



Benutzerhandbuch

Amazon Security Lake



Amazon Security Lake: Benutzerhandbuch

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

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

Table of Contents

Was ist Amazon Security Lake?	1
Überblick über Security Lake	2
Funktionen von Security Lake	2
Zugriff auf Security Lake	4
Zugehörige Services	4
Konzepte und Terminologie	6
Erste Schritte	8
Ersteinrichtung AWS-Konto	8
Melde dich an für ein AWS-Konto	8
Erstellen Sie einen Benutzer mit Administratorzugriff	9
Identifizieren Sie das Konto, das Sie verwenden werden, um Security Lake zu aktivieren	10
Überlegungen zur Aktivierung von Amazon Security Lake	10
Erste Schritte auf der Konsole	11
Schritt 1: Quellen konfigurieren	11
Schritt 2: Definieren Sie Speichereinstellungen und Rollup-Regionen (optional)	13
Schritt 3: Überprüfen und erstellen Sie einen Data Lake	13
Schritt 4: Ihre eigenen Daten anzeigen und abfragen	14
Schritt 5: Abonnenten erstellen	14
Programmgesteuerter Einstieg	14
Schritt 1: IAM-Rollen erstellen	14
Schritt 2: Amazon Security Lake aktivieren	15
Schritt 3: Quellen konfigurieren	17
Schritt 4: Speichereinstellungen und Rollup-Regionen konfigurieren (optional)	18
Schritt 5: Ihre eigenen Daten anzeigen und abfragen	19
Schritt 6: Abonnenten erstellen	19
Verwalten mehrerer Konten	20
Wichtige Überlegungen für delegierte Security-Lake-Administratoren	20
Erforderliche IAM-Berechtigungen zum Benennen des delegierten Administrators	22
Benennen des delegierten Security-Lake-Administrators und Hinzufügen von Mitgliedskonten	22
Entfernen des delegierten Security-Lake-Administrators	25
Vertrauenswürdiger Zugriff auf Security Lake	26
Verwalten von -Regionen	27
Der Status der Region wird überprüft	27

Regionseinstellungen ändern	28
Konfiguration von Rollup-Regionen	30
IAM-Rolle für die Datenreplikation	30
IAM-Rolle zur Registrierung von Partitionen AWS Glue	33
Rollup-Regionen hinzufügen	34
Rollup-Regionen aktualisieren oder entfernen	36
Verwaltung der Quellen	38
Erfassung von Daten von AWS-Services	38
Voraussetzung: Überprüfen Sie die Berechtigungen	39
CloudTrail Ereignisprotokolle	40
Amazon EKS-Auditprotokolle	42
Route-53-Resolver-Abfrageprotokolle	42
Ergebnisse von Security Hub	43
VPC Flow Logs	43
AWS WAF Logs	44
Eine als Quelle hinzufügen AWS-Service	45
Rollenberechtigungen werden aktualisiert	47
Die AmazonSecurityLakeMetaStoreManager Rolle wird gelöscht	48
AWS-Service Als Quelle entfernen	48
Den Status der Quellensammlung abrufen	50
Sammeln von Daten aus benutzerdefinierten Quellen	51
Bewährte Methoden für die Aufnahme benutzerdefinierter Quellen	52
Voraussetzungen für das Hinzufügen einer benutzerdefinierten Quelle	53
Eine benutzerdefinierte Quelle hinzufügen	57
Halten Sie die benutzerdefinierten Quelldaten auf dem neuesten Stand in AWS Glue	58
Löschen einer benutzerdefinierten Quelle	59
Abonnentenverwaltung	61
Zugriff auf Abonnentendaten	62
Voraussetzungen für die Erstellung eines Abonnenten mit Datenzugriff	62
Einen Abonnenten mit Datenzugriff erstellen	65
Beispiel für eine Objektbenachrichtigung	69
Aktualisierung eines Datenabonnenten	69
Einen Datenabonnenten entfernen	71
Zugriff auf Abonnentenanfragen	71
Voraussetzungen für die Erstellung eines Abonnenten mit Abfragezugriff	72
Einen Abonnenten mit Abfragezugriff erstellen	74

Einrichtung der kontenübergreifenden gemeinsamen Nutzung von Tabellen (Abbonnentenschritt)	76
Einen Abonnenten mit Abfragezugriff bearbeiten	78
Security-Lake-Abfragen	83
Security Lake fragt Version 1 ab	83
Quellentabelle für das Protokoll	83
Datenbank-Region	84
Datum der Partition	85
Beispielabfragen für CloudTrail Daten	87
Beispielabfragen für Route 53-Resolver-Abfrageprotokolle	89
Beispielabfragen für Security Hub Hub-Ergebnisse	91
Beispielabfragen für Amazon VPC Flow Logs	94
Security Lake fragt Version 2 ab	98
Protokollquellentabelle	83
Datenbank-Region	84
Datum der Partition	85
Security Lake-Observables abfragen	101
Abfragen nach Daten CloudTrail	87
Abfragen für Route 53-Resolver-Abfrageprotokolle	89
Abfragen zu Ergebnissen von Security Hub	91
Abfragen für Amazon-VPC-Flow-Protokolle	94
Abfragen für Amazon EKS-Auditprotokolle	112
Abfragen für v2-Protokolle AWS WAF	114
Verwaltung des Lebenszyklus	117
Verwaltung der Aufbewahrung	117
Konfiguration der Aufbewahrungseinstellungen bei der Aktivierung von Security Lake	117
Aufbewahrungseinstellungen werden aktualisiert	119
Regionen zusammenfassen	120
Offenes Cybersecurity Schema Framework (OCSF)	122
Was ist OCSF?	122
OCSF-Ereignisklassen	122
Identifizierung der OCSF-Quelle	122
Integrationen	126
AWS-Service Integrationen	126
AWS AppFabric Integration	126
Detective-Integration	127

OpenSearch Serviceintegration	128
QuickSight Amazon-Integration	128
SageMaker Integration	129
Integration mit Amazon Bedrock	129
Integration in Security Hub	130
Integrationen von Drittanbietern	131
Integration abfragen	132
Accenture – MxDR	133
Aqua Security	133
Barracuda – Email Protection	133
Booz Allen Hamilton	133
Bosch Software and Digital Solutions – AIShield	134
ChaosSearch	134
Cisco Security – Secure Firewall	134
Claroty – xDome	134
CMD Solutions	135
Confluent – Amazon S3 Sink Connector	135
Contrast Security	135
Cribl – Search	136
Cribl – Stream	136
CrowdStrike – Falcon Data Replicator	136
CyberArk – Unified Identify Security Platform	136
Cyber Security Cloud – Cloud Fastener	136
DataBahn	137
Darktrace – Cyber AI Loop	137
Datadog	137
Deloitte – MXDR Cyber Analytics and AI Engine (CAE)	137
Devo	138
DXC – SecMon	138
Eviden— Alsaac (früherAtos)	138
ExtraHop – Reveal(x) 360	138
Falcosidekick	139
Fortinet - Cloud Native Firewall	139
Gigamon – Application Metadata Intelligence	139
Hoop Cyber	139
IBM – QRadar	140

Infosys	140
Insbuilt	140
Kyndryl – AIOps	140
Lacework – Polygraph	141
Laminar	141
MegazoneCloud	141
Monad	141
NETSCOUT – Omnis Cyber Intelligence	142
Netskope – CloudExchange	142
New Relic ONE	142
Okta – Workforce Identity Cloud	142
Orca – Cloud Security Platform	143
Palo Alto Networks – Prisma Cloud	143
Palo Alto Networks – XSOAR	143
Panther	143
Ping Identity – PingOne	144
PwC – Fusion center	144
Query.AI – Query Federated Search	144
Rapid7 – InsightIDR	144
RipJar – Labyrinth for Threat Investigations	145
Sailpoint	145
Securonix	145
SentinelOne	145
Sentra – Data Lifecycle Security Platform	146
SOC Prime	146
Splunk	146
Stellar Cyber	147
Sumo Logic	147
Swimlane – Turbine	147
Sysdig Secure	147
Talon	147
Tanium	148
TCS	148
Tego Cyber	148
Tines – No-code security automation	149
Torq – Enterprise Security Automation Platform	149

Trellix – XDR	149
Trend Micro – CloudOne	149
Uptycs – Uptycs XDR	150
Vectra AI – Vectra Detect for AWS	150
VMware Aria Automation for Secure Clouds	150
Wazuh	151
Wipro	151
Wiz – CNAPP	151
Zscaler – Zscaler Posture Control	151
Sicherheit	152
Identity and Access Management	153
Zielgruppe	153
Authentifizierung mit Identitäten	154
Verwalten des Zugriffs mit Richtlinien	158
So funktioniert Amazon Security Lake mit IAM	161
Beispiele für identitätsbasierte Richtlinien	171
AWS verwaltete Richtlinien	176
Servicegebundene Rolle	198
Datenschutz	204
Verschlüsselung im Ruhezustand	205
Verschlüsselung während der Übertragung	208
Abmeldung von der Verwendung Ihrer Daten zur Serviceverbesserung	208
Compliance-Validierung	209
Bewährte Sicherheitsmethoden für Security Lake	210
Gewähren Sie Security Lake-Benutzern die geringstmöglichen Berechtigungen	210
Sehen Sie sich die Übersichtsseite an	211
In Security Hub integrieren	211
Achten Sie auf Security Lake-Ereignisse	211
Ausfallsicherheit	211
Sicherheit der Infrastruktur	213
Konfigurations- und Schwachstellenanalyse in Security Lake	213
Überwachung	213
CloudWatchMetriken Amazon Security Lake Lake Lake Lake Lake Lake Lake	214
Protokollieren von API-Aufrufen	217
Informationen zu Security Lake in CloudTrail	217
Grundlegendes zu Security Lake-Protokolldateieinträgen	218

Markieren von Ressourcen	220
Grundlagen der Markierung	220
Verwenden von Tags in IAM-Richtlinien	222
Hinzufügen von Tags zu Ressourcen	223
Überprüfen von Tags für -Ressourcen	226
Bearbeiten von Tags für Ressourcen	228
Entfernen von Tags von Ressourcen	230
Fehlerbehebung	234
Fehlerbehebung beim Data Lake-Status	234
Behebung von Problemen mit Lake Formation	235
Die Tabelle wurde nicht gefunden	235
400 AccessDenied	235
SYNTAX_ERROR: Zeile 1:8: SELECT * ist für eine Beziehung, die keine Spalten hat, nicht zulässig	236
Security Lake konnte den Prinzipal-ARN des Anrufers nicht zum Lake Formation Data Lake Admin hinzufügen. Aktuelle Data Lake-Administratoren schließen möglicherweise ungültige Principals ein, die nicht mehr existieren.	236
Security Lake CreateSubscriber with Lake Formation hat keine neue Einladung zur gemeinsamen Nutzung von RAM-Ressourcen erstellt, um akzeptiert zu werden	237
Problembehandlung bei Abfragen in Amazon Athena	237
Beim Abfragen werden keine neuen Objekte im Data Lake zurückgegeben	237
Auf AWS Glue Tabellen kann nicht zugegriffen werden	238
Behebung von Problemen mit Organizations	238
Beim Aufrufen des CreateDataLake Vorgangs ist ein Fehler aufgetreten: Ihr Konto muss das delegierte Administratorkonto für eine Organisation oder ein eigenständiges Konto sein.	238
Behebung von IAM-Problemen	239
Ich bin nicht berechtigt, eine Aktion in Security Lake durchzuführen	239
Ich bin nicht berechtigt, iam durchzuführen: PassRole	239
Ich möchte Personen außerhalb von mir den Zugriff AWS-Konto auf meine Security Lake-Ressourcen ermöglichen	240
Preise für Security Lake	241
Überprüfung der Nutzung und der geschätzten Kosten	242
Unterstützte	244
Deaktivieren von Security Lake	245
Häufig gestellte Fragen	247
Security Lake-Update auf die neueste Version von Parquet	247

Dokumentverlauf	249
.....	ccliv

Was ist Amazon Security Lake?

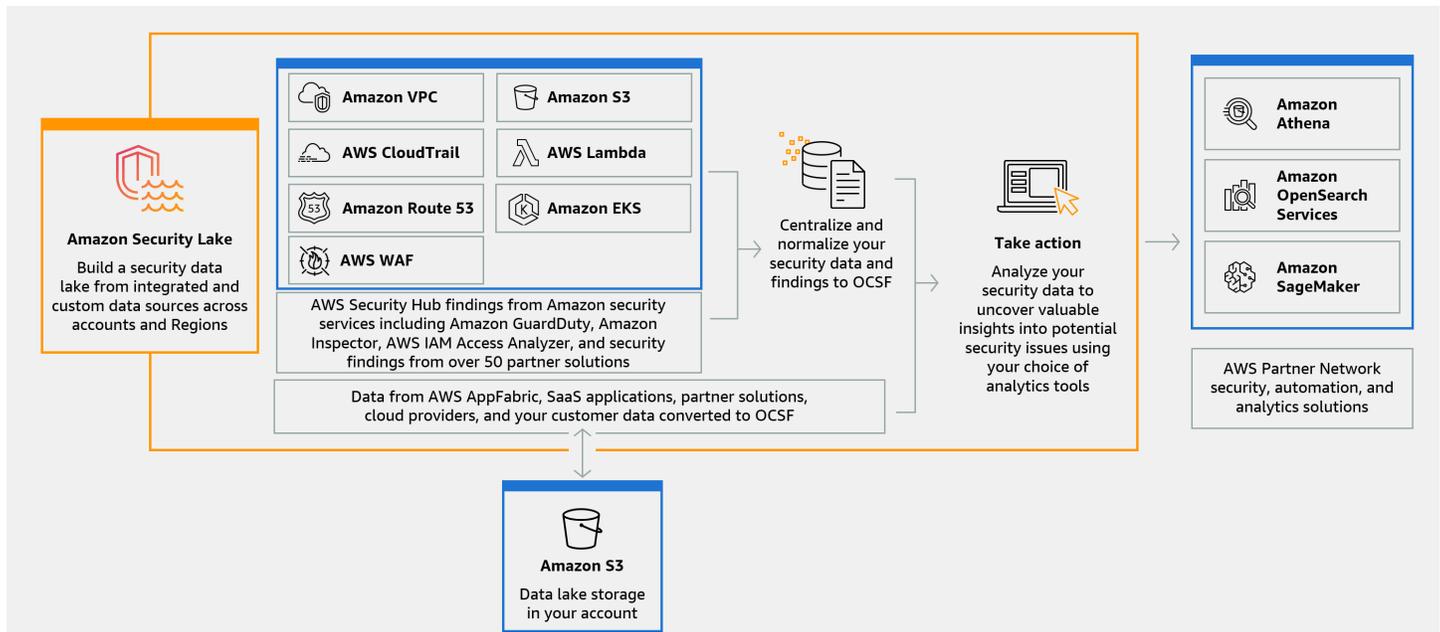
Amazon Security Lake ist ein vollständig verwalteter Sicherheits-Data-Lake-Dienst. Sie können Security Lake verwenden, um Sicherheitsdaten aus AWS Umgebungen, SaaS-Anbietern, lokalen Umgebungen, Cloud-Quellen und Quellen von Drittanbietern automatisch in einem speziell entwickelten Data Lake zu zentralisieren, der in Ihrem gespeichert wird. AWS-Konto Security Lake hilft Ihnen bei der Analyse von Sicherheitsdaten, sodass Sie sich ein umfassenderes Bild von Ihrer Sicherheitslage im gesamten Unternehmen machen können. Mit Security Lake können Sie auch den Schutz Ihrer Workloads, Anwendungen und Daten verbessern.

Der Data Lake wird von Amazon Simple Storage Service (Amazon S3) -Buckets unterstützt, und Sie behalten das Eigentum an Ihren Daten.

Security Lake automatisiert die Erfassung sicherheitsrelevanter Protokoll- und Ereignisdaten von integrierten AWS-Services Diensten und Diensten von Drittanbietern. Es hilft Ihnen auch dabei, den Lebenszyklus von Daten mit anpassbaren Aufbewahrungs- und Replikationseinstellungen zu verwalten. Security Lake konvertiert aufgenommene Daten in das Apache Parquet-Format und ein Standard-Open-Source-Schema namens Open Cybersecurity Schema Framework (OCSF). Mit der OCSF-Unterstützung normalisiert und kombiniert Security Lake Sicherheitsdaten aus einer Vielzahl von AWS Sicherheitsdatenquellen für Unternehmen.

Andere Dienste AWS-Services und Dienste von Drittanbietern können die in Security Lake gespeicherten Daten abonnieren, um auf Vorfälle zu reagieren und Sicherheitsdaten zu analysieren.

Überblick über Security Lake



Funktionen von Security Lake

Im Folgenden finden Sie einige wichtige Möglichkeiten, wie Sie mit Security Lake sicherheitsrelevante Protokoll- und Ereignisdaten zentralisieren, verwalten und abonnieren können.

Datenaggregation in Ihrem Konto

Security Lake erstellt einen speziell entwickelten Sicherheitsdatensee in Ihrem Konto. Security Lake sammelt Protokoll- und Ereignisdaten aus Cloud-, lokalen und benutzerdefinierten Datenquellen für Konten und Regionen. Der Data Lake wird von Amazon Simple Storage Service (Amazon S3) -Buckets unterstützt, und Sie behalten das Eigentum an Ihren Daten.

Eine Vielzahl unterstützter Protokoll- und Ereignisquellen

Security Lake sammelt Sicherheitsprotokolle und Ereignisse aus verschiedenen Quellen, darunter lokale Dienste und Dienste von Drittanbietern. AWS-Services Nach der Erfassung von Protokollen können Sie unabhängig von der Quelle zentral auf sie zugreifen und ihren Lebenszyklus verwalten. Einzelheiten zu den Quellen, aus denen Protokolle und Ereignisse von Security Lake gesammelt werden, finden Sie unter [Quellmanagement](#)

Datentransformation und Normalisierung

Security Lake partitioniert automatisch eingehende Daten von nativ unterstützten Daten AWS-Services und konvertiert sie in ein speicher- und abfrageeffizientes Parquet-Format. Außerdem werden Daten aus nativ unterstützten AWS-Services Daten in das Open-Source-Schema Open Cybersecurity Schema Framework (OCSF) umgewandelt. Dadurch sind die Daten mit anderen Anbietern AWS-Services und Drittanbietern kompatibel, ohne dass eine Nachbearbeitung erforderlich ist. Da Security Lake Daten normalisiert, können viele Sicherheitslösungen diese Daten parallel nutzen.

Mehrere Zugriffsebenen für Abonnenten

Abonnenten nutzen die in Security Lake gespeicherten Daten. Sie können die Zugriffsebene eines Abonnenten auf Ihre Daten auswählen. Abonnenten dürfen nur Daten aus den von Ihnen angegebenen Quellen und in den AWS-Regionen von Ihnen angegebenen Quellen nutzen. Abonnenten werden möglicherweise automatisch über neue Objekte informiert, wenn diese in den Data Lake geschrieben werden. Abonnenten können auch Daten aus dem Data Lake abfragen. Security Lake erstellt automatisch die Anmeldeinformationen, die zwischen Security Lake und dem Abonnenten benötigt werden, und tauscht sie aus.

Datenmanagement für mehrere Konten und mehrere Regionen

Sie können Security Lake zentral in allen Regionen, in denen es verfügbar ist, und in mehreren Regionen aktivieren. AWS-Konten In Security Lake können Sie auch Rollup-Regionen festlegen, um Sicherheitsprotokoll- und Ereignisdaten aus mehreren Regionen zu konsolidieren. Dies kann Ihnen helfen, die Anforderungen an die Datenresidenz zu erfüllen.

Konfigurierbar und anpassbar

Security Lake ist ein konfigurierbarer und anpassbarer Dienst. Sie können angeben, für welche Quellen, Konten und Regionen Sie die Protokollerfassung konfigurieren möchten. Sie können auch die Zugriffsebene eines Abonnenten auf den Data Lake angeben.

Verwaltung und Optimierung des Datenlebenszyklus

Security Lake verwaltet den Lebenszyklus Ihrer Daten mit anpassbaren Aufbewahrungseinstellungen und Speicherkosten mit automatisiertem Speicher-Tiering. Security Lake partitioniert und konvertiert eingehende Sicherheitsdaten automatisch in ein speicher- und abfrageeffizientes Apache Parquet-Format.

Zugriff auf Security Lake

Eine Liste der Regionen, in denen Security Lake derzeit verfügbar ist, finden Sie unter [Amazon Security Lake e](#)-. Weitere Informationen zu Regionen finden Sie unter [AWS Service-Endpunkte](#) im Allgemeine AWS-Referenz.

In jeder Region können Sie auf eine der folgenden Arten auf Security Lake zugreifen:

AWS Management Console

Das AWS Management Console ist eine browserbasierte Oberfläche, mit der Sie AWS Ressourcen erstellen und verwalten können. Die Security Lake-Konsole bietet Zugriff auf Ihr Security Lake-Konto und Ihre Ressourcen. Sie können die meisten Security Lake-Aufgaben mithilfe der Security Lake-Konsole ausführen.

Security Lake-API

Um programmgesteuert auf Security Lake zuzugreifen, verwenden Sie die Security Lake-API und senden Sie HTTPS-Anfragen direkt an den Dienst. Weitere Informationen finden Sie in der [Security Lake API-Referenz](#).

AWS Command Line Interface (AWS CLI)

Mit dem AWS CLI können Sie Befehle an der Befehlszeile Ihres Systems ausgeben, um Security Lake-Aufgaben und AWS -Aufgaben auszuführen. Die Verwendung der Befehlszeile kann schneller und bequemer sein als die Verwendung der Konsole. Die Befehlszeilen-Tools können auch beim Erstellen von Skripts für -Aufgaben hilfreich sein. Informationen zur Installation und Verwendung von finden Sie unter [AWS Command Line Interface](#). AWS CLI

AWS SDKs

AWS stellt SDKs bereit, die aus Bibliotheken und Beispielcode für verschiedene Programmiersprachen und Plattformen wie Java, Go, Python, C++ und .NET bestehen. Die SDKs bieten bequemen, programmatischen Zugriff auf Security Lake und andere AWS-Services Sie übernehmen auch Aufgaben wie das kryptografische Signieren von Anfragen, das Verwalten von Fehlern und das automatische Wiederholen von Anfragen. Informationen zur Installation und Verwendung der AWS SDKs finden Sie unter [Tools](#) to Build On. AWS

Zugehörige Services

Die folgenden sind weitere AWS-Services , die Security Lake verwendet:

- [Amazon EventBridge](#) — Security Lake benachrichtigt Abonnenten EventBridge, wenn Objekte in den Data Lake geschrieben werden.
- [AWS Glue](#) — Security Lake verwendet AWS Glue Crawler, um die AWS Glue Data Catalog Tabellen zu erstellen und neu geschriebene Daten an den Datenkatalog zu senden. Security Lake speichert auch Partitionsmetadaten für AWS Lake Formation Tabellen im Datenkatalog.
- [AWS Lake Formation](#) — Security Lake erstellt für jede Quelle, die Daten zu Security Lake beiträgt, eine separate Lake Formation-Tabelle. Lake Formation-Tabellen enthalten Informationen zu Daten aus jeder Quelle, einschließlich Schema-, Partitions- und Datenstandortinformationen. Abonnenten haben die Möglichkeit, Daten zu konsumieren, indem sie die Lake Formation-Tabellen abfragen.
- [AWS Lambda](#) — Security Lake verwendet Lambda-Funktionen, um Extraktions-, Transformations- und Ladeaufträge (ETL) für Rohdaten zu unterstützen und Partitionen für Quelldaten zu registrieren. AWS Glue
- [Amazon S3](#) — Security Lake speichert Ihre Daten als Amazon S3 S3-Objekte. Speicherklassen und Aufbewahrungseinstellungen basieren auf Amazon S3 S3-Angeboten. Security Lake unterstützt Amazon S3 Select nicht.

Security Lake sammelt zusätzlich zu den folgenden Daten Daten aus benutzerdefinierten Quellen AWS-Services:

- AWS CloudTrail Verwaltung und Datenereignisse (S3, Lambda)
- Auditprotokolle für Amazon Elastic Kubernetes Service (Amazon EKS)
- Amazon-Route-53-Resolver-Abfrageprotokolle
- AWS Security Hub Feststellungen
- Amazon Virtual Private Cloud (Amazon VPC)-Datendurchflussprotokolle
- AWS WAF v2-Protokolle

Weitere Informationen zu diesen Quellen finden Sie unter [Erfassung von Daten von AWS-Services](#). Sie können die Amazon S3 S3-Objekte in Ihrem Security Data Lake nutzen, indem Sie einen Abonnenten erstellen, der Daten im OCSF-Schema lesen kann. Sie können Daten auch mithilfe von Amazon Athena, Amazon Redshift und Abonnementdiensten von Drittanbietern abfragen, die in integriert sind. AWS Glue

Konzepte und Terminologie

In diesem Abschnitt werden die wichtigsten Konzepte und Begriffe beschrieben, die Ihnen bei der Verwendung von Amazon Security Lake helfen.

Beitragende Region

Eine oder mehrere AWS-Regionen, die Daten zu einer Rollup-Region beitragen.

Date-ies

Ihre persistenten Daten, die in Amazon Simple Storage Service (Amazon S3) gespeichert und von Security Dates verwaltet werden. Security Lake verwendet AWS Glue, um neu geschriebene Daten an den Datenkatalog zu senden. Security Lake erstellt außerdem eine AWS Lake Formation Tabelle für jede Quelle, die Daten zum Data Lake beiträgt. In einem Data Lake wird in der Regel Folgendes gespeichert:

- Strukturierte und unstrukturierte Daten
- Rohe und transformierte Daten

Security Lake ist ein Data Lake-Dienst, der für die Erfassung sicherheitsrelevanter Protokolle und Ereignisse entwickelt wurde.

Offenes Cybersecurity Schema Framework (OCSF)

Ein standardisiertes [Open-Source-Schema](#) für Sicherheitsprotokolle und Ereignisse. Es wurde von AWS und anderen führenden Unternehmen der Sicherheitsbranche in verschiedenen Sicherheitsbereichen entwickelt. Security Lake konvertiert die Protokolle und Ereignisse, die es sammelt, automatisch AWS-Services in das OCSF-Schema. Benutzerdefinierte Quellen konvertieren ihre Protokolle und Ereignisse in OCSF, bevor sie an Security Lake gesendet werden.

Bereich zusammenfassen

Und AWS-Region das konsolidiert Sicherheitsprotokolle und Ereignisse aus einer oder mehreren beitragenden Regionen. Die Angabe einer oder mehrerer Rollup-Regionen kann Ihnen helfen, die regionalen Compliance-Anforderungen zu erfüllen.

Quelle

Eine Reihe von Protokollen und Ereignissen, die von einem einzigen System generiert wurden und einer bestimmten Ereignisklasse in [OCSF](#) entsprechen. Security Lake kann Daten aus

einer Quelle sammeln. Eine Quelle kann ein anderer DienstAWS-Service oder ein Dienst eines Drittanbieters sein. Bei Quellen von Drittanbietern müssen Sie die Daten in das OCSF-Schema konvertieren, bevor Sie sie an Security Lake senden.

Abonnent

Ein Dienst, der Protokolle und Ereignisse von Security Lake verwendet. Ein Abonnent kann ein anderer DienstAWS-Service oder ein Dienst eines Drittanbieters sein.

Erste Schritte mit Amazon Security Lake

In diesem Abschnitt wird erklärt, wie Sie Security Lake aktivieren und mit der Nutzung beginnen. Sie erfahren, wie Sie Ihre Data Lake-Einstellungen konfigurieren und die Protokollerfassung einrichten. Sie können Security Lake über AWS Management Console oder programmgesteuert aktivieren und verwenden. Unabhängig davon, welche Methode Sie verwenden, müssen Sie zuerst einen Benutzer AWS-Konto und einen Administratorbenutzer einrichten. Die nachfolgenden Schritte unterscheiden sich je nach Zugriffsmethode. Die Security Lake-Konsole bietet einen optimierten Prozess für den Einstieg und erstellt alle erforderlichen AWS Identity and Access Management (IAM-) Rollen, die Sie für die Erstellung Ihres Data Lakes benötigen.

Ersteinrichtung AWS-Konto

Melde dich an für ein AWS-Konto

Wenn Sie noch keine haben AWS-Konto, führen Sie die folgenden Schritte aus, um eine zu erstellen.

Um sich für eine anzumelden AWS-Konto

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

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

Wenn Sie sich für eine anmelden AWS-Konto, Root-Benutzer des AWS-Kontos wird eine erstellt. Der Root-Benutzer hat Zugriff auf alle AWS-Services und Ressourcen des Kontos. Aus Sicherheitsgründen sollten Sie einem Benutzer Administratorzugriff zuweisen und nur den Root-Benutzer verwenden, um [Aufgaben auszuführen, für die Root-Benutzerzugriff erforderlich](#) ist.

AWS sendet Ihnen nach Abschluss des Anmeldevorgangs eine Bestätigungs-E-Mail. Sie können jederzeit Ihre aktuelle Kontoaktivität anzeigen und Ihr Konto verwalten. Rufen Sie dazu <https://aws.amazon.com/> auf und klicken Sie auf Mein Konto.

Erstellen Sie einen Benutzer mit Administratorzugriff

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

Sichern Sie Ihre Root-Benutzer des AWS-Kontos

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

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

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

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

Erstellen Sie einen Benutzer mit Administratorzugriff

1. Aktivieren Sie das IAM Identity Center.

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

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

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

Melden Sie sich als Benutzer mit Administratorzugriff an

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

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

Weisen Sie weiteren Benutzern Zugriff zu

1. Erstellen Sie in IAM Identity Center einen Berechtigungssatz, der der bewährten Methode zur Anwendung von Berechtigungen mit den geringsten Rechten folgt.

Anweisungen finden Sie im Benutzerhandbuch unter [Einen Berechtigungssatz erstellen](#).AWS IAM Identity Center

2. Weisen Sie Benutzer einer Gruppe zu und weisen Sie der Gruppe dann Single Sign-On-Zugriff zu.

Anweisungen finden [Sie im AWS IAM Identity Center Benutzerhandbuch unter Gruppen hinzufügen](#).

Identifizieren Sie das Konto, das Sie verwenden werden, um Security Lake zu aktivieren

Security Lake lässt sich integrieren AWS Organizations , um die Protokollerfassung für mehrere Konten in einer Organisation zu verwalten. Wenn Sie Security Lake für eine Organisation verwenden möchten, müssen Sie Ihr Organisationsverwaltungskonto verwenden, um einen delegierten Security Lake-Administrator zu benennen. Anschließend müssen Sie die Anmeldeinformationen des delegierten Administrators verwenden, um Security Lake zu aktivieren, Mitgliedskonten hinzuzufügen und Security Lake für sie zu aktivieren. Weitere Informationen finden Sie unter [Verwalten mehrerer Konten mit AWS Organizations](#).

Alternativ können Sie Security Lake ohne die Organisationsintegration für ein eigenständiges Konto verwenden, das nicht Teil einer Organisation ist.

Überlegungen zur Aktivierung von Amazon Security Lake

Bevor Sie Security Lake aktivieren, sollten Sie Folgendes berücksichtigen:

- Security Lake bietet regionsübergreifende Verwaltungsfunktionen, was bedeutet, dass Sie Ihren Data Lake erstellen und die Protokollerfassung auf allen AWS-Regionen Ebenen konfigurieren können. Um Security Lake in [allen unterstützten Regionen](#) zu aktivieren, können Sie einen beliebigen unterstützten regionalen Endpunkt auswählen. Sie können auch [Rollup-Regionen](#) hinzufügen, um Daten aus mehreren Regionen in einer einzigen Region zusammenzufassen.
- Wir empfehlen, Security Lake in allen unterstützten Programmen zu aktivieren. AWS-Regionen Wenn Sie dies tun, kann Security Lake Daten sammeln, die mit nicht autorisierten oder

ungewöhnlichen Aktivitäten in Verbindung stehen, auch in Regionen, die Sie nicht aktiv nutzen. Wenn Security Lake nicht in allen unterstützten Regionen aktiviert ist, ist seine Fähigkeit, Daten von anderen Diensten zu sammeln, die Sie in mehreren Regionen verwenden, eingeschränkt.

- Wenn Sie Security Lake zum ersten Mal in einer beliebigen Region aktivieren, wird für Ihr Konto eine [dienstbezogene Rolle mit](#) dem Namen `AWSServiceRoleForSecurityLake` erstellt. Diese Rolle beinhaltet die Berechtigungen, andere in AWS-Services Ihrem Namen anzurufen und den Security Data Lake zu betreiben. Weitere Informationen zur Funktionsweise von serviceverknüpften Rollen finden Sie unter [Verwenden von serviceverknüpften Rollen](#) im IAM-Benutzerhandbuch. Wenn Sie Security Lake als [delegierten Security Lake-Administrator aktivieren, erstellt Security Lake](#) die [dienstverknüpfte Rolle](#) in jedem Mitgliedskonto der Organisation.
- Security Lake unterstützt Amazon S3 Object Lock nicht. Wenn die Data Lake-Buckets erstellt werden, ist S3 Object Lock standardmäßig deaktiviert. Wenn Object Lock für einen Bucket aktiviert wird, wird die Übermittlung von normalisierten Protokolldaten an den Data Lake unterbrochen.

Erste Schritte auf der Konsole

In diesem Tutorial wird erklärt, wie Sie Security Lake über den aktivieren und konfigurieren AWS Management Console. Als Teil von bietet die AWS Management Console Security Lake-Konsole einen optimierten Prozess für den Einstieg und erstellt alle erforderlichen AWS Identity and Access Management (IAM-) Rollen, die Sie für die Erstellung Ihres Data Lakes benötigen.

Schritt 1: Quellen konfigurieren

Security Lake sammelt Protokoll- und Ereignisdaten aus einer Vielzahl von Quellen und in Ihrem AWS-Konten Land AWS-Regionen. Folgen Sie diesen Anweisungen, um herauszufinden, welche Daten Security Lake sammeln soll. Sie können diese Anweisungen nur verwenden, um eine nativ unterstützte Quelle AWS-Service hinzuzufügen. Informationen zum Hinzufügen einer benutzerdefinierten Quelle finden Sie unter. [Sammeln von Daten aus benutzerdefinierten Quellen](#)

So konfigurieren Sie die Erfassung von Protokollquellen

1. Öffnen Sie die Security Lake-Konsole unter <https://console.aws.amazon.com/securitylake/>.
2. Wählen Sie mithilfe der AWS-Region Auswahl in der oberen rechten Ecke der Seite eine Region aus. Sie können Security Lake während des Onboardings in der aktuellen Region und anderen Regionen aktivieren.
3. Wählen Sie Erste Schritte.

4. Wählen Sie für Protokoll- und Ereignisquellen auswählen eine der folgenden Optionen:
 - a. AWS Standardquellen aufnehmen — Wenn Sie die empfohlene Option wählen, CloudTrail werden S3-Datenereignisse nicht für die Aufnahme berücksichtigt. Dies liegt daran, dass die Aufnahme großer Mengen an CloudTrail S3-Datenereignissen die Nutzungskosten erheblich beeinflussen kann. Um diese Quelle aufzunehmen, wählen Sie die Option Bestimmte AWS Quellen aufnehmen.
 - b. Bestimmte AWS Quellen aufnehmen — Mit dieser Option können Sie eine oder mehrere Protokoll- und Ereignisquellen auswählen, die Sie aufnehmen möchten.

 Note

Wenn Sie Security Lake zum ersten Mal in einem Konto aktivieren, sind alle ausgewählten Protokoll- und Ereignisquellen Teil einer 15-tägigen kostenlosen Testphase. Weitere Informationen zu Nutzungsstatistiken finden Sie unter [Überprüfung der Nutzung und der geschätzten Kosten](#).

5. Wählen Sie unter Versionen die Version der Datenquelle aus, aus der Sie Protokoll- und Ereignisquellen aufnehmen möchten.

 Important

Wenn Sie nicht über die erforderlichen Rollenberechtigungen verfügen, um die neue Version der AWS Protokollquelle in der angegebenen Region zu aktivieren, wenden Sie sich an Ihren Security Lake-Administrator. Weitere Informationen finden Sie unter [Rollenberechtigungen aktualisieren](#).

6. Wählen Sie unter Ausgewählte Regionen aus, ob Protokoll- und Ereignisquellen aus allen unterstützten Regionen oder aus bestimmten Regionen aufgenommen werden sollen. Wenn Sie „Bestimmte Regionen“ wählen, wählen Sie aus, aus welchen Regionen Daten aufgenommen werden sollen.
7. Erstellen Sie für den Zugriff auf Dienste eine neue IAM-Rolle oder verwenden Sie eine bestehende IAM-Rolle, die Security Lake die Erlaubnis erteilt, Daten aus Ihren Quellen zu sammeln und sie Ihrem Data Lake hinzuzufügen. Eine Rolle wird in allen Regionen verwendet, in denen Sie Security Lake aktivieren.
8. Wählen Sie Weiter aus.

Schritt 2: Definieren Sie Speichereinstellungen und Rollup-Regionen (optional)

Sie können die Amazon S3 S3-Speicherklasse angeben, in der Security Lake Ihre Daten speichern soll und für wie lange. Sie können auch eine Rollup-Region angeben, um Daten aus mehreren Regionen zu konsolidieren. Dies sind optionale Schritte. Weitere Informationen finden Sie unter [Lebenszyklusmanagement in Security Lake](#).

Um Speicher- und Rollup-Einstellungen zu konfigurieren

1. Wenn Sie Daten aus mehreren beteiligten Regionen in einer Rollup-Region konsolidieren möchten, wählen Sie unter Rollup-Regionen auswählen die Option Rollup-Region hinzufügen aus. Geben Sie die Rollup-Region und die Regionen an, die dazu beitragen sollen. Sie können eine oder mehrere Rollup-Regionen einrichten.
2. Wählen Sie für Ausgewählte Speicherklassen eine Amazon S3 S3-Speicherklasse aus. Die Standard-Speicherklasse ist S3 Standard. Geben Sie einen Aufbewahrungszeitraum (in Tagen) an, wenn Sie möchten, dass die Daten nach dieser Zeit in eine andere Speicherklasse übertragen werden, und wählen Sie Übergang hinzufügen aus. Nach Ablauf der Aufbewahrungsfrist laufen die Objekte ab und Amazon S3 löscht sie. Weitere Informationen zu Amazon S3 S3-Speicherklassen und Aufbewahrung finden Sie unter [Verwaltung der Aufbewahrung](#).
3. Wenn Sie im ersten Schritt eine Rollup-Region ausgewählt haben, erstellen Sie für den Servicezugriff eine neue IAM-Rolle oder verwenden Sie eine bestehende IAM-Rolle, die Security Lake die Erlaubnis erteilt, Daten über mehrere Regionen hinweg zu replizieren.
4. Wählen Sie Weiter aus.

Schritt 3: Überprüfen und erstellen Sie einen Data Lake

Überprüfen Sie die Quellen, aus denen Security Lake Daten sammelt, Ihre Rollup-Regionen und Ihre Aufbewahrungseinstellungen. Erstellen Sie dann Ihren Data Lake.

Um den Data Lake zu überprüfen und zu erstellen

1. Überprüfen Sie bei der Aktivierung von Security Lake die Protokoll- und Ereignisquellen, Regionen, Rollup-Regionen und Speicherklassen.
2. Wählen Sie Erstellen.

Nachdem Sie Ihren Data Lake erstellt haben, wird die Übersichtsseite in der Security Lake-Konsole angezeigt. Diese Seite bietet einen Überblick über die Anzahl der Regionen und Rollup-Regionen, Informationen zu Abonnenten und Probleme.

Das Menü Probleme zeigt Ihnen eine Zusammenfassung der Probleme der letzten 14 Tage, die sich auf den Security Lake-Service oder Ihre Amazon S3 S3-Buckets auswirken. Weitere Informationen zu den einzelnen Problemen finden Sie auf der Seite Probleme der Security Lake-Konsole.

Schritt 4: Ihre eigenen Daten anzeigen und abfragen

Nachdem Sie Ihren Data Lake erstellt haben, können Sie Amazon Athena oder ähnliche Dienste verwenden, um Ihre Daten aus AWS Lake Formation Datenbanken und Tabellen anzuzeigen und abzufragen. Wenn Sie die Konsole verwenden, gewährt Security Lake der Rolle, die Sie zur Aktivierung von Security Lake verwenden, automatisch Datenbankansichtsberechtigungen. Die Rolle muss mindestens über Datenanalytistenberechtigungen verfügen. Weitere Informationen zu Berechtigungsstufen finden Sie in der Referenz zu [Personas und IAM-Berechtigungen von Lake Formation](#). Anweisungen zum Erteilen von SELECT Berechtigungen finden Sie unter [Erteilen von Datenkatalogberechtigungen mithilfe der benannten Ressourcenmethode](#) im AWS Lake Formation Entwicklerhandbuch.

Schritt 5: Abonnenten erstellen

Nachdem Sie Ihren Data Lake erstellt haben, können Sie Abonnenten hinzufügen, um Ihre Daten zu nutzen. Abonnenten können Daten konsumieren, indem sie direkt auf Objekte in Ihren Amazon S3 S3-Buckets zugreifen oder den Data Lake abfragen. Weitere Informationen zu Abonnenten finden Sie unter [Abonnentenverwaltung in Amazon Security Lake](#)

Programmgesteuerter Einstieg

In diesem Tutorial wird erklärt, wie Sie Security Lake programmgesteuert aktivieren und verwenden können. Die Amazon Security Lake-API bietet Ihnen umfassenden, programmatischen Zugriff auf Ihr Security Lake-Konto, Ihre Daten und Ressourcen. Alternativ können Sie AWS Befehlszeilentools — die [AWS Command Line Interface](#) oder die [AWS Tools für PowerShell](#) — oder die [AWS SDKs verwenden, um auf Security Lake](#) zuzugreifen.

Schritt 1: IAM-Rollen erstellen

Wenn Sie programmgesteuert auf Security Lake zugreifen, müssen Sie einige AWS Identity and Access Management (IAM-) Rollen erstellen, um Ihren Data Lake zu konfigurieren.

⚠ Important

Es ist nicht erforderlich, diese IAM-Rollen zu erstellen, wenn Sie die Security Lake-Konsole verwenden, um Security Lake zu aktivieren und zu konfigurieren.

Sie müssen Rollen in IAM erstellen, wenn Sie eine oder mehrere der folgenden Aktionen ausführen möchten (klicken Sie auf die Links, um weitere Informationen zu den IAM-Rollen für jede Aktion zu erhalten):

- [Eine benutzerdefinierte Quelle erstellen — Benutzerdefinierte](#) Quellen sind Quellen, die nicht systemintern unterstützt werden und Daten an Security AWS-Services Lake senden.
- [Einen Abonnenten mit Datenzugriff erstellen](#) — Abonnenten mit Berechtigungen können direkt von Ihrem Data Lake aus auf S3-Objekte zugreifen.
- [Einen Abonnenten mit Abfragezugriff erstellen](#) — Abonnenten mit Berechtigungen können mithilfe von Diensten wie Amazon Athena Daten von Security Lake abfragen.
- [Konfiguration einer Rollup-Region — Eine Rollup-Region](#) konsolidiert Daten aus mehreren AWS-Regionen

Nachdem Sie die zuvor genannten Rollen erstellt haben, fügen Sie die [AmazonSecurityLakeAdministrator](#) AWS verwaltete Richtlinie der Rolle hinzu, die Sie zur Aktivierung von Security Lake verwenden. Diese Richtlinie gewährt Administratorberechtigungen, die es einem Principal ermöglichen, sich bei Security Lake anzumelden und auf alle Security Lake-Aktionen zuzugreifen.

Fügen Sie die [AmazonSecurityLakeMetaStoreManager](#) AWS verwaltete Richtlinie an, um Ihren Data Lake zu erstellen oder Daten von Security Lake abzufragen. Diese Richtlinie ist erforderlich, damit Security Lake ETL-Jobs (Extrahieren, Transformieren und Laden) für rohe Protokoll- und Ereignisdaten unterstützt, die es aus Quellen empfängt.

Schritt 2: Amazon Security Lake aktivieren

Verwenden Sie den [CreateDataLake](#) Betrieb der Security Lake-API, um Security Lake programmgesteuert zu aktivieren. Wenn Sie den verwenden AWS CLI, führen Sie den Befehl [create-data-lake](#) aus. Verwenden Sie in Ihrer Anfrage das `region` Feld des `configurations` Objekts, um den Regionalcode für die Region anzugeben, in der Security Lake aktiviert werden soll. Eine Liste der Regionscodes finden Sie unter [Amazon Security Lake-Endpoints](#) in der Allgemeine AWS-Referenz.

Beispiel 1

Der folgende Beispielbefehl aktiviert Security Lake in den us-east-2 Regionen us-east-1 und. In beiden Regionen ist dieser Data Lake mit verwalteten Amazon S3 S3-Schlüsseln verschlüsselt. Objekte laufen nach 365 Tagen ab, und Objekte werden nach 60 Tagen in die Speicherklasse ONEZONE_IA S3 überführt. Dieses Beispiel ist für Linux, macOS oder Unix formatiert und verwendet den umgekehrten Schrägstrich (\) zur Verbesserung der Lesbarkeit.

```
$ aws securitylake create-data-lake \
--configurations '[{"encryptionConfiguration":
{"kmsKeyId":"S3_MANAGED_KEY"},"region":"us-east-1","lifecycleConfiguration":
{"expiration":{"days":365},"transitions":[{"days":60,"storageClass":"ONEZONE_IA"}]}},
{"encryptionConfiguration": {"kmsKeyId":"S3_MANAGED_KEY"},"region":"us-
east-2","lifecycleConfiguration": {"expiration":{"days":365},"transitions":
[{"days":60,"storageClass":"ONEZONE_IA"}]}]'] \
--meta-store-manager-role-arn "arn:aws:iam:us-east-1:123456789012:role/service-role/
AmazonSecurityLakeMetaStoreManager"
```

Beispiel 2

Der folgende Beispielbefehl aktiviert Security Lake in der us-east-2 Region. Dieser Data Lake ist mit einem vom Kunden verwalteten Schlüssel verschlüsselt, der in AWS Key Management Service (AWS KMS) erstellt wurde. Objekte laufen nach 500 Tagen ab, und Objekte werden nach 30 Tagen in die Speicherklasse GLACIER S3 überführt. Dieses Beispiel ist für Linux, macOS oder Unix formatiert und verwendet den umgekehrten Schrägstrich (\) zur Verbesserung der Lesbarkeit.

```
$ aws securitylake create-data-lake \
--configurations '[{"encryptionConfiguration":
{"kmsKeyId":"1234abcd-12ab-34cd-56ef-1234567890ab"},"region":"us-
east-2","lifecycleConfiguration": {"expiration":{"days":500},"transitions":
[{"days":30,"storageClass":"GLACIER"}]}]'] \
--meta-store-manager-role-arn "arn:aws:iam:us-east-1:123456789012:role/service-role/
AmazonSecurityLakeMetaStoreManager"
```

Note

Wenn Sie Security Lake bereits aktiviert haben und die Konfigurationseinstellungen für eine Region oder Quelle aktualisieren möchten, verwenden Sie den [UpdateDataLake](#) Vorgang oder, falls Sie den verwenden AWS CLI, den Befehl [update-data-lake](#). Verwenden Sie den Vorgang nicht. CreateDataLake

Schritt 3: Quellen konfigurieren

Security Lake sammelt Protokoll- und Ereignisdaten aus einer Vielzahl von Quellen und in Ihrem AWS-Konten Land AWS-Regionen. Folgen Sie diesen Anweisungen, um herauszufinden, welche Daten Security Lake sammeln soll. Sie können diese Anweisungen nur verwenden, um eine nativ unterstützte Quelle AWS-Service hinzuzufügen. Informationen zum Hinzufügen einer benutzerdefinierten Quelle finden Sie unter [Sammeln von Daten aus benutzerdefinierten Quellen](#)

Um eine oder mehrere Sammlungsquellen programmgesteuert zu definieren, verwenden Sie den [CreateAwsLogSource](#) Betrieb der Security Lake-API. Geben Sie für jede Quelle einen regional eindeutigen Wert für den Parameter an. `sourceName` Verwenden Sie optional zusätzliche Parameter, um den Geltungsbereich der Quelle auf bestimmte Konten (`accounts`) oder eine bestimmte Version (`sourceVersion`) zu beschränken.

Note

Wenn Sie keinen optionalen Parameter in Ihre Anfrage aufnehmen, wendet Security Lake Ihre Anfrage auf alle Konten oder alle Versionen der angegebenen Quelle an, je nachdem, welchen Parameter Sie ausschließen. Wenn Sie beispielsweise der delegierte Security Lake-Administrator für eine Organisation sind und den `accounts` Parameter ausschließen, wendet Security Lake Ihre Anfrage auf alle Konten in Ihrer Organisation an. Wenn Sie den `sourceVersion` Parameter ausschließen, wendet Security Lake Ihre Anfrage ebenfalls auf alle Versionen der angegebenen Quelle an.

Wenn Ihre Anfrage eine Region angibt, in der Sie Security Lake nicht aktiviert haben, tritt ein Fehler auf. Um diesen Fehler zu beheben, stellen Sie sicher, dass das `regions` Array nur die Regionen angibt, in denen Sie Security Lake aktiviert haben. Alternativ können Sie Security Lake in der Region aktivieren und Ihre Anfrage dann erneut einreichen.

Wenn Sie Security Lake zum ersten Mal in einem Konto aktivieren, sind alle ausgewählten Protokoll- und Ereignisquellen Teil einer 15-tägigen kostenlosen Testphase. Weitere Informationen zu Nutzungsstatistiken finden Sie unter [Überprüfung der Nutzung und der geschätzten Kosten](#).

Schritt 4: Speichereinstellungen und Rollup-Regionen konfigurieren (optional)

Sie können die Amazon S3 S3-Speicherklasse angeben, in der Security Lake Ihre Daten speichern soll und für wie lange. Sie können auch eine Rollup-Region angeben, um Daten aus mehreren Regionen zu konsolidieren. Dies sind optionale Schritte. Weitere Informationen finden Sie unter [Lebenszyklusmanagement in Security Lake](#).

Um bei der Aktivierung von Security Lake programmgesteuert ein Zielziel zu definieren, verwenden Sie den [CreateDataLake](#)Betrieb der Security Lake-API. Wenn Sie Security Lake bereits aktiviert haben und ein Zielziel definieren möchten, verwenden Sie den [UpdateDataLake](#)Vorgang, nicht den `CreateDataLake` Vorgang.

Verwenden Sie für beide Operationen die unterstützten Parameter, um die gewünschten Konfigurationseinstellungen anzugeben:

- Um eine Rollup-Region anzugeben, geben Sie in dem `region` Feld die Region an, aus der Sie Daten zu den Rollup-Regionen beitragen möchten. Geben Sie im `regions` Array des `replicationConfiguration` Objekts den Regionalcode für jede Rollup-Region an. Eine Liste der Regioncodes finden Sie unter [Amazon Security Lake-Endpoints](#) in der Allgemeine AWS-Referenz.
- Verwenden Sie die folgenden `lifecycleConfiguration` Parameter, um Aufbewahrungseinstellungen für Ihre Daten festzulegen:
 - Geben Sie für die Gesamtzahl der Tage (`days`) `antransitions`, an denen Sie S3-Objekte in einer bestimmten Amazon S3 S3-Speicherklasse (`storageClass`) speichern möchten.
 - Geben Sie für die Gesamtzahl der Tage `anexpiration`, an denen Sie Objekte in Amazon S3 speichern möchten, und verwenden Sie dabei eine beliebige Speicherklasse, nachdem Objekte erstellt wurden. Wenn diese Aufbewahrungsfrist endet, laufen Objekte ab und Amazon S3 löscht sie.

Security Lake wendet die angegebenen Aufbewahrungseinstellungen auf die Region an, die Sie im `region` Feld des `configurations` Objekts angeben.

Mit dem folgenden Befehl wird beispielsweise ein Data Lake mit `ap-northeast-2` einer Rollup-Region erstellt. Die `us-east-1` Region wird Daten zur Region beitragen. `ap-northeast-2` In diesem Beispiel wird auch eine 10-tägige Ablauffrist für Objekte festgelegt, die dem Data Lake hinzugefügt werden.

```
$ aws securitylake create-data-lake \
--configurations '[{"encryptionConfiguration":
{"kmsKeyId":"S3_MANAGED_KEY"},"region":"us-east-1","replicationConfiguration":
{"regions": ["ap-northeast-2"],"roleArn":"arn:aws:iam::123456789012:role/service-
role/AmazonSecurityLakeS3ReplicationRole"},"lifecycleConfiguration": {"expiration":
{"days":10}}}]' \
--meta-store-manager-role-arn "arn:aws:iam::123456789012:role/service-role/
AmazonSecurityLakeMetaStoreManager"
```

Sie haben jetzt Ihren Data Lake erstellt. Verwenden Sie den [ListDataLakes](#) Betrieb der Security Lake-API, um die Aktivierung von Security Lake und Ihre Data Lake-Einstellungen in jeder Region zu überprüfen.

Wenn bei der Erstellung Ihres Data Lakes Probleme oder Fehler auftreten, können Sie mithilfe des Vorgangs eine Liste von Ausnahmen anzeigen und Benutzer über Ausnahmen im Zusammenhang mit dem [ListDataLakeExceptionsCreateDataLakeExceptionSubscription](#) Vorgang informieren. Weitere Informationen finden Sie unter [Fehlerbehebung beim Data Lake-Status](#).

Schritt 5: Ihre eigenen Daten anzeigen und abfragen

Nachdem Sie Ihren Data Lake erstellt haben, können Sie Amazon Athena oder ähnliche Dienste verwenden, um Ihre Daten aus AWS Lake Formation Datenbanken und Tabellen anzuzeigen und abzufragen. Wenn Sie Security Lake programmgesteuert aktivieren, werden Datenbankansichtsberechtigungen nicht automatisch gewährt. Das Data Lake-Administratorkonto in AWS Lake Formation muss SELECT Berechtigungen für die IAM-Rolle gewähren, mit der Sie die entsprechenden Datenbanken und Tabellen abfragen möchten. Die Rolle muss mindestens über Datenanalytistenberechtigungen verfügen. Weitere Informationen zu Berechtigungsstufen finden Sie in der Referenz zu [Personas und IAM-Berechtigungen von Lake Formation](#). Anweisungen zum Erteilen von SELECT Berechtigungen finden Sie unter [Erteilen von Datenkatalogberechtigungen mithilfe der benannten Ressourcenmethode](#) im AWS Lake Formation Entwicklerhandbuch.

Schritt 6: Abonnenten erstellen

Nachdem Sie Ihren Data Lake erstellt haben, können Sie Abonnenten hinzufügen, um Ihre Daten zu nutzen. Abonnenten können Daten konsumieren, indem sie direkt auf Objekte in Ihren Amazon S3 S3-Buckets zugreifen oder den Data Lake abfragen. Weitere Informationen zu Abonnenten finden Sie unter [Abonnentenverwaltung in Amazon Security Lake](#)

Verwalten mehrerer Konten mit AWS Organizations

Sie können Amazon Security Lake verwenden, um Sicherheitsprotokolle und Ereignisse aus mehreren zu sammeln AWS-Konten. Um die Verwaltung mehrerer Konten zu automatisieren und zu optimieren, empfehlen wir dringend, Security Lake in zu integrieren [AWS Organizations](#).

In Organizations wird das Konto, mit dem Sie die Organisation erstellen, als Verwaltungskonto bezeichnet. Um Security Lake in Organizations zu integrieren, muss das Verwaltungskonto ein delegiertes Security-Lake-Administratorkonto für die Organisation festlegen.

Der delegierte Security-Lake-Administrator kann Security Lake aktivieren und Security-Lake-Einstellungen für Mitgliedskonten konfigurieren. Der delegierte Administrator kann Protokolle und Ereignisse in der gesamten Organisation in allen erfassen AWS-Regionen , in denen Security Lake aktiviert ist (unabhängig davon, welchen regionalen Endpunkt er derzeit verwendet). Der delegierte Administrator kann Security Lake auch so konfigurieren, dass Protokoll- und Ereignisdaten für neue Organisationskonten automatisch erfasst werden.

Der delegierte Security-Lake-Administrator hat Zugriff auf Protokoll- und Ereignisdaten für zugehörige Mitgliedskonten. Dementsprechend können sie Security Lake so konfigurieren, dass Daten erfasst werden, die den zugehörigen Mitgliedskonten gehören. Sie können Abonnenten auch die Berechtigung erteilen, Daten zu verarbeiten, die den zugehörigen Mitgliedskonten gehören.

Um Security Lake für mehrere Konten in einer Organisation zu aktivieren, muss das Organisationsverwaltungskonto zunächst ein delegiertes Security-Lake-Administratorkonto für die Organisation festlegen. Der delegierte Administrator kann dann Security Lake für die Organisation aktivieren und konfigurieren.

Informationen zum Einrichten von Organizations finden Sie unter [Erstellen und Verwalten einer Organisation](#) im AWS Organizations -Benutzerhandbuch.

Wichtige Überlegungen für delegierte Security-Lake-Administratoren

Beachten Sie die folgenden Faktoren, die definieren, wie sich ein delegierter Administrator in Security Lake verhält:

Der delegierte Administrator ist in allen Regionen gleich.

Wenn Sie den delegierten Administrator erstellen, wird er für jede Region, in der Sie Security Lake aktivieren, zum delegierten Administrator.

Wir empfehlen, das Log-Archive-Konto als delegierten Security-Lake-Administrator festzulegen.

Das Log-Archive-Konto ist ein AWS-Konto, das für die Aufnahme und Archivierung aller sicherheitsrelevanten Protokolle bestimmt ist. Der Zugriff auf dieses Konto ist in der Regel auf einige Benutzer beschränkt, z. B. Prüfer und Sicherheitsteams für Compliance-Untersuchungen. Wir empfehlen, das Log-Archive-Konto als delegierten Security-Lake-Administrator festzulegen, damit Sie sicherheitsbezogene Protokolle und Ereignisse mit minimalem Kontextwechsel anzeigen können.

Darüber hinaus empfehlen wir, dass nur ein minimaler Satz von Benutzern direkten Zugriff auf das Log-Archive-Konto hat. Wenn ein Benutzer außerhalb dieser Auswahlgruppe Zugriff auf die Daten benötigt, die Security Lake sammelt, können Sie sie als Security-Lake-Abonnent hinzufügen. Informationen zum Hinzufügen eines Abonnenten finden Sie unter [Abonnentenverwaltung in Amazon Security Lake](#).

Wenn Sie den AWS Control Tower Service nicht verwenden, haben Sie möglicherweise kein Log-Archive-Konto. Weitere Informationen zum Log-Archive-Konto finden Sie unter [Security OU – Log Archive account](#) in der AWS Security Reference Architecture.

Eine Organisation kann nur einen delegierten Administrator haben.

Sie können nur einen delegierten Security-Lake-Administrator für jede Organisation haben.

Das Verwaltungskonto der Organisation kann nicht der delegierte Administrator sein.

Basierend auf den bewährten Methoden für AWS Sicherheit und dem Prinzip der geringsten Berechtigung kann Ihr Organisationsverwaltungskonto nicht der delegierte Administrator sein.

Der delegierte Administrator muss Teil einer aktiven Organisation sein.

Wenn Sie eine Organisation löschen, kann das delegierte Administratorkonto Security Lake nicht mehr verwalten. Sie müssen einen delegierten Administrator aus einer anderen Organisation benennen oder Security Lake mit einem eigenständigen Konto verwenden, das nicht Teil einer Organisation ist.

Erforderliche IAM-Berechtigungen zum Benennen des delegierten Administrators

Wenn Sie den delegierten Security-Lake-Administrator festlegen, müssen Sie über Berechtigungen verfügen, um Security Lake zu aktivieren und bestimmte AWS Organizations API-Operationen zu verwenden, die in der folgenden Richtlinienanweisung aufgeführt sind.

Sie können die folgende Anweisung am Ende einer AWS Identity and Access Management (IAM)-Richtlinie hinzufügen, um diese Berechtigungen zu erteilen.

```
{
  "Sid": "Grant permissions to designate a delegated Security Lake administrator",
  "Effect": "Allow",
  "Action": [
    "securitylake:RegisterDataLakeDelegatedAdministrator",
    "organizations:EnableAWSServiceAccess",
    "organizations:RegisterDelegatedAdministrator",
    "organizations:ListAccounts",
    "organizations:ListDelegatedAdministrators",
    "organizations:ListAWSServiceAccessForOrganization",
    "organizations:DescribeOrganizationalUnit",
    "organizations:DescribeAccount",
    "organizations:DescribeOrganization"
  ],
  "Resource": "*"
}
```

Benennen des delegierten Security-Lake-Administrators und Hinzufügen von Mitgliedskonten

Wählen Sie Ihre Zugriffsmethode aus, um das delegierte Security-Lake-Administratorkonto für Ihre Organisation festzulegen. Nur das Verwaltungskonto der Organisation kann das delegierte Administratorkonto für seine Organisation festlegen. Das Verwaltungskonto der Organisation kann nicht das delegierte Administratorkonto für seine Organisation sein.

 Note

- Das Verwaltungskonto der Organisation sollte die Security-Lake-RegisterDataLakeDelegatedAdministratorOperation verwenden, um das delegierte Security-Lake-Administratorkonto zu bestimmen. Die Benennung des delegierten Security-Lake-Administrators über Organizations wird nicht unterstützt.
- Wenn Sie den delegierten Administrator für die Organisation ändern möchten, müssen Sie zuerst [den aktuellen delegierten Administrator entfernen](#). Anschließend können Sie einen neuen delegierten Administrator festlegen.

Console

1. Öffnen Sie die Security-Lake-Konsole unter <https://console.aws.amazon.com/securitylake/>.
Melden Sie sich mit den Anmeldeinformationen des Verwaltungskontos für Ihre Organisation an.
2.
 - Wenn Security Lake noch nicht aktiviert ist, wählen Sie Erste Schritte aus und weisen Sie dann auf der Seite Security Lake aktivieren den delegierten Security-Lake-Administrator zu.
 - Wenn Security Lake bereits aktiviert ist, weisen Sie den delegierten Security-Lake-Administrator auf der Seite Einstellungen zu.
3. Wählen Sie unter Delegieren der Administration an ein anderes Konto das Konto aus, das bereits als delegierter Administrator für andere - AWS Sicherheitsservices fungiert (empfohlen). Alternativ können Sie die 12-stellige AWS-Konto ID des Kontos eingeben, das Sie als delegierten Security-Lake-Administrator festlegen möchten.
4. Wählen Sie Delegate (Delegieren). Wenn Security Lake noch nicht aktiviert ist, aktiviert die Benennung des delegierten Administrators Security Lake für dieses Konto in Ihrer aktuellen Region.

API

Um den delegierten Administrator programmgesteuert zu benennen, verwenden Sie die [-RegisterDataLakeDelegatedAdministrator](#) Operation der Security-Lake-API. Sie müssen die Operation über das Verwaltungskonto der Organisation aufrufen. Wenn Sie die verwenden AWS CLI, führen Sie den [register-data-lake-delegated-administrator](#) Befehl über das Verwaltungskonto der Organisation aus. Verwenden Sie in Ihrer Anfrage den `accountId` Parameter, um die 12-

stellige Konto-ID des anzugeben AWS-Konto , das als delegiertes Administratorkonto für die Organisation festgelegt werden soll.

Mit dem folgenden AWS CLI Befehl wird beispielsweise der delegierte Administrator bezeichnet. Dieses Beispiel ist für Linux, macOS oder Unix formatiert und verwendet den umgekehrten Schrägstrich (\) zur Verbesserung der Lesbarkeit.

```
$ aws securitylake register-data-lake-delegated-administrator \  
--account-id 123456789012
```

Der delegierte Administrator kann auch die Erfassung von AWS Protokoll- und Ereignisdaten für neue Organisationskonten automatisieren. Mit dieser Konfiguration wird Security Lake automatisch in neuen Konten aktiviert, wenn die Konten der Organisation in hinzugefügt werden AWS Organizations. Als delegierter Administrator können Sie diese Konfiguration aktivieren, indem Sie die [-CreateDataLakeOrganizationConfiguration](#) Operation der Security Lake-API verwenden oder, wenn Sie die AWS CLI verwenden, den [create-data-lake-organization-configuration](#) Befehl ausführen. In Ihrer Anfrage können Sie auch bestimmte Konfigurationseinstellungen für neue Konten angeben.

Der folgende AWS CLI Befehl aktiviert beispielsweise automatisch Security Lake und die Sammlung von Amazon Route 53 Resolver-Abfrageprotokollen, AWS Security Hub Erkenntnissen und Amazon Virtual Private Cloud (Amazon VPC) Flow Logs in neuen Organisationskonten. Dieses Beispiel ist für Linux, macOS oder Unix formatiert und verwendet den umgekehrten Schrägstrich (\) zur Verbesserung der Lesbarkeit.

```
$ aws securitylake create-data-lake-organization-configuration \  
--auto-enable-new-account '[{"region": "us-east-1", "sources":  
[{"sourceName": "ROUTE53"}, {"sourceName": "SH_FINDINGS"}, {"sourceName": "VPC_FLOW"}] ]'
```

Nachdem das Verwaltungskonto der Organisation den delegierten Administrator benannt hat, kann der Administrator Security Lake für die Organisation aktivieren und konfigurieren. Dazu gehört die Aktivierung und Konfiguration von Security Lake zum Sammeln von AWS Protokoll- und Ereignisdaten für einzelne Konten in der Organisation. Weitere Informationen finden Sie unter [Erfassung von Daten von AWS-Services](#).

Sie können die [-GetDataLakeOrganizationConfiguration](#) Operation verwenden, um Details zur aktuellen Konfiguration Ihrer Organisation für neue Mitgliedskonten abzurufen.

Entfernen des delegierten Security-Lake-Administrators

Nur das Verwaltungskonto der Organisation kann den delegierten Security-Lake-Administrator für seine Organisation entfernen. Wenn Sie den delegierten Administrator für die Organisation ändern möchten, entfernen Sie den aktuellen delegierten Administrator und weisen Sie dann den neuen delegierten Administrator zu.

Important

Durch das Entfernen des delegierten Security-Lake-Administrators wird Ihr Data Lake gelöscht und Security Lake für die Konten in Ihrer Organisation deaktiviert.

Sie können den delegierten Administrator nicht mithilfe der Security-Lake-Konsole ändern oder entfernen. Diese Aufgaben können nur programmgesteuert ausgeführt werden.

Um den delegierten Administrator programmgesteuert zu entfernen, verwenden Sie die [-DeregisterDataLakeDelegatedAdministrator](#) Operation der Security-Lake-API. Sie müssen die Operation über das Verwaltungskonto der Organisation aufrufen. Wenn Sie die verwenden AWS CLI, führen Sie den [deregister-data-lake-delegated-administrator](#) Befehl über das Verwaltungskonto der Organisation aus.

Mit dem folgenden AWS CLI Befehl wird beispielsweise der delegierte Security-Lake-Administrator entfernt.

```
$ aws securitylake deregister-data-lake-delegated-administrator
```

Um die Bezeichnung des delegierten Administrators beizubehalten, aber die automatischen Konfigurationseinstellungen neuer Mitgliedskonten zu ändern, verwenden Sie die [-DeleteDataLakeOrganizationConfiguration](#) Operation der Security-Lake-API oder, wenn Sie die verwenden AWS CLI, den [-delete-data-lake-organization-configuration](#) Befehl. Nur der delegierte Administrator kann diese Einstellungen für die Organisation ändern.

Mit dem folgenden AWS CLI Befehl wird beispielsweise die automatische Erfassung von Security Hub-Ergebnissen von neuen Mitgliedskonten, die der Organisation beitreten, gestoppt. Neue Mitgliedskonten tragen keine Security Hub-Ergebnisse zum Data Lake bei, nachdem der delegierte Administrator diesen Vorgang aufgerufen hat. Dieses Beispiel ist für Linux, macOS oder Unix formatiert und verwendet den umgekehrten Schrägstrich (\) zur Verbesserung der Lesbarkeit.

```
$ aws securitylake delete-data-lake-organization-configuration \  
--auto-enable-new-account '[{"region":"us-east-1","sources":  
[{"sourceName":"SH_FINDINGS"}]}'
```

Vertrauenswürdiger Zugriff auf Security Lake

Nachdem Sie Security Lake für eine Organisation eingerichtet haben, kann das AWS Organizations Verwaltungskonto den vertrauenswürdigen Zugriff mit Security Lake aktivieren. Vertrauenswürdiger Zugriff ermöglicht es Security Lake, eine serviceverknüpfte IAM-Rolle zu erstellen und Aufgaben in Ihrer Organisation und ihren Konten in Ihrem Namen auszuführen. Weitere Informationen finden Sie unter [Verwenden von AWS Organizations mit anderen AWS-Services](#) im AWS Organizations - Benutzerhandbuch.

Als Benutzer des Organisationsverwaltungskontos können Sie den vertrauenswürdigen Zugriff für Security Lake in deaktivieren AWS Organizations. Anweisungen zum Deaktivieren des vertrauenswürdigen Zugriffs finden Sie unter [So aktivieren oder deaktivieren Sie den vertrauenswürdigen Zugriff](#) im AWS Organizations -Benutzerhandbuch.

Wir empfehlen, den vertrauenswürdigen Zugriff zu deaktivieren, wenn der des delegierten Administrators gesperrt, isoliert oder geschlossen AWS-Konto ist.

Verwalten von -Regionen

Amazon Security Lake kann Sicherheitsprotokolle und Ereignisse sammeln, AWS-Regionen in denen Sie den Service aktiviert haben. Für jede Region werden Ihre Daten in einem anderen Amazon S3 S3-Bucket gespeichert. Sie können unterschiedliche Data Lake-Konfigurationen (z. B. unterschiedliche Quellen und Aufbewahrungseinstellungen) für verschiedene Regionen angeben. Sie können auch eine oder mehrere Rollup-Regionen definieren, um Daten aus mehreren Regionen zu konsolidieren.

Der Status der Region wird überprüft

Security Lake kann Daten über mehrere sammeln AWS-Regionen. Um den Status Ihres Data Lakes nachzuverfolgen, kann es hilfreich sein, zu verstehen, wie die einzelnen Regionen derzeit konfiguriert sind. Wählen Sie Ihre bevorzugte Zugriffsmethode und folgen Sie diesen Schritten, um den aktuellen Status einer Region abzurufen.

Console

Um den Status der Region zu überprüfen

1. Öffnen Sie die Security Lake-Konsole unter <https://console.aws.amazon.com/securitylake/>.
2. Wählen Sie im Navigationsbereich Regionen aus. Die Seite Regionen wird angezeigt und bietet einen Überblick über die Regionen, in denen Security Lake derzeit aktiviert ist.
3. Wählen Sie eine Region aus und klicken Sie dann auf Bearbeiten, um Details für diese Region anzuzeigen.

API

Um den Status der Protokollerfassung in der aktuellen Region abzurufen, verwenden Sie den [GetDataLakeSources](#) Betrieb der Security Lake-API. Wenn Sie den verwenden AWS CLI, führen Sie den [get-data-lake-sources](#) Befehl aus. Geben Sie für den `accounts` Parameter eine oder mehrere AWS-Konto IDs als Liste an. Wenn Ihre Anfrage erfolgreich ist, gibt Security Lake einen Snapshot für die Konten in der aktuellen Region zurück, einschließlich der AWS Quellen, aus denen Security Lake Daten sammelt, und des Status der einzelnen Quellen. Wenn Sie den `accounts` Parameter nicht angeben, enthält die Antwort den Status der Protokollerfassung für alle Konten, für die Security Lake in der aktuellen Region konfiguriert ist.

Mit dem folgenden AWS CLI Befehl wird beispielsweise der Status der Protokollerfassung für die angegebenen Konten in der aktuellen Region abgerufen. Dieses Beispiel ist für Linux, macOS oder Unix formatiert und verwendet den umgekehrten Schrägstrich (\) zur Verbesserung der Lesbarkeit.

```
$ aws securitylake get-data-lake-sources \  
--accounts "123456789012" "111122223333"
```

Der folgende AWS CLI Befehl listet den Protokollerfassungsstatus für alle Konten und aktivierten Quellen in der angegebenen Region auf. Dieses Beispiel ist für Linux, macOS oder Unix formatiert und verwendet den umgekehrten Schrägstrich (\) zur Verbesserung der Lesbarkeit.

```
$ aws securitylake get-data-lake-sources \  
--regions "us-east-1" \  
--query 'dataLakeSources[].[account,sourceName]'
```

Verwenden Sie den [ListDataLakes](#) Vorgang, um festzustellen, ob Sie Security Lake für eine Region aktiviert haben. Wenn Sie den verwenden AWS CLI, führen Sie den [list-data-lakes](#) Befehl aus. Geben Sie für den `regions` Parameter den Regionalcode für die Region an, z. B. `us-east-1` für die Region USA Ost (Nord-Virginia). Eine Liste der Regioncodes finden Sie unter [Amazon Security Lake-Endpoints](#) in der Allgemeine AWS-Referenz. Der `ListDataLakes` Vorgang gibt die Data Lake-Konfigurationseinstellungen für jede Region zurück, die Sie in Ihrer Anfrage angeben. Wenn Sie keine Region angeben, gibt Security Lake den Status und die Konfigurationseinstellungen Ihres Data Lakes in jeder Region zurück, in der Security Lake verfügbar ist.

Der folgende AWS CLI Befehl zeigt beispielsweise den Status und die Konfigurationseinstellungen Ihres Data Lakes in der `eu-central-1` Region. Dieses Beispiel ist für Linux, macOS oder Unix formatiert und verwendet den umgekehrten Schrägstrich (\) zur Verbesserung der Lesbarkeit.

```
$ aws securitylake list-data-lakes \  
--regions "us-east-1" "eu-central-1"
```

Regionseinstellungen ändern

Wählen Sie Ihre bevorzugte Methode und folgen Sie diesen Anweisungen, um die Einstellungen für Ihren Data Lake in einem oder mehreren zu aktualisieren AWS-Regionen.

Console

1. Öffnen Sie die Security Lake-Konsole unter <https://console.aws.amazon.com/securitylake/>.
2. Wählen Sie im Navigationsbereich Regionen aus.
3. Wählen Sie eine Region aus und klicken Sie dann auf Bearbeiten.
4. Aktivieren Sie das Kontrollkästchen Quellen für alle Konten außer Kraft setzen, <Region>um zu bestätigen, dass Ihre Auswahl hier die vorherigen Auswahlen für diese Region überschreibt.
5. Wählen Sie unter Speicherklassen auswählen die Option Übergang hinzufügen aus, um neue Speicherklassen für Ihre Daten hinzuzufügen.
6. Weisen Sie für Tags optional die Tags für die Region zu oder bearbeiten Sie sie. Ein Tag ist eine Bezeichnung, die Sie definieren und bestimmten Ressourcentypen zuweisen können, einschließlich der Data-Lake-Konfiguration für Sie AWS-Konto in einer bestimmten Region. AWS Weitere Informationen hierzu finden Sie unter [Markieren von Amazon Security Lake-Ressourcen](#).
7. Um eine Region in eine Rollup-Region umzuwandeln, wählen Sie im Navigationsbereich Rollup-Regionen (unter Einstellungen) aus. Wählen Sie dann Modify. Wählen Sie im Abschnitt „Rollup-Regionen auswählen“ die Option Rollup-Region hinzufügen aus. Wählen Sie die beitragenden Regionen aus und erteilen Sie Security Lake die Erlaubnis, Daten über mehrere Regionen hinweg zu replizieren. Wenn Sie fertig sind, wählen Sie Speichern, um Ihre Änderungen zu speichern.

API

Verwenden Sie die Security Lake-API, um die Regionseinstellungen für Ihren Data Lake programmgesteuert zu aktualisieren. [UpdateDataLake](#) Wenn Sie den verwenden AWS CLI, führen Sie den [update-data-lake](#)Befehl aus. Geben Sie für den `region` Parameter den Regionalcode für die Region an, für die Sie die Einstellungen ändern möchten, z. B. `us-east-1` für die Region USA Ost (Nord-Virginia). Eine Liste der Regionscodes finden Sie unter [Amazon Security Lake-Endpoints](#) in der Allgemeine AWS-Referenz.

Verwenden Sie zusätzliche Parameter, um für jede Einstellung, die Sie ändern möchten, einen neuen Wert anzugeben, z. B. den Verschlüsselungsschlüssel (`encryptionConfiguration`) und die Aufbewahrungseinstellungen (`lifecycleConfiguration`).

Mit dem folgenden AWS CLI Befehl werden beispielsweise die Einstellungen für Datenablauf und Speicherklassenübergang für die `us-east-1` Region aktualisiert. Dieses Beispiel ist für Linux,

macOS oder Unix formatiert und verwendet den umgekehrten Schrägstrich (\) zur Verbesserung der Lesbarkeit.

```
$ update-data-lake \  
--configurations '[{"region":"us-east-1","lifecycleConfiguration": {"expiration":  
{"days":500},"transitions":[{"days":45,"storageClass":"ONEZONE_IA"}]}]'
```

Konfiguration von Rollup-Regionen

Eine Rollup-Region konsolidiert Daten aus einer oder mehreren beitragenden Regionen. Die Angabe einer Rollup-Region kann Ihnen dabei helfen, die regionalen Compliance-Anforderungen zu erfüllen.

Bevor Sie eine Rollup-Region hinzufügen, müssen Sie zunächst zwei verschiedene Rollen in AWS Identity and Access Management (IAM) erstellen:

- [IAM-Rolle für die Datenreplikation](#)
- [IAM-Rolle zur Registrierung von Partitionen AWS Glue](#)

Note

Security Lake erstellt diese IAM-Rollen oder verwendet vorhandene Rollen in Ihrem Namen, wenn Sie die Security Lake-Konsole verwenden. Sie müssen diese Rollen jedoch erstellen, wenn Sie die Security Lake-API oder AWS CLI verwenden.

IAM-Rolle für die Datenreplikation

Diese IAM-Rolle erteilt Amazon S3 die Erlaubnis, Quellprotokolle und Ereignisse in mehreren Regionen zu replizieren.

Um diese Berechtigungen zu gewähren, erstellen Sie eine IAM-Rolle, die mit dem Präfix `SecurityLake` beginnt, und fügen Sie der Rolle die folgende Beispielrichtlinie hinzu. Sie benötigen den Amazon-Ressourcennamen (ARN) der Rolle, wenn Sie eine Rollup-Region in Security Lake erstellen. In dieser Richtlinie `sourceRegions` handelt es sich um beitragende Regionen und um `destinationRegions` Rollup-Regionen.

```
{  
  "Version": "2012-10-17",
```

```

"Statement": [
  {
    "Sid": "AllowReadS3ReplicationSetting",
    "Action": [
      "s3:ListBucket",
      "s3:GetReplicationConfiguration",
      "s3:GetObjectVersionForReplication",
      "s3:GetObjectVersion",
      "s3:GetObjectVersionAcl",
      "s3:GetObjectVersionTagging",
      "s3:GetObjectRetention",
      "s3:GetObjectLegalHold"
    ],
    "Effect": "Allow",
    "Resource": [
      "arn:aws:s3:::aws-security-data-lake-[[sourceRegions]]*",
      "arn:aws:s3:::aws-security-data-lake-[[sourceRegions]]*/*"
    ],
    "Condition": {
      "StringEquals": {
        "s3:ResourceAccount": [
          "{{bucketOwnerAccountId}}"
        ]
      }
    }
  },
  {
    "Sid": "AllowS3Replication",
    "Action": [
      "s3:ReplicateObject",
      "s3:ReplicateDelete",
      "s3:ReplicateTags",
      "s3:GetObjectVersionTagging"
    ],
    "Effect": "Allow",
    "Resource": [
      "arn:aws:s3:::aws-security-data-lake-[[destinationRegions]]*/*"
    ],
    "Condition": {
      "StringEquals": {
        "s3:ResourceAccount": [
          "{{bucketOwnerAccountId}}"
        ]
      }
    }
  }
]

```

```

    }
  }
]
}

```

Fügen Sie Ihrer Rolle die folgende Vertrauensrichtlinie hinzu, damit Amazon S3 die Rolle übernehmen kann:

```

{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Sid": "AllowS3ToAssume",
      "Effect": "Allow",
      "Principal": {
        "Service": "s3.amazonaws.com"
      },
      "Action": "sts:AssumeRole"
    }
  ]
}

```

Wenn Sie einen vom Kunden verwalteten Schlüssel von AWS Key Management Service (AWS KMS) verwenden, um Ihren Security Lake Data Lake zu verschlüsseln, müssen Sie zusätzlich zu den Berechtigungen in der Datenreplikationsrichtlinie die folgenden Berechtigungen gewähren.

```

{
  "Action": [
    "kms:Decrypt"
  ],
  "Effect": "Allow",
  "Condition": {
    "StringLike": {
      "kms:ViaService": [
        "s3.{sourceRegion1}.amazonaws.com",
        "s3.{sourceRegion2}.amazonaws.com"
      ],
      "kms:EncryptionContext:aws:s3:arn": [
        "arn:aws:s3:::aws-security-data-lake-{sourceRegion1}*",
        "arn:aws:s3:::aws-security-data-lake-{sourceRegion2}*"
      ]
    }
  ]
}

```

```

    },
    "Resource": [
        "{sourceRegion1KmsKeyArn}",
        "{sourceRegion2KmsKeyArn}"
    ]
},
{
    "Action": [
        "kms:Encrypt"
    ],
    "Effect": "Allow",
    "Condition": {
        "StringLike": {
            "kms:ViaService": [
                "s3.{destinationRegion1}.amazonaws.com",
            ],
            "kms:EncryptionContext:aws:s3:arn": [
                "arn:aws:s3:::aws-security-data-lake-{destinationRegion1}*",
            ]
        }
    },
    "Resource": [
        "{destinationRegionKmsKeyArn}"
    ]
}

```

Weitere Informationen zu Replikationsrollen finden Sie unter [Berechtigungen einrichten](#) im Amazon Simple Storage Service-Benutzerhandbuch.

IAM-Rolle zur Registrierung von Partitionen AWS Glue

Diese IAM-Rolle gewährt Berechtigungen für eine AWS Lambda Partitionsaktualisierungsfunktion, die von Security Lake verwendet wird, um AWS Glue Partitionen für die S3-Objekte zu registrieren, die aus anderen Regionen repliziert wurden. Ohne diese Rolle zu erstellen, können Abonnenten keine Ereignisse von diesen Objekten abfragen.

Um diese Berechtigungen zu gewähren, erstellen Sie eine Rolle mit dem Namen `AmazonSecurityLakeMetaStoreManager` (möglicherweise haben Sie diese Rolle bereits beim Onboarding in Security Lake erstellt). Weitere Informationen zu dieser Rolle, einschließlich einer Beispielrichtlinie, finden Sie unter [Schritt 1: IAM-Rollen erstellen](#).

In der Lake Formation Formation-Konsole müssen Sie auch `AmazonSecurityLakeMetaStoreManager` Berechtigungen als Data Lake-Administrator gewähren, indem Sie die folgenden Schritte ausführen:

1. Öffnen Sie die Lake-Formation-Konsole unter <https://console.aws.amazon.com/lakeformation/>.
2. Melden Sie sich als Administratorbenutzer an.
3. Wenn das Fenster Willkommen bei Lake Formation angezeigt wird, wählen Sie den Benutzer aus, den Sie in Schritt 1 erstellt oder ausgewählt haben, und wählen Sie dann Erste Schritte aus.
4. Wenn das Fenster Willkommen bei Lake Formation nicht angezeigt wird, führen Sie die folgenden Schritte aus, um einen Lake Formation-Administrator zu konfigurieren.
 1. Wählen Sie im Navigationsbereich unter Berechtigungen die Option Administrative Rollen und Aufgaben aus. Wählen Sie auf der Konsolenseite im Abschnitt Data Lake-Administratoren die Option Administratoren auswählen aus.
 2. Wählen Sie im Dialogfeld Data Lake-Administratoren verwalten für IAM-Benutzer und -Rollen die `AmazonSecurityLakeMetaStoreManagerIAM`-Rolle aus, die Sie erstellt haben, und klicken Sie dann auf Speichern.

Weitere Informationen zum Ändern der Berechtigungen für Data Lake-Administratoren finden Sie unter [Erstellen eines Data Lake-Administrators](#) im AWS Lake Formation Entwicklerhandbuch.

Rollup-Regionen hinzufügen

Wählen Sie Ihre bevorzugte Zugriffsmethode und folgen Sie diesen Schritten, um eine Rollup-Region hinzuzufügen.

Note

Eine Region kann Daten zu mehreren Rollup-Regionen beitragen. Eine Rollup-Region kann jedoch keine beitragende Region für eine andere Rollup-Region sein.

Console

1. [Öffnen Sie die Security Lake-Konsole unter https://console.aws.amazon.com/securitylake/](https://console.aws.amazon.com/securitylake/).
2. Wählen Sie im Navigationsbereich unter Einstellungen die Option Rollup Regions aus.
3. Wählen Sie Ändern und dann Rollup-Region hinzufügen aus.

4. Geben Sie die Rollup-Region und die beteiligten Regionen an. Wiederholen Sie diesen Schritt, wenn Sie mehrere Rollup-Regionen hinzufügen möchten.
5. Wenn Sie zum ersten Mal eine Rollup-Region hinzufügen, erstellen Sie für den Servicezugriff eine neue IAM-Rolle oder verwenden Sie eine bestehende IAM-Rolle, die Security Lake die Berechtigung erteilt, Daten über mehrere Regionen hinweg zu replizieren.
6. Wählen Sie Save (Speichern) aus, wenn Sie fertig sind.

Sie können auch eine Rollup-Region hinzufügen, wenn Sie bei Security Lake einsteigen. Weitere Informationen finden Sie unter [Erste Schritte mit Amazon Security Lake](#).

API

Um eine Rollup-Region programmgesteuert hinzuzufügen, verwenden Sie den [UpdateDataLake](#) Betrieb der Security Lake-API. Wenn Sie den verwenden, führen Sie den Befehl aus AWS CLI. [update-data-lake](#) Geben Sie in Ihrer Anfrage in dem `region` Feld die Region an, aus der Sie Daten zur Rollup-Region beitragen möchten. Geben Sie im `regions` Array des `replicationConfiguration` Parameters den Regionalcode für jede Rollup-Region an. Eine Liste der Regioncodes finden Sie unter [Amazon Security Lake-Endpoints](#) in der Allgemeine AWS-Referenz.

Die folgenden Befehlssätze werden beispielsweise `ap-northeast-2` als Rollup-Region festgelegt. Die `us-east-1` Region wird Daten zur Region beitragen. `ap-northeast-2` In diesem Beispiel wird auch ein Ablaufzeitraum von 365 Tagen für Objekte festgelegt, die dem Data Lake hinzugefügt werden. Dieses Beispiel ist für Linux, macOS oder Unix formatiert und verwendet den umgekehrten Schrägstrich (`\`) zur Verbesserung der Lesbarkeit.

```
$ aws securitylake update-data-lake \  
--configurations '[{"encryptionConfiguration":  
{"kmsKeyId": "S3_MANAGED_KEY"}, "region": "us-east-1", "replicationConfiguration":  
{"regions": ["ap-northeast-2"], "roleArn": "arn:aws:iam::123456789012:role/service-  
role/AmazonSecurityLakeS3ReplicationRole"}, "lifecycleConfiguration": {"expiration":  
{"days": 365}}}]'
```

Sie können auch eine Rollup-Region hinzufügen, wenn Sie in Security Lake einsteigen. Verwenden Sie dazu die [CreateDataLake](#) Operation (oder, falls Sie den verwenden AWS CLI, den [create-data-lake](#) Befehl). Weitere Informationen zur Konfiguration von Rollup-Regionen beim Onboarding finden Sie unter [Erste Schritte mit Amazon Security Lake](#)

Rollup-Regionen aktualisieren oder entfernen

Wählen Sie Ihre bevorzugte Zugriffsmethode und gehen Sie wie folgt vor, um Rollup-Regionen in Security Lake zu aktualisieren oder zu entfernen.

Console

1. [Öffnen Sie die Security Lake-Konsole unter https://console.aws.amazon.com/securitylake/](https://console.aws.amazon.com/securitylake/).
2. Wählen Sie im Navigationsbereich unter Einstellungen die Option Rollup Regions aus.
3. Wählen Sie Ändern aus.
4. Um die beitragenden Regionen für eine Rollup-Region zu ändern, geben Sie die aktualisierten beitragenden Regionen in der Zeile für die Rollup-Region an.
5. Um eine Rollup-Region zu entfernen, wählen Sie in der Zeile für die Rollup-Region die Option Entfernen aus.
6. Wählen Sie Save (Speichern) aus, wenn Sie fertig sind.

API

Verwenden Sie den Betrieb der Security Lake-API, um Rollup-Regionen programmgesteuert zu konfigurieren. [UpdateDataLake](#) Wenn Sie den verwenden, führen Sie den Befehl aus AWS CLI. [update-data-lake](#) Verwenden Sie in Ihrer Anfrage die unterstützten Parameter, um die Rollup-Einstellungen anzugeben:

- Um eine beitragende Region hinzuzufügen, geben Sie in dem `region` Feld den Regionalcode für die hinzuzufügende Region an. Geben Sie im `regions` Array des `replicationConfiguration` Objekts den Regionalcode für jede Rollup-Region an, zu der Daten beigetragen werden sollen. Eine Liste der Regionscodes finden Sie unter [Amazon Security Lake-Endpoints](#) in der Allgemeine AWS-Referenz.
- Um eine beitragende Region zu entfernen, geben Sie in dem `region` Feld den Regionalcode für die Region an, die entfernt werden soll. Geben Sie für die `replicationConfiguration` Parameter keine Werte an.

Mit dem folgenden Befehl werden beispielsweise sowohl als auch `us-east-2` als `us-east-1` beitragende Regionen konfiguriert. Beide Regionen werden Daten zur `ap-northeast-3` Rollup-Region beitragen. Dieses Beispiel ist für Linux, macOS oder Unix formatiert und verwendet den umgekehrten Schrägstrich (`\`) zur Verbesserung der Lesbarkeit.

```
$ aws securitylake update-data-lake \  
--configurations '[{"encryptionConfiguration":  
  {"kmsKeyId":"S3_MANAGED_KEY"},"region":"us-east-1","replicationConfiguration":  
  {"regions": ["ap-northeast-3"],"roleArn":"arn:aws:iam::123456789012:role/service-  
role/AmazonSecurityLakeS3ReplicationRole"},"lifecycleConfiguration": {"expiration":  
{"days":365}}},  
{"encryptionConfiguration": {"kmsKeyId":"S3_MANAGED_KEY"},"region":"us-  
east-2","replicationConfiguration": {"regions": ["ap-  
northeast-3"],"roleArn":"arn:aws:iam::123456789012:role/service-role/  
AmazonSecurityLakeS3ReplicationRole"}, "lifecycleConfiguration": {"expiration":  
{"days":500},"transitions":[{"days":60,"storageClass":"ONEZONE_IA"}]}]'
```

Quellmanagement

Quellen sind Protokolle und Ereignisse, die von einem einzigen System generiert wurden und einer bestimmten Ereignisklasse im [Offenes Cybersecurity Schema Framework \(OCSF\)](#) Schema entsprechen. Amazon Security Lake kann Protokolle und Ereignisse aus einer Vielzahl von Quellen sammeln, einschließlich nativ unterstützter Quellen AWS-Services und benutzerdefinierter Quellen von Drittanbietern.

Security Lake runs extract, transform, and load (ETL) jobs on raw source data, and converts the data to Apache Parquet format and the OCSF schema. Nach der Verarbeitung speichert Security Lake AWS-Konto AWS-Region Security Lake creates a different Amazon S3 bucket for each Region in which you enable the service. Jede Quelle erhält ein separates Präfix in Ihrem S3-Bucket, und Security Lake organisiert Daten aus jeder Quelle in einem separaten Satz von AWS Lake Formation Tabellen.

Themen

- [Erfassung von Daten von AWS-Services](#)
- [Sammeln von Daten aus benutzerdefinierten Quellen](#)

Erfassung von Daten von AWS-Services

Amazon Security Lake kann Protokolle und Ereignisse von den folgenden nativ AWS-Services unterstützten Geräten sammeln:

- AWS CloudTrail Verwaltung und Datenereignisse (S3, Lambda)
- Auditprotokolle für Amazon Elastic Kubernetes Service (Amazon EKS)
- Amazon-Route-53-Resolver-Abfrageprotokolle
- AWS Security Hub Ergebnisse
- Amazon Virtual Private Cloud (Amazon VPC)-Datendurchflussprotokolle
- AWS WAF v2-Protokolle

Security Lake wandelt diese Daten automatisch in das Apache [Offenes Cybersecurity Schema Framework \(OCSF\)](#) Parquet-Format um.

Tip

Um einen oder mehrere der oben genannten Dienste als Protokollquelle in Security Lake hinzuzufügen, müssen Sie die Protokollierung für diese Dienste nicht separat konfigurieren, mit Ausnahme von CloudTrail Verwaltungsereignissen. Wenn Sie die Protokollierung in diesen Diensten konfiguriert haben, müssen Sie Ihre Protokollierungskonfiguration nicht ändern, um sie als Protokollquellen in Security Lake hinzuzufügen. Security Lake ruft Daten über einen unabhängigen und duplizierten Ereignisstrom direkt von diesen Diensten ab.

Voraussetzung: Überprüfen Sie die Berechtigungen

Um eine AWS-Service als Quelle in Security Lake hinzuzufügen, benötigen Sie die erforderlichen Berechtigungen. Stellen Sie sicher, dass die AWS Identity and Access Management (IAM-) Richtlinie, die der Rolle zugeordnet ist, die Sie zum Hinzufügen einer Quelle verwenden, berechtigt ist, die folgenden Aktionen auszuführen:

- `glue:CreateDatabase`
- `glue:CreateTable`
- `glue:GetDatabase`
- `glue:GetTable`
- `glue:UpdateTable`
- `iam:CreateServiceLinkedRole`
- `s3:GetObject`
- `s3:PutObject`

Es wird empfohlen, dass die Rolle die folgenden Bedingungen und den folgenden Ressourcenbereich für die `s3:PutObject` Berechtigungen `S3:getObject` und erfüllt.

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Sid": "AllowUpdatingSecurityLakeS3Buckets",
      "Effect": "Allow",
      "Action": [
        "s3:GetObject",
```

```
        "s3:PutObject"
    ],
    "Resource": "arn:aws:s3::aws-security-data-lake*",
    "Condition": {
        "StringEquals": {
            "aws:ResourceAccount": "${aws:PrincipalAccount}"
        }
    }
}
]
```

Diese Aktionen ermöglichen es Ihnen, Protokolle und Ereignisse aus dem AN zu sammeln AWS-Service und sie an die richtige AWS Glue Datenbank und Tabelle zu senden.

Wenn Sie einen AWS KMS Schlüssel für die serverseitige Verschlüsselung Ihres Data Lakes verwenden, benötigen Sie auch eine Genehmigung dafür `kms:DescribeKey`.

CloudTrail Ereignisprotokolle

AWS CloudTrail bietet Ihnen einen Verlauf der AWS API-Aufrufe für Ihr Konto, einschließlich API-Aufrufe, die mithilfe der AWS SDKs AWS Management Console, der Befehlszeilentools und bestimmter AWS Dienste getätigt wurden. CloudTrail ermöglicht es Ihnen auch, zu ermitteln, welche Benutzer und Konten AWS APIs für unterstützte Dienste aufgerufen haben CloudTrail, von welcher Quell-IP-Adresse aus die Aufrufe getätigt wurden und wann die Aufrufe erfolgten. Weitere Informationen finden Sie im [AWS CloudTrail -Benutzerhandbuch](#).

Security Lake kann Protokolle im Zusammenhang mit CloudTrail Verwaltungsereignissen und CloudTrail Datenereignissen für S3 und Lambda sammeln. CloudTrail Verwaltungsereignisse, S3-Datenereignisse und Lambda-Datenereignisse sind drei separate Quellen in Security Lake. Aus diesem Grund haben sie unterschiedliche Werte, [sourceName](#) wenn Sie einen dieser Werte als aufgenommene Protokollquelle hinzufügen. Verwaltungsereignisse, auch bekannt als Ereignisse auf Kontrollebene, geben Aufschluss über Verwaltungsvorgänge, die mit Ressourcen in Ihrem AWS-Konto System ausgeführt werden. CloudTrail Datenereignisse, auch bekannt als Operationen auf Datenebene, zeigen die Ressourcenoperationen, die auf oder innerhalb von Ressourcen in Ihrem System ausgeführt wurden AWS-Konto. Bei diesen Vorgängen handelt es sich häufig um umfangreiche Aktivitäten.

Um CloudTrail Verwaltungsereignisse in Security Lake zu sammeln, benötigen Sie mindestens einen CloudTrail regionsübergreifenden Organisationspfad, der CloudTrail Verwaltungsereignisse

mit Lese- und Schreibzugriff sammelt. Die Protokollierung muss für den Trail aktiviert sein. Wenn Sie die Protokollierung in den anderen Diensten konfiguriert haben, müssen Sie Ihre Protokollierungskonfiguration nicht ändern, um sie als Protokollquellen in Security Lake hinzuzufügen. Security Lake ruft Daten über einen unabhängigen und duplizierten Ereignisstrom direkt von diesen Diensten ab.

Ein Trail mit mehreren Regionen liefert Protokolldateien aus mehreren Regionen an einen einzigen Amazon Simple Storage Service (Amazon S3) -Bucket für einen einzigen AWS-Konto. Wenn Sie bereits einen Trail mit mehreren Regionen haben, der über die CloudTrail Konsole oder verwaltet wird AWS Control Tower, sind keine weiteren Maßnahmen erforderlich.

- Informationen zum Erstellen und Verwalten eines Trails finden CloudTrail Sie im AWS CloudTrail Benutzerhandbuch unter [Erstellen eines Trails für eine Organisation](#).
- Informationen zum Erstellen und Verwalten eines AWS Control Tower Trail-Through finden Sie AWS CloudTrail im AWS Control Tower Benutzerhandbuch unter [AWS Control Tower Aktionen protokollieren mit](#).

Wenn Sie CloudTrail Ereignisse als Quelle hinzufügen, beginnt Security Lake sofort mit der Erfassung Ihrer CloudTrail Ereignisprotokolle. Es verarbeitet CloudTrail Verwaltungs- und Datenereignisse direkt aus CloudTrail einem unabhängigen und duplizierten Ereignisstrom.

Security Lake verwaltet Ihre CloudTrail Ereignisse nicht und hat auch keine Auswirkungen auf Ihre bestehenden CloudTrail Konfigurationen. Um den Zugriff und die Aufbewahrung Ihrer CloudTrail Ereignisse direkt zu verwalten, müssen Sie die CloudTrail Servicekonsole oder API verwenden. Weitere Informationen finden Sie im AWS CloudTrail Benutzerhandbuch unter [Ereignisse mit CloudTrail Ereignisverlauf anzeigen](#).

Die folgende Liste enthält GitHub Repository-Links zur Mapping-Referenz, in der beschrieben wird, wie Security Lake CloudTrail Ereignisse auf OCSF normalisiert.

GitHub OCSF-Repository für Ereignisse CloudTrail

- Quellversion 1 ([v1.0.0-rc.2](#))
- [Quellversion 2 \(v1.1.0\)](#)

Amazon EKS-Auditprotokolle

Wenn Sie Amazon EKS Audit Logs als Quelle hinzufügen, beginnt Security Lake mit der Erfassung detaillierter Informationen über die Aktivitäten, die auf den Kubernetes-Ressourcen ausgeführt werden, die in Ihren Elastic Kubernetes Service (EKS) -Clustern ausgeführt werden. EKS-Auditprotokolle helfen Ihnen dabei, potenziell verdächtige Aktivitäten in Ihren EKS-Clustern innerhalb des Amazon Elastic Kubernetes Service zu erkennen.

Security Lake verarbeitet EKS-Audit-Log-Ereignisse direkt aus der Protokollierungsfunktion der Amazon EKS-Kontrollebene über einen unabhängigen und duplizierten Stream von Audit-Protokollen. Dieser Prozess ist so konzipiert, dass keine zusätzliche Einrichtung erforderlich ist und sich auch nicht auf bestehende Protokollierungskonfigurationen der Amazon EKS-Steuerungsebene auswirkt, die Sie möglicherweise haben. Weitere Informationen finden Sie unter [Protokollierung der Amazon EKS-Kontrollebene](#) im Amazon EKS-Benutzerhandbuch.

Amazon EKS-Auditprotokolle werden nur in OCSF v1.1.0 unterstützt. Informationen darüber, wie Security Lake EKS Audit Logs-Ereignisse auf OCSF normalisiert, finden Sie in der Zuordnungsreferenz im [GitHub OCSF-Repository für Amazon EKS Audit Logs-Ereignisse \(v1.1.0\)](#).

Route-53-Resolver-Abfrageprotokolle

Route 53-Resolver-Abfrageprotokolle verfolgen DNS-Abfragen, die von Ressourcen in Ihrer Amazon Virtual Private Cloud (Amazon VPC) gestellt wurden. Auf diese Weise können Sie besser verstehen, wie Ihre Anwendungen funktionieren, und Sicherheitsbedrohungen erkennen.

Wenn Sie Route 53-Resolver-Abfrageprotokolle als Quelle in Security Lake hinzufügen, beginnt Security Lake sofort, Ihre Resolver-Abfrageprotokolle direkt von Route 53 über einen unabhängigen und duplizierten Ereignisstrom zu sammeln.

Security Lake verwaltet Ihre Route 53-Protokolle nicht und hat auch keinen Einfluss auf Ihre bestehenden Resolver-Abfrageprotokollierungskonfigurationen. Um Resolver-Abfrageprotokolle zu verwalten, müssen Sie die Route 53-Servicekonsole verwenden. Weitere Informationen finden Sie unter [Managing Resolver Query Logging Configurations](#) im Amazon Route 53 Developer Guide.

Die folgende Liste enthält GitHub Repository-Links zur Mapping-Referenz, in der beschrieben wird, wie Security Lake Route 53-Protokolle auf OCSF normalisiert.

GitHub OCSF-Repository für Route 53-Protokolle

- Quellversion 1 ([v1.0.0-rc.2](#))

- [Quellversion 2 \(v1.1.0\)](#)

Ergebnisse von Security Hub

Die Ergebnisse von Security Hub helfen Ihnen dabei, Ihre Sicherheitslage zu verstehen, AWS und ermöglichen es Ihnen, Ihre Umgebung anhand von Industriestandards und Best Practices zu überprüfen. Security Hub sammelt Ergebnisse aus verschiedenen Quellen, einschließlich Integrationen mit anderen Produktintegrationen von Drittanbietern AWS-Services, und überprüft sie anhand der Security Hub Hub-Kontrollen. Security Hub verarbeitet Ergebnisse in einem Standardformat namens AWS Security Finding Format (ASFF).

Wenn Sie Security Hub-Ergebnisse als Quelle in Security Lake hinzufügen, beginnt Security Lake sofort, Ihre Ergebnisse über einen unabhängigen und duplizierten Ereignisstrom direkt von Security Hub zu sammeln. Security Lake wandelt auch die Ergebnisse von ASFF in [Offenes Cybersecurity Schema Framework \(OCSF\)](#) (OCSF) um.

Security Lake verwaltet Ihre Security Hub Hub-Ergebnisse nicht und hat auch keinen Einfluss auf Ihre Security Hub Hub-Einstellungen. Um die Security Hub-Ergebnisse zu verwalten, müssen Sie die Security Hub-Servicekonsole, API oder verwenden AWS CLI. Weitere Informationen finden Sie unter [Ergebnisse AWS Security Hub im AWS Security Hub](#) Benutzerhandbuch.

Die folgende Liste enthält GitHub Repository-Links zur Mapping-Referenz, in der beschrieben wird, wie Security Lake Security Hub Hub-Ergebnisse auf OCSF normalisiert.

GitHub OCSF-Repository für Security Hub Hub-Ergebnisse

- Quellversion 1 ([v1.0.0-rc.2](#))
- [Quellversion 2 \(v1.1.0\)](#)

VPC Flow Logs

Die VPC Flow Logs-Funktion von Amazon VPC erfasst Informationen über den IP-Verkehr zu und von Netzwerkschnittstellen in Ihrer Umgebung.

Wenn Sie VPC Flow Logs als Quelle in Security Lake hinzufügen, beginnt Security Lake sofort mit der Erfassung Ihrer VPC Flow Logs. Es verwendet VPC Flow Logs direkt von Amazon VPC über einen unabhängigen und duplizierten Stream von Flow Logs.

Security Lake verwaltet Ihre VPC Flow Logs nicht und hat auch keinen Einfluss auf Ihre Amazon VPC-Konfigurationen. Um Ihre Flow Logs zu verwalten, müssen Sie die Amazon VPC-Servicekonsole verwenden. Weitere Informationen finden Sie unter [Arbeiten mit Flow-Protokollen](#) im Amazon VPC Developer Guide.

Die folgende Liste enthält GitHub Repository-Links zur Mapping-Referenz, in der beschrieben wird, wie Security Lake VPC Flow Logs auf OCSF normalisiert.

GitHub OCSF-Repository für VPC Flow Logs

- Quellversion 1 ([v1.0.0-rc.2](#))
- [Quellversion 2 \(v1.1.0\)](#)

AWS WAF Logs

Wenn Sie Security Lake AWS WAF als Protokollquelle hinzufügen, beginnt Security Lake sofort mit der Erfassung der Protokolle. AWS WAF ist eine Firewall für Webanwendungen, mit der Sie Webanfragen überwachen können, die Ihre Endbenutzer an Ihre Anwendungen senden, und den Zugriff auf Ihre Inhalte kontrollieren können. Zu den protokollierten Informationen gehören die Uhrzeit, zu der eine Webanfrage von Ihrer AWS Ressource AWS WAF empfangen wurde, detaillierte Informationen zu der Anfrage und Details zu den Regeln, denen die Anfrage entsprach.

Security Lake verarbeitet AWS WAF Protokolle direkt aus einem AWS WAF unabhängigen und duplizierten Protokollstrom. Dieser Prozess ist so konzipiert, dass keine zusätzliche Einrichtung erforderlich ist und sich auch nicht auf bestehende AWS WAF Konfigurationen auswirkt. Weitere Informationen dazu, wie Sie Ihre Anwendungsressourcen schützen können, finden Sie im AWS WAF Entwicklerhandbuch unter [So AWS WAF funktioniert](#) es. AWS WAF

Important

Wenn Sie Amazon CloudFront Distribution als Ressourcentyp verwenden AWS WAF, müssen Sie USA Ost (Nord-Virginia) auswählen, um die globalen Protokolle in Security Lake aufzunehmen.

AWS WAF Logs wird nur in OCSF v1.1.0 unterstützt. Informationen darüber, wie Security Lake AWS WAF Log-Ereignisse auf OCSF normalisiert, finden Sie in der Mapping-Referenz im [GitHub OCSF-Repository für AWS WAF Logs \(v1.1.0\)](#).

Eine als Quelle hinzufügen AWS-Service

Nachdem Sie eine AWS-Service als Quelle hinzugefügt haben, beginnt Security Lake automatisch mit der Erfassung von Sicherheitsprotokollen und Ereignissen aus dieser Quelle. In diesen Anweisungen erfahren Sie, wie Sie eine nativ unterstützte Quelle in AWS-Service Security Lake hinzufügen. Anweisungen zum Hinzufügen einer benutzerdefinierten Quelle finden Sie unter

[Sammeln von Daten aus benutzerdefinierten Quellen](#)

Console

So fügen Sie eine AWS Protokollquelle hinzu (Konsole)

1. Öffnen Sie die Security Lake-Konsole unter <https://console.aws.amazon.com/securitylake/>.
2. Wählen Sie im Navigationsbereich Quellen aus.
3. Wählen Sie AWS-Service die Datei aus, von der Sie Daten sammeln möchten, und klicken Sie auf Konfigurieren.
4. Aktivieren Sie im Abschnitt Quelleinstellungen die Quelle und wählen Sie die Version der Datenquelle aus, die Sie für die Datenaufnahme verwenden möchten. Standardmäßig wird die neueste Version der Datenquelle von Security Lake aufgenommen.

Important

Wenn Sie nicht über die erforderlichen Rollenberechtigungen verfügen, um die neue Version der AWS Protokollquelle in der angegebenen Region zu aktivieren, wenden Sie sich an Ihren Security Lake-Administrator. Weitere Informationen finden Sie unter [Rollenberechtigungen aktualisieren](#).

Damit Ihre Abonnenten die ausgewählte Version der Datenquelle aufnehmen können, müssen Sie auch Ihre Abonenteneinstellungen aktualisieren. Einzelheiten zur Bearbeitung eines Abonnenten finden Sie unter [Abonnementverwaltung in Amazon Security Lake](#).

Optional können Sie festlegen, dass nur die neueste Version aufgenommen und alle vorherigen Quellversionen, die für die Datenaufnahme verwendet wurden, deaktiviert werden.

5. Wählen Sie im Abschnitt Regionen die Regionen aus, in denen Sie Daten für die Quelle sammeln möchten. Security Lake sammelt Daten aus der Quelle von allen Konten in den ausgewählten Regionen.

6. Wählen Sie Enable (Aktivieren) aus.

API

Um eine AWS Protokollquelle (API) hinzuzufügen

Verwenden Sie den [CreateAwsLogSource](#) Betrieb der Security Lake-API, um eine programmgesteuert AWS-Service als Quelle hinzuzufügen. Wenn Sie AWS Command Line Interface (AWS CLI) verwenden, führen Sie den Befehl [create-aws-log-source](#) aus. Die Parameter `sourceName` und `regions` müssen angegeben werden. Optional können Sie den Umfang der Quelle auf einen bestimmten oder einen bestimmten Bereich beschränken. `accounts` `sourceVersion`

Important

Wenn Sie in Ihrem Befehl keinen Parameter angeben, geht Security Lake davon aus, dass sich der fehlende Parameter auf den gesamten Satz bezieht. Wenn Sie den `accounts` Parameter beispielsweise nicht angeben, gilt der Befehl für die gesamte Gruppe von Konten in Ihrer Organisation.

Im folgenden Beispiel werden VPC Flow Logs als Quelle in den angegebenen Konten und Regionen hinzugefügt. Dieses Beispiel ist für Linux, macOS oder Unix formatiert und verwendet den umgekehrten Schrägstrich (\) zur Verbesserung der Lesbarkeit.

Note

Wenn Sie diese Anfrage auf eine Region anwenden, in der Sie Security Lake nicht aktiviert haben, erhalten Sie eine Fehlermeldung. Sie können den Fehler beheben, indem Sie Security Lake in dieser Region aktivieren oder indem Sie den `regions` Parameter verwenden, um nur die Regionen anzugeben, in denen Sie Security Lake aktiviert haben.

```
$ aws securitylake create-aws-log-source \  
--sources sourceName=VPC_FLOW,accounts='["123456789012",  
"111122223333"]',regions=["us-east-2"],sourceVersion="2.0"
```

Rollenberechtigungen werden aktualisiert

Wenn Sie nicht über die erforderlichen Rollenberechtigungen oder Ressourcen — neue AWS Lambda Funktion und Amazon Simple Queue Service (Amazon SQS) -Warteschlange — verfügen, um Daten aus einer neuen Version der Datenquelle aufzunehmen, müssen Sie Ihre AmazonSecurityLakeMetaStoreManagerV2 Rollenberechtigungen aktualisieren und einen neuen Satz von Ressourcen erstellen, um Daten aus Ihren Quellen zu verarbeiten.

Wählen Sie Ihre bevorzugte Methode und folgen Sie den Anweisungen, um Ihre Rollenberechtigungen zu aktualisieren und neue Ressourcen zu erstellen, um Daten aus einer neuen Version einer AWS Protokollquelle in einer bestimmten Region zu verarbeiten. Dies ist eine einmalige Aktion, da die Berechtigungen und Ressourcen automatisch auf future Datenquellenversionen angewendet werden.

Console

Um die Rollenberechtigungen zu aktualisieren (Konsole)

1. Öffnen Sie die Security Lake-Konsole unter <https://console.aws.amazon.com/securitylake/>.

Melden Sie sich mit den Anmeldeinformationen des delegierten Security Lake-Administrators an.

2. Klicken Sie im Navigationsbereich unter Settings auf General.
3. Wählen Sie „Rollenberechtigungen aktualisieren“.
4. Führen Sie im Abschnitt Dienstzugriff einen der folgenden Schritte aus:
 - Eine neue Servicerolle erstellen und verwenden — Sie können die von Security Lake erstellte AmazonSecurityLakeMetaStoreManagerV2-Rolle verwenden.
 - Eine bestehende Servicerolle verwenden — Sie können eine vorhandene Servicerolle aus der Liste der Servicerollenamen auswählen.
5. Wählen Sie Apply (Anwenden) aus.

API

So aktualisieren Sie die Rollenberechtigungen (API)

Verwenden Sie den [UpdateDataLake](#) Betrieb der Security Lake-API, um Berechtigungen programmgesteuert zu aktualisieren. Um Berechtigungen mit dem zu aktualisieren AWS CLI, führen Sie den [update-data-lake](#) Befehl aus.

Um Ihre Rollenberechtigungen zu aktualisieren, müssen Sie die [AmazonSecurityLakeMetaStoreManager](#) Richtlinie an die Rolle anhängen.

Die AmazonSecurityLakeMetaStoreManager Rolle wird gelöscht

Important

Nachdem Sie Ihre Rollenberechtigungen auf aktualisiert haben [AmazonSecurityLakeMetaStoreManagerV2](#), stellen Sie sicher, dass der Data Lake ordnungsgemäß funktioniert, bevor Sie die alte [AmazonSecurityLakeMetaStoreManager](#) Rolle entfernen. Es wird empfohlen, mindestens 4 Stunden zu warten, bevor Sie die Rolle entfernen.

Wenn Sie sich entscheiden, die Rolle zu entfernen, müssen Sie zuerst die [AmazonSecurityLakeMetaStoreManager](#) Rolle von AWS Lake Formation löschen.

Gehen Sie wie folgt vor, um die [AmazonSecurityLakeMetaStoreManager](#) Rolle aus der Lake Formation Formation-Konsole zu entfernen.

1. Melden Sie sich bei der AWS Management Console an und öffnen Sie die Lake Formation Formation-Konsole unter <https://console.aws.amazon.com/lakeformation/>.
2. Wählen Sie in der Lake Formation Formation-Konsole im Navigationsbereich die Option Administrative Rollen und Aufgaben aus.
3. [AmazonSecurityLakeMetaStoreManager](#) Aus jeder Region entfernen.

AWS-Service Als Quelle entfernen

Wählen Sie Ihre Zugriffsmethode und gehen Sie wie folgt vor, um eine nativ AWS-Service als Security Lake unterstützte Quelle zu entfernen. Sie können eine Quelle für eine oder mehrere Regionen entfernen. Wenn Sie die Quelle entfernen, beendet Security Lake die Erfassung von Daten aus dieser Quelle in den angegebenen Regionen und Konten, und Abonnenten können keine neuen Daten mehr aus der Quelle nutzen. Abonnenten können jedoch weiterhin Daten

nutzen, die Security Lake vor dem Entfernen aus der Quelle gesammelt hat. Sie können diese Anweisungen nur verwenden, um eine nativ unterstützte AS-Quelle AWS-Service zu entfernen. Informationen zum Entfernen einer benutzerdefinierten Quelle finden Sie unter [Sammeln von Daten aus benutzerdefinierten Quellen](#)

Console

1. Öffnen Sie die Security Lake-Konsole unter <https://console.aws.amazon.com/securitylake/>.
2. Wählen Sie im Navigationsbereich Quellen aus.
3. Wählen Sie eine Quelle aus und klicken Sie auf Deaktivieren.
4. Wählen Sie eine oder mehrere Regionen aus, in denen Sie die Erfassung von Daten aus dieser Quelle beenden möchten. Security Lake beendet die Erfassung von Daten aus der Quelle für alle Konten in den ausgewählten Regionen.

API

Verwenden Sie den [DeleteAwsLogSource](#) Betrieb der Security Lake-API, um eine AWS-Service als Quelle programmgesteuert zu entfernen. Wenn Sie AWS Command Line Interface (AWS CLI) verwenden, führen Sie den Befehl [delete-aws-log-source](#) aus. Die Parameter `sourceName` und `regions` müssen angegeben werden. Optional können Sie den Umfang der Entfernung auf einen bestimmten oder einen bestimmten Bereich beschränken. `accounts sourceVersion`

Important

Wenn Sie in Ihrem Befehl keinen Parameter angeben, geht Security Lake davon aus, dass sich der fehlende Parameter auf den gesamten Satz bezieht. Wenn Sie den `accounts` Parameter beispielsweise nicht angeben, gilt der Befehl für die gesamte Gruppe von Konten in Ihrer Organisation.

Im folgenden Beispiel werden VPC Flow Logs als Quelle in den angegebenen Konten und Regionen entfernt.

```
$ aws securitylake delete-aws-log-source \
--sources sourceName=VPC_FLOW,accounts='["123456789012",
"111122223333"]',regions='["us-east-1", "us-east-2"]',sourceVersion="2.0"
```

Im folgenden Beispiel wird Route 53 als Quelle im angegebenen Konto und in den angegebenen Regionen entfernt.

```
$ aws securitylake delete-aws-log-source \  
--sources sourceName=ROUTE53,accounts='["123456789012"]',regions='["us-east-1", "us-  
east-2"]',sourceVersion="2.0"
```

Die obigen Beispiele sind für Linux, macOS oder Unix formatiert und verwenden zur besseren Lesbarkeit den umgekehrten Schrägstrich (\) als Zeilenfortsetzung.

Den Status der Quellensammlung abrufen

Wählen Sie Ihre Zugriffsmethode und folgen Sie den Schritten, um einen Überblick über die Konten und Quellen zu erhalten, für die die Protokollerfassung in der aktuellen Region aktiviert ist.

Console

Um den Status der Protokollerfassung in der aktuellen Region abzurufen

1. Öffnen Sie die Security Lake-Konsole unter <https://console.aws.amazon.com/securitylake/>.
2. Wählen Sie im Navigationsbereich Accounts aus.
3. Zeigen Sie mit der Maus auf die Zahl in der Spalte Quellen, um zu sehen, welche Protokolle für das ausgewählte Konto aktiviert sind.

API

Um den Status der Protokollerfassung in der aktuellen Region abzurufen, verwenden Sie den [GetDataLakeSources](#) Betrieb der Security Lake-API. Wenn Sie den verwenden AWS CLI, führen Sie den [Befehl get-data-lake-sources](#) aus. Für den `accounts` Parameter können Sie eine oder mehrere AWS-Konto IDs als Liste angeben. Wenn Ihre Anfrage erfolgreich ist, gibt Security Lake einen Snapshot für die Konten in der aktuellen Region zurück, einschließlich der AWS Quellen, aus denen Security Lake Daten sammelt, und des Status der einzelnen Quellen. Wenn Sie den `accounts` Parameter nicht angeben, enthält die Antwort den Status der Protokollerfassung für alle Konten, für die Security Lake in der aktuellen Region konfiguriert ist.

Mit dem folgenden AWS CLI Befehl wird beispielsweise der Status der Protokollerfassung für die angegebenen Konten in der aktuellen Region abgerufen. Dieses Beispiel ist für Linux, macOS

oder Unix formatiert und verwendet den umgekehrten Schrägstrich (\) zur Verbesserung der Lesbarkeit.

```
$ aws securitylake get-data-lake-sources \  
--accounts "123456789012" "111122223333"
```

Sammeln von Daten aus benutzerdefinierten Quellen

Amazon Security Lake kann Protokolle und Ereignisse aus benutzerdefinierten Quellen von Drittanbietern sammeln. Für jede benutzerdefinierte Quelle verarbeitet Security Lake Folgendes:

- Stellt ein eindeutiges Präfix für die Quelle in Ihrem Amazon S3 S3-Bucket bereit.
- Erstellt eine Rolle in AWS Identity and Access Management (IAM), die es einer benutzerdefinierten Quelle ermöglicht, Daten in den Data Lake zu schreiben. Die Berechtigungsgrenze für diese Rolle wird durch eine AWS verwaltete Richtlinie mit dem Namen [AmazonSecurityLakePermissionsBoundary](#) festgelegt.
- Erstellt eine AWS Lake Formation Tabelle zur Organisation von Objekten, die die Quelle in Security Lake schreibt.
- Richtet einen AWS Glue Crawler ein, um Ihre Quelldaten zu partitionieren. Der Crawler füllt die AWS Glue Data Catalog mit der Tabelle. Außerdem erkennt er automatisch neue Quelldaten und extrahiert Schemadefinitionen.

Um Security Lake eine benutzerdefinierte Quelle hinzuzufügen, muss sie die folgenden Anforderungen erfüllen:

1. Ziel — Die benutzerdefinierte Quelle muss in der Lage sein, Daten als Gruppe von S3-Objekten unter dem der Quelle zugewiesenen Präfix in Security Lake zu schreiben. Bei Quellen, die mehrere Datenkategorien enthalten, sollten Sie jede eindeutige [Open Cybersecurity Schema Framework \(OCSF\) -Ereignisklasse](#) als separate Quelle bereitstellen. Security Lake erstellt eine IAM-Rolle, die es der benutzerdefinierten Quelle ermöglicht, an den angegebenen Speicherort in Ihrem S3-Bucket zu schreiben.

Note

Verwenden Sie das [OCSF-Validierungstool](#), um zu überprüfen, ob die benutzerdefinierte Quelle kompatibel ist mit. OCSF Schema 1.1

2. Format — Jedes S3-Objekt, das aus der benutzerdefinierten Quelle gesammelt wurde, sollte als Apache Parquet-Datei formatiert werden.
3. Schema — Dieselbe OCSF-Ereignisklasse sollte für jeden Datensatz innerhalb eines Parquet-formatierten Objekts gelten.

Bewährte Methoden für die Aufnahme benutzerdefinierter Quellen

Um eine effiziente Datenverarbeitung und Abfrage zu ermöglichen, empfehlen wir, beim Hinzufügen einer benutzerdefinierten Quelle zu Security Lake die folgenden bewährten Methoden zu befolgen:

Partitionierung

Objekte sollten nach Quellort, AWS-Region und Datum partitioniert werden. AWS-Konto Der Datenpfad der Partition ist formatiert als. *bucket-name/source-location/region=region/accountId=accountID/eventDay=YYYYMMDD*

Eine Beispielpartition ist *aws-security-data-lake-us-west-2-lake-uid/source-location/region=us-west-2/accountId=123456789012/eventDay=20230428/*.

- *bucket-name*— Der Name des Amazon S3 S3-Buckets, in dem Security Lake Ihre benutzerdefinierten Quelldaten speichert.
- *source-location*— Präfix für die benutzerdefinierte Quelle in Ihrem S3-Bucket. Security Lake speichert alle S3-Objekte für eine bestimmte Quelle unter diesem Präfix, und das Präfix ist für die angegebene Quelle eindeutig.
- *region*— AWS-Region in die die Daten geschrieben werden.
- *accountId*— AWS-Konto ID, auf die sich die Datensätze in der Quellpartition beziehen.
- *eventDay*— Datum, an dem das Ereignis eingetreten ist, formatiert als achtstellige Zeichenfolge (YYYYMMDD).

Größe und Geschwindigkeit des Objekts

In Security Lake geschriebene Objekte sollten Datensätze für 5 Minuten zwischenspeichern. Wenn die Pufferzeit zu viele Daten enthält, um effizient abgefragt werden zu können, können

benutzerdefinierte Quellen mehrere Datensätze innerhalb des 5-Minuten-Fensters schreiben, sofern die durchschnittliche Größe dieser Dateien unter 256 MB bleibt. Benutzerdefinierte Quellen mit geringem Durchsatz können kleinere Objekte alle 5 Minuten schreiben, um eine Aufnahmelatenz von 5 Minuten aufrechtzuerhalten, und können Datensätze für längere Zeiträume zwischenspeichern.

Parquet-Einstellungen

Security Lake unterstützt die Versionen 1.x und 2.x von Parquet. Die Größe der Datenseite sollte auf 1 MB (unkomprimiert) begrenzt sein. Die Zeilengruppengröße sollte nicht größer als 256 MB (komprimiert) sein. Für die Komprimierung innerhalb des Parquet-Objekts wird Standard bevorzugt.

Sortieren

In jedem Objekt im Parquet-Format sollten die Datensätze nach Zeit sortiert werden, um die Kosten für das Abfragen von Daten zu reduzieren.

Voraussetzungen für das Hinzufügen einer benutzerdefinierten Quelle

Beim Hinzufügen einer benutzerdefinierten Quelle erstellt Security Lake eine IAM-Rolle, die es der Quelle ermöglicht, Daten an den richtigen Ort im Data Lake zu schreiben. Der Name der Rolle folgt dem Format `AmazonSecurityLake-Provider-{name of the custom source}-{region}`, AWS-Region in dem Sie die benutzerdefinierte Quelle hinzufügen. `region` Security Lake fügt der Rolle eine Richtlinie hinzu, die den Zugriff auf den Data Lake ermöglicht. Wenn Sie den Data Lake mit einem vom Kunden verwalteten AWS KMS Schlüssel verschlüsselt haben, fügt Security Lake der Rolle auch eine Richtlinie `kms:Decrypt` und `kms:GenerateDataKey` Berechtigungen hinzu. Die Berechtigungsgrenze für diese Rolle wird durch eine AWS verwaltete Richtlinie mit dem Namen [AmazonSecurityLakePermissionsBoundary](#) festgelegt.

Themen

- [Überprüfen der Berechtigungen](#)
- [Erstellen Sie eine IAM-Rolle, um Schreibzugriff auf den Security Lake-Bucket-Speicherort zu gewähren \(API und nur Schritt AWS CLI\)](#)

Überprüfen der Berechtigungen

Stellen Sie vor dem Hinzufügen einer benutzerdefinierten Quelle sicher, dass Sie über die erforderlichen Berechtigungen verfügen, um die folgenden Aktionen auszuführen.

Um Ihre Berechtigungen zu überprüfen, verwenden Sie IAM, um die IAM-Richtlinien zu überprüfen, die mit Ihrer IAM-Identität verknüpft sind. Vergleichen Sie dann die Informationen in diesen Richtlinien mit der folgenden Liste von Aktionen, die Sie ausführen dürfen müssen, um eine benutzerdefinierte Quelle hinzuzufügen.

- `glue:CreateCrawler`
- `glue:CreateDatabase`
- `glue:CreateTable`
- `glue:StopCrawlerSchedule`
- `iam:GetRole`
- `iam:PutRolePolicy`
- `iam>DeleteRolePolicy`
- `iam:PassRole`
- `lakeformation:RegisterResource`
- `lakeformation:GrantPermissions`
- `s3:ListBucket`
- `s3:PutObject`

Diese Aktionen ermöglichen es Ihnen, Protokolle und Ereignisse aus einer benutzerdefinierten Quelle zu sammeln, sie an die richtige AWS Glue Datenbank und Tabelle zu senden und sie in Amazon S3 zu speichern.

Wenn Sie einen AWS KMS Schlüssel für die serverseitige Verschlüsselung Ihres Data Lakes verwenden, benötigen Sie auch die Erlaubnis für `kms:CreateGrant`, `kms:DescribeKey`, und `kms:GenerateDataKey`.

 **Important**

Wenn Sie die Security Lake-Konsole verwenden möchten, um eine benutzerdefinierte Quelle hinzuzufügen, können Sie den nächsten Schritt überspringen und mit fortfahren [Eine benutzerdefinierte Quelle hinzufügen](#). Die Security Lake-Konsole bietet einen optimierten Prozess für den Einstieg und erstellt alle erforderlichen IAM-Rollen oder verwendet bestehende Rollen in Ihrem Namen.

Wenn Sie die Security Lake-API verwenden oder eine benutzerdefinierte Quelle hinzufügen AWS CLI möchten, fahren Sie mit dem nächsten Schritt fort, um eine IAM-Rolle zu erstellen, die Schreibzugriff auf den Security Lake-Bucket-Speicherort ermöglicht.

Erstellen Sie eine IAM-Rolle, um Schreibzugriff auf den Security Lake-Bucket-Speicherort zu gewähren (API und nur Schritt AWS CLI)

Wenn Sie die Security Lake-API verwenden oder eine benutzerdefinierte Quelle hinzufügen AWS CLI möchten, fügen Sie diese IAM-Rolle hinzu, um die AWS Glue Erlaubnis zu erteilen, Ihre benutzerdefinierten Quelldaten zu crawlen und Partitionen in den Daten zu identifizieren. Diese Partitionen sind erforderlich, um Ihre Daten zu organisieren und Tabellen im Datenkatalog zu erstellen und zu aktualisieren.

Nachdem Sie diese IAM-Rolle erstellt haben, benötigen Sie den Amazon-Ressourcennamen (ARN) der Rolle, um eine benutzerdefinierte Quelle hinzuzufügen.

Sie müssen die `arn:aws:iam::aws:policy/service-role/AWSGlueServiceRole` AWS verwaltete Richtlinie anhängen.

Um die erforderlichen Berechtigungen zu gewähren, müssen Sie außerdem die folgende Inline-Richtlinie erstellen und in Ihre Rolle einbetten, um das Lesen von Datendateien aus der benutzerdefinierten Quelle und das Erstellen/Aktualisieren der Tabellen im AWS Glue Datenkatalog AWS-Glue-Crawler zu ermöglichen.

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Sid": "S3WriteRead",
      "Effect": "Allow",
      "Action": [
        "s3:GetObject",
        "s3:PutObject"
      ],
      "Resource": [
        "arn:aws:s3:::{{bucketName}}/*"
      ]
    }
  ]
}
```

```
}
```

Fügen Sie die folgende Vertrauensrichtlinie hinzu, um zuzulassen und AWS-Konto anhand derer es die Rolle auf der Grundlage der externen ID übernehmen kann:

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Principal": {
        "Service": "glue.amazonaws.com"
      },
      "Action": "sts:AssumeRole"
    }
  ]
}
```

Wenn der S3-Bucket in der Region, in der Sie die benutzerdefinierte Quelle hinzufügen, mit einem vom Kunden verwalteten Bucket verschlüsselt ist AWS KMS key, müssen Sie der Rolle und Ihrer KMS-Schlüsselrichtlinie auch die folgende Richtlinie hinzufügen:

```
{
  "Effect": "Allow",
  "Action": [
    "kms:GenerateDataKey",
    "kms:Decrypt"
  ],
  "Condition": {
    "StringLike": {
      "kms:EncryptionContext:aws:s3:arn": [
        "arn:aws:s3:::{{name of S3 bucket created by Security Lake}}"
      ]
    }
  },
  "Resource": [
    "{{ARN of customer managed key}}"
  ]
}
```

Eine benutzerdefinierte Quelle hinzufügen

Nachdem Sie die IAM-Rolle zum Aufrufen des AWS Glue Crawlers erstellt haben, gehen Sie wie folgt vor, um eine benutzerdefinierte Quelle in Security Lake hinzuzufügen.

Console

1. [Öffnen Sie die Security Lake-Konsole unter `https://console.aws.amazon.com/securitylake/`.](https://console.aws.amazon.com/securitylake/)
2. Wählen Sie mithilfe der AWS-Region Auswahl in der oberen rechten Ecke der Seite die Region aus, in der Sie die benutzerdefinierte Quelle erstellen möchten.
3. Wählen Sie im Navigationsbereich Benutzerdefinierte Quellen und dann Benutzerdefinierte Quelle erstellen aus.
4. Geben Sie im Abschnitt Benutzerdefinierte Quelldetails einen weltweit eindeutigen Namen für Ihre benutzerdefinierte Quelle ein. Wählen Sie dann eine OCSF-Ereignisklasse aus, die den Datentyp beschreibt, den die benutzerdefinierte Quelle an Security Lake sendet.
5. Geben Sie für AWS-Konto mit der Berechtigung zum Schreiben von Daten die AWS-Konto ID und die externe ID der benutzerdefinierten Quelle ein, die Protokolle und Ereignisse in den Data Lake schreiben soll.
6. Erstellen und verwenden Sie für Service Access eine neue Servicerolle oder verwenden Sie eine vorhandene Servicerolle, die Security Lake die Berechtigung zum Aufrufen AWS Glue erteilt.
7. Wählen Sie Erstellen.

API

Verwenden Sie den [CreateCustomLogSource](#) Betrieb der Security Lake-API, um programmgesteuert eine benutzerdefinierte Quelle hinzuzufügen. Verwenden Sie den Vorgang AWS-Region dort, wo Sie die benutzerdefinierte Quelle erstellen möchten. Wenn Sie AWS Command Line Interface (AWS CLI) verwenden, führen Sie den Befehl [create-custom-log-source](#) aus.

Verwenden Sie in Ihrer Anfrage die unterstützten Parameter, um die Konfigurationseinstellungen für die benutzerdefinierte Quelle anzugeben:

- `sourceName`— Geben Sie einen Namen für die Quelle an. Der Name muss ein regional eindeutiger Wert sein.

- `eventClasses`— Geben Sie eine oder mehrere OCSF-Ereignisklassen an, um den Datentyp zu beschreiben, den die Quelle an Security Lake sendet. Eine Liste der OCSF-Ereignisklassen, die in Security Lake als Quelle unterstützt werden, finden Sie unter [Open Cybersecurity Schema Framework \(OCSF\)](#).
- `sourceVersion`— Geben Sie optional einen Wert an, um die Protokollerfassung auf eine bestimmte Version von benutzerdefinierten Quelldaten zu beschränken.
- `crawlerConfiguration`— Geben Sie den Amazon-Ressourcennamen (ARN) der IAM-Rolle an, die Sie zum Aufrufen des AWS Glue Crawlers erstellt haben. Die detaillierten Schritte zum Erstellen einer IAM-Rolle finden Sie unter [Voraussetzungen für das Hinzufügen einer benutzerdefinierten Quelle](#)
- `providerIdentity`— Geben Sie die AWS Identität und die externe ID an, die die Quelle zum Schreiben von Protokollen und Ereignissen in den Data Lake verwenden soll.

Im folgenden Beispiel wird dem angegebenen Protokollanbieter-Konto in bestimmten Regionen eine benutzerdefinierte Quelle als Protokollquelle hinzugefügt. Dieses Beispiel ist für Linux, macOS oder Unix formatiert und verwendet den umgekehrten Schrägstrich (\) zur Verbesserung der Lesbarkeit.

```
$ aws securitylake create-custom-log-source \  
--source-name EXAMPLE_CUSTOM_SOURCE \  
--event-classes ['"DNS_ACTIVITY", '"NETWORK_ACTIVITY"'] \  
--configuration crawlerConfiguration={"roleArn=arn:aws:iam::XXX:role/service-role/RoLeName"},providerIdentity={"externalId=ExternalId,principal=principal"} \  
--region=["ap-southeast-2"]
```

Halten Sie die benutzerdefinierten Quelldaten auf dem neuesten Stand in AWS Glue

Nachdem Sie eine benutzerdefinierte Quelle in Security Lake hinzugefügt haben, erstellt Security Lake einen AWS Glue Crawler. Der Crawler stellt eine Verbindung zu Ihrer benutzerdefinierten Quelle her, bestimmt die Datenstrukturen und füllt den AWS Glue Datenkatalog mit Tabellen.

Wir empfehlen, den Crawler manuell auszuführen, um Ihr benutzerdefiniertes Quellschema auf dem neuesten Stand zu halten und die Abfragefunktionen in Athena und anderen Abfragediensten aufrechtzuerhalten. Insbesondere sollten Sie den Crawler ausführen, wenn eine der folgenden Änderungen in Ihrem Eingabedatensatz für eine benutzerdefinierte Quelle eintritt:

- Der Datensatz hat eine oder mehrere neue Spalten auf oberster Ebene.
- Der Datensatz enthält ein oder mehrere neue Felder in einer Spalte mit einem struct Datentyp.

Anweisungen zum Ausführen eines Crawlers finden Sie unter [Planung eines AWS Glue Crawlers](#) im Entwicklerhandbuch.AWS Glue

Security Lake kann bestehende Crawler in Ihrem Konto nicht löschen oder aktualisieren. Wenn Sie eine benutzerdefinierte Quelle löschen, empfehlen wir, den zugehörigen Crawler zu löschen, wenn Sie in future eine benutzerdefinierte Quelle mit demselben Namen erstellen möchten.

Löschen einer benutzerdefinierten Quelle

Löschen Sie eine benutzerdefinierte Quelle, um das Senden von Daten von der Quelle an Security Lake zu beenden.

Console

1. Öffnen Sie die Security Lake-Konsole unter <https://console.aws.amazon.com/securitylake/>.
2. Wählen Sie mithilfe der AWS-Region Auswahl in der oberen rechten Ecke der Seite die Region aus, aus der Sie die benutzerdefinierte Quelle entfernen möchten.
3. Wählen Sie im Navigationsbereich Benutzerdefinierte Quellen aus.
4. Wählen Sie die benutzerdefinierte Quelle aus, die Sie entfernen möchten.
5. Wählen Sie „Benutzerdefinierte Quelle abmelden“ und anschließend „Löschen“, um die Aktion zu bestätigen.

API

Um eine benutzerdefinierte Quelle programmgesteuert zu löschen, verwenden Sie den [DeleteCustomLogSource](#) Betrieb der Security Lake-API. Wenn Sie AWS Command Line Interface (AWS CLI) verwenden, führen Sie den Befehl [delete-custom-log-source](#) aus. Verwenden Sie den Vorgang an der AWS-Region Stelle, an der Sie die benutzerdefinierte Quelle löschen möchten.

Verwenden Sie in Ihrer Anfrage den `sourceName` Parameter, um den Namen der benutzerdefinierten Quelle anzugeben, die gelöscht werden soll. Oder geben Sie den Namen der benutzerdefinierten Quelle an und verwenden Sie den `sourceVersion` Parameter, um den Umfang des Löschvorgangs auf eine bestimmte Version von Daten aus der benutzerdefinierten Quelle zu beschränken.

Im folgenden Beispiel wird eine benutzerdefinierte Protokollquelle aus Security Lake gelöscht.

Dieses Beispiel ist für Linux, macOS oder Unix formatiert und verwendet den umgekehrten Schrägstrich (\) zur Verbesserung der Lesbarkeit.

```
$ aws securitylake delete-custom-log-source \  
--source-name EXAMPLE_CUSTOM_SOURCE
```

Abonnentenverwaltung in Amazon Security Lake

Ein Amazon Security Lake-Abonnent nutzt Protokolle und Ereignisse von Security Lake. Um die Kosten unter Kontrolle zu halten und die bewährten Methoden für den Zugriff mit geringsten Rechten einzuhalten, gewähren Sie Abonnenten Zugriff auf Daten auf Quellenbasis. Weitere Informationen zu Quellen finden Sie unter [Quellmanagement](#).

Security Lake unterstützt zwei Arten des Abonnentenzugriffs:

- **Datenzugriff** — Abonnenten werden über neue Amazon S3 S3-Objekte für eine Quelle informiert, wenn die Objekte in den Security Lake Data Lake geschrieben werden. Abonnenten können über einen Abonnementendpunkt oder durch Abfragen einer Amazon Simple Queue Service (Amazon SQS) -Warteschlange direkt auf die S3-Objekte zugreifen und Benachrichtigungen über neue Objekte erhalten. Dieser Abonnementtyp wird wie S3 im `accessTypes` API-Parameter angegeben. [CreateSubscriber](#)
- **Zugriff abfragen** — Abonnenten fragen mithilfe von Diensten wie Amazon Athena Quelldaten aus AWS Lake Formation Tabellen in Ihrem S3-Bucket ab. Dieser Abonnementtyp wird wie LAKEFORMATION im `accessTypes` Parameter der [CreateSubscriber](#) API identifiziert.

Abonnenten haben nur Zugriff auf die Quelldaten AWS-Region, die Sie bei der Erstellung des Abonnenten auswählen. Um einem Abonnenten Zugriff auf Daten aus mehreren Regionen zu gewähren, können Sie die Region, in der Sie den Abonnenten erstellen, als Rollup-Region angeben und andere Regionen Daten dazu beitragen lassen. Weitere Informationen zu Rollup-Regionen und beitragenden Regionen finden Sie unter [Verwalten von -Regionen](#)

Important

Die maximale Anzahl von Quellen, die Security Lake pro Abonnent hinzufügen kann, ist 10. Dies kann eine Kombination aus AWS Quellen und benutzerdefinierten Quellen sein.

Themen

- [Verwaltung des Datenzugriffs für Security Lake-Abonnenten](#)
- [Verwaltung des Abfragezugriffs für Security Lake-Abonnenten](#)

Verwaltung des Datenzugriffs für Security Lake-Abonnenten

Abonnenten mit Datenzugriff auf Quelldaten in Amazon Security Lake werden über neue Objekte für die Quelle informiert, wenn die Daten in den S3-Bucket geschrieben werden. Standardmäßig werden Abonnenten über einen von ihnen bereitgestellten HTTPS-Endpunkt über neue Objekte informiert. Alternativ können Abonnenten über neue Objekte informiert werden, indem sie eine Amazon Simple Queue Service (Amazon SQS) -Warteschlange abfragen.

Voraussetzungen für die Erstellung eines Abonnenten mit Datenzugriff

Sie müssen die folgenden Voraussetzungen erfüllen, bevor Sie einen Abonnenten mit Datenzugriff in Security Lake erstellen können.

Themen

- [Überprüfen der Berechtigungen](#)
- [Rufen Sie die externe ID des Abonnenten ab](#)
- [Erstellen Sie eine IAM-Rolle zum Aufrufen von EventBridge API-Zielen \(Schritt „Nur API“\) AWS CLI](#)

Überprüfen der Berechtigungen

Um Ihre Berechtigungen zu überprüfen, verwenden Sie IAM, um die IAM-Richtlinien zu überprüfen, die mit Ihrer IAM-Identität verknüpft sind. Vergleichen Sie dann die Informationen in diesen Richtlinien mit der folgenden Liste von (Berechtigungs-) Aktionen, die Sie benötigen, um Abonnenten zu benachrichtigen, wenn neue Daten in den Data Lake geschrieben werden.

Sie benötigen eine Genehmigung, um die folgenden Aktionen ausführen zu können:

- `iam:CreateRole`
- `iam>DeleteRolePolicy`
- `iam:GetRole`
- `iam:PutRolePolicy`
- `lakeformation:GrantPermissions`
- `lakeformation:ListPermissions`
- `lakeformation:RegisterResource`
- `lakeformation:RevokePermissions`

- `ram:GetResourceShareAssociations`
- `ram:GetResourceShares`
- `ram:UpdateResourceShare`

Zusätzlich zu der obigen Liste benötigen Sie auch die Erlaubnis, die folgenden Aktionen auszuführen:

- `events:CreateApiDestination`
- `events:CreateConnection`
- `events:DescribeRule`
- `events:ListApiDestinations`
- `events:ListConnections`
- `events:PutRule`
- `events:PutTargets`
- `s3:GetBucketNotification`
- `s3:PutBucketNotification`
- `sqs:CreateQueue`
- `sqs>DeleteQueue`
- `sqs:GetQueueAttributes`
- `sqs:GetQueueUrl`
- `sqs:SetQueueAttributes`

Rufen Sie die externe ID des Abonnenten ab

Um einen Abonnenten zu erstellen, benötigen Sie neben der AWS-Konto Abonnenten-ID auch dessen externe ID. Die externe ID ist eine eindeutige Kennung, die Ihnen der Abonnent zur Verfügung stellt. Security Lake fügt die externe ID der Abonnenten-IAM-Rolle hinzu, die es erstellt. Sie verwenden die externe ID, wenn Sie einen Abonnenten in der Security Lake-Konsole, über die API oder AWS CLI erstellen.

Weitere Informationen zu externen IDs finden Sie im IAM-Benutzerhandbuch unter [So verwenden Sie eine externe ID, wenn Sie Dritten Zugriff auf Ihre AWS Ressourcen gewähren](#).

⚠ Important

Wenn Sie die Security Lake-Konsole verwenden möchten, um einen Abonnenten hinzuzufügen, können Sie den nächsten Schritt überspringen und mit fortfahren [Einen Abonnenten mit Datenzugriff erstellen](#). Die Security Lake-Konsole bietet einen optimierten Prozess für den Einstieg und erstellt alle erforderlichen IAM-Rollen oder verwendet bestehende Rollen in Ihrem Namen.

Wenn Sie die Security Lake-API verwenden oder einen Abonnenten hinzufügen AWS CLI möchten, fahren Sie mit dem nächsten Schritt fort, um eine IAM-Rolle zum Aufrufen EventBridge von API-Zielen zu erstellen.

Erstellen Sie eine IAM-Rolle zum Aufrufen von EventBridge API-Zielen (Schritt „Nur API“) AWS CLI

Wenn Sie Security Lake über API oder verwenden AWS CLI, erstellen Sie eine Rolle in AWS Identity and Access Management (IAM), die Amazon EventBridge Berechtigungen zum Aufrufen von API-Zielen und zum Senden von Objektbenachrichtigungen an die richtigen HTTPS-Endpunkte gewährt.

Nachdem Sie diese IAM-Rolle erstellt haben, benötigen Sie den Amazon-Ressourcennamen (ARN) der Rolle, um den Abonnenten zu erstellen. Diese IAM-Rolle ist nicht erforderlich, wenn der Abonnent Daten aus einer Amazon Simple Queue Service (Amazon SQS) -Warteschlange abfragt oder Daten direkt abfragt. AWS Lake Formation Weitere Informationen zu dieser Art von Datenzugriffsmethode (Zugriffstyp) finden Sie unter. [Verwaltung des Abfragezugriffs für Security Lake-Abbonenten](#)

Fügen Sie Ihrer IAM-Rolle die folgende Richtlinie hinzu:

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Sid": "AllowInvokeApiDestination",
      "Effect": "Allow",
      "Action": [
        "events:InvokeApiDestination"
      ],
      "Resource": [
        "arn:aws:events:{us-west-2}:{123456789012}:api-destination/AmazonSecurityLake*/*"
      ]
    }
  ]
}
```

```
    ]
  }
]
}
```

Fügen Sie Ihrer IAM-Rolle die folgende Vertrauensrichtlinie hinzu, damit Sie diese Rolle übernehmen EventBridge können:

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Sid": "AllowEventBridgeToAssume",
      "Effect": "Allow",
      "Principal": {
        "Service": "events.amazonaws.com"
      },
      "Action": "sts:AssumeRole"
    }
  ]
}
```

Security Lake erstellt automatisch eine IAM-Rolle, die es dem Abonnenten ermöglicht, Daten aus dem Data Lake zu lesen (oder Ereignisse aus einer Amazon SQS SQS-Warteschlange abzufragen, wenn dies die bevorzugte Benachrichtigungsmethode ist). Diese Rolle ist durch eine AWS verwaltete Richtlinie namens geschützt. [AmazonSecurityLakePermissionsBoundary](#)

Einen Abonnenten mit Datenzugriff erstellen

Wählen Sie eine der folgenden Zugriffsmethoden, um einen Abonnenten mit Zugriff auf aktuelle Daten zu erstellen AWS-Region.

Console

1. Öffnen Sie die Security Lake-Konsole unter <https://console.aws.amazon.com/securitylake/>.
2. Wählen Sie mithilfe der AWS-Region Auswahl in der oberen rechten Ecke der Seite die Region aus, in der Sie den Abonnenten erstellen möchten.
3. Wählen Sie im Navigationsbereich Abonnenten aus.
4. Wählen Sie auf der Seite Abonnenten die Option Abonnent erstellen aus.

5. Geben Sie für Abonentendetails den Namen des Abonnenten und optional eine Beschreibung ein.

Die Region wird automatisch so ausgefüllt, wie Sie sie aktuell ausgewählt haben, AWS-Region und kann nicht geändert werden.

6. Wählen Sie für Protokoll- und Ereignisquellen aus, welche Quellen der Abonnent nutzen darf.
7. Wählen Sie als Datenzugriffsmethode S3 aus, um den Datenzugriff für den Abonnenten einzurichten.
8. Geben Sie für Abonentenanmeldedaten die AWS-Konto ID und die [externe ID](#) des Abonnenten an.
9. (Optional) Wenn Sie möchten, dass Security Lake eine Amazon SQS SQS-Warteschlange erstellt, die der Abonnent nach Objektbenachrichtigungen abfragen kann, wählen Sie SQS-Warteschlange aus. Wenn Sie möchten, dass Security Lake Benachrichtigungen an einen HTTPS-Endpunkt sendet, wählen Sie Abonnement-Endpunkt aus. EventBridge

Wenn Sie Abonnement-Endpunkt auswählen, gehen Sie außerdem wie folgt vor:

- a. Geben Sie den Abonnement-Endpunkt ein. Beispiele für gültige Endpunktformate sind: **http://example.com** Optional können Sie auch einen HTTPS-Schlüsselnamen und einen HTTPS-Schlüsselwert angeben.
- b. Erstellen Sie für Service Access eine neue IAM-Rolle oder verwenden Sie eine vorhandene IAM-Rolle, die das Aufrufen von API-Zielen und das Senden von Objektbenachrichtigungen an die richtigen Endpunkte ermöglicht EventBridge.

Informationen zum Erstellen einer neuen IAM-Rolle finden Sie unter [Erstellen einer IAM-Rolle zum Aufrufen von API-Zielen](#). EventBridge

10. (Optional) Geben Sie für Tags bis zu 50 Tags ein, die dem Abonnenten zugewiesen werden sollen.

Ein Tag ist eine Bezeichnung, die Sie definieren und bestimmten Ressourcentypen AWS zuweisen können. Jedes Tag besteht aus einem erforderlichen Tag-Schlüssel und einem optionalen Tag-Wert. Mithilfe von Tags können Sie Ressourcen auf unterschiedliche Weise identifizieren, kategorisieren und verwalten. Weitere Informationen hierzu finden Sie unter [Markieren von Amazon Security Lake-Ressourcen](#).

11. Wählen Sie Erstellen.

API

Verwenden Sie die Security Lake-API, um programmgesteuert einen Abonnenten mit [CreateSubscriber](#)Datenzugriff zu erstellen. Wenn Sie AWS Command Line Interface (AWS CLI) verwenden, führen Sie den Befehl [create-subscriber](#) aus.

Verwenden Sie in Ihrer Anfrage diese Parameter, um die folgenden Einstellungen für den Abonnenten anzugeben:

- Geben Sie für `sources` jede Quelle an, auf die der Abonnent zugreifen soll.
- Geben Sie für `subscriberIdentity` die AWS Konto-ID und die externe ID an, die der Abonnent für den Zugriff auf Quelldaten verwenden wird.
- Geben Sie für `subscriber-name` den Namen des Abonnenten an.
- Legen Sie für `accessTypes` die Option `S3` fest.

Beispiel 1

Im folgenden Beispiel wird ein Abonnent mit Zugriff auf Daten in der aktuellen AWS Region für die angegebene Abonnenten-Identität für eine AWS Quelle erstellt.

```
$ aws securitylake create-subscriber \  
--subscriber-identity {"accountID": 1293456789123,"externalId": 123456789012} \  
--sources [{"awsLogSource": {"sourceName": VPC_FLOW, sourceVersion": 2.0}}] \  
--subscriber-name subscriber name \  
--access-types S3
```

Beispiel 2

Im folgenden Beispiel wird ein Abonnent mit Zugriff auf Daten in der aktuellen AWS Region für die angegebene Abonnenten-Identität für eine benutzerdefinierte Quelle erstellt.

```
$ aws securitylake create-subscriber \  
--subscriber-identity {"accountID": 1293456789123,"externalId": 123456789012} \  
--sources [{"customLogSource": {"sourceName": custom-source-name, sourceVersion": 2.0}}] \  
\  
--subscriber-name subscriber name \  
--access-types S3
```

Die obigen Beispiele sind für Linux, macOS oder Unix formatiert und verwenden zur besseren Lesbarkeit den umgekehrten Schrägstrich (\) als Zeilenfortsetzung.

(Optional) Nachdem Sie einen Abonnenten erstellt haben, geben Sie mit dem Vorgang [CreateSubscriberBenachrichtigung](#) an, wie der Abonnent benachrichtigt werden soll, wenn neue Daten für die Quellen, auf die der Abonnent zugreifen soll, in den Data Lake geschrieben werden. Wenn Sie AWS Command Line Interface (AWS CLI) verwenden, führen Sie den Befehl [create-subscriber-notification](#) aus.

- Um die Standardbenachrichtigungsmethode (HTTPS-Endpunkt) zu überschreiben und eine Amazon SQS SQS-Warteschlange zu erstellen, geben Sie Werte für die `sqsNotificationConfiguration` Parameter an.
- Wenn Sie eine Benachrichtigung mit einem HTTPS-Endpunkt bevorzugen, geben Sie Werte für die `httpsNotificationConfiguration` Parameter an.
- Geben Sie für das `targetRoleArn` Feld den ARN der IAM-Rolle an, die Sie zum Aufrufen von EventBridge API-Zielen erstellt haben.

```
$ aws securitylake create-subscriber-notification \  
--subscriber-id "12345ab8-1a34-1c34-1bd4-12345ab9012" \  
--configuration  
httpsNotificationConfiguration={"targetRoleArn":"arn:aws:iam::XXX:role/service-  
role/RoleName", "endpoint":"https://account-management.$3.$2.securitylake.aws.dev/  
v1/dataLake"}
```

Um das abzurufensubscriberID, verwenden Sie den [ListSubscribers](#) Betrieb der Security Lake-API. Wenn Sie AWS Command Line Interface (AWS CLI) verwenden, führen Sie den Befehl [list-subscriber](#) aus.

```
$ aws securitylake list-subscribers
```

Um anschließend die Benachrichtigungsmethode (Amazon SQS SQS-Warteschlange oder HTTPS-Endpunkt) für den Abonnenten zu ändern, verwenden Sie den Vorgang [UpdateSubscriberBenachrichtigung](#) oder, falls Sie den verwenden AWS CLI, führen Sie den Befehl [update-subscriber-notification](#) aus. Sie können die Benachrichtigungsmethode auch mithilfe der Security Lake-Konsole ändern: Wählen Sie den Abonnenten auf der Abonnentenseite aus und klicken Sie dann auf Bearbeiten.

Beispiel für eine Objektbenachrichtigung

```
{
  "source": "aws.s3",
  "time": "2021-11-12T00:00:00Z",
  "account": "123456789012",
  "region": "ca-central-1",
  "resources": [
    "arn:aws:s3:::example-bucket"
  ],
  "detail": {
    "bucket": {
      "name": "example-bucket"
    },
    "object": {
      "key": "example-key",
      "size": 5,
      "etag": "b57f9512698f4b09e608f4f2a65852e5"
    },
    "request-id": "N4N7GDK58NMKJ12R",
    "requester": "securitylake.amazonaws.com"
  }
}
```

Aktualisierung eines Datenabonnenten

Sie können einen Abonnenten aktualisieren, indem Sie die Quellen ändern, aus denen der Abonnent Daten bezieht. Sie können einem Abonnenten auch die Tags zuweisen oder bearbeiten. Ein Tag ist eine Bezeichnung, die Sie definieren und bestimmten Ressourcentypen AWS, einschließlich Abonnenten, zuweisen können. Weitere Informationen hierzu finden Sie unter [Markieren von Amazon Security Lake-Ressourcen](#).

Wählen Sie eine der Zugriffsmethoden und folgen Sie diesen Schritten, um neue Quellen für ein vorhandenes Abonnement zu definieren.

Console

1. Öffnen Sie die Security Lake-Konsole unter <https://console.aws.amazon.com/securitylake/>.
2. Wählen Sie im Navigationsbereich Abonnenten aus.
3. Wählen Sie den Abonnenten aus.

4. Wählen Sie Bearbeiten und führen Sie dann einen der folgenden Schritte aus:
 - Um die Quellen für den Abonnenten zu aktualisieren, geben Sie die neuen Einstellungen im Abschnitt Protokoll- und Ereignisquellen ein.
 - Um dem Abonnenten Tags zuzuweisen oder zu bearbeiten, ändern Sie die Tags nach Bedarf im Abschnitt Tags.
5. Wählen Sie Save (Speichern) aus, wenn Sie fertig sind.

API

Um die Datenzugriffsquellen für einen Abonnenten programmgesteuert zu aktualisieren, verwenden Sie den [UpdateSubscriber](#) Betrieb der Security Lake-API. Wenn Sie AWS Command Line Interface (AWS CLI) verwenden, führen Sie den Befehl [update-subscriber](#) aus. Verwenden Sie in Ihrer Anfrage die `sources` Parameter, um jede Quelle anzugeben, auf die der Abonnent zugreifen soll.

```
$ aws securitylake update-subscriber --subscriber-id subscriber ID
```

Verwenden Sie den [ListSubscribers](#) Vorgang, um eine Liste von Abonnenten zu erhalten, die einer bestimmten Organisation AWS-Konto oder einem bestimmten Unternehmen zugeordnet sind. Wenn Sie AWS Command Line Interface (AWS CLI) verwenden, führen Sie den Befehl [list-subscribers](#) aus.

```
$ aws securitylake list-subscribers
```

[Verwenden Sie die GetSubscriberOperation, um die aktuellen Einstellungen für einen bestimmten Abonnenten zu überprüfen. Führen Sie den Befehl get-subscriber aus.](#) Security Lake gibt dann den Namen und die Beschreibung des Abonnenten, die externe ID und weitere Informationen zurück. Wenn Sie AWS Command Line Interface (AWS CLI) verwenden, führen Sie den Befehl [get-subscriber](#) aus.

[Verwenden Sie den Vorgang Notification, um die Benachrichtigungsmethode für einen Abonnenten zu aktualisieren. UpdateSubscriber](#) Wenn Sie AWS Command Line Interface (AWS CLI) verwenden, führen Sie den Befehl [update-subscriber-notification](#) aus. Sie können beispielsweise einen neuen HTTPS-Endpunkt für den Abonnenten angeben oder von einem HTTPS-Endpunkt zu einer Amazon SQS SQS-Warteschlange wechseln.

Einen Datenabonnenten entfernen

Wenn Sie nicht mehr möchten, dass ein Abonnent Daten von Security Lake nutzt, können Sie den Abonnenten entfernen, indem Sie die folgenden Schritte ausführen.

Console

1. Öffnen Sie die Security Lake-Konsole unter <https://console.aws.amazon.com/securitylake/>.
2. Wählen Sie im Navigationsbereich Abonnenten aus.
3. Wählen Sie den Abonnenten aus, den Sie entfernen möchten.
4. Wählen Sie Delete (Löschen) und bestätigen Sie die Aktion. Dadurch werden der Abonnent und alle zugehörigen Benachrichtigungseinstellungen gelöscht.

API

Gehen Sie je nach Szenario wie folgt vor:

- Verwenden Sie die Security Lake-API, um den [DeleteSubscriber](#) Abonnenten und alle zugehörigen Benachrichtigungseinstellungen zu löschen. Wenn Sie AWS Command Line Interface (AWS CLI) verwenden, führen Sie den Befehl [delete-subscriber](#) aus.
- Um den Abonnenten zu behalten, aber future Benachrichtigungen an den Abonnenten zu beenden, verwenden Sie den [DeleteSubscriberNotification](#) der Security Lake-API. Wenn Sie AWS Command Line Interface (AWS CLI) verwenden, führen Sie den Befehl run the [delete-subscriber-notification](#) aus.

Verwaltung des Abfragezugriffs für Security Lake-Abonnenten

Abonnenten mit Abfragezugriff können Daten abfragen, die Security Lake sammelt. Diese Abonnenten fragen mit Diensten wie Amazon Athena direkt AWS Lake Formation Tabellen in Ihrem S3-Bucket ab. Obwohl Athena die primäre Abfrage-Engine für Security Lake ist, können Sie auch andere Dienste wie [Amazon Redshift Spectrum](#) und Spark SQL verwenden, die in den integriert sind. AWS Glue Data Catalog

Note

In diesem Abschnitt wird erklärt, wie Sie einem Drittanbieter Abfragezugriff gewähren. Hinweise zum Ausführen von Abfragen für Ihren eigenen Data Lake finden Sie unter [Schritt 4: Ihre eigenen Daten anzeigen und abfragen](#).

Voraussetzungen für die Erstellung eines Abonnenten mit Abfragezugriff

Sie müssen die folgenden Voraussetzungen erfüllen, bevor Sie einen Abonnenten mit Datenzugriff in Security Lake erstellen können.

Themen

- [Überprüfen der Berechtigungen](#)
- [Erstellen Sie eine IAM-Rolle, um Security Lake-Daten abzufragen \(API und nur Schritt AWS CLI\)](#)
- [Gewähren Sie Lake Formation-Administratorrechte](#)

Überprüfen der Berechtigungen

Bevor Sie einen Abonnenten mit Abfragezugriff erstellen, stellen Sie sicher, dass Sie berechtigt sind, die folgende Liste von Aktionen auszuführen.

Um Ihre Berechtigungen zu überprüfen, verwenden Sie IAM, um die IAM-Richtlinien zu überprüfen, die mit Ihrer IAM-Identität verknüpft sind. Vergleichen Sie dann die Informationen in diesen Richtlinien mit der folgenden Liste von Aktionen, die Sie ausführen dürfen müssen, um einen Abonnenten mit Abfragezugriff zu erstellen.

- iam:CreateRole
- iam>DeleteRolePolicy
- iam:GetRole
- iam:PutRolePolicy
- lakeformation:GrantPermissions
- lakeformation:ListPermissions
- lakeformation:RegisterResource
- lakeformation:RevokePermissions

- `ram:GetResourceShareAssociations`
- `ram:GetResourceShares`
- `ram:UpdateResourceShare`

Important

Nachdem Sie die Berechtigungen überprüft haben:

- Wenn Sie die Security Lake-Konsole verwenden möchten, um einen Abonnenten mit Abfragezugriff hinzuzufügen, können Sie den nächsten Schritt überspringen und mit fortfahren [Gewähren Sie Lake Formation-Administratorrechte](#). Security Lake erstellt alle erforderlichen IAM-Rollen oder verwendet vorhandene Rollen in Ihrem Namen.
- Wenn Sie die Security Lake-API oder CLI verwenden möchten, um einen Abonnenten mit Abfragezugriff hinzuzufügen, fahren Sie mit dem nächsten Schritt fort, um eine IAM-Rolle für die Abfrage von Security Lake-Daten zu erstellen.

Erstellen Sie eine IAM-Rolle, um Security Lake-Daten abzufragen (API und nur Schritt AWS CLI)

Wenn Sie die Security Lake-API verwenden oder AWS CLI einem Abonnenten Abfragezugriff gewähren möchten, müssen Sie eine Rolle mit dem Namen erstellen.

AmazonSecurityLakeMetaStoreManager Security Lake verwendet diese Rolle, um AWS Glue Partitionen zu registrieren und AWS Glue Tabellen zu aktualisieren. Möglicherweise haben Sie diese Rolle bereits unter [Erforderliche IAM-Rollen erstellen](#) erstellt.

Gewähren Sie Lake Formation-Administratorrechte

Außerdem müssen Sie der IAM-Rolle, die Sie für den Zugriff auf die Security Lake-Konsole und das Hinzufügen von Abonnenten verwenden, Lake Formation-Administratorberechtigungen hinzufügen.

Gehen Sie wie folgt vor, um Lake Formation-Administratorberechtigungen für Ihre Rolle zu gewähren:

1. Öffnen Sie die Lake-Formation-Konsole unter <https://console.aws.amazon.com/lakeformation/>.
2. Melden Sie sich als Administratorbenutzer an.
3. Wenn das Fenster Willkommen bei Lake Formation angezeigt wird, wählen Sie den Benutzer aus, den Sie in Schritt 1 erstellt oder ausgewählt haben, und wählen Sie dann Erste Schritte aus.

4. Wenn das Fenster Willkommen bei Lake Formation nicht angezeigt wird, führen Sie die folgenden Schritte aus, um einen Lake Formation-Administrator zu konfigurieren.
 1. Wählen Sie im Navigationsbereich unter Berechtigungen die Option Administrative Rollen und Aufgaben aus. Wählen Sie im Abschnitt Data Lake-Administratoren die Option Administratoren auswählen aus.
 2. Wählen Sie im Dialogfeld Data Lake-Administratoren verwalten für IAM-Benutzer und -Rollen die Administratorrolle aus, die beim Zugriff auf die Security Lake-Konsole verwendet wird, und klicken Sie dann auf Speichern.

Weitere Informationen zum Ändern der Berechtigungen für Data Lake-Administratoren finden Sie unter [Erstellen eines Data Lake-Administrators](#) im AWS Lake Formation Entwicklerhandbuch.

Die IAM-Rolle muss über SELECT Berechtigungen für die Datenbank und die Tabellen verfügen, auf die Sie einem Abonnenten Zugriff gewähren möchten. Anweisungen dazu finden Sie im AWS Lake Formation Entwicklerhandbuch unter [Gewähren von Datenkatalogberechtigungen mithilfe der benannten Ressourcenmethode](#).

Einen Abonnenten mit Abfragezugriff erstellen

Wählen Sie Ihre bevorzugte Methode, um einen Abonnenten mit Abfragezugriff in der aktuellen Version zu erstellen AWS-Region. Ein Abonnent kann Daten nur von dem abfragen AWS-Region , in dem er erstellt wurde. Um einen Abonnenten zu erstellen, benötigen Sie die AWS-Konto ID und die externe ID des Abonnenten. Die externe ID ist eine eindeutige Kennung, die Ihnen der Abonnent zur Verfügung stellt. Weitere Informationen zu externen IDs finden Sie im IAM-Benutzerhandbuch unter [So verwenden Sie eine externe ID, wenn Sie einem Dritten Zugriