID \_ CloudTrail \_ trail\_region.*

### Note

Wenn das Volumen der CloudTrail Protokolle groß ist, können mehrere Protokollstreams erstellt werden, um Protokolldaten an Ihre Protokollgruppe zu liefern. *Wenn es mehrere Protokollstreams gibt, CloudTrail benennt jeder Protokollstream im folgenden Format: Account\_ID \_ \_ trail\_region CloudTrail \_ number.*

Weitere Informationen zu CloudWatch Protokollgruppen finden Sie unter [Arbeiten mit Protokollgruppen und Protokollstreams](#) im Amazon CloudWatch Logs-Benutzerhandbuch und [CreateLogGroup](#) in der Amazon CloudWatch Logs-API-Referenz.

## Rollenrichtlinien-Dokument CloudTrail zur Verwendung von CloudWatch Logs zur Überwachung

In diesem Abschnitt wird die Berechtigungsrichtlinie beschrieben, die für die CloudTrail Rolle erforderlich ist, um Protokollereignisse an CloudWatch Logs zu senden. Sie können ein Richtliniendokument an eine Rolle anhängen, wenn Sie CloudTrail das Senden von Ereignissen konfigurieren, wie unter beschrieben [Ereignisse an CloudWatch Logs senden](#). Darüber hinaus können Sie auch eine Rolle mit IAM erstellen. Weitere Informationen finden Sie unter [Erstellen einer Rolle zum Delegieren von Berechtigungen an eine AWS-Service](#) oder [Erstellen einer IAM-Rolle \(AWS CLI\)](#).

Das folgende Beispielrichtliniendokument enthält die Berechtigungen, die erforderlich sind, um einen CloudWatch Protokollstream in der von Ihnen angegebenen Protokollgruppe zu erstellen und CloudTrail Ereignisse an diesen Protokollstream in der Region USA Ost (Ohio) zu übermitteln. (Dies ist die Standardrichtlinie für die Standard-IAM-Rolle `CloudTrail_CloudWatchLogs_Role`.)

### Note

[Der Schutz vor unverständlichen Stellvertretern](#) gilt nicht für die Rollenrichtlinie für die CloudWatch Protokollüberwachung. Die Rollenrichtlinie unterstützt die Verwendung von `aws:SourceArn` und nicht `aws:SourceAccount`.

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Sid": "AWSCloudTrailCreateLogStream2014110",
      "Effect": "Allow",
      "Action": [
        "logs:CreateLogStream"
      ],
      "Resource": [
        "arn:aws:logs:us-east-2:accountID:log-group:log_group_name:log-stream:CloudTrail_log_stream_name_prefix*"
      ]
    }
  ]
}
```

```

    ]
  },
  {
    "Sid": "AWSCloudTrailPutLogEvents20141101",
    "Effect": "Allow",
    "Action": [
      "logs:PutLogEvents"
    ],
    "Resource": [
      "arn:aws:logs:us-east-2:accountID:log-group:log_group_name:log-
stream:CloudTrail_log_stream_name_prefix*"
    ]
  }
]
}

```

Wenn Sie eine Richtlinie erstellen, die möglicherweise auch für Organisations-Trails verwendet wird, müssen Sie diese aus der für die Rolle erstellten Standardrichtlinie heraus ändern. *Die folgende Richtlinie gewährt beispielsweise die erforderlichen Berechtigungen, um in CloudTrail der Protokollgruppe, die Sie als Wert für `log_group_name` angeben, einen CloudWatch Log-Log-Stream zu erstellen und CloudTrail Ereignisse für diesen Log-Stream sowohl für Pfade im Konto 111111111111 als auch für Organisationspfade, die im AWS Konto 111111111111 erstellt wurden und auf die Organisation mit der ID `o-exampleorgid` angewendet werden, zu übermitteln: AWS Organizations*

```

{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Sid": "AWSCloudTrailCreateLogStream20141101",
      "Effect": "Allow",
      "Action": [
        "logs:CreateLogStream"
      ],
      "Resource": [
        "arn:aws:logs:us-east-2:111111111111:log-group:log_group_name:log-
stream:111111111111_CloudTrail_us-east-2*",
        "arn:aws:logs:us-east-2:111111111111:log-group:log_group_name:log-
stream:o-exampleorgid*"
      ]
    }
  ]
}

```

```
    },
    {
      "Sid": "AWSCloudTrailPutLogEvents20141101",
      "Effect": "Allow",
      "Action": [
        "logs:PutLogEvents"
      ],
      "Resource": [
        "arn:aws:logs:us-east-2:111111111111:log-group:log_group_name:log-stream:111111111111_CloudTrail_us-east-2*",
        "arn:aws:logs:us-east-2:111111111111:log-group:log_group_name:log-stream:o-exampleorgid_"
      ]
    }
  ]
}
```

Weitere Informationen zu Organisations-Trails finden Sie unter [Erstellen eines Trails für eine Organisation](#).

## Empfangen von CloudTrail Protokolldateien von mehreren Konten

Sie können Protokolldateien von mehreren AWS-Konten in einen einzigen Amazon S3 S3-Bucket CloudTrail liefern lassen. Sie haben beispielsweise vier AWS-Konten mit den Konto-IDs 111111111111, 2222222222, 333333333333 und 444444444444, und Sie möchten die Konfiguration so konfigurieren, dass Protokolldateien von allen vier dieser Konten an einen Bucket gesendet werden, der zum Konto 111111111111 gehört. CloudTrail Führen Sie dazu die Schritte in der angegebenen Reihenfolge aus:

1. Erstellen Sie einen Trail in dem Konto mit dem Ziel-Bucket (in diesem Beispiel 111111111111). Erstellen Sie noch keinen Trail für andere Konten.


Anweisungen finden Sie unter [Erstellen eines Trails in der Konsole](#).

2. Aktualisieren Sie die Bucket-Richtlinie für Ihren CloudTrail Ziel-Bucket, um kontoübergreifende Berechtigungen zu gewähren.

Anweisungen finden Sie unter [Festlegen der Bucket-Richtlinie für mehrere Konten](#).

3. Erstellen Sie einen Trail in anderen Konten (in diesem Beispiel 222222222222, 333333333333 und 444444444444) für den Sie Aktivitäten protokollieren können. Wenn Sie den Trail in jedem Konto erstellen, geben Sie den Amazon-S3-Bucket an, der zu dem Konto gehört, das Sie in

Schritt 1 angegeben haben (in diesem Beispiel 111111111111). Anweisungen finden Sie unter [Erstellen von Trails in zusätzlichen Konten](#).

 Note

Wenn Sie sich dafür entscheiden, die SSE-KMS-Verschlüsselung zu aktivieren, muss die KMS-Schlüsselrichtlinie die Verwendung des Schlüssels zum Verschlüsseln Ihrer Protokolldateien zulassen und den von Ihnen angegebenen Benutzern das Lesen von Protokolldateien in unverschlüsselter Form ermöglichen. CloudTrail Informationen zur manuellen Bearbeitung der Schlüsselrichtlinie finden Sie unter [Konfigurieren Sie AWS KMS wichtige Richtlinien für CloudTrail](#).

## Redigieren von Bucket-Eigentümer-Konto-IDs für Datenereignisse, die von anderen Konten aufgerufen werden

In AWS-Konto der Vergangenheit wurde, wenn CloudTrail Datenereignisse in einem Amazon S3 S3-Datenereignis-API-Aufrufer aktiviert waren, CloudTrail die Konto-ID des S3-Bucket-Besitzers im Datenereignis angezeigt (z. B. PutObject). Dies trat auch dann auf, wenn das Bucket-Eigentümerkonto S3-Datenereignisse nicht aktiviert hatte.

CloudTrail löscht nun die Konto-ID des S3-Bucket-Besitzers im `resources` Block, wenn beide der folgenden Bedingungen erfüllt sind:

- Der API-Aufruf für Datenereignisse stammt von einem anderen Benutzer AWS-Konto als dem Besitzer des Amazon S3 S3-Buckets.
- Der API-Aufrufer erhielt einen `AccessDenied`-Fehler, der nur für das Aufruferkonto galt.

Der Besitzer der Ressource, auf der der API-Aufruf durchgeführt wurde, erhält weiterhin das vollständige Ereignis.

Die folgenden Ereignisdatensnippets sind ein Beispiel für das erwartete Verhalten. Im `Historic`-Snippet wird die Konto-ID 123456789012 des S3-Bucket-Eigentümers einem API-Aufrufer aus einem anderen Konto angezeigt. Im Beispiel des aktuellen Verhaltens wird die Konto-ID des Bucket-Eigentümers nicht angezeigt.

```
# Historic
```

```
"resources": [  
  {  
    "type": "AWS::S3::Object",  
    "ARNPrefix": "arn:aws:s3:::test-my-bucket-2/"  
  },  
  {  
    "accountId": "123456789012",  
    "type": "AWS::S3::Bucket",  
    "ARN": "arn:aws:s3:::test-my-bucket-2"  
  }  
]
```

Das aktuelle Verhalten ist wie folgt.

```
# Current  
  
"resources": [  
  {  
    "type": "AWS::S3::Object",  
    "ARNPrefix": "arn:aws:s3:::test-my-bucket-2/"  
  },  
  {  
    "accountId": "",  
    "type": "AWS::S3::Bucket",  
    "ARN": "arn:aws:s3:::test-my-bucket-2"  
  }  
]
```

## Themen

- [Festlegen der Bucket-Richtlinie für mehrere Konten](#)
- [Erstellen von Trails in zusätzlichen Konten](#)

## Festlegen der Bucket-Richtlinie für mehrere Konten


Damit ein Bucket Protokolldateien von mehreren Konten empfangen kann, muss seine Bucket-Richtlinie die CloudTrail Berechtigung zum Schreiben von Protokolldateien von allen von Ihnen angegebenen Konten gewähren. Das bedeutet, dass Sie die Bucket-Richtlinie für Ihren Ziel-Bucket ändern müssen, um die CloudTrail Erlaubnis zu erteilen, Logdateien von jedem angegebenen Konto aus zu schreiben.

 Note

Aus Sicherheitsgründen können nicht autorisierte Benutzer einen Trail erstellen, der `AWLogs/` als `S3KeyPrefix`-Parameter enthält.

So ändern Sie Ihre Bucket-Berechtigungen, damit Dateien von mehreren Konten empfangen werden können

1. Melden Sie sich AWS Management Console mit dem Konto an, dem der Bucket gehört (in diesem Beispiel 111111111111), und öffnen Sie die Amazon S3 S3-Konsole.
2. Wählen Sie den Bucket aus, in den Ihre Protokolldateien CloudTrail geliefert werden, und wählen Sie dann Berechtigungen.
3. Wählen Sie unter Bucket policy (Bucket-Richtlinie) Edit (Bearbeiten) aus.
4. Ändern Sie die vorhandene Richtlinie und fügen Sie für jedes zusätzliche Konto, dessen Protokolldateien an diesen Bucket gesendet werden sollen, eine Zeile hinzu. Weitere Informationen finden Sie in der folgenden Beispielrichtlinie. Achten Sie auf die unterstrichene Resource-Zeile, die eine zweite Konto-ID angibt. Als bewährte Sicherheitsmethode gilt es, der Amazon S3-Bucket-Richtlinie einen `aws:SourceArn`-Bedingungsschlüssel hinzuzufügen. Dies verhindert unbefugten Zugriff auf Ihren S3-Bucket. Wenn bereits Trails vorhanden sind, fügen Sie unbedingt einen oder mehrere Bedingungsschlüssel hinzu.

 Note

Eine AWS Konto-ID ist eine zwölfstellige Zahl, einschließlich führender Nullen.

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Sid": "AWSCloudTrailAclCheck20131101",
      "Effect": "Allow",
      "Principal": {
        "Service": "cloudtrail.amazonaws.com"
      },
      "Action": "s3:GetBucketAcl",
      "Resource": "arn:aws:s3:::myBucketName",
```

```

    "Condition": {
      "StringEquals": {
        "aws:SourceArn": [
          "arn:aws:cloudtrail:region:111111111111:trail/primaryTrailName",
          "arn:aws:cloudtrail:region:222222222222:trail/secondaryTrailName"
        ]
      }
    },
    {
      "Sid": "AWSCloudTrailWrite20131101",
      "Effect": "Allow",
      "Principal": {
        "Service": "cloudtrail.amazonaws.com"
      },
      "Action": "s3:PutObject",
      "Resource": [
        "arn:aws:s3:::myBucketName/optionalLogFilePrefix/AWSLogs/111111111111/*",
        "arn:aws:s3:::myBucketName/optionalLogFilePrefix/AWSLogs/222222222222/*"
      ],
      "Condition": {
        "StringEquals": {
          "aws:SourceArn": [
            "arn:aws:cloudtrail:region:111111111111:trail/primaryTrailName",
            "arn:aws:cloudtrail:region:222222222222:trail/secondaryTrailName"
          ],
          "s3:x-amz-acl": "bucket-owner-full-control"
        }
      }
    }
  ]
}

```

## Erstellen von Trails in zusätzlichen Konten

Sie können die Konsole oder die verwenden AWS CLI , um zusätzliche Trails zu erstellen AWS-Konten und deren Protokolldateien in einem Amazon S3 S3-Bucket zusammenzufassen. Alternativ können Sie einen Organisationspfad erstellen AWS-Konten , um alle Mitglieder einer Organisation zu protokollieren AWS Organizations. Weitere Informationen finden Sie unter [Erstellen eines Trails für eine Organisation](#).



## Verwenden Sie die Konsole, um Trails für zusätzliche AWS Konten zu erstellen

Sie können die CloudTrail Konsole verwenden, um Trails in zusätzlichen Konten zu erstellen.

1. Melde dich AWS Management Console mit dem Konto an, für das du einen Trail erstellen möchtest. Befolgen Sie die Schritte unter [Erstellen eines Trails in der Konsole](#), um mit der Konsole einen Trail zu erstellen.
2. Wählen Sie für Storage location (Speicherort) die Option Use existing S3 bucket (Vorhandenen S3-Bucket verwenden) aus. Verwenden Sie das Textfeld, um den Namen des Buckets einzugeben, den Sie verwenden, um Protokolldateien in verschiedenen Konten zu speichern.

### Note

Die Bucket-Richtlinie muss die CloudTrail Schreibberechtigung für den Bucket gewähren. Informationen zur manuellen Bearbeitung der Bucket-Richtlinie finden Sie im Abschnitt [Festlegen der Bucket-Richtlinie für mehrere Konten](#).

#### Storage location [Info](#)

Create new S3 bucket  
Create a bucket to store logs for the trail.

Use existing S3 bucket  
Choose an existing bucket to store logs for this trail.

#### Trail log bucket name

Enter a new S3 bucket name and folder (prefix) to store your logs. Bucket names must be globally unique.

#### Prefix - optional

Logs will be stored in cross-account-bucket-name/cross-account-bucket-prefix/

3. Geben Sie unter Präfix das Präfix ein, das Sie zum kontenübergreifenden Speichern von Protokolldateien verwenden. Wenn Sie ein Präfix verwenden möchten, das sich von dem unterscheidet, was Sie in Ihrer Bucket-Richtlinie angegeben haben, müssen Sie die Bucket-Richtlinie in Ihrem Ziel-Bucket bearbeiten, CloudTrail damit Sie mit diesem neuen Präfix Protokolldateien in Ihren Bucket schreiben können.

## Verwenden der CLI zum Erstellen eines Trails in zusätzlichen AWS Konten

Sie können die AWS Befehlszeilentools verwenden, um Trails in zusätzlichen Konten zu erstellen und deren Protokolldateien in einem Amazon S3 S3-Bucket zusammenzufassen. Weitere Informationen zu diesen Tools finden Sie unter [cloudtrail](#) in der AWS CLI Befehlsreferenz.

Erstellen Sie mit dem Befehl `create-trail` einen Trail und geben Sie dabei Folgendes an:

- `--name` legt den Namen des Trails fest.
- `--s3-bucket-name` gibt den Amazon-S3-Bucket an, den Sie verwenden, um Protokolldateien in Konten zu speichern.
- `--s3-prefix` legt ein Präfix für den Protokolldatei-Übermittlungspfad fest (optional).
- `--is-multi-region-trail` gibt an, dass dieser Trail Ereignisse in allen AWS Regionen der Partition protokolliert, in der Sie arbeiten.

Sie können für jede Region, in der ein Konto AWS Ressourcen ausführt, einen Trail erstellen.

Der folgende Beispielbefehl zeigt, wie Sie mithilfe der AWS CLI einen Trail für zusätzliche Konten erstellen. Wenn Protokolldateien zu diesen Konten an den Bucket übertragen werden sollen, den Sie im ersten Konto (in diesem Beispiel 111111111111) erstellt haben, geben Sie den Namen des Buckets in der Option `--s3-bucket-name` an. Die Namen von Amazon-S3-Buckets sind global eindeutig.

```
aws cloudtrail create-trail --name my-trail --s3-bucket-name my-bucket --is-multi-region-trail
```

Wenn Sie den Befehl ausführen, wird eine Ausgabe ähnlich der Folgenden angezeigt:

```
{
  "IncludeGlobalServiceEvents": true,
  "Name": "AWSCloudTrailExample",
  "TrailARN": "arn:aws:cloudtrail:us-east-2:222222222222:trail/my-trail",
  "LogFileValidationEnabled": false,
  "IsMultiRegionTrail": true,
  "IsOrganizationTrail": false,
  "S3BucketName": "MyBucketBelongingToAccount111111111111"
}
```

Weitere Informationen zur Verwendung CloudTrail von Tools über die AWS Befehlszeile finden Sie in der [CloudTrail Befehlszeilenreferenz](#).

## CloudTrail Protokolldateien zwischen AWS Konten teilen

In diesem Abschnitt wird erklärt, wie CloudTrail Protokolldateien zwischen mehreren AWS Konten gemeinsam genutzt werden können. Welchen Ansatz Sie verwenden, um Logs gemeinsam zu nutzen, AWS-Konten hängt von der Konfiguration Ihres S3-Buckets ab. Dies sind die Optionen für das Freigeben von Protokolldateien:

- [Bucket-Eigentümer erzwungen](#) – [S3-Objekteigentümerschaft](#) ist eine Amazon-S3-Einstellung auf Bucket-Ebene, mit der Sie die Eigentümerschaft von Objekten steuern können, die in Ihre Buckets hochgeladen werden, und Zugriffssteuerungslisten (ACLs) deaktivieren oder aktivieren können. Standardmäßig ist die Objekteigentümerschaft auf die Einstellung Bucket-Eigentümer erzwungen festgelegt und alle ACLs sind deaktiviert. Wenn ACLs deaktiviert sind, besitzt der Bucket-Eigentümer alle Objekte im Bucket und verwaltet den Datenzugriff ausschließlich mithilfe von Zugriffsverwaltungsrichtlinien. Wenn die Option Bucket-Eigentümer erzwungen aktiviert ist, wird der Zugriff über die Bucket-Richtlinie verwaltet, sodass Benutzer keine Rolle übernehmen müssen.
- [Rolle für die gemeinsame Nutzung von Protokolldateien annehmen](#) – Wenn Sie die Einstellung Bucket-Eigentümer erzwungen nicht ausgewählt haben, müssen Benutzer eine Rolle übernehmen, um auf die Protokolldateien in Ihrem S3-Bucket zugreifen zu können.

## Freigeben von Protokolldateien zwischen Konten durch Annehmen einer Rolle

### Note

Dieser Abschnitt gilt nur für Amazon-S3-Buckets, die nicht die Einstellung Bucket-Eigentümer erzwungen verwenden.

In diesem Abschnitt wird erklärt, wie Sie CloudTrail Protokolldateien gemeinsam nutzen können, AWS-Konten indem Sie eine Rolle übernehmen, und es werden die Szenarien für die gemeinsame Nutzung von Protokolldateien beschrieben.


- Szenario 1: Gewähren Sie den schreibgeschützten Zugriff für die Konten, von denen die Protokolldateien generiert wurden, die sich im Amazon-S3-Bucket befinden.
- Szenario 2: Gewähren Sie einem Drittanbieter-Konto Zugriff auf alle Protokolldateien in Ihrem Amazon-S3-Bucket, das die Protokolldateien für Sie analysieren kann.

So gewähren Sie schreibgeschützten Zugriff auf die Protokolldateien in Ihrem Amazon-S3-Bucket

1. [Erstellen Sie eine IAM-Rolle](#) für jedes Konto, für das die Protokolldateien freigegeben werden sollen. Sie müssen ein Administrator sein, um die Berechtigung zu gewähren.

Gehen Sie wie folgt vor, wenn Sie die VPC erstellen:

- Wählen Sie die Option Anderes AWS-Konto.
- Geben Sie die zwölfstellige Konto-ID des Kontos ein, dem Zugriff gewährt werden soll.
- Aktivieren Sie das Kontrollkästchen MFA erforderlich, wenn der Benutzer vor Übernahme der Rolle eine Multifaktor-Authentifizierung ausführen soll.
- Wählen Sie die AmazonS3-Richtlinie aus ReadOnlyAccess.

 Note

Standardmäßig gewährt die ReadOnlyAccessAmazonS3-Richtlinie Abruf- und Listenrechte für alle Amazon S3 S3-Buckets in Ihrem Konto.

Weitere Informationen zur Berechtigungsverwaltung bei IAM-Rollen finden Sie unter [IAM-Rollen](#) im IAM-Benutzerhandbuch.


2. [Erstellen Sie eine Zugriffsrichtlinie](#), die dem Konto, für das Sie die Protokolldateien freigeben möchten, schreibgeschützten Zugriff gewährt.
3. Weisen Sie jedes Konto an, [eine Rolle beim Abrufen der Protokolldateien anzunehmen](#).

So gewähren Sie einem Drittanbieter-Konto schreibgeschützten Zugriff auf die Protokolldateien

1. [Erstellen Sie eine IAM-Rolle](#) für das Drittanbieterkonto, mit dem Sie Protokolldateien gemeinsam nutzen möchten. Sie müssen ein Administrator sein, um die Berechtigung zu gewähren.

Gehen Sie wie folgt vor, wenn Sie die VPC erstellen:

- Wählen Sie die Option **Anderes AWS-Konto**.
- Geben Sie die zwölfstellige Konto-ID des Kontos ein, dem Zugriff gewährt werden soll.
- Geben Sie eine externe ID an, mit der zusätzlich kontrolliert wird, wer die Rolle übernehmen kann. Weitere Informationen finden Sie im IAM-Benutzerhandbuch unter [So verwenden Sie eine externe ID, wenn Sie Dritten Zugriff auf Ihre AWS Ressourcen gewähren](#).
- Wählen Sie die AmazonS3-Richtlinie aus. **ReadOnlyAccess**

 **Note**

Standardmäßig gewährt die **ReadOnlyAccessAmazonS3**-Richtlinie Abruf- und Listenrechte für alle Amazon S3 S3-Buckets in Ihrem Konto.

2. [Erstellen Sie eine Zugriffsrichtlinie](#), die dem Drittanbieter-Konto, für das Sie die Protokolldateien freigeben möchten, schreibgeschützten Zugriff gewährt.
3. Weisen Sie das Drittanbieter-Konto an, [eine Rolle beim Abrufen der Protokolldateien anzunehmen](#).

In den folgenden Abschnitten erhalten Sie weitere Informationen zu diesen Schritten.

#### Themen

- [Erstellen einer vordefinierten Zugriffsrichtlinie, um Zugriff auf Konten, deren Inhaber Sie sind, zu gewähren](#)
- [Erstellen einer vordefinierten Zugriffsrichtlinie für den Zugriff für Dritte](#)
- [Übernehmen einer Rolle](#)
- [Beenden Sie die gemeinsame Nutzung von CloudTrail Protokolldateien zwischen Konten AWS](#)

### Erstellen einer vordefinierten Zugriffsrichtlinie, um Zugriff auf Konten, deren Inhaber Sie sind, zu gewähren

Als Besitzer des Amazon S3 S3-Buckets haben Sie die volle Kontrolle über den Amazon S3 S3-Bucket, in den Protokolldateien für die anderen Konten CloudTrail geschrieben werden. Sie möchten die Protokolldateien mit jeder Geschäftseinheit gemeinsam nutzen, die sie erstellt hat. Aber Sie möchten nicht, dass ein Geschäftsbereich die Protokolldateien eines anderen Geschäftsbereichs lesen kann.

Um beispielsweise die Protokolldateien des Kontos B mit Konto B, aber nicht mit Konto C zu teilen, müssen Sie eine neue IAM-Rolle in Ihrem Konto erstellen, die angibt, dass es sich bei Konto B um ein vertrauenswürdigen Konto handelt. Diese rollenbasierte Vertrauensrichtlinie gibt an, dass Konto B vertrauenswürdig ist, die von Ihrem Konto erstellte Rolle zu übernehmen, und sollte wie im folgenden Beispiel aussehen. Die Vertrauensrichtlinie wird automatisch erstellt, wenn Sie die Rolle mithilfe der Konsole anlegen. Wenn Sie die Rolle mit dem SDK erstellen, müssen Sie die Vertrauensrichtlinie als Parameter an die `CreateRole`-API übergeben. Wenn Sie die Rolle mit der CLI erstellen, müssen Sie die Vertrauensrichtlinie im CLI-Befehl `create-role` angeben.

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Sid": "",
      "Effect": "Allow",
      "Principal": {
        "AWS": "arn:aws:iam::account-B-id:root"
      },
      "Action": "sts:AssumeRole"
    }
  ]
}
```

Außerdem müssen Sie eine vordefinierte Zugriffsrichtlinie erstellen, um festzulegen, dass Konto B nur von dem Speicherort aus lesen kann, in den das Konto B die Protokolldateien schreibt. Die vordefinierte Zugriffsrichtlinie wird in etwa wie folgt aussehen. Beachten Sie, dass der Ressourcen-ARN die zwölfstellige Konto-ID für Konto B und gegebenenfalls das Präfix enthält, das Sie bei der Aktivierung CloudTrail für Konto B während des Aggregationsprozesses angegeben haben. Weitere Informationen zur Angabe eines Präfixes finden Sie unter [Erstellen von Trails in zusätzlichen Konten](#).

#### Important

Sie müssen sicherstellen, dass das Präfix in der Zugriffsrichtlinie genau mit dem Präfix übereinstimmt, das Sie bei der Aktivierung CloudTrail für Konto B angegeben haben. Ist dies nicht der Fall, müssen Sie die IAM-Rollenzugriffsrichtlinie in Ihrem Konto bearbeiten, um das tatsächliche Präfix für Konto B aufzunehmen. Wenn das Präfix in der Rollen zugriffsrichtlinie nicht genau mit dem Präfix übereinstimmt, das Sie bei der Aktivierung CloudTrail in Konto B angegeben haben, kann Konto B nicht auf seine Protokolldateien zugreifen.

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Action": [
        "s3:Get*",
        "s3:List*"
      ],
      "Resource": "arn:aws:s3:::bucket-name/prefix/AWSLogs/account-B-id/*"
    },
    {
      "Effect": "Allow",
      "Action": [
        "s3:Get*",
        "s3:List*"
      ],
      "Resource": "arn:aws:s3:::bucket-name"
    }
  ]
}
```

Verwenden Sie diesen Vorgang für alle weiteren Konten.

Nachdem Sie die Rollen für jedes Konto erstellt haben und die entsprechenden Vertrauens- und Zugriffsrichtlinien angegeben haben und nachdem einem IAM-Benutzer vom Administrator dieses Kontos in jedem Konto Zugriff gewährt wurde, kann ein IAM-Benutzer in den Konten B oder C die Rolle programmgesteuert übernehmen.

Weitere Informationen finden Sie unter [Übernehmen einer Rolle](#).

## Erstellen einer vordefinierten Zugriffsrichtlinie für den Zugriff für Dritte

Sie müssen eine separate IAM-Rolle für ein Drittanbieter-Konto erstellen. Wenn Sie die Rolle erstellen, erstellt AWS automatisch die Vertrauensbeziehung, die angibt, dass das Drittanbieter-Konto die Rolle übernehmen darf. Die vordefinierte Zugriffsrichtlinie für die Rolle gibt an, welche Aktionen dieses Konto durchführen kann. Weitere Informationen zum Erstellen von Rollen finden Sie unter [Erstellen einer IAM-Rolle](#).

Die von erstellte Vertrauensstellung AWS gibt beispielsweise an, dass dem Drittanbieterkonto (in diesem Beispiel Konto Z) die von Ihnen erstellte Rolle als vertrauenswürdig eingestuft wird. Im Folgenden finden Sie ein Beispiel für eine Vertrauensrichtlinie:

```
{
  "Version": "2012-10-17",
  "Statement": [{
    "Sid": "",
    "Effect": "Allow",
    "Principal": {"AWS": "arn:aws:iam::account-Z-id:root"},
    "Action": "sts:AssumeRole"
  }]
}
```

Wenn Sie bei der Erstellung der Rolle für das Drittanbieter-Konto eine externe ID angegeben haben, enthält Ihre Zugriffsrichtlinie ein zusätzliches Condition-Element, das die von diesem Konto zugewiesene eindeutige ID testet. Der Test wird durchgeführt, wenn die Rolle übernommen wird. Im folgenden Beispiel umfasst die Zugriffsrichtlinie ein Element Condition.

Weitere Informationen finden Sie im IAM-Benutzerhandbuch unter [So verwenden Sie eine externe ID, wenn Sie einem Dritten Zugriff auf Ihre AWS Ressourcen gewähren](#).

```
{
  "Version": "2012-10-17",
  "Statement": [{
    "Sid": "",
    "Effect": "Allow",
    "Principal": {"AWS": "arn:aws:iam::account-Z-id:root"},
    "Action": "sts:AssumeRole",
    "Condition": {"StringEquals": {"sts:ExternalId": "external-ID-issued-by-account-Z"}}
  }]
}
```

Sie müssen auch eine vordefinierte Zugriffsrichtlinie für die Rolle Ihres Kontos erstellen, um festzulegen, dass das Drittanbieter-Konto alle Protokolle im Amazon-S3-Bucket lesen kann. Die Zugriffsrichtlinie sollte etwa wie im folgenden Beispiel dargestellt aussehen. Der Platzhalter (\*) am Ende des Resource-Wertes gibt an, dass das Drittanbieter-Konto auf alle Protokolldateien im S3-Bucket zugreifen kann, für die ihm Zugriff erteilt wurde.

```
{
```



```
"Version": "2012-10-17",
"Statement": [
  {
    "Effect": "Allow",
    "Action": [
      "s3:Get*",
      "s3:List*"
    ],
    "Resource": "arn:aws:s3:::bucket-name/*"
  },
  {
    "Effect": "Allow",
    "Action": [
      "s3:Get*",
      "s3:List*"
    ],
    "Resource": "arn:aws:s3:::bucket-name"
  }
]
```

Nachdem Sie eine Rolle für das Drittanbieter-Konto erstellt und die entsprechende Vertrauensbeziehung und Zugriffsrichtlinie angegeben haben, muss ein IAM-Benutzer im Drittanbieter-Konto die Rolle programmgesteuert übernehmen, um Protokolldateien im Bucket lesen zu können. Weitere Informationen finden Sie unter [Übernehmen einer Rolle](#).

## Übernehmen einer Rolle

Sie müssen einen separaten IAM-Benutzer angeben, der jede Rolle übernimmt, die Sie in jedem Konto erstellen. Anschließend müssen Sie sicherstellen, dass jeder IAM-Benutzer über die entsprechenden Berechtigungen verfügt.

### IAM-Benutzer und -Rollen

Nach dem Erstellen der erforderlichen Rollen und Richtlinien müssen Sie in den Konten, für die Sie Dateien freigeben möchten, einen IAM-Benutzer zuordnen. Jeder IAM-Benutzer übernimmt programmatisch die entsprechende Rolle für den Zugriff auf die Protokolldateien. Wenn ein Benutzer eine Rolle übernimmt, gibt AWS temporäre Sicherheitsanmeldeinformationen an diesen Benutzer. Sie können dann Anfragen zum Auflisten, Abrufen, Kopieren oder Löschen von Protokolldateien stellen, abhängig von den Berechtigungen, die durch die der Rolle zugeordnete Zugriffsrichtlinie gewährt wurden.

Weitere Informationen zum Arbeiten mit IAM-Identitäten finden Sie unter [IAM-Identitäten \(Benutzer, Benutzergruppen und Rollen\)](#).

Der Hauptunterschied besteht in der Zugriffsrichtlinie, die Sie für jede IAM-Rolle in den einzelnen Szenarien erstellen.

- In Szenario 1 beschränkt die Zugriffsrichtlinie jedes Konto darauf, nur seine eigenen Protokolldateien lesen zu können. Weitere Informationen finden Sie unter [Erstellen einer vordefinierten Zugriffsrichtlinie, um Zugriff auf Konten, deren Inhaber Sie sind, zu gewähren](#).
- In Szenario 2 erlaubt die Zugriffsrichtlinie einem Drittanbieter, alle Protokolldateien zu lesen, die im Amazon S3-Bucket zusammengefasst sind. Weitere Informationen finden Sie unter [Erstellen einer vordefinierten Zugriffsrichtlinie für den Zugriff für Dritte](#).

## Erstellen von Berechtigungsrichtlinien für IAM-Benutzer


Um die von einer Rolle erlaubten Aktionen ausführen zu können, muss der IAM-Benutzer über die Berechtigung verfügen, die API aufzurufen. AWS STS [AssumeRole](#) Sie müssen die Richtlinie für die einzelnen Benutzer bearbeiten, um ihnen die entsprechenden Berechtigungen zu gewähren. Dafür müssen Sie ein Ressourcenelement in der Richtlinie festlegen, die Sie dem IAM-Benutzer anfügen. Das folgende Beispiel zeigt eine Richtlinie für einen IAM-Benutzer in einem anderen Konto, die es diesem Benutzer erlaubt, eine Rolle namens Test zu übernehmen, die zuvor von Konto A erstellt wurde.

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Action": ["sts:AssumeRole"],
      "Resource": "arn:aws:iam::account-A-id:role/Test"
    }
  ]
}
```

So bearbeiten Sie eine vom Kunden verwaltete Richtlinie (Konsole)

1. [Melden Sie sich bei der an AWS Management Console und öffnen Sie die IAM-Konsole unter https://console.aws.amazon.com/iam/.](https://console.aws.amazon.com/iam/)

2. Wählen Sie im Navigationsbereich Richtlinien.
3. Wählen Sie in der Richtlinienliste den Namen der zu bearbeitenden Richtlinie. Sie können über das Suchfeld die Liste der Gruppen filtern.
4. Wählen Sie die Registerkarte Berechtigungen und anschließend Richtlinie bearbeiten aus.
5. Führen Sie eine der folgenden Aktionen aus:
  - Wählen Sie die Option Visual aus, um Ihre Richtlinie zu ändern, ohne mit der JSON-Syntax vertraut sein zu müssen. Sie können Änderungen am Service, an Aktionen, Ressourcen oder optionalen Bedingungen für jeden Berechtigungsblock in Ihrer Richtlinie vornehmen. Sie können auch eine Richtlinie importieren, um unten in der Richtlinie zusätzliche Berechtigungen hinzuzufügen. Wenn Sie alle gewünschten Änderungen vorgenommen haben, wählen Sie Weiter aus, um fortzufahren.
  - Wählen Sie die Option JSON aus, um Ihre Richtlinie zu ändern, indem Sie Text in das JSON-Textfeld eingeben oder einfügen. Sie können auch eine Richtlinie importieren, um unten in der Richtlinie zusätzliche Berechtigungen hinzuzufügen. Beheben Sie alle Sicherheitswarnungen, Fehler oder allgemeinen Warnungen, die während der [Richtlinien-Validierung](#) erzeugt wurden, und wählen Sie dann Weiter.

 Note

Sie können jederzeit zwischen den Editoroptionen Visual und JSON wechseln. Wenn Sie jedoch Änderungen vornehmen oder im Visual-Editor Weiter wählen, strukturiert IAM Ihre Richtlinie möglicherweise um, um sie für den visuellen Editor zu optimieren. Weitere Informationen finden Sie unter [Richtlinienrestrukturierung](#) im IAM-Benutzerhandbuch.

6. Überprüfen Sie auf der Seite Überprüfen und Speichern den Bereich In dieser Richtlinie definierte Berechtigungen und wählen Sie dann Änderungen speichern aus, um Ihre Arbeit zu speichern.
7. Wenn die verwaltete Richtlinie bereits das Maximum von fünf Versionen aufweist, wird ein Dialogfeld angezeigt, wenn Sie Save changes (Änderungen speichern) auswählen. Damit Ihre neue Version gespeichert wird, wird die älteste Version der Richtlinie, die nicht die Standardversion ist, entfernt und durch diese neue Version ersetzt. Optional können Sie die neue Version als Standardversion der Richtlinie einrichten.

Wählen Sie Änderungen speichern aus, um Ihre neue Richtlinienversion zu speichern.

## Rufen Sie an AssumeRole

Ein Benutzer kann eine Rolle übernehmen, indem er eine Anwendung erstellt, die die AWS STS [AssumeRole](#) API aufruft und den Namen der Rollensitzung, die Amazon-Ressourcennummer (ARN) der zu übernehmenden Rolle und eine optionale externe ID übergibt. Der Rollensitzungsname wird vom Konto definiert, das die zu übernehmende Rolle erstellt hat. Die externe ID, falls vorhanden, wird vom Drittanbieter-Konto definiert und an das besitzende Konto weitergegeben, damit sie bei der Rollenerstellung berücksichtigt wird. Weitere Informationen finden Sie im IAM-Benutzerhandbuch unter [So verwenden Sie eine externe ID, wenn Sie Dritten Zugriff auf Ihre AWS Ressourcen gewähren](#). Sie können die ARN von Konto A abrufen, indem Sie die IAM-Konsole öffnen.

So finden Sie den ARN-Wert in Konto A mit der IAM-Konsole

1. Wählen Sie Rollen.
2. Wählen Sie die Rolle aus, die Sie überprüfen möchten.
3. Suchen Sie Rolle ARN im Abschnitt Zusammenfassung.

Die AssumeRole API gibt temporäre Anmeldeinformationen zurück, die für den Zugriff auf Ressourcen im eigenen Konto verwendet werden können. In diesem Beispiel sind die Ressourcen, auf die Sie zugreifen möchten, der Amazon-S3-Bucket und die in diesem Bucket enthaltenen Protokolldateien. Die temporären Anmeldeinformationen verfügen über die von Ihnen in der vordefinierten Rollen-Zugriffsrichtlinie festgelegten Berechtigungen.

Das folgende Python-Beispiel (unter Verwendung von [AWS SDK for Python \(Boto\)](#)) zeigt, wie AssumeRole aufgerufen und wie die zurückgegebenen temporären Sicherheitsanmeldeinformationen verwendet werden können, um alle durch Konto A gesteuerten Amazon-S3-Buckets aufzulisten.

```
def list_buckets_from_assumed_role(user_key, assume_role_arn, session_name):
    """
    Assumes a role that grants permission to list the Amazon S3 buckets in the account.
    Uses the temporary credentials from the role to list the buckets that are owned
    by the assumed role's account.

    :param user_key: The access key of a user that has permission to assume the role.
    :param assume_role_arn: The Amazon Resource Name (ARN) of the role that
                           grants access to list the other account's buckets.
    :param session_name: The name of the STS session.
    """
```

```
sts_client = boto3.client(
    "sts", aws_access_key_id=user_key.id, aws_secret_access_key=user_key.secret
)
try:
    response = sts_client.assume_role(
        RoleArn=assume_role_arn, RoleSessionName=session_name
    )
    temp_credentials = response["Credentials"]
    print(f"Assumed role {assume_role_arn} and got temporary credentials.")
except ClientError as error:
    print(
        f"Couldn't assume role {assume_role_arn}. Here's why: "
        f"{error.response['Error']['Message']}"
    )
    raise

# Create an S3 resource that can access the account with the temporary credentials.
s3_resource = boto3.resource(
    "s3",
    aws_access_key_id=temp_credentials["AccessKeyId"],
    aws_secret_access_key=temp_credentials["SecretAccessKey"],
    aws_session_token=temp_credentials["SessionToken"],
)
print(f"Listing buckets for the assumed role's account:")
try:
    for bucket in s3_resource.buckets.all():
        print(bucket.name)
except ClientError as error:
    print(
        f"Couldn't list buckets for the account. Here's why: "
        f"{error.response['Error']['Message']}"
    )
    raise
```

## Beenden Sie die gemeinsame Nutzung von CloudTrail Protokolldateien zwischen Konten AWS

Um die gemeinsame Nutzung von Protokolldateien für andere Benutzer zu beenden AWS-Konto, löschen Sie die Rolle, die Sie für dieses Konto erstellt haben. Weitere Informationen zum Löschen von Rollen finden Sie unter [Löschen von Rollen oder Instance-Profilen](#).

# Überprüfen der Integrität der CloudTrail Protokolldatei

Um festzustellen, ob eine Protokolldatei nach CloudTrail der Übermittlung geändert, gelöscht oder unverändert wurde, können Sie die Integritätsprüfung der CloudTrail Protokolldatei verwenden. Dieses Feature wurde mit dem Branchenstandard entsprechenden Algorithmen entwickelt: SHA-256 für die Hashfunktion und SHA-256 mit RSA für digitale Signaturen. Dadurch ist es rechnerisch unmöglich, CloudTrail Protokolldateien unbemerkt zu ändern, zu löschen oder zu fälschen. Sie können den verwenden AWS CLI , um die Dateien an dem Ort zu validieren, an dem sie CloudTrail geliefert wurden.

## Warum sollten Sie diese Funktion nutzen?

Validierte Protokolldateien sind bei Sicherheits- und kriminaltechnischen Ermittlungen unersetzlich. Beispiel: Mit einer validierten Protokolldatei können Sie bestätigen, dass die Protokolldatei selbst nicht geändert wurde oder dass mit bestimmten Benutzeranmeldeinformationen spezifische API-Aktivitäten ausgeführt wurden. Der Prozess zur Überprüfung der Integrität von CloudTrail Protokolldateien informiert Sie auch darüber, ob eine Protokolldatei gelöscht oder geändert wurde, oder bestätigt, dass in einem bestimmten Zeitraum keine Protokolldateien an Ihr Konto übermittelt wurden.

## Funktionsweise

Wenn Sie die Überprüfung der Integrität von Protokolldateien aktivieren, CloudTrail wird für jede übermittelte Protokolldatei ein Hash erstellt. CloudTrail Außerdem wird jede Stunde eine Datei erstellt und bereitgestellt, die auf die Protokolldateien der letzten Stunde verweist und jeweils einen Hash enthält. Diese Datei wird als Digest-Datei bezeichnet. CloudTrail signiert jede Digest-Datei mit dem privaten Schlüssel eines öffentlichen und privaten key pair. Nach der Lieferung können Sie den öffentlichen Schlüssel verwenden, um die Digest-Datei zu validieren. CloudTrail verwendet jeweils AWS-Region unterschiedliche Schlüsselpaare.

Die Digest-Dateien werden an denselben Amazon S3 S3-Bucket übermittelt, der mit Ihrem Trail verknüpft ist wie Ihre CloudTrail Protokolldateien. Wenn Ihre Protokolldateien aus allen Regionen oder von mehreren Konten in einen einzigen Amazon S3 S3-Bucket geliefert CloudTrail werden, werden die Digest-Dateien aus diesen Regionen und Konten in denselben Bucket übertragen.

Die Digest-Dateien werden in einem anderen Ordner gespeichert als die Protokolldateien. Diese Trennung von Digest- und Protokolldateien ermöglicht Ihnen das Erzwingen der differenzierten Sicherheitsrichtlinien und stellt sicher, dass eine vorhandene Protokollverarbeitung ohne Änderung lauffähig bleibt. Jede Digest-Datei enthält außerdem die digitale Signatur der vorherigen Digest-

Datei, sofern eine vorhanden ist. Die Signatur für die aktuelle Digest-Datei ist in den Metadaten-Eigenschaften des Amazon-S3-Objekts der Digest-Datei gespeichert. Weitere Informationen über Inhalte von Digest-Dateien finden Sie unter [CloudTrail Struktur der Digest-Datei](#).

## Speichern von Protokoll- und Digest-Dateien

Sie können die CloudTrail Protokolldateien und Digest-Dateien auf unbestimmte Zeit sicher, dauerhaft und kostengünstig in Amazon S3 oder S3 Glacier speichern. Zur Verbesserung der Sicherheit der Digest-Dateien, die in Amazon S3 gespeichert sind, können Sie [Amazon S3 MFA Delete](#) verwenden.

## Aktivieren der Validierung und Validieren der Dateien

Um die Integritätsprüfung der Protokolldatei zu aktivieren, können Sie die API AWS Management Console, die oder verwenden. AWS CLI CloudTrail Wenn Sie die Integritätsprüfung für Protokolldateien aktivieren CloudTrail , können Sie Digest-Protokolldateien an Ihren Amazon S3 S3-Bucket senden, die Integrität der Dateien wird jedoch nicht überprüft. Weitere Informationen finden Sie unter [Aktivierung der Integritätsprüfung der Protokolldatei für CloudTrail](#).

Um die Integrität von CloudTrail Protokolldateien zu überprüfen, können Sie die Lösung verwenden AWS CLI oder eine eigene Lösung erstellen. Die AWS CLI validiert Dateien an dem Ort, CloudTrail an dem sie geliefert wurden. Wenn Sie Protokolle validieren möchten, die Sie an einen anderen Speicherort, entweder in Amazon S3 oder außerhalb, verschoben haben, können Sie eigene Validierungstools entwickeln.

Informationen zur Validierung von Protokollen mithilfe von finden Sie AWS CLI unter [Überprüfen der Integrität der CloudTrail Protokolldatei mit dem AWS CLI](#). Hinweise zur Entwicklung benutzerdefinierter Implementierungen der CloudTrail Protokolldateiüberprüfung finden Sie unter [Benutzerdefinierte Implementierungen der CloudTrail Integritätsprüfung von Protokolldateien](#)

## Aktivierung der Integritätsprüfung der Protokolldatei für CloudTrail

Sie können die Überprüfung der Integrität von Protokolldateien mithilfe der AWS Management Console AWS Befehlszeilenschnittstelle (AWS CLI) oder der CloudTrail API aktivieren. CloudTrail beginnt in etwa einer Stunde mit der Bereitstellung von Digest-Dateien.

### AWS Management Console

Um die Integritätsprüfung der Protokolldatei mit der CloudTrail Konsole zu aktivieren, wählen Sie Ja für die Option Überprüfung der Protokolldatei aktivieren, wenn Sie einen Trail erstellen oder

aktualisieren. Standardmäßig ist diese Funktion für neue Trails aktiviert. Weitere Informationen finden Sie unter [Erstellen und Aktualisieren eines Trails mit der Konsole](#).

## AWS CLI

Um die Integritätsprüfung der Protokolldatei mit dem zu aktivieren AWS CLI, verwenden Sie die `--enable-log-file-validation` Option mit den Befehlen [create-trail](#) oder [update-trail](#). Sie können die Integritätsvalidierung für Protokolldateien mit der Option `--no-enable-log-file-validation` deaktivieren.

### Beispiel

Der folgende `update-trail`-Befehl ermöglicht die Protokolldateivalidierung und beginnt mit der Zustellung von Digest-Dateien im Amazon-S3-Bucket für den angegebenen Trail.

```
aws cloudtrail update-trail --name your-trail-name --enable-log-file-validation
```

## CloudTrail API

Um die Integritätsprüfung der Protokolldatei mit der CloudTrail API zu aktivieren, setzen Sie den `EnableLogFileValidation` Anforderungsparameter auf, `true` wenn Sie `CreateTrail` oder `updateTrail` aufrufen.

Weitere Informationen finden Sie unter [CreateTrail](#) und [UpdateTrail](#) in der [AWS CloudTrail API-Referenz](#).

## Überprüfen der Integrität der CloudTrail Protokolldatei mit dem AWS CLI

Verwenden Sie den CloudTrail `validate-logs` Befehl AWS Command Line Interface, um Protokolle mit dem zu validieren. Der Befehl verwendet die Digest-Dateien, die an den Amazon-S3-Bucket gesendet wurden, um die Validierung durchzuführen. Weitere Informationen über Digest-Dateien finden Sie unter [CloudTrail Struktur der Digest-Datei](#).

Der AWS CLI ermöglicht es Ihnen, die folgenden Arten von Änderungen zu erkennen:

- Änderung oder Löschung von CloudTrail Protokolldateien
- Änderung oder Löschung von CloudTrail Digest-Dateien
- Änderung oder Löschung von Protokoll- und Digest-Dateien



**Note**

Das AWS CLI validiert nur Protokolldateien, auf die von Digestdateien verwiesen wird. Weitere Informationen finden Sie unter [Es wird geprüft, ob eine bestimmte Datei geliefert wurde von CloudTrail](#).

## Voraussetzungen

Um die Integrität der Protokolldatei mit der zu überprüfen AWS CLI, müssen die folgenden Bedingungen erfüllt sein:

- Sie müssen über eine Online-Verbindung zu verfügen AWS.
- Sie müssen über Lesezugriff auf den Amazon-S3-Bucket verfügen, der die Digest- und Protokolldateien enthält.
- Die Digest- und Protokolldateien dürfen nicht von dem ursprünglichen Amazon S3 S3-Speicherort verschoben worden sein, CloudTrail an dem sie geliefert wurden.

**Note**

Protokolldateien, die auf einen lokalen Datenträger heruntergeladen wurden, können mit der AWS CLI nicht validiert werden. Eine Anleitung zum Erstellen Ihrer eigenen Tools zur Validierung finden Sie unter [Benutzerdefinierte Implementierungen der CloudTrail Integritätsprüfung von Protokolldateien](#).

## validate-logs

### Syntax

Im Folgenden wird die Syntax für `validate-logs` beschrieben. Optionale Parameter sind in Klammern angegeben.

```
aws cloudtrail validate-logs --trail-arn <trailARN> --start-time <start-time> [--end-time <end-time>] [--s3-bucket <bucket-name>] [--s3-prefix <prefix>] [--account-id <account-id>] [--verbose]
```

**Note**

Der Befehl `validate-logs` ist regionsspezifisch. Sie müssen die `--region` globale Option angeben, um Protokolle für einen bestimmten AWS-Region Bereich zu validieren.

**Optionen**

Im Folgenden werden die Befehlszeilen-Optionen für `validate-logs` aufgeführt. Die Optionen `--trail-arn` und `--start-time` sind erforderlich. Die Option `--account-id` ist zusätzlich für organisatorische Trails erforderlich.

**--start-time**

Gibt an, dass die Protokolldateien, die an oder nach dem angegebenen UTC-Zeitstempelwert zugestellt wurden, validiert werden. Beispiel: `2015-01-08T05:21:42Z`.

**--end-time**

Gibt optional an, dass die Protokolldateien, die an oder vor dem angegebenen UTC-Zeitstempelwert zugestellt wurden, validiert werden. Der Standardwert ist die aktuelle UTC-Zeit (`Date.now()`). Beispiel: `2015-01-08T12:31:41Z`.

**Note**

Für den angegebenen Zeitraum werden mit dem `validate-logs`-Befehl nur die Protokolldateien geprüft, auf die in den entsprechenden Digest-Dateien verwiesen wird. Andere Protokolldateien im Amazon-S3-Bucket werden nicht geprüft. Weitere Informationen finden Sie unter [Es wird geprüft, ob eine bestimmte Datei geliefert wurde von CloudTrail](#).

**--s3-bucket**

Gibt optional den Amazon-S3-Bucket an, in dem die Digest-Dateien gespeichert sind. Wenn kein Bucket-Name angegeben ist, AWS CLI ruft sie ihn durch einen Aufruf `abDescribeTrails()`.

## --s3-prefix

Gibt optional das Amazon-S3-Präfix an, mit dem die Digest-Dateien gespeichert sind. Wenn nicht angegeben, AWS CLI ruft sie ihn durch einen Aufruf `abDescribeTrails()`.

### Note

Verwenden Sie diese Option nur, wenn Ihr aktuelles Präfix nicht mit dem Präfix identisch ist, das in dem angegebenen Zeitraum verwendet wurde.

## --account-id

Gibt optional das Konto für die Validierung von Protokollen an. Dieser Parameter ist für Organisations-Trails zur Validierung von Protokollen für das jeweilige Konto innerhalb einer Organisation erforderlich.

## --trail-arn

Gibt den Amazon-Ressourcennamen (ARN) des zu validierenden Trails an. Nachfolgend ist das Format eines Trail-ARN angegeben.

```
arn:aws:cloudtrail:us-east-2:111111111111:trail/MyTrailName
```

### Note

Zum Abrufen des Trail-ARN für einen Trail können Sie den `describe-trails`-Befehl verwenden, bevor Sie `validate-logs` ausführen.

Sie können den Bucket-Namen und das Präfix zusätzlich zum Trail-ARN angeben, wenn Protokolldateien in dem von Ihnen angegebenen Zeitraum an mehrere Buckets gesendet wurden und Sie die Validierung auf die Protokolldateien in nur einem der Buckets beschränken möchten.

## --verbose

Gibt optional Validierungsinformationen für jede Protokoll- oder Digest-Datei in dem angegebenen Zeitraum aus. Die Ausgabe gibt an, ob die Datei unverändert ist oder geändert bzw. gelöscht

wurde. Im Non-Verbose-Modus (Standard) werden Informationen nur für die Fälle zurückgegeben, in denen Fehler bei der Validierung aufgetreten sind.

## Beispiel

Im folgenden Beispiel werden die Protokolldateien von der angegebenen Anfangszeit bis zum aktuellen Zeitpunkt mit dem Amazon-S3-Bucket, der für den aktuellen Trail konfiguriert ist, und unter Angabe der ausführlichen Ausgabe validiert.

```
aws cloudtrail validate-logs --start-time 2015-08-27T00:00:00Z --end-time
2015-08-28T00:00:00Z --trail-arn arn:aws:cloudtrail:us-east-2:111111111111:trail/my-
trail-name --verbose
```

## Funktionsweise von **validate-logs**

Der `validate-logs`-Befehl beginnt mit der Validierung der letzten Digest-Datei in dem angegebenen Zeitraum. Zunächst wird überprüft, dass die Digest-Datei von dem Speicherort heruntergeladen wurde, zu dem sie angeblich gehört. Mit anderen Worten, wenn die CLI die Digest-Datei `df1` vom S3-Speicherort `p1` herunterlädt, überprüft `validate-logs` das entsprechende `p1 == df1.digestS3Bucket + '/' + df1.digestS3Object`.

Wenn die Signatur der Digest-Datei gültig ist, wird der Hash-Wert jedes der Protokolle, auf die in der Digest-Datei verwiesen wird, überprüft. Der Befehl validiert dann nacheinander die vorherigen Digest-Dateien und ihre referenzierten Protokolldateien. Der Vorgang wird so lange fortgesetzt, bis der angegebene Wert für `start-time` erreicht ist oder die Digest-Kette endet. Wenn eine Digest-Datei fehlt oder ungültig ist, wird der Zeitraum, der nicht validiert werden kann, in der Ausgabe angegeben.

## Validierungsergebnisse

Validierungsergebnisse beginnen mit einem Zusammenfassungs-Header in folgendem Format:

```
Validating log files for trail trail_ARN between time_stamp and time_stamp
```

Jede Zeile der Hauptausgabe enthält die Validierungsergebnisse für eine einzelne Digest- oder Protokolldatei in folgendem Format:

```
<Digest file | Log file> <S3 path> <Validation Message>
```

Die folgende Tabelle beschreibt die möglichen Validierungsmeldungen für Protokoll- und Digest-Dateien.

Dateityp	Validierungsmeldung	Beschreibung
Digest file	valid	Die Signatur der Digest-Datei ist gültig. Die Protokolldateien, auf die sie verweist, können überprüft werden. Diese Meldung ist nur im Verbose-Modus enthalten.
Digest file	INVALID: has been moved from its original location	Der S3-Bucket oder das S3-Objekt, aus dem die Digest-Datei abgerufen wurde, stimmt nicht mit den S3-Bucket- oder S3-Objekt-Speicherorten überein, die in der Digest-Datei selbst aufgezeichnet sind.
Digest file	INVALID: invalid format	Das Format der Digest-Datei ist ungültig. Die Protokolldateien, die dem Zeitraum entsprechen, den die Digest-Datei repräsentiert, können nicht validiert werden.
Digest file	INVALID: not found	Die Digest-Datei wurde nicht gefunden. Die Protokolldateien, die dem Zeitraum entsprechen, den die Digest-Datei repräsentiert, können nicht validiert werden.
Digest file	INVALID: public key not found for fingerprint <i>Fingerabdruck</i>	Der öffentliche Schlüssel, der zu dem Fingerabdruck in der Digest-Datei gehört, wurde nicht gefunden. Die Digest-Datei kann nicht validiert werden.
Digest file	INVALID: signature verification failed	Die Signatur der Digest-Datei ist ungültig. Da die Digest-Datei ungültig ist, können die Protokolldateien, auf die sie verweist, nicht validiert werden, und es können keine Aussagen über die darin enthaltenen API-Aktivitäten getroffen werden.

Dateityp	Validierungsmeldung	Beschreibung
Digest file	INVALID: Unable to load PKCS #1 key with fingerprint <i>Fingerabdruck</i>	Da der DER-codierte öffentliche Schlüssel im PKCS # 1-Format mit dem angegebenen Fingerabdruck nicht geladen werden konnte, kann die Digest-Datei nicht validiert werden.
Log file	valid	Die Protokolldatei wurde validiert und seit der Bereitstellung nicht geändert. Diese Meldung ist nur im Verbose-Modus enthalten.
Log file	INVALID: hash value doesn't match	Der Hash für die Protokolldatei stimmt nicht überein. Die Protokolldatei wurde nach der Lieferung von geändert CloudTrail.
Log file	INVALID: invalid format	Das Format der Protokolldatei ist ungültig. Die Protokolldatei kann nicht validiert werden.
Log file	INVALID: not found	Die Protokolldatei wurde nicht gefunden und kann nicht validiert werden.

Die Ausgabe umfasst zusammenfassende Informationen über die zurückgegebenen Ergebnisse.

## Beispielausgaben

### Verbose

Der folgende `validate-logs`-Beispielbefehl verwendet das Flag `--verbose` und erzeugt die folgende Beispielausgabe. [...] gibt an, dass die Beispielausgabe gekürzt wurde.

```
aws cloudtrail validate-logs --trail-arn arn:aws:cloudtrail:us-east-2:111111111111:trail/example-trail-name --start-time 2015-08-31T22:00:00Z --end-time 2015-09-01T19:17:29Z --verbose
```

```
Validating log files for trail arn:aws:cloudtrail:us-east-2:111111111111:trail/example-trail-name between 2015-08-31T22:00:00Z and 2015-09-01T19:17:29Z
```

```
Digest file    s3://example-bucket/AWSLogs/111111111111/CloudTrail-Digest/us-
east-2/2015/09/01/111111111111_CloudTrail-Digest_us-east-2_example-trail-name_us-
east-2_20150901T201728Z.json.gz valid
Log file      s3://example-bucket/AWSLogs/111111111111/
CloudTrail/us-east-2/2015/09/01/111111111111_CloudTrail_us-
east-2_20150901T1925Z_WZZw1RymnjCRjxXc.json.gz valid
Log file      s3://example-bucket/AWSLogs/111111111111/
CloudTrail/us-east-2/2015/09/01/111111111111_CloudTrail_us-
east-2_20150901T1915Z_POuvV87nu6pfAV2W.json.gz valid
Log file      s3://example-bucket/AWSLogs/111111111111/
CloudTrail/us-east-2/2015/09/01/111111111111_CloudTrail_us-
east-2_20150901T1930Z_l2QgXhAKVm1QXiIA.json.gz valid
Log file      s3://example-bucket/AWSLogs/111111111111/
CloudTrail/us-east-2/2015/09/01/111111111111_CloudTrail_us-
east-2_20150901T1920Z_eQJteBBrfpBCq0qw.json.gz valid
Log file      s3://example-bucket/AWSLogs/111111111111/
CloudTrail/us-east-2/2015/09/01/111111111111_CloudTrail_us-
east-2_20150901T1950Z_9g5A6qlR2B5KaRdq.json.gz valid
Log file      s3://example-bucket/AWSLogs/111111111111/
CloudTrail/us-east-2/2015/09/01/111111111111_CloudTrail_us-
east-2_20150901T1920Z_i4DNCC12BuXd6Ru7.json.gz valid
Log file      s3://example-bucket/AWSLogs/111111111111/
CloudTrail/us-east-2/2015/09/01/111111111111_CloudTrail_us-
east-2_20150901T1915Z_Sg5caf2RH6Jdx0EJ.json.gz valid
Digest file    s3://example-bucket/AWSLogs/111111111111/CloudTrail-Digest/us-
east-2/2015/09/01/111111111111_CloudTrail-Digest_us-east-2_example-trail-name_us-
east-2_20150901T191728Z.json.gz valid
Log file      s3://example-bucket/AWSLogs/111111111111/
CloudTrail/us-east-2/2015/09/01/111111111111_CloudTrail_us-
east-2_20150901T1910Z_YYSFiuFQk4nrtnEW.json.gz valid
[...]
Log file      s3://example-bucket/AWSLogs/144218288521/
CloudTrail/us-east-2/2015/09/01/144218288521_CloudTrail_us-
east-2_20150901T1055Z_0Sfy6m9f6iBzmoPF.json.gz valid
Log file      s3://example-bucket/AWSLogs/144218288521/
CloudTrail/us-east-2/2015/09/01/144218288521_CloudTrail_us-
east-2_20150901T1040Z_lLa3QzVLp0ed7igR.json.gz valid

Digest file    s3://example-bucket/AWSLogs/144218288521/CloudTrail-Digest/us-
east-2/2015/09/01/144218288521_CloudTrail-Digest_us-east-2_example-trail-name_us-
east-2_20150901T101728Z.json.gz INVALID: signature verification failed
```

```
Digest file    s3://example-bucket/AWSLogs/144218288521/CloudTrail-Digest/us-
east-2/2015/09/01/144218288521_CloudTrail-Digest_us-east-2_example-trail-name_us-
east-2_20150901T091728Z.json.gz valid
Log file      s3://example-bucket/AWSLogs/144218288521/
CloudTrail/us-east-2/2015/09/01/144218288521_CloudTrail_us-
east-2_20150901T0830Z_eaFv03dwHo4NCqqc.json.gz valid
Digest file    s3://example-bucket/AWSLogs/144218288521/CloudTrail-Digest/us-
east-2/2015/09/01/144218288521_CloudTrail-Digest_us-east-2_example-trail-name_us-
east-2_20150901T081728Z.json.gz valid
Digest file    s3://example-bucket/AWSLogs/144218288521/CloudTrail-Digest/us-
east-2/2015/09/01/144218288521_CloudTrail-Digest_us-east-2_example-trail-name_us-
east-2_20150901T071728Z.json.gz valid
[...]
Log file      s3://example-bucket/AWSLogs/111111111111/
CloudTrail/us-east-2/2015/08/31/111111111111_CloudTrail_us-
east-2_20150831T2245Z_mbJkE05kNcDnVhGh.json.gz valid
Log file      s3://example-bucket/AWSLogs/111111111111/
CloudTrail/us-east-2/2015/08/31/111111111111_CloudTrail_us-
east-2_20150831T2225Z_IQ6kXy8sKU03RSPr.json.gz valid
Log file      s3://example-bucket/AWSLogs/111111111111/
CloudTrail/us-east-2/2015/08/31/111111111111_CloudTrail_us-
east-2_20150831T2230Z_eRPVRTxHQ5498ROA.json.gz valid
Log file      s3://example-bucket/AWSLogs/111111111111/
CloudTrail/us-east-2/2015/08/31/111111111111_CloudTrail_us-
east-2_20150831T2255Z_IlWawYZGvTWB5vYN.json.gz valid
Digest file    s3://example-bucket/AWSLogs/111111111111/CloudTrail-Digest/us-
east-2/2015/08/31/111111111111_CloudTrail-Digest_us-east-2_example-trail-name_us-
east-2_20150831T221728Z.json.gz valid

Results requested for 2015-08-31T22:00:00Z to 2015-09-01T19:17:29Z
Results found for 2015-08-31T22:17:28Z to 2015-09-01T20:17:28Z:

22/23 digest files valid, 1/23 digest files INVALID
63/63 log files valid
```

## Non-Verbose

Der folgende `validate-logs`-Beispielbefehl verwendet kein `--verbose`-Flag. In der folgenden Beispielausgabe wurde ein Fehler gefunden. Es werden nur Header-, Fehler- und Zusammenfassungsinformationen zurückgegeben.



```
aws cloudtrail validate-logs --trail-arn arn:aws:cloudtrail:us-east-2:111111111111:trail/example-trail-name --start-time 2015-08-31T22:00:00Z --end-time 2015-09-01T19:17:29Z
```

```
Validating log files for trail arn:aws:cloudtrail:us-east-2:111111111111:trail/example-trail-name between 2015-08-31T22:00:00Z and 2015-09-01T19:17:29Z
```

```
Digest file s3://example-bucket/AWSLogs/144218288521/CloudTrail-Digest/us-east-2/2015/09/01/144218288521_CloudTrail-Digest_us-east-2_example-trail-name_us-east-2_20150901T101728Z.json.gz INVALID: signature verification failed
```

```
Results requested for 2015-08-31T22:00:00Z to 2015-09-01T19:17:29Z  
Results found for 2015-08-31T22:17:28Z to 2015-09-01T20:17:28Z:
```

```
22/23 digest files valid, 1/23 digest files INVALID  
63/63 log files valid
```

## Es wird geprüft, ob eine bestimmte Datei geliefert wurde von CloudTrail

Um zu überprüfen, ob eine bestimmte Datei in Ihrem Bucket von zugestellt wurde CloudTrail, führen Sie den Vorgang für den Zeitraum, der die Datei enthält, `validate-logs` im ausführlichen Modus aus. Wenn die Datei in der Ausgabe von `validate-logs` erscheint, dann wurde die Datei geliefert von CloudTrail.

## CloudTrail Struktur der Digest-Datei

Jede Digest-Datei enthält die Namen der Protokolldateien, die während der letzten Stunde an den Amazon-S3-Bucket übermittelt wurden, die Hashwerte für diese Protokolldateien und die digitalen Signaturen der vorherigen Digest-Datei. Die Signatur für die aktuelle Digest-Datei ist in den Metadateneigenschaften des Digest-Dateiobjekts gespeichert. Die digitalen Signaturen und Hashwerte werden zur Validierung der Integrität der Protokolldateien und der Digest-Datei selbst verwendet.

## Speicherort von Digest-Dateien

Digest-Dateien werden an einen Amazon-S3-Bucket-Speicherort übermittelt, der dieser Syntax folgt.

```
s3://s3-bucket-name/optional-prefix/AWSLogs/aws-account-id/CloudTrail-Digest/  
region/digest-end-year/digest-end-month/digest-end-date/
```

```
aws-account-id_CloudTrail-Digest_region_trail-
name_region_digest_end_timestamp.json.gz
```

### Note

Für Organisationstrails enthält der Bucket-Speicherort auch die ID der Organisationseinheit, wie folgt:

```
s3://s3-bucket-name/optional-prefix/AWSLogs/0-ID/aws-account-id/CloudTrail-
Digest/
region/digest-end-year/digest-end-month/digest-end-date/
aws-account-id_CloudTrail-Digest_region_trail-
name_region_digest_end_timestamp.json.gz
```

## Inhalt von Digest-Beispieldateien

Die folgende Beispiel-Digest-Datei enthält Informationen für ein CloudTrail Protokoll.

```
{
  "awsAccountId": "111122223333",
  "digestStartTime": "2015-08-17T14:01:31Z",
  "digestEndTime": "2015-08-17T15:01:31Z",
  "digestS3Bucket": "S3-bucket-name",
  "digestS3Object": "AWSLogs/111122223333/CloudTrail-Digest/us-
east-2/2015/08/17/111122223333_CloudTrail-Digest_us-east-2_your-trail-name_us-
east-2_20150817T150131Z.json.gz",
  "digestPublicKeyFingerprint": "31e8b5433410dfb61a9dc45cc65b22ff",
  "digestSignatureAlgorithm": "SHA256withRSA",
  "newestEventTime": "2015-08-17T14:52:27Z",
  "oldestEventTime": "2015-08-17T14:42:27Z",
  "previousDigestS3Bucket": "S3-bucket-name",
  "previousDigestS3Object": "AWSLogs/111122223333/CloudTrail-Digest/us-
east-2/2015/08/17/111122223333_CloudTrail-Digest_us-east-2_your-trail-name_us-
east-2_20150817T140131Z.json.gz",
  "previousDigestHashValue":
  "97fb791cf91ffc440d274f8190dbdd9aa09c34432aba82739df18b6d3c13df2d",
  "previousDigestHashAlgorithm": "SHA-256",
  "previousDigestSignature":
  "50887ccffad4c002b97caa37cc9dc626e3c680207d41d27fa5835458e066e0d3652fc4dfc30937e4d5f4cc7f796e7
  "logFiles": [
```

```
{
  "s3Bucket": "S3-bucket-name",
  "s3Object": "AWSLogs/111122223333/CloudTrail/us-
east-2/2015/08/17/111122223333_CloudTrail_us-
east-2_20150817T1445Z_9nYN7gp2eWAJHIIfT.json.gz",
  "hashValue": "9bb6196fc6b84d6f075a56548feca262bd99ba3c2de41b618e5b6e22c1fc71f6",
  "hashAlgorithm": "SHA-256",
  "newestEventTime": "2015-08-17T14:52:27Z",
  "oldestEventTime": "2015-08-17T14:42:27Z"
}
]
```

## Beschreibungen der Felder in Digest-Dateien

Im Folgenden sind Beschreibungen für die einzelnen Felder in der Digest-Datei aufgeführt:

### awsAccountId

Die AWS Konto-ID, für die die Digest-Datei geliefert wurde.

### digestStartTime

Der UTC-Startzeitraum, den die Digest-Datei abdeckt, wobei als Referenz die Zeit verwendet wird, bis zu der die Protokolldateien übermittelt wurden. CloudTrail Dies bedeutet, dass, wenn der Zeitraum [Ta, Tb] ist, die Digest-Datei alle Protokolldateien enthält, die zwischen Ta und Tb an den Kunden übermittelt wurden.

### digestEndTime

Der letzte UTC-Zeitraum, den die Digest-Datei abdeckt, wobei als Referenz die Zeit verwendet wird, bis zu der die Protokolldateien übermittelt wurden. CloudTrail Dies bedeutet, dass, wenn der Zeitraum [Ta, Tb] ist, die Digest-Datei alle Protokolldateien enthält, die zwischen Ta und Tb an den Kunden übermittelt wurden.

### digestS3Bucket

Der Name des Amazon-S3-Buckets, an den die aktuelle Digest-Datei übermittelt wurde.

## digestS3Object

Der Amazon-S3-Objektschlüssel (d. h. der Amazon-S3-Bucket-Speicherort) der aktuellen Digest-Datei. Die ersten beiden Regionen in der Zeichenfolge zeigen die Region an, aus der die Digest-Datei übermittelt wurde. Die letzte Region (nach `your-trail-name`) ist die Ursprungsregion des Trails. Die Ursprungsregion ist die Region, in der der Trail erstellt wurde. Bei einem Trail mit mehreren Regionen kann diese von der Region abweichen, aus der die Digest-Datei übermittelt wurde.

## newestEventTime

Die UTC-Zeit des letzten Ereignisses unter allen Ereignissen in den Protokolldateien im Digest.

## oldestEventTime

Die UTC-Zeit des ältesten Ereignisses unter allen Ereignissen in den Protokolldateien im Digest.

### Note

Wenn die Digest-Datei spät übermittelt wird, ist der `oldestEventTime`-Wert früher als der `digestStartTime`-Wert.

## previousDigestS3Bucket

Der Amazon-S3-Bucket, an den die vorherige Digest-Datei übermittelt wurde.

## previousDigestS3Object

Der Amazon-S3-Objektschlüssel (d. h. der Amazon-S3-Bucket-Speicherort) der vorherigen Digest-Datei.

## previousDigestHashValue

Der im Hexadezimalformat verschlüsselte Hashwert des unkomprimierten Inhalts der vorherigen Digest-Datei.

## previousDigestHashAlgorithm

Der Name des Hash-Algorithmus, der für das Hashing der vorherigen Digest-Datei verwendet wurde.

## publicKeyFingerprint

Der im Hexadezimalformat verschlüsselte Fingerabdruck des öffentlichen Schlüssels, der dem privaten Schlüssel entspricht, der zum Signieren dieser Digest-Datei verwendet wurde. Sie können die öffentlichen Schlüssel für den Zeitraum abrufen, der der Digest-Datei entspricht, indem Sie die AWS CLI oder die CloudTrail API verwenden. Von den zurückgegebenen öffentlichen Schlüsseln kann derjenige zum Validieren der Digest-Datei verwendet werden, dessen Fingerabdruck mit diesem Wert übereinstimmt. Informationen zum Abrufen von öffentlichen Schlüsseln für Digestdateien finden Sie im AWS CLI [list-public-keys](#) Befehl oder in der API. CloudTrail [ListPublicKeys](#)

### Note

CloudTrail verwendet pro Region unterschiedliche private/öffentliche Schlüsselpaare. Jede Digest-Datei ist mit einem für die jeweilige Region eindeutigen privaten Schlüssel signiert. Wenn Sie also eine Digest-Datei aus einer bestimmten Region validieren, müssen Sie in derselben Region nach dem entsprechenden öffentlichen Schlüssel suchen.

## digestSignatureAlgorithm

Der zum Signieren der Digest-Datei verwendete Algorithmus.

## logFiles.s3Bucket

Der Name des Amazon-S3-Buckets für die Protokolldatei.

## logFiles.s3Object

Der Amazon-S3-Objektschlüssel der aktuellen Protokolldatei.

## `logFiles.newestEventTime`

Die UTC-Uhrzeit des letzten Ereignisses in der Protokolldatei. Diese Uhrzeit entspricht auch dem Zeitstempel der Protokolldatei selbst.

## `logFiles.oldestEventTime`

Die UTC-Uhrzeit des ältesten Ereignisses in der Protokolldatei.

## `logFiles.hashValue`

Der im Hexadezimalformat verschlüsselte Hashwert des unkomprimierten Inhalts der Protokolldatei.

## `logFiles.hashAlgorithm`

Der für das Hashing der Protokolldatei verwendete Hash-Algorithmus.

## Digest-Startdatei

Beim Start der Integritätsvalidierung von Protokolldateien wird eine Digest-Startdatei erstellt. Eine Digest-Startdatei wird ebenfalls erstellt, wenn die Integritätsvalidierung von Protokolldateien erneut gestartet wird (wenn entweder die Integritätsvalidierung von Protokolldateien deaktiviert und anschließend erneut aktiviert wird oder wenn die Protokollierung beendet und anschließend erneut gestartet wird, wobei die Validierung aktiviert ist). In einer Digest-Startdatei sind die folgenden Felder mit Bezug auf die vorherige Digest-Datei leer:

- `previousDigestS3Bucket`
- `previousDigestS3Object`
- `previousDigestHashValue`
- `previousDigestHashAlgorithm`
- `previousDigestSignature`

## „Leere“ Digest-Dateien

CloudTrail stellt eine Digest-Datei auch dann bereit, wenn in Ihrem Konto während des Zeitraums von einer Stunde, für den die Digest-Datei steht, keine API-Aktivität stattgefunden hat. Dies kann nützlich

sein, wenn Sie sicherstellen müssen, dass während der in der Digest-Datei dargestellten Stunde keine Protokolldateien übermittelt wurden.

Das folgende Beispiel zeigt den Inhalt einer Digest-Datei, die eine Stunde aufzeichnete, in der keine API-Aktivitäten auftraten. Beachten Sie, dass das Feld `logFiles: [ ]` am Ende der Digest-Datei leer ist.

```
{
  "awsAccountId": "111122223333",
  "digestStartTime": "2015-08-20T17:01:31Z",
  "digestEndTime": "2015-08-20T18:01:31Z",
  "digestS3Bucket": "example-bucket-name",
  "digestS3Object": "AWSLogs/111122223333/CloudTrail-Digest/us-
east-2/2015/08/20/111122223333_CloudTrail-Digest_us-east-2_example-trail-name_us-
east-2_20150820T180131Z.json.gz",
  "digestPublicKeyFingerprint": "31e8b5433410dfb61a9dc45cc65b22ff",
  "digestSignatureAlgorithm": "SHA256withRSA",
  "newestEventTime": null,
  "oldestEventTime": null,
  "previousDigestS3Bucket": "example-bucket-name",
  "previousDigestS3Object": "AWSLogs/111122223333/CloudTrail-Digest/us-
east-2/2015/08/20/111122223333_CloudTrail-Digest_us-east-2_example-trail-name_us-
east-2_20150820T170131Z.json.gz",
  "previousDigestHashValue":
"ed96c4bac9eaa8fe9716ca0e515da51938be651b1db31d781956416a9d05cdfa",
  "previousDigestHashAlgorithm": "SHA-256",
  "previousDigestSignature":
"82705525fb0fe7f919f9434e5b7138cb41793c776c7414f3520c0242902daa8cc8286b29263d2627f2f259471c745
  "logFiles": [ ]
}
```

## Signatur der Digest-Datei

Die Signaturinformationen für eine Digest-Datei befinden sich in zwei Objektmetadaten-Eigenschaften des Amazon-S3-Digest-Dateiobjekts. Jede Digest-Datei weist die folgenden Metadateneinträge auf:

- `x-amz-meta-signature`

Der im Hexadezimalformat verschlüsselte Wert der Digest-Dateisignatur. Es folgt ein Beispiel für eine Signatur:

```
3be472336fa2989ef34de1b3c1bf851f59eb030eaff3e2fb6600a082a23f4c6a82966565b994f9de4a5989d053d9d  
28f1cc237f372264a51b611c01da429565def703539f4e71009051769469231bc22232fa260df02740047af532229  
05d3ffcb5d2dd5dc28f8bb5b7993938e8a5f912a82b448a367eccb2ec0f198ba71e23eb0b97278cf65f3c8d1e652c
```

- `x-amz-meta-signature-algorithm`

Das folgende Beispiel zeigt einen Wert des zum Erstellen der Digest-Signatur verwendeten Algorithmus:

```
SHA256withRSA
```

## Verkettung von Digest-Dateien

Die Tatsache, dass jede Digest-Datei einen Verweis auf ihre vorherige Digest-Datei enthält, ermöglicht eine „Verkettung“, mit der Validierungstools wie die AWS CLI erkennen können, ob eine Digest-Datei gelöscht wurde. Außerdem ermöglicht diese Tatsache eine sukzessive Prüfung der Digest-Dateien in einem angegebenen Zeitraum, beginnend mit der aktuellen Datei.

### Note

Wenn Sie die Integritätsprüfung der Protokolldatei deaktivieren, ist die Kette der Digestdateien nach einer Stunde unterbrochen. CloudTrail erstellt keine Digest-Dateien für Protokolldateien, die während eines Zeitraums übermittelt wurden, in dem die Überprüfung der Integrität der Protokolldateien deaktiviert war. Wenn Sie beispielsweise die Integritätsvalidierung von Protokolldateien am Mittag des 1. Januar aktivieren, am Mittag des 2. Januar deaktivieren und am Mittag des 10. Januar erneut aktivieren, werden keine Digest-Dateien für die Protokolldateien erstellt, die zwischen dem Mittag des 2. Januar und dem Mittag des 10. Januar übermittelt wurden. Das Gleiche gilt, wenn Sie die CloudTrail Protokollierung beenden oder einen Trail löschen.

Wenn die [S3-Bucket-Richtlinie](#) Ihres Trails falsch konfiguriert ist oder es zu CloudTrail einer unerwarteten Dienstunterbrechung kommt, erhalten Sie möglicherweise nicht alle oder einige Digest-Dateien. Führen Sie den [get-trail-status](#) Befehl aus und überprüfen Sie den `LatestDigestDeliveryError` Parameter auf Fehler, um zu überprüfen, ob Ihr Trail Fehler bei der Übermittlung der Digests aufweist. Sobald das Zustellungsproblem behoben ist (z. B. durch Korrektur der Bucket-Richtlinie), CloudTrail wird versucht, alle fehlenden Digest-Dateien erneut zuzustellen.



Während des Zeitraums für die erneute Zustellung werden die Digest-Dateien möglicherweise nicht in der richtigen Reihenfolge zugestellt, sodass die Kette vorübergehend anscheinend unterbrochen ist.

Wenn die Protokollierung gestoppt oder der Trail gelöscht wird, CloudTrail wird eine endgültige Übersichtsdatei geliefert. Diese Digest-Datei kann Informationen für alle verbleibenden Protokolldateien enthalten, die Ereignisse bis einschließlich des Ereignisses `StopLogging` abdecken.

## Benutzerdefinierte Implementierungen der CloudTrail Integritätsprüfung von Protokolldateien

Da branchenübliche, offen verfügbare kryptografische Algorithmen und Hashfunktionen CloudTrail verwendet werden, können Sie Ihre eigenen Tools erstellen, um die Integrität von CloudTrail Protokolldateien zu überprüfen. Wenn die Integritätsprüfung der Protokolldatei aktiviert ist, werden CloudTrail Digest-Dateien an Ihren Amazon S3 S3-Bucket gesendet. Sie können diese Dateien zum Implementieren einer eigenen Validierungslösung verwenden. Weitere Informationen über Digest-Dateien finden Sie unter [CloudTrail Struktur der Digest-Datei](#).

In diesem Thema wird das Signieren von Digest-Dateien beschrieben. Zudem werden detailliert die Schritte dargelegt, die zur Implementierung einer Lösung für die Validierung von Digest-Dateien sowie den referenzierten Protokolldateien ausgeführt werden müssen.

### Verstehen Sie, wie CloudTrail Digest-Dateien signiert werden

CloudTrail Digest-Dateien werden mit digitalen RSA-Signaturen signiert. CloudTrail führt für jede Digest-Datei Folgendes aus:

1. Für die Datensignatur wird eine Zeichenfolge erstellt, die auf bestimmten Digest-Dateifeldern basiert (siehe nächster Abschnitt).
2. Ein privater Schlüssel, der für die Region eindeutig ist, wird abgerufen.
3. Der SHA-256-Hash der Zeichenfolge und der private Schlüssel werden an den RSA-Signaturalgorithmus übergeben, der die digitale Signatur generiert.
4. Der Byte-Signaturcode wird im Hexadezimalformat verschlüsselt.
5. Die digitale Signatur wird in der Metadateneigenschaft `x-amz-meta-signature` des Digest-Dateiobjekts von Amazon S3 bereitgestellt.

## Inhalt der Datensignatur-Zeichenfolge

Die folgenden CloudTrail Objekte sind in der Zeichenfolge für die Datensignierung enthalten:

- Letzter Zeitstempel der Digest-Datei im erweiterten UTC-Format (z. B. 2015-05-08T07:19:37Z)
- S3-Pfad der aktuellen Digest-Datei
- Im Hexadezimalformat verschlüsselter SHA-256-Hash der aktuellen Digest-Datei
- Im Hexadezimalformat verschlüsselte Signatur der vorherigen Digest-Datei

Das Format für die Zeichenfolgenberechnung und eine Beispielzeichenfolge finden Sie weiter unten in diesem Dokument.

## Schritte der benutzerdefinierten Validierungsimplementierung

Bei der Implementierung einer benutzerdefinierten Validierungslösung müssen Sie zunächst die Digest-Datei und anschließend die referenzierten Protokolldateien validieren.

### Validieren der Digest-Datei

Zur Validierung einer Digest-Datei benötigen Sie die Signatur, den öffentlichen Schlüssel, dessen privater Schlüssel zum Signieren verwendet wurde, und eine berechnete Datensignatur-Zeichenfolge.

1. Rufen Sie die Digest-Datei ab.
2. Überprüfen Sie, ob die Digest-Datei vom ursprünglichen Speicherort abgerufen wurde.
3. Rufen Sie die im Hexadezimalformat verschlüsselte Signatur der Digest-Datei ab.
4. Rufen Sie den im Hexadezimalformat verschlüsselten Fingerabdruck des öffentlichen Schlüssels ab, dessen privater Schlüssel zum Signieren der Digest-Datei verwendet wurde.
5. Rufen Sie die öffentlichen Schlüssel für den entsprechenden Zeitraum der Digest-Datei ab.
6. Wählen Sie aus den abgerufenen öffentlichen Schlüsseln denjenigen aus, dessen Fingerabdruck mit dem in der Digest-Datei übereinstimmt.
7. Verwenden Sie den Digest-Datei-Hash und weitere Digest-Dateifelder, um die Datensignatur-Zeichenfolge, anhand der die Digest-Dateisignatur überprüft wird, neu zu erstellen.
8. Überprüfen Sie die Signatur, indem Sie den SHA-256-Hash der Zeichenfolge, den öffentlichen Schlüssel und die Signatur als Parameter an den RSA-Signaturprüfalgorithmus übergeben. Wenn das Ergebnis „True“ lautet, ist die Digest-Datei gültig.

## Validieren der Protokolldateien

Wenn die Digest-Datei gültig ist, validieren Sie alle von der Digest-Datei referenzierten Protokolldateien.

1. Um die Integrität einer Protokolldatei zu validieren, wird der SHA-256-Hashwert für den unkomprimierten Inhalt berechnet und die Ergebnisse werden mit dem Hash für die Protokolldatei verglichen, der im Hexadezimalformat in der Digest-Datei erfasst ist. Stimmen die Hashwerte überein, ist die Protokolldatei gültig.
2. Validieren Sie nun anhand der Informationen über die vorherige Digest-Datei, die in der aktuellen Digest-Datei enthalten sind, die vorherige Digest-Datei und dann die entsprechenden Protokolldateien.

In den folgenden Abschnitten werden diese Schritte ausführlich beschrieben.

### A. Abrufen der Digest-Datei

Die ersten Schritte bestehen darin, die neueste Digest-Datei herunterzuladen und sicherzustellen, dass diese vom ursprünglichen Speicherort stammt, die digitale Signatur zu überprüfen und den Fingerabdruck des öffentlichen Schlüssels abzurufen.

1. Rufen Sie mithilfe von S3 [GetObject](#) oder der Klasse `AmazonS3Client` (z. B.) die neueste Digest-Datei aus Ihrem Amazon S3 S3-Bucket für den Zeitraum ab, den Sie validieren möchten.
2. Stellen Sie sicher, dass der S3-Bucket und das S3-Objekt für den Dateiabruf mit den Speicherorten des S3-Buckets und des S3-Objekts übereinstimmen, die in der Digest-Datei erfasst wurden.
3. Rufen Sie anschließend die digitale Signatur der Digest-Datei aus der Metadateneigenschaft `x-amz-meta-signature` des Digest-Dateiobjekts in Amazon S3 ab.
4. Rufen Sie in der Digest-Datei den Fingerabdruck des öffentlichen Schlüssels, dessen privater Schlüssel zum Signieren der Digest-Datei verwendet wurde, aus dem Feld `digestPublicKeyFingerprint` ab.

### B. Abrufen des öffentlichen Schlüssels zur Validierung der Digest-Datei

Um den öffentlichen Schlüssel zur Validierung der Digest-Datei zu erhalten, können Sie entweder die CLI oder die API verwenden. AWS CLI CloudTrail In beiden Fällen geben Sie einen Zeitraum (Start- und Endzeitpunkt) für die zu validierenden Digest-Dateien an. Für den angegebenen Zeitraum können ein

oder mehrere öffentliche Schlüssel zurückgegeben werden. Möglicherweise überschneiden sich die Gültigkeitszeiträume der zurückgegebenen Schlüssel.

### Note

Da pro Region unterschiedliche private/öffentliche Schlüsselpaare CloudTrail verwendet werden, ist jede Digest-Datei mit einem privaten Schlüssel signiert, der für ihre Region einzigartig ist. Wenn Sie also die Digest-Datei einer bestimmten Region validieren, müssen Sie den öffentlichen Schlüssel dieser Region abrufen.

Verwenden Sie die, um öffentliche Schlüssel abzurufen AWS CLI

Verwenden Sie den `cloudtrail list-public-keys` Befehl, um öffentliche Schlüssel für Digest-Dateien mithilfe von abzurufen. AWS CLI Der Befehl hat das folgende Format:

```
aws cloudtrail list-public-keys [--start-time <start-time>] [--end-time <end-time>]
```

Bei den Parametern für den Start- und den Endzeitpunkt handelt es sich um optionale UTC-Zeitstempel. Wenn diese Parameter nicht angegeben werden, wird die aktuelle Uhrzeit verwendet und der aktuell aktive öffentliche Schlüssel (oder mehrere) wird zurückgegeben.

### Beispielantwort

Die Antwort besteht aus einer Liste mit JSON-Objekten, die den bzw. die zurückgegebenen Schlüssel darstellen:

```
{
  "publicKeyList": [
    {
      "ValidityStartTime": "1436317441.0",
      "ValidityEndTime": "1438909441.0",
      "Value": "MIIBCgKCAQEA11L2YZ9h7onug2ILi1MwyHiMRsTQjfWE
+pHVRLk1QjfWhirG+lp0a8NrwQ/r7Ah5bNL6Hepzn0U9XTDSfmmnP97mqyc7z/upfZdS/AHhYcGaz7n6Wc/
RRBU6VmiPCrAUojuSk6/GjvA8i0PFsYDuBtviXarvuLPlrT9kAd4Lb+rFfR5peEgBEkh1zc5HuW07S0y
+KunqxX6jQBnXGMtxmPBPP0FylgWGNdFtks/4YSKcgqW0YDcawP9GGGDAeCIqPWIXDLG1j0jRRzWfCmD0iJUkz8vTsn4ho
      "Fingerprint": "8eba5db5bea9b640d1c96a77256fe7f2"
    },
    {
      "ValidityStartTime": "1434589460.0",
      "ValidityEndTime": "1437181460.0",
    }
  ]
}
```

```

    "Value": "MIIBCgKCAQEApfYL2FiZhpN74LNWVUzhR
+VheYhwhYm8w0n5Gf6i95y1W5kBAWKVEmnAQG7BvS5g9SMqFDQx52fW7NWV44IvfJ2xGXT
+wT+DgR6ZQ+6yxskQNqV5YcXj4Aa5Zz4jJfsYjDu02MDTZNIzNvBNzaBJ+r2WIWAJ/
Xq54kyF63B6WE38vKuDE7nSd1FqQuEoNBFLPInvgggYe2Ym1Refe2z71wNcJ2kY
+q0h1BShrSM8RWuJIw7MXwF9iQncg9jYzU1NJomozQzAG5wSRfbplcCYNY40xvGd/aAm00m+Y
+XFMrKwtLCwseHPvj843qVno6x4BJN9bpWnoPo9sdsbGoiK3QIDAQAB",
    "Fingerprint": "8933b39ddc64d26d8e14ffbf6566fee4"
  },
  {
    "ValidityStartTime": "1434589370.0",
    "ValidityEndTime": "1437181370.0",
    "Value":
      "MIIBIjANBgkqhkiG9w0BAQEFAAOCAQ8AMIIBCgKCAQEAqlzPJbvZJ42UdcmLfPUqXYNf0s6I81Cfao/
t0s8CmzP0EdtLWugB9xoIUz78qVhDKIqxbaG4jWHfJBi0SSFBM0lt8cdVo4TnRa7oG9io5pysS6DJhBBAeXsicufsiFJR
+wrUNh8RSLxL4k6G1+BhLX20tJkZ/erT97tDGBujAelqseGg3vPZbTx9SMf0LN65PdLFudLP7Gat0Z9p5jw/
rjpcLkfo9Bfc3heeBxWGKwBB0KnFAa9V57p0aosCvPKmHd9bg7jsQkI9Xp22IzGLsTFJZYVA3KiTAE1DMu80iFXPHEq9hK
+1utKVEiLkR2disdCmPTK0VQIDAQAB",
    "Fingerprint": "31e8b5433410dfb61a9dc45cc65b22ff"
  }
]
}

```

Verwenden Sie die CloudTrail API, um öffentliche Schlüssel abzurufen

Um öffentliche Schlüssel für Digest-Dateien mithilfe der CloudTrail API abzurufen, übergeben Sie Werte für die Startzeit und die Endzeit an die `ListPublicKeys` API. Die API `ListPublicKeys` gibt die öffentlichen Schlüssel, deren private Schlüssel zum Signieren der Digest-Dateien verwendet wurden, für den angegebenen Zeitraum zurück. Für jeden öffentlichen Schlüssel gibt die API außerdem den entsprechenden Fingerabdruck zurück.

## ListPublicKeys

In diesem Abschnitt werden die Anforderungsparameter sowie die Antwortelemente der `ListPublicKeys`-API beschrieben.

### Note

Hinsichtlich der Codierung der binären Felder von `ListPublicKeys` sind Änderungen vorbehalten.

## Anfrageparameter

Name	Beschreibung
<code>StartTime</code>	Gibt optional in UTC den Beginn des Zeitbereichs an, in dem nach öffentlichen Schlüsseln für CloudTrail Digest-Dateien gesucht werden soll. Wenn nicht angegeben, <code>StartTime</code> wird die aktuelle Uhrzeit verwendet und der aktuelle öffentliche Schlüssel wird zurückgegeben.  Typ: <code>DateTime</code>
<code>EndTime</code>	Gibt optional in UTC das Ende des Zeitbereichs an, in dem nach öffentlichen Schlüsseln für CloudTrail Digest-Dateien gesucht werden soll. Wenn nicht angegeben, <code>EndTime</code> wird die aktuelle Zeit verwendet.  Typ: <code>DateTime</code>

## Antwortelemente

`PublicKeyList` ist ein Array aus `PublicKey`-Objekten und enthält folgende Elemente:

Name	Beschreibung
<code>Value</code>	Dies gibt den mit DER-verschlüsselten öffentlichen Schlüsselwert im PKCS #1-Format an.  Typ: <code>Blob</code>
<code>ValidityStartTime</code>	Dies gibt den Beginn des Gültigkeitszeitraums für den öffentlichen Schlüssel an.  Typ: <code>DateTime</code>
<code>ValidityEndTime</code>	Dies gibt das Ende des Gültigkeitszeitraums für den öffentlichen Schlüssel an.  Typ: <code>DateTime</code>
<code>Fingerprint</code>	Die Fingerabdruck des öffentlichen Schlüssels. Mit dem Fingerabdruck kann der öffentliche Schlüssel identifiziert werden, der zur Validierung der Digest-Datei verwendet werden muss.

## Typ: Zeichenfolge

### C. Auswählen des öffentlichen Schlüssels für die Validierung

Wählen Sie aus den von `list-public-keys` oder `ListPublicKeys` abgerufenen öffentlichen Schlüsseln denjenigen aus, dessen Fingerabdruck mit dem Fingerabdruck im Feld `digestPublicKeyFingerprint` der Digest-Datei übereinstimmt. Diesen öffentlichen Schlüssel verwenden Sie für die Validierung der Digest-Datei.

### D. Neues Erstellen der Datensignatur-Zeichenfolge

Nachdem Sie über die Signatur der Digest-Datei und den entsprechenden öffentlichen Schlüssel verfügen, berechnen Sie die Datensignatur-Zeichenfolge. Wenn Sie die Datensignatur-Zeichenfolge berechnet haben, stehen Ihnen alle für die Signaturvalidierung benötigten Daten zur Verfügung.

Die Datensignatur-Zeichenfolge hat folgendes Format:

```
Data_To_Sign_String =  
  Digest_End_Timestamp_in_UTC_Extended_format + '\n' +  
  Current_Digest_File_S3_Path + '\n' +  
  Hex(Sha256(current-digest-file-content)) + '\n' +  
  Previous_digest_signature_in_hex
```

Ein `Data_To_Sign_String`-Beispiel folgt.

```
2015-08-12T04:01:31Z  
S3-bucket-name/AWSLogs/111122223333/CloudTrail-Digest/us-  
east-2/2015/08/12/111122223333_us-east-2_CloudTrail-Digest_us-  
east-2_20150812T040131Z.json.gz  
4ff08d7c6ecd6eb313257e839645d20363ee3784a2328a7d76b99b53cc9bcacd  
6e8540b83c3ac86a0312d971a225361d28ed0af20d70c211a2d405e32abf529a8145c2966e3bb47362383a52441545e  
d4c7c09dd152b84e79099ce7a9ec35d2b264eb92eb6e090f1e5ec5d40ec8a0729c02ff57f9e30d5343a8591638f8b79  
98b0aee2c1c8af74ec620261529265e83a9834ebef6054979d3e9a6767dfa6fdb4ae153436c567d6ae208f988047ccf
```

Wenn Sie diese Zeichenfolge neu erstellt haben, können Sie die Digest-Datei validieren.

## E. Validieren der Digest-Datei

Übergeben Sie den SHA-256-Hash der neu erstellten Datensignatur-Zeichenfolge, die digitale Signatur und den öffentlichen Schlüssel an den RSA-Signaturprüfalgorithmus. Wenn das Ergebnis „True“ lautet, wurde die Signatur der Digest-Datei überprüft und die Digest-Datei ist gültig.

## F. Validieren der Protokolldateien

Nachdem Sie die Digest-Dateien validiert haben, können Sie die referenzierten Protokolldateien überprüfen. Die Digest-Datei enthält die SHA-256-Hashwerte der Protokolldateien. Wenn eine der Protokolldateien nach der CloudTrail Lieferung geändert wurde, ändern sich die SHA-256-Hashes und die Signatur der Digest-Datei stimmt nicht überein.

Das folgende Beispiel veranschaulicht die Validierung der Protokolldateien:

1. Führen Sie einen S3 Get-Vorgang für die Protokolldatei aus. Verwenden Sie dabei die S3-Speicherortinformationen aus den Feldern `logFiles.s3Bucket` und `logFiles.s3Object`.
2. Sofern der S3 Get-Vorgang erfolgreich ist, führen Sie für die Protokolldateien, die im Array „logFiles“ der Digest-Datei aufgelistet sind, die folgenden Schritte aus:
  - a. Rufen Sie den ursprünglichen Hash der Datei aus dem Feld `logFiles.hashValue` des entsprechenden Protokolls in der Digest-Datei ab.
  - b. Führen Sie für den unkomprimierten Inhalt der Protokolldatei einen Hash mit dem Hash-Algorithmus in `logFiles.hashAlgorithm` aus.
  - c. Vergleichen Sie den generierten Hashwert mit dem Hashwert für das Protokoll in der Digest-Datei. Stimmen die Hashwerte überein, ist die Protokolldatei gültig.

## G. Validieren weiterer Digest- und Protokolldateien

In jeder Digest-Datei enthalten die folgenden Felder den Speicherort und die Signatur der vorherigen Digest-Datei:

- `previousDigestS3Bucket`
- `previousDigestS3Object`
- `previousDigestSignature`

Mithilfe der Schritte in den vorigen Abschnitten und mit diesen Informationen können Sie vorherige Digest-Dateien sequenziell aufrufen und die jeweilige Signatur sowie die referenzierten Protokolldateien validieren. Der einzige Unterschied besteht darin, dass Sie für vorherige



Digest-Dateien nicht die digitale Signatur aus den Amazon-S3-Metadateneigenschaften des Digest-Datei-Objekts abrufen müssen. Die Signatur der vorherigen Digest-Datei wird im Feld `previousDigestSignature` bereitgestellt.

Sie können bis zur ersten Digest-Datei oder bis zur Unterbrechung der Kette von Digest-Dateien zurückkehren, je nachdem, was zuerst auftritt.

## Ausführen der Offline-Validierung von Digest- und Protokolldateien

Wenn Sie Digest- und Protokolldateien offline validieren möchten, können Sie dazu die in den vorherigen Abschnitten beschriebenen Verfahren nutzen. Dabei sind folgende Aspekte zu berücksichtigen:

### Verwenden der neuesten Digest-Datei

Die digitale Signatur der neuesten (also der „aktuellen“) Digest-Datei befindet sich in den Amazon-S3-Metadateneigenschaften des Digest-Dateiobjekts. In einem Offline-Szenario steht daher die digitale Signatur der aktuellen Digest-Datei nicht zur Verfügung.

Nachfolgend finden Sie zwei Möglichkeiten für dieses Szenario:

- Da sich die digitale Signatur für die vorherige Digest-Datei in der aktuellen Digest-Datei befindet, beginnen Sie mit der Validierung anhand der Digest-Datei. `next-to-last` Bei dieser Methode kann die neueste Digest-Datei nicht validiert werden.
- In einem ersten Schritt wird die Signatur für die aktuelle Digest-Datei aus den Metadateneigenschaften des Digest-Dateiobjekts abgerufen und anschließend sicher offline gespeichert. Auf diese Weise können Sie neben den vorherigen Dateien in der Kette auch die aktuelle Digest-Datei validieren.

### Pfadauflösung

In den heruntergeladenen Digest-Dateien verweisen Felder wie `s3Object` und `previousDigestS3Object` nach wie vor auf die Online-Speicherorte der Protokoll- und Digest-Dateien in Amazon S3. Bei einer Offline-Lösung muss eine Möglichkeit gefunden werden, um diese auf den aktuellen Pfad der heruntergeladenen Protokoll- und Digest-Dateien umzuleiten.

### Öffentliche Schlüssel

Bei einer Offline-Validierung müssen alle öffentlichen Schlüssel, die für die Validierung der Protokolldateien in einem bestimmten Zeitraum erforderlich sind, zuvor online abgerufen (z. B.

über den Aufruf von `ListPublicKeys`) und dann sicher offline gespeichert werden. Dieser Schritt muss stets wiederholt werden, wenn Sie weitere Dateien außerhalb des ursprünglich angegebenen Zeitraums validieren möchten.

## Snippet mit Beispielvalidierung

Der folgende Beispielausschnitt enthält einen Grundcode für die Validierung von Digest- und Protokolldateien. CloudTrail Das Code-Skelett basiert nicht auf einer Online- oder Offline-Validierung, sodass Sie entscheiden können, ob es mit oder ohne Online-Verbindung zu AWS implementiert werden soll. Die empfohlene Implementierung nutzt [Java Cryptography Extension \(JCE\)](#) und [Bouncy Castle](#) als Sicherheitsanbieter.

Das Beispiel-Snippet zeigt die folgenden Schritte:

- So erstellen Sie die Datensignaturzeichenfolge für die Validierung der Digest-Dateisignatur.
- So überprüfen Sie die Digest-Dateisignatur.
- So überprüfen Sie die Hashwerte der Protokolldatei.
- Eine Codestruktur zur Validierung einer Kette von Digest-Dateien.

```
import java.util.Arrays;
import java.security.MessageDigest;
import java.security.KeyFactory;
import java.security.PublicKey;
import java.security.Security;
import java.security.Signature;
import java.security.spec.X509EncodedKeySpec;
import org.json.JSONObject;
import org.bouncycastle.jce.provider.BouncyCastleProvider;
import org.apache.commons.codec.binary.Hex;

public class DigestFileValidator {

    public void validateDigestFile(String digestS3Bucket, String digestS3Object, String
digestSignature) {

        // Using the Bouncy Castle provider as a JCE security provider - http://
www.bouncycastle.org/
        Security.addProvider(new BouncyCastleProvider());
```

```

// Load the digest file from S3 (using Amazon S3 Client) or from your local
copy
JSONObject digestFile = loadDigestFileInMemory(digestS3Bucket, digestS3Object);

// Check that the digest file has been retrieved from its original location
if (!digestFile.getString("digestS3Bucket").equals(digestS3Bucket) ||
    !digestFile.getString("digestS3Object").equals(digestS3Object)) {
    System.err.println("Digest file has been moved from its original
location.");
} else {
    // Compute digest file hash
    MessageDigest messageDigest = MessageDigest.getInstance("SHA-256");
    messageDigest.update(convertToByteArray(digestFile));
    byte[] digestFileHash = messageDigest.digest();
    messageDigest.reset();

    // Compute the data to sign
    String dataToSign = String.format("%s%n%s/%s%n%s%n%s",
        digestFile.getString("digestEndTime"),
        digestFile.getString("digestS3Bucket"),
        digestFile.getString("digestS3Object"), // Constructing the S3 path of the digest file
        as part of the data to sign
        Hex.encodeHexString(digestFileHash),
        digestFile.getString("previousDigestSignature"));

    byte[] signatureContent = Hex.decodeHex(digestSignature);

    /*
    NOTE:
    To find the right public key to verify the signature, call CloudTrail
ListPublicKey API to get a list
of public keys, then match by the publicKeyFingerprint in the digest
file. Also, the public key bytes
returned from ListPublicKey API are DER encoded in PKCS#1 format:

    PublicKeyInfo ::= SEQUENCE {
        algorithm      AlgorithmIdentifier,
        PublicKey      BIT STRING
    }

    AlgorithmIdentifier ::= SEQUENCE {
        algorithm      OBJECT IDENTIFIER,
        parameters    ANY DEFINED BY algorithm OPTIONAL
    }

```

```
    */
    pkcs1PublicKeyBytes =
getPublicKey(digestFile.getString("digestPublicKeyFingerprint"));

    // Transform the PKCS#1 formatted public key to x.509 format.
    RSAPublicKey rsaPublicKey = RSAPublicKey.getInstance(pkcs1PublicKeyBytes);
    AlgorithmIdentifier rsaEncryption = new
AlgorithmIdentifier(PKCSObjectIdentifiers.rsaEncryption, null);
    SubjectPublicKeyInfo publicKeyInfo = new
SubjectPublicKeyInfo(rsaEncryption, rsaPublicKey);

    // Create the PublicKey object needed for the signature validation
    PublicKey publicKey = KeyFactory.getInstance("RSA",
"BC").generatePublic(new X509EncodedKeySpec(publicKeyInfo.getEncoded()));

    // Verify signature
    Signature signature = Signature.getInstance("SHA256withRSA", "BC");
    signature.initVerify(publicKey);
    signature.update(dataToSign.getBytes("UTF-8"));

    if (signature.verify(signatureContent)) {
        System.out.println("Digest file signature is valid, validating log
files...");
        for (int i = 0; i < digestFile.getJSONArray("logFiles").length(); i++)
        {

            JSONObject logFileMetadata =
digestFile.getJSONArray("logFiles").getJSONObject(i);

            // Compute log file hash
            byte[] logFileContent = loadUncompressedLogFileInMemory(
                logFileMetadata.getString("s3Bucket"),
                logFileMetadata.getString("s3Object")
            );
            messageDigest.update(logFileContent);
            byte[] logFileHash = messageDigest.digest();
            messageDigest.reset();

            // Retrieve expected hash for the log file being processed
            byte[] expectedHash =
Hex.decodeHex(logFileMetadata.getString("hashValue"));

            boolean signaturesMatch = Arrays.equals(expectedHash, logFileHash);
            if (!signaturesMatch) {
```

```
        System.err.println(String.format("Log file: %s/%s hash doesn't
match.\tExpected: %s Actual: %s",
        logFileMetadata.getString("s3Bucket"),
logFileMetadata.getString("s3Object"),
        Hex.encodeHexString(expectedHash),
Hex.encodeHexString(logFileHash)));
    } else {
        System.out.println(String.format("Log file: %s/%s hash match",
logFileMetadata.getString("s3Bucket"),
logFileMetadata.getString("s3Object")));
    }
}

} else {
    System.err.println("Digest signature failed validation.");
}

System.out.println("Digest file validation completed.");

if (chainValidationIsEnabled()) {
    // This enables the digests' chain validation
    validateDigestFile(
        digestFile.getString("previousDigestS3Bucket"),
        digestFile.getString("previousDigestS3Object"),
        digestFile.getString("previousDigestSignature"));
}
}
}
}
```

## CloudTrail Beispiele für Protokolldateien

CloudTrail überwacht Ereignisse für Ihr Konto. Wenn Sie einen Trail erstellen, werden diese Ereignisse als Protokolldateien an den Amazon-S3-Bucket übermittelt. Wenn Sie in CloudTrail Lake einen Ereignisdatenspeicher erstellen, werden Ereignisse in Ihrem Ereignisdatenspeicher protokolliert. Ereignisdatenspeicher verwenden keine S3-Buckets.

### Themen

- [CloudTrail Format des Protokolldateinamens](#)

- [Beispiele für Protokolldateien](#)

## CloudTrail Format des Protokolldateinamens

CloudTrail verwendet das folgende Dateinamenformat für die Protokolldateiobjekte, die es an Ihren Amazon S3 S3-Bucket übermittelt:

```
AccountID_CloudTrail_RegionName_YYYYMMDDTHHmmZ_UniqueString.FileNameFormat
```

- YYYYMM, DD, HH und mm sind die Ziffern von Jahr, Monat, Tag, Stunde und Minute des Zeitpunkts, an dem die Protokolldatei übermittelt wurde. Die Stunden sind im 24-Stunden-Format angegeben. Das Z bedeutet, dass es sich um eine Zeitangabe in koordinierter Weltzeit (UTC) handelt.

### Note

Eine Protokolldatei, die zu einem bestimmten Zeitpunkt bereitgestellt wurde, kann Datensätze enthalten, die an einem beliebigen Zeitpunkt davor geschrieben wurden.

- Die 16-Zeichen-Komponente UniqueString der Protokolldatei verhindert, dass Dateien überschrieben werden. Sie hat keine Bedeutung und wird normalerweise von Protokollverarbeitungssoftware ignoriert.
- FileNameFormat ist die Codierung der Datei. Derzeit ist dies json.gz. Dabei handelt es sich um eine im gzip-Format komprimierte JSON-Textdatei.

Beispiel für einen CloudTrail Protokolldateinamen

```
111122223333_CloudTrail_us-east-2_20150801T0210Z_Mu0Ks0htH1ar15ZZ.json.gz
```

## Beispiele für Protokolldateien

Eine Protokolldatei enthält einen oder mehrere Datensätze. Die folgenden Beispiele sind Ausschnitte von Protokollen mit den Datensätzen zu einer Aktion, die die Erstellung einer Protokolldatei bewirkt hat.

Hinweise zu Feldern für CloudTrail Ereignisdatensätze finden Sie unter [CloudTrail Inhalt aufzeichnen](#).

Inhalt

- [Amazon-EC2-Protokollbeispiele](#)
- [Beispiele für IAM-Protokolle](#)
- [Beispiel für ein Protokoll mit Fehlercode und Fehlermeldung](#)
- [CloudTrail Beispiel für ein Insights-Ereignisprotokoll](#)

## Amazon-EC2-Protokollbeispiele

Amazon Elastic Compute Cloud (Amazon EC2) bietet anpassbare Rechenkapazität in der AWS Cloud. Sie können virtuelle Server starten, Sicherheit und Netzwerk konfigurieren und Speicher verwalten. Amazon EC2 kann zudem schnell in beide Richtungen skalieren, um auf geänderte Anforderungen oder Datenverkehrsspitzen zu reagieren, und reduziert so die Notwendigkeit genauer Voraussagen des Datenverkehrs auf einem Server. Weitere Informationen finden Sie im [Amazon-EC2-Benutzerhandbuch für Linux-Instances](#).

Das folgende Beispiel zeigt, dass ein IAM-Benutzer namens Mateo den Befehl `aws ec2 start-instances` verwendet hat, um die Amazon-EC2-[StartInstances](#)-Aktion für die Instance `i-EXAMPLE56126103cb` und `i-EXAMPLEaff4840c22` aufzurufen.

```
{
  "Records": [
    {
      "eventVersion": "1.08",
      "userIdentity": {
        "type": "IAMUser",
        "principalId": "EXAMPLE6E4XEGITWATV6R",
        "arn": "arn:aws:iam::123456789012:user/Mateo",
        "accountId": "123456789012",
        "accessKeyId": "AKIAIOSFODNN7EXAMPLE",
        "userName": "Mateo",
        "sessionContext": {
          "sessionIssuer": {},
          "webIdFederationData": {},
          "attributes": {
            "creationDate": "2023-07-19T21:11:57Z",
            "mfaAuthenticated": "false"
          }
        }
      },
      "eventTime": "2023-07-19T21:17:28Z",
      "eventSource": "ec2.amazonaws.com",
      "eventName": "StartInstances",
      "awsRegion": "us-east-1",
    }
  ]
}
```

```
"sourceIPAddress": "192.0.2.0",
"userAgent": "aws-cli/2.13.5 Python/3.11.4 Linux/4.14.255-314-253.539.amzn2.x86_64
exec-env/CloudShell exe/x86_64.amzn.2 prompt/off command/ec2.start-instances",
"requestParameters": {
  "instancesSet": {
    "items": [
      {
        "instanceId": "i-EXAMPLE56126103cb"
      },
      {
        "instanceId": "i-EXAMPLEaff4840c22"
      }
    ]
  }
},
"responseElements": {
  "requestId": "e4336db0-149f-4a6b-844d-EXAMPLEb9d16",
  "instancesSet": {
    "items": [
      {
        "instanceId": "i-EXAMPLEaff4840c22",
        "currentState": {
          "code": 0,
          "name": "pending"
        },
        "previousState": {
          "code": 80,
          "name": "stopped"
        }
      },
      {
        "instanceId": "i-EXAMPLE56126103cb",
        "currentState": {
          "code": 0,
          "name": "pending"
        },
        "previousState": {
          "code": 80,
          "name": "stopped"
        }
      }
    ]
  }
},
},
```



```
"requestID": "e4336db0-149f-4a6b-844d-EXAMPLEb9d16",
"eventID": "e755e09c-42f9-4c5c-9064-EXAMPLE228c7",
"readOnly": false,
"eventType": "AwsApiCall",
"managementEvent": true,
"recipientAccountId": "123456789012",
"eventCategory": "Management",
"tlsDetails": {
  "tlsVersion": "TLSv1.2",
  "cipherSuite": "ECDHE-RSA-AES128-GCM-SHA256",
  "clientProvidedHostHeader": "ec2.us-east-1.amazonaws.com"
},
"sessionCredentialFromConsole": "true"
}]}
```

Das folgende Beispiel zeigt, dass ein IAM-Benutzer namens Nikki den Befehl `aws ec2 stop-instances` verwendet hat, um die Amazon-EC2-[StopInstances](#)-Aktion aufzurufen und zwei Instances zu stoppen.

```
{"Records": [{
  "eventVersion": "1.08",
  "userIdentity": {
    "type": "IAMUser",
    "principalId": "EXAMPLE6E4XEGITWATV6R",
    "arn": "arn:aws:iam::777788889999:user/Nikki",
    "accountId": "777788889999",
    "accessKeyId": "AKIAI44QH8DHBEXAMPLE",
    "userName": "Nikki",
    "sessionContext": {
      "sessionIssuer": {},
      "webIdFederationData": {},
      "attributes": {
        "creationDate": "2023-07-19T21:11:57Z",
        "mfaAuthenticated": "false"
      }
    }
  },
  "eventTime": "2023-07-19T21:14:20Z",
  "eventSource": "ec2.amazonaws.com",
  "eventName": "StopInstances",
  "awsRegion": "us-east-1",
  "sourceIPAddress": "192.0.2.0",
```

```
"userAgent": "aws-cli/2.13.5 Python/3.11.4 Linux/4.14.255-314-253.539.amzn2.x86_64
exec-env/CloudShell exe/x86_64.amzn.2 prompt/off command/ec2.stop-instances",
"requestParameters": {
  "instancesSet": {
    "items": [
      {
        "instanceId": "i-EXAMPLE56126103cb"
      },
      {
        "instanceId": "i-EXAMPLEaaff4840c22"
      }
    ]
  },
  "force": false
},
"responseElements": {
  "requestId": "c308a950-e43e-444e-afc1-EXAMPLE73e49",
  "instancesSet": {
    "items": [
      {
        "instanceId": "i-EXAMPLE56126103cb",
        "currentState": {
          "code": 64,
          "name": "stopping"
        },
        "previousState": {
          "code": 16,
          "name": "running"
        }
      },
      {
        "instanceId": "i-EXAMPLEaaff4840c22",
        "currentState": {
          "code": 64,
          "name": "stopping"
        },
        "previousState": {
          "code": 16,
          "name": "running"
        }
      }
    ]
  }
},
},
```

```

"requestID": "c308a950-e43e-444e-afc1-EXAMPLE73e49",
"eventID": "9357a8cc-a0eb-46a1-b67e-EXAMPLE19b14",
"readOnly": false,
"eventType": "AwsApiCall",
"managementEvent": true,
"recipientAccountId": "777788889999",
"eventCategory": "Management",
"tlsDetails": {
  "tlsVersion": "TLSv1.2",
  "cipherSuite": "ECDHE-RSA-AES128-GCM-SHA256",
  "clientProvidedHostHeader": "ec2.us-east-1.amazonaws.com"
},
"sessionCredentialFromConsole": "true"
}]}
```

Das folgende Beispiel zeigt, dass ein IAM-Benutzer namens Arnav den Befehl `aws ec2 create-key-pair` verwendet hat, um die [CreateKeyPair](#)-Aktion aufzurufen. Beachten Sie, dass sie einen Hash des `key pair responseElements` enthalten und dadurch das Schlüsselmaterial AWS entfernt wurde.

```

{"Records": [{
  "eventVersion": "1.08",
  "userIdentity": {
    "type": "IAMUser",
    "principalId": "AIDA60N6E4XEGIEEXAMPLE",
    "arn": "arn:aws:iam::444455556666:user/Arnav",
    "accountId": "444455556666",
    "accessKeyId": "AKIAI44QH8DHBEXAMPLE",
    "userName": "Arnav",
    "sessionContext": {
      "sessionIssuer": {},
      "webIdFederationData": {},
      "attributes": {
        "creationDate": "2023-07-19T21:11:57Z",
        "mfaAuthenticated": "false"
      }
    }
  }
},
  "eventTime": "2023-07-19T21:19:22Z",
  "eventSource": "ec2.amazonaws.com",
  "eventName": "CreateKeyPair",
  "awsRegion": "us-east-1",
  "sourceIPAddress": "192.0.2.0",
```

```
"userAgent": "aws-cli/2.13.5 Python/3.11.4 Linux/4.14.255-314-253.539.amzn2.x86_64
exec-env/CloudShell exe/x86_64.amzn.2 prompt/off command/ec2.create-key-pair",
  "requestParameters": {
    "keyName": "my-key",
    "keyType": "rsa",
    "keyFormat": "pem"
  },
  "responseElements": {
    "requestId": "9aa4938f-720f-4f4b-9637-EXAMPLE9a196",
    "keyName": "my-key",
    "keyFingerprint":
"1f:51:ae:28:bf:89:e9:d8:1f:25:5d:37:2d:7d:b8:ca:9f:f5:f1:6f",
    "keyPairId": "key-abcd12345eEXAMPLE",
    "keyMaterial": "<sensitiveDataRemoved>"
  },
  "requestID": "9aa4938f-720f-4f4b-9637-EXAMPLE9a196",
  "eventID": "2ae450ff-e72b-4de1-87b0-EXAMPLE5227cb",
  "readOnly": false,
  "eventType": "AwsApiCall",
  "managementEvent": true,
  "recipientAccountId": "444455556666",
  "eventCategory": "Management",
  "tlsDetails": {
    "tlsVersion": "TLSv1.2",
    "cipherSuite": "ECDHE-RSA-AES128-GCM-SHA256",
    "clientProvidedHostHeader": "ec2.us-east-1.amazonaws.com"
  },
  "sessionCredentialFromConsole": "true"
}]}
```

## Beispiele für IAM-Protokolle

AWS Identity and Access Management (IAM) ist ein Webservice, mit dem Sie den Zugriff auf AWS Ressourcen sicher kontrollieren können. Mit IAM können Sie Berechtigungen, die festlegen, auf welche AWS -Ressourcen Benutzer zugreifen dürfen, zentral verwalten. Sie verwenden IAM, um zu steuern, wer authentifiziert (angemeldet) und autorisiert (Berechtigungen besitzt) ist, Ressourcen zu nutzen. Weitere Informationen finden Sie im [IAM-Benutzerhandbuch](#).

Das folgende Beispiel zeigt, dass der IAM-Benutzer namens Mary den Befehl `aws iam create-user` verwendet hat, um die [CreateUser](#)-Aktion aufzurufen und einen neuen Benutzer namens Richard zu erstellen.

```

{"Records": [{
  "eventVersion": "1.08",
  "userIdentity": {
    "type": "IAMUser",
    "principalId": "AIDA60N6E4XEGITEXAMPLE",
    "arn": "arn:aws:iam::888888888888:user/Mary",
    "accountId": "888888888888",
    "accessKeyId": "AKIAIOSFODNN7EXAMPLE",
    "userName": "Mary",
    "sessionContext": {
      "sessionIssuer": {},
      "webIdFederationData": {},
      "attributes": {
        "creationDate": "2023-07-19T21:11:57Z",
        "mfaAuthenticated": "false"
      }
    }
  },
  "eventTime": "2023-07-19T21:25:09Z",
  "eventSource": "iam.amazonaws.com",
  "eventName": "CreateUser",
  "awsRegion": "us-east-1",
  "sourceIPAddress": "192.0.2.0",
  "userAgent": "aws-cli/2.13.5 Python/3.11.4 Linux/4.14.255-314-253.539.amzn2.x86_64
exec-env/CloudShell exe/x86_64.amzn.2 prompt/off command/iam.create-user",
  "requestParameters": {
    "userName": "Richard"
  },
  "responseElements": {
    "user": {
      "path": "/",
      "arn": "arn:aws:iam::888888888888:user/Richard",
      "userId": "AIDA60N6E4XEP7EXAMPLE",
      "createDate": "Jul 19, 2023 9:25:09 PM",
      "userName": "Richard"
    }
  },
  "requestID": "2d528c76-329e-410b-9516-EXAMPLE565dc",
  "eventID": "ba0801a1-87ec-4d26-be87-EXAMPLE75bbb",
  "readOnly": false,
  "eventType": "AwsApiCall",
  "managementEvent": true,
  "recipientAccountId": "888888888888",

```

```

    "eventCategory": "Management",
    "tlsDetails": {
      "tlsVersion": "TLSv1.2",
      "cipherSuite": "ECDHE-RSA-AES128-GCM-SHA256",
      "clientProvidedHostHeader": "iam.amazonaws.com"
    },
    "sessionCredentialFromConsole": "true"
  ]}]

```

Das folgende Beispiel zeigt, dass der IAM-Benutzer namens Paulo den Befehl `aws iam add-user-to-group` verwendet hat, um die [AddUserToGroup](#)-Aktion aufzurufen und einen neuen Benutzer namens Jane zur Gruppe Admin hinzuzufügen.

```

{"Records": [{
  "eventVersion": "1.08",
  "userIdentity": {
    "type": "IAMUser",
    "principalId": "AIDA6ON6E4XEGIEEXAMPLE",
    "arn": "arn:aws:iam::555555555555:user/Paulo",
    "accountId": "555555555555",
    "accessKeyId": "AKIAIOSFODNN7EXAMPLE",
    "userName": "Paulo",
    "sessionContext": {
      "sessionIssuer": {},
      "webIdFederationData": {},
      "attributes": {
        "creationDate": "2023-07-19T21:11:57Z",
        "mfaAuthenticated": "false"
      }
    }
  },
  "eventTime": "2023-07-19T21:25:09Z",
  "eventSource": "iam.amazonaws.com",
  "eventName": "AddUserToGroup",
  "awsRegion": "us-east-1",
  "sourceIPAddress": "192.0.2.0",
  "userAgent": "aws-cli/2.13.5 Python/3.11.4 Linux/4.14.255-314-253.539.amzn2.x86_64
exec-env/CloudShell exe/x86_64.amzn.2 prompt/off command/iam.add-user-to-group",
  "requestParameters": {
    "groupName": "Admin",
    "userName": "Jane"
  },
  "responseElements": null,

```

```

"requestID": "ecd94349-b36f-44bf-b6f5-EXAMPLE9c463",
"eventID": "2939ba50-1d26-4a5a-83bd-EXAMPLE85850",
"readOnly": false,
"eventType": "AwsApiCall",
"managementEvent": true,
"recipientAccountId": "555555555555",
"eventCategory": "Management",
"tlsDetails": {
  "tlsVersion": "TLSv1.2",
  "cipherSuite": "ECDHE-RSA-AES128-GCM-SHA256",
  "clientProvidedHostHeader": "iam.amazonaws.com"
},
"sessionCredentialFromConsole": "true"
}]}
```

Das folgende Beispiel zeigt, dass der IAM-Benutzer namens Saanvi den Befehl `aws iam create-role` verwendet hat, um die [CreateRole](#)-Aktion aufzurufen und eine neue Rolle zu erstellen.

```

{"Records": [{
  "eventVersion": "1.08",
  "userIdentity": {
    "type": "IAMUser",
    "principalId": "AIDA60N6E4XEGITEXAMPLE",
    "arn": "arn:aws:iam::777777777777:user/Saanvi",
    "accountId": "777777777777",
    "accessKeyId": "AKIAIOSFODNN7EXAMPLE",
    "userName": "Saanvi",
    "sessionContext": {
      "sessionIssuer": {},
      "webIdFederationData": {},
      "attributes": {
        "creationDate": "2023-07-19T21:11:57Z",
        "mfaAuthenticated": "false"
      }
    }
  },
  "eventTime": "2023-07-19T21:29:12Z",
  "eventSource": "iam.amazonaws.com",
  "eventName": "CreateRole",
  "awsRegion": "us-east-1",
  "sourceIPAddress": "192.0.2.0",
  "userAgent": "aws-cli/2.13.5 Python/3.11.4 Linux/4.14.255-314-253.539.amzn2.x86_64
exec-env/CloudShell exe/x86_64.amzn.2 prompt/off command/iam.create-role",
}
```

```

    "requestParameters": {
      "roleName": "TestRole",
      "description": "Allows EC2 instances to call AWS services on your behalf.",
      "assumeRolePolicyDocument": "{\"Version\":\"2012-10-17\",\"Statement\":
[{\n\"Effect\":"Allow\", \"Action\":[\n\"sts:AssumeRole\"], \"Principal\":{\n\"Service\":
[\"ec2.amazonaws.com\"]}]}]"
    },
    "responseElements": {
      "role": {
        "assumeRolePolicyDocument": "%7B%22Version%22%3A%222012-10-17%22%2C
%22Statement%22%3A%5B%7B%22Effect%22%3A%22Allow%22%2C%22Action%22%3A%5B%22sts
%3AAssumeRole%22%5D%2C%22Principal%22%3A%7B%22Service%22%3A%5B%22ec2.amazonaws.com
%22%5D%7D%7D%5D%7D",
        "arn": "arn:aws:iam::777777777777:role/TestRole",
        "roleId": "AROA6ON6E4XEFFEXAMPLE",
        "createDate": "Jul 19, 2023 9:29:12 PM",
        "roleName": "TestRole",
        "path": "/"
      }
    },
    "requestID": "ff38f36e-ebd3-425b-9939-EXAMPLE1bbe",
    "eventID": "9da77cd0-493f-4c89-8852-EXAMPLEa887c",
    "readOnly": false,
    "eventType": "AwsApiCall",
    "managementEvent": true,
    "recipientAccountId": "777777777777",
    "eventCategory": "Management",
    "tlsDetails": {
      "tlsVersion": "TLSv1.2",
      "cipherSuite": "ECDHE-RSA-AES128-GCM-SHA256",
      "clientProvidedHostHeader": "iam.amazonaws.com"
    },
    "sessionCredentialFromConsole": "true"
  ]}]

```

## Beispiel für ein Protokoll mit Fehlercode und Fehlermeldung

Das folgende Beispiel zeigt, dass der IAM-Benutzer namens Terry den Befehl `aws cloudtrail update-trail` verwendet hat, um die Aktion [UpdateTrail](#) aufzurufen und einen Trail namens `myTrail2` zu aktualisieren. Dieser Trail-Name wurde jedoch nicht gefunden. Im Protokoll wird dieser Fehler in den Elementen `errorCode` und `errorMessage` angezeigt.

```

{"Records": [{

```



```
"eventVersion": "1.09",
"userIdentity": {
  "type": "IAMUser",
  "principalId": "AIDA60N6E4XEGIEEXAMPLE",
  "arn": "arn:aws:iam::111122223333:user/Terry",
  "accountId": "111122223333",
  "accessKeyId": "AKIAIOSFODNN7EXAMPLE",
  "userName": "Terry",
  "sessionContext": {
    "attributes": {
      "creationDate": "2023-07-19T21:11:57Z",
      "mfaAuthenticated": "false"
    }
  }
},
"eventTime": "2023-07-19T21:35:03Z",
"eventSource": "cloudtrail.amazonaws.com",
"eventName": "UpdateTrail",
"awsRegion": "us-east-1",
"sourceIPAddress": "192.0.2.0",
"userAgent": "aws-cli/2.13.0 Python/3.11.4 Linux/4.14.255-314-253.539.amzn2.x86_64
exec-env/CloudShell exe/x86_64.amzn.2 prompt/off command/cloudtrail.update-trail",
"errorCode": "TrailNotFoundException",
"errorMessage": "Unknown trail: arn:aws:cloudtrail:us-east-1:111122223333:trail/
myTrail2 for the user: 111122223333",
"requestParameters": {
  "name": "myTrail2",
  "isMultiRegionTrail": true
},
"responseElements": null,
"requestID": "28d2faaf-3319-4649-998d-EXAMPLE72818",
"eventID": "694d604a-d190-4470-8dd1-EXAMPLEe20c1",
"readOnly": false,
"eventType": "AwsApiCall",
"managementEvent": true,
"recipientAccountId": "111122223333",
"eventCategory": "Management",
"tlsDetails": {
  "tlsVersion": "TLSv1.2",
  "cipherSuite": "ECDHE-RSA-AES128-GCM-SHA256",
  "clientProvidedHostHeader": "cloudtrail.us-east-1.amazonaws.com"
},
"sessionCredentialFromConsole": "true"
```

}}}

## CloudTrail Beispiel für ein Insights-Ereignisprotokoll

Das folgende Beispiel zeigt ein CloudTrail Insights-Ereignisprotokoll. Bei einem Insights-Ereignis handelt es sich eigentlich um ein Ereignispaar. Mit diesen beiden Ereignissen werden der Beginn und das Ende eines Zeitraums angegeben, in dem ungewöhnliche Aktivitäten bei der Schreibmanagement-API oder bei Fehlerantworten aufgetreten sind. Im Feld `state` wird angezeigt, ob das Ereignis zu Beginn oder am Ende des Zeitraums mit den ungewöhnlichen Aktivitäten protokolliert wurde. Der Ereignisname, `UpdateInstanceInformation`, ist derselbe Name wie die AWS Systems Manager API, für die Verwaltungsereignisse CloudTrail analysiert wurden, um festzustellen, dass ungewöhnliche Aktivitäten aufgetreten sind. Die Start- und Endereignisse weisen zwar eindeutige `eventID`-Werte auf, verfügen aber auch über einen `sharedEventID`-Wert, der vom Ereignispaar verwendet wird. Mit dem Insights-Ereignis werden die `baseline` (das übliche Muster der Aktivität), die gewonnene Erkenntnis (`insight`) – also die durchschnittlichen ungewöhnlichen Aktivitäten als Grund für die Auslösung des Insights-Startereignisses – und im Endereignis der `insight`-Wert zu den durchschnittlichen ungewöhnlichen Aktivitäten während der Dauer des Insights-Ereignisses angezeigt. Weitere Informationen zu CloudTrail Insights finden Sie unter [Protokollieren von Insights-Ereignissen](#).

```
{
  "Records": [{
    "eventVersion": "1.08",
    "eventTime": "2023-01-02T02:51:00Z",
    "awsRegion": "us-east-1",
    "eventID": "654a30ff-b0f3-4527-81b6-EXAMPLEf2393",
    "eventType": "AwsCloudTrailInsight",
    "recipientAccountId": "123456789012",
    "sharedEventID": "bcbfc274-8559-4a56-beb0-EXAMPLEa6c34",
    "insightDetails": {
      "state": "Start",
      "eventSource": "ssm.amazonaws.com",
      "eventName": "UpdateInstanceInformation",
      "insightType": "ApiCallRateInsight",
      "insightContext": {
        "statistics": {
          "baseline": {
            "average": 84.410596421
          },
          "insight": {
```

```
        "average": 669
      }
    }
  },
  "eventCategory": "Insight"
},
{
  "eventVersion": "1.08",
  "eventTime": "2023-01-02T00:22:00Z",
  "awsRegion": "us-east-1",
  "eventID": "258de2fb-e2a9-4fb5-aeb2-EXAMPLE449a4",
  "eventType": "AwsCloudTrailInsight",
  "recipientAccountId": "123456789012",
  "sharedEventID": "8b74a7bc-d5d3-4d19-9d60-EXAMPLE08b51",
  "insightDetails": {
    "state": "End",
    "eventSource": "ssm.amazonaws.com",
    "eventName": "UpdateInstanceInformation",
    "insightType": "ApiCallRateInsight",
    "insightContext": {
      "statistics": {
        "baseline": {
          "average": 74.156423842
        },
        "insight": {
          "average": 657
        },
        "insightDuration": 1
      }
    }
  },
  "eventCategory": "Insight"
}]
}
```

## Verwendung der CloudTrail Processing Library

Die CloudTrail Processing Library ist eine Java-Bibliothek, die eine einfache Möglichkeit bietet, AWS CloudTrail Logs zu verarbeiten. Sie geben Konfigurationsdetails zu Ihrer CloudTrail SQS-Warteschlange an und schreiben Code zur Verarbeitung von Ereignissen. Die CloudTrail Processing Library erledigt den Rest. Es fragt Ihre Amazon SQS SQS-Warteschlange ab, liest und analysiert

Warteschlangennachrichten, lädt CloudTrail Protokolldateien herunter, analysiert Ereignisse in den Protokolldateien und übergibt die Ereignisse als Java-Objekte an Ihren Code.

Die CloudTrail Processing Library ist hochgradig skalierbar und fehlertolerant. Sie verarbeitet Protokolldateien parallel, damit Sie so viele Protokolle verarbeiten können wie erforderlich. Sie verarbeitet Netzwerkausfälle im Zusammenhang mit Netzwerk-Timeouts und Ressourcen, auf die nicht zugegriffen werden kann.

Das folgende Thema zeigt Ihnen, wie Sie die CloudTrail Processing Library verwenden, um CloudTrail Logs in Ihren Java-Projekten zu verarbeiten.

Die Bibliothek wird als Apache-lizenziertes Open-Source-Projekt bereitgestellt, verfügbar unter: GitHub <https://github.com/aws/aws-cloudtrail-processing-library> Die Bibliotheksquelle enthält Beispiel-Code, den Sie als Grundlage für Ihre eigenen Projekte verwenden können.

## Themen

- [Mindestanforderungen](#)
- [Protokolle werden verarbeitet CloudTrail](#)
- [Erweiterte Themen](#)
- [Weitere Ressourcen](#)

## Mindestanforderungen

Um die CloudTrail Processing Library verwenden zu können, benötigen Sie Folgendes:

- [AWS SDK for Java 1.11.830](#)
- [Java 1.8 \(Java SE 8\)](#)

## Protokolle werden verarbeitet CloudTrail

Um CloudTrail Logs in Ihrer Java-Anwendung zu verarbeiten:

1. [Hinzufügen der CloudTrail Processing Library zu Ihrem Projekt](#)
2. [Konfiguration der CloudTrail Processing Library](#)
3. [Implementieren der Verarbeitungsausführung](#)
4. [Instanzieren und Ausführen der Verarbeitungsausführung](#)

## Hinzufügen der CloudTrail Processing Library zu Ihrem Projekt

Um die CloudTrail Processing Library zu verwenden, fügen Sie sie dem Klassenpfad Ihres Java-Projekts hinzu.

### Inhalt

- [Hinzufügen der Bibliothek zu einem Apache-Ant-Projekt](#)
- [Hinzufügen der Bibliothek zu einem Apache-Maven-Projekt](#)
- [Hinzufügen der Bibliothek zu einem Eclipse-Projekt](#)
- [Hinzufügen der Bibliothek zu einem IntelliJ-Projekt](#)

### Hinzufügen der Bibliothek zu einem Apache-Ant-Projekt

Um die CloudTrail Processing Library zu einem Apache Ant-Projekt hinzuzufügen

1. Laden Sie den Quellcode der CloudTrail Processing Library herunter oder klonen Sie ihn von GitHub:
  - <https://github.com/aws/aws-cloudtrail-processing-library>
2. Erstellen Sie die JAR-Datei aus der Quelle, wie in der [README](#):

```
mvn clean install -Dpgg.skip=true
```

3. Kopieren Sie die resultierende JAR-Datei in Ihr Projekt und fügen Sie sie zur Datei `build.xml` in Ihrem Projekt hinzu. Beispielsweise:

```
<classpath>
  <pathelement path="{classpath}"/>
  <pathelement location="lib/aws-cloudtrail-processing-library-1.6.1.jar"/>
</classpath>
```

### Hinzufügen der Bibliothek zu einem Apache-Maven-Projekt

Die CloudTrail Processing Library ist für [Apache Maven](#) verfügbar. Sie können sie Ihrem Projekt hinzufügen, indem Sie in der `pom.xml`-Datei Ihres Projekts eine Einzelabhängigkeit schreiben.

## Um die CloudTrail Processing Library zu einem Maven-Projekt hinzuzufügen

- Öffnen Sie die `pom.xml`-Datei Ihres Maven-Projekts und fügen Sie die folgende Abhängigkeit hinzu:

```
<dependency>
  <groupId>com.amazonaws</groupId>
  <artifactId>aws-cloudtrail-processing-library</artifactId>
  <version>1.6.1</version>
</dependency>
```

## Hinzufügen der Bibliothek zu einem Eclipse-Projekt

### Um die CloudTrail Processing Library zu einem Eclipse-Projekt hinzuzufügen

- Laden Sie den Quellcode der CloudTrail Processing Library herunter oder klonen Sie ihn von GitHub:

- <https://github.com/aws/aws-cloudtrail-processing-library>

- Erstellen Sie die JAR-Datei aus der Quelle, wie in der [README](#)-Datei beschrieben:

```
mvn clean install -Dpgg.skip=true
```

- Kopieren Sie das erstellte `aws-cloudtrail-processing-library-1.6.1.jar` in ein Verzeichnis in Ihrem Projekt (normalerweise) `lib`
- Klicken Sie im Eclipse Projekt-Explorer mit der rechten Maustaste auf den Namen Ihres Projekts, wählen Sie Pfad erstellen und anschließend Konfigurieren.
- Klicken Sie im Fenster Java Build-Pfad die Registerkarte Bibliotheken.
- Wählen Sie JARs hinzufügen... und navigieren Sie zu dem Pfad, in den Sie `aws-cloudtrail-processing-library-1.6.1.jar` kopiert haben.
- Wählen Sie OK, um `.jar` Ihrem Projekt hinzuzufügen.

## Hinzufügen der Bibliothek zu einem IntelliJ-Projekt

Um die CloudTrail Processing Library zu einem IntelliJ-Projekt hinzuzufügen

1. Laden Sie den Quellcode der CloudTrail Processing Library herunter oder klonen Sie ihn von:  
GitHub
  - <https://github.com/aws/aws-cloudtrail-processing-library>
2. Erstellen Sie die JAR-Datei aus der Quelle, wie in der [README](#):

```
mvn clean install -Dpgg.skip=true
```

3. Wählen Sie in Datei die Option Projektstruktur.
4. Wählen Sie Module und anschließend Abhängigkeiten.
5. Wählen Sie + JARS oder Verzeichnisse und navigieren Sie anschließend zu dem Pfad, in dem Sie `aws-cloudtrail-processing-library-1.6.1.jar` erstellt haben.
6. Wählen Sie Anwenden und anschließend OK, um die Hinzufügung von `.jar` zu Ihrem Projekt abzuschließen.

## Konfiguration der CloudTrail Processing Library

Sie können die CloudTrail Verarbeitungsbibliothek konfigurieren, indem Sie eine Klassenpfad-Eigenschaftendatei erstellen, die zur Laufzeit geladen wird, oder indem Sie ein `ClientConfiguration` Objekt erstellen und Optionen manuell festlegen.

### Bereitstellen einer Eigenschaftendatei

Sie können eine Klassenpfad-Eigenschaftendatei schreiben, die Konfigurationsoptionen zu Ihrer Anwendung bereitstellt. Die folgende Beispieldatei zeigt die Optionen, die Sie festlegen können:

```
# AWS access key. (Required)
accessKey = your_access_key

# AWS secret key. (Required)
secretKey = your_secret_key

# The SQS URL used to pull CloudTrail notification from. (Required)
sqsUrl = your_sqs_queue_url
```

```
# The SQS end point specific to a region.
sqsRegion = us-east-1

# A period of time during which Amazon SQS prevents other consuming components
# from receiving and processing that message.
visibilityTimeout = 60

# The S3 region to use.
s3Region = us-east-1

# Number of threads used to download S3 files in parallel. Callbacks can be
# invoked from any thread.
threadCount = 1

# The time allowed, in seconds, for threads to shut down after
# AWSCloudTrailEventProcessingExecutor.stop() is called. If they are still
# running beyond this time, they will be forcibly terminated.
threadTerminationDelaySeconds = 60

# The maximum number of AWSCloudTrailClientEvents sent to a single invocation
# of processEvents().
maxEventsPerEmit = 10

# Whether to include raw event information in CloudTrailDeliveryInfo.
enableRawEventInfo = false

# Whether to delete SQS message when the CloudTrail Processing Library is unable to
# process the notification.
deleteMessageUponFailure = false
```

Die folgenden Parameter sind erforderlich:

- `sqsUrl`— Stellt die URL bereit, von der Sie Ihre Benachrichtigungen abrufen können. CloudTrail Wenn Sie diesen Wert nicht angeben, gibt `AWSCloudTrailProcessingExecutor` eine `IllegalStateException` aus.
- `accessKey` – Eine eindeutige Bezeichnung für Ihr Konto, wie `AKIAIOSFODNN7EXAMPLE`.
- `secretKey`— Eine eindeutige Kennung für Ihr Konto, z. B. `bPXRfi wjalrxutnfeMI/K7MDENG/CYEXAMPLEKEY`.

Die `secretKey` Parameter `accessKey` und geben Ihre Anmeldeinformationen für die Bibliothek an, sodass die Bibliothek in Ihrem Namen darauf zugreifen kann. AWS AWS



Die Standardwerte für die anderen Parameter werden von der Bibliothek festgelegt. Weitere Informationen finden Sie in der [AWS CloudTrail -Referenz zur Verarbeitungsbibliothek](#).

## Erstellen eines ClientConfiguration

Anstatt Optionen in den Klassenpfadeigenschaften festzulegen, können Sie Optionen für den `AWSCloudTrailProcessingExecutor` bereitstellen, indem Sie Optionen auf einem `ClientConfiguration`-Objekt initialisieren und festlegen, wie im folgenden Beispiel gezeigt:

```
ClientConfiguration basicConfig = new ClientConfiguration(
    "http://sqs.us-east-1.amazonaws.com/123456789012/queue2",
    new DefaultAWSCredentialsProviderChain());

basicConfig.setEnableRawEventInfo(true);
basicConfig.setThreadCount(4);
basicConfig.setnEventsPerEmit(20);
```

## Implementieren der Verarbeitungsausführung

Um CloudTrail Protokolle zu verarbeiten, müssen Sie einen `implementierenEventsProcessor`, der die CloudTrail Protokolldaten empfängt. Im Folgenden wird eine Beispielimplementierung gezeigt:

```
public class SampleEventsProcessor implements EventsProcessor {

    public void process(List<CloudTrailEvent> events) {
        int i = 0;
        for (CloudTrailEvent event : events) {
            System.out.println(String.format("Process event %d : %s", i++,
                event.getEventData()));
        }
    }
}
```

Bei der Implementierung von `implementieren` Sie den `process()` Callback, den der `AWSCloudTrailProcessingExecutor` verwendet, um Ihnen CloudTrail Ereignisse zu senden. `EventsProcessor` Ereignisse werden in einer Liste von `CloudTrailClientEvent`-Objekten bereitgestellt.

Das `CloudTrailClientEvent` Objekt stellt ein Band `CloudTrailEvent` bereit `CloudTrailEventMetadata`, mit dem Sie die CloudTrail Ereignis- und Zustellungsinformationen lesen können.

In diesem Beispiel werden die Ereignisinformationen zu den Ereignissen ausgegeben, die an die `SampleEventsProcessor` übergeben wurden. In Ihrer eigenen Implementierung können Sie Protokolle je nach Bedarf verarbeiten. Der `AWSCloudTrailProcessingExecutor` sendet solange Ereignisse an die `EventsProcessor`, wie er ausgeführt wird und Ereignisse zum Senden vorhanden sind.

## Instanzieren und Ausführen der Verarbeitungsausführung

Nachdem Sie eine geschriebenen `EventsProcessor` und Konfigurationswerte für die CloudTrail Processing Library festgelegt haben (entweder in einer Eigenschaftendatei oder mithilfe der `ClientConfiguration` Klasse), können Sie diese Elemente verwenden, um eine `AWSCloudTrailProcessingExecutor` zu initialisieren und zu verwenden.

Wird **`AWSCloudTrailProcessingExecutor`** zur Verarbeitung CloudTrail von Ereignissen verwendet

1. Instanzieren Sie ein `AWSCloudTrailProcessingExecutor.Builder`-Objekt. Dem Konstruktor von `Builder` wird ein `EventsProcessor`-Objekt und der Name einer Klassenpfad-Eigenschaftendatei übergeben.
2. Rufen Sie die `Builder`-Factory-Methode im `build()` auf, um ein `AWSCloudTrailProcessingExecutor`-Objekt zu konfigurieren und abzurufen.
3. Verwenden Sie `AWSCloudTrailProcessingExecutor` die `stop()` Methoden `start()` und um die CloudTrail Ereignisverarbeitung zu starten und zu beenden.

```
public class SampleApp {
    public static void main(String[] args) throws InterruptedException {
        AWSCloudTrailProcessingExecutor executor = new
            AWSCloudTrailProcessingExecutor.Builder(new SampleEventsProcessor(),
                "/myproject/cloudtrailprocessing.properties").build();

        executor.start();
        Thread.sleep(24 * 60 * 60 * 1000); // let it run for a while (optional)
        executor.stop(); // optional
    }
}
```

## Erweiterte Themen

### Themen

- [Filtern der zu verarbeitenden Ereignisse](#)
- [Datenergebnisverarbeitung](#)
- [Berichterstellung zum Fortschritt](#)
- [Fehlerbehandlung](#)

### Filtern der zu verarbeitenden Ereignisse

Standardmäßig werden alle Protokolle im S3 Bucket der Amazon-SQS-Warteschlange und alle Ereignisse, die sie enthalten, an die `EventsProcessor` gesendet. Die `CloudTrail Processing Library` bietet optionale Schnittstellen, die Sie implementieren können, um die Quellen zu filtern, die zum Abrufen von CloudTrail Protokollen verwendet werden, und um die Ereignisse zu filtern, die Sie verarbeiten möchten.

### `SourceFilter`

Sie können die `SourceFilter`-Schnittstelle implementieren, um zu wählen, ob Sie die Protokolle aus einer bereitgestellten Quelle verarbeiten möchten. `SourceFilter` deklariert eine einzelne Rückruf-Methode (`filterSource()`), die ein `CloudTrailSource`-Objekt abrufen. Wenn Ereignisse aus einer bestimmten Quelle nicht verarbeitet werden sollen, geben Sie `false` über `filterSource()` zurück.

Die `CloudTrail Processing Library` ruft die `filterSource()` Methode auf, nachdem die Bibliothek nach Protokollen in der Amazon SQS-Warteschlange gesucht hat. Dies erfolgt, bevor die Bibliothek mit dem Filtern von Ereignissen oder der Verarbeitung für die Protokolle beginnt.

Im Folgenden wird eine Beispielimplementierung gezeigt:

```
public class SampleSourceFilter implements SourceFilter{
    private static final int MAX_RECEIVED_COUNT = 3;

    private static List<String> accountIDs ;
    static {
        accountIDs = new ArrayList<>();
        accountIDs.add("123456789012");
        accountIDs.add("234567890123");
    }
}
```

```
}

@Override
public boolean filterSource(CloudTrailSource source) throws CallbackException {
    source = (SQSBasedSource) source;
    Map<String, String> sourceAttributes = source.getSourceAttributes();

    String accountId = sourceAttributes.get(
        SourceAttributeKeys.ACCOUNT_ID.getAttributeKey());

    String receivedCount = sourceAttributes.get(
        SourceAttributeKeys.APPROXIMATE_RECEIVE_COUNT.getAttributeKey());

    int approximateReceivedCount = Integer.parseInt(receivedCount);

    return approximateReceivedCount <= MAX_RECEIVED_COUNT &&
        accountIDs.contains(accountId);
}
}
```

Wenn Sie keinen eigenen `SourceFilter` bereitstellen, wird `DefaultSourceFilter` verwendet. In diesem Fall können alle Quellen verarbeitet werden (es wird stets `true` ausgegeben).

## EventFilter

Sie können die `EventFilter` Schnittstelle implementieren, um auszuwählen, ob ein CloudTrail Ereignis an Ihre gesendet wird. `EventsProcessor` `EventFilter` deklariert eine einzelne Callback-Methode `filterEvent()`, die ein `CloudTrailEvent` Objekt empfängt. Wenn das Ereignis nicht verarbeitet werden soll, geben Sie `false` über `filterEvent()` zurück.

Die CloudTrail Processing Library ruft die `filterEvent()` Methode auf, nachdem die Bibliothek nach Protokollen in der Amazon SQS-Warteschlange gesucht hat und nach der Quellfilterung. Dies erfolgt, bevor die Bibliothek mit der Verarbeitung für die Protokolle beginnt.

Im Folgenden wird eine Beispielimplementierung gezeigt:

```
public class SampleEventFilter implements EventFilter{

    private static final String EC2_EVENTS = "ec2.amazonaws.com";

    @Override
```

```
public boolean filterEvent(CloudTrailClientEvent clientEvent) throws
CallbackException {
    CloudTrailEvent event = clientEvent.getEvent();

    String eventSource = event.getEventSource();
    String eventName = event.getEventName();

    return eventSource.equals(EC2_EVENTS) && eventName.startsWith("Delete");
}
}
```

Wenn Sie keinen eigenen `EventFilter` bereitstellen, wird `DefaultEventFilter` verwendet. In diesem Fall können alle Ereignisse verarbeitet werden (es wird stets `true` ausgegeben).

## Datenereignisverarbeitung

Bei der CloudTrail Verarbeitung von Datenereignissen werden Zahlen in ihrem ursprünglichen Format beibehalten, unabhängig davon, ob es sich um eine Ganzzahl (`int`) oder eine Zahl handelt `float` (eine Zahl, die eine Dezimalzahl enthält). Bei Ereignissen, die ganze Zahlen in den Feldern eines Datenereignisses enthielten, wurden diese Zahlen in der CloudTrail Vergangenheit als Gleitkommazahlen verarbeitet. Derzeit CloudTrail werden Zahlen in diesen Feldern unter Beibehaltung ihres ursprünglichen Formats verarbeitet.

Um zu verhindern, dass Ihre Automatisierungen beschädigt werden, sollten Sie bei jedem Code oder jeder Automatisierung, die Sie zum Verarbeiten oder Filtern von CloudTrail Datenereignissen verwenden, flexibel sein `int` und beides sowie `float` formatierte Zahlen zulassen. Optimale Ergebnisse erzielen Sie, wenn Sie Version 1.4.0 oder höher der CloudTrail Processing Library verwenden.

Der folgende Beispielausschnitt zeigt eine `float` formatierte Zahl, `2.0`, für den Parameter `desiredCount` im `ResponseParameters`-Block eines Datenereignisses.

```
"eventName": "CreateService",
  "awsRegion": "us-east-1",
  "sourceIPAddress": "000.00.00.00",
  "userAgent": "console.amazonaws.com",
  "requestParameters": {
    "clientToken": "EXAMPLE",
    "cluster": "default",
    "desiredCount": 2.0
```

...

Der folgende Beispielausschnitt zeigt eine `int` formatierte Zahl, 2, für den Parameter `desiredCount` im `ResponseParameters`-Block eines Datenereignisses.

```
"eventName": "CreateService",
  "awsRegion": "us-east-1",
  "sourceIPAddress": "000.00.00.00",
  "userAgent": "console.amazonaws.com",
  "requestParameters": {
    "clientToken": "EXAMPLE",
    "cluster": "default",
    "desiredCount": 2
  }
...
```

## Berichterstellung zum Fortschritt

Implementieren Sie die `ProgressReporter` Schnittstelle, um die Berichterstattung über den Fortschritt der `CloudTrail Processing Library` individuell anzupassen. `ProgressReporter` deklariert zwei Methoden: `reportStart()` und `reportEnd()`, die am Anfang und am Ende der folgenden Operationen aufgerufen werden:

- Abrufen von Nachrichten aus Amazon SQS
- Analyse von Nachrichten aus Amazon SQS
- Verarbeitung einer Amazon SQS SQS-Quelle für Protokolle CloudTrail
- Löschen von Nachrichten aus Amazon SQS
- Eine CloudTrail Protokolldatei wird heruntergeladen
- Eine CloudTrail Protokolldatei wird verarbeitet

Beide Methoden erhalten ein `ProgressStatus`-Objekt mit Informationen zum Vorgang, der ausgeführt wurde. Das `progressState`-Element enthält ein Mitglied der `ProgressState`-Aufzählung, die den aktuellen Vorgang identifiziert. Dieses Element kann zusätzliche Informationen im `progressInfo`-Element enthalten. Darüber hinaus werden alle Objekte, die Sie aus `reportStart()` zurückgeben, an `reportEnd()` übergeben, sodass Sie kontextbezogene Informationen wie die Startzeit der Ereignisverarbeitung bereitstellen können.

Im Folgenden finden Sie eine Beispielimplementierung, bei der Informationen zu der für den Vorgang benötigten Zeitdauer bereitgestellt werden:

```
public class SampleProgressReporter implements ProgressReporter {
    private static final Log logger =
        LoggerFactory.getLog(DefaultProgressReporter.class);

    @Override
    public Object reportStart(ProgressStatus status) {
        return new Date();
    }

    @Override
    public void reportEnd(ProgressStatus status, Object startDate) {
        System.out.println(status.getProgressState().toString() + " is " +
            status.getProgressInfo().isSuccess() + " , and latency is " +
            Math.abs(((Date) startDate).getTime()-new Date().getTime()) + "
            milliseconds.");
    }
}
```

Wenn Sie keinen eigenen `ProgressReporter` implementieren, wird `DefaultExceptionHandler` verwendet. Dabei wird stattdessen der Name des ausgeführten Status verwendet.

## Fehlerbehandlung

Die `ExceptionHandler`-Schnittstelle ermöglicht Ihnen die Bereitstellung einer speziellen Verarbeitung, wenn während der Protokollverarbeitung eine Ausnahme auftritt.

`ExceptionHandler` deklariert eine Rückruf-Methode (`handleException()`), der ein `ProcessingLibraryException`-Objekt mit Kontextinformationen zur aufgetretenen Ausnahme übergeben wird.

Sie können die übergebene `ProcessingLibraryException`-Methode `getStatus()` verwenden, um zu ermitteln, welche Operation ausgeführt wurde, als die Ausnahme auftrat, und um zusätzliche Informationen zum Status der Operation abzurufen. `ProcessingLibraryException` ist von der `Exception`-Standardklasse von Java abgeleitet, sodass Sie Informationen zur Ausnahme abrufen können, indem eine der Ausnahmefunktionen abgerufen wird.

Im Folgenden wird eine Beispielimplementierung gezeigt:

```
public class SampleExceptionHandler implements ExceptionHandler{
    private static final Log logger =
        LoggerFactory.getLog(DefaultProgressReporter.class);
```

```
@Override
public void handleException(ProcessingLibraryException exception) {
    ProgressStatus status = exception.getStatus();
    ProgressState state = status.getProgressState();
    ProgressInfo info = status.getProgressInfo();

    System.err.println(String.format(
        "Exception. Progress State: %s. Progress Information: %s.", state, info));
}
}
```

Wenn Sie keinen eigenen `ExceptionHandler` bereitstellen, wird `DefaultExceptionHandler` verwendet. Dabei wird stattdessen eine Standardfehlermeldung verwendet.

### Note

Ist der `deleteMessageUponFailure` Parameter gleich `true`, unterscheidet die CloudTrail Processing Library nicht zwischen allgemeinen Ausnahmen und Verarbeitungsfehlern und löscht möglicherweise Warteschlangenmeldungen.

1. Beispielsweise verwenden Sie den `SourceFilter`, um Nachrichten nach Zeitstempel zu filtern.
2. Sie verfügen jedoch nicht über die erforderlichen Berechtigungen für den Zugriff auf den S3-Bucket, der die CloudTrail Protokolldateien empfängt. Da Sie nicht die erforderlichen Berechtigungen besitzen, wird eine `AmazonServiceException` ausgelöst. Die CloudTrail Processing Library verpackt dies in eine `CallbackException`.
3. Der `DefaultExceptionHandler` protokolliert dies als einen Fehler, identifiziert jedoch nicht die Ursache, d. h., dass Sie die erforderlichen Berechtigungen nicht besitzen. Die CloudTrail Verarbeitungsbibliothek betrachtet dies als Verarbeitungsfehler und löscht die Nachricht, auch wenn die Nachricht eine gültige CloudTrail Protokolldatei enthält.

Wenn Sie Nachrichten mit `SourceFilter` filtern möchten, müssen Sie überprüfen, ob Ihr `ExceptionHandler` zwischen Service-Ausnahmen und Verarbeitungsfehlern unterscheiden kann.



## Weitere Ressourcen

Weitere Informationen zur CloudTrail Processing Library finden Sie im Folgenden:

- [CloudTrail Processing GitHub Library-Projekt](#), das [Beispielcode](#) enthält, der veranschaulicht, wie eine CloudTrail Processing Library-Anwendung implementiert wird.
- [CloudTrail Dokumentation zum Java-Paket der Verarbeitungsbibliothek](#).

# Sicherheit in AWS CloudTrail

Cloud-Sicherheit AWS hat höchste Priorität. Als AWS Kunde profitieren Sie von einer Rechenzentrums- und Netzwerkarchitektur, die darauf ausgelegt sind, die Anforderungen der sicherheitssensibelsten Unternehmen zu erfüllen.

Sicherheit ist eine gemeinsame Verantwortung von Ihnen AWS und Ihnen. Das [Modell der geteilten Verantwortung](#) beschreibt dies als Sicherheit der Cloud und Sicherheit in der Cloud:

- **Sicherheit der Cloud** — AWS ist verantwortlich für den Schutz der Infrastruktur, die AWS Dienste in der AWS Cloud ausführt. AWS bietet Ihnen auch Dienste, 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 gelten AWS CloudTrail, finden Sie unter [AWS Services in Umfang nach Compliance-Programmen](#).
- **Sicherheit in der Cloud** — Ihre Verantwortung richtet sich nach dem AWS Dienst, den Sie nutzen. 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 gemeinsamen Verantwortung bei der Nutzung anwenden können CloudTrail. In den folgenden Themen erfahren Sie, wie Sie die Konfiguration vornehmen CloudTrail , um Ihre Sicherheits- und Compliance-Ziele zu erreichen. Sie erfahren auch, wie Sie andere AWS Dienste nutzen können, die Sie bei der Überwachung und Sicherung Ihrer CloudTrail Ressourcen unterstützen.

## Themen

- [Datenschutz in AWS CloudTrail](#)
- [Identity and Access Management für AWS CloudTrail](#)
- [Konformitätsvalidierung für AWS CloudTrail](#)
- [Resilienz in AWS CloudTrail](#)
- [Infrastruktursicherheit in AWS CloudTrail](#)
- [Serviceübergreifende Confused-Deputy-Prävention](#)
- [Bewährte Sicherheitsmethoden in AWS CloudTrail](#)
- [CloudTrail Logdateien mit AWS KMS Schlüsseln verschlüsseln \(SSE-KMS\)](#)

# Datenschutz in AWS CloudTrail

Das AWS [Modell](#) der gilt für den Datenschutz in AWS CloudTrail. Wie in diesem Modell beschrieben, AWS ist verantwortlich für den Schutz der globalen Infrastruktur, auf der alle Systeme laufen AWS Cloud. 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, dass Sie AWS-Konto Anmeldeinformationen schützen und einzelne Benutzer mit AWS IAM Identity Center oder AWS Identity and Access Management (IAM) einrichten. So erhält jeder Benutzer nur die Berechtigungen, die zum Durchführen seiner Aufgaben erforderlich sind. Außerdem empfehlen wir, die Daten mit folgenden Methoden schützen:

- Verwenden Sie für jedes Konto die Multi-Faktor-Authentifizierung (MFA).
- Verwenden Sie SSL/TLS, um mit Ressourcen zu kommunizieren. AWS Wir benötigen TLS 1.2 und empfehlen TLS 1.3.
- Richten Sie die API und die Protokollierung von Benutzeraktivitäten mit ein. AWS CloudTrail
- Verwenden Sie AWS Verschlüsselungslösungen zusammen mit allen darin enthaltenen Standardsicherheitskontrollen 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 AWS über eine Befehlszeilenschnittstelle oder 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 der Konsole, der API CloudTrail oder den SDKs arbeiten oder diese anderweitig AWS-Services verwenden. AWS CLI AWS 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.

Standardmäßig werden CloudTrail Ereignisprotokolldateien mit der serverseitigen Verschlüsselung (SSE) von Amazon S3 verschlüsselt. Sie können sich auch dafür entscheiden, Ihre Protokolldateien mit einem AWS Key Management Service (AWS KMS) -Schlüssel zu verschlüsseln. Sie können Ihre Protokolldateien beliebig lange in Ihrem -Bucket speichern. Außerdem können Sie Amazon-S3-Lebenszyklusregeln definieren, um Protokolldateien automatisch zu archivieren oder zu löschen. Wenn Sie über die Protokolldateilieferung und -validierung informiert werden möchten, können Sie Amazon-SNS-Benachrichtigungen einrichten.

Die folgenden bewährten Sicherheitsmethoden beziehen sich auch auf den Datenschutz in CloudTrail:

- [CloudTrail Logdateien mit AWS KMS Schlüsseln verschlüsseln \(SSE-KMS\)](#)
- [Amazon S3 S3-Bucket-Richtlinie für CloudTrail](#)
- [Überprüfen der Integrität der CloudTrail Protokolldatei](#)
- [CloudTrail Protokolldateien zwischen AWS Konten teilen](#)

Da CloudTrail Protokolldateien in Amazon S3 in einem oder mehreren Buckets gespeichert werden, sollten Sie auch die Datenschutzinformationen im Amazon Simple Storage Service-Benutzerhandbuch lesen. Weitere Informationen finden Sie unter [Datenschutz in Amazon S3](#).

## Identity and Access Management für AWS CloudTrail

AWS Identity and Access Management (IAM) hilft einem Administrator AWS-Service, den Zugriff auf AWS Ressourcen sicher zu kontrollieren. IAM-Administratoren kontrollieren, wer authentifiziert (angemeldet) und autorisiert werden kann (über Berechtigungen verfügt), um Ressourcen zu verwenden. CloudTrail IAM ist ein Programm AWS-Service, das Sie ohne zusätzliche Kosten nutzen können.

Themen

- [Zielgruppe](#)
- [Authentifizierung mit Identitäten](#)
- [Verwalten des Zugriffs mit Richtlinien](#)

- [Wie AWS CloudTrail funktioniert mit IAM](#)
- [Beispiele für identitätsbasierte Richtlinien für AWS CloudTrail](#)
- [AWS CloudTrail Beispiele für ressourcenbasierte Richtlinien](#)
- [Amazon S3 S3-Bucket-Richtlinie für CloudTrail](#)
- [Amazon S3 S3-Bucket-Richtlinie für CloudTrail Lake-Abfrageergebnisse](#)
- [Amazon SNS SNS-Themenrichtlinie für CloudTrail](#)
- [Fehlerbehebung bei AWS CloudTrail Identität und Zugriff](#)
- [Verwenden von serviceverknüpften Rollen für AWS CloudTrail](#)
- [AWS verwaltete Richtlinien für AWS CloudTrail](#)

## Zielgruppe

Die Art und Weise, wie Sie AWS Identity and Access Management (IAM) verwenden, hängt von der Arbeit ab, in der Sie tätig sind. CloudTrail

**Dienstbenutzer** — Wenn Sie den CloudTrail Dienst für Ihre Arbeit verwenden, stellt Ihnen Ihr Administrator die erforderlichen Anmeldeinformationen und Berechtigungen zur Verfügung. Wenn Sie für Ihre Arbeit mehr CloudTrail Funktionen verwenden, benötigen Sie möglicherweise zusätzliche Berechtigungen. Wenn Sie die Funktionsweise der Zugriffskontrolle nachvollziehen, wissen Sie bereits, welche Berechtigungen Sie von Ihrem Administrator anfordern müssen. Wenn Sie nicht auf eine Funktion zugreifen können CloudTrail, finden Sie weitere Informationen unter [Fehlerbehebung bei AWS CloudTrail Identität und Zugriff](#).

**Serviceadministrator** — Wenn Sie in Ihrem Unternehmen für die CloudTrail Ressourcen verantwortlich sind, haben Sie wahrscheinlich vollen Zugriff auf CloudTrail. Es ist Ihre Aufgabe, zu bestimmen, auf welche CloudTrail Funktionen und Ressourcen Ihre Servicebenutzer 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 darüber, wie Ihr Unternehmen IAM nutzen kann CloudTrail, finden Sie unter [Wie AWS CloudTrail funktioniert mit IAM](#).

**IAM-Administrator** — Wenn Sie ein IAM-Administrator sind, möchten Sie vielleicht mehr darüber erfahren, wie Sie Richtlinien schreiben können, um den Zugriff darauf zu verwalten. CloudTrail Beispiele für CloudTrail identitätsbasierte Richtlinien, die Sie in IAM verwenden können, finden Sie unter [Beispiele für identitätsbasierte Richtlinien für AWS CloudTrail](#)

## Authentifizierung mit Identitäten

Authentifizierung ist die Art und Weise, wie Sie sich AWS mit Ihren Identitätsdaten anmelden. Sie müssen als IAM-Benutzer authentifiziert (angemeldet AWS) sein oder eine IAM-Rolle annehmen. Root-Benutzer des AWS-Kontos

Sie können sich AWS als föderierte Identität anmelden, indem Sie Anmeldeinformationen verwenden, die über eine Identitätsquelle bereitgestellt wurden. AWS IAM Identity Center (IAM Identity Center) -Benutzer, die Single Sign-On-Authentifizierung Ihres Unternehmens und Ihre Google- oder Facebook-Anmeldeinformationen sind Beispiele für föderierte Identitäten. Wenn Sie sich als Verbundidentität anmelden, hat der Administrator vorher mithilfe von IAM-Rollen einen Identitätsverbund eingerichtet. Wenn Sie über den Verbund darauf zugreifen AWS, übernehmen Sie indirekt eine Rolle.

Je nachdem, welcher Benutzertyp Sie sind, können Sie sich beim AWS Management Console oder beim AWS Zugangsportale anmelden. Weitere Informationen zur Anmeldung finden Sie [AWS unter So melden Sie sich bei Ihrem an AWS-Konto](#) im AWS-Anmeldung Benutzerhandbuch.

Wenn Sie AWS programmgesteuert darauf zugreifen, AWS stellt es ein Software Development Kit (SDK) und eine Befehlszeilenschnittstelle (CLI) bereit, mit denen Sie Ihre Anfragen mithilfe Ihrer Anmeldeinformationen kryptografisch signieren können. Wenn Sie keine AWS Tools verwenden, müssen Sie Anfragen selbst signieren. Weitere Informationen zur Verwendung der empfohlenen Methode, um Anfragen selbst zu [signieren, finden Sie im IAM-Benutzerhandbuch unter AWS API-Anfragen](#) signieren.

Unabhängig von der verwendeten Authentifizierungsmethode müssen Sie möglicherweise zusätzliche Sicherheitsinformationen angeben. AWS empfiehlt beispielsweise, die Multi-Faktor-Authentifizierung (MFA) zu verwenden, um die Sicherheit Ihres Kontos zu erhöhen. 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 neues AWS-Konto erstellen, beginnen Sie mit einer Anmeldeidentität, die vollständigen Zugriff auf alle AWS-Services Ressourcen im Konto hat. Diese Identität wird als AWS-Konto Root-Benutzer bezeichnet. Sie können darauf zugreifen, indem Sie sich mit der E-Mail-Adresse und dem Passwort anmelden, mit denen Sie das Konto erstellt haben. 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.

## Verbundidentität

Als bewährte Methode sollten menschliche Benutzer, einschließlich Benutzer, die Administratorzugriff benötigen, für den Zugriff AWS-Services mithilfe temporärer Anmeldeinformationen den Verbund mit einem Identitätsanbieter verwenden.

Eine föderierte Identität ist ein Benutzer aus Ihrem Unternehmensbenutzerverzeichnis, einem Web-Identitätsanbieter AWS Directory Service, dem Identity Center-Verzeichnis oder einem beliebigen Benutzer, der mithilfe AWS-Services von Anmeldeinformationen zugreift, die über eine Identitätsquelle bereitgestellt wurden. Wenn föderierte Identitäten darauf zugreifen AWS-Konten, übernehmen sie Rollen, und die Rollen stellen temporäre Anmeldeinformationen bereit.

Für die zentrale Zugriffsverwaltung empfehlen wir Ihnen, AWS IAM Identity Center zu verwenden. Sie können Benutzer und Gruppen in IAM Identity Center erstellen, oder Sie können eine Verbindung zu einer Gruppe von Benutzern und Gruppen in Ihrer eigenen Identitätsquelle herstellen und diese synchronisieren, um sie in all Ihren AWS-Konten Anwendungen zu verwenden. Informationen zu IAM Identity Center finden Sie unter [Was ist IAM Identity Center?](#) im AWS IAM Identity Center - Benutzerhandbuch.

## IAM-Benutzer und -Gruppen

Ein [IAM-Benutzer](#) ist eine Identität innerhalb Ihres Unternehmens AWS-Konto, die über spezifische Berechtigungen für eine einzelne Person oder Anwendung verfügt. 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 innerhalb Ihres Unternehmens AWS-Konto, die über bestimmte Berechtigungen verfügt. Sie ist einem IAM-Benutzer vergleichbar, ist aber nicht mit einer bestimmten Person verknüpft. Sie können vorübergehend eine IAM-Rolle in der übernehmen, AWS Management Console indem Sie die Rollen [wechseln](#). Sie können eine Rolle übernehmen, 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. Bei einigen können Sie AWS-Services jedoch eine Richtlinie direkt an eine Ressource anhängen (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 Funktionen 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 verwenden, um Aktionen auszuführen AWS, gelten Sie als Principal. Bei einigen Services könnte es Aktionen geben, die dann eine andere Aktion in einem anderen Service initiieren. FAS verwendet die Berechtigungen des Prinzipals, der einen aufruft AWS-Service, in Kombination mit der Anfrage, Anfragen an AWS-Service nachgelagerte Dienste zu stellen. FAS-Anfragen werden nur gestellt, wenn ein Dienst eine Anfrage erhält, für deren Abschluss Interaktionen mit anderen AWS-Services oder Ressourcen erforderlich sind. 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.
- Dienstbezogene Rolle — Eine dienstbezogene Rolle ist eine Art von Servicerolle, die mit einer verknüpft ist. AWS-Service Der Service kann die Rolle übernehmen, um eine Aktion in Ihrem Namen auszuführen. Servicebezogene Rollen erscheinen in Ihrem Dienst AWS-Konto und gehören dem Dienst. Ein IAM-Administrator kann die Berechtigungen für Service-verknüpfte Rollen anzeigen, aber nicht bearbeiten.
- Anwendungen, die auf Amazon EC2 ausgeführt werden — Sie können eine IAM-Rolle verwenden, um temporäre Anmeldeinformationen für Anwendungen zu verwalten, die auf einer EC2-Instance ausgeführt werden und API-Anfragen stellen AWS CLI . AWS Das ist eher zu empfehlen, als Zugriffsschlüssel innerhalb der EC2-Instance zu speichern. Um einer EC2-Instance eine AWS Rolle zuzuweisen und sie allen ihren Anwendungen zur Verfügung zu stellen, erstellen Sie ein Instance-Profil, das an die Instance angehängt ist. 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

Sie kontrollieren den Zugriff, AWS indem Sie Richtlinien erstellen und diese an AWS Identitäten oder Ressourcen anhängen. Eine Richtlinie ist ein Objekt, AWS das, wenn es einer Identität oder Ressource zugeordnet ist, deren Berechtigungen definiert. AWS wertet diese Richtlinien aus, wenn ein Prinzipal (Benutzer, Root-Benutzer oder Rollensitzung) eine Anfrage stellt. Berechtigungen in den Richtlinien bestimmen, ob die Anforderung zugelassen oder abgelehnt wird. Die meisten Richtlinien werden 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 angeben, wer Zugriff auf was hat. 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 Rolleninformationen von der AWS Management Console AWS CLI, der oder der 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 System zuordnen können AWS-Konto. Zu den verwalteten Richtlinien gehören AWS verwaltete Richtlinien und vom 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](#). Zu den Prinzipalen können Konten, Benutzer, Rollen, Verbundbenutzer oder gehören. AWS-Services

Ressourcenbasierte Richtlinien sind Richtlinien innerhalb dieses Diensts. Sie können AWS verwaltete 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 und Amazon VPC sind Beispiele für Services, die ACLs unterstützen. AWS WAF 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 verbreitete 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 Control Policies (SCPs)** — SCPs sind JSON-Richtlinien, die die maximalen Berechtigungen für eine Organisation oder Organisationseinheit (OU) festlegen. AWS Organizations ist ein Dienst zur Gruppierung und zentralen Verwaltung mehrerer AWS-Konten, die Ihrem Unternehmen gehören. Wenn Sie innerhalb einer Organisation alle Features aktivieren, können Sie Service-Kontrollrichtlinien (SCPs) auf alle oder einzelne Ihrer Konten anwenden. Das SCP schränkt die Berechtigungen für Entitäten in Mitgliedskonten ein, einschließlich der einzelnen Entitäten. Root-Benutzer des AWS-Kontos 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 darüber, wie AWS bestimmt wird, ob eine Anfrage zulässig ist, wenn mehrere Richtlinientypen betroffen sind, finden Sie im IAM-Benutzerhandbuch unter [Bewertungslogik für Richtlinien](#).

## Wie AWS CloudTrail funktioniert mit IAM

Bevor Sie IAM verwenden, um den Zugriff auf zu verwalten CloudTrail, sollten Sie sich darüber informieren, mit welchen IAM-Funktionen Sie verwenden können. CloudTrail

## IAM-Funktionen, die Sie mit verwenden können AWS CloudTrail

IAM-Feature	CloudTrail Unterstützung
<a href="#">Identitätsbasierte Richtlinien</a>	Ja
<a href="#">Ressourcenbasierte Richtlinien</a>	Teilweise
<a href="#">Richtlinienaktionen</a>	Ja
<a href="#">Richtlinienressourcen</a>	Ja
<a href="#">Richtlinienbedingungsschlüssel (servicespezifisch)</a>	Nein
<a href="#">ACLs</a>	Nein
<a href="#">ABAC (Tags in Richtlinien)</a>	Teilweise
<a href="#">Temporäre Anmeldeinformationen</a>	Ja
<a href="#">Forward Access Sessions (FAS)</a>	Ja
<a href="#">Servicerollen</a>	Ja
<a href="#">Service-verknüpfte Rollen</a>	Ja

Einen allgemeinen Überblick darüber, wie CloudTrail und andere AWS Dienste mit den meisten IAM-Funktionen funktionieren, finden Sie im [IAM-Benutzerhandbuch unter AWS Dienste, die mit IAM funktionieren](#).

## Identitätsbasierte Richtlinien für CloudTrail

Unterstützt Richtlinien auf Identitätsbasis.	Ja
--	----

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.

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. Sie können den Prinzipal nicht in einer identitätsbasierten Richtlinie angeben, da er für den Benutzer oder die Rolle gilt, dem er zugeordnet ist. Informationen zu sämtlichen Elementen, die Sie in einer JSON-Richtlinie verwenden, finden Sie in der [IAM-Referenz für JSON-Richtlinienelemente](#) im IAM-Benutzerhandbuch.

Beispiele für identitätsbasierte Richtlinien für CloudTrail

Beispiele für CloudTrail identitätsbasierte Richtlinien finden Sie unter [Beispiele für identitätsbasierte Richtlinien für AWS CloudTrail](#)

Ressourcenbasierte Richtlinien in CloudTrail

Unterstützt ressourcenbasierte Richtlinien

Teilweise

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](#). Zu den Prinzipalen können Konten, Benutzer, Rollen, Verbundbenutzer oder gehören. AWS-Services

Um kontoübergreifenden Zugriff zu ermöglichen, können Sie ein gesamtes Konto oder IAM-Entitäten in einem anderen Konto als Prinzipal in einer ressourcenbasierten Richtlinie angeben. Durch das Hinzufügen eines kontoübergreifenden Auftraggebers zu einer ressourcenbasierten Richtlinie ist nur die halbe Vertrauensbeziehung eingerichtet. Wenn sich der Prinzipal und die Ressource unterscheiden AWS-Konten, muss ein IAM-Administrator des vertrauenswürdigen Kontos auch der Prinzipalentität (Benutzer oder Rolle) die Berechtigung zum Zugriff auf die Ressource erteilen. Sie erteilen Berechtigungen, indem Sie der juristischen Stelle eine identitätsbasierte Richtlinie anfügen. Wenn jedoch eine ressourcenbasierte Richtlinie Zugriff auf einen Prinzipal in demselben Konto gewährt, ist keine zusätzliche identitätsbasierte Richtlinie erforderlich. Weitere Informationen

finden Sie unter [Wie sich IAM-Rollen von ressourcenbasierten Richtlinien unterscheiden](#) im IAM-Benutzerhandbuch.

CloudTrail unterstützt ressourcenbasierte Richtlinien für Kanäle, die für CloudTrail Lake-Integrationen mit Ereignisquellen außerhalb von verwendet werden. AWS Die ressourcenbasierte Richtlinie definiert, welche Prinzipal-Entitäten (Konten, Benutzer, Rollen und Verbundbenutzer) PutAuditEvents auf dem Kanal aufrufen können, um Ereignisse an den Zielereignisdatenspeicher zu übermitteln. Weitere Informationen zum Erstellen von Integrationen mit CloudTrail Lake finden Sie unter [Erstellen Sie eine Integration mit einer Ereignisquelle außerhalb von AWS](#)

## Beispiele

Beispiele für CloudTrail ressourcenbasierte Richtlinien finden Sie unter [AWS CloudTrail Beispiele für ressourcenbasierte Richtlinien](#)

## Politische Maßnahmen für CloudTrail

Unterstützt Richtlinienaktionen
---------------------------------

Ja
----

Administratoren können mithilfe von AWS JSON-Richtlinien angeben, wer Zugriff auf was hat. 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 der zugehörige AWS API-Vorgang. 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.

Eine Liste der CloudTrail Aktionen finden Sie unter [Definierte Aktionen von AWS CloudTrail](#) in der Serviceautorisierungsreferenz.

Bei Richtlinienaktionen wird vor der Aktion das folgende Präfix CloudTrail verwendet:

```
cloudtrail
```

Beispiel: Um jemandem die Berechtigung zum Auflisten von Tags für einen Trail mit der API-Operation `ListTags` zu gewähren, fügen Sie die Aktion `cloudtrail:ListTags` in die entsprechende Richtlinie ein. Richtlinienanweisungen müssen entweder ein `Action`-Element oder ein `NotAction`-Element enthalten. CloudTrail definiert einen eigenen Satz von Aktionen, die Aufgaben beschreiben, die Sie mit diesem Dienst ausführen können.

Um mehrere Aktionen in einer einzigen Anweisung anzugeben, trennen Sie sie wie folgt durch Kommata:

```
"Action": [
    "cloudtrail:AddTags",
    "cloudtrail:ListTags",
    "cloudtrail:RemoveTags"
```

Sie können auch Platzhalter verwenden, um mehrere Aktionen anzugeben (\*). Beispielsweise können Sie alle Aktionen festlegen, die mit dem Wort `Get` beginnen, einschließlich der folgenden Aktion:

```
"Action": "cloudtrail:Get*"
```

## Politische Ressourcen für CloudTrail

Unterstützt Richtlinienressourcen

Ja

Administratoren können mithilfe von AWS JSON-Richtlinien angeben, wer Zugriff auf was hat. 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`-Element 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": "*"
```

Eine Liste der CloudTrail Ressourcentypen und ihrer ARNs finden Sie unter [Resources Defined by AWS CloudTrail](#) in der Service Authorization Reference. Informationen zu den Aktionen, mit denen Sie den ARN einzelner Ressourcen angeben können, finden Sie unter [Von AWS CloudTrail definierte Aktionen](#).

In CloudTrail gibt es drei Ressourcentypen: Pfade, Ereignisdatenspeicher und Kanäle. Jeder dieser Ressourcen ist ein eindeutiger Amazon-Ressourcenname (ARN) zugeordnet. In einer Richtlinie verwenden Sie einen ARN, um die Ressource zu identifizieren, für die die Richtlinie gilt. CloudTrail unterstützt derzeit keine anderen Ressourcentypen, die manchmal als Unterressourcen bezeichnet werden.

Die CloudTrail Trail-Ressource hat den folgenden ARN:

```
arn:${Partition}:cloudtrail:${Region}:${Account}:trail/{TrailName}
```

Die CloudTrail Ereignisdatenspeicherressource hat den folgenden ARN:

```
arn:${Partition}:cloudtrail:${Region}:${Account}:eventdatastore/{EventDataStoreId}
```

Die CloudTrail Kanalressource hat den folgenden ARN:

```
arn:${Partition}:cloudtrail:${Region}:${Account}:channel/{ChannelId}
```

Weitere Informationen zum Format von ARNs finden Sie unter [Amazon Resource Names \(ARNs\) und AWS Service Namespaces](#).

Um beispielsweise für einen AWS-Konto mit der ID **123456789012** einen Trail mit dem Namen **My-Trail** anzugeben, der in der Region USA Ost (Ohio) existiert, verwenden Sie den folgenden ARN:

```
"Resource": "arn:aws:cloudtrail:us-east-2:123456789012:trail/My-Trail"
```

Um darin alle Pfade anzugeben, die zu einem bestimmten Konto gehören AWS-Region, verwenden Sie den Platzhalter (\*):

```
"Resource": "arn:aws:cloudtrail:us-east-2:123456789012:trail/*"
```

Einige CloudTrail Aktionen, z. B. die zum Erstellen von Ressourcen, können für eine bestimmte Ressource nicht ausgeführt werden. In diesen Fällen müssen Sie den Platzhalter (\*) verwenden.

```
"Resource": "*"
```

Viele CloudTrail API-Aktionen beinhalten mehrere Ressourcen. Zum Beispiel erfordert `CreateTrail` einen Amazon-S3-Bucket zum Speichern von Protokolldateien, so dass ein Benutzer über Schreibberechtigungen für den Bucket verfügen muss. Um mehrere Ressourcen in einer einzigen Anweisung anzugeben, trennen Sie die ARNs durch Kommata voneinander.

```
"Resource": [  
    "resource1",  
    "resource2"
```

## Schlüssel zur Richtlinienbedingung für CloudTrail

Unterstützt servicespezifische Richtlinienbedingungsschlüssel	Nein
---	------

Administratoren können mithilfe von AWS JSON-Richtlinien angeben, wer auf was Zugriff hat. 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 die

Bedingung mithilfe 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 dienstspezifische Bedingungsschlüssel. Eine Übersicht aller AWS globalen Bedingungsschlüssel finden Sie unter [Kontextschlüssel für AWS globale Bedingungen](#) im IAM-Benutzerhandbuch.

CloudTrail definiert keine eigenen Bedingungsschlüssel, unterstützt aber die Verwendung einiger globaler Bedingungsschlüssel. Eine Übersicht aller AWS globalen Bedingungsschlüssel finden Sie unter [AWS Globale Bedingungskontextschlüssel](#) im IAM-Benutzerhandbuch.

Eine Liste der CloudTrail Bedingungsschlüssel finden Sie unter [Bedingungsschlüssel für AWS CloudTrail](#) in der Service Authorization Reference. Informationen darüber, mit welchen Aktionen und Ressourcen Sie einen Bedingungsschlüssel verwenden können, finden Sie unter [Definierte Aktionen von AWS CloudTrail](#).

## ACLs in CloudTrail

Unterstützt ACLs

Nein

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.

## ABAC mit CloudTrail

Unterstützt ABAC (Tags in Richtlinien)

Teilweise

Die attributbasierte Zugriffskontrolle (ABAC) ist eine Autorisierungsstrategie, bei der Berechtigungen basierend auf Attributen definiert werden. In AWS werden diese Attribute als Tags bezeichnet. Sie können Tags an IAM-Entitäten (Benutzer oder Rollen) und an viele AWS Ressourcen anhängen. Das

Markieren von Entitäten und Ressourcen ist der erste Schritt von ABAC. Anschließend entwerfen Sie ABAC-Richtlinien, um Operationen zuzulassen, wenn das Tag des Prinzipals mit dem Tag der Ressource übereinstimmt, auf die sie zugreifen möchten.

ABAC ist in Umgebungen hilfreich, die schnell wachsen, und unterstützt Sie in Situationen, in denen die Richtlinienverwaltung mühsam wird.

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.

Wenn ein Service alle drei Bedingungsschlüssel für jeden Ressourcentyp unterstützt, lautet der Wert für den Service Ja. Wenn ein Service alle drei Bedingungsschlüssel für nur einige Ressourcentypen unterstützt, lautet der Wert Teilweise.

Weitere Informationen zu ABAC finden Sie unter [Was ist ABAC?](#) im IAM-Benutzerhandbuch. Um ein Tutorial mit Schritten zur Einstellung von ABAC anzuzeigen, siehe [Attributbasierte Zugriffskontrolle \(ABAC\)](#) verwenden im IAM-Benutzerhandbuch.

Sie können zwar Tags an CloudTrail Ressourcen anhängen, unterstützt jedoch CloudTrail nur die Steuerung des Zugriffs auf [CloudTrail Lake-Ereignisdatenspeicher](#) und -Kanäle auf der Grundlage von Tags. Sie können den Zugriff auf Trails nicht auf Grundlage von Tags steuern.

Sie können Tags an CloudTrail Ressourcen anhängen oder Tags in einer Anfrage an diese weiterleiten CloudTrail. Weitere Informationen zum Markieren von CloudTrail Ressourcen finden Sie unter [Erstellen eines Trails](#) und [Trails erstellen, aktualisieren und verwalten mit dem AWS CLI](#).

## Verwenden temporärer Anmeldeinformationen mit CloudTrail

Unterstützt temporäre Anmeldeinformationen	Ja
--	----

Einige funktionieren AWS-Services nicht, wenn Sie sich mit temporären Anmeldeinformationen anmelden. Weitere Informationen, einschließlich Informationen, die mit temporären Anmeldeinformationen AWS-Services [funktionieren AWS-Services](#), [finden Sie im IAM-Benutzerhandbuch unter Diese Option funktioniert mit IAM](#).

Sie verwenden temporäre Anmeldeinformationen, wenn Sie sich mit einer anderen AWS Management Console Methode als einem Benutzernamen und einem Passwort anmelden. Wenn

Sie beispielsweise AWS über den Single Sign-On-Link (SSO) Ihres Unternehmens darauf zugreifen, werden bei diesem Vorgang automatisch temporäre Anmeldeinformationen erstellt. Sie erstellen auch automatisch temporäre Anmeldeinformationen, wenn Sie sich als Benutzer bei der Konsole anmelden und dann die Rollen wechseln. Weitere Informationen zum Wechseln von Rollen finden Sie unter [Wechseln zu einer Rolle \(Konsole\)](#) im IAM-Benutzerhandbuch.

Mithilfe der AWS API AWS CLI oder können Sie temporäre Anmeldeinformationen manuell erstellen. Sie können diese temporären Anmeldeinformationen dann für den Zugriff verwenden AWS. AWS empfiehlt, temporäre Anmeldeinformationen dynamisch zu generieren, anstatt langfristige Zugriffsschlüssel zu verwenden. Weitere Informationen finden Sie unter [Temporäre Sicherheitsanmeldeinformationen in IAM](#).

## Zugriffssitzungen weiterleiten für CloudTrail

Unterstützt Forward Access Sessions (FAS)	Ja
---	----

Wenn Sie einen IAM-Benutzer oder eine IAM-Rolle verwenden, um Aktionen auszuführen AWS, gelten Sie als Principal. Bei einigen Services könnte es Aktionen geben, die dann eine andere Aktion in einem anderen Service initiieren. FAS verwendet die Berechtigungen des Prinzipals, der einen aufruft AWS-Service, kombiniert mit der Anforderung, Anfragen an nachgelagerte Dienste AWS-Service zu stellen. FAS-Anfragen werden nur gestellt, wenn ein Dienst eine Anfrage erhält, für deren Abschluss Interaktionen mit anderen AWS-Services oder Ressourcen erforderlich sind. In diesem Fall müssen Sie über Berechtigungen zum Ausführen beider Aktionen verfügen. Einzelheiten zu den Richtlinien für FAS-Anfragen finden Sie unter [Zugriffssitzungen weiterleiten](#).

## Servicerollen für CloudTrail

Unterstützt Servicerollen	Ja
---------------------------	----

Eine Servicerolle ist eine [IAM-Rolle](#), die ein Service annimmt, 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.

**⚠ Warning**

Durch das Ändern der Berechtigungen für eine Servicerolle kann die CloudTrail Funktionalität beeinträchtigt werden. Bearbeiten Sie Servicerollen nur, CloudTrail wenn Sie dazu eine Anleitung erhalten.

## Dienstbezogene Rollen für CloudTrail

Unterstützt serviceverknüpfte Rollen	Ja
--------------------------------------	----

Eine dienstbezogene Rolle ist eine Art von Servicerolle, die mit einer Service-Verknüpfung ist. AWS-Service Der Service kann die Rolle übernehmen, um eine Aktion in Ihrem Namen auszuführen. Dienstbezogene Rollen werden in Ihrem Dienst angezeigt AWS-Konto und gehören dem Dienst. Ein IAM-Administrator kann die Berechtigungen für Service-verknüpfte Rollen anzeigen, aber nicht bearbeiten.

CloudTrail unterstützt eine dienstbezogene Rolle für die Integration mit. AWS Organizations Diese Rolle ist für die Erstellung eines Datenspeichers für Organisationspfade oder Ereignisse erforderlich. Organisationspfade und Ereignisdatenpeicher protokollieren Ereignisse für alle AWS-Konten Mitglieder einer Organisation. Weitere Informationen zum Erstellen oder Verwalten von CloudTrail dienstbezogenen Rollen finden Sie unter [Verwenden von serviceverknüpften Rollen für AWS CloudTrail](#).

## Beispiele für identitätsbasierte Richtlinien für AWS CloudTrail

Standardmäßig sind Benutzer und Rollen nicht berechtigt, CloudTrail Ressourcen zu erstellen oder zu ändern. Sie können auch keine Aufgaben mithilfe der AWS Management Console, AWS Command Line Interface (AWS CLI) oder AWS API ausführen. 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.

Informationen dazu, wie Sie unter Verwendung dieser beispielhaften JSON-Richtliniendokumente eine identitätsbasierte IAM-Richtlinie erstellen, finden Sie unter [Erstellen von IAM-Richtlinien](#) im IAM-Benutzerhandbuch.

Einzelheiten zu Aktionen und Ressourcentypen, die von definiert wurden CloudTrail, einschließlich des Formats der ARNs für jeden der Ressourcentypen, finden Sie unter [Aktionen, Ressourcen und Bedingungsschlüssel für AWS CloudTrail](#) in der Service Authorization Reference.

## Themen

- [Bewährte Methoden für Richtlinien](#)
- [Beispiel: Zulassen und Verweigern von Aktionen für einen bestimmten Trail](#)
- [Beispiele: Erstellen und Anwenden von Richtlinien bei Aktionen für bestimmte Trails](#)
- [Beispiele: Verweigern des Zugriffs zum Erstellen oder Löschen von Ereignisdatenspeichern basierend auf Tags](#)
- [Verwenden der CloudTrail-Konsole](#)
- [Gewähren der Berechtigung zur Anzeige der eigenen Berechtigungen für Benutzer](#)
- [Gewährung benutzerdefinierter Berechtigungen für Benutzer CloudTrail](#)

## Bewährte Methoden für Richtlinien

Identitätsbasierte Richtlinien legen fest, ob jemand CloudTrail 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:

- Beginnen Sie mit AWS verwalteten Richtlinien und wechseln Sie zu Berechtigungen mit den geringsten Rechten — Verwenden Sie die AWS verwalteten Richtlinien, die Berechtigungen für viele gängige Anwendungsfälle gewähren, um Ihren Benutzern und Workloads zunächst Berechtigungen zu gewähren. Sie sind in Ihrem verfügbar. AWS-Konto Wir empfehlen Ihnen, die Berechtigungen weiter zu reduzieren, indem Sie vom AWS Kunden verwaltete Richtlinien definieren, die speziell auf Ihre Anwendungsfälle zugeschnitten sind. Weitere Informationen finden Sie unter [AWS -verwaltete Richtlinien](#) oder [AWS -verwaltete Richtlinien für Auftrags-Funktionen](#) 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 Serviceaktionen zu gewähren, wenn diese für einen bestimmten Zweck verwendet werden AWS-Service, z. AWS CloudFormation B. 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.
- Multi-Faktor-Authentifizierung (MFA) erforderlich — Wenn Sie ein Szenario haben, das IAM-Benutzer oder einen Root-Benutzer in Ihrem System erfordert AWS-Konto, 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.

CloudTrail hat keine dienstspezifischen Kontextschlüssel, die Sie im Element der Condition Richtlinienanweisungen verwenden können.

### Beispiel: Zulassen und Verweigern von Aktionen für einen bestimmten Trail

Das folgende Beispiel zeigt eine Richtlinie, die es Benutzern mit dieser Richtlinie ermöglicht, den Status und die Konfiguration eines Trails anzuzeigen sowie die Protokollierung für einen Trail namens *My-First-Trail* zu starten oder anzuhalten. Dieser Trail wurde in der Region USA Ost (Ohio) (seiner Heimatregion) AWS-Konto mit der ID **123456789012** angelegt.

```
{  
  "Version": "2012-10-17",  
  "Statement": [  

```



```
{
  "Effect": "Allow",
  "Action": [
    "cloudtrail:StartLogging",
    "cloudtrail:StopLogging",
    "cloudtrail:GetTrail",
    "cloudtrail:GetTrailStatus",
    "cloudtrail:GetEventSelectors"
  ],
  "Resource": [
    "arn:aws:cloudtrail:us-east-2:123456789012:trail/My-First-Trail"
  ]
}
```

*Das folgende Beispiel zeigt eine Richtlinie, die explizit CloudTrail Aktionen für alle Pfade verweigert, die nicht My-First-Trail heißen.*

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Deny",
      "Action": [
        "cloudtrail:*"
      ],
      "NotResource": [
        "arn:aws:cloudtrail:us-east-2:123456789012:trail/My-First-Trail"
      ]
    }
  ]
}
```

## Beispiele: Erstellen und Anwenden von Richtlinien bei Aktionen für bestimmte Trails

Mithilfe von Berechtigungen und Richtlinien können Sie die Fähigkeit eines Benutzers steuern, bestimmte Aktionen auf Pfaden auszuführen. CloudTrail

Sie möchten zum Beispiel nicht, dass Benutzer der Entwicklergruppe Ihres Unternehmens die Protokollierung auf einem bestimmten Trail beginnen oder beenden. Möglicherweise möchten Sie ihnen jedoch die Erlaubnis erteilen, die Aktionen `DescribeTrails` und `GetTrailStatus` auf dem

Trail auszuführen. Zudem sollen die Benutzer der Developer-Gruppe die Aktion `StartLogging` oder `StopLogging` für die Trails ausführen können, die von ihnen verwaltet werden.

Sie können zwei Richtlinienanweisungen erstellen und diese der in IAM erstellten Developer-Benutzergruppe anfügen. Weitere Informationen zu Gruppen in IAM finden Sie unter [IAM-Gruppen](#) im IAM-Benutzerhandbuch.

In der ersten Richtlinie verweigern Sie die Aktionen `StartLogging` und `StopLogging` für den spezifizierten Trail-ARN. Im folgenden Beispiel lautet der Trail-ARN `arn:aws:cloudtrail:us-east-2:123456789012:trail/Example-Trail`.

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Sid": "Stmt1446057698000",
      "Effect": "Deny",
      "Action": [
        "cloudtrail:StartLogging",
        "cloudtrail:StopLogging"
      ],
      "Resource": [
        "arn:aws:cloudtrail:us-east-2:123456789012:trail/Example-Trail"
      ]
    }
  ]
}
```

In der zweiten Richtlinie sind die `GetTrailStatus` Aktionen `DescribeTrails` und für alle CloudTrail Ressourcen zulässig:

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Sid": "Stmt1446072643000",
      "Effect": "Allow",
      "Action": [
        "cloudtrail:DescribeTrails",
        "cloudtrail:GetTrail",
        "cloudtrail:GetTrailStatus"
      ],
    }
  ]
}
```

```
        "Resource": [
            "*"
        ]
    }
]
```

Wenn ein Benutzer der Developer-Gruppe versucht, die Protokollierung für den Trail, den Sie in der ersten Richtlinie angegeben haben, zu starten oder zu beenden, wird dem Benutzer der Zugriff verweigert. Benutzer der Developer-Gruppe können die Protokollierung für Trails, die von ihnen erstellt und verwaltet werden, starten und beenden.

Die folgenden Beispiele zeigen, dass die konfigurierte Entwicklergruppe in einem AWS CLI Profil den Namen `hatdevgroup`. Zuerst führt ein `devgroup`-Benutzer den Befehl `describe-trails` aus.

```
$ aws --profile devgroup cloudtrail describe-trails
```

Der Befehl wird mit der folgenden Ausgabe erfolgreich abgeschlossen:

```
{
  "trailList": [
    {
      "IncludeGlobalServiceEvents": true,
      "Name": "Default",
      "TrailARN": "arn:aws:cloudtrail:us-east-2:123456789012:trail/Example-Trail",
      "IsMultiRegionTrail": false,
      "S3BucketName": "myS3bucket ",
      "HomeRegion": "us-east-2"
    }
  ]
}
```

Anschließend führt der Benutzer den Befehl `get-trail-status` für den Trail aus, den Sie in der ersten Richtlinie angegeben haben.

```
$ aws --profile devgroup cloudtrail get-trail-status --name Example-Trail
```

Der Befehl wird mit der folgenden Ausgabe erfolgreich abgeschlossen:

```
{
```

```
"LatestDeliveryTime": 1449517556.256,  
"LatestDeliveryAttemptTime": "2015-12-07T19:45:56Z",  
"LatestNotificationAttemptSucceeded": "",  
"LatestDeliveryAttemptSucceeded": "2015-12-07T19:45:56Z",  
"IsLogging": true,  
"TimeLoggingStarted": "2015-12-07T19:36:27Z",  
"StartLoggingTime": 1449516987.685,  
"StopLoggingTime": 1449516977.332,  
"LatestNotificationAttemptTime": "",  
"TimeLoggingStopped": "2015-12-07T19:36:17Z"  
}
```

Als Nächstes führt eine devgroup-Gruppe den Befehl `stop-logging` für denselben Trail aus.

```
$ aws --profile devgroup cloudtrail stop-logging --name Example-Trail
```

Der Befehl gibt eine Ausnahme zurück, bei der der Zugriff verweigert wurde, z. B. die folgende:

```
A client error (AccessDeniedException) occurred when calling the StopLogging operation:  
Unknown
```

Der Benutzer führt den Befehl `start-logging` für denselben Trail aus.

```
$ aws --profile devgroup cloudtrail start-logging --name Example-Trail
```

Auch hier gibt der Befehl eine Ausnahme zurück, bei der der Zugriff verweigert wurde, z. B. die folgende:

```
A client error (AccessDeniedException) occurred when calling the StartLogging  
operation: Unknown
```

## Beispiele: Verweigern des Zugriffs zum Erstellen oder Löschen von Ereignisdatenspeichern basierend auf Tags

Im folgenden Richtlinienbeispiel wird die Berechtigung zum Erstellen eines Ereignisdatenspeichers mit `CreateEventDataStore` verweigert, wenn mindestens eine der folgenden Bedingungen nicht erfüllt ist:

- Der Ereignisdatenspeicher hat keinen Tag-Schlüssel von `stage` auf sich selbst angewendet

- Der Wert des Stage-Tags ist nicht alpha, beta, gamma oder prod.

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Deny",
      "Action": "cloudtrail:CreateEventDataStore",
      "Resource": "*",
      "Condition": {
        "Null": {
          "aws:RequestTag/stage": "true"
        }
      }
    },
    {
      "Effect": "Deny",
      "Action": "cloudtrail:CreateEventDataStore",
      "Resource": "*",
      "Condition": {
        "ForAnyValue:StringNotEquals": {
          "aws:RequestTag/stage": [
            "alpha",
            "beta",
            "gamma",
            "prod"
          ]
        }
      }
    }
  ]
}
```

Im folgenden Beispiel wird das Löschen eines Ereignisdatenspeichers mit `DeleteEventDataStore` verweigert, wenn der Ereignisdatenspeicher ein `stage`-Tag mit dem Wert `prod` hat. Eine Richtlinie wie diese kann helfen, einen Ereignisdatenspeicher vor versehentlicher Löschung zu schützen.

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Deny",
```

```
    "Action": "cloudtrail:DeleteEventDataStore",
    "Resource": "*",
    "Condition": {
      "StringEquals": {
        "aws:ResourceTag/stage": "prod"
      }
    }
  ]
}
```

## Verwenden der CloudTrail-Konsole

Um auf die AWS CloudTrail Konsole zugreifen zu können, benötigen Sie ein Mindestmaß an Berechtigungen. Diese Berechtigungen müssen es Ihnen ermöglichen, Details zu den CloudTrail Ressourcen in Ihrem aufzulisten und anzuzeigen AWS-Konto. Wenn Sie eine identitätsbasierte Richtlinie erstellen, die strenger ist als die mindestens erforderlichen Berechtigungen, funktioniert die Konsole nicht wie vorgesehen für Entitäten (Benutzer oder Rollen) mit dieser Richtlinie.

Sie müssen Benutzern, die nur die API AWS CLI oder die AWS API aufrufen, keine Mindestberechtigungen für die Konsole gewähren. Stattdessen sollten Sie nur Zugriff auf die Aktionen zulassen, die der API-Operation entsprechen, die die Benutzer ausführen möchten.

### Erteilen von Berechtigungen für die CloudTrail Verwaltung

Damit IAM-Rollen oder -Benutzer eine CloudTrail Ressource verwalten können, z. B. einen Trail, einen Ereignisdatenspeicher oder einen Kanal, müssen Sie explizite Berechtigungen für die Ausführung der mit CloudTrail Aufgaben verbundenen Aktionen gewähren. In den meisten Situationen können Sie eine AWS verwaltete Richtlinie verwenden, die vordefinierte Berechtigungen enthält.

#### Note


Die Berechtigungen, die Sie Benutzern zur Durchführung von CloudTrail Verwaltungsaufgaben gewähren, sind nicht dieselben wie die Berechtigungen, die für die Übermittlung von Protokolldateien an Amazon S3 S3-Buckets oder das Senden von Benachrichtigungen an Amazon SNS SNS-Themen CloudTrail erforderlich sind. Weitere Informationen zu diesen Berechtigungen finden Sie unter [Amazon S3 S3-Bucket-Richtlinie für CloudTrail](#).

Wenn Sie die Integration mit Amazon CloudWatch Logs konfigurieren, benötigt es CloudTrail auch eine Rolle, die es übernehmen kann, um Ereignisse an eine Amazon CloudWatch Logs-Protokollgruppe zu übermitteln. Sie müssen die Rolle erstellen, die CloudTrail verwendet. Weitere Informationen finden Sie unter [Erteilen der Berechtigung zum Anzeigen und Konfigurieren von Amazon CloudWatch Logs-Informationen auf der CloudTrail Konsole](#) und [Ereignisse an CloudWatch Logs senden](#).

Die folgenden AWS verwalteten Richtlinien sind verfügbar für CloudTrail:

- [AWSCloudTrail\\_FullAccess](#)— Diese Richtlinie bietet vollen Zugriff auf CloudTrail Aktionen in CloudTrail Bezug auf Ressourcen wie Pfade, Ereignisdatenspeicher und Kanäle. Diese Richtlinie bietet die erforderlichen Berechtigungen zum Erstellen, Aktualisieren und Löschen von CloudTrail Pfaden, Ereignisdatenspeichern und Kanälen.

Diese Richtlinie bietet auch Berechtigungen zur Verwaltung des Amazon S3 S3-Buckets, der Protokollgruppe für CloudWatch Logs und eines Amazon SNS SNS-Themas für einen Trail. Die `AWSCloudTrail_FullAccess` verwaltete Richtlinie bietet jedoch keine Berechtigungen zum Löschen des Amazon S3 S3-Buckets, der Protokollgruppe für CloudWatch Logs oder eines Amazon SNS SNS-Themas. Informationen zu verwalteten Richtlinien für andere AWS-Services finden Sie im [Referenzhandbuch für AWS verwaltete Richtlinien](#).

 Note

Die `AWSCloudTrail_FullAccess`Richtlinie ist nicht für die allgemeine Verbreitung in Ihrem Unternehmen vorgesehen AWS-Konto. Benutzer mit dieser Rolle können die sensibelsten und wichtigsten Auditing-Funktionen in ihren AWS-Konten deaktivieren oder konfigurieren. Aus diesem Grund dürfen Sie diese Richtlinie nur auf Kontoadministratoren anwenden. Sie müssen die Anwendung dieser Richtlinie genau kontrollieren und überwachen.

- [AWSCloudTrail\\_ReadOnlyAccess](#)— Diese Richtlinie gewährt Berechtigungen zum Anzeigen der CloudTrail Konsole, einschließlich aktueller Ereignisse und des Ereignisverlaufs. Diese Richtlinie ermöglicht es Ihnen auch, vorhandene Trails, Ereignisdatenspeicher und Kanäle einzusehen. Rollen und Benutzer mit dieser Richtlinie können [den Ereignisverlauf herunterladen](#), aber sie können keine Trails, Ereignisdatenspeicher oder Kanäle erstellen oder aktualisieren.

Um Zugriff zu gewähren, fügen Sie Ihren Benutzern, Gruppen oder Rollen Berechtigungen hinzu:

- Benutzer und Gruppen in AWS IAM Identity Center:

Erstellen Sie einen Berechtigungssatz. Befolgen Sie die Anweisungen unter [Erstellen eines Berechtigungssatzes](#) im AWS IAM Identity Center -Benutzerhandbuch.

- Benutzer, die in IAM über einen Identitätsanbieter verwaltet werden:

Erstellen Sie eine Rolle für den Identitätsverbund. Befolgen Sie die Anweisungen unter [Erstellen einer Rolle für einen externen Identitätsanbieter \(Verbund\)](#) im IAM-Benutzerhandbuch.

- IAM-Benutzer:

- Erstellen Sie eine Rolle, die Ihr Benutzer annehmen kann. Folgen Sie den Anweisungen unter [Erstellen einer Rolle für einen IAM-Benutzer](#) im IAM-Benutzerhandbuch.
- (Nicht empfohlen) Weisen Sie einem Benutzer eine Richtlinie direkt zu oder fügen Sie einen Benutzer zu einer Benutzergruppe hinzu. Befolgen Sie die Anweisungen unter [Hinzufügen von Berechtigungen zu einem Benutzer \(Konsole\)](#) im IAM-Benutzerhandbuch.

## Weitere Ressourcen

Weitere Informationen zur Verwendung von IAM, um Identitäten wie Benutzern und Rollen Zugriff auf Ressourcen in Ihrem Konto zu gewähren, finden Sie unter [Einrichtung von IAM und Zugriffsverwaltung für AWS Ressourcen im IAM-Benutzerhandbuch](#).

Sie müssen Benutzern, die nur die API oder die API aufrufen, keine Mindestberechtigungen für die AWS CLI Konsole gewähren. AWS Stattdessen sollten Sie nur Zugriff auf die Aktionen zulassen, die den API-Operation entsprechen, die Sie ausführen möchten.

## 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 umfasst Berechtigungen zum Ausführen dieser Aktion auf der Konsole oder programmgesteuert mithilfe der API AWS CLI oder AWS .

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Sid": "ViewOwnUserInfo",
      "Effect": "Allow",
      "Action": [
```



```

        "iam:GetUserPolicy",
        "iam:ListGroupsWithUser",
        "iam:ListAttachedUserPolicies",
        "iam:ListUserPolicies",
        "iam:GetUser"
    ],
    "Resource": ["arn:aws:iam::*:user/${aws:username}"]
},
{
    "Sid": "NavigateInConsole",
    "Effect": "Allow",
    "Action": [
        "iam:GetGroupPolicy",
        "iam:GetPolicyVersion",
        "iam:GetPolicy",
        "iam:ListAttachedGroupPolicies",
        "iam:ListGroupPolicies",
        "iam:ListPolicyVersions",
        "iam:ListPolicies",
        "iam:ListUsers"
    ],
    "Resource": "*"
}
]
}

```

## Gewährung benutzerdefinierter Berechtigungen für Benutzer CloudTrail

CloudTrail Richtlinien gewähren Benutzern, die mit arbeiten, Berechtigungen CloudTrail. Wenn Sie Benutzern unterschiedliche Berechtigungen gewähren müssen, können Sie eine CloudTrail Richtlinie an eine IAM-Gruppe oder an einen Benutzer anhängen. Sie können die Richtlinie bearbeiten, um bestimmte Berechtigungen einzubinden oder auszuschließen. Zudem können Sie eine eigene benutzerdefinierte Richtlinie erstellen. Richtlinien sind JSON-Dokumente, in denen die Aktionen, die ein Benutzer ausführen darf, und die Ressourcen, für die der Benutzer diese Aktionen ausführen darf, definiert sind. Beispiele finden Sie unter [Beispiel: Zulassen und Verweigern von Aktionen für einen bestimmten Trail](#) und [Beispiele: Erstellen und Anwenden von Richtlinien bei Aktionen für bestimmte Trails](#).

### Inhalt

- [Schreibgeschützter Zugriff](#)
- [Vollzugriff](#)

- [Erteilen Sie die Berechtigung zum Anzeigen von AWS Config Informationen auf der Konsole CloudTrail](#)
- [Erteilen der Berechtigung zum Anzeigen und Konfigurieren von Amazon CloudWatch Logs-Informationen auf der CloudTrail Konsole](#)
- [Zusätzliche Informationen](#)

## Schreibgeschützter Zugriff

Das folgende Beispiel zeigt eine Richtlinie, die nur Lesezugriff auf Trails gewährt. CloudTrail Dies ist gleichbedeutend mit der verwalteten Richtlinie `AWSCloudTrail_ReadOnlyAccess`. Damit können Benutzer Informationen zu Trails anzeigen, aber die Trails weder erstellen noch aktualisieren.

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Action": [
        "cloudtrail:Get*",
        "cloudtrail:Describe*",
        "cloudtrail:List*",
        "cloudtrail:LookupEvents"
      ],
      "Resource": "*"
    }
  ]
}
```

In den Richtlinienanweisungen gibt das Element `Effect` an, ob die Aktionen zugelassen oder verweigert werden. Das Element `Action` listet die spezifischen Aktionen auf, die der Benutzer ausführen darf. Das `Resource` Element listet die AWS Ressourcen auf, auf denen der Benutzer diese Aktionen ausführen darf. Bei Richtlinien, die den Zugriff auf CloudTrail Aktionen steuern, ist das `Resource` Element normalerweise auf einen Platzhalter gesetzt\*, der „alle Ressourcen“ bedeutet.

Die Werte im Element `Action` entsprechen den APIs, die von den Services unterstützt werden. Den Aktionen wird ein vorangestellt, `cloudtrail:` um darauf hinzuweisen, dass sie sich auf Aktionen beziehen CloudTrail . Sie können das Platzhalterzeichen `*` im Element `Action` beispielsweise wie folgt verwenden:

- `"Action": ["cloudtrail:*Logging"]`

Dies ermöglicht alle CloudTrail Aktionen, die mit „Logging“ (StartLogging, StopLogging) enden.

- "Action": ["cloudtrail:\*"]

Dies erlaubt alle CloudTrail Aktionen, aber keine Aktionen für andere AWS Dienste.

- "Action": ["\*"]

Dies ermöglicht alle AWS Aktionen. Diese Berechtigung eignet sich für Benutzer, die als AWS - Administrator für Ihr Konto fungieren.

Die Richtlinie für den schreibgeschützten Zugriff gewährt Benutzern keine Berechtigung für die Aktionen CreateTrail, UpdateTrail, StartLogging und StopLogging. Benutzer mit dieser Richtlinie dürfen weder Trails erstellen oder aktualisieren noch die Protokollierung aktivieren und deaktivieren. Die Liste der CloudTrail Aktionen finden Sie in der [AWS CloudTrail API-Referenz](#).

## Vollzugriff

Das folgende Beispiel zeigt eine Richtlinie, die vollen Zugriff auf gewährt CloudTrail. Dies ist gleichbedeutend mit der verwalteten Richtlinie AWSCloudTrail\_FullAccess. Sie gewährt Benutzern die Berechtigung, alle CloudTrail Aktionen auszuführen. Außerdem können Benutzer Datenereignisse in Amazon S3 protokollieren und AWS Lambda Dateien in Amazon S3 S3-Buckets verwalten, verwalten, wie CloudWatch Logs Ereignisse überwacht CloudTrail , und Amazon SNS SNS-Themen in dem Konto verwalten, mit dem der Benutzer verknüpft ist.

### Important

Die AWSCloudTrail\_FullAccessRichtlinie oder gleichwertige Berechtigungen sind nicht für die gemeinsame Nutzung in Ihrem AWS Konto vorgesehen. Benutzer mit dieser Rolle oder einem gleichwertigen Zugriff haben die Möglichkeit, die sensibelsten und wichtigsten Prüfungsfunktionen in ihren AWS Konten zu deaktivieren oder neu zu konfigurieren. Aus diesem Grund sollte die Richtlinie nur für Kontoadministratoren verwendet werden; die Verwendung muss eng kontrolliert und überwacht werden.

```
{
  "Version": "2012-10-17",
  "Statement": [
```

```
{
  "Effect": "Allow",
  "Action": [
    "sns:AddPermission",
    "sns:CreateTopic",
    "sns:SetTopicAttributes",
    "sns:GetTopicAttributes"
  ],
  "Resource": [
    "arn:aws:sns:*:*:aws-cloudtrail-logs*"
  ]
},
{
  "Effect": "Allow",
  "Action": [
    "sns:ListTopics"
  ],
  "Resource": "*"
},
{
  "Effect": "Allow",
  "Action": [
    "s3:CreateBucket",
    "s3:PutBucketPolicy"
  ],
  "Resource": [
    "arn:aws:s3:::aws-cloudtrail-logs*"
  ]
},
{
  "Effect": "Allow",
  "Action": [
    "s3:ListAllMyBuckets",
    "s3:GetBucketLocation",
    "s3:GetBucketPolicy"
  ],
  "Resource": "*"
},
{
  "Effect": "Allow",
  "Action": "cloudtrail:*",
  "Resource": "*"
},
{
```

```
    "Effect": "Allow",
    "Action": [
      "logs:CreateLogGroup"
    ],
    "Resource": [
      "arn:aws:logs:*:*:log-group:aws-cloudtrail-logs*"
    ]
  },
  {
    "Effect": "Allow",
    "Action": [
      "iam:ListRoles",
      "iam:GetRolePolicy",
      "iam:GetUser"
    ],
    "Resource": "*"
  },
  {
    "Effect": "Allow",
    "Action": [
      "iam:PassRole"
    ],
    "Resource": "*",
    "Condition": {
      "StringEquals": {
        "iam:PassedToService": "cloudtrail.amazonaws.com"
      }
    }
  },
  {
    "Effect": "Allow",
    "Action": [
      "kms:CreateKey",
      "kms:CreateAlias",
      "kms:ListKeys",
      "kms:ListAliases"
    ],
    "Resource": "*"
  },
  {
    "Effect": "Allow",
    "Action": [
      "lambda:ListFunctions"
    ],
```

```

        "Resource": "*"
    },
    {
        "Effect": "Allow",
        "Action": [
            "dynamodb:ListGlobalTables",
            "dynamodb:ListTables"
        ],
        "Resource": "*"
    }
]
}

```

Erteilen Sie die Berechtigung zum Anzeigen von AWS Config Informationen auf der Konsole CloudTrail

Sie können Ereignisinformationen auf der CloudTrail Konsole anzeigen, einschließlich Ressourcen, die sich auf dieses Ereignis beziehen. Für diese Ressourcen können Sie das AWS Config Symbol auswählen, um die Zeitleiste für diese Ressource in der AWS Config Konsole anzuzeigen. Hängen Sie diese Richtlinie an Ihre Benutzer an, um ihnen nur Lesezugriff AWS Config zu gewähren. Die Richtlinie gewährt Benutzern keine Berechtigung zum Ändern von Einstellungen in AWS Config.

```

{
  "Version": "2012-10-17",
  "Statement": [{
    "Effect": "Allow",
    "Action": [
      "config:Get*",
      "config:Describe*",
      "config:List*"
    ],
    "Resource": "*"
  }]
}

```

Weitere Informationen finden Sie unter [Anzeigen von mit AWS Config referenzierten Ressourcen](#).

Erteilen der Berechtigung zum Anzeigen und Konfigurieren von Amazon CloudWatch Logs-Informationen auf der CloudTrail Konsole

Sie können die Übertragung von Ereignissen an CloudWatch Logs in der CloudTrail Konsole anzeigen und konfigurieren, sofern Sie über ausreichende Berechtigungen verfügen. Dies sind

Berechtigungen, die möglicherweise über die Berechtigungen hinausgehen, die CloudTrail Administratoren gewährt wurden. Hängen Sie diese Richtlinie an Administratoren an, die die CloudTrail Integration mit CloudWatch Logs konfigurieren und verwalten. Die Richtlinie gewährt ihnen nicht direkt Berechtigungen in CloudTrail oder in CloudWatch Logs, sondern gewährt stattdessen die Berechtigungen, die für die Erstellung und Konfiguration der Rolle erforderlich sind, die für die erfolgreiche Übertragung von Ereignissen an Ihre CloudWatch Logs-Gruppe verwendet CloudTrail wird.

```
{
  "Version": "2012-10-17",
  "Statement": [{
    "Effect": "Allow",
    "Action": [
      "iam:CreateRole",
      "iam:PutRolePolicy",
      "iam:AttachRolePolicy",
      "iam:ListRoles",
      "iam:GetRolePolicy",
      "iam:GetUser"
    ],
    "Resource": "*"
  }]
}
```

Weitere Informationen finden Sie unter [Überwachung von CloudTrail Protokolldateien mit Amazon CloudWatch Logs](#).

### Zusätzliche Informationen

Weitere Informationen zur Verwendung von IAM, um Identitäten wie Benutzern und Rollen Zugriff auf Ressourcen in Ihrem Konto zu gewähren, finden Sie unter [Erste Schritte](#) und [Zugriffsverwaltung für AWS Ressourcen](#) im IAM-Benutzerhandbuch.

## AWS CloudTrail Beispiele für ressourcenbasierte Richtlinien

CloudTrail unterstützt ressourcenbasierte Berechtigungsrichtlinien für CloudTrail Kanäle, die für Lake-Integrationen verwendet werden. CloudTrail Weitere Informationen zum Erstellen von Integrationen mit CloudTrail Lake finden Sie unter [Erstellen Sie eine Integration mit einer Ereignisquelle außerhalb von AWS](#)

Die für die Richtlinie erforderlichen Informationen werden durch den Integrationstyp bestimmt.

- Bei einer Direktionsintegration CloudTrail muss die Richtlinie die AWS-Konto IDs des Partners enthalten und Sie müssen die vom Partner bereitgestellte eindeutige externe ID eingeben. CloudTrail fügt die AWS-Konto IDs des Partners automatisch zur Ressourcenrichtlinie hinzu, wenn Sie eine Integration mithilfe der CloudTrail Konsole erstellen. In der [Dokumentation des Partners](#) erfahren Sie, wie Sie die für die Richtlinie erforderlichen AWS-Konto Nummern erhalten.
- Für eine Lösungsintegration müssen Sie mindestens eine AWS-Konto ID als Principal angeben und können optional eine externe ID eingeben, um zu verhindern, dass der Stellvertreter verwirrt wird.

Die folgenden Anforderungen gelten für die ressourcenbasierte Richtlinie:

- Der in der Richtlinie definierte Ressourcen-ARN muss mit dem Kanal-ARN übereinstimmen, an den die Richtlinie angehängt ist.
- Die Richtlinie enthält nur eine Aktion: `cloudtrail:data:PutAuditEvents`
- Jede Richtlinie muss mindestens eine Aussage enthalten. Die Richtlinie kann maximal 20 Aussagen umfassen.
- Jede Aussage enthält mindestens einen Prinzipal. Eine Aussage kann maximal 50 Prinzipale haben.

Der Kanalbesitzer kann die `PutAuditEvents`-API auf dem Kanal aufrufen, es sei denn, die Richtlinie verweigert dem Besitzer den Zugriff auf die Ressource.

Themen

- [Beispiel: Bereitstellung von Kanalzugriff für Prinzipale](#)
- [Beispiel: Verwendung einer externen ID, um einem verwirrten Stellvertreter vorzubeugen](#)

## Beispiel: Bereitstellung von Kanalzugriff für Prinzipale

Im folgenden Beispiel werden den Prinzipalen mit den ARNs `arn:aws:iam::111122223333:root`, `arn:aws:iam::444455556666:root`, und die Berechtigungen `arn:aws:iam::123456789012:root` zum Aufrufen der [PutAuditEvents](#) API auf dem CloudTrail Kanal mit dem ARN erteilt. `arn:aws:cloudtrail:us-east-1:777788889999:channel/EXAMPLE-80b5-40a7-ae65-6e099392355b`

```
{
```



```
"Version": "2012-10-17",
"Statement":
[
  {
    "Sid": "ChannelPolicy",
    "Effect": "Allow",
    "Principal":
    {
      "AWS":
      [
        "arn:aws:iam::111122223333:root",
        "arn:aws:iam::444455556666:root",
        "arn:aws:iam::123456789012:root"
      ]
    },
    "Action": "cloudtrail-data:PutAuditEvents",
    "Resource": "arn:aws:cloudtrail:us-east-1:777788889999:channel/
EXAMPLE-80b5-40a7-ae65-6e099392355b"
  }
]
}
```

## Beispiel: Verwendung einer externen ID, um einem verwirrten Stellvertreter vorzubeugen

Das folgende Beispiel verwendet eine externe ID, um [verwirrte Stellvertreter](#) anzusprechen und zu verhindern. Das Problem des verwirrten Stellvertreters ist ein Sicherheitsproblem, bei dem eine Entität, die keine Berechtigung zur Durchführung einer Aktion hat, eine privilegiere Entität zur Durchführung der Aktion zwingen kann.

Der Integrationspartner erstellt die externe ID, die in der Richtlinie verwendet werden soll. Anschließend stellt er Ihnen die externe ID im Rahmen der Integrationserstellung zur Verfügung. Dieser Wert kann eine beliebige eindeutige Zeichenfolge sein, wie eine Passphrase oder Kontonummer.

Im Beispiel werden den Prinzipalen mit den ARNs `arn:aws:iam::111122223333:root` und die Berechtigungen `arn:aws:iam::123456789012:root` zum Aufrufen der [PutAuditEvents](#) API auf der CloudTrail Kanalressource erteilt `arn:aws:iam::444455556666:root`, wenn der `PutAuditEvents` API-Aufruf den in der Richtlinie definierten externen ID-Wert enthält.

```
{
```

```

"Version": "2012-10-17",
"Statement":
[
  {
    "Sid": "ChannelPolicy",
    "Effect": "Allow",
    "Principal":
    {
      "AWS":
      [
        "arn:aws:iam::111122223333:root",
        "arn:aws:iam::444455556666:root",
        "arn:aws:iam::123456789012:root"
      ]
    },
    "Action": "cloudtrail-data:PutAuditEvents",
    "Resource": "arn:aws:cloudtrail:us-east-1:777788889999:channel/
EXAMPLE-80b5-40a7-ae65-6e099392355b",
    "Condition":
    {
      "StringEquals":
      {
        "cloudtrail:ExternalId": "uniquePartnerExternalID"
      }
    }
  }
]
}

```

## Amazon S3 S3-Bucket-Richtlinie für CloudTrail

Standardmäßig werden Amazon-S3-Buckets und -Objekte als privat eingestuft. Nur der Ressourcenbesitzer (das AWS -Konto, das den Bucket erstellt hat) kann auf den Bucket und die darin enthaltenen Objekte zugreifen. Der Ressourcenbesitzer kann anderen Ressourcen und Benutzern Zugriffsberechtigungen gewähren, indem er eine Zugriffsrichtlinie schreibt.

Um einen Amazon-S3-Bucket für den Empfang der Protokolldateien für einen Organisations-Trail zu erstellen oder zu modifizieren, müssen Sie die Bucket-Richtlinie ändern. Weitere Informationen finden Sie unter [Erstellen eines Trails für eine Organisation mit dem AWS Command Line Interface](#).

Um Protokolldateien an einen S3-Bucket zu übermitteln, CloudTrail müssen Sie über die erforderlichen Berechtigungen verfügen und der Bucket kann nicht als Bucket mit [anfordernder](#) Zahlung konfiguriert werden.

CloudTrail fügt der Richtlinie die folgenden Felder für Sie hinzu:

- Die zulässigen SIDs
- Den Bucket-Namen
- Der Dienstprinzipalname für CloudTrail
- Der Name des Ordners, in dem die Protokolldateien gespeichert sind, einschließlich des Bucket-Namens, eines Präfixes (falls Sie eines angegeben haben) und Ihrer AWS Konto-ID

Als bewährte Sicherheitsmethode gilt es, der Amazon S3-Bucket-Richtlinie einen `aws:SourceArn`-Bedingungsschlüssel hinzuzufügen. Der globale IAM-Bedingungsschlüssel `aws:SourceArn` trägt dazu bei, dass nur für einen oder mehrere bestimmte Trails in den S3-Bucket CloudTrail geschrieben wird. Der Wert von `aws:SourceArn` ist immer der ARN des Trails (oder ein Array von Trail-ARNs), der den Bucket zum Speichern von Protokollen verwendet. Denken Sie daran, den `aws:SourceArn`-Bedingungsschlüssel S3-Bucket-Richtlinien für bestehende Trails hinzuzufügen.

Die folgende Richtlinie ermöglicht CloudTrail das Schreiben von Protokolldateien von der unterstützten AWS-Regionen Seite in den Bucket. Ersetzen Sie *myBucketName*[*OptionalPrefix*]/, *MyAccountID*, *Region* und *TrailName* durch die entsprechenden Werte für Ihre Konfiguration.

### S3-Bucket-Richtlinie

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Sid": "AWSCloudTrailAclCheck20150319",
      "Effect": "Allow",
      "Principal": {"Service": "cloudtrail.amazonaws.com"},
      "Action": "s3:GetBucketAcl",
      "Resource": "arn:aws:s3:::myBucketName",
      "Condition": {
        "StringEquals": {
          "aws:SourceArn":
            "arn:aws:cloudtrail:region:myAccountID:trail/trailName"
        }
      }
    }
  ]
}
```

```

    }
  },
  {
    "Sid": "AWSCloudTrailWrite20150319",
    "Effect": "Allow",
    "Principal": {"Service": "cloudtrail.amazonaws.com"},
    "Action": "s3:PutObject",
    "Resource":
"arn:aws:s3:::myBucketName/[optionalPrefix]/AWSLogs/myAccountID/*",
    "Condition": {
      "StringEquals": {
        "s3:x-amz-acl": "bucket-owner-full-control",
        "aws:SourceArn":
"arn:aws:cloudtrail:region:myAccountID:trail/trailName"
      }
    }
  }
]
}

```

Weitere Informationen zu finden Sie unter [AWS-Regionen CloudTrail unterstützte Regionen](#)

## Inhalt

- [Angaben eines vorhandenen Buckets für die CloudTrail Protokollzustellung](#)
- [Empfangen von Protokolldateien anderer Konten](#)
- [Erstellen oder Aktualisieren eines Amazon-S3-Buckets zum Speichern der Protokolldateien für einen Organisations-Trail](#)
- [Amazon-S3-Bucket-Richtlinien korrigieren](#)
  - [Häufige Konfigurationsfehler in der Amazon-S3-Richtlinie](#)
  - [Ein Präfix für einen vorhandenen Bucket ändern](#)
- [Weitere Ressourcen](#)

## Angaben eines vorhandenen Buckets für die CloudTrail Protokollzustellung

Wenn Sie einen vorhandenen S3-Bucket als Speicherort für die Übertragung von Protokolldateien angegeben haben, müssen Sie dem Bucket eine Richtlinie hinzufügen, die das Schreiben in den Bucket ermöglicht CloudTrail .

**Note**

Es hat sich bewährt, einen speziellen S3-Bucket für CloudTrail Protokolle zu verwenden.

Um die erforderliche CloudTrail Richtlinie zu einem Amazon S3 S3-Bucket hinzuzufügen

1. Öffnen Sie die Amazon-S3-Konsole unter <https://console.aws.amazon.com/s3/>.
2. Wählen Sie den Bucket aus, in CloudTrail den Sie Ihre Protokolldateien bereitstellen möchten, und wählen Sie dann Berechtigungen aus.
3. Wählen Sie Bearbeiten aus.
4. Kopieren Sie die [S3 bucket policy](#) in das Fenster Bucket Policy Editor. Ersetzen Sie die Platzhalter in Kursivschrift durch die Namen des Buckets, durch den Präfix und die Kontonummer. Wenn Sie beim Erstellen eines Trails ein Präfix angegeben haben, fügen Sie ihn hier ein. Der Präfix ist ein optionaler Zusatz zum S3-Objektschlüssel, mit dem der Bucket ordnerähnlich organisiert wird.

**Note**

Wenn dem vorhandenen Bucket bereits eine oder mehrere Richtlinien angehängt sind, fügen Sie die Anweisungen für den CloudTrail Zugriff auf diese Richtlinie oder Richtlinien hinzu. Nehmen Sie eine Beurteilung der daraus resultierenden Berechtigungen vor, um sicherzustellen, dass sie für die Benutzer, die auf den Bucket zugreifen werden, geeignet sind.

## Empfangen von Protokolldateien anderer Konten

Sie können so konfigurieren CloudTrail , dass Protokolldateien von mehreren AWS Konten an einen einzigen S3-Bucket gesendet werden. Weitere Informationen finden Sie unter [Empfangen von CloudTrail Protokolldateien von mehreren Konten](#).

## Erstellen oder Aktualisieren eines Amazon-S3-Buckets zum Speichern der Protokolldateien für einen Organisations-Trail

Sie müssen einen Amazon-S3-Bucket für den Empfang der Protokolldateien für einen Organisationstrail angeben. Dieser Bucket muss über eine Richtlinie verfügen, die es CloudTrail ermöglicht, die Protokolldateien für die Organisation in den Bucket zu übernehmen.

Im Folgenden finden Sie eine Beispielrichtlinie für einen Amazon S3 S3-Bucket mit dem Namen *myOrganizationBucket*, der dem Verwaltungskonto der Organisation gehört. Ersetzen Sie *Region myOrganizationBucket*, *ManagementAccountID*, *TrailName* und *OrganizationId* durch die Werte für Ihre Organisation

Diese Bucket-Richtlinie besteht aus drei Anweisungen:

- Die erste Anweisung ermöglicht CloudTrail den Aufruf der Amazon S3 GetBucketAcl S3-Aktion im Amazon S3 S3-Bucket.
- Die zweite Anweisung ermöglicht die Protokollierung des Ereignisses für den Fall, dass der Trail von einem Organisations-Trail zu einem kontospezifischen Trail geändert wird.
- Die dritte Anweisung ermöglicht die Protokollierung eines Organisations-Trails.

Die Beispielrichtlinie enthält einen `aws:SourceArn`-Bedingungsschlüssel für die Richtlinie von Amazon-S3-Bucket. Der globale IAM-Bedingungsschlüssel `aws:SourceArn` trägt dazu bei, dass nur für einen oder mehrere bestimmte Pfade in den S3-Bucket CloudTrail geschrieben wird. In einem Organisations-Trail muss der Wert von `aws:SourceArn` ein Trail-ARN sein, der im Besitz des Verwaltungskontos ist und die Verwaltungskonto-ID verwendet.

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Sid": "AWSCloudTrailAclCheck20150319",
      "Effect": "Allow",
      "Principal": {
        "Service": [
          "cloudtrail.amazonaws.com"
        ]
      },
      "Action": "s3:GetBucketAcl",
      "Resource": "arn:aws:s3:::myOrganizationBucket",
      "Condition": {
        "StringEquals": {
          "aws:SourceArn":
            "arn:aws:cloudtrail:region:managementAccountID:trail/trailName"
        }
      }
    },
    {
```

```

    "Sid": "AWSCloudTrailWrite20150319",
    "Effect": "Allow",
    "Principal": {
      "Service": [
        "cloudtrail.amazonaws.com"
      ]
    },
    "Action": "s3:PutObject",
    "Resource": "arn:aws:s3:::myOrganizationBucket/AWSLogs/managementAccountID/
*",
    "Condition": {
      "StringEquals": {
        "s3:x-amz-acl": "bucket-owner-full-control",
        "aws:SourceArn":
"arn:aws:cloudtrail:region:managementAccountID:trail/trailName"
      }
    }
  },
  {
    "Sid": "AWSCloudTrailOrganizationWrite20150319",
    "Effect": "Allow",
    "Principal": {
      "Service": [
        "cloudtrail.amazonaws.com"
      ]
    },
    "Action": "s3:PutObject",
    "Resource": "arn:aws:s3:::myOrganizationBucket/AWSLogs/o-organizationID/*",
    "Condition": {
      "StringEquals": {
        "s3:x-amz-acl": "bucket-owner-full-control",
        "aws:SourceArn":
"arn:aws:cloudtrail:region:managementAccountID:trail/trailName"
      }
    }
  }
]
}

```

Diese Beispielrichtlinie sieht nicht vor, dass beliebige Benutzer über Mitgliedskonten auf die für die Organisation erstellten Protokolldateien zugreifen können. Standardmäßig ist der Zugriff auf die Protokolldateien der Organisation nur über das Verwaltungskonto möglich. Weitere Informationen

dazu, wie Sie IAM-Benutzern in Mitgliedskonten den Lesezugriff auf den Amazon-S3-Bucket gewähren, finden Sie unter [CloudTrail Protokolldateien zwischen AWS Konten teilen](#).

## Amazon-S3-Bucket-Richtlinien korrigieren

In den folgenden Abschnitten wird beschrieben, wie Sie Fehler in der S3-Bucket-Richtlinie beheben.

### Häufige Konfigurationsfehler in der Amazon-S3-Richtlinie

Wenn Sie im Rahmen der Erstellung oder Aktualisierung eines Trails einen neuen Bucket erstellen, werden Ihrem CloudTrail Bucket die erforderlichen Berechtigungen zugewiesen. Die Bucket-Richtlinie verwendet den Dienstprinzipalnamen "cloudtrail.amazonaws.com", der die Bereitstellung von Protokollen für alle Regionen ermöglicht CloudTrail .

Wenn CloudTrail keine Logs für eine Region zugestellt werden, ist es möglich, dass Ihr Bucket über eine ältere Richtlinie verfügt, die CloudTrail Konto-IDs für jede Region festlegt. Diese Richtlinie erteilt die CloudTrail Erlaubnis, Logs nur für die angegebenen Regionen zu liefern.

Es hat sich bewährt, die Richtlinie so zu aktualisieren, dass eine Genehmigung mit dem CloudTrail Dienstprinzipal verwendet wird. Ersetzen Sie dazu die Konto-ID-ARNs durch den Prinzipalnamen des Services: "cloudtrail.amazonaws.com". Dadurch wird die CloudTrail Erlaubnis erteilt, Protokolle für aktuelle und neue Regionen bereitzustellen. Als bewährte Sicherheitsmethode gilt es, der Amazon S3-Bucket-Richtlinie einen `aws:SourceArn`- oder `aws:SourceAccount`-Bedingungsschlüssel hinzuzufügen. Dadurch verhindern Sie nicht autorisierten Kontozugriff auf Ihren S3-Bucket. Wenn bereits Trails vorhanden sind, fügen Sie unbedingt einen oder mehrere Bedingungsschlüssel hinzu. Im Folgenden finden Sie ein Beispiel für eine empfohlene Richtlinienkonfiguration. Ersetzen Sie *myBucketName[optionalPrefix]*, *myAccountId*, *region* und *trailName* durch die entsprechenden Werte für Ihre Konfiguration.

### Example Beispiel einer Bucket-Richtlinie mit dem Service-Prinzipalnamen

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Sid": "AWSCloudTrailAclCheck20150319",
      "Effect": "Allow",
      "Principal": {"Service": "cloudtrail.amazonaws.com"},
      "Action": "s3:GetBucketAcl",
      "Resource": "arn:aws:s3:::myBucketName",
      "Condition": {
```



```

        "StringEquals": {
            "aws:SourceArn":
"arn:aws:cloudtrail:region:myAccountID:trail/trailName"
        }
    },
    {
        "Sid": "AWSCloudTrailWrite20150319",
        "Effect": "Allow",
        "Principal": {"Service": "cloudtrail.amazonaws.com"},
        "Action": "s3:PutObject",
        "Resource":
"arn:aws:s3::myBucketName/[optionalPrefix]/AWSLogs/myAccountID/*",
        "Condition": {"StringEquals": {
            "s3:x-amz-acl": "bucket-owner-full-control",
            "aws:SourceArn":
"arn:aws:cloudtrail:region:myAccountID:trail/trailName"
        }}
    }
}

```

Ein Präfix für einen vorhandenen Bucket ändern

Wenn Sie versuchen, ein Protokolldateipräfix für einen S3-Bucket hinzuzufügen, zu ändern oder zu entfernen, der Protokolle aus einem Trail erhält, wird möglicherweise folgende Fehlermeldung angezeigt: There is a problem with the bucket policy. Eine Bucket-Richtlinie mit einem falschen Präfix kann verhindern, dass über den Trail Protokolle an den Bucket übermittelt werden. Um dieses Problem zu beheben, verwenden Sie die Amazon S3 S3-Konsole, um das Präfix in der Bucket-Richtlinie zu aktualisieren, und verwenden Sie dann die CloudTrail Konsole, um dasselbe Präfix für den Bucket im Trail anzugeben.

So aktualisieren Sie das Präfix der Protokolldatei für einen Amazon-S3-Bucket

1. Öffnen Sie die Amazon-S3-Konsole unter <https://console.aws.amazon.com/s3/>.
2. Wählen Sie den Bucket aus, für den Sie das Präfix ändern möchten, und anschließend Permissions (Berechtigungen).
3. Wählen Sie Bearbeiten aus.
4. Bearbeiten Sie in der Bucket-Richtlinie unter der Aktion s3:PutObject den Resource-Eintrag, um das *Präfix*/ der Protokolldatei je nach Bedarf hinzuzufügen, zu ändern oder zu entfernen.

```
"Action": "s3:PutObject",  
  "Resource": "arn:aws:s3:::myBucketName/prefix/AWSLogs/myAccountID/*",
```

5. Wählen Sie Speichern.
6. Öffnen Sie die CloudTrail Konsole unter <https://console.aws.amazon.com/cloudtrail/>.
7. Wählen Sie Ihren Trail und klicken Sie in Storage location auf das Stiftsymbol, um die Einstellungen für Ihren Bucket zu bearbeiten.
8. Wählen Sie in S3 bucket den Bucket mit dem Präfix aus, den Sie ändern möchten.
9. Aktualisieren Sie in Log file prefix das Präfix, damit es dem Präfix entspricht, das Sie in der Bucket-Richtlinie eingegeben haben.
10. Wählen Sie Speichern.

## Weitere Ressourcen

Weitere Informationen zu S3-Buckets und Richtlinien finden Sie unter [Verwenden von Bucket-Richtlinien](#) im Amazon Simple Storage Service-Entwicklerleitfaden.

## Amazon S3 S3-Bucket-Richtlinie für CloudTrail Lake-Abfrageergebnisse

Standardmäßig werden Amazon-S3-Buckets und -Objekte als privat eingestuft. Nur der Ressourcenbesitzer (das AWS -Konto, das den Bucket erstellt hat) kann auf den Bucket und die darin enthaltenen Objekte zugreifen. Der Ressourcenbesitzer kann anderen Ressourcen und Benutzern Zugriffsberechtigungen gewähren, indem er eine Zugriffsrichtlinie schreibt.

Um CloudTrail Lake-Abfrageergebnisse an einen S3-Bucket zu übertragen, CloudTrail müssen Sie über die erforderlichen Berechtigungen verfügen und der Bucket kann nicht als Bucket mit [Anforderungszahlungen](#) konfiguriert werden.

CloudTrail fügt der Richtlinie die folgenden Felder für Sie hinzu:

- Die zulässigen SIDs
- Den Bucket-Namen
- Der Dienstprinzipalname für CloudTrail

Als bewährte Sicherheitsmethode gilt es, der Amazon S3-Bucket-Richtlinie einen `aws:SourceArn`-Bedingungsschlüssel hinzuzufügen. Der globale IAM-Bedingungsschlüssel `aws:SourceArn` trägt dazu bei, dass nur für den Ereignisdatenspeicher in den S3-Bucket CloudTrail geschrieben wird.

Die folgende Richtlinie ermöglicht CloudTrail die Übermittlung von Abfrageergebnissen aus dem unterstützten AWS-Regionen Bereich an den Bucket. Ersetzen Sie *myBucketNameMyAccountID* und *myQueryRunningRegion* durch die entsprechenden Werte für Ihre Konfiguration. Die *myAccountID* ist die für verwendete AWS Konto-ID CloudTrail, die möglicherweise nicht mit der AWS Konto-ID für den S3-Bucket identisch ist.

### Note

Wenn Ihre Bucket-Richtlinie eine Aussage für einen KMS-Schlüssel enthält, empfehlen wir, einen vollqualifizierten KMS-Schlüssel-ARN zu verwenden. Wenn Sie stattdessen einen KMS-Schlüsselalias verwenden, AWS KMS wird der Schlüssel im Konto des Anfragenden aufgelöst. Dieses Verhalten kann dazu führen, dass Daten mit einem KMS-Schlüssel verschlüsselt werden, der dem Anforderer und nicht dem Bucket-Eigentümer gehört. Wenn es sich um einen Ereignisdatenspeicher einer Organisation handelt, muss der ARN des Ereignisdatenspeichers die AWS -Konto-ID für das Verwaltungskonto enthalten. Der Grund hierfür ist, dass das Verwaltungskonto das Eigentum an allen Ressourcen der Organisation behält.

## S3-Bucket-Richtlinie

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Sid": "AWSCloudTrailLake1",
      "Effect": "Allow",
      "Principal": {"Service": "cloudtrail.amazonaws.com"},
      "Action": [
        "s3:PutObject*",
        "s3:Abort*"
      ],
      "Resource": [
        "arn:aws:s3:::myBucketName",
        "arn:aws:s3:::myBucketName/*"
      ],
    }
  ],
}
```

```

        "Condition": {
            "StringLike": {
                "aws:sourceAccount": "myAccountID",
                "aws:sourceArn":
"arn:aws:cloudtrail:myQueryRunningRegion:myAccountID:eventdatastore/*"
            }
        }
    },
    {
        "Sid": "AWSCloudTrailLake2",
        "Effect": "Allow",
        "Principal": {"Service":"cloudtrail.amazonaws.com"},
        "Action": "s3:GetBucketAcl",
        "Resource": "arn:aws:s3:::myBucketName",
        "Condition": {
            "StringLike": {
                "aws:sourceAccount": "myAccountID",
                "aws:sourceArn":
"arn:aws:cloudtrail:myQueryRunningRegion:myAccountID:eventdatastore/*"
            }
        }
    }
]
}

```

## Inhalt

- [Angaben eines vorhandenen Buckets für CloudTrail Lake-Abfrageergebnisse](#)
- [Weitere Ressourcen](#)

## Angaben eines vorhandenen Buckets für CloudTrail Lake-Abfrageergebnisse


Wenn Sie einen vorhandenen S3-Bucket als Speicherort für die Lieferung von CloudTrail Lake-Abfrageergebnissen angegeben haben, müssen Sie dem Bucket eine Richtlinie hinzufügen, die es ermöglicht, die Abfrageergebnisse an den Bucket CloudTrail zu übermitteln.

### Note

Es hat sich bewährt, einen speziellen S3-Bucket für CloudTrail Lake-Abfrageergebnisse zu verwenden.

Um die erforderliche CloudTrail Richtlinie zu einem Amazon S3 S3-Bucket hinzuzufügen

1. Öffnen Sie die Amazon-S3-Konsole unter <https://console.aws.amazon.com/s3/>.
2. Wählen Sie den Bucket aus, in CloudTrail den Sie Ihre Lake-Abfrageergebnisse liefern möchten, und wählen Sie dann Berechtigungen aus.
3. Wählen Sie Bearbeiten aus.
4. Kopieren Sie die [S3 bucket policy for query results](#) in das Fenster Bucket Policy Editor. Ersetzen Sie die Platzhalter in Kursivschrift durch die Namen des Buckets, der Region und die Kontonummer.

 Note


Wenn dem vorhandenen Bucket bereits eine oder mehrere Richtlinien angehängt sind, fügen Sie die Anweisungen für den CloudTrail Zugriff auf diese Richtlinie oder Richtlinien hinzu. Nehmen Sie eine Beurteilung der daraus resultierenden Berechtigungen vor, um sicherzustellen, dass sie für die Benutzer, die auf den Bucket zugreifen, geeignet sind.

## Weitere Ressourcen

Weitere Informationen zu S3-Buckets und Richtlinien finden Sie unter [Verwenden von Bucket-Richtlinien](#) im Amazon Simple Storage Service-Entwicklerleitfaden.

## Amazon SNS SNS-Themenrichtlinie für CloudTrail

Um Benachrichtigungen zu einem SNS-Thema zu senden, CloudTrail müssen Sie über die erforderlichen Berechtigungen verfügen. CloudTrail fügt dem Thema automatisch die erforderlichen Berechtigungen hinzu, wenn Sie im Rahmen der Erstellung oder Aktualisierung eines Trails in der Konsole ein Amazon SNS SNS-Thema erstellen. CloudTrail

 Important

Als bewährte Methode, den Zugriff auf Ihr SNS-Thema einzuschränken, wird dringend empfohlen, nach dem Erstellen oder Aktualisieren eines Trails zum Senden von SNS-Benachrichtigungen die IAM-Richtlinie manuell zu bearbeiten, die dem SNS-Thema zugeordnet ist, um Bedingungsschlüssel anzufügen. Weitere Informationen finden Sie unter

[the section called “Bewährte Sicherheitsmethoden für SNS-Themenrichtlinien”](#) in diesem Thema.

CloudTrail fügt der Richtlinie für Sie die folgende Erklärung mit den folgenden Feldern hinzu:

- Die zulässigen SIDs.
- Der Dienstprinzipalname für CloudTrail.
- Das SNS-Thema, einschließlich Region, Konto-ID und Name des Themas

Die folgende Richtlinie ermöglicht CloudTrail das Senden von Benachrichtigungen über die Übermittlung von Protokolldateien aus unterstützten Regionen. Weitere Informationen finden Sie unter [CloudTrail unterstützte Regionen](#). Dies ist die Standardrichtlinie, die einer neuen oder vorhandenen SNS-Themenrichtlinie angefügt ist, wenn Sie einen Trail erstellen oder aktualisieren und SNS-Benachrichtigungen aktivieren möchten.

### SNS-Themenrichtlinie

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Sid": "AWSCloudTrailSNSPolicy20131101",
      "Effect": "Allow",
      "Principal": {
        "Service": "cloudtrail.amazonaws.com"
      },
      "Action": "SNS:Publish",
      "Resource": "arn:aws:sns:region:SNSTopicOwnerAccountId:SNSTopicName"
    }
  ]
}
```

Um ein AWS KMS-verschlüsseltes Amazon SNS SNS-Thema zum Senden von Benachrichtigungen zu verwenden, müssen Sie auch die Kompatibilität zwischen der Ereignisquelle (CloudTrail) und dem verschlüsselten Thema aktivieren, indem Sie die folgende Erklärung zur Richtlinie von hinzufügen.

### AWS KMS key

### KMS-Schlüsselrichtlinie

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Principal": {
        "Service": "cloudtrail.amazonaws.com"
      },
      "Action": [
        "kms:GenerateDataKey*",
        "kms:Decrypt"
      ],
      "Resource": "*"
    }
  ]
}
```

Weitere Informationen finden Sie unter [Aktivieren der Kompatibilität zwischen Ereignisquellen aus AWS Diensten und verschlüsselten Themen](#).

## Inhalt

- [Bewährte Sicherheitsmethoden für SNS-Themenrichtlinien](#)
- [Angaben eines vorhandenen Themas zum Senden von Benachrichtigungen](#)
- [Beheben von Fehlern in der SNS-Themarihtlinie](#)
  - [CloudTrail sendet keine Benachrichtigungen für eine Region](#)
  - [CloudTrail sendet keine Benachrichtigungen für ein Mitgliedskonto in einer Organisation](#)
- [Weitere Ressourcen](#)

## Bewährte Sicherheitsmethoden für SNS-Themenrichtlinien

Standardmäßig erlaubt die IAM-Richtlinienerklärung, die Ihrem Amazon SNS CloudTrail SNS-Thema beigefügt ist, dem CloudTrail Service Principal, unter einem SNS-Thema zu veröffentlichen, das durch einen ARN identifiziert wird. Um zu verhindern, dass ein Angreifer Zugriff auf Ihr SNS-Thema erhält und Benachrichtigungen im Namen von CloudTrail Themenempfängern sendet, bearbeiten Sie Ihre CloudTrail SNS-Themenrichtlinie manuell und fügen Sie der von angehängten Richtlinienerklärung einen `aws:SourceArn` Bedingungsschlüssel hinzu. CloudTrail Der Wert dieses Schlüssels ist der ARN des Trails oder ein Array von Trail-ARNs, die das SNS-Thema verwenden. Da er sowohl die spezifische Trail-ID als auch die ID des Kontos enthält, das Besitzer des Trails ist,

beschränkt er den SNS-Themenzugriff auf nur die Konten, die über die Berechtigung zum Verwalten des Trails verfügen. Bevor Sie Bedingungsschlüssel zu Ihrer SNS-Themenrichtlinie hinzufügen, sollten Sie den Namen des SNS-Themas aus den Einstellungen Ihres Trails in der Konsole abrufen. CloudTrail

Der `aws:SourceAccount`-Bedingungsschlüssel wird ebenfalls unterstützt, aber nicht empfohlen.

So fügen Sie den Bedingungsschlüssel **aws:SourceArn** zu Ihrer SNS-Themenrichtlinie hinzu:

1. Öffnen Sie die Amazon SNS-Konsole unter <https://console.aws.amazon.com/sns/v3/home>.
2. Wählen Sie im Navigationsbereich Themen aus.
3. Wählen Sie das SNS-Thema aus, das in Ihren Trail-Einstellungen angezeigt wird und wählen Sie dann Bearbeiten.
4. Erweitern Sie die Option Zugriffsrichtlinie.
5. Suchen Sie im JSON-Editor für Zugriffsrichtlinien nach einem Block, der dem folgenden Beispiel ähnelt.

```
{
  "Sid": "AWSCloudTrailSNSPolicy20150319",
  "Effect": "Allow",
  "Principal": {
    "Service": "cloudtrail.amazonaws.com"
  },
  "Action": "SNS:Publish",
  "Resource": "arn:aws:sns:us-west-2:111122223333:aws-cloudtrail-logs-111122223333-61bbe496"
}
```

6. Fügen Sie einen neuen Block für eine Bedingung `aws:SourceArn` hinzu, wie im folgenden Beispiel gezeigt. Der Wert von `aws:SourceArn` ist der ARN des Trails, über den Sie Benachrichtigungen an SNS senden.

```
{
  "Sid": "AWSCloudTrailSNSPolicy20150319",
  "Effect": "Allow",
  "Principal": {
    "Service": "cloudtrail.amazonaws.com"
  },
  "Action": "SNS:Publish",
```



```

    "Resource": "arn:aws:sns:us-west-2:111122223333:aws-cloudtrail-logs-111122223333-61bbe496",
    "Condition": {
      "StringEquals": {
        "aws:SourceArn": "arn:aws:cloudtrail:us-west-2:123456789012:trail/Trail3"
      }
    }
  }
}

```

7. Wenn Sie mit der Bearbeitung der SNS-Themenrichtlinie fertig sind, wählen Sie Änderungen speichern.

So fügen Sie den Bedingungsschlüssel **aws:SourceAccount** zu Ihrer SNS-Themenrichtlinie hinzu

1. Öffnen Sie die Amazon SNS-Konsole unter <https://console.aws.amazon.com/sns/v3/home>.
2. Wählen Sie im Navigationsbereich Themen aus.
3. Wählen Sie das SNS-Thema aus, das in Ihren Trail-Einstellungen angezeigt wird und wählen Sie dann Bearbeiten.
4. Erweitern Sie die Option Zugriffsrichtlinie.
5. Suchen Sie im JSON-Editor für Zugriffsrichtlinien nach einem Block, der dem folgenden Beispiel ähnelt.

```

{
  "Sid": "AWSCloudTrailSNSPolicy20150319",
  "Effect": "Allow",
  "Principal": {
    "Service": "cloudtrail.amazonaws.com"
  },
  "Action": "SNS:Publish",
  "Resource": "arn:aws:sns:us-west-2:111122223333:aws-cloudtrail-logs-111122223333-61bbe496"
}

```

6. Fügen Sie einen neuen Block für eine Bedingung **aws:SourceAccount** hinzu, wie im folgenden Beispiel gezeigt. Der Wert von **aws:SourceAccount** ist die ID des Accounts, dem der Trail gehört. CloudTrail In diesem Beispiel wird der Zugriff auf das SNS-Thema auf die Benutzer beschränkt, die sich mit dem AWS Konto 123456789012 anmelden können.

```

{
  "Sid": "AWSCloudTrailSNSPolicy20150319",

```

```
"Effect": "Allow",
"Principal": {
  "Service": "cloudtrail.amazonaws.com"
},
"Action": "SNS:Publish",
"Resource": "arn:aws:sns:us-west-2:111122223333:aws-cloudtrail-logs-111122223333-61bbe496",
"Condition": {
  "StringEquals": {
    "aws:SourceAccount": "123456789012"
  }
}
}
```

7. Wenn Sie mit der Bearbeitung der SNS-Themenrichtlinie fertig sind, wählen Sie Änderungen speichern.

## Angeben eines vorhandenen Themas zum Senden von Benachrichtigungen

Sie können die Berechtigungen für ein Amazon SNS SNS-Thema manuell zu Ihrer Themenrichtlinie in der Amazon SNS SNS-Konsole hinzufügen und dann das Thema in der CloudTrail Konsole angeben.

So aktualisieren Sie eine SNS-Themenrichtlinie manuell:

1. Öffnen Sie die Amazon SNS-Konsole unter <https://console.aws.amazon.com/sns/v3/home>.
2. Klicken Sie auf Themen und wählen Sie das Thema aus.
3. Wählen Sie Bearbeiten und scrollen Sie dann nach unten zu Zugriffsrichtlinie.
4. Fügen Sie den Kontoauszug [SNS topic policy](#) mit den entsprechenden Werten für die Region, die Konto-ID und den Themennamen hinzu.
5. Wenn es sich bei Ihrem Thema um ein verschlüsseltes Thema handelt, CloudTrail müssen `kms:GenerateDataKey*` Sie die `kms:Decrypt` entsprechenden Berechtigungen angeben. Weitere Informationen finden Sie unter [Encrypted SNS topic KMS key policy](#).
6. Wählen Sie Save Changes (Änderungen speichern).
7. Kehren Sie zur CloudTrail Konsole zurück und geben Sie das Thema für den Trail an.

## Beheben von Fehlern in der SNS-Themenrichtlinie

In den folgenden Abschnitten wird beschrieben, wie Sie Fehler in der SNS-Themenrichtlinie beheben.

Szenarien:

- [CloudTrail sendet keine Benachrichtigungen für eine Region](#)
- [CloudTrail sendet keine Benachrichtigungen für ein Mitgliedskonto in einer Organisation](#)

### CloudTrail sendet keine Benachrichtigungen für eine Region

Wenn Sie im Rahmen der Erstellung oder Aktualisierung eines Trails ein neues Thema erstellen, CloudTrail ordnet es Ihrem Thema die erforderlichen Berechtigungen zu. Die Themenrichtlinie verwendet den Dienstprinzipalnamen "cloudtrail.amazonaws.com", der das Senden von Benachrichtigungen für alle Regionen ermöglicht CloudTrail .

Wenn für eine Region keine Benachrichtigungen gesendet werden, CloudTrail ist es möglich, dass für Ihr Thema eine ältere Richtlinie gilt, die CloudTrail Konto-IDs für jede Region festlegt. Diese Richtlinie CloudTrail erlaubt das Senden von Benachrichtigungen nur für die angegebenen Regionen.

Die folgende Themenrichtlinie ermöglicht CloudTrail das Senden von Benachrichtigungen nur für die angegebenen neun Regionen:

### Example Themenrichtlinie mit Konto-IDs

```
{
  "Version": "2012-10-17",
  "Statement": [{
    "Sid": "AWSCloudTrailSNSPolicy20131101",
    "Effect": "Allow",
    "Principal": {"AWS": [
      "arn:aws:iam::903692715234:root",
      "arn:aws:iam::035351147821:root",
      "arn:aws:iam::859597730677:root",
      "arn:aws:iam::814480443879:root",
      "arn:aws:iam::216624486486:root",
      "arn:aws:iam::086441151436:root",
      "arn:aws:iam::388731089494:root",
      "arn:aws:iam::284668455005:root",
      "arn:aws:iam::113285607260:root"
    ]},
    "Action": "SNS:Publish",
```

```

    "Resource": "aws:arn:sns:us-east-1:123456789012:myTopic"
  }]
}

```

Diese Richtlinie verwendet eine Berechtigung, die auf individuellen CloudTrail Konto-IDs basiert. Um Protokolle für eine neue Region bereitzustellen, müssen Sie die Richtlinie manuell aktualisieren, sodass sie die CloudTrail Konto-ID für diese Region enthält. Da beispielsweise Unterstützung für die Region USA Ost (Ohio) CloudTrail hinzugefügt wurde, müssen Sie die Richtlinie aktualisieren, um die Konto-ID ARN für diese Region hinzuzufügen: "arn:aws:iam::475085895292:root".

Es hat sich bewährt, die Richtlinie so zu aktualisieren, dass sie eine Berechtigung mit dem CloudTrail Service Principal verwendet. Ersetzen Sie dazu die Konto-ID-ARNs durch den Prinzipalnamen des Services: "cloudtrail.amazonaws.com".

Dadurch wird CloudTrail das Senden von Benachrichtigungen für aktuelle und neue Regionen ermöglicht. Im Folgenden finden Sie eine aktualisierte Version der vorherigen Richtlinie:

Example Themenrichtlinie mit Prinzipalnamen des Services

```

{
  "Version": "2012-10-17",
  "Statement": [{
    "Sid": "AWSCloudTrailSNSPolicy20131101",
    "Effect": "Allow",
    "Principal": {"Service": "cloudtrail.amazonaws.com"},
    "Action": "SNS:Publish",
    "Resource": "arn:aws:sns:us-west-2:123456789012:myTopic"
  }]
}

```

Überprüfen Sie, ob die Richtlinie die richtigen Werte enthält:

- Geben Sie im Feld `Resource` die Kontonummer des Themeneigentümers an. Geben Sie bei Themen, die Sie erstellen, Ihre Kontonummer an.
- Geben Sie die entsprechenden Werte für die Region und den Namen des SNS-Themas an.

CloudTrail sendet keine Benachrichtigungen für ein Mitgliedskonto in einer Organisation

Wenn ein Mitgliedskonto mit einem AWS Organizations Organisations-Trail keine Amazon SNS SNS-Benachrichtigungen sendet, liegt möglicherweise ein Problem mit der Konfiguration der SNS-

Themenrichtlinie vor. CloudTrail erstellt Organisationstrails in Mitgliedskonten, auch wenn eine Ressourcenvalidierung fehlschlägt. Beispielsweise enthält das SNS-Thema des Organisationstrails nicht alle Mitgliedskonto-IDs. Wenn die SNS-Themenrichtlinie falsch ist, tritt ein Autorisierungsfehler auf.

Um zu überprüfen, ob die SNS-Themenrichtlinie eines Trails einen Autorisierungsfehler aufweist:

- Überprüfe von der CloudTrail Konsole aus die Detailseite des Trails. Wenn die Autorisierung fehlschlägt, enthält die Detailseite eine Warnung `SNS authorization failed` und weist darauf hin, dass die SNS-Themenrichtlinie repariert werden muss.
- Führen Sie von der AWS CLI aus den [get-trail-status](#) Befehl aus. Wenn die Autorisierung fehlschlägt, enthält die Befehlsausgabe das `LastNotificationError` Feld mit dem Wert `AuthorizationError`.

## Weitere Ressourcen

Weitere Informationen zu SNS-Themen und zum Abonnieren von diesen finden Sie im [Entwicklerhandbuch zu Amazon Simple Notification Service](#).

## Fehlerbehebung bei AWS CloudTrail Identität und Zugriff

Verwenden Sie die folgenden Informationen, um häufig auftretende Probleme zu diagnostizieren und zu beheben, die bei der Arbeit mit CloudTrail IAM auftreten können.

### Themen

- [Ich bin nicht berechtigt, eine Aktion durchzuführen in CloudTrail](#)
- [Ich bin nicht zur Ausführung von iam:PassRole autorisiert.](#)
- [Ich möchte Personen außerhalb von mir den Zugriff AWS-Konto auf meine CloudTrail Ressourcen ermöglichen](#)
- [Ich bin nicht zur Ausführung von iam:PassRole autorisiert.](#)
- [Ich erhalte eine NoManagementAccountSLRExistsException-Ausnahme, wenn ich versuche, einen Organisations-Trail oder einen Ereignisdatenspeicher zu erstellen](#)

## Ich bin nicht berechtigt, eine Aktion durchzuführen in CloudTrail

Wenn Sie eine Fehlermeldung erhalten, dass Sie nicht zur Durchführung einer Aktion berechtigt sind, müssen Ihre Richtlinien aktualisiert werden, damit Sie die Aktion durchführen können.

Der folgende Beispielfehler tritt auf, wenn der IAM-Benutzer `mateojackson` versucht, über die Konsole Details zu einer fiktiven `my-example-widget`-Ressource anzuzeigen, jedoch nicht über `cloudtrail:GetWidget`-Berechtigungen verfügt.

```
User: arn:aws:iam::123456789012:user/mateojackson is not authorized to perform:
cloudtrail:GetWidget on resource: my-example-widget
```

In diesem Fall muss die Richtlinie für den Benutzer `mateojackson` aktualisiert werden, damit er mit der `cloudtrail:GetWidget`-Aktion auf die `my-example-widget`-Ressource zugreifen kann.

Wenn Sie Hilfe benötigen, wenden Sie sich an Ihren AWS Administrator. Ihr Administrator hat Ihnen Ihre Anmeldeinformationen zur Verfügung gestellt.

Wenn Ihnen AWS Management Console mitgeteilt wird, dass Sie nicht berechtigt sind, eine Aktion auszuführen, 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` IAM-Benutzer versucht, die Konsole zu verwenden, um Details zu einem Trail anzuzeigen, aber weder die entsprechende CloudTrail verwaltete Richtlinie (`AWSCloudTrail_FullAccess` oder `AWSCloudTrail_ReadOnlyAccess`) noch die entsprechenden Berechtigungen auf sein Konto angewendet wurden.

```
User: arn:aws:iam::123456789012:user/mateojackson is not authorized to perform:
cloudtrail:GetTrailStatus on resource: My-Trail
```

In diesem Fall bittet Mateo seinen Administrator, seine Richtlinien zu aktualisieren, damit er in der Konsole auf Trail-Informationen und -Status zugreifen kann.

Wenn Sie sich mit einem IAM-Benutzer oder einer IAM-Rolle anmelden, die über die `AWSCloudTrail_FullAccess`-verwaltete Richtlinie oder entsprechende Berechtigungen verfügt, und Sie die Amazon CloudWatch Logs-Integration mit einem Trail nicht konfigurieren können, fehlen Ihnen möglicherweise die erforderlichen Berechtigungen für die Integration mit diesen Diensten. Weitere Informationen finden Sie unter [Erteilen Sie die Berechtigung zum Anzeigen von AWS Config Informationen auf der Konsole CloudTrail](#) und [Erteilen der Berechtigung zum Anzeigen und Konfigurieren von Amazon CloudWatch Logs-Informationen auf der CloudTrail Konsole](#).

## Ich bin nicht zur Ausführung von **iam:PassRole** autorisiert.

Wenn Sie eine Fehlermeldung erhalten, dass Sie nicht berechtigt sind, die `iam:PassRole` Aktion durchzuführen, müssen Ihre Richtlinien aktualisiert werden, damit Sie eine Rolle an CloudTrail diese Person übergeben können.

Einige AWS-Services ermöglichen es Ihnen, eine bestehende Rolle an diesen Dienst zu übergeben, anstatt eine neue Servicerolle oder eine dienstverknüpfte Rolle zu erstellen. 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 auszuführen. CloudTrail 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.

Wenn Sie Hilfe benötigen, wenden Sie sich an Ihren AWS Administrator. Ihr Administrator hat Ihnen Ihre Anmeldeinformationen zur Verfügung gestellt.

## Ich möchte Personen außerhalb von mir den Zugriff AWS-Konto auf meine CloudTrail Ressourcen ermöglichen

Sie können eine Rolle erstellen und CloudTrail Informationen zwischen mehreren Personen austauschen AWS-Konten. Weitere Informationen finden Sie unter [CloudTrail Protokolldateien zwischen AWS Konten teilen](#).

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 darüber, ob diese Funktionen CloudTrail unterstützt werden, finden Sie unter [Wie AWS CloudTrail funktioniert mit IAM](#).
- Informationen dazu, wie Sie Zugriff auf Ihre Ressourcen gewähren können, AWS-Konten die Ihnen gehören, finden Sie im IAM-Benutzerhandbuch unter [Gewähren des Zugriffs auf einen IAM-Benutzer in einem anderen AWS-Konto , den Sie besitzen](#).
- Informationen dazu, wie Sie Dritten Zugriff auf Ihre Ressourcen gewähren können AWS-Konten, finden Sie [AWS-Konten im IAM-Benutzerhandbuch unter Gewähren des Zugriffs für Dritte](#).
- 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.

Ich bin nicht zur Ausführung von **iam:PassRole** autorisiert.

Wenn Sie eine Fehlermeldung erhalten, dass Sie nicht berechtigt sind, die `iam:PassRole` Aktion auszuführen, müssen Ihre Richtlinien aktualisiert werden, damit Sie eine Rolle an CloudTrail diese Person übergeben können.

Einige AWS-Services ermöglichen es Ihnen, eine bestehende Rolle an diesen Dienst zu übergeben, anstatt eine neue Servicerolle oder eine dienstverknüpfte Rolle zu erstellen. 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 auszuführen. CloudTrail 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.

Wenn Sie Hilfe benötigen, wenden Sie sich an Ihren AWS Administrator. Ihr Administrator hat Ihnen Ihre Anmeldeinformationen zur Verfügung gestellt.



Ich erhalte eine **NoManagementAccountSLRExistsException**-Ausnahme, wenn ich versuche, einen Organisations-Trail oder einen Ereignisdatenspeicher zu erstellen

Die Ausnahme `NoManagementAccountSLRExistsException` wird ausgelöst, wenn das Verwaltungskonto keine serviceverknüpfte Rolle hat. Wenn Sie mithilfe des API-Vorgangs `AWS Organizations` `AWS CLI` oder einen delegierten Administrator hinzufügen, wird die dienstbezogene Rolle nicht erstellt, sofern sie nicht existiert.

Wenn Sie das Verwaltungskonto Ihrer Organisation verwenden, um einen delegierten Administrator hinzuzufügen oder einen Organisationspfad- oder Ereignisdatenspeicher in der CloudTrail Konsole zu erstellen oder die CloudTrail API `AWS CLI` oder zu verwenden, CloudTrail wird automatisch eine dienstverknüpfte Rolle für Ihr Verwaltungskonto erstellt, sofern noch keine vorhanden ist.

Wenn Sie keinen delegierten Administrator hinzugefügt haben, verwenden Sie die CloudTrail Konsole `AWS CLI` oder die CloudTrail API, um den delegierten Administrator hinzuzufügen. Weitere Informationen zum Hinzufügen eines delegierten Administrators finden Sie unter [Fügen Sie einen delegierten Administrator hinzu CloudTrail](#) und [RegisterOrganizationDelegatedAdmin](#)(API).

Wenn Sie den delegierten Administrator bereits hinzugefügt haben, verwenden Sie das Verwaltungskonto, um den Organisationspfad- oder Ereignisdatenspeicher in der CloudTrail Konsole oder mithilfe der `AWS CLI` API oder zu erstellen. CloudTrail Weitere Informationen zum Erstellen eines Organisationspfads finden Sie unter [Vorbereiten der Erstellung eines Trails für Ihre Organisation in der Konsole](#)[Erstellen eines Trails für eine Organisation mit dem AWS Command Line Interface](#), und [CreateTrail](#)(API).

## Verwenden von serviceverknüpften Rollen für AWS CloudTrail

AWS CloudTrail verwendet AWS Identity and Access Management (IAM) [serviceverknüpfte](#) Rollen. Eine serviceverknüpfte Rolle ist ein einzigartiger Typ von IAM-Rolle, mit der direkt verknüpft ist. CloudTrail Mit Diensten verknüpfte Rollen sind vordefiniert CloudTrail und enthalten alle Berechtigungen, die der Dienst benötigt, um andere AWS-Services in Ihrem Namen anzurufen.

Eine dienstbezogene Rolle CloudTrail erleichtert die Einrichtung, da Sie die erforderlichen Berechtigungen nicht manuell hinzufügen müssen. CloudTrail definiert die Berechtigungen ihrer dienstbezogenen Rollen und CloudTrail kann, sofern nicht anders definiert, nur ihre Rollen übernehmen. Die definierten Berechtigungen umfassen die Vertrauens- und Berechtigungsrichtlinie. Diese Berechtigungsrichtlinie kann keinen anderen IAM-Entitäten zugewiesen werden.

Informationen zu anderen Services, die serviceverknüpften Rollen unterstützen, finden Sie unter [AWS -Services, die mit IAM funktionieren](#). Suchen Sie nach den Services, für die Ja in der Spalte

Serviceverknüpfte Rolle angegeben ist. Wählen Sie über einen Link Ja aus, um die Dokumentation zu einer serviceverknüpften Rolle für diesen Service anzuzeigen.

## Dienstbezogene Rollenberechtigungen für CloudTrail

CloudTrail verwendet die mit dem Dienst verknüpfte Rolle mit dem Namen `AWSServiceRoleForCloudTrail`— Diese dienstverknüpfte Rolle wird zur Unterstützung von Organisationstrails und Datenspeichern für Organisationsereignisse verwendet.

Die `AWSServiceRoleForCloudTrail` dienstbezogene Rolle vertraut darauf, dass die folgenden Dienste die Rolle übernehmen:

- `cloudtrail.amazonaws.com`

Diese Rolle wird verwendet, um die Erstellung und Verwaltung von CloudTrail Organisationspfaden und Datenspeichern von Organisationsereignissen in CloudTrail Lake zu unterstützen. CloudTrail Weitere Informationen finden Sie unter [Erstellen eines Trails für eine Organisation](#).

Die der Rolle zugeordnete [CloudTrailServiceRolePolicy](#) Richtlinie CloudTrail ermöglicht es, die folgenden Aktionen für die angegebenen Ressourcen durchzuführen:

- Aktionen für alle CloudTrail Ressourcen:
  - `All`
- Maßnahmen für alle AWS Organizations Ressourcen:
  - `organizations:DescribeAccount`
  - `organizations:DescribeOrganization`
  - `organizations:ListAccounts`
  - `organizations:ListAWSServiceAccessForOrganization`
- Aktionen für alle Organisationsressourcen für den CloudTrail Dienstprinzipal, um die delegierten Administratoren für die Organisation aufzulisten:
  - `organizations:ListDelegatedAdministrators`
- Aktionen zur [Deaktivierung des Lake-Verbunds](#) im Ereignisdatenspeicher einer Organisation:
  - `glue>DeleteTable`
  - `lakeformation:DeRegisterResource`

Sie müssen Berechtigungen konfigurieren, damit eine juristische Stelle von IAM (z. B. Benutzer, Gruppe oder Rolle) eine serviceverknüpfte Rolle erstellen, bearbeiten oder löschen kann. Weitere Informationen finden Sie unter [serviceverknüpfte Rollenberechtigungen](#) im IAM-Benutzerhandbuch.

## Erstellen einer dienstbezogenen Rolle für CloudTrail

Sie müssen eine serviceverknüpfte Rolle nicht manuell erstellen. Wenn Sie einen Organization-Trail- oder Organisationsereignisdatenspeicher erstellen, einen delegierten Administrator in der CloudTrail Konsole hinzufügen oder mithilfe des API-Vorgangs oder mithilfe des AWS CLI API-Vorgangs, CloudTrail wird die dienstbezogene Rolle für Sie erstellt, sofern sie noch nicht vorhanden ist.

Wenn Sie diese serviceverknüpfte Rolle löschen und dann erneut erstellen müssen, können Sie die Rolle in Ihrem Konto mit demselben Verfahren neu anlegen. Wenn Sie einen Organisationspfad- oder Organisationsereignisdatenspeicher erstellen oder einen delegierten Administrator hinzufügen, wird die dienstbezogene Rolle erneut für Sie CloudTrail erstellt.

## Bearbeiten einer serviceverknüpften Rolle für CloudTrail

CloudTrail erlaubt es Ihnen nicht, die `AWSServiceRoleForCloudTrail` dienstbezogene Rolle zu bearbeiten. Da möglicherweise verschiedene Entitäten auf die Rolle verweisen, kann der Rollename nach dem Erstellen einer serviceverknüpften Rolle nicht mehr geändert werden. Sie können jedoch die Beschreibung der Rolle mit IAM bearbeiten. Weitere Informationen finden Sie unter [Bearbeiten einer serviceverknüpften Rolle](#) im IAM-Benutzerhandbuch.

## Löschen einer dienstbezogenen Rolle für CloudTrail

Sie müssen die `AWSServiceRoleForCloudTrail` Rolle nicht manuell löschen. Wenn eine aus einer Organisation entfernt AWS-Konto wird, wird die `AWSServiceRoleForCloudTrail` Rolle automatisch aus dieser Organisation entfernt AWS-Konto. Sie können Richtlinien nicht von der serviceverknüpften Rolle `AWSServiceRoleForCloudTrail` in einem Organisationsverwaltungskonto trennen oder entfernen, ohne das Konto aus der Organisation zu entfernen.

Sie können die mit dem Service verknüpfte Rolle auch mithilfe der IAM-Konsole, der AWS CLI oder der AWS API manuell löschen. Sie müssen jedoch die Ressourcen für Ihre serviceverknüpfte Rolle zuerst manuell bereinigen, bevor Sie diese manuell löschen können.

**Note**

Wenn der CloudTrail Dienst die Rolle verwendet, wenn Sie versuchen, die Ressourcen zu löschen, schlägt das Löschen möglicherweise fehl. Wenn dies passiert, warten Sie einige Minuten und versuchen Sie es erneut.

Um eine Ressource, die von der Rolle AWSServiceRoleForCloudTrail verwendet wird, zu entfernen, können Sie einen der folgenden Schritte ausführen:

- Entfernen Sie den AWS-Konto aus der Organisation in Organizations.
- Aktualisieren Sie den Trail so, dass er nicht mehr ein Organisationstrail ist. Weitere Informationen finden Sie unter [Aktualisieren eines Trails](#).
- Aktualisieren Sie den Ereignisdatenspeicher, sodass er kein Ereignisdatenspeicher einer Organisation mehr ist. Weitere Informationen finden Sie unter [Aktualisieren Sie einen Ereignisdatenspeicher mit der Konsole](#).
- Löschen Sie den Trail. Weitere Informationen finden Sie unter [Löschen eines Trails](#).
- Löschen Sie den Ereignisdatenspeicher. Weitere Informationen finden Sie unter [Löschen Sie einen Ereignisdatenspeicher mit der Konsole](#).

So löschen Sie die serviceverknüpfte Rolle mit IAM

Verwenden Sie die IAM-Konsole, die oder die AWS API AWS CLI, um die AWSServiceRoleForCloudTrail serviceverknüpfte Rolle zu löschen. Weitere Informationen finden Sie unter [Löschen einer serviceverknüpften Rolle](#) im IAM-Benutzerhandbuch.

## Unterstützte Regionen für serviceverknüpfte Rollen CloudTrail

CloudTrail unterstützt die Verwendung von serviceverknüpften Rollen in allen Bereichen, in AWS-Regionen denen CloudTrail sowohl Where als auch Organizations verfügbar sind. Weitere Informationen finden Sie unter [AWS-Service -Endpunkte](#) in Allgemeine AWS-Referenz.

## AWS verwaltete Richtlinien für AWS CloudTrail

Um Benutzern, Gruppen und Rollen Berechtigungen hinzuzufügen, ist es einfacher, AWS verwaltete Richtlinien zu verwenden, als Richtlinien selbst zu schreiben. Es erfordert Zeit und Fachwissen, um [von Kunden verwaltete IAM-Richtlinien zu erstellen](#), die Ihrem Team nur die benötigten

Berechtigungen bieten. Um schnell loszulegen, können Sie AWS verwaltete Richtlinien verwenden. Diese Richtlinien decken allgemeine Anwendungsfälle ab und sind in Ihrem AWS-Konto verfügbar. Weitere Informationen zu AWS verwalteten Richtlinien finden Sie im IAM-Benutzerhandbuch unter [AWS Verwaltete Richtlinien](#).

AWS Dienste verwalten und aktualisieren AWS verwaltete Richtlinien. Sie können die Berechtigungen in AWS verwalteten Richtlinien nicht ändern. Services fügen einer von AWS verwalteten Richtlinien gelegentlich zusätzliche Berechtigungen hinzu, um neue Features zu unterstützen. Diese Art von Update betrifft alle Identitäten (Benutzer, Gruppen und Rollen), an welche die Richtlinie angehängt ist. Services aktualisieren eine von AWS verwaltete Richtlinie am ehesten, ein neues Feature gestartet wird oder neue Vorgänge verfügbar werden. Dienste entfernen keine Berechtigungen aus einer AWS verwalteten Richtlinie, sodass durch Richtlinienaktualisierungen Ihre bestehenden Berechtigungen nicht beeinträchtigt werden.

AWS Unterstützt außerdem verwaltete Richtlinien für Jobfunktionen, die sich über mehrere Dienste erstrecken. Die `ReadOnlyAccess` AWS verwaltete Richtlinie bietet beispielsweise schreibgeschützten Zugriff auf alle AWS Dienste und Ressourcen. Wenn ein Dienst eine neue Funktion startet, werden nur Leseberechtigungen für neue Operationen und Ressourcen AWS hinzugefügt. Eine Liste und Beschreibungen der Richtlinien für Auftragsfunktionen finden Sie in [Verwaltete AWS -Richtlinien für Auftragsfunktionen](#) im IAM-Leitfaden.

### AWS verwaltete Richtlinie: **`AWSCloudTrail_ReadOnlyAccess`**

Eine Benutzeridentität, deren Rolle die [AWSCloudTrail\\_ReadOnlyAccess](#) Richtlinie zugewiesen ist, kann schreibgeschützte Aktionen in CloudTrail, und `Describe*` Aktionen auf Pfaden `Get*List*`, CloudTrail Lake-Ereignisdatenspeichern oder Lake-Abfragen ausführen.

### AWS verwaltete Richtlinie: **`AWSServiceRoleForCloudTrail`**

Die [CloudTrailServiceRolePolicy](#) Richtlinie ermöglicht es AWS CloudTrail, in Ihrem Namen Aktionen an Organisationstrails und Datenspeichern von Organisationsereignissen durchzuführen. Die Richtlinie umfasst die erforderlichen AWS Organizations Berechtigungen für die Beschreibung und Auflistung der Organisationskonten und delegierten Administratoren in einer AWS Organizations Organisation.

Diese Richtlinie umfasst zusätzlich die erforderlichen AWS Lake Formation Berechtigungen AWS Glue und Berechtigungen zur [Deaktivierung von Lake Federation](#) in einem Ereignisdatenspeicher einer Organisation.

Diese Richtlinie ist der `AWSServiceRoleForCloudTrail`-dienstbezogenen Rolle zugeordnet, mit der CloudTrail Sie Aktionen in Ihrem Namen ausführen können. Sie können diese Richtlinie nicht an Ihre Benutzer, Gruppen oder Rollen anhängen.

## CloudTrail Aktualisierungen der AWS verwalteten Richtlinien

Details zu Aktualisierungen AWS verwalteter Richtlinien für anzeigen CloudTrail. Abonnieren Sie den RSS-Feed auf der Seite, um automatische Benachrichtigungen über Änderungen an dieser CloudTrail [Dokumentverlauf](#) Seite zu erhalten.

Änderung	Beschreibung	Datum
<a href="#">CloudTrailServiceRolePolicy</a> – Aktualisierung auf eine bestehende Richtlinie	Die Richtlinie wurde aktualisiert, um die folgenden Aktionen für einen Ereignisdatenspeicher einer Organisation zuzulassen, wenn der Verbund deaktiviert ist: <ul style="list-style-type: none"> <li><code>glue:DeleteTable</code></li> <li><code>lakeformation:DeregisterResource</code></li> </ul>	26. November 2023
<a href="#">AWSCloudTrail_ReadOnlyAccess</a> – Aktualisierung auf eine bestehende Richtlinie	CloudTrail hat den Namen der <code>AWSCloudTrailReadOnlyAccess</code> Richtlinie geändert in <code>AWSCloudTrail_ReadOnlyAccess</code> . Außerdem wurde der Umfang der Berechtigungen in der Richtlinie auf CloudTrail Aktionen reduziert. Amazon S3 oder AWS Lambda Aktionsberechtigungen sind nicht mehr enthalten. AWS KMS	6. Juni 2022

Änderung	Beschreibung	Datum
CloudTrail hat begonnen, Änderungen zu verfolgen	CloudTrail hat begonnen, Änderungen für die AWS verwalteten Richtlinien zu verfolgen.	6. Juni 2022

## Konformitätsvalidierung für AWS CloudTrail

Externe Prüfer bewerten die Sicherheit und Einhaltung von Vorschriften im AWS CloudTrail Rahmen mehrerer AWS Compliance-Programme. Hierzu zählen unter anderem SOC, PCI, FedRAMP und HIPAA.

Informationen darüber, ob AWS-Service ein [AWS-Services in den Geltungsbereich bestimmter Compliance-Programme fällt, finden Sie unter Umfang nach Compliance-Programm AWS-Services unter](#) . Wählen Sie dort das Compliance-Programm aus, an dem Sie interessiert sind. Allgemeine Informationen finden Sie unter [AWS Compliance-Programme AWS](#) .

Sie können Prüfberichte von Drittanbietern unter herunterladen AWS Artifact. Weitere Informationen finden Sie unter [Berichte herunterladen unter](#) .

Ihre Verantwortung für die Einhaltung der Vorschriften bei der Nutzung AWS-Services hängt von der Vertraulichkeit Ihrer Daten, den Compliance-Zielen Ihres Unternehmens und den geltenden Gesetzen und Vorschriften ab. AWS stellt die folgenden Ressourcen zur Verfügung, die Sie bei der Einhaltung der Vorschriften unterstützen:

- [Schnellstartanleitungen zu Sicherheit und Compliance](#) — In diesen Bereitstellungsleitfäden werden architektonische Überlegungen erörtert und Schritte für die Implementierung von Basisumgebungen beschrieben AWS , bei denen Sicherheit und Compliance im Mittelpunkt stehen.
- [Architecting for HIPAA Security and Compliance on Amazon Web Services](#) — In diesem Whitepaper wird beschrieben, wie Unternehmen HIPAA-fähige Anwendungen erstellen AWS können.

### Note

AWS-Services Nicht alle sind HIPAA-fähig. Weitere Informationen finden Sie in der [Referenz für HIPAA-berechtigte Services](#).

- [AWS Compliance-Ressourcen](#) — Diese Sammlung von Arbeitsmappen und Leitfäden gilt möglicherweise für Ihre Branche und Ihren Standort.
- [AWS Leitfäden zur Einhaltung von Vorschriften für Kunden](#) — Verstehen Sie das Modell der gemeinsamen Verantwortung aus dem Blickwinkel der Einhaltung von Vorschriften. In den Leitfäden werden die bewährten Verfahren zur Sicherung zusammengefasst AWS-Services 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.
- [Evaluierung von Ressourcen anhand von Regeln](#) im AWS Config Entwicklerhandbuch — Der AWS Config Service bewertet, wie gut Ihre Ressourcenkonfigurationen den internen Praktiken, Branchenrichtlinien und Vorschriften entsprechen.
- [AWS Security Hub](#)— Dies AWS-Service bietet einen umfassenden Überblick über Ihren internen Sicherheitsstatus. 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](#).
- [Amazon GuardDuty](#) — Dies AWS-Service erkennt potenzielle Bedrohungen für Ihre Workloads AWS-Konten, Container und Daten, indem es Ihre Umgebung auf verdächtige und böswillige Aktivitäten überwacht. GuardDuty kann Ihnen helfen, verschiedene Compliance-Anforderungen wie PCI DSS zu erfüllen, indem es die in bestimmten Compliance-Frameworks vorgeschriebenen Anforderungen zur Erkennung von Eindringlingen erfüllt.
- [AWS Audit Manager](#)— Auf diese AWS-Service Weise können Sie Ihre AWS Nutzung kontinuierlich überprüfen, um das Risikomanagement und die Einhaltung von Vorschriften und Industriestandards zu vereinfachen.

## Resilienz in AWS CloudTrail

Die AWS globale Infrastruktur basiert auf AWS Regionen und Availability Zones. AWS Regionen bieten mehrere physisch getrennte und isolierte Availability Zones, die über Netzwerke mit niedriger Latenz, hohem Durchsatz und hoher Redundanz miteinander verbunden sind. Mithilfe von Availability Zones können Sie Anwendungen und Datenbanken erstellen und ausführen, die automatisch Failover zwischen Availability Zones ausführen, ohne dass es zu Unterbrechungen kommt. Availability Zones sind besser hoch verfügbar, fehlertoleranter und skalierbarer als herkömmliche Infrastrukturen mit einem oder mehreren Rechenzentren. Wenn Sie Ihre CloudTrail Protokolldateien speziell über größere geografische Entfernungen replizieren müssen, können Sie



die [regionsübergreifende Replikation](#) für Ihre Amazon S3 S3-Trail-Buckets verwenden, wodurch das automatische, asynchrone Kopieren von Objekten zwischen Buckets in verschiedenen Regionen ermöglicht wird. AWS

[Weitere Informationen zu AWS Regionen und Availability Zones finden Sie unter Globale Infrastruktur.AWS](#)

Neben der AWS globalen Infrastruktur CloudTrail bietet es mehrere Funktionen zur Unterstützung Ihrer Datenausfallsicherheit und Backup-Anforderungen.

Datenspeicher für Pfade und Ereignisse, die Ereignisse in allen AWS Regionen protokollieren

Wenn Sie einen Trail auf alle AWS Regionen anwenden, werden in allen anderen Regionen der [AWS Partition](#), AWS-Regionen in der Sie arbeiten, Pfade mit identischer Konfiguration CloudTrail erstellt. Wenn eine neue Region AWS hinzugefügt wird, wird diese Trail-Konfiguration automatisch in der neuen Region erstellt.

Wenn Sie einen Datenspeicher für Ereignisse mit mehreren Regionen erstellen, werden alle Ereignisse AWS-Regionen in Ihrem Konto CloudTrail erfasst.

Versionierung, Lebenszykluskonfiguration und Objektspererschutz für Protokolldaten CloudTrail

Da Amazon S3-Buckets zum Speichern von Protokolldateien CloudTrail verwendet werden, können Sie auch die von Amazon S3 bereitgestellten Funktionen nutzen, um Ihre Datenausfallsicherheit und Ihre Sicherheitsanforderungen zu erfüllen. Weitere Informationen finden Sie unter [Belastbarkeit in Amazon S3](#).

## Infrastruktursicherheit in AWS CloudTrail

Als verwalteter Dienst AWS CloudTrail ist er durch AWS globale Netzwerksicherheit geschützt. Informationen zu AWS Sicherheitsdiensten und zum AWS Schutz der Infrastruktur finden Sie unter [AWS Cloud-Sicherheit](#). Informationen zum Entwerfen Ihrer AWS Umgebung unter Verwendung der bewährten Methoden für die Infrastruktursicherheit finden Sie unter [Infrastructure Protection](#) in Security Pillar AWS Well-Architected Framework.

Sie verwenden AWS veröffentlichte API-Aufrufe für den Zugriff CloudTrail über das Netzwerk. 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.

Die folgenden bewährten Sicherheitsmethoden befassen sich auch mit der Infrastruktursicherheit in folgenden Bereichen CloudTrail:

- [Erwägen Sie Amazon VPC-Endpunkte für den Trail-Zugriff.](#)
- Erwägen Sie Amazon-VPC-Endpunkte für den Zugriff zum Amazon-S3-Bucket. Weitere Informationen finden Sie unter [Steuern des Zugriffs von VPC-Endpunkten mit Bucket-Richtlinien.](#)
- Identifizieren und prüfen Sie alle Amazon S3 S3-Buckets, die CloudTrail Protokolldateien enthalten. Erwägen Sie die Verwendung von Tags, um sowohl Ihre CloudTrail Trails als auch die Amazon S3 S3-Buckets zu identifizieren, die CloudTrail Protokolldateien enthalten. Sie können dann Ressourcengruppen für Ihre CloudTrail Ressourcen verwenden. Weitere Informationen finden Sie unter [AWS Resource Groups](#).

## Serviceübergreifende Confused-Deputy-Prävention

Das Problem des verwirrten Stellvertreters ist ein Sicherheitsproblem, bei dem eine Entität, die keine Berechtigung zur Durchführung einer Aktion hat, eine privilegiertere Entität zur Durchführung der Aktion zwingen kann. Ein AWS dienstübergreifendes Identitätswechsels kann zum Problem des verwirrten Stellvertreters führen. Ein dienstübergreifender Identitätswechsel kann auftreten, wenn ein Dienst (der Anruf-Dienst) einen anderen Dienst anruft (den aufgerufenen Dienst). Der aufrufende Service kann manipuliert werden, um seine Berechtigungen zu verwenden, um Aktionen auf die Ressourcen eines anderen Kunden auszuführen, für die er sonst keine Zugriffsberechtigung haben sollte. Um dies zu verhindern, bietet AWS Tools, mit denen Sie Ihre Daten für alle Services mit Serviceprinzipalen schützen können, die Zugriff auf Ressourcen in Ihrem Konto erhalten haben.

Wir empfehlen, die Kontextschlüssel [aws:SourceArn](#) und die [aws:SourceAccount](#) globalen Bedingungsschlüssel in Ressourcenrichtlinien zu verwenden, um die Berechtigungen einzuschränken, die der AWS CloudTrail Ressource einen anderen Dienst gewähren. Verwenden Sie `aws:SourceArn`, wenn Sie nur eine Ressource mit dem betriebsübergreifenden Zugriff verknüpfen

möchten. Verwenden Sie `aws:SourceAccount`, wenn Sie zulassen möchten, dass Ressourcen in diesem Konto mit der betriebsübergreifenden Verwendung verknüpft 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 globalen Bedingungskontext-Schlüssel `aws:SourceArn` mit Platzhaltern (\*) für die unbekannt Teile des ARN. z. B. `"arn:aws:cloudtrail:*:AccountID:trail/*"`. Wenn Sie einen Platzhalter hinzufügen, müssen Sie auch den Bedingungsoperator `StringLike` verwenden.

Der Wert von `aws:SourceArn` muss der ARN des Trails, Ereignisdatenspeichers oder Kanals sein, der die Ressource verwendet.

Das folgende Beispiel zeigt, wie Sie die Kontextschlüssel `aws:SourceArn` und die `aws:SourceAccount` globale Bedingung verwenden können, CloudTrail um das Problem des verwirrten Stellvertreters zu verhindern: [Amazon S3 S3-Bucket-Richtlinie für CloudTrail Lake-Abfrageergebnisse](#).

## Bewährte Sicherheitsmethoden in AWS CloudTrail

AWS CloudTrail bietet eine Reihe von Sicherheitsfunktionen, die Sie bei der Entwicklung und Implementierung Ihrer eigenen Sicherheitsrichtlinien berücksichtigen sollten. Die folgenden bewährten Methoden sind allgemeine Richtlinien und keine vollständige Sicherheitslösung. Da diese bewährten Methoden für Ihre Umgebung möglicherweise nicht angemessen oder ausreichend sind, sollten Sie sie als hilfreiche Überlegungen und nicht als bindend ansehen.

### Themen

- [CloudTrail Bewährte Methoden zur Detektivsicherheit](#)
- [CloudTrail Bewährte Methoden zur präventiven Sicherheit](#)

## CloudTrail Bewährte Methoden zur Detektivsicherheit

### Einen Trail anlegen

Für eine fortlaufende Aufzeichnung der Ereignisse in Ihrem AWS Konto müssen Sie einen Trail erstellen. In der CloudTrail Konsole werden zwar Informationen zum Ereignisverlauf von 90 Tagen für Verwaltungsereignisse CloudTrail bereitgestellt, ohne dass ein Protokoll erstellt wird, es

handelt sich jedoch nicht um eine permanente Aufzeichnung und es werden keine Informationen zu allen möglichen Ereignistypen bereitgestellt. Für eine fortlaufende Aufzeichnung, die auch alle Ereignisarten berücksichtigt, die Sie angeben, müssen Sie einen Trail erstellen, der die Protokolldateien an einen von Ihnen angegebenen Amazon-S3-Bucket überträgt.

Um Ihnen die Verwaltung Ihrer CloudTrail Daten zu erleichtern, sollten Sie erwägen, einen Trail zu erstellen, der alle Verwaltungsereignisse protokolliert AWS-Regionen, und dann zusätzliche Trails zu erstellen, die bestimmte Ereignistypen für Ressourcen protokollieren, wie z. B. Amazon S3 S3-Bucket-Aktivitäten oder AWS Lambda -Funktionen.

Im Folgenden werden einige mögliche Maßnahmen aufgeführt:

- [Erstellen eines Trails für Ihr AWS -Konto](#)
- [Erstellen eines Trails für eine Organisation](#)

Wenden Sie Trails auf alle an AWS-Regionen

Um eine vollständige Aufzeichnung der Ereignisse zu erhalten, die von einer IAM-Identität oder einem Dienst in Ihrem AWS Konto erfasst wurden, sollte jeder Trail so konfiguriert sein, dass alle AWS-Regionen Ereignisse protokolliert werden. Indem Sie alle Ereignisse protokollieren AWS-Regionen, stellen Sie sicher, dass alle Ereignisse in Ihrem AWS Konto protokolliert werden, unabhängig davon, in welcher AWS Region sie aufgetreten sind. Dazu gehört die Protokollierung [globaler Serviceereignisse](#), die in einer für diesen Dienst spezifischen AWS Region protokolliert werden. Wenn Sie einen Trail erstellen, der für alle Regionen gilt, Ereignisse in jeder Region CloudTrail aufzeichnet und die CloudTrail Ereignisprotokolldateien an einen von Ihnen angegebenen S3-Bucket übermittelt. Wenn eine AWS -Region hinzugefügt wird, nachdem Sie einen Trail erstellt haben, der auf alle Regionen angewendet wird, wird diese neue Region automatisch aufgenommen, und alle Ereignisse in dieser Region werden protokolliert. Dies ist die Standardoption, wenn Sie einen Trail in der CloudTrail Konsole erstellen.

Im Folgenden werden einige mögliche Maßnahmen aufgeführt:

- [Erstellen eines Trails für Ihr AWS -Konto](#)
- [Aktualisieren eines vorhandenen Trails](#) für das Protokollieren von Ereignissen in allen AWS-Regionen
- Implementieren Sie fortlaufende Erkennungskontrollen, um sicherzustellen, dass alle erstellten Trails Ereignisse protokollieren, AWS-Regionen indem Sie die Regel in [multi-region-cloud-trail AWS Config-enabled](#) verwenden.

## Aktivieren Sie die Integrität der CloudTrail Protokolldatei

Validierte Protokolldateien sind bei Sicherheits- und kriminaltechnischen Ermittlungen unersetzlich. Beispiel: Mit einer validierten Protokolldatei können Sie bestätigen, dass die Protokolldatei selbst nicht geändert wurde oder dass mit bestimmten IAM-Anmeldeinformationen spezifische API-Aktivitäten ausgeführt wurden. Der Prozess zur Überprüfung der Integrität von CloudTrail Protokolldateien informiert Sie auch darüber, ob eine Protokolldatei gelöscht oder geändert wurde, oder Sie können bestätigen, dass in einem bestimmten Zeitraum keine Protokolldateien an Ihr Konto übermittelt wurden. CloudTrail Bei der Überprüfung der Integrität von Protokolldateien werden Industriestandardalgorithmen verwendet: SHA-256 für Hashing und SHA-256 mit RSA für digitale Signaturen. Das macht es rechnerisch unmöglich, Protokolldateien unbemerkt zu ändern, zu löschen oder zu fälschen. CloudTrail Weitere Informationen finden Sie unter [Aktivieren der Validierung und Validieren der Dateien](#).

## Integrieren Sie mit Amazon CloudWatch Logs

CloudWatch Logs ermöglicht es Ihnen, bestimmte Ereignisse zu überwachen und Warnmeldungen zu erhalten, die von erfasst wurden CloudTrail. Die an CloudWatch Logs gesendeten Ereignisse sind so konfiguriert, dass sie von Ihrem Trail protokolliert werden. Stellen Sie also sicher, dass Sie Ihren Trail oder Ihre Trails so konfiguriert haben, dass die Ereignistypen (Verwaltungsereignisse und/oder Datenereignisse) protokolliert werden, die Sie überwachen möchten.

Sie können beispielsweise wichtige sicherheits- und netzwerkbezogene Verwaltungsereignisse überwachen, z. B. [fehlgeschlagene AWS Management Console Anmeldeereignisse](#).

Im Folgenden werden einige mögliche Maßnahmen aufgeführt:

- Sehen Sie sich das Beispiel für die [Integration von CloudWatch Logs](#) für an. CloudTrail
- Konfigurieren Sie Ihren Trail so, dass [Ereignisse an CloudWatch Logs gesendet werden](#).
- Erwägen Sie die Implementierung fortlaufender Erkennungskontrollen, um sicherzustellen, dass alle Trails Ereignisse zur Überwachung an CloudWatch Logs senden, indem Sie die Regel [cloud-trail-cloud-watch-logs-enabled](#) in verwenden. AWS Config

## Verwenden Sie Amazon GuardDuty

Amazon GuardDuty ist ein Service zur Bedrohungserkennung, der Ihnen hilft, Ihre Konten, Container, Workloads und die Daten in Ihrer AWS Umgebung zu schützen. Mithilfe von Modellen für maschinelles Lernen (ML) und Funktionen zur Erkennung von Anomalien und Bedrohungen werden

GuardDuty kontinuierlich verschiedene Protokollquellen überwacht, um potenzielle Sicherheitsrisiken und böswillige Aktivitäten in Ihrer Umgebung zu identifizieren und zu priorisieren.

Erkennt beispielsweise eine potenzielle Exfiltration von Anmeldeinformationen, falls Anmeldeinformationen erkannt GuardDuty werden, die ausschließlich für eine Amazon EC2 EC2-Instance über eine Instance-Startrolle erstellt wurden, aber von einem anderen Konto innerhalb verwendet werden. AWS Weitere Informationen finden Sie im [GuardDuty Amazon-Benutzerhandbuch](#).

Verwenden Sie AWS Security Hub

Überwachen Sie Ihre Nutzung von CloudTrail in Bezug auf bewährte Sicherheitsmethoden mithilfe von [AWS Security Hub](#). Security Hub verwendet aufdeckende Sicherheitskontrollen für die Bewertung von Ressourcenkonfigurationen und Sicherheitsstandards, um Sie bei der Einhaltung verschiedener Compliance-Frameworks zu unterstützen. Weitere Informationen zur Verwendung von Security Hub zur Bewertung von CloudTrail Ressourcen finden Sie unter [AWS CloudTrail Kontrollen](#) im AWS Security Hub Benutzerhandbuch.

## CloudTrail Bewährte Methoden zur präventiven Sicherheit

Die folgenden bewährten Methoden für CloudTrail können dazu beitragen, Sicherheitsvorfälle zu verhindern.

Anmelden bei einem dedizierten und zentralisierten Amazon-S3-Bucket

CloudTrail Protokolldateien sind ein Auditprotokoll der Aktionen, die von einer IAM-Identität oder einem AWS Dienst ausgeführt werden. Die Integrität, Vollständigkeit und Verfügbarkeit dieser Protokolle ist entscheidend für forensische und Auditing-Zwecke. Durch die Protokollierung in einem dedizierten und zentralisierten Amazon-S3-Bucket können Sie strenge Sicherheitskontrollen, Zugriff und Aufgabentrennungen durchsetzen.

Im Folgenden werden einige mögliche Maßnahmen aufgeführt:

- Erstellen Sie ein separates AWS Konto als Protokollarchivkonto. Wenn Sie dieses Konto verwenden AWS Organizations, registrieren Sie es in der Organisation und erwägen Sie, [einen Organisationspfad zu erstellen](#), um Daten für alle AWS Konten in Ihrer Organisation zu protokollieren.
- Wenn Sie Organizations nicht verwenden, aber Daten für mehrere AWS Konten protokollieren möchten, [erstellen Sie einen Trail](#), um Aktivitäten in diesem Protokollarchivkonto zu protokollieren.

Beschränken Sie den Zugriff auf dieses Konto auf vertrauenswürdige administrative Benutzer, die auf Konto- und Auditing-Daten zugreifen können sollten.

- Erstellen Sie im Rahmen der Erstellung eines Trails, unabhängig davon, ob es sich um einen Organisations-Trail oder einen Trail für ein einzelnes AWS Konto handelt, einen speziellen Amazon S3 S3-Bucket, um Protokolldateien für diesen Trail zu speichern.
- Wenn Sie Aktivitäten für mehr als ein AWS Konto protokollieren möchten, [ändern Sie die Bucket-Richtlinie](#) so, dass Protokolldateien für alle AWS Konten protokolliert und gespeichert werden können, für die Sie AWS Kontoaktivitäten protokollieren möchten.
- Wenn Sie keinen Organisationstrail verwenden, erstellen Sie Trails in allen Ihren AWS -Konten und geben Sie den Amazon-S3-Bucket im Protokollarchivkonto an.

Verwenden Sie serverseitige Verschlüsselung mit AWS KMS verwalteten Schlüsseln

Standardmäßig werden die von Ihrem S3-Bucket CloudTrail übermittelten Protokolldateien mithilfe einer [serverseitigen Verschlüsselung mit einem KMS-Schlüssel \(SSE-KMS\)](#) verschlüsselt. Um SSE-KMS mit zu verwenden CloudTrail, erstellen und verwalten Sie einen [AWS KMS key](#), auch als KMS-Schlüssel bezeichnet.

#### Note

Wenn Sie SSE-KMS und die Validierung von Protokolldateien verwenden und Ihre Amazon-S3-Bucket-Richtlinie so geändert haben, dass nur mit SSE-KMS verschlüsselte Dateien zugelassen sind, können Sie keine Trails erstellen, die diesen Bucket verwenden, es sei denn, Sie modifizieren Ihre Bucket-Richtlinie zur spezifischen Zulassung der AES256-Verschlüsselung, wie in der nachfolgenden Beispiel-Richtlinienzeile gezeigt.

```
"StringNotEquals": { "s3:x-amz-server-side-encryption": ["aws:kms", "AES256"] }
```

Im Folgenden werden einige mögliche Maßnahmen aufgeführt:

- [Überprüfen Sie die Vorteile der Verschlüsselung Ihrer Protokolldateien mit SSE-KMS.](#)
- [Erstellen Sie einen KMS-Schlüssel für die Verschlüsselung von Protokolldateien.](#)
- [Konfigurieren Sie die Protokolldateiverschlüsselung für Ihre Trails.](#)

- Erwägen Sie die Implementierung fortlaufender Erkennungskontrollen, um sicherzustellen, dass alle Trails Protokolldateien mit SSE-KMS verschlüsseln, indem Sie die Regel in verwenden. [cloud-trail-encryption-enabled](#) AWS Config

Hinzufügen eines Bedingungsschlüssels zur standardmäßigen Amazon-SNS-Themenrichtlinie

Wenn Sie einen Trail für das Senden von Benachrichtigungen an Amazon SNS konfigurieren, CloudTrail fügt er Ihrer Zugriffsrichtlinie für SNS-Themen eine Richtlinienerklärung hinzu, die das Senden von Inhalten CloudTrail an ein SNS-Thema ermöglicht. Aus Sicherheitsgründen empfehlen wir, der Richtlinienerklärung einen `aws:SourceArn` (oder optionalen `aws:SourceAccount`) Bedingungsschlüssel hinzuzufügen. CloudTrail Dadurch verhindern Sie nicht autorisierten Kontozugriff auf Ihr SNS-Thema. Weitere Informationen finden Sie unter [Amazon SNS SNS-Themenrichtlinie für CloudTrail](#).

Implementieren des Zugriffs mit den geringsten Berechtigungen zu Amazon-S3-Buckets, in denen Sie Protokolldateien speichern

CloudTrail protokolliert Ereignisse in einem von Ihnen angegebenen Amazon S3 S3-Bucket. Diese Protokolldateien enthalten ein Auditprotokoll der Aktionen, die von IAM-Identitäten und AWS - Services ausgeführt wurden. Die Integrität und Vollständigkeit dieser Protokolldateien sind von zentraler Bedeutung für Audit- und forensische Zwecke. Um diese Integrität zu gewährleisten, sollten Sie bei der Erstellung oder Änderung des Zugriffs auf einen Amazon S3 S3-Bucket, der zum Speichern von CloudTrail Protokolldateien verwendet wird, das Prinzip der geringsten Rechte einhalten.

Gehen Sie dazu wie folgt vor:

- Überprüfen Sie die [Amazon S3-Bucket-Richtlinie](#) für alle Buckets, in denen Sie Protokolldateien speichern und passen Sie sie gegebenenfalls an, um unnötige Zugriffsrechte entfernen. Diese Bucket-Richtlinie wird für Sie generiert, wenn Sie mit der CloudTrail Konsole einen Trail erstellen. Sie kann aber auch manuell erstellt und verwaltet werden.
- Als bewährte Sicherheitsmethode gilt es, der Bucket-Richtlinie manuell einen `aws:SourceArn`-Bedingungsschlüssel hinzuzufügen. Weitere Informationen finden Sie unter [Amazon S3 S3-Bucket-Richtlinie für CloudTrail](#).
- Wenn Sie denselben Amazon S3 S3-Bucket verwenden, um Protokolldateien für mehrere AWS Konten zu speichern, folgen Sie den Anweisungen zum [Empfangen von Protokolldateien für mehrere Konten](#).



- Wenn Sie einen Organisationstrail verwenden, stellen Sie sicher, dass Sie die Anleitung für [Organisationstrails](#) befolgen, und sehen Sie sich die Beispielrichtlinie für einen Amazon-S3-Bucket für einen Organisationstrail in [Erstellen eines Trails für eine Organisation mit dem AWS Command Line Interface](#) an.
- Überprüfen Sie die [Amazon-S3-Sicherheits-Dokumentation](#) und die [beispielhafte Anleitung zum Sichern eines Buckets](#).

Aktivieren von MFA Delete für den Amazon-S3-Bucket, in dem Sie Protokolldateien speichern

Wenn Sie Multi-Faktor-Authentifizierung (MFA) konfigurieren, ist eine zusätzliche Authentifizierung erforderlich, um den Versionsverwaltungsstatus Ihres Buckets zu ändern oder eine Objektversion in einem Bucket zu löschen. Dadurch werden, selbst wenn sich ein Benutzer das Kennwort eines IAM-Benutzers mit Berechtigungen zum dauerhaften Löschen von Amazon-S3-Objekten verschafft hat, Operationen verhindert, die die Integrität Ihrer Protokolldateien beeinträchtigen könnten.

Im Folgenden werden einige mögliche Maßnahmen aufgeführt:

- Lesen Sie die Anleitung zu [MFA delete](#) im Benutzerhandbuch von Amazon Simple Storage Service.
- [Fügen Sie eine Amazon-S3-Bucket-Richtlinie hinzu, die MFA erfordert.](#)

#### Note

Sie können MFA Löschen nicht mit Lebenszykluskonfigurationen verwenden. Weitere Informationen zu Lebenszykluskonfigurationen und deren Interaktion mit anderen Konfigurationen finden Sie unter [Lebenszykluskonfigurationen und andere Bucket-Konfigurationen](#) im Benutzerhandbuch von Amazon Simple Storage Service.

Konfigurieren des Objekt-Lebenszyklusmanagements auf dem Amazon-S3-Bucket, in dem Sie Protokolldateien speichern

Standardmäßig werden Protokolldateien auf unbestimmte Zeit in dem für den Trail konfigurierten Amazon S3 S3-Bucket gespeichert. CloudTrail Sie können die [Amazon S3-Objektlebenszyklusregeln](#) verwenden, um Ihre eigene Aufbewahrungsrichtlinie zu erstellen, die besser zu Ihren geschäftlichen und Auditing-Anforderungen passt. So könnten Sie beispielsweise Protokolldateien, die mehr als

ein Jahr alt sind, in Amazon Glacier archivieren wollen, oder Protokolldateien nach Ablauf einer bestimmten Zeit löschen.

#### Note

Eine Lebenszyklus-Konfiguration wird auf MFA-fähigen Buckets (Multi-Factor Authentication) nicht unterstützt.

Beschränken Sie den Zugriff auf die Richtlinie `AWSCloudTrail_FullAccess`

Benutzer mit dieser [AWSCloudTrail\\_FullAccess](#)Richtlinie haben die Möglichkeit, die sensibelsten und wichtigsten Überwachungsfunktionen in ihren AWS Konten zu deaktivieren oder neu zu konfigurieren. Diese Richtlinie ist nicht dafür vorgesehen, gemeinsam genutzt oder allgemein auf IAM-Identitäten in Ihrem Konto angewendet zu werden. AWS Beschränken Sie die Anwendung dieser Richtlinie auf so wenige Personen wie möglich, d. h. auf Personen, von denen Sie erwarten, dass sie als AWS Kontoadministratoren agieren.

## CloudTrail Logdateien mit AWS KMS Schlüsseln verschlüsseln (SSE-KMS)

Standardmäßig werden die von an Ihren Bucket übermittelten CloudTrail Protokolldateien mithilfe einer [serverseitigen Verschlüsselung mit einem KMS-Schlüssel \(SSE-KMS\)](#) verschlüsselt. [Wenn Sie die SSE-KMS-Verschlüsselung nicht aktivieren, werden Ihre Protokolle mit der SSE-S3-Verschlüsselung verschlüsselt.](#)

#### Note

Die Aktivierung der serverseitigen Verschlüsselung verschlüsselt die Protokolldateien mit SSE-KMS, aber nicht die Digest-Dateien. Digest-Dateien werden mit [S3-verwalteten Verschlüsselungsschlüsseln \(SSE-S3\) von Amazon](#) verschlüsselt.

Wenn Sie einen vorhandenen S3-Bucket mit einem S3-Bucket-Schlüssel verwenden, CloudTrail müssen Sie in der [Schlüsselrichtlinie](#) über die entsprechenden Berechtigungen verfügen, um die Aktionen und verwenden zu können. AWS KMS `GenerateDataKey` `DescribeKey` Wenn `cloudtrail.amazonaws.com` diese Berechtigungen in der Schlüsselrichtlinie nicht gewährt werden, können Sie keinen Trail erstellen oder aktualisieren.

Um SSE-KMS mit zu verwenden CloudTrail, erstellen und verwalten Sie einen KMS-Schlüssel, auch bekannt als [AWS KMS key](#). Sie fügen dem Schlüssel eine Richtlinie hinzu, die festlegt, welche Benutzer den Schlüssel zum Verschlüsseln und CloudTrail Entschlüsseln von Protokolldateien verwenden können. Die Entschlüsselung erfolgt nahtlos über S3. Wenn autorisierte Benutzer des Schlüssels CloudTrail Protokolldateien lesen, verwaltet S3 die Entschlüsselung, und die autorisierten Benutzer können Protokolldateien in unverschlüsselter Form lesen.

Dieser Ansatz bietet folgende Vorteile:

- Sie können den KMS-Schlüssel-Verschlüsselungsschlüssel selbst erstellen und verwalten.
- Sie können mit einem einzelnen KMS-Schlüssel Protokolldateien für mehrere Konten in allen Regionen ver- und entschlüsseln.
- Sie haben die Kontrolle darüber, wer Ihren Schlüssel zum Verschlüsseln und CloudTrail Entschlüsseln von Protokolldateien verwenden kann. Sie können den Benutzern in Ihrer Organisation Berechtigungen für den Schlüssel entsprechend Ihren Anforderungen zuweisen.
- Sie profitieren von verbesserter Sicherheit. Um mit dieser Funktion Protokolldateien zu lesen, sind die folgenden Berechtigungen erforderlich:
  - Ein Benutzer muss über Leseberechtigungen für den S3-Bucket mit den Protokolldateien verfügen.
  - Ein Benutzer muss zudem über eine Richtlinie oder Rolle verfügen, die das Entschlüsseln von Berechtigungen mit der KMS-Schlüssel-Richtlinie erlaubt.
- Da S3 die Protokolldateien für Anfragen von Benutzern, die zur Verwendung des KMS-Schlüssels autorisiert sind, automatisch entschlüsselt, ist die SSE-KMS-Verschlüsselung für CloudTrail Protokolldateien abwärtskompatibel mit Anwendungen, die Protokolldaten lesen. CloudTrail

#### Note

Der von Ihnen gewählte KMS-Schlüssel muss in derselben AWS Region erstellt werden wie der Amazon S3 S3-Bucket, der Ihre Protokolldateien empfängt. Beispiel: Wenn die Protokolldateien in einem Bucket in der Region USA Ost (Ohio) gespeichert werden, müssen Sie einen KMS-Schlüssel erstellen oder wählen, der in dieser Region erstellt wurde. Zum Überprüfen der Region für einen Amazon-S3-Bucket sehen Sie sich die entsprechenden Eigenschaften in der Amazon-S3-Konsole an.

## Aktivieren der Verschlüsselung von Protokolldateien

### Note

Wenn Sie in der CloudTrail Konsole einen KMS-Schlüssel erstellen, werden die erforderlichen Abschnitte mit den KMS-Schlüsselrichtlinien für Sie CloudTrail hinzugefügt. Gehen Sie wie folgt vor, wenn Sie einen Schlüssel in der IAM-Konsole erstellt haben oder AWS CLI die erforderlichen Richtlinienabschnitte manuell hinzufügen müssen.

Führen Sie die folgenden allgemeinen Schritte aus, um die SSE-KMS-Verschlüsselung für CloudTrail Protokolldateien zu aktivieren:

#### 1. Erstellen eines KMS-Schlüssels.

- Informationen zum Erstellen eines KMS-Schlüssels mit dem AWS Management Console finden Sie unter [Creating Keys](#) im AWS Key Management Service Developer Guide.
- Informationen zum Erstellen eines KMS-Schlüssels mit dem finden Sie AWS CLI unter [create-key](#).

### Note

Der von Ihnen ausgewählte KMS-Schlüssel muss sich in derselben Region befinden wie der S3-Bucket, der Ihre Protokolldateien empfängt. Zum Überprüfen der Region für einen S3-Bucket sehen Sie sich die Eigenschaften des Buckets in der S3-Konsole an.

#### 2. Fügen Sie dem Schlüssel Richtlinienabschnitte hinzu, die das Verschlüsseln und CloudTrail das Entschlüsseln von Protokolldateien durch Benutzer ermöglichen.

- Weitere Informationen zu den erforderlichen Inhalten der Richtlinie finden Sie unter [Konfigurieren Sie AWS KMS wichtige Richtlinien für CloudTrail](#).

### Warning

Stellen Sie sicher, Berechtigungen zum Entschlüsseln für alle Benutzer, die Protokolldateien lesen müssen, in die Richtlinie aufzunehmen. Wenn Sie diesen Schritt nicht ausführen, bevor Sie den Schlüssel der Trail-Konfiguration hinzufügen, können

Benutzer ohne Berechtigungen zum Entschlüsseln keine verschlüsselten Dateien lesen, bis Sie ihnen diese Berechtigungen erteilen.

- Weitere Informationen zum Bearbeiten einer Richtlinie mit der IAM-Konsole finden Sie unter [Bearbeiten einer Schlüsselrichtlinie](#) im AWS Key Management Service -Entwicklerhandbuch.
  - Informationen zum Anhängen einer Richtlinie an einen KMS-Schlüssel mit dem AWS CLI finden Sie unter. [put-key-policy](#)
3. Aktualisieren Sie Ihren Trail, sodass er den KMS-Schlüssel verwendet, dessen Richtlinie Sie geändert haben. CloudTrail
- Informationen zum Aktualisieren Ihrer Trail-Konfiguration mithilfe der CloudTrail Konsole finden Sie unter [Aktualisieren einer Ressource zur Verwendung des KMS-Schlüssels](#).
  - Informationen zum Aktualisieren Ihrer Trail-Konfiguration mithilfe der AWS CLI finden Sie unter [Aktivieren und Deaktivieren der CloudTrail Protokolldateiverschlüsselung mit dem AWS CLI](#).

CloudTrail unterstützt auch Schlüssel AWS KMS für mehrere Regionen. Weitere Informationen finden Sie über Multi-Regions-Schlüssel finden Sie unter [Verwenden von Schlüsseln für mehrere Regionen](#) im AWS Key Management Service -Entwicklerhandbuch.

Im nächsten Abschnitt werden die Richtlinienabschnitte beschrieben, die für die Verwendung mit CloudTrail Ihrer KMS-Schlüsselrichtlinie erforderlich sind.

## Erteilen der Berechtigung zum Erstellen eines KMS-Schlüssels

Mit der `AWSKeyManagementServicePowerUser` Richtlinie können Sie Benutzern die Erlaubnis erteilen, AWS KMS key einen zu erstellen.

Erteilt die Berechtigung zum Erstellen eines KMS-Schlüssels

1. Öffnen Sie die IAM-Konsole unter <https://console.aws.amazon.com/iam/>.
2. Wählen Sie die Gruppen oder den Benutzer aus, der/dem Sie eine Berechtigung zuweisen möchten.
3. Wählen Sie Permissions und anschließend Attach Policy.
4. Suchen Sie nach `AWSKeyManagementServicePowerUser`, wählen Sie die Richtlinie und wählen Sie anschließend Attach Richtlinie aus.

Der Benutzer verfügt jetzt über die Berechtigung zum Erstellen eines KMS-Schlüssel. Weitere Informationen zum Erstellen von Richtlinien finden Sie unter [Erstellen von IAM-Richtlinien](#) im IAM-Benutzerhandbuch.

## Konfigurieren Sie AWS KMS wichtige Richtlinien für CloudTrail

Sie können eine AWS KMS key auf drei Arten erstellen:

- Die CloudTrail Konsole
- Die AWS Management-Konsole
- Die AWS CLI

### Note

Wenn Sie in der CloudTrail Konsole einen KMS-Schlüssel erstellen, CloudTrail fügt er die erforderliche KMS-Schlüsselrichtlinie für Sie hinzu. Sie müssen die Richtlinienanweisungen nicht manuell hinzufügen. Siehe [In CloudTrail der Konsole erstellte Standard-KMS-Schlüsselrichtlinie](#).

Wenn Sie einen KMS-Schlüssel in der AWS Verwaltung oder im erstellen AWS CLI, müssen Sie dem Schlüssel Richtlinienabschnitte hinzufügen, damit Sie ihn mit verwenden können CloudTrail. Die Richtlinie muss die Verwendung des Schlüssels zur Verschlüsselung Ihrer Protokolldateien und Ereignisdatenspeicher ermöglichen und den von Ihnen angegebenen Benutzern das Lesen von Protokolldateien in unverschlüsselter Form ermöglichen. CloudTrail

Weitere Informationen finden Sie in den folgenden Ressourcen:

- [Informationen zum Erstellen eines KMS-Schlüssels mit dem finden Sie unter AWS CLI create-key.](#)
- Informationen zum Bearbeiten einer KMS-Schlüsselrichtlinie für CloudTrail finden Sie unter [Bearbeiten einer Schlüsselrichtlinie](#) im AWS Key Management Service Entwicklerhandbuch.
- Technische Informationen zur CloudTrail Verwendung finden Sie AWS KMS unter [So AWS CloudTrail verwenden](#) Sie AWS KMS im AWS Key Management Service Entwicklerhandbuch.

## Erforderliche Abschnitte mit den wichtigsten KMS-Richtlinien für die Verwendung mit CloudTrail

Wenn Sie einen KMS-Schlüssel mit der AWS Managementkonsole oder der erstellt haben AWS CLI, müssen Sie Ihrer KMS-Schlüsselrichtlinie mindestens die folgenden Anweisungen hinzufügen, damit sie verwendet werden kann CloudTrail.

### Themen

- [Für Trails erforderliche Elemente der KMS-Schlüsselrichtlinie](#)
- [Für Ereignisdatenspeicher erforderliche Elemente der KMS-Schlüsselrichtlinie](#)

### Für Trails erforderliche Elemente der KMS-Schlüsselrichtlinie

1. Aktivieren CloudTrail Sie die Berechtigungen zum Verschlüsseln von Protokollen. Siehe [Gewähren von Verschlüsselungsberechtigungen](#).
2. Aktivieren CloudTrail Sie die Berechtigungen zum Entschlüsseln von Protokollen. Siehe [Gewähren von Entschlüsselungsberechtigungen](#). Wenn Sie einen vorhandenen S3 Bucket mit einem [S3-Bucket-Schlüssel](#) verwenden, sind `kms:Decrypt` Berechtigungen erforderlich, um einen Trail mit aktivierter SSE-KMS-Verschlüsselung zu erstellen oder zu aktualisieren.
3. Aktivieren Sie CloudTrail diese Option, um Eigenschaften von KMS-Schlüsseln zu beschreiben. Siehe [Aktivieren Sie CloudTrail diese Option, um KMS-Schlüsseleigenschaften zu beschreiben](#).

Als bewährte Sicherheitsmethode gilt es, der KMS-Schlüsselrichtlinie einen `aws:SourceArn`-Bedingungsschlüssel hinzuzufügen. Mit dem globalen IAM-Bedingungsschlüssel wird `aws:SourceArn` sichergestellt, dass der KMS-Schlüssel nur für einen oder mehrere bestimmte Pfade CloudTrail verwendet wird. Der Wert von `aws:SourceArn` ist immer der Trail-ARN (oder ein Array von Trail-ARNs), der den KMS-Schlüssel verwendet. Denken Sie daran, den `aws:SourceArn`-Bedingungsschlüssel KMS-Schlüsselrichtlinien für bestehende Trails hinzuzufügen.

Der `aws:SourceAccount`-Bedingungsschlüssel wird ebenfalls unterstützt, aber nicht empfohlen. Der Wert von `aws:SourceAccount` ist die Konto-ID des Trail-Besitzers oder die Verwaltungskonto-ID für Organisations-Trails.

#### Important

Ändern Sie beim Hinzufügen der neuen Abschnitte zur KMS-Schlüsselrichtlinie keinen der vorhandenen Abschnitte.

Wenn die Verschlüsselung für einen Trail aktiviert und der KMS-Schlüssel deaktiviert ist oder die KMS-Schlüsselrichtlinie nicht richtig konfiguriert ist CloudTrail, CloudTrail können keine Protokolle übermittelt werden.

Für Ereignisdatenspeicher erforderliche Elemente der KMS-Schlüsselrichtlinie

1. Aktivieren CloudTrail Sie die Berechtigungen zum Verschlüsseln von Protokollen. Siehe [Gewähren von Verschlüsselungsberechtigungen](#).
2. Aktivieren CloudTrail Sie die Berechtigungen zum Entschlüsseln von Protokollen. Siehe [Gewähren von Entschlüsselungsberechtigungen](#).
3. Erteilen Sie Benutzern und Rollen die Berechtigung zum Ver- und Entschlüsseln von Daten aus einem Ereignisdatenspeicher mit dem KMS-Schlüssel.

Wenn Sie einen Ereignisdatenspeicher erstellen und ihn mit einem KMS-Schlüssel verschlüsseln oder Abfragen in einem Ereignisdatenspeicher ausführen, den Sie mit einem KMS-Schlüssel verschlüsseln, benötigen Sie Schreibzugriff auf den KMS-Schlüssel. Die KMS-Schlüsselrichtlinie muss Zugriff auf den Ereignisdatenspeicher haben CloudTrail, und der KMS-Schlüssel sollte von Benutzern verwaltet werden können, die Operationen (z. B. Abfragen) im Ereignisdatenspeicher ausführen.

4. Aktivieren Sie CloudTrail diese Option, um KMS-Schlüsseleigenschaften zu beschreiben. Siehe [Aktivieren Sie CloudTrail diese Option, um KMS-Schlüsseleigenschaften zu beschreiben](#).

Die Bedingungsschlüssel `aws:SourceArn` und `aws:SourceAccount` werden in KMS-Schlüsselrichtlinien für Ereignisdatenspeicher nicht unterstützt.

**⚠ Important**

Ändern Sie beim Hinzufügen der neuen Abschnitte zur KMS-Schlüsselrichtlinie keinen der vorhandenen Abschnitte.

Wenn die Verschlüsselung in einem Ereignisdatenspeicher aktiviert ist und der KMS-Schlüssel deaktiviert oder gelöscht ist oder die KMS-Schlüsselrichtlinie nicht richtig konfiguriert ist CloudTrail, CloudTrail können keine Ereignisse an Ihren Ereignisdatenspeicher übermittelt werden.



## Gewähren von Verschlüsselungsberechtigungen

Example Erlauben CloudTrail Sie die Verschlüsselung von Protokollen für bestimmte Konten

CloudTrail benötigt die ausdrückliche Genehmigung, den KMS-Schlüssel zum Verschlüsseln von Protokollen für bestimmte Konten zu verwenden. Um ein Konto anzugeben, fügen Sie der KMS-Schlüsselrichtlinie die folgende erforderliche Anweisung hinzu und ersetzen Sie *account-id*, *region* und *trailName* durch die entsprechenden Werte für Ihre Konfiguration. Sie können dem EncryptionContext Abschnitt zusätzliche Konto-IDs hinzufügen, damit diese Konten Ihren KMS-Schlüssel CloudTrail zum Verschlüsseln von Protokolldateien verwenden können.

Fügen Sie der KMS-Schlüsselrichtlinie für einen Trail als bewährte Sicherheitsmethode den Bedingungsschlüssel `aws:SourceArn` hinzu. Mit dem globalen IAM-Bedingungsschlüssel wird `aws:SourceArn` sichergestellt, dass der KMS-Schlüssel nur für einen oder mehrere bestimmte Pfade CloudTrail verwendet wird.

```
{
  "Sid": "Allow CloudTrail to encrypt logs",
  "Effect": "Allow",
  "Principal": {
    "Service": "cloudtrail.amazonaws.com"
  },
  "Action": "kms:GenerateDataKey*",
  "Resource": "*",
  "Condition": {
    "StringEquals": {
      "aws:SourceArn": "arn:aws:cloudtrail:region:account-id:trail/trail-name"
    },
    "StringLike": {
      "kms:EncryptionContext:aws:cloudtrail:arn": "arn:aws:cloudtrail:*:account-id:trail/*"
    }
  }
}
```

Eine Richtlinie für einen KMS-Schlüssel, der zur Verschlüsselung von CloudTrail Lake-Ereignisdatenspeicherprotokollen verwendet wird, kann die Bedingungsschlüssel `aws:SourceArn` oder nicht verwenden. `aws:SourceAccount` Im Folgenden finden Sie ein Beispiel für eine KMS-Schlüsselrichtlinie für einen Ereignisdatenspeicher.

```
{
```

```
"Sid": "Allow CloudTrail to encrypt event data store",
"Effect": "Allow",
"Principal": {
  "Service": "cloudtrail.amazonaws.com"
},
"Action": [
  "kms:GenerateDataKey",
  "kms:Decrypt"
],
"Resource": "*"
}
```

## Example

Das folgende Beispiel für eine Richtlinienanweisung veranschaulicht, wie ein anderes Konto Ihren KMS-Schlüssel zum Verschlüsseln CloudTrail von Protokollen verwenden kann.

## Szenario

- Ihr KMS-Schlüssel befindet sich im Konto **111111111111**.
- Sowohl Sie als auch das Konto **222222222222** verschlüsseln Protokolle.

In der Richtlinie fügen Sie ein oder mehrere Konten hinzu, die mit Ihrem Schlüssel verschlüsseln. CloudTrail EncryptionContext Dies beschränkt die CloudTrail Verwendung Ihres Schlüssels zum Verschlüsseln von Protokollen nur für die von Ihnen angegebenen Konten. Wenn Sie dem Stamm des Kontos **222222222222** die Berechtigung zur Protokollverschlüsselung erteilen, wird die Berechtigung an den Kontoverwalter delegiert, die erforderlichen Berechtigungen für andere Benutzer dieses Kontos zu verschlüsseln. Dies geschieht, indem der Kontoadministrator die diesen IAM-Benutzern zugeordneten Richtlinien ändert.

Als bewährte Sicherheitsmethode gilt es, der KMS-Schlüsselrichtlinie einen `aws:SourceArn`-Bedingungsschlüssel hinzuzufügen. Mit dem globalen IAM-Bedingungsschlüssel wird `aws:SourceArn` sichergestellt, dass der KMS-Schlüssel nur für die angegebenen Pfade CloudTrail verwendet wird. Diese Bedingung wird in KMS-Schlüsselrichtlinien für Ereignisdatenspeicher nicht unterstützt.

## KMS-Schlüsselrichtlinie:

```
{
  "Sid": "Enable CloudTrail encrypt permissions",
```

```

"Effect": "Allow",
"Principal": {
  "Service": "cloudtrail.amazonaws.com"
},
"Action": "kms:GenerateDataKey*",
"Resource": "*",
"Condition": {
  "StringLike": {
    "kms:EncryptionContext:aws:cloudtrail:arn": [
      "arn:aws:cloudtrail:*:111111111111:trail/*",
      "arn:aws:cloudtrail:*:222222222222:trail/*"
    ]
  },
  "StringEquals": {
    "aws:SourceArn": "arn:aws:cloudtrail:region:account-id:trail/trail-name"
  }
}
}

```

Weitere Informationen zum Bearbeiten einer KMS-Schlüsselrichtlinie zur Verwendung mit CloudTrail finden Sie unter [Bearbeiten einer Schlüsselrichtlinie](#) im AWS Key Management Service Entwicklerhandbuch.

## Gewähren von Entschlüsselungsberechtigungen

Bevor Sie Ihren KMS-Schlüssel zu Ihrer CloudTrail Konfiguration hinzufügen, ist es wichtig, allen Benutzern, die diese benötigen, Entschlüsselungsberechtigungen zu erteilen. Benutzer, die zwar über Verschlüsselungs-, aber nicht über Entschlüsselungsberechtigungen verfügen, können verschlüsselte Protokolle nicht lesen. Wenn Sie einen vorhandenen S3-Bucket mit einem [S3-Bucket-Schlüssel](#) verwenden, sind `kms:Decrypt`-Berechtigungen erforderlich, um einen Trail mit aktivierter SSE-KMS-Verschlüsselung zu erstellen oder zu aktualisieren.

Aktivieren Sie die Berechtigungen zum Entschlüsseln von CloudTrail Protokollen

Benutzern Ihres Schlüssels müssen ausdrückliche Rechte zum Lesen der verschlüsselten Protokolldateien CloudTrail erteilt werden. Damit Benutzer verschlüsselte Protokolle lesen können, fügen Sie der KMS-Schlüsselrichtlinie die folgenden erforderlichen Anweisungen hinzu und fügen Sie dazu dem Abschnitt `Principal` für jeden Prinzipal, der zur Entschlüsselung mithilfe Ihres KMS-Schlüssel berechtigt sein soll, eine Zeile hinzu.

```

{
  "Sid": "Enable CloudTrail log decrypt permissions",

```

```

"Effect": "Allow",
"Principal": {
  "AWS": "arn:aws:iam::account-id:user/username"
},
"Action": "kms:Decrypt",
"Resource": "*",
"Condition": {
  "Null": {
    "kms:EncryptionContext:aws:cloudtrail:arn": "false"
  }
}
}
}

```

Im Folgenden finden Sie ein Beispiel für eine Richtlinie, die erforderlich ist, damit der CloudTrail Dienstprinzipal Trail-Logs entschlüsseln kann.

```

{
  "Sid": "Allow CloudTrail to decrypt a trail",
  "Effect": "Allow",
  "Principal": {
    "Service": "cloudtrail.amazonaws.com"
  },
  "Action": "kms:Decrypt",
  "Resource": "*"
}

```

Eine Entschlüsselungsrichtlinie für einen KMS-Schlüssel, der mit einem CloudTrail Lake-Ereignisdatenspeicher verwendet wird, ähnelt der folgenden. Die als Werte für `Principal` angegebenen Benutzer- oder Rollen-ARNs benötigen Entschlüsselungsberechtigungen, um Ereignisdatenspeicher erstellen oder aktualisieren, Abfragen ausführen oder Abfrageergebnisse abrufen zu können.

```

{
  "Sid": "Enable user key permissions for event data stores"
  "Effect": "Allow",
  "Principal": {
    "AWS": "arn:aws:iam::account-id:user/username"
  },
  "Action": [
    "kms:Decrypt",
    "kms:GenerateDataKey"
  ],
}

```

```
"Resource": "*"
}
```

Im Folgenden finden Sie ein Beispiel für eine Richtlinie, die erforderlich ist, damit der CloudTrail Dienstprinzipal die Protokolle des Ereignisdatenspeichers entschlüsseln kann.

```
{
  "Sid": "Allow CloudTrail to decrypt an event data store",
  "Effect": "Allow",
  "Principal": {
    "Service": "cloudtrail.amazonaws.com"
  },
  "Action": "kms:Decrypt",
  "Resource": "*"
}
```

Zulassen, dass Benutzer in Ihrem Konto Trail-Protokolle mit Ihrem KMS-Schlüssel entschlüsseln

### Beispiel

Diese Richtlinienanweisung zeigt, wie Sie es einem Benutzer oder einer Rolle in Ihrem Konto ermöglichen, Ihren Schlüssel zu verwenden, um verschlüsselte Protokolle im S3-Bucket Ihres Kontos zu lesen.

### Example Szenario

- Ihr KMS-Schlüssel, der S3-Bucket und der IAM-Benutzer Bob befinden sich im Konto **111111111111**.
- Sie erteilen dem IAM-Benutzer Bob die Erlaubnis, CloudTrail Logs im S3-Bucket zu entschlüsseln.

In der Schlüsselrichtlinie aktivieren Sie die Berechtigungen zur CloudTrail Protokollentschlüsselung für den IAM-Benutzer Bob.

### KMS-Schlüsselrichtlinie:

```
{
  "Sid": "Enable CloudTrail log decrypt permissions",
  "Effect": "Allow",
  "Principal": {
    "AWS": "arn:aws:iam::111111111111:user/Bob"
  },
}
```

```
"Action": "kms:Decrypt",
"Resource": "arn:aws:kms:region:account-id:key/key-id",
"Condition": {
  "Null": {
    "kms:EncryptionContext:aws:cloudtrail:arn": "false"
  }
}
}
```

Zulassen, dass Benutzer in anderen Konten Trail-Protokolle mit Ihrem KMS-Schlüssel entschlüsseln

Sie können Benutzern in anderen Konten erlauben, mit Ihrem KMS-Schlüssel Trail-Protokolle zu entschlüsseln, aber keine Protokolle für Ereignisdatenspeicher. Die erforderlichen Änderungen an der Schlüsselrichtlinie sind abhängig davon, ob der S3-Bucket sich in Ihrem Konto oder in einem anderen Konto befindet.

Zulassen der Entschlüsselung von Protokollen für Benutzer eines Buckets in einem anderen Konto

### Beispiel

Diese Richtlinienanweisung zeigt, wie Sie einem IAM-Benutzer oder einer IAM-Rolle in einem anderen Konto ermöglichen, Ihren Schlüssel zu verwenden, um verschlüsselte Protokolle aus einem S3-Bucket in dem anderen Konto zu lesen.

### Szenario

- Ihr KMS-Schlüssel befindet sich im Konto **111111111111**.
- Der IAM-Benutzer Alice und der S3-Bucket befinden sich im Konto **222222222222**.

In diesem Fall erteilen Sie unter dem Konto **222222222222** die CloudTrail Erlaubnis zum Entschlüsseln von Protokollen und Sie erteilen Alice in der IAM-Benutzerrichtlinie die Erlaubnis, Ihren Schlüssel zu verwenden **KeyA**, der sich im Konto befindet. **111111111111**

KMS-Schlüsselrichtlinie:

```
{
  "Sid": "Enable encrypted CloudTrail log read access",
  "Effect": "Allow",
  "Principal": {
    "AWS": [
      "arn:aws:iam::222222222222:root"
    ]
  }
}
```

```

},
"Action": "kms:Decrypt",
"Resource": "arn:aws:kms:region:account-id:key/key-id",
"Condition": {
  "Null": {
    "kms:EncryptionContext:aws:cloudtrail:arn": "false"
  }
}
}
}

```

Anweisung in der IAM-Benutzerrichtlinie von Alice:

```

{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Action": "kms:Decrypt",
      "Resource": "arn:aws:kms:us-west-2:111111111111:key/KeyA"
    }
  ]
}

```

Zulassen, dass Benutzer in einem anderen Konto Trail-Protokolle aus Ihrem Bucket entschlüsseln

### Example

Diese Richtlinie zeigt, wie ein anderes Konto Ihren Schlüssel verwenden kann, um verschlüsselte Protokolle aus Ihrem S3-Bucket zu lesen.

### Example Szenario

- Ihr KMS-Schlüssel und S3-Bucket befinden sich in Konto *111111111111*.
- Der Benutzer, der Protokolle aus Ihrem Bucket liest, befindet sich in Konto *222222222222*.

Um dieses Szenario zu aktivieren, aktivieren Sie die Entschlüsselungsberechtigungen für die IAM-Rolle CloudTrailReadRole in Ihrem Konto und geben dann dem anderen Konto die Erlaubnis, diese Rolle anzunehmen.

KMS-Schlüsselrichtlinie:

```
{
```

```

"Sid": "Enable encrypted CloudTrail log read access",
"Effect": "Allow",
"Principal": {
  "AWS": [
    "arn:aws:iam::111111111111:role/CloudTrailReadRole"
  ]
},
"Action": "kms:Decrypt",
"Resource": "arn:aws:kms:region:account-id:key/key-id",
"Condition": {
  "Null": {
    "kms:EncryptionContext:aws:cloudtrail:arn": "false"
  }
}
}

```

CloudTrailReadRoleGrundsatzerklärung zur Vertrauensstelle:

```

{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Sid": "Allow CloudTrail access",
      "Effect": "Allow",
      "Principal": {
        "AWS": "arn:aws:iam::222222222222:root"
      },
      "Action": "sts:AssumeRole"
    }
  ]
}

```

Informationen zum Bearbeiten einer KMS-Schlüsselrichtlinie zur Verwendung mit CloudTrail finden Sie unter [Bearbeiten einer Schlüsselrichtlinie](#) im AWS Key Management Service Entwicklerhandbuch.

Aktivieren Sie CloudTrail diese Option, um KMS-Schlüsseleigenschaften zu beschreiben

CloudTrail erfordert die Fähigkeit, die Eigenschaften des KMS-Schlüssels zu beschreiben. Um diese Funktion zu aktivieren, fügen Sie der KMS-Schlüssel-Richtlinie die folgende erforderliche Anweisung hinzu. Diese Anweisung gewährt CloudTrail keine Berechtigungen, die über die anderen von Ihnen angegebenen Berechtigungen hinausgehen.



Als bewährte Sicherheitsmethode gilt es, der KMS-Schlüsselrichtlinie einen `aws:SourceArn`-Bedingungsschlüssel hinzuzufügen. Mit dem globalen IAM-Bedingungsschlüssel wird `aws:SourceArn` sichergestellt, dass der KMS-Schlüssel nur für einen oder mehrere bestimmte Pfade CloudTrail verwendet wird.

```
{
  "Sid": "Allow CloudTrail access",
  "Effect": "Allow",
  "Principal": {
    "Service": "cloudtrail.amazonaws.com"
  },
  "Action": "kms:DescribeKey",
  "Resource": "arn:aws:kms:region:account-id:key/key-id",
  "Condition": {
    "StringEquals": {
      "aws:SourceArn": "arn:aws:cloudtrail:region:account-id:trail/trail-name"
    }
  }
}
```

Weitere Informationen zum Bearbeiten von KMS-Schlüsselrichtlinien finden Sie unter [Bearbeiten einer Schlüsselrichtlinie](#) im AWS Key Management Service -Entwicklerhandbuch.

## In CloudTrail der Konsole erstellte Standard-KMS-Schlüsselrichtlinie

Wenn Sie eine AWS KMS key in der CloudTrail Konsole erstellen, werden die folgenden Richtlinien automatisch für Sie erstellt. Die Richtlinie gewährt die folgenden Berechtigungen:

- Erlaubt AWS-Konto (Root-) Berechtigungen für den KMS-Schlüssel.
- Ermöglicht CloudTrail die Verschlüsselung von Protokolldateien unter dem KMS-Schlüssel und die Beschreibung des KMS-Schlüssels.
- Ermöglicht allen Benutzern in dem angegebenen Konto das Entschlüsseln von Protokolldateien.
- Ermöglicht allen Benutzern in dem angegebenen Konto das Erstellen eines KMS-Alias für den KMS-Schlüssel.
- Aktiviert die kontoübergreifende Protokollentschlüsselung für die Konto-ID des Kontos, das den Trail erstellt hat.

## Themen

- [Standardmäßige KMS-Schlüsselrichtlinie für CloudTrail Lake-Ereignisdatenspeicher](#)

- [Standardmäßige KMS-Schlüsselrichtlinie für Trails](#)

## Standardmäßige KMS-Schlüsselrichtlinie für CloudTrail Lake-Ereignisdatenspeicher

Im Folgenden finden Sie die Standardrichtlinie, die für eine erstellt wurde AWS KMS key , die Sie mit einem Ereignisdatenspeicher in CloudTrail Lake verwenden.

```
{
  "Version": "2012-10-17",
  "Id": "Key policy created by CloudTrail",
  "Statement": [
    {
      "Sid": "The key created by CloudTrail to encrypt event data stores. Created
${new Date().toUTCString()}",
      "Effect": "Allow",
      "Principal": {
        "Service": "cloudtrail.amazonaws.com"
      },
      "Action": [
        "kms:GenerateDataKey",
        "kms:Decrypt"
      ],
      "Resource": "*"
    },
    {
      "Sid": "Enable IAM user permissions",
      "Effect": "Allow",
      "Principal": {
        "AWS": "arn:aws:iam::account-id:root"
      },
      "Action": "kms:*",
      "Resource": "*"
    },
    {
      "Sid": "Enable user to have permissions",
      "Effect": "Allow",
      "Principal": {
        "AWS" : "arn:aws:sts::account-id:role-arn"
      },
      "Action": [
        "kms:Decrypt",
        "kms:GenerateDataKey"
      ],
    }
  ]
}
```

```

    "Resource": "*"
  }
]
}

```

## Standardmäßige KMS-Schlüsselrichtlinie für Trails

Die folgende Standardrichtlinie wurde für eine erstellt AWS KMS key , die Sie mit einem Trail verwenden.

### Note

Die Richtlinie enthält eine Anweisung, die die kontoübergreifende Entschlüsselung von Dateien mit dem KMS-Schlüssel erlaubt.

```

{
  "Version": "2012-10-17",
  "Id": "Key policy created by CloudTrail",
  "Statement": [
    {
      "Sid": "Enable IAM user permissions",
      "Effect": "Allow",
      "Principal": {
        "AWS": [
          "arn:aws:iam::account-id:root",
          "arn:aws:iam::account-id:user/username"
        ]
      },
      "Action": "kms:*",
      "Resource": "*"
    },
    {
      "Sid": "Allow CloudTrail to encrypt logs",
      "Effect": "Allow",
      "Principal": {
        "Service": "cloudtrail.amazonaws.com"
      },
      "Action": "kms:GenerateDataKey*",
      "Resource": "*",
      "Condition": {
        "StringEquals": {

```

```

        "aws:SourceArn": "arn:aws:cloudtrail:region:account-id:trail/trail-
name"
    },
    "StringLike": {
        "kms:EncryptionContext:aws:cloudtrail:arn":
"arn:aws:cloudtrail:*:account-id:trail/*"
    }
},
{
    "Sid": "Allow CloudTrail to describe key",
    "Effect": "Allow",
    "Principal": {
        "Service": "cloudtrail.amazonaws.com"
    },
    "Action": "kms:DescribeKey",
    "Resource": "*"
},
{
    "Sid": "Allow principals in the account to decrypt log files",
    "Effect": "Allow",
    "Principal": {
        "AWS": "*"
    },
    "Action": [
        "kms:Decrypt",
        "kms:ReEncryptFrom"
    ],
    "Resource": "*",
    "Condition": {
        "StringEquals": {
            "kms:CallerAccount": "account-id"
        },
        "StringLike": {
            "kms:EncryptionContext:aws:cloudtrail:arn":
"arn:aws:cloudtrail:*:account-id:trail/*"
        }
    }
},
{
    "Sid": "Allow alias creation during setup",
    "Effect": "Allow",
    "Principal": {
        "AWS": "*"
    }
}

```

```

    },
    "Action": "kms:CreateAlias",
    "Resource": "arn:aws:kms:region:account-id:key/key-id",
    "Condition": {
      "StringEquals": {
        "kms:ViaService": "ec2.region.amazonaws.com",
        "kms:CallerAccount": "account-id"
      }
    }
  },
  {
    "Sid": "Enable cross account log decryption",
    "Effect": "Allow",
    "Principal": {
      "AWS": "*"
    },
    "Action": [
      "kms:Decrypt",
      "kms:ReEncryptFrom"
    ],
    "Resource": "*",
    "Condition": {
      "StringEquals": {
        "kms:CallerAccount": "account-id"
      },
      "StringLike": {
        "kms:EncryptionContext:aws:cloudtrail:arn":
"arn:aws:cloudtrail:*:account-id:trail/*"
      }
    }
  }
]
}

```

## Aktualisieren einer Ressource zur Verwendung des KMS-Schlüssels

Aktualisieren Sie in der AWS CloudTrail Konsole einen Trail- oder Ereignisdatenspeicher, um einen AWS Key Management Service Schlüssel zu verwenden. Beachten Sie, dass die Verwendung Ihres eigenen KMS-Schlüssels AWS KMS Kosten für die Verschlüsselung und Entschlüsselung verursacht. Weitere Informationen finden Sie unter [AWS Key Management Service -Preisgestaltung](#).

### Themen

- [Aktualisieren eines Trails zur Verwendung eines KMS-Schlüssels](#)
- [Aktualisieren eines Ereignisdatenspeichers zur Verwendung eines KMS-Schlüssels](#)

## Aktualisieren eines Trails zur Verwendung eines KMS-Schlüssels

Führen Sie die folgenden Schritte in der Konsole aus AWS KMS key , um einen Trail zu aktualisieren, sodass er den Pfad verwendet CloudTrail, für den Sie ihn geändert haben. CloudTrail

### Note

Das Aktualisieren eines Trails mit dem folgenden Verfahren verschlüsselt die Protokolldateien, aber nicht die Digest-Dateien mit SSE-KMS. Digest-Dateien werden mit [S3-verwalteten Verschlüsselungsschlüsseln \(SSE-S3\) von Amazon](#) verschlüsselt. Wenn Sie einen vorhandenen S3-Bucket mit einem [S3-Bucket-Schlüssel](#) verwenden, CloudTrail müssen Sie in der Schlüsselrichtlinie über die entsprechende Berechtigung verfügen, um die AWS KMS Aktionen GenerateDataKey und verwenden zu könnenDescribeKey. Wenn `cloudtrail.amazonaws.com` diese Berechtigungen in der Schlüsselrichtlinie nicht gewährt werden, können Sie keinen Trail erstellen oder aktualisieren.


Informationen zum Aktualisieren eines Trails mithilfe von finden Sie unter [Aktivieren und Deaktivieren der CloudTrail Protokolldateiverschlüsselung mit dem AWS CLI](#). AWS CLI

So aktualisieren Sie einen Trail zur Verwendung des KMS-Schlüssel

1. Melden Sie sich unter <https://console.aws.amazon.com/cloudtrail/> bei der an AWS Management Console und öffnen Sie die CloudTrail Konsole.
2. Wählen Sie Trails und anschließend einen Trail-Namen.
3. Wählen Sie unter Allgemeine Details Bearbeiten aus.
4. Wählen Sie unter Log file SSE-KMS encryption (SSE-KMS-Verschlüsselung der Protokolldatei) die Option Enabled (Aktiviert) aus, wenn Sie Ihre Protokolldateien mit der SSE-KMS-Verschlüsselung anstelle der SSE-S3-Verschlüsselung verschlüsseln möchten. Der Standard ist aktiviert. Wenn Sie die SSE-KMS-Verschlüsselung nicht aktivieren, werden die Protokolle mit der SSE-S3-Verschlüsselung verschlüsselt. Weitere Informationen zur SSE-KMS-Verschlüsselung finden Sie unter [Verwenden der serverseitigen Verschlüsselung mit AWS Key Management Service \(SSE-KMS\)](#). Weitere Informationen zur SSE-S3-Verschlüsselung

finden Sie unter [Verwenden der serverseitigen Verschlüsselung mit von Amazon S3 verwalteten Verschlüsselungsschlüsseln \(SSE-S3\)](#).

Wählen Sie Vorhanden, um Ihren Trail mit Ihrem AWS KMS key zu aktualisieren. Wählen Sie einen KMS-Schlüssel aus, der sich in derselben Region befindet wie der S3-Bucket, der Ihre Protokolldateien empfängt. Zum Überprüfen der Region für einen S3-Bucket sehen Sie sich die entsprechenden Eigenschaften in der S3-Konsole an.

 Note

Sie können auch den ARN eines Schlüssels aus einem anderen Konto eingeben. Weitere Informationen finden Sie unter [Aktualisieren einer Ressource zur Verwendung des KMS-Schlüssels](#). Die Schlüsselrichtlinie muss die Verwendung des Schlüssels CloudTrail zum Verschlüsseln Ihrer Protokolldateien ermöglichen und den von Ihnen angegebenen Benutzern das Lesen von Protokolldateien in unverschlüsselter Form ermöglichen. Informationen zur manuellen Bearbeitung der Schlüsselrichtlinie finden Sie unter [Konfigurieren Sie AWS KMS wichtige Richtlinien für CloudTrail](#).

Geben Sie im Feld AWS KMS Alias den Alias, für den Sie die Richtlinie zur Verwendung mit geändert haben CloudTrail, im folgenden Format an. `alias/MyAliasName` Weitere Informationen finden Sie unter [Aktualisieren einer Ressource zur Verwendung des KMS-Schlüssels](#).

Sie können den Aliasnamen, ARN oder die global eindeutige Schlüssel-ID angeben. Wenn der KMS-Schlüssel zu einem anderen Konto gehört, stellen Sie sicher, dass die Schlüsselrichtlinie über entsprechende Berechtigungen verfügt, damit Sie sie verwenden können. Der Wert kann in einem der folgenden Formate angegeben sein:

- Aliasname: `alias/MyAliasName`
- Alias-ARN: `arn:aws:kms:region:123456789012:alias/MyAliasName`
- Schlüssel-ARN:  
`arn:aws:kms:region:123456789012:key/12345678-1234-1234-1234-123456789012`
- Global eindeutige Schlüssel-ID: `12345678-1234-1234-1234-123456789012`

5. Wählen Sie Trail aktualisieren aus.


 Note

Wenn der KMS-Schlüssel, den Sie ausgewählt haben, deaktiviert ist oder gelöscht werden soll, können Sie den Trail mit diesem KMS-Schlüssel nicht speichern. Sie können den KMS-Schlüssel aktivieren oder einen anderen auswählen. Weitere Informationen finden Sie unter [Schlüsselzustand: Auswirkung auf Ihren KMS-Schlüssel](#) im AWS Key Management Service -Entwicklerhandbuch.

## Aktualisieren eines Ereignisdatenspeichers zur Verwendung eines KMS-Schlüssels

Um einen Ereignisdatenspeicher so zu aktualisieren, AWS KMS key dass er den, für den Sie geändert haben CloudTrail, verwendet, führen Sie die folgenden Schritte in der CloudTrail Konsole aus.

Informationen zum Aktualisieren eines Ereignisdatenspeichers mithilfe von finden Sie unter [Aktualisieren Sie einen Ereignisdatenspeicher mit dem AWS CLI](#). AWS CLI

 Important

Durch das Deaktivieren oder Löschen des KMS-Schlüssels oder das Entfernen von CloudTrail Berechtigungen für den Schlüssel wird CloudTrail verhindert, dass Ereignisse in den Ereignisdatenspeicher aufgenommen werden, und verhindert, dass Benutzer Daten im Ereignisdatenspeicher abfragen, die mit dem Schlüssel verschlüsselt wurden. Nachdem Sie einen KMS-Schlüssel einem Ereignisdatenspeicher zugeordnet haben, kann der KMS-Schlüssel nicht entfernt oder geändert werden. Bevor Sie einen KMS-Schlüssel, den Sie bei einem Ereignisdatenspeicher verwenden, deaktivieren oder löschen, sollten Sie den Ereignisdatenspeicher löschen oder sichern.

So aktualisieren Sie einen Ereignisdatenspeicher zur Verwendung Ihres KMS-Schlüssels

1. [Melden Sie sich bei der an AWS Management Console und öffnen Sie die CloudTrail Konsole unter `https://console.aws.amazon.com/cloudtrail/`.](#)
2. Wählen Sie im linken Navigationsbereich Event data stores (Ereignisdatenspeicher) in Lake aus. Wählen Sie einen zu aktualisierenden Ereignisdatenspeicher aus.
3. Wählen Sie unter Allgemeine Details Bearbeiten aus.




4. Wählen Sie unter Verschlüsselung, sofern noch nicht aktiviert, die Option Meinen eigenen AWS KMS key verwenden aus, um die Protokolldateien mit Ihrem eigenen KMS-Schlüssel zu verschlüsseln.

Wählen Sie Existing (Bestehende) aus, um den Ereignisdatenspeicher mit Ihrem KMS-Schlüssel zu aktualisieren. Wählen Sie einen KMS-Schlüssel aus, der sich in derselben Region befindet wie der Ereignisdatenspeicher. Schlüssel aus anderen Konten werden nicht unterstützt.

Geben Sie unter AWS KMS Alias eingeben den Alias, für den Sie die Richtlinie zur Verwendung mit geändert haben CloudTrail, im folgenden Format an `alias/MyAliasName`. Weitere Informationen finden Sie unter [Aktualisieren einer Ressource zur Verwendung des KMS-Schlüssels](#).

Sie können einen Alias auswählen oder die global eindeutige Schlüssel-ID verwenden. Der Wert kann in einem der folgenden Formate angegeben sein:

- Aliasname: `alias/MyAliasName`
  - Alias-ARN: `arn:aws:kms:region:123456789012:alias/MyAliasName`
  - Schlüssel-ARN:  
`arn:aws:kms:region:123456789012:key/12345678-1234-1234-1234-123456789012`
  - Global eindeutige Schlüssel-ID: `12345678-1234-1234-1234-123456789012`
5. Wählen Sie Änderungen speichern.

 Note

Wenn der von Ihnen ausgewählte KMS-Schlüssel deaktiviert ist oder dessen Löschung ansteht, können Sie den Ereignisdatenspeicher mit diesem KMS-Schlüssel nicht speichern. Sie können den KMS-Schlüssel aktivieren oder einen anderen auswählen. Weitere Informationen finden Sie unter [Schlüsselzustand: Auswirkung auf Ihren KMS-Schlüssel](#) im AWS Key Management Service -Entwicklerhandbuch.

# Aktivieren und Deaktivieren der CloudTrail Protokolldateiverschlüsselung mit dem AWS CLI

In diesem Thema wird beschrieben, wie die SSE-KMS-Protokolldateiverschlüsselung für aktiviert und deaktiviert CloudTrail wird. AWS CLI Hintergrundinformationen dazu finden Sie unter [CloudTrail Logdateien mit AWS KMS Schlüsseln verschlüsseln \(SSE-KMS\)](#).

## Themen

- [Aktivieren der CloudTrail Protokolldateiverschlüsselung mit dem AWS CLI](#)
- [Deaktivierung der CloudTrail Protokolldateiverschlüsselung mithilfe von AWS CLI](#)

## Aktivieren der CloudTrail Protokolldateiverschlüsselung mit dem AWS CLI

- [Aktivieren der Protokolldateiverschlüsselung für einen Trail](#)
- [Aktivieren der Protokolldateiverschlüsselung für einen Ereignisdatenspeicher](#)

### Aktivieren der Protokolldateiverschlüsselung für einen Trail

1. Erstellen Sie einen Schlüssel mit der AWS CLI. Der Schlüssel, den Sie erstellen, muss sich in derselben Region befinden wie der S3-Bucket, der Ihre CloudTrail Protokolldateien empfängt. Für diesen Schritt verwenden Sie den AWS KMS [create-key](#) Befehl.
2. Rufen Sie die vorhandene Schlüsselrichtlinie ab, damit Sie sie für die Verwendung mit ändern können CloudTrail. Sie können die Schlüsselrichtlinie mit dem AWS KMS [get-key-policy](#) Befehl abrufen.
3. Fügen Sie der Schlüsselrichtlinie die erforderlichen Abschnitte hinzu, CloudTrail damit Ihre Protokolldateien verschlüsselt und Benutzer sie entschlüsseln können. Stellen Sie sicher, dass alle Benutzer, die die Protokolldateien lesen sollen, entsprechende Entschlüsselungsberechtigungen erhalten. Nehmen Sie keine Änderungen an bestehenden Abschnitten der Richtlinie vor. Weitere Informationen zu den einzubeziehenden Richtlinienabschnitten finden Sie unter [Konfigurieren Sie AWS KMS wichtige Richtlinien für CloudTrail](#).
4. Hängen Sie die geänderte JSON-Richtliniendatei mithilfe des Befehls an den AWS KMS [put-key-policy](#) Schlüssel an.

5. Führen Sie den `update-trail` Befehl CloudTrail `create-trail` oder mit dem `--kms-key-id` Parameter aus. Mit diesem Befehl wird die Protokollverschlüsselung aktiviert.

```
aws cloudtrail update-trail --name Default --kms-key-id alias/MyKmsKey
```

Der `--kms-key-id` Parameter gibt den Schlüssel an, für dessen Richtlinie Sie Änderungen vorgenommen haben CloudTrail. Die folgenden Formate sind möglich:

- Aliasname. Beispiel: `alias/MyAliasName`
- Alias-ARN. Beispiel: `arn:aws:kms:us-east-2:123456789012:alias/MyAliasName`
- Schlüssel-ARN. Beispiel: `arn:aws:kms:us-east-2:123456789012:key/12345678-1234-1234-1234-123456789012`
- Global eindeutige Schlüssel-ID. Beispiel: `12345678-1234-1234-1234-123456789012`

Nachfolgend finden Sie eine Beispielantwort:

```
{
  "IncludeGlobalServiceEvents": true,
  "Name": "Default",
  "TrailARN": "arn:aws:cloudtrail:us-east-2:123456789012:trail/Default",
  "LogFileValidationEnabled": false,
  "KmsKeyId": "arn:aws:kms:us-east-2:123456789012:key/12345678-1234-1234-1234-123456789012",
  "S3BucketName": "my-bucket-name"
}
```

Wenn das Element `KmsKeyId` vorhanden ist, bedeutet das, dass die Verschlüsselung der Protokolldateien aktiviert wurde. Die verschlüsselten Protokolldateien sollten nach etwa 5 Minuten in Ihrem Bucket angezeigt werden.

## Aktivieren der Protokolldateiverschlüsselung für einen Ereignisdatenspeicher

1. Erstellen Sie einen Schlüssel mit der AWS CLI. Der erstellte Schlüssel muss sich in derselben Region befinden wie der Ereignisdatenspeicher. Führen Sie für diesen Schritt den AWS KMS [create-key](#) Befehl aus.

2. Holen Sie sich die vorhandene Schlüsselrichtlinie, die Sie bearbeiten möchten, damit sie verwendet werden kann CloudTrail. Sie können die Schlüsselrichtlinie abrufen, indem Sie den AWS KMS [get-key-policy](#) Befehl ausführen.
3. Fügen Sie der Schlüsselrichtlinie die erforderlichen Abschnitte hinzu, CloudTrail damit Ihre Protokolldateien verschlüsselt und Benutzer sie entschlüsseln können. Stellen Sie sicher, dass alle Benutzer, die die Protokolldateien lesen sollen, entsprechende Entschlüsselungsberechtigungen erhalten. Nehmen Sie keine Änderungen an bestehenden Abschnitten der Richtlinie vor. Weitere Informationen zu den einzubeziehenden Richtlinienabschnitten finden Sie unter [Konfigurieren Sie AWS KMS wichtige Richtlinien für CloudTrail](#).
4. Hängen Sie die bearbeitete JSON-Richtliniendatei an den Schlüssel an, indem Sie den AWS KMS [put-key-policy](#) Befehl ausführen.
5. Führen Sie den `update-event-data-store` Befehl CloudTrail `create-event-data-store` oder `delete-event-data-store` aus und fügen Sie den `--kms-key-id` Parameter hinzu. Mit diesem Befehl wird die Protokollverschlüsselung aktiviert.

```
aws cloudtrail update-event-data-store --name my-event-data-store --kms-key-id  
alias/MyKmsKey
```

Der `--kms-key-id` Parameter gibt den Schlüssel an, für dessen Richtlinie Sie Änderungen vorgenommen haben CloudTrail. Die folgenden vier Formate sind möglich:

- Aliasname. Beispiel: `alias/MyAliasName`
- Alias-ARN. Beispiel: `arn:aws:kms:us-east-2:123456789012:alias/MyAliasName`
- Schlüssel-ARN. Beispiel: `arn:aws:kms:us-east-1:123456789012:key/12345678-1234-1234-1234-123456789012`
- Global eindeutige Schlüssel-ID. Beispiel: `12345678-1234-1234-1234-123456789012`

Nachfolgend finden Sie eine Beispielantwort:

```
{  
  "Name": "my-event-data-store",  
  "ARN": "arn:aws:cloudtrail:us-east-1:12345678910:eventdatastore/  
EXAMPLEf852-4e8f-8bd1-bcf6cEXAMPLE",  
  "RetentionPeriod": "90",  
  "KmsKeyId": "arn:aws:kms:us-  
east-1:123456789012:key/12345678-1234-1234-1234-123456789012"
```

```
"MultiRegionEnabled": false,
"OrganizationEnabled": false,
"TerminationProtectionEnabled": true,
"AdvancedEventSelectors": [{
  "Name": "Select all external events",
  "FieldSelectors": [{
    "Field": "eventCategory",
    "Equals": [
      "ActivityAuditLog"
    ]
  }]
}]
}
```

Wenn das Element `KmsKeyId` vorhanden ist, bedeutet das, dass die Verschlüsselung der Protokolldateien aktiviert wurde. Die verschlüsselten Protokolldateien sollten nach etwa 5 Minuten in Ihrem Ereignisdatenspeicher angezeigt werden.

## Deaktivierung der CloudTrail Protokolldateiverschlüsselung mithilfe von AWS CLI


Um die Verschlüsselung von Protokolldateien für einen Trail beenden, führen Sie `update-trail` aus und übergeben eine leere Zeichenfolge an den Parameter `kms-key-id`:

```
aws cloudtrail update-trail --name my-test-trail --kms-key-id ""
```

Nachfolgend finden Sie eine Beispielantwort:

```
{
  "IncludeGlobalServiceEvents": true,
  "Name": "Default",
  "TrailARN": "arn:aws:cloudtrail:us-east-2:123456789012:trail/Default",
  "LogFileValidationEnabled": false,
  "S3BucketName": "my-bucket-name"
}
```

Wenn der Wert `KmsKeyId` nicht vorhanden ist, bedeutet das, dass die Verschlüsselung der Protokolldateien deaktiviert wurde.

** Important**

Die Verschlüsselung von Protokolldateien in einem Ereignisdatenspeicher lässt sich nicht beenden.

# Dokumentverlauf

In der folgenden Tabelle werden die wichtigen Änderungen an der Dokumentation für AWS CloudTrail beschrieben. Um Benachrichtigungen über Aktualisierungen dieser Dokumentation zu erhalten, können Sie einen RSS-Feed abonnieren.

- API-Version: 2013-11-01
- Letzte Aktualisierung der Dokumentation: 2024-05-30

Änderung	Beschreibung	Datum
<a href="#">Aktualisierte Dokumentation</a>	Es wurde ein Abschnitt hinzugefügt, der beschreibt, wie Datenereignisse mithilfe erweiterter Event-Selektoren gefiltert werden. Weitere Informationen finden Sie unter <a href="#">Filtern von Datenereignissen mithilfe erweiterter Ereignis selektoren</a> .	29. Mai 2024
<a href="#">Hinzugefügte Funktionalität</a>	Sie können jetzt CloudTrail Datenereignisse in Amazon Kinesis Data Streams und Stream-Verbrauchern protokollieren, indem Sie erweiterte Event-Selektoren verwenden . Weitere Informationen finden Sie unter <a href="#">Datenereignisse</a> .	21. Mai 2024
<a href="#">Aktualisierte Dokumentation</a>	Die Seite mit den <a href="#">vom CloudTrail See unterstützten Regionen</a> wurde aktualisiert und die Region Asien-Pazifik (Hyderabad) (ap-south-2), die Region Europa (Zürich)	16. Mai 2024

(eu-central-2) und die Region Israel (Tel Aviv) (il-central-1) hinzugefügt.

### Hinzugefügte Funktionalität

Sie können jetzt CloudTrail Datenereignisse auf AWS Step Functions Zustandsmaschinen protokollieren, indem Sie erweiterte Event-Selektoren verwenden. Weitere Informationen finden Sie unter [Datenereignisse](#).

16. Mai 2024

### Aktualisierte Dokumentation

Es wurde ein Abschnitt über die CloudTrail Kosten der Anzeige und die Nutzung hinzugefügt AWS Cost Explorer. Weitere Informationen finden Sie unter [CloudTrail Kosten und Nutzung anzeigen mit AWS Cost Explorer](#).

14. Mai 2024

### Hinzugefügte Funktionalität

Sie können jetzt CloudTrail Datenereignisse in Amazon Q Apps mithilfe erweiterter Event-Selektoren protokollieren. Weitere Informationen finden Sie unter [Datenereignisse](#).

1. Mai 2024



## [Aktualisierte Dokumentation](#)

Allgemeine organisatorische Verbesserungen an den Abschnitten und Seitentiteln des Benutzerhandbuchs, darunter Folgendes: Der Titel der Referenzseite für CloudTrail Protokollereignisse wurde in „[CloudTrail Ereignisse verstehen](#)“ geändert und es wurden Beschreibungen von Verwaltungsereignissen, Datenereignissen und Insights-Ereignissen hinzugefügt. Der Titel der Seite „Einstellungen“ wurde in „[CloudTrail Einstellungen konfigurieren](#)“ geändert. Die Seiten „[Datenereignisse protokollieren](#)“, „[Verwaltungsereignisse protokollieren](#)“ und „[Logging Insights-Ereignisse](#)“ wurden in den Abschnitt „CloudTrail Ereignisse protokollieren“ verschoben. Die Seite mit den [Beispielen für CloudTrail Protokolldateien](#) wurde in den Bereich [CloudTrail Protokolldateien](#) verschoben. Es wurden separate Seiten hinzugefügt, um die AWS CLI Befehle für CloudTrail [Lake-Ereignisdatspeicher](#), [Abfragen](#) und [Integrationen](#) aufzulisten.

10. April 2024

---

<a href="#">Aktualisierte Dokumentation</a>	Die Seite mit den <a href="#">vom CloudTrail See unterstützten Regionen</a> wurde aktualisiert und die Region Europa (Spanien) (eu-south-2) hinzugefügt.	10. April 2024
<a href="#">Zusätzlicher Service-Support</a>	Diese Version unterstützt AWS Control Catalog. Weitere Informationen finden Sie in den <a href="#">AWS-Service Themen CloudTrail</a> und <a href="#">Protokollierung von AWS Control Catalog-API-Aufrufen mithilfe von AWS CloudTrail</a> .	8. April 2024
<a href="#">Zusätzlicher Service-Support</a>	Diese Version unterstützt AWS Deadline Cloud. Weitere Informationen finden Sie in den <a href="#">AWS-Service Themen für CloudTrail</a> .	2. April 2024
<a href="#">Hinzugefügte Funktionalität</a>	Die AWS CloudTrail Event-Version ist jetzt 1.10. Weitere Informationen finden Sie unter <a href="#">Inhalt des CloudTrail Datensatzes</a> .	26. März 2024
<a href="#">Zusätzlicher Service-Support</a>	Diese Version unterstützt AWS Billing Conductor. Weitere Informationen finden Sie in den <a href="#">AWS-Service Themen CloudTrail</a> und <a href="#">Protokollierung von AWS Billing Conductor API-Aufrufen mithilfe von AWS CloudTrail</a> .	12. März 2024

Hinzugefügte Funktionalität

Sie können jetzt CloudTrail  
I Datenereignisse auf AWS  
X-Ray Traces und AWS  
Systems Manager verwaltet  
en Knoten protokollieren,  
indem Sie erweiterte Event-Selektoren verwenden. Weitere Informationen finden Sie unter [Datenereignisse](#).

7. März 2024

Hinzugefügte Funktionalität

Sie können jetzt CloudTrail  
Datenereignisse auf Amazon  
Simple Workflow Service  
(Amazon SWF) -Domänen  
protokollieren, indem Sie  
erweiterte Event-Selektoren  
verwenden. Weitere Informationen finden Sie unter [Datenereignisse](#).

14. Februar 2024

Hinzugefügte Funktionalität

CloudTrail hat die ListInsightsMetricData API hinzugefügt. Die ListInsightsMetricData API gibt Insights-Metriken für Trails zurück, für die Insights aktiviert wurde. Weitere Informationen finden Sie [ListInsightsMetricData](#) in der AWS CloudTrail API-Referenz.

6. Februar 2024

<a href="#">Hinzugefügte Funktionalität</a>	Sie können jetzt CloudTrail Datenereignisse für AWS IoT, und protokollieren AWS IoT SiteWise, AWS AppConfig indem Sie erweiterte Event-Sektoren verwenden. Weitere Informationen finden Sie unter <a href="#">Datenereignisse</a> .	04. Januar 2024
<a href="#">Hinzugefügte Funktionalität</a>	Sie können jetzt CloudTrail Datenereignisse für protokollieren, AWS IoT Greengrass indem Sie erweiterte Event-Sektoren verwenden. Weitere Informationen finden Sie unter <a href="#">Datenereignisse</a> .	22. Dezember 2023
<a href="#">Neue Region unterstützt</a>	CloudTrail erweiterte die Unterstützung auf eine neue Region, die Region Canada West (Calgary). Weitere Informationen finden Sie unter <a href="#">CloudTrail Unterstützte Regionen</a> .	20. Dezember 2023
<a href="#">Hinzugefügte Funktionalität</a>	Sie können jetzt CloudTrail Datenereignisse für Amazon Keyspaces (für Apache Cassandra) AWS IoT TwinMaker, Amazon RDS und AWS Supply Chain mithilfe erweiterter Event-Sektoren protokollieren. <a href="#">Weitere Informationen finden Sie unter Datenereignisse</a> .	20. Dezember 2023

### Die AWS verwaltete Richtlinie wurde aktualisiert

Die verwaltete Richtlinie [CloudTrailServiceRolePolicy](#) wurde aktualisiert, sodass die folgenden Aktionen für den Ereignisdatenspeicher einer Organisation möglich sind, wenn der Verbund deaktiviert ist: `glue:DeleteTable` und `lakeformation:DeregisterResource` .

26. November 2023

### Hinzugefügte Funktionalität

Sie können jetzt einen CloudTrail Lake-Ereignisdatenspeicher verbinden, um die mit dem Ereignisdatenspeicher verknüpften Metadaten im AWS Glue [Datenkatalog](#) zu sehen und mithilfe von Amazon Athena SQL-Abfragen für die Ereignisdaten auszuführen. Anhand der im AWS Glue Datenkatalog gespeicherten Tabellenmetadaten weiß die Athena-Abfrage-Engine, wie die Daten, die Sie abfragen möchten, gesucht, gelesen und verarbeitet werden. Weitere Informationen finden Sie unter [Verbinden eines Ereignisdatenspeichers](#).

26. November 2023

Hinzugefügte Funktionalität

Sie können jetzt CloudTrail Datenereignisse protokollieren, AWS Cloud Map indem Sie erweiterte Event-Selektoren verwenden. Weitere Informationen finden Sie unter [Protokollieren von Datenereignissen](#).

16. November 2023

Hinzugefügte Funktionalität

Sie können jetzt CloudTrail Datenereignisse in Amazon SQS SQS-Nachrichten protokollieren, indem Sie erweiterte Event-Selektoren verwenden. Weitere Informationen finden Sie unter [Protokollieren von Datenereignissen](#).

16. November 2023

## Hinzugefügte Funktionalität

CloudTrail Lake bietet jetzt zwei Preisoptionen für Event-Datenspeicher: eine verlängerbare Aufbewahrungsfrist für ein Jahr und eine siebenjährige Aufbewahrung. Die Preisoption bestimmt die Kosten für die Erfassung und Speicherung von Ereignissen sowie die standardmäßige und maximale Aufbewahrungsdauer für den Ereignisdatenspeicher. Vor dieser Version wurde für alle Ereignisdatenspeicher die Preisoption für die Aufbewahrung von sieben Jahren verwendet. [Mithilfe der Konsole oder des API-Vorgangs können Sie für einen Event-Datenspeicher von der Preisoption mit siebenjähriger Aufbewahrung auf die verlängerbare Aufbewahrungsfrist für ein Jahr umstellen.](#) [CloudTrail AWS CLI UpdateEventDataStore](#) Weitere Informationen zu den Preisoptionen finden Sie unter [AWS CloudTrail -Preisgestaltung](#) und [Preisoptionen für Ereignisdatenspeicher](#).

15. November 2023

## Hinzugefügte Funktionalität

Sie können jetzt Insights-Ereignisse in Lake sammeln. CloudTrail AWS CloudTrail Insights helfen AWS Benutzern, ungewöhnliche Aktivitäten im Zusammenhang mit API-Aufrufen und API-Fehlerraten zu identifizieren und darauf zu reagieren, indem CloudTrail Verwaltungseignisse kontinuierlich analysiert werden. Um Insights-Ereignisse in CloudTrail Lake zu sammeln, benötigen Sie einen Quellereignisdatenspeicher, der Verwaltungseignisse protokolliert und Insights aktiviert, sowie einen Zielergebnisdatenspeicher, der Insights-Ereignisse auf der Grundlage ungewöhnlicher Verwaltungseignisaktivitäten im Quellereignisdatenspeicher sammelt. Weitere Informationen finden Sie unter [Erstellen eines Ereignisdatenspeichers für CloudTrail Insights-Ereignisse](#) und [Logging Insights-Ereignisse](#).

9. November 2023



---

<a href="#">Zusätzlicher Service-Support</a>	Diese Version unterstützt AWS Launch Wizard. Weitere Informationen finden Sie in den <a href="#">AWS-Service Themen CloudTrail</a> und <a href="#">Protokollierung von AWS Launch Wizard API-Aufrufen mithilfe von AWS CloudTrail</a> .	8. November 2023
<a href="#">Zusätzlicher Service-Support</a>	Diese Version unterstützt Amazon Bedrock. Weitere Informationen finden Sie in den <a href="#">AWS-Service Themen für CloudTrail</a> und <a href="#">Protokollieren von Amazon Bedrock API-Aufrufen mithilfe von AWS CloudTrail</a> .	23. Oktober 2023
<a href="#">Hinzugefügte Funktionalität</a>	Sie können jetzt CloudTrail Datenereignisse Amazon CodeWhisperer Amazon-Anpassungen mithilfe erweiterter Event-Selektoren protokollieren. Weitere Informationen finden Sie unter <a href="#">Protokollieren von Datenereignissen</a> .	18. Oktober 2023
<a href="#">Hinzugefügte Funktionalität</a>	Sie können jetzt CloudTrail Datenereignisse in Amazon Timestream Timestream-Datenbanken und -Tabellen protokollieren, indem Sie erweiterte Event-Selektoren verwenden. Weitere Informationen finden Sie unter <a href="#">Protokollieren von Datenereignissen</a> .	28. September 2023

### Hinzugefügte Funktionalität

Sie können jetzt CloudTrail Datenereignisse zu Amazon SNS SNS-Themen und Plattformendpunkten protokollieren, indem Sie erweiterte Event-Selektoren verwenden. Weitere Informationen finden Sie unter [Protokollieren von Datenereignissen](#).

28. September 2023

### Aktualisierte Dokumentation

Es wurde eine Tabelle hinzugefügt, in der die Aufgaben aufgeführt sind, die das Verwaltungskonto, delegierte Administratorkonten und Mitgliedskonten innerhalb einer AWS Organizations Organisation ausführen können. CloudTrail Weitere Informationen finden Sie unter [Delegierte Administratoren einer Organisation](#).

25. September 2023

### Zusätzlicher Service-Support

Diese Version unterstützt AWS Marketplace Agreement s. Weitere Informationen finden Sie in den [AWS-Service Themen Agreements API-Aufrufe CloudTrail und Protokollierung von Agreements mit AWS CloudTrail](#).

1. September 2023

### Hinzugefügte Funktionalität

Sie können jetzt CloudTrail Datenereignisse auf Amazon Kinesis Kinesis-Videostreams und SageMaker Amazon-Endpunkten protokollieren, indem Sie erweiterte Event-Sektoren verwenden. Weitere Informationen finden Sie unter [Protokollieren von Datenereignissen](#).

31. August 2023

### Zusätzlicher Service-Support

Diese Version unterstützt den AWS Application Transformation Service. AWS Der Application Transformation Service ist ein Back-End-Dienst, der von Diensten wie AWS Microservice Extractor für .NET verwendet wird. Weitere Informationen finden Sie unter [CloudTrailUnterstützte Dienste](#) und Integrationen.

26. August 2023

### Hinzugefügte Funktionalität

Sie können jetzt CloudTrail Datenereignisse auf dem AWS Private CA Connector für Active Directory protokollieren, indem Sie erweiterte Ereignisauswahlen verwenden. Weitere Informationen finden Sie unter [Protokollieren von Datenereignissen](#).

24. August 2023

### [Aktualisierte Dokumentation](#)

Neue CloudTrail Lake-Szenarien wurden hinzugefügt, um zu zeigen, wie Sie Ereignisdatenspeicher erstellen, CloudTrail Lake-Dashboards anzeigen, Trail-Ereignisse in einen Ereignisdatenspeicher kopieren, Beispielabfragen anzeigen und ausführen und Abfrageergebnisse mithilfe von in einem Amazon S3 S3-Bucket speichern. AWS Management Console Weitere Informationen finden Sie unter [Szenarien für Lake CloudTrail](#)

16. August 2023

### [Neue Region unterstützt](#)

CloudTrail erweiterte die Unterstützung auf eine neue Region, die Region Israel (Tel Aviv). Weitere Informationen finden Sie unter [CloudTrail Unterstützte Regionen](#).

1. August 2023

### [Zusätzlicher Service-Support](#)

Diese Version unterstützt AWS HealthImaging. Weitere Informationen finden Sie unter [CloudTrail Unterstützte Dienste und Integrationen und Protokollierung von AWS HealthImaging API-Aufrufen mithilfe von AWS CloudTrail](#).

26. Juli 2023

---

<a href="#">Hinzugefügte Funktionalität</a>	Sie können jetzt CloudTrail Datenereignisse in AWS HealthImaging Datenspeichern protokollieren, indem Sie erweiterte Event-Selektoren verwenden. Weitere Informationen finden Sie unter <a href="#">Protokollieren von Datenereignissen</a> .	26. Juli 2023
<a href="#">Hinzugefügte Funktionalität</a>	Sie können jetzt CloudTrail Datenereignisse auf AWS Systems Manager Kontrollkärtchen und Amazon Managed Blockchain Blockchain-Netzwerken protokollieren, indem Sie erweiterte Event-Selektoren verwenden. Weitere Informationen finden Sie unter <a href="#">Protokollieren von Datenereignissen</a> .	21. Juni 2023
<a href="#">Hinzugefügte Funktionalität</a>	Sie können jetzt die von CloudTrail Lake gespeicherten Abfrageergebnisse mit dem <code>aws cloudtrail verify-query-results</code> Befehl überprüfen. Weitere Informationen finden Sie unter <a href="#">Validieren von gespeicherten Abfrageergebnissen mit der AWS CLI</a> .	21. Juni 2023

<a href="#">Zusätzlicher Service-Support</a>	Diese Version unterstützt Amazon Verified Permissions. Weitere Informationen finden Sie unter <a href="#">CloudTrailUnterstützte Dienste und Integrationen und Protokollierung von API-Aufrufen von Amazon Verified Permissions mithilfe von AWS CloudTrail</a> .	13. Juni 2023
<a href="#">Hinzugefügte Funktionalität</a>	Sie können jetzt CloudTrail Lake-Dashboards verwenden , um die Ereignisse in einem Ereignisdatenspeicher zu visualisieren. Weitere Informationen finden Sie unter <a href="#">Anzeigen von Lake-Dashboards</a> .	13. Juni 2023
<a href="#">Hinzugefügte Funktionalität</a>	Sie können jetzt CloudTrail Datenereignisse in den Richtlinienspeichern von Amazon Verified Permissions protokollieren, indem Sie erweiterte Event-Selektoren verwenden. Weitere Informationen finden Sie unter <a href="#">Protokollieren von Datenereignissen</a> .	13. Juni 2023
<a href="#">Hinzugefügte Funktionalität</a>	Sie können jetzt CloudTrail Datenereignisse in einem CodeWhisperer Amazon-Profil protokollieren, indem Sie erweiterte Event-Selektoren verwenden. Weitere Informationen finden Sie unter <a href="#">Protokollieren von Datenereignissen</a> .	6. Juni 2023

### Hinzugefügte Funktionalität

Sie können jetzt die Erfassung von Ereignissen in Ereignisdatenspeichern starten und beenden. CloudTrail Informationen zum Beenden der Ereignisaufnahme mithilfe der Konsole finden Sie unter [Beenden der Ereignisaufnahme eines Ereignisdatenspeichers](#). Informationen zum Stoppen der Ereignisaufnahme mithilfe von finden Sie unter [Beenden der AWS CLI Erfassung in einem Ereignisdatenspeicher](#).

02. Juni 2023

### Hinzugefügte Funktionalität

Sie können jetzt CloudTrail Datenereignisse in einem Amazon EMR-Write-Ahead-Log-Workspace protokollieren, indem Sie erweiterte Event-Selektoren verwenden. Weitere Informationen finden Sie unter [Protokollieren von Datenereignissen](#).

31. Mai 2023

### Zusätzlicher Service-Support

Diese Version unterstützt Amazon Security Lake. Weitere Informationen finden Sie unter [CloudTrail Unterstützte Dienste und Integrationen und Protokollieren von Amazon Security Lake-API-Aufrufen mithilfe von AWS CloudTrail](#).

30. Mai 2023

[Aktualisierte Dokumentation](#)

Das Thema des Elements CloudTrail userIdentity wurde aktualisiert und enthält nun ein Beispiel und Felddesreibungen für eine Anfrage, die im Namen eines IAM Identity Center-Benutzers gestellt wurde. Weitere Informationen finden Sie unter [CloudTrail - Element userIdentity](#).

23. Mai 2023

[Aktualisierte Dokumentation](#)

Dieses Update unterstützt die folgende Patch-Version für die CloudTrail Processing Library: -1.6.1.jar. aws-cloud-trail-processing-library [Weitere Informationen finden Sie unter Verwenden der CloudTrail Verarbeitungsbibliothek und der CloudTrail Verarbeitungsbibliothek unter](#). GitHub

23. Mai 2023

[Hinzugefügte Funktionalität](#)

CloudTrail Lake unterstützt jetzt alle Presto-Funktionen und -Operatoren. Weitere Informationen finden Sie unter [CloudTrail Lake SQL-Einschränkungen](#).

09. Mai 2023



### Hinzugefügte Funktionalität

Sie können jetzt CloudTrail Datenereignisse auf einem GuardDuty Amazon-Detektor protokollieren, indem Sie erweiterte Event-Sektoren verwenden. Weitere Informationen finden Sie unter [Protokollieren von Datenereignissen](#) und [Protokollieren von GuardDuty Amazon-API-Aufrufen mit AWS CloudTrail](#).

30. März 2023

### Aktualisierte Dokumentation

Wir haben einen neuen Abschnitt über die Erstellung von benutzerdefinierten Kostenzuweisungs-Tags für Ereignisdatenspeicher hinzugefügt. Weitere Informationen finden Sie unter [Benutzerdefinierte Kostenzuordnungs-Tags für CloudTrail Lake-Event-Datenspeicher](#) erstellen.

24. März 2023

### Zusätzlicher Service-Support

Diese Version unterstützt AWS Telco Network Builder (AWS TNB). Weitere Informationen finden Sie unter [CloudTrail Unterstützte Dienste und Integrationen](#) und [Protokollierung von AWS Telco Network Builder-API-Aufrufen](#) mithilfe von AWS CloudTrail

21. Februar 2023

---

<a href="#">Hinzugefügte Funktionalität</a>	Sie können jetzt CloudTrail Datenereignisse in Amazon Cognito Cognito-Identitäts pools protokollieren, indem Sie erweiterte Event-Selektoren verwenden. Weitere Informationen finden Sie unter <a href="#">Protokollieren von Datenereignissen</a> .	15. Februar 2023
<a href="#">Aktualisierte Dokumentation</a>	Ein neuer Abschnitt über die für CloudTrail Lake verfügbaren Lernressourcen wurde hinzugefügt. Weitere Informationen finden Sie unter <a href="#">Lernressourcen</a> .	9. Februar 2023
<a href="#">Hinzugefügte Funktionalität</a>	Sie können jetzt CloudTrail Lake-Integrationen mit Ereignisquellen außerhalb von AWS erstellen. Sie können Benutzeraktivitätsdaten aus beliebigen Quellen in Ihren hybriden Umgebungen protokollieren und speichern, beispielsweise aus internen oder SaaS-Anwendungen, die On-Premises oder in der Cloud gehostet werden, aus virtuellen Maschinen oder Containern. Weitere Informationen finden Sie unter <a href="#">Erstellen Sie eine Integration mit einer Ereignisquelle außerhalb von AWS</a> .	31. Januar 2023

---

<a href="#">Hinzugefügte Funktionalität</a>	Sie können jetzt CloudTrail Datenereignisse zu CloudTrail PutAuditEvents Aktivitäten auf einem CloudTrail Lake-Kanal protokollieren, indem Sie erweiterte Event-Selektoren verwenden. Weitere Informationen finden Sie unter <a href="#">Protokollieren von Datenereignissen</a> .	31. Januar 2023
<a href="#">Neue Region unterstützt</a>	CloudTrail erweiterte die Unterstützung auf eine neue Region, die Region Asien-Pazifik (Melbourne). Weitere Informationen finden Sie unter <a href="#">CloudTrail Unterstützte Regionen</a> .	24. Januar 2023
<a href="#">Aktualisierte Dokumentation</a>	Ein neuer Abschnitt zur Verwaltung der Datenkonsistenz wurde hinzugefügt CloudTrail, siehe <a href="#">Datenkonsistenz verwalten in CloudTrail</a> .	18. Januar 2023
<a href="#">Hinzugefügte Funktionalität</a>	Sie können jetzt CloudTrail Datenereignisse in Amazon SageMaker Feature Stores protokollieren, indem Sie erweiterte Event-Selektoren verwenden. Weitere Informationen finden Sie unter <a href="#">Protokollieren von Datenereignissen</a> .	27. Dezember 2022

---

<a href="#">Zusätzlicher Service-Support</a>	Diese Version unterstützt AWS Marketplace Discovery. Siehe <a href="#">Von AWS CloudTrail unterstützte Services und Integrationen</a> .	15. Dezember 2022
<a href="#">Hinzugefügte Funktionalität</a>	Sie können jetzt CloudTrail Datenereignisse in Testkomponenten von Amazon SageMaker Metrics Experiments protokollieren, indem Sie erweiterte Event-Selektoren verwenden. Weitere Informationen finden Sie unter <a href="#">Protokollieren von Datenereignissen</a> .	15. Dezember 2022
<a href="#">Hinzugefügte Funktionalität</a>	Sie können jetzt einen Ereignisdatenspeicher erstellen, der AWS Config Konfigurationselemente enthält, und den Ereignisdatenspeicher verwenden, um nicht konforme Änderungen an Ihren Produktionsumgebungen zu untersuchen. Weitere Informationen finden Sie unter <a href="#">Erstellen eines Ereignisdatenspeichers für AWS Config Konfigurationselemente</a> .	28. November 2022
<a href="#">Neue Region unterstützt</a>	CloudTrail erweiterte den Support auf eine neue Region, die Region Asien-Pazifik (Hyderabad). Weitere Informationen finden Sie unter <a href="#">CloudTrail Unterstützte Regionen</a> .	22. November 2022

<a href="#">Hinzugefügte Funktionalität</a>	Sie können jetzt CloudTrail Datenereignisse in Amazon FinSpace Umgebungen protokollieren, indem Sie erweiterte Event-Selektoren verwenden. Weitere Informationen finden Sie unter <a href="#">Protokollieren von Datenereignissen</a> .	18. November 2022
<a href="#">Neue Region unterstützt</a>	CloudTrail erweiterte die Unterstützung auf eine neue Region, die Region Europa (Spanien). Weitere Informationen finden Sie unter <a href="#">CloudTrail Unterstützte Regionen</a> .	16. November 2022
<a href="#">Neue Region unterstützt</a>	CloudTrail erweiterte die Unterstützung auf eine neue Region, die Region Europa (Zürich). Weitere Informationen finden Sie unter <a href="#">CloudTrail Unterstützte Regionen</a> .	9. November 2022
<a href="#">Hinzugefügte Funktionalität</a>	Das Verwaltungskonto einer AWS Organizations Organisation kann jetzt einen delegierten Administrator hinzufügen, der die CloudTrail Trails und Event-Datenspeicher der Organisation verwaltet. Weitere Informationen finden Sie unter <a href="#">Delegierte Administratoren einer Organisation</a> .	7. November 2022

Hinzugefügte Funktionalität

Sie können jetzt die AWS Key Management Service Verschlüsselung für einen CloudTrail Lake-Ereignisdaten speicher aktivieren. Weitere Informationen finden Sie unter [Erstellen eines Ereignisdatenspeichers](#).

7. November 2022

Hinzugefügte Funktionalität

Sie können jetzt CloudTrail Lake-Abfrageergebnisse in einem Amazon S3 S3-Bucket speichern, wenn Sie eine Abfrage ausführen. Weitere Informationen zum Ausführen einer Abfrage finden Sie unter [Ausführen einer Abfrage und Speichern von Abfrageergebnissen](#). Weitere Informationen zum Herunterladen von Abfrageergebnissen finden Sie unter [Abrufen und Herunterladen von gespeicherten Abfrageergebnissen](#).

21. Oktober 2022

Hinzugefügte Funktionalität

Sie können jetzt CloudTrail Trail-Ereignisse in einen CloudTrail Lake-Event-Datenspeicher kopieren. Weitere Informationen finden Sie unter [Trail-Ereignisse nach CloudTrail Lake kopieren](#).

19. September 2022

### [Aktualisierte Dokumentation](#)

Eine Liste der unterstützten CloudWatch Amazon-Metriken für CloudTrail Lake wurde hinzugefügt. Weitere Informationen finden Sie unter [Unterstützte CloudWatch Metriken](#).

16. September 2022

### [Hinzugefügte Funktionalität](#)

Mit dem können Sie nun CloudTrail mit Services verknüpfte Kanäle anzeigen. AWS CLI Weitere Informationen finden Sie unter [Dienstverknüpfte Kanäle anzeigen für mithilfe CloudTrail von AWS CLI](#)

09. September 2022

### [Neue Region unterstützt](#)

CloudTrail erweiterte den Support auf eine neue Region, die Region Naher Osten (VAE). Weitere Informationen finden Sie unter [CloudTrail Unterstützte Regionen](#).

30. August 2022

## Geänderte Funktionalität

CloudTrail hat den Namen der verwalteten Richtlinie `AWSCloudTrailReadOnlyAccess` in `AWSCloudTrail_ReadOnlyAccess` geändert. Die Berechtigungen in dieser Richtlinie wurden detaillierter festgelegt. Standardmäßig gewährt die Richtlinie nicht mehr die Erlaubnis, alle Amazon S3 S3-Buckets, AWS Lambda -Funktionen oder AWS KMS -Aliase aufzulisten. Weitere Informationen finden Sie unter [Schreibgeschützter Zugriff](#) aus.

6. Juni 2022

## Geänderte Funktionalität

Als bewährte Sicherheitmethode gilt es, dem `s3:GetBucketAcl` - ACL-Kontrollblock und den Richtlinien von Amazon-S3 -Bucket einen `aws:SourceArn` - oder `aws:SourceAccount` -Bedingungsschlüssel hinzuzufügen. Weitere Informationen finden Sie unter [Amazon S3 S3-Bucket-Richtlinien konfigurieren für CloudTrail](#).

11. Mai 2022



## Geänderte Funktionalität

Ab dem 24. Februar 2022 AWS CloudTrail begann die Änderung der `sourceIPAddress` Feldwerte `userAgent` und in allen Fällen, die auf eine AWS Management Console Sitzung zurückzuführen waren, in der ein Proxy-Client verwendet wurde. CloudTrail ersetzt bei diesen Ereignissen die Werte der `sourceIPAddress` Felder `userAgent` und durch `AWS Internal`. CloudTrail hat diese Änderung vorgenommen, um die Protokollierung von Informationen für Serviceaktionen für alle AWS Dienste zu standardisieren. Weitere Informationen finden Sie unter [Inhalt von CloudTrail Datensätzen](#).

12. April 2022

## Zusätzlicher Service-Support

Diese Version unterstützt Amazon GameSparks. Siehe [Von AWS CloudTrail unterstützte Services und Integrationen](#).

24. März 2022

## Zusätzlicher Service-Support

Diese Version unterstützt den AWS App Mesh Envoy Management Service. Siehe [Von AWS CloudTrail unterstützte Services und Integrationen](#).

18. März 2022

## Aktualisierte Dokumentation

Neue Abfragebeispiele wurden für CloudTrail Lake hinzugefügt, eine neue Funktion, mit der Sie feinkörnige SQL-Abfragen mit mehreren Feldern für Ihre Ereignisse ausführen können. Auch ein neues Feld, `BytesScanned`, wurde den Ergebnissen der Abfragemetadaten der Operationen `DescribeQuery` und `GetQueryResults` hinzugefügt. [Weitere Informationen finden Sie unter Arbeiten mit Lake. CloudTrail](#)

4. März 2022

## Geänderte Funktionalität

CloudTrail entfernt jetzt die Konto-ID des Amazon S3 S3-Bucket-Besitzers im `resources` Block eines Datenereignisses, wenn beide der folgenden Bedingungen erfüllt sind: Der Datenereignis-API-Aufruf stammt von einem anderen AWS Konto als dem Amazon S3 S3-Bucket-Besitzer, und der API-Aufrufer hat einen `AccessDenied` Fehler erhalten, der nur für das Anruferkonto gilt. Weitere Informationen finden Sie unter [Redigieren von Bucket-Eigentümer-Konto-IDs für Datenereignisse, die von anderen Konten aufgerufen werden](#).

3. März 2022

## [Aktualisierte Dokumentation](#)

Dieses Update unterstützt die folgende Version für die CloudTrail Processing Library: Unterstützung für die Implementierung eines benutzerdefinierten S3-Managers hinzugefügt, Ereignisprotokollierung zum Protokollieren von Ausnahmen im Zusammenhang mit der Dateianalyse, Unterstützung für das Parsen eines optionalen `errorCode` Felds in und Aktualisierung der Regex zur Konto-ID-ParsinginsightDetails, sodass er nicht numerische Werte akzeptiert. [Weitere Informationen finden Sie unter Using the Processing Library und The CloudTrail Processing Library on. CloudTrail GitHub](#)

28. Januar 2022

### Hinzugefügte Funktionalität

CloudTrail stellt CloudTrail Lake vor, ein neues Feature, mit dem Sie detaillierte SQL-Abfragen mit mehreren Feldern für Ihre Ereignisse ausführen können. Die Ereignisse werden in Ereignisdatenspeichern zusammengefasst, bei denen es sich um unveränderliche Sammlungen von Ereignissen handelt, die auf Kriterien basieren, die Sie mit Hilfe von erweiterten Ereignisselektoren auswählen können. [Weitere Informationen finden Sie unter Arbeiten mit Lake.](#)  
[CloudTrail](#)

5. Januar 2022

### Neue Region unterstützt

CloudTrail erweiterte die Unterstützung auf eine neue Region, die Region Asien-Pazifik (Jakarta). Weitere Informationen finden Sie unter [CloudTrail Unterstützte Regionen](#).

13. Dezember 2021

### Zusätzlicher Service-Support

Diese Version unterstützt Amazon WorkSpaces Web. Siehe [Von AWS CloudTrail unterstützte Services und Integrationen](#).

3. Dezember 2021

### Hinzugefügte Funktionalität

Sie können jetzt CloudTrail Datenereignisse in AWS Glue Tabellen protokollieren, die von Lake Formation erstellt wurden, indem Sie erweiterte Event-Selektoren verwenden. Weitere Informationen finden Sie unter [Protokollieren von Datenereignissen](#).

30. November 2021

### Geänderte Funktionalität

Aus Sicherheitsgründen können Sie jetzt Schlüsselrichtlinien und Amazon S3 S3-Bucket-Richtlinien einen `aws:SourceAccount` AWS KMS Bedingung `sschlüssel aws:SourceArn` oder einen Bedingung `sschlüssel` hinzufügen. Weitere Informationen finden Sie unter [Konfiguration AWS KMS wichtiger Richtlinien für CloudTrail](#) und [Konfiguration von Amazon S3 S3-Bucket-Richtlinien für CloudTrail](#).

15. November 2021

### Zusätzlicher Service-Support

Diese Version unterstützt AWS Resilience Hub. Siehe [Von AWS CloudTrail unterstützte Services und Integrationen](#).

10. November 2021

---

<a href="#">Hinzugefügte Funktionalität</a>	Ein neuer CloudTrail Insights-Ereignistyp ist verfügbar : Insights-Ereignisse mit Fehlerrate. Ein Fehlerrate-Insights-Ereignis erfasst ungewöhnliche Aktivitäten bei einem Fehler, der für APIs auftritt, die in Ihrem Konto aufgerufen werden. Weitere Informationen finden Sie unter <a href="#">Protokollieren von Insights-Ereignissen für Trails</a> .	10. November 2021
<a href="#">Hinzugefügte Funktionalität</a>	Sie können jetzt CloudTrail Datenereignisse in DynamoDB-Streams protokollieren, indem Sie erweiterte Event-Selektoren verwenden . Weitere Informationen finden Sie unter <a href="#">Protokollieren von Datenereignissen</a> .	22. September 2021
<a href="#">Hinzugefügte Funktionalität</a>	Sie können jetzt Datenereignisse auf Amazon-S3-Zugriffspunkten protokollieren. Sie können Amazon-S3-Zugriffspunkt-Datenereignisse mithilfe erweiterter Ereignisselektoren protokollieren. Weitere Informationen finden Sie unter <a href="#">Protokollieren von Datenereignissen</a> .	24. August 2021

## Geänderte Funktionalität

Wenn Sie einen Trail für das Senden von Benachrichtigungen an Amazon SNS konfigurieren, CloudTrail fügt er Ihrer Zugriffsrichtlinie für SNS-Themen eine Richtlinienerklärung hinzu, die das Senden von Inhalten CloudTrail an ein SNS-Thema ermöglicht. Aus Sicherheitsgründen empfehlen wir, der Richtlinienerklärung einen Bedingungschlüssel `aws:SourceArn` oder einen `aws:SourceAccount` Bedingungschlüssel hinzuzufügen. CloudTrail Weitere Informationen finden Sie unter [Amazon SNS SNS-Themenrichtlinie für CloudTrail](#).

16. August 2021

## Zusätzlicher Service-Support

Diese Version unterstützt Amazon Route 53 Application Recovery Controller. Siehe [Von AWS CloudTrail unterstützte Services und Integrationen](#).

27. Juli 2021

### Hinzugefügte Funktionalität

Sie können jetzt Datenereignisse in Amazon-EBS-Direct-APIs protokollieren, die auf EBS-Snapshots ausgeführt werden. Sie können Amazon-EBS-Direct-API-Datenereignisse protokollieren, indem Sie erweiterte Ereignisfilter verwenden. Weitere Informationen finden Sie unter [Protokollieren von Datenereignissen](#).

27. Juli 2021

### Geänderte Funktionalität

Bei der CloudTrail Verarbeitung von Datenereignissen werden Zahlen in ihrem ursprünglichen Format beibehalten, unabhängig davon, ob es sich um eine Ganzzahl (`int`) oder eine Zahl handelt. `float` Bei Ereignissen, die ganze Zahlen in den Feldern eines Datenereignisses enthielten, wurden diese Zahlen in der CloudTrail Vergangenheit als Gleitkommazahlen verarbeitet. CloudTrail behält jetzt das ursprüngliche Format von Ganzzahlen in Datenereignissen bei. Weitere Informationen finden Sie unter [Verwenden der CloudTrail Verarbeitungsbibliothek](#).

13. Juli 2021



---

<a href="#">Hinzugefügte Funktionalität</a>	Sie können jetzt Amazon-RDS-Data-API-Verwaltungsereignisse von Ihren Trails ausschließen. Weitere Informationen finden Sie unter <a href="#">Protokollverwaltungsereignisse für Trails</a> .	1. Juli 2021
<a href="#">Zusätzlicher Service-Support</a>	Diese Version unterstützt AWS BugBust. Siehe <a href="#">Von AWS CloudTrail unterstützte Services und Integrationen</a> .	24. Juni 2021
<a href="#">Zusätzlicher Service-Support</a>	Diese Version unterstützt Amazon Managed Grafana und Amazon Managed Service für Prometheus. Siehe <a href="#">Von AWS CloudTrail unterstützte Services und Integrationen</a> .	2. Juni 2021
<a href="#">Zusätzlicher Service-Support</a>	Diese Version unterstützt AWS App Runner. Siehe <a href="#">Von AWS CloudTrail unterstützte Services und Integrationen</a> .	18. Mai 2021
<a href="#">Zusätzlicher Service-Support</a>	Diese Version unterstützt AWS Systems Manager Incident Manager. Siehe <a href="#">Von AWS CloudTrail unterstützte Services und Integrationen</a> .	10. Mai 2021

<a href="#">Aktualisierte Dokumentation</a>	Dieses Update beschreibt die Anforderungen an die Protokollierung von Datenereignissen für AWS Config Konformitätspakete, insbesondere für Compliance-Frameworks wie HIPAA oder FedRAMP. Weitere Informationen finden Sie unter <a href="#">Protokollieren von Datenereignissen</a> .	7. Mai 2021
<a href="#">Zusätzlicher Service-Support</a>	Diese Version unterstützt Service Quotas und Amazon EBS Direct APIs. Siehe <a href="#">Von AWS CloudTrail unterstützte Services und Integrationen</a> .	13. April 2021
<a href="#">Hinzugefügte Funktionalität</a>	CloudTrail protokolliert nach der Konfiguration durch einen IAM-Administrator sourceIdentity Informationen in Ereignissen <a href="#">AWS STS</a> , wenn Benutzer eine IAM-Rolle übernehmen oder Aktionen mit der übernommenen Rolle ausführen. Weitere Informationen finden Sie unter <a href="#">CloudTrail -Element userIdentity</a> .	13. April 2021
<a href="#">Aktualisierte Dokumentation</a>	Dieses Update dokumentiert die Grenzwerte für Inhalte in einigen Ereignisdatensatzfeldern in Kilobyte (KB). CloudTrail Weitere Informationen finden Sie unter Inhalt von <a href="#">CloudTrail Datensätzen</a> .	8. April 2021

---

<a href="#">Hinzugefügte Funktionalität</a>	CloudTrail protokolliert nach der Konfiguration durch einen IAM-Administrator sourceIdentity Informationen in Ereignissen <a href="#">AWS STS</a> , wenn Benutzer eine IAM-Rolle übernehmen oder Aktionen mit der angenommenen Rolle ausführen. Weitere Informationen finden Sie unter <a href="#">CloudTrail -Element userIdentity</a> .	6. April 2021
<a href="#">Hinzugefügte Funktionalität</a>	Sie können jetzt Datenereignisse in Amazon-DynamoDB-Tabellen protokollieren. Sie können DynamoDB-Datenereignisse mithilfe von Ereignisselectoren oder erweiterten Ereignisselectoren protokollieren. Weitere Informationen finden Sie unter <a href="#">Protokollieren von Datenereignissen</a> .	23. März 2021
<a href="#">Zusätzlicher Service-Support</a>	Diese Version unterstützt Amazon Managed Workflows for Apache Airflow. Siehe <a href="#">Von AWS CloudTrail unterstützte Services und Integrationen</a> .	22. März 2021

Hinzugefügte Funktionalität

Sie können jetzt Datenereignisse auf S3-Objekt-Lambda-Zugriffspunkten protokollieren, wenn Sie sich für die Verwendung erweiterter Ereigniselektoren entschieden haben. Weitere Informationen finden Sie unter [Protokollieren von Datenereignissen](#).

18. März 2021

Zusätzlicher Service-Support

Diese Version unterstützt den AWS Fault Injection Simulator. Siehe [Von AWS CloudTrail unterstützte Services und Integrationen](#).

15. März 2021

Hinzugefügte Funktionalität

Sie können nun Datenereignisse auf Ethereum-Knoten in Amazon Managed Blockchain protokollieren, wenn Sie sich für die Verwendung erweiterter Ereigniselektoren entschieden haben. Weitere Informationen finden Sie unter [Protokollieren von Datenereignissen](#).

1. März 2021

Zusätzlicher Service-Support

Diese Version unterstützt Amazon Managed Blockchain und die Vorschau von Ethereum für Managed Blockchain. Siehe [Von AWS CloudTrail unterstützte Services und Integrationen](#).

4. Februar 2021

<a href="#">Zusätzlicher Service-Support</a>	Diese Version unterstützt AWS Amplify. Siehe <a href="#">Von AWS CloudTrail unterstützte Services und Integrationen</a> .	3. Februar 2021
<a href="#">Zusätzlicher Service-Support</a>	Diese Version unterstützt Amazon Lookout for Metrics. Siehe <a href="#">Von AWS CloudTrail unterstützte Services und Integrationen</a> .	1. Februar 2021
<a href="#">Aktualisierte Dokumentation</a>	Dieses Update unterstützt die folgende Patch-Version für die CloudTrail Processing Library: Aktualisieren Sie die Dateiverweise auf die .jar-Datei im Benutzerhandbuch, um die neueste Version, aws-cloudtrail-processing-library -1.4.0.jar, zu verwenden. <a href="#">Weitere Informationen finden Sie unter Verwenden der CloudTrail Verarbeitungsbibliothek und der Verarbeitungsbibliothek unter. CloudTrail GitHub</a>	12. Januar 2021
<a href="#">Hinzugefügte Funktionalität</a>	Sie können jetzt Datenereignisse auf Amazon S3 auf AWS Outposts protokollieren. Weitere Informationen finden Sie unter <a href="#">Protokollieren von Datenereignissen</a> .	21. Dezember 2020

---

<a href="#"><u>Zusätzlicher Service-Support</u></a>	Diese Version unterstützt Amazon Lookout for Equipment und Amazon Location Service. AWS Well-Architected Tool Siehe <a href="#"><u>Von AWS CloudTrail unterstützte Services und Integrationen.</u></a>	16. Dezember 2020
<a href="#"><u>Zusätzlicher Service-Support</u></a>	Diese Version unterstützt AWS IoT Greengrass V2. Siehe <a href="#"><u>Von AWS CloudTrail unterstützte Services und Integrationen.</u></a>	15. Dezember 2020
<a href="#"><u>Zusätzlicher Service-Support</u></a>	Diese Version unterstützt Amazon EMR auf EKS. Siehe <a href="#"><u>Von AWS CloudTrail unterstützte Services und Integrationen.</u></a>	10. Dezember 2020
<a href="#"><u>Zusätzlicher Service-Support</u></a>	Diese Version unterstützt AWS Audit Manager und Amazon HealthLake. Siehe <a href="#"><u>Von AWS CloudTrail unterstützte Services und Integrationen.</u></a>	8. Dezember 2020
<a href="#"><u>Zusätzlicher Service-Support</u></a>	Diese Version unterstützt Amazon Lookout for Vision. Siehe <a href="#"><u>Von AWS CloudTrail unterstützte Services und Integrationen.</u></a>	1. Dezember 2020

---

<a href="#">Hinzugefügte Funktionalität</a>	Die AWS CloudTrail Event-Version ist jetzt 1.08. Version 1.08 führt neue Felder für ein. CloudTrail Weitere Informationen finden Sie unter <a href="#">Inhalt des CloudTrail Datensatzes</a> .	24. November 2020
<a href="#">Hinzugefügte Funktionalität</a>	AWS CloudTrail führt erweiterte Ereignisselektoren für Datenereignisse ein. Erweiterte Ereignisselektoren ermöglichen eine präzisere Kontrolle der Datenereignisse, die Sie in Ihrem Trail protokollieren. Sie können Datenereignisse für bestimmte AWS Ressourcen ein- oder ausschließen und bestimmte APIs für diese Ressourcen auswählen, um sie in Ihrem Trail zu protokollieren. Weitere Informationen finden Sie unter <a href="#">Protokollieren von Datenereignissen</a> .	24. November 2020
<a href="#">Zusätzlicher Service-Support</a>	Diese Version unterstützt AWS Network Firewall. Siehe <a href="#">Von AWS CloudTrail unterstützte Services und Integrationen</a> .	17. November 2020
<a href="#">Zusätzlicher Service-Support</a>	Diese Version unterstützt AWS Trusted Advisor. Siehe <a href="#">Von AWS CloudTrail unterstützte Services und Integrationen</a> .	22. Oktober 2020

### Aktualisierte Dokumentation

Es wurden zwei neue Beispiele für Ereignisdatensätze für Anmeldeereignisse für Root-Benutzer hinzugefügt. Weitere Informationen finden Sie unter [AWS - Konsolen-Anmeldeereignisse](#).

13. Oktober 2020

### Geänderte Funktionalität

Die Berechtigungen in der `AWSCloudTrail_FullAccess`-Richtlinie wurden eingeschränkt. Mit dieser Richtlinie können Sie nicht mehr Amazon-SNS-Themen oder Amazon-S3-Buckets löschen und die `getObject`-Aktion wurde entfernt. Weitere Informationen finden Sie unter [Gewährung benutzerdefinierter Berechtigungen für CloudTrail Benutzer](#).

29. September 2020



### Aktualisierte Dokumentation

Dieses Update unterstützt die folgende Patch-Version für die CloudTrail Processing Library: Aktualisieren Sie die Dateiverweise auf die .jar-Datei im Benutzerhandbuch, um die neueste Version, aws-cloudtrail-processing-library -1.3.0.jar, zu verwenden. [Weitere Informationen finden Sie unter Verwenden der CloudTrail Verarbeitungsbibliothek und der Verarbeitungsbibliothek unter. CloudTrail GitHub](#)

28. August 2020

### Zusätzlicher Service-Support

Diese Version unterstützt AWS Outposts. Siehe [Von AWS CloudTrail unterstützte Services und Integrationen.](#)

28. August 2020

### Hinzugefügte Funktionalität

AWS CloudTrail Insights führt Attributionsfelder für CloudTrail Insights-Ereignisse ein. Attributionsfelder zeigen die obersten Benutzeridentitäten, Benutzeragenten und Fehlercodes an, die der anomalen Aktivität zugeordnet sind, die Insights-Ereignisse auslöst. Zu Vergleichszwecken zeigen Attributionsfelder auch die wichtigsten Benutzeridentitäten, Benutzeragenten und Fehlercodes an, die mit normalen oder grundlegenden Aktivitäten verbunden sind. Weitere Informationen finden Sie unter [Protokollieren von Insights-Ereignissen für Trails](#).

13. August 2020

### Hinzugefügte Funktionalität

Die AWS CloudTrail Konsole hat ein neues Design, das die Bedienung vereinfachen soll. Das AWS CloudTrail Benutzerhandbuch wurde aktualisiert und enthält nun Änderungen an den Verfahren für die Ausführung von Aufgaben in der Konsole, z. B. das Erstellen von Pfaden, das Aktualisieren von Pfaden und das Herunterladen des Ereignisverlaufs.

13. August 2020

<a href="#">Zusätzlicher Service-Support</a>	Diese Version unterstützt Amazon Interactive Video Service. Siehe <a href="#">Von AWS CloudTrail unterstützte Services und Integrationen</a> .	15. Juli 2020
<a href="#">Zusätzlicher Service-Support</a>	Diese Version unterstützt Amazon Honeycode. Siehe <a href="#">Von AWS CloudTrail unterstützte Services und Integrationen</a> .	24. Juni 2020
<a href="#">Zusätzlicher Service-Support</a>	Diese Version unterstützt Amazon Macie. Siehe <a href="#">Von AWS CloudTrail unterstützte Services und Integrationen</a> .	19. Mai 2020
<a href="#">Zusätzlicher Service-Support</a>	Diese Version unterstützt Amazon Kendra. Siehe <a href="#">Von AWS CloudTrail unterstützte Services und Integrationen</a> .	13. Mai 2020
<a href="#">Zusätzlicher Service-Support</a>	Diese Version unterstützt AWS IoT SiteWise. Siehe <a href="#">Von AWS CloudTrail unterstützte Services und Integrationen</a> .	29. April 2020
<a href="#">Unterstützung einer weiteren Region hinzugefügt</a>	Diese Version unterstützt eine zusätzliche Region: Europa (Mailand). Siehe <a href="#">Regionen mit AWS CloudTrail -Unterstützung</a> .	28. April 2020

### Unterstützung für neuen Service/neue Region

Diese Version unterstützt Amazon AppFlow. Siehe [Von AWS CloudTrail unterstützte Services und Integrationen](#). Außerdem wurde Support für die Region Afrika (Kapstadt) hinzugefügt. Siehe [Regionen mit AWS CloudTrail -Unterstützung](#).

22. April 2020

### Hinzugefügte Funktionalität

AWS KMS Aktionen mit hohem Volumen wie EncryptDecrypt, und GenerateDataKey werden jetzt als Read-Ereignisse protokolliert. Wenn Sie sich dafür entscheiden, alle AWS KMS Ereignisse auf Ihrem Trail zu protokollieren und auch Ereignisse der Schreibverwaltung zu protokollieren, protokolliert Ihr Trail relevante AWS KMS Aktionen wie Disable, Delete und ScheduleKey .

7. April 2020

### Zusätzlicher Service-Support

Diese Version unterstützt Amazon CodeGuru Reviewer. Siehe [Von AWS CloudTrail unterstützte Services und Integrationen](#).

7. Februar 2020

### Zusätzlicher Service-Support

Diese Version unterstützt Amazon Managed Apache Cassandra Service. Siehe [Von AWS CloudTrail unterstützte Services und Integrationen](#).

17. Januar 2020

---

<a href="#">Zusätzlicher Service-Support</a>	Diese Version unterstützt Amazon Connect. Siehe <a href="#">Von AWS CloudTrail unterstützte Services und Integrationen</a> .	13. Dezember 2019
<a href="#">Aktualisierte Dokumentation</a>	Dieses Update unterstützt die folgende Patch-Version für die CloudTrail Processing Library: Aktualisieren Sie die Verweise auf die .jar-Datei im Benutzerhandbuch, um die neueste Version, aws-cloudtrail-processing-library -1.2.0.jar, zu verwenden. <a href="#">Weitere Informationen finden Sie unter Using the CloudTrail Processing Library und Processing Library on. CloudTrail</a> GitHub	21. November 2019
<a href="#">Hinzugefügte Funktionalität</a>	Diese Version unterstützt AWS CloudTrail Insights, damit Sie ungewöhnliche Aktivitäten in Ihrem Konto erkennen können. Siehe <a href="#">Protokollieren von Insights-Ereignissen für Trails</a> .	20. November 2019
<a href="#">Hinzugefügte Funktionalität</a>	Diese Version bietet eine Option zum Herausfiltern von AWS Key Management Service Ereignissen aus einer Spur. Siehe <a href="#">Erstellen eines Trails</a> .	20. November 2019

<a href="#">Zusätzlicher Service-Support</a>	Diese Version unterstützt AWS CodeStar Benachrichtigungen . Siehe <a href="#">Von AWS CloudTrail unterstützte Services und Integrationen</a> .	7. November 2019
<a href="#">Hinzugefügte Funktionalität</a>	Diese Version unterstützt das Hinzufügen von Tags beim Erstellen eines Trails CloudTrail, unabhängig davon, ob Sie die CloudTrail Konsole oder die API verwenden. Diese Version fügt zwei neue APIs hinzu, <code>GetTrail</code> und <code>ListTrails</code> .	1. November 2019
<a href="#">Zusätzlicher Service-Support</a>	Diese Version unterstützt AWS App Mesh. Siehe <a href="#">Von AWS CloudTrail unterstützte Services und Integrationen</a> .	17. Oktober 2019
<a href="#">Zusätzlicher Service-Support</a>	Diese Version unterstützt Amazon Translate. Siehe <a href="#">Von AWS CloudTrail unterstützte Services und Integrationen</a> .	17. Oktober 2019
<a href="#">Aktualisierung der Dokumentation</a>	Das Thema Nicht unterstützte Dienste wurde wiederhergestellt und aktualisiert und umfasst nun nur die AWS Dienste, bei denen derzeit keine Ereignisse protokolliert werden. CloudTrail Siehe <a href="#">Von CloudTrail nicht unterstützte Services</a> .	7. Oktober 2019

## [Aktualisierung der Dokumentation](#)

Die Dokumentation wurde mit Änderungen an der `AWSCloudTrailFullAccess`-Richtlinie aktualisiert. Ein Richtlinienbeispiel, das gleichwertige Berechtigungen für `AWSCloudTrailFullAccess` zeigt, wurde aktualisiert, um die Ressourcen, auf die die Aktion `iam:PassRole` angewendet werden kann, auf diejenigen zu beschränken, die der folgenden Bedingungsanweisung entsprechen: `"iam:PassedToService": "cloudtrail.amazonaws.com"`.  
Siehe [Beispiele für identitätsbasierte AWS CloudTrail-Richtlinien](#).

24. September 2019

## [Aktualisierung der Dokumentation](#)

Die Dokumentation wurde um ein neues Thema, die [Verwaltung der CloudTrail Kosten](#), aktualisiert, damit Sie die benötigten Protokoll Daten abrufen CloudTrail und gleichzeitig Ihr Budget einhalten können.

03. September 2019

## [Zusätzlicher Service-Support](#)

Diese Version unterstützt AWS Control Tower. Siehe [Von AWS CloudTrail unterstützte Services und Integrationen](#).

13. August 2019

<a href="#">Unterstützung einer weiteren Region hinzugefügt</a>	Diese Version unterstützt eine zusätzliche Region: Naher Osten (Bahrain). Siehe <a href="#">Regionen mit AWS CloudTrail -Unterstützung</a> .	29. Juli 2019
<a href="#">Aktualisierung der Dokumentation</a>	Die Dokumentation wurde mit Informationen zur Sicherheit von aktualisiert CloudTrail. Weitere Informationen finden Sie unter <a href="#">Sicherheit in AWS CloudTrail</a> .	3. Juli 2019
<a href="#">Zusätzlicher Service-Support</a>	Diese Version unterstützt AWS Ground Station. Siehe <a href="#">Von AWS CloudTrail unterstützte Services und Integrationen</a> .	6. Juni 2019
<a href="#">Zusätzlicher Service-Support</a>	Diese Version unterstützt AWS IoT Things Graph. Siehe <a href="#">Von AWS CloudTrail unterstützte Services und Integrationen</a> .	4. Juni 2019
<a href="#">Zusätzlicher Service-Support</a>	Diese Version unterstützt Amazon AppStream 2.0. Siehe <a href="#">Von AWS CloudTrail unterstützte Services und Integrationen</a> .	25. April 2019
<a href="#">Unterstützung einer weiteren Region hinzugefügt</a>	Diese Version unterstützt eine zusätzliche Region: Asien-Pazifik (Hongkong). Siehe <a href="#">Regionen mit AWS CloudTrail -Unterstützung</a> .	24. April 2019



<a href="#">Zusätzlicher Service-Support</a>	Diese Version unterstützt Amazon Managed Service für Apache Flink. Siehe <a href="#">Von AWS CloudTrail unterstützte Services und Integrationen</a> .	22. März 2019
<a href="#">Zusätzlicher Service-Support</a>	Diese Version unterstützt AWS Backup. Siehe <a href="#">Von AWS CloudTrail unterstützte Services und Integrationen</a> .	4. Februar 2019
<a href="#">Zusätzlicher Service-Support</a>	Diese Version unterstützt Amazon WorkLink. Siehe <a href="#">Von AWS CloudTrail unterstützte Services und Integrationen</a> .	23. Januar 2019
<a href="#">Zusätzlicher Service-Support</a>	Diese Version unterstützt AWS Cloud9. Siehe <a href="#">Von AWS CloudTrail unterstützte Services und Integrationen</a> .	21. Januar 2019
<a href="#">Zusätzlicher Service-Support</a>	Diese Version unterstützt AWS Elemental MediaLive. Siehe <a href="#">Von AWS CloudTrail unterstützte Services und Integrationen</a> .	19. Januar 2019
<a href="#">Zusätzlicher Service-Support</a>	Diese Version unterstützt Amazon Comprehend. Siehe <a href="#">Von AWS CloudTrail unterstützte Services und Integrationen</a> .	18. Januar 2019
<a href="#">Zusätzlicher Service-Support</a>	Diese Version unterstützt AWS Elemental MediaPackage. Siehe <a href="#">Von AWS CloudTrail unterstützte Services und Integrationen</a> .	21. Dezember 2018

<a href="#">Unterstützung einer weiteren Region hinzugefügt</a>	Diese Version unterstützt eine zusätzliche Region: EU (Stockholm). Siehe <a href="#">Regionen mit AWS CloudTrail -Unterstützung</a> .	11. Dezember 2018
<a href="#">Aktualisierung der Dokumentation</a>	Die Dokumentation wurde mit Informationen über unterstützte und nicht unterstützte Services aktualisiert. Siehe <a href="#">Von AWS CloudTrail unterstützte Services und Integrationen</a> .	3. Dezember 2018
<a href="#">Zusätzlicher Service-Support</a>	Diese Version unterstützt AWS Resource Access Manager (AWS RAM). Siehe <a href="#">Von AWS CloudTrail unterstützte Services und Integrationen</a> .	20. November 2018
<a href="#">Aktualisierte Funktionalität</a>	Diese Version unterstützt die Erstellung eines Trails CloudTrail , in dem Ereignisse für alle AWS Konten in einer Organisation protokolliert werden. Siehe <a href="#">Erstellen eines Trails für eine Organisation</a> .	19. November 2018
<a href="#">Zusätzlicher Service-Support</a>	Diese Version unterstützt Amazon Pinpoint SMS und die Sprach-API. Siehe <a href="#">Von AWS CloudTrail unterstützte Services und Integrationen</a> .	16. November 2018

---

<a href="#">Zusätzlicher Service-Support</a>	Diese Version unterstützt AWS IoT Greengrass. Siehe <a href="#">Von AWS CloudTrail unterstützte Services und Integrationen</a> .	29. Oktober 2018
<a href="#">Aktualisierte Dokumentation</a>	Dieses Update unterstützt die folgende Patch-Version für die CloudTrail Processing Library: Aktualisieren Sie die Dateiverweise auf die .jar-Datei im Benutzerhandbuch, um die neueste Version, aws-cloudtrail-processing-library-1.1.3.jar, zu verwenden. <a href="#">Weitere Informationen finden Sie unter Verwenden der CloudTrail Verarbeitungsbibliothek und der CloudTrail Verarbeitungsbibliothek unter GitHub</a>	18. Oktober 2018
<a href="#">Hinzugefügte Funktionalität</a>	Diese Version unterstützt die Verwendung zusätzlicher Filter unter Event history (Ereignisverlauf). Siehe <a href="#">CloudTrail Ereignisse in der CloudTrail Konsole anzeigen</a> .	18. Oktober 2018
<a href="#">Hinzugefügte Funktionalität</a>	Diese Version unterstützt die Verwendung von Amazon Virtual Private Cloud (Amazon VPC), um eine private Verbindung zwischen Ihrer VPC und AWS CloudTrail. Siehe <a href="#">AWS CloudTrail Mit Interface VPC-Endpoints</a> verwenden.	9. August 2018

<a href="#">Zusätzlicher Service-Support</a>	Diese Version unterstützt Amazon Data Lifecycle Manager. Siehe <a href="#">Von AWS CloudTrail unterstützte Services und Integrationen</a> .	24. Juli 2018
<a href="#">Zusätzlicher Service-Support</a>	Diese Version unterstützt Amazon MQ. Siehe <a href="#">Von AWS CloudTrail unterstützte Services und Integrationen</a> .	19. Juli 2018
<a href="#">Zusätzlicher Service-Support</a>	Diese Version unterstützt AWS Mobile CLI. Siehe <a href="#">Von AWS CloudTrail unterstützte Services und Integrationen</a> .	29. Juni 2018
<a href="#">AWS CloudTrail Benachrichtigung über den Dokumentationsverlauf als RSS-Feed verfügbar</a>	Sie können jetzt Benachrichtigungen über Aktualisierungen der AWS CloudTrail Dokumentation erhalten, indem Sie einen RSS-Feed abonnieren.	29. Juni 2018

## Frühere Aktualisierungen

In der folgenden Tabelle wird der Versionsverlauf der Dokumentation AWS CloudTrail vor dem 29. Juni 2018 beschrieben.

Änderung	Beschreibung	Veröffentlichungsdatum
Zusätzlicher Service-Support	Diese Version unterstützt Amazon RDS Performance Insights. Weitere Informationen finden Sie unter <a href="#">CloudTrail Unterstützte Dienste und Integrationen</a> .	21. Juni 2018

Änderung	Beschreibung	Veröffentlichungsdatum
Hinzugefügte Funktionalität	Diese Version unterstützt die Protokollierung aller CloudTrail Verwaltungsereignisse im Ereignisverlauf. Weitere Informationen finden Sie unter <a href="#">Mit dem CloudTrail Eventverlauf arbeiten</a> .	14. Juni 2018
Zusätzlicher Service-Support	Diese Version unterstützt AWS Billing and Cost Management. Siehe <a href="#">CloudTrail unterstützte Dienste und Integrationen</a> .	7. Juni 2018
Zusätzlicher Service-Support	Diese Version unterstützt Amazon Elastic Container Service for Kubernetes (Amazon EKS). Siehe <a href="#">CloudTrail unterstützte Dienste und Integrationen</a> .	5. Juni 2018
Aktualisierte Dokumentation	<p>Dieses Update unterstützt die folgende Patch-Version für die CloudTrail Processing Library:</p> <ul style="list-style-type: none"> <li>• Aktualisieren Sie die Dateiverweise auf die .jar-Datei im Benutzerhandbuch, um die neueste Version, aws-cloudtrail-processing-library -1.1.2.jar, zu verwenden.</li> </ul> <p><a href="#">Weitere Informationen finden Sie unter Verwendung der CloudTrail Processing Library und in der Processing Library unter CloudTrail . GitHub</a></p>	16. Mai 2018
Zusätzlicher Service-Support	Diese Version unterstützt AWS Billing and Cost Management. Siehe <a href="#">CloudTrail unterstützte Dienste und Integrationen</a> .	7. Juni 2018
Zusätzlicher Service-Support	Diese Version unterstützt Amazon Elastic Container Service for Kubernetes (Amazon EKS). Siehe <a href="#">CloudTrail unterstützte Dienste und Integrationen</a> .	5. Juni 2018

Änderung	Beschreibung	Veröffentlichungsdatum
Aktualisierte Dokumentation	<p>Dieses Update unterstützt die folgende Patch-Version für die CloudTrail Processing Library:</p> <ul style="list-style-type: none"><li>• Aktualisieren Sie die Dateiverweise auf die .jar-Datei im Benutzerhandbuch, um die neueste Version, aws-cloudtrail-processing-library -1.1.2.jar, zu verwenden.</li></ul> <p><a href="#">Weitere Informationen finden Sie unter Verwendung der CloudTrail Processing Library und in der Processing Library unter CloudTrail . GitHub</a></p>	16. Mai 2018
Zusätzlicher Service-Support	Diese Version unterstützt AWS X-Ray. Siehe <a href="#">CloudTrail unterstützte Dienste und Integrationen</a> .	25. April 2018
Zusätzlicher Service-Support	Diese Version unterstützt AWS IoT Analytics. Siehe <a href="#">CloudTrail unterstützte Dienste und Integrationen</a> .	23. April 2018
Zusätzlicher Service-Support	Diese Version unterstützt Secrets Manager. Siehe <a href="#">CloudTrail unterstützte Dienste und Integrationen</a> .	10. April 2018
Zusätzlicher Service-Support	Diese Version unterstützt Amazon Rekognition. Siehe <a href="#">CloudTrail unterstützte Dienste und Integrationen</a> .	6. April 2018
Zusätzlicher Service-Support	Diese Version unterstützt AWS Private Certificate Authority (PCA). Siehe <a href="#">CloudTrail unterstützte Dienste und Integrationen</a> .	4. April 2018

Änderung	Beschreibung	Veröffentlichungsdatum
Hinzugefügte Funktionalität	Diese Version unterstützt die Vereinfachung der Suche nach CloudTrail Protokolldateien mit Amazon Athena. Sie können automatisch Tabellen für die Abfrage von Protokollen direkt von der CloudTrail Konsole erstellen und diese Tabellen verwenden, um Abfragen in Athena auszuführen. Weitere Informationen finden Sie unter <a href="#">CloudTrail unterstützte Dienste und Integrationen</a> und <a href="#">Eine Tabelle für CloudTrail Protokolle in der CloudTrail Konsole erstellen</a> .	15. März 2018
Zusätzlicher Service-Support	Diese Version unterstützt AWS AppSync. Siehe <a href="#">CloudTrail unterstützte Dienste und Integrationen</a> .	13. Februar 2018
Zusätzliche Unterstützung für Regionen hinzugefügt	Diese Version unterstützt eine zusätzliche Region: Asien-Pazifik (Osaka) (ap-northeast-3). Siehe <a href="#">CloudTrail unterstützte Regionen</a> .	12. Februar 2018
Zusätzlicher Service-Support	Diese Version unterstützt AWS Shield. Siehe <a href="#">CloudTrail unterstützte Dienste und Integrationen</a> .	12. Februar 2018
Zusätzlicher Service-Support	Diese Version unterstützt Amazon SageMaker. Siehe <a href="#">CloudTrail unterstützte Dienste und Integrationen</a> .	11. Januar 2018
Zusätzlicher Service-Support	Diese Version unterstützt AWS Batch. Siehe <a href="#">CloudTrail unterstützte Dienste und Integrationen</a> .	10. Januar 2018
Hinzugefügte Funktionalität	Diese Version unterstützt die Verlängerung der Anzahl der Kontoaktivitäten, die im CloudTrail Event-Verlauf verfügbar sind, auf 90 Tage. Sie können auch die Anzeige der Spalten anpassen, um die Übersicht Ihrer CloudTrail Ereignisse zu verbessern. Weitere Informationen finden Sie unter <a href="#">Mit dem CloudTrail Eventverlauf arbeiten</a> .	12. Dezember 2017

Änderung	Beschreibung	Veröffentlichungsdatum
Zusätzlicher Service-Support	Diese Version unterstützt Amazon WorkMail. Siehe <a href="#">CloudTrail unterstützte Dienste und Integrationen</a> .	12. Dezember 2017
Zusätzlicher Service-Support	Diese Version unterstützt Alexa for Business, AWS Elemental MediaConvert, und AWS Elemental MediaStore. Siehe <a href="#">CloudTrail unterstützte Dienste und Integrationen</a> .	1. Dezember 2017
Erweiterte Funktionen und Dokumentationen	Diese Version unterstützt die Protokollierung von Datenereignissen für AWS Lambda Funktionen.  Weitere Informationen finden Sie unter <a href="#">Protokollieren von Datenereignissen</a> .	30. November 2017
Erweiterte Funktionen und Dokumentationen	Diese Version unterstützt die Protokollierung von Datenereignissen für AWS Lambda Funktionen.  Weitere Informationen finden Sie unter <a href="#">Protokollieren von Datenereignissen</a> .	30. November 2017
Erweiterte Funktionen und Dokumentationen	Diese Version unterstützt die folgenden Updates der CloudTrail Processing Library:  <ul style="list-style-type: none"> <li>• Neu: Unterstützung für die boolesche Identifizierung von Verwaltungsereignissen</li> <li>• Aktualisieren Sie die CloudTrail Event-Version auf 1.06.</li> </ul> Weitere Informationen finden Sie unter <a href="#">Verwendung der CloudTrail Processing Library</a> und in der <a href="#">CloudTrail Processing Library</a> unter GitHub.	30. November 2017



Änderung	Beschreibung	Veröffentlichungsdatum
Zusätzlicher Service-Support	Diese Version unterstützt AWS Glue. Siehe <a href="#">CloudTrail unterstützte Dienste und Integrationen</a> .	7. November 2017
Neue Dokumentation	In dieser Version wurde ein neues Thema <a href="#">Kontingente in AWS CloudTrail</a> hinzugefügt.	19. Oktober 2017
Aktualisierte Dokumentation	Diese Version aktualisiert die Dokumentation der unterstützten APIs im CloudTrail Event-Verlauf für Amazon Athena AWS CodeBuild, Amazon Elastic Container Registry und AWS Migration Hub.	13. Oktober 2017
Zusätzlicher Service-Support	Diese Version unterstützt Amazon Chime. Siehe <a href="#">CloudTrail unterstützte Dienste und Integrationen</a> .	27. September 2017
Erweiterte Funktionen und Dokumentationen	Diese Version unterstützt die Konfiguration der Datenereignisprotokollierung für alle Amazon S3 S3-Buckets in Ihrem AWS Konto. Siehe <a href="#">Protokollieren von Datenereignissen</a> .	20. September 2017
Zusätzlicher Service-Support	Diese Version unterstützt Amazon Lex. Siehe <a href="#">CloudTrail unterstützte Dienste und Integrationen</a> .	15. August 2017
Zusätzlicher Service-Support	Diese Version unterstützt AWS Migration Hub. Siehe <a href="#">CloudTrail unterstützte Dienste und Integrationen</a> .	14. August 2017
Erweiterte Funktionen und Dokumentationen	Diese Version unterstützt CloudTrail die standardmäßige Aktivierung für alle AWS Konten. Die Kontoaktivitäten der letzten sieben Tage sind im CloudTrail Eventverlauf verfügbar, und die neuesten Ereignisse werden im Konsolen-Dashboard angezeigt. Die Funktion, die bisher als API-Aktivitätsverlauf bezeichnet wurde, wurde durch den Ereignisverlauf ersetzt.	14. August 2017

Änderung	Beschreibung	Veröffentlichungsdatum
Erweiterte Funktionen und Dokumentationen	<p>Diese Version unterstützt das Herunterladen von Ereignissen von der CloudTrail Konsole auf der Seite mit dem API-Aktivitätsverlauf. Sie können Ereignisse im JSON- oder CSV-Format herunterladen.</p> <p>Weitere Informationen finden Sie unter <a href="#">Herunterladen von Ereignissen</a>.</p>	27. Juli 2017
Hinzugefügte Funktionalität	<p>Diese Version unterstützt die Protokollierung von API-Operationen auf Amazon-S3-Objektebene in zwei weiteren Regionen: Europa (London) und Kanada (Zentral).</p> <p>Weitere Informationen finden Sie unter <a href="#">Mit CloudTrail Protokolldateien arbeiten</a>.</p>	19. Juli 2017
Zusätzlicher Service-Support	<p>Diese Version unterstützt das Nachschlagen von APIs für Amazon CloudWatch Events in der CloudTrail API-Aktivitätsverlaufsfunktion.</p>	27. Juni 2017
Erweiterte Funktionen und Dokumentationen	<p>Diese Version unterstützt zusätzliche APIs in der CloudTrail API-Aktivitätsverlaufsfunktion für die folgenden Dienste:</p> <ul style="list-style-type: none"><li>• AWS CloudHSM</li><li>• Amazon Cognito</li><li>• Amazon-DynamoDB</li><li>• Amazon EC2</li><li>• Kinesis</li><li>• AWS Storage Gateway</li></ul>	27. Juni 2017

Änderung	Beschreibung	Veröffentlichungsdatum
Zusätzlicher Service-Support	Diese Version unterstützt AWS CodeStar. Siehe <a href="#">CloudTrail unterstützte Dienste und Integrationen</a> .	14. Juni 2017
Erweiterte Funktionen und Dokumentationen	<p>Diese Version unterstützt die folgenden Aktualisierungen der CloudTrail Processing Library:</p> <ul style="list-style-type: none"><li>• Unterstützung für verschiedene Formate für SQS-Nachrichten aus derselben SQS-Warteschlange hinzugefügt, um CloudTrail Protokolldateien zu identifizieren. Folgende Formate werden unterstützt:<ul style="list-style-type: none"><li>• Benachrichtigungen, die CloudTrail an ein SNS-Thema gesendet werden</li><li>• Benachrichtigungen, die von Amazon S3 an ein SNS-Thema gesendet werden</li><li>• Benachrichtigungen, die von Amazon S3 direkt an eine SQS-Warteschlange gesendet werden</li></ul></li><li>• Hinzufügung von Unterstützung für die Eigenschaft <code>deleteMessageUponFailure</code>, die Sie verwenden können, um Nachrichten zu löschen, die nicht verarbeitet werden können.</li></ul> <p>Weitere Informationen finden Sie unter <a href="#">Verwendung der CloudTrail Processing Library</a> und in der <a href="#">CloudTrail Processing Library</a> unter GitHub.</p>	1. Juni 2017
Zusätzlicher Service-Support	Diese Version unterstützt Amazon Athena. Siehe <a href="#">CloudTrail unterstützte Dienste und Integrationen</a> .	19. Mai 2017

Änderung	Beschreibung	Veröffentlichungsdatum
Hinzugefügte Funktionalität	<p>Diese Version unterstützt das Senden von Datenereignissen an Amazon CloudWatch Logs.</p> <p>Weitere Informationen zur Konfiguration Ihres Trails für die Protokollierung von Datenereignissen finden Sie unter <a href="#">Datenereignisse</a>.</p> <p>Weitere Informationen zum Senden von Ereignissen an CloudWatch Logs finden Sie unter <a href="#">Überwachung von CloudTrail Protokolldateien mit Amazon CloudWatch Logs</a>.</p>	9. Mai 2017
Zusätzlicher Service-Support	Diese Version unterstützt den AWS Marketplace Messdienst. Siehe <a href="#">CloudTrail unterstützte Dienste und Integrationen</a> .	2. Mai 2017
Zusätzlicher Service-Support	Diese Version unterstützt Amazon QuickSight. Siehe <a href="#">CloudTrail unterstützte Dienste und Integrationen</a> .	28. April 2017
Erweiterte Funktionen und Dokumentationen	Diese Version unterstützt eine aktualisierte Konsolenumgebung für die Erstellung neuer Trails. Sie können jetzt einen neuen Trail konfigurieren, um Verwaltungs- und Datenereignisse zu protokollieren. Weitere Informationen finden Sie unter <a href="#">Erstellen eines Trails</a> .	11. April 2017

Änderung	Beschreibung	Veröffentlichungsdatum
Erweiterte Dokumentationen	<p>Wenn CloudTrail in Ihrem Konto keine Protokolle an Ihren S3-Bucket gesendet oder keine SNS-Benachrichtigungen aus einigen Regionen gesendet werden, müssen Sie möglicherweise die Richtlinien aktualisieren.</p> <p>Weitere Informationen zum Aktualisieren der S3-Bucket-Richtlinien finden Sie unter <a href="#">Häufige Konfigurationsfehler in der Amazon-S3-Richtlinie</a>.</p> <p>Weitere Informationen zum Aktualisieren der SNS-Themariichtlinie finden Sie unter <a href="#">CloudTrail sendet keine Benachrichtigungen für eine Region</a>.</p>	31. März 2017
Zusätzlicher Service-Support	Diese Version unterstützt AWS Organizations. Siehe <a href="#">CloudTrail unterstützte Dienste und Integrationen</a> .	27. Februar 2017
Erweiterte Funktionen und Dokumentationen	Diese Version unterstützt eine aktualisierte Konsolenumgebung für die Konfiguration von Trails zur Protokollierung von Verwaltungs- und Datenereignissen. Weitere Informationen finden Sie unter <a href="#">Mit CloudTrail Protokolldateien arbeiten</a> .	10. Februar 2017
Zusätzlicher Service-Support	Diese Version unterstützt Amazon Cloud Directory. Siehe <a href="#">CloudTrail unterstützte Dienste und Integrationen</a> .	26. Januar 2017
Erweiterte Funktionen und Dokumentationen	Diese Version unterstützt das Nachschlagen von APIs für AWS CodeCommit Amazon GameLift und AWS Managed Services im CloudTrail API-Aktivitätsverlauf.	26. Januar 2017

Änderung	Beschreibung	Veröffentlichungsdatum
Hinzugefügte Funktionalität	<p>Diese Version unterstützt die Integration mit AWS Health Dashboard.</p> <p>Sie können den verwenden AWS Health Dashboard , um festzustellen, ob Ihre Trails keine Logs an ein SNS-Thema oder einen S3-Bucket übermitteln können. Dies kann der Fall sein, wenn ein Problem mit der Richtlinie für den S3-Bucket oder das SNS-Thema vorliegt. AWS Health Dashboard informiert Sie über die betroffenen Trails und empfiehlt Möglichkeiten zur Behebung der Richtlinie.</p> <p>Weitere Informationen finden Sie im <a href="#">AWS Health - Benutzerhandbuch</a>.</p>	24. Januar 2017
Erweiterte Funktionen und Dokumentationen	<p>Diese Version unterstützt das Filtern nach Ereignisquelle in der CloudTrail Konsole. Die Ereignisquelle zeigt den AWS Dienst an, an den die Anfrage gestellt wurde.</p> <p>Weitere Informationen finden Sie unter <a href="#">Aktuelle Verwaltungsereignisse mit der Konsole anzeigen</a>.</p>	12. Januar 2017
Zusätzlicher Service-Support	Diese Version unterstützt AWS CodeCommit. Siehe <a href="#">CloudTrail unterstützte Dienste und Integrationen</a> .	11. Januar 2017
Zusätzlicher Service-Support	Diese Version unterstützt Amazon Lightsail. Siehe <a href="#">CloudTrail unterstützte Dienste und Integrationen</a> .	23. Dezember 2016
Zusätzlicher Service-Support	Diese Version unterstützt AWS Managed Services. Siehe <a href="#">CloudTrail unterstützte Dienste und Integrationen</a> .	21. Dezember 2016

Änderung	Beschreibung	Veröffentlichungsdatum
Zusätzliche Unterstützung für Regionen hinzugefügt	Diese Version unterstützt die Region Europa (London). Siehe <a href="#">CloudTrail unterstützte Regionen</a> .	13. Dezember 2016
Zusätzliche Unterstützung für Regionen hinzugefügt	Diese Version unterstützt die Region Kanada (Zentral). Siehe <a href="#">CloudTrail unterstützte Regionen</a> .	8. Dezember 2016
Zusätzlicher Service-Support	Diese Version unterstützt AWS CodeBuild See <a href="#">CloudTrail unterstützte Dienste und Integrationen</a> .  Diese Version unterstützt AWS Health. Siehe <a href="#">CloudTrail unterstützte Dienste und Integrationen</a> .  Diese Version unterstützt AWS Step Functions. Siehe <a href="#">CloudTrail unterstützte Dienste und Integrationen</a> .	1. Dezember 2016
Zusätzlicher Service-Support	Diese Version unterstützt Amazon Polly. Siehe <a href="#">CloudTrail unterstützte Dienste und Integrationen</a> .	30. November 2016
Zusätzlicher Service-Support	Diese Version unterstützt AWS OpsWorks for Chef Automate. Siehe <a href="#">CloudTrail unterstützte Dienste und Integrationen</a> .	23. November 2016

Änderung	Beschreibung	Veröffentlichungsdatum
Erweiterte Funktionen und Dokumentationen	<p>Diese Version unterstützt die Konfiguration Ihres Trails für die Protokollierung von schreibgeschützten, lesegeschützten oder allen Ereignissen.</p> <p>CloudTrail unterstützt die Protokollierung von Amazon S3 S3-API-Operationen auf Objektebene wie <code>GetObject</code>, <code>PutObject</code>, und <code>DeleteObject</code>. Sie können Ihre Trails so konfigurieren, dass API-Operationen auf Objektebene protokolliert werden.</p> <p>Weitere Informationen finden Sie unter <a href="#">Mit CloudTrail Protokolldateien arbeiten</a>.</p>	21. November 2016
Erweiterte Funktionen und Dokumentationen	<p>Diese Version unterstützt zusätzliche Werte für das <code>type</code>-Feld im <code>userIdentity</code>-Element: <code>AWSAccount</code> und <code>AWSService</code>. Weitere Informationen finden Sie unter <a href="#">Felder für userIdentity</a>.</p>	16. November 2016
Zusätzlicher Service-Support	<p>Diese Version unterstützt Application Auto Scaling. Siehe <a href="#">CloudTrail unterstützte Dienste und Integrationen</a>.</p>	31. Oktober 2016
Zusätzliche Unterstützung für Regionen hinzugefügt	<p>Diese Version unterstützt die Region USA Ost (Ohio). Siehe <a href="#">CloudTrail unterstützte Regionen</a>.</p>	17. Oktober 2016
Erweiterte Funktionen und Dokumentationen	<p>Diese Version unterstützt die Protokollierung von AWS Nicht-API-Serviceereignissen. Weitere Informationen finden Sie unter <a href="#">AWS Serviceereignisse</a>.</p>	23. September 2016
Erweiterte Funktionen und Dokumentationen	<p>Diese Version unterstützt die Verwendung der CloudTrail Konsole zum Anzeigen von Ressourcentypen, die von AWS Config unterstützt werden. Weitere Informationen finden Sie unter <a href="#">Anzeigen von mit AWS Config referenzierten Ressourcen</a>.</p>	7. Juli 2016



Änderung	Beschreibung	Veröffentlichungsdatum
Zusätzlicher Service-Support	Diese Version unterstützt AWS Service Catalog. Siehe <a href="#">CloudTrail unterstützte Dienste und Integrationen</a> .	6. Juli 2016
Zusätzlicher Service-Support	Diese Version unterstützt Amazon Elastic File System (Amazon EFS). Siehe <a href="#">CloudTrail unterstützte Dienste und Integrationen</a> .	28. Juni 2016
Zusätzliche Unterstützung für Regionen hinzugefügt	Diese Version unterstützt eine zusätzliche Region: ap-south-1 (Asien-Pazifik (Mumbai)). Siehe <a href="#">CloudTrail unterstützte Regionen</a> .	27. Juni 2016
Zusätzlicher Service-Support	Diese Version unterstützt AWS Application Discovery Service. Siehe <a href="#">CloudTrail unterstützte Dienste und Integrationen</a> .	12. Mai 2016
Zusätzlicher Service-Support	Diese Version unterstützt CloudWatch Logs in der Region Südamerika (São Paulo). Weitere Informationen finden Sie unter <a href="#">Überwachung von CloudTrail Protokolldateien mit Amazon CloudWatch Logs</a> .	6. Mai 2016
Zusätzlicher Service-Support	Diese Version unterstützt AWS WAF. Siehe <a href="#">CloudTrail unterstützte Dienste und Integrationen</a> .	28. April 2016
Zusätzlicher Service-Support	Diese Version unterstützt AWS Support. Siehe <a href="#">CloudTrail unterstützte Dienste und Integrationen</a> .	21. April 2016
Zusätzlicher Service-Support	Diese Version unterstützt Amazon Inspector. Siehe <a href="#">CloudTrail unterstützte Dienste und Integrationen</a> .	20. April 2016
Zusätzlicher Service-Support	Diese Version unterstützt AWS IoT. Siehe <a href="#">CloudTrail unterstützte Dienste und Integrationen</a> .	11. April 2016

Änderung	Beschreibung	Veröffentlichungsdatum
Erweiterte Funktionen und Dokumentationen	Diese Version unterstützt Logging AWS Security Token Service (AWS STS) -API-Aufrufe, die mit Security Assertion Markup Language (SAML) und Web Identity Federation getätigt wurden. Weitere Informationen finden Sie unter <a href="#">Werte für AWS STS APIs mit SAML und Web-Identitätsverbund</a> .	28. März 2016
Zusätzlicher Service-Support	Diese Version unterstützt AWS Certificate Manager. Siehe <a href="#">CloudTrail unterstützte Dienste und Integrationen</a> .	25. März 2016
Zusätzlicher Service-Support	Diese Version unterstützt Amazon Data Firehose. Siehe <a href="#">CloudTrail unterstützte Dienste und Integrationen</a> .	17. März 2016
Zusätzlicher Service-Support	Diese Version unterstützt Amazon CloudWatch Logs. Siehe <a href="#">CloudTrail unterstützte Dienste und Integrationen</a> .	10. März 2016
Zusätzlicher Service-Support	Diese Version unterstützt Amazon Cognito. Siehe <a href="#">CloudTrail unterstützte Dienste und Integrationen</a> .	18. Februar 2016
Zusätzlicher Service-Support	Diese Version unterstützt AWS Database Migration Service. Siehe <a href="#">CloudTrail unterstützte Dienste und Integrationen</a> .	4. Februar 2016
Zusätzlicher Service-Support	Diese Version unterstützt Amazon GameLift (Amazon GameLift). Siehe <a href="#">CloudTrail unterstützte Dienste und Integrationen</a> .	27. Januar 2016
Zusätzlicher Service-Support	Diese Version unterstützt Amazon CloudWatch Events. Siehe <a href="#">CloudTrail unterstützte Dienste und Integrationen</a> .	16. Januar 2016

Änderung	Beschreibung	Veröffentlichungsdatum
Zusätzliche Unterstützung für Regionen hinzugefügt	Diese Version unterstützt eine zusätzliche Region: ap-northeast-2 (Asien-Pazifik (Seoul)). Siehe <a href="#">CloudTrail unterstützte Regionen</a> .	6. Januar 2016
Zusätzlicher Service-Support	Diese Version unterstützt Amazon Elastic Container Registry (Amazon ECR). Siehe <a href="#">CloudTrail unterstützte Dienste und Integrationen</a> .	21. Dezember 2015
Erweiterte Funktionen und Dokumentationen	Diese Version unterstützt die Aktivierung CloudTrail in allen Regionen und unterstützt mehrere Pfade pro Region. Weitere Informationen finden Sie unter <a href="#">Mit CloudTrail Trails arbeiten</a> .	17. Dezember 2015
Zusätzlicher Service-Support	Diese Version unterstützt Amazon Machine Learning. Siehe <a href="#">CloudTrail unterstützte Dienste und Integrationen</a> .	10. Dezember 2015
Erweiterte Funktionen und Dokumentationen	Diese Version unterstützt die Verschlüsselung von Protokolldateien, die Integritätsvalidierung von Protokolldateien sowie Markierungen. Weitere Informationen finden Sie unter <a href="#">CloudTrail Logdateien mit AWS KMS Schlüsseln verschlüsseln (SSE-KMS)</a> , <a href="#">Überprüfen der Integrität der CloudTrail Protokolldatei</a> und <a href="#">Aktualisieren eines Trails</a> .	1. Oktober 2015
Zusätzlicher Service-Support	Diese Version unterstützt Amazon OpenSearch Service. Siehe <a href="#">CloudTrail unterstützte Dienste und Integrationen</a> .	1. Oktober 2015
Zusätzlicher Service-Support	Diese Version unterstützt Ereignisse auf Amazon-S3-Bucket-Ebene. Siehe <a href="#">CloudTrail unterstützte Dienste und Integrationen</a> .	1. September 2015

Änderung	Beschreibung	Veröffentlichungsdatum
Zusätzlicher Service-Support	Diese Version unterstützt AWS Device Farm. Siehe <a href="#">CloudTrail unterstützte Dienste und Integrationen</a> .	13. Juli 2015
Zusätzlicher Service-Support	Diese Version unterstützt Amazon API Gateway. Siehe <a href="#">CloudTrail unterstützte Dienste und Integrationen</a> .	9. Juli 2015
Zusätzlicher Service-Support	Diese Version unterstützt CodePipeline. Siehe <a href="#">CloudTrail unterstützte Dienste und Integrationen</a> .	9. Juli 2015
Zusätzlicher Service-Support	Diese Version unterstützt Amazon DynamoDB. Siehe <a href="#">CloudTrail unterstützte Dienste und Integrationen</a> .	28. Mai 2015
Zusätzlicher Service-Support	Diese Version unterstützt CloudWatch Logs in der Region USA West (Nordkalifornien). Weitere Informationen zur CloudTrail Unterstützung der CloudWatch Protokollüberwachung finden Sie unter <a href="#">Überwachung von CloudTrail Protokolldateien mit Amazon CloudWatch Logs</a> .	19. Mai 2015
Zusätzlicher Service-Support	Diese Version unterstützt AWS Directory Service. Siehe <a href="#">CloudTrail unterstützte Dienste und Integrationen</a> .	14. Mai 2015
Zusätzlicher Service-Support	Diese Version unterstützt Amazon Simple Email Service (Amazon SES). Siehe <a href="#">CloudTrail unterstützte Dienste und Integrationen</a> .	7. Mai 2015
Zusätzlicher Service-Support	Diese Version unterstützt Amazon Elastic Container Service, siehe <a href="#">CloudTrail unterstützte Dienste und Integrationen</a> .	9. April 2015
Zusätzlicher Service-Support	Diese Version unterstützt AWS Lambda. Siehe <a href="#">CloudTrail unterstützte Dienste und Integrationen</a> .	9. April 2015

Änderung	Beschreibung	Veröffentlichungsdatum
Zusätzlicher Service-Support	Diese Version unterstützt Amazon WorkSpaces. Siehe <a href="#">CloudTrail unterstützte Dienste und Integrationen</a> .	9. April 2015
	Diese Version unterstützt die Suche nach AWS Aktivitäten, die von CloudTrail (CloudTrail Ereignissen) erfasst wurden. Sie können in Ihrem Konto Ereignisse im Zusammenhang mit dem Erstellen, Ändern oder Löschen abfragen und filtern. Um nach diesen Ereignissen zu suchen, können Sie die CloudTrail Konsole, das AWS Command Line Interface (AWS CLI) oder das AWS SDK verwenden. Weitere Informationen finden Sie unter <a href="#">Mit dem CloudTrail Eventverlauf arbeiten</a> .	12. März 2015
Support eines weiteren Services und neue Dokumentation	Diese Version unterstützt Amazon CloudWatch Logs in den Regionen Asien-Pazifik (Singapur), Asien-Pazifik (Sydney), Asien-Pazifik (Tokio) und Europa (Frankfurt). Weitere Informationen finden Sie unter <a href="#">Ereignisse an CloudWatch Logs senden</a> .	5. März 2015
Neue Dokumentation	Der Seite <a href="#">CloudTrail Konzepte</a> wurde ein neuer Abschnitt hinzugefügt, in dem die CloudTrail Unterstützung für AWS Security Token Service (AWS STS) regionale Endpunkte beschrieben wird.	17. Februar 2015
Zusätzlicher Service-Support	Diese Version unterstützt Amazon Route 53. Siehe <a href="#">CloudTrail unterstützte Dienste und Integrationen</a> .	11. Februar 2015
Zusätzlicher Service-Support	Diese Version unterstützt AWS Config. Siehe <a href="#">CloudTrail unterstützte Dienste und Integrationen</a> .	10. Februar 2015

Änderung	Beschreibung	Veröffentlichungsdatum
Zusätzlicher Service-Support	Diese Version unterstützt AWS CloudHSM. Siehe <a href="#">CloudTrail unterstützte Dienste und Integrationen</a> .	8. Januar 2015
Zusätzlicher Service-Support	Diese Version unterstützt AWS CodeDeploy. Siehe <a href="#">CloudTrail unterstützte Dienste und Integrationen</a> .	17. Dezember 2014
Zusätzlicher Service-Support	Diese Version unterstützt AWS Storage Gateway. Siehe <a href="#">CloudTrail unterstützte Dienste und Integrationen</a> .	16. Dezember 2014
Zusätzliche Unterstützung für Regionen hinzugefügt	Diese Version unterstützt eine weitere Region: us-gov-west -1 (AWS GovCloud (US-West)). Siehe <a href="#">CloudTrail unterstützte Regionen</a> .	16. Dezember 2014
Zusätzlicher Service-Support	Diese Version unterstützt Amazon S3 Glacier. Siehe <a href="#">CloudTrail unterstützte Dienste und Integrationen</a> .	11. Dezember 2014
Zusätzlicher Service-Support	Diese Version unterstützt AWS Data Pipeline. Siehe <a href="#">CloudTrail unterstützte Dienste und Integrationen</a> .	2. Dezember 2014
Zusätzlicher Service-Support	Diese Version unterstützt AWS Key Management Service. Siehe <a href="#">CloudTrail unterstützte Dienste und Integrationen</a> .	12. November 2014
Neue Dokumentation	Einer neuer Abschnitt, <a href="#">Überwachung von CloudTrail Protokolldateien mit Amazon CloudWatch Logs</a> , wurde dem Leitfaden hinzugefügt. Es beschreibt, wie Amazon CloudWatch Logs zur Überwachung von CloudTrail Protokollereignissen verwendet wird.	10. November 2014

Änderung	Beschreibung	Veröffentlichungsdatum
Neue Dokumentation	Einer neuer Abschnitt, <a href="#">Verwendung der CloudTrail Processing Library</a> , wurde dem Leitfaden hinzugefügt. Es enthält Informationen darüber, wie Sie mithilfe der AWS CloudTrail Processing Library einen CloudTrail Protokollprozessor in Java schreiben.	5. November 2014
Zusätzlicher Service-Support	Diese Version unterstützt Amazon Elastic Transcoder. Siehe <a href="#">CloudTrail unterstützte Dienste und Integrationen</a> .	27. Oktober 2014
Zusätzliche Unterstützung für Regionen hinzugefügt	Diese Version unterstützt eine zusätzliche Region: eu-central-1 (Europa (Frankfurt)). Siehe <a href="#">CloudTrail unterstützte Regionen</a> .	23. Oktober 2014
Zusätzlicher Service-Support	Diese Version unterstützt Amazon CloudSearch. Siehe <a href="#">CloudTrail unterstützte Dienste und Integrationen</a> .	16. Oktober 2014
Zusätzlicher Service-Support	Diese Version unterstützt Amazon Simple Notification Service. Siehe <a href="#">CloudTrail unterstützte Dienste und Integrationen</a> .	09. Oktober 2014
Zusätzlicher Service-Support	Diese Version unterstützt Amazon ElastiCache. Siehe <a href="#">CloudTrail unterstützte Dienste und Integrationen</a> .	15. September 2014
Zusätzlicher Service-Support	Diese Version unterstützt Amazon WorkDocs. Siehe <a href="#">CloudTrail unterstützte Dienste und Integrationen</a> .	27. August 2014
Zusätzliche neue Inhalte	Diese Version beinhaltet ein Thema, in dem die Protokollierung von Anmeldeereignissen erläutert wird. Siehe <a href="#">AWS Management Console Anmeldeereignisse</a> .	24. Juli 2014
Zusätzliche neue Inhalte	Das Element eventVersion für diese Version wurde auf die Version 1.02 aktualisiert und es wurden drei neue Felder hinzugefügt. Siehe <a href="#">CloudTrail Inhalt aufzeichnen</a> .	18. Juli 2014

Änderung	Beschreibung	Veröffentlichungsdatum
Zusätzlicher Service-Support	Diese Version unterstützt Auto Scaling (siehe <a href="#">CloudTrail unterstützte Dienste und Integrationen</a> ).	17. Juli 2014
Zusätzliche Unterstützung für Regionen hinzugefügt	Diese Version unterstützt drei zusätzliche Regionen: ap-southeast-1 (Asien-Pazifik (Singapur)), ap-northeast-1 (Asien-Pazifik (Tokio)), sa-east-1 (Südamerika (São Paulo)). Siehe <a href="#">CloudTrail unterstützte Regionen</a> .	30. Juni 2014
Zusätzlicher Service-Support	Diese Version unterstützt Amazon Redshift. Siehe <a href="#">CloudTrail unterstützte Dienste und Integrationen</a> .	10. Juni 2014
Zusätzlicher Service-Support	Diese Version unterstützt AWS OpsWorks. Siehe <a href="#">CloudTrail unterstützte Dienste und Integrationen</a> .	5. Juni 2014
Zusätzlicher Service-Support	Diese Version unterstützt Amazon CloudFront. Siehe <a href="#">CloudTrail unterstützte Dienste und Integrationen</a> .	28. Mai 2014
Zusätzliche Unterstützung für Regionen hinzugefügt	Diese Version unterstützt drei zusätzliche Regionen: us-west-1 (USA West (Nordkalifornien)), eu-west-1 (Europa (Irland)), ap-southeast-2 (Asien-Pazifik (Sydney)). Siehe <a href="#">CloudTrail unterstützte Regionen</a> .	13. Mai 2014
Zusätzlicher Service-Support	Diese Version unterstützt Amazon Simple Workflow Service. Siehe <a href="#">CloudTrail unterstützte Dienste und Integrationen</a> .	9. Mai 2014
Zusätzliche neue Inhalte	Diese Version beinhaltet Themen, in denen die Freigabe von Protokolldateien zwischen Konten erläutert wird. Siehe <a href="#">CloudTrail Protokolldateien zwischen AWS Konten teilen</a> .	2. Mai 2014
Zusätzlicher Service-Support	Diese Version unterstützt Amazon CloudWatch. Siehe <a href="#">CloudTrail unterstützte Dienste und Integrationen</a> .	28. April 2014



Änderung	Beschreibung	Veröffentlichungsdatum
Zusätzlicher Service-Support	Diese Version unterstützt Amazon Kinesis. Siehe <a href="#">CloudTrail unterstützte Dienste und Integrationen</a> .	22. April 2014
Zusätzlicher Service-Support	Diese Version unterstützt AWS Direct Connect. Siehe <a href="#">CloudTrail unterstützte Dienste und Integrationen</a> .	11. April 2014
Zusätzlicher Service-Support	Diese Version unterstützt Amazon EMR. Siehe <a href="#">CloudTrail unterstützte Dienste und Integrationen</a> .	4. April 2014
Zusätzlicher Service-Support	Diese Version unterstützt Elastic Beanstalk. Siehe <a href="#">CloudTrail unterstützte Dienste und Integrationen</a> .	2. April 2014
Zusätzlicher Service-Support	Diese Version unterstützt AWS CloudFormation. Siehe <a href="#">CloudTrail unterstützte Dienste und Integrationen</a> .	7. März 2014
Neues Handbuch	Mit dieser Version wird AWS CloudTrail eingeführt.	13. November 2013

# AWS-Glossar

Die neueste AWS-Terminologie finden Sie im [AWS-Glossar](#) in der AWS-Glossar-Referenz.

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.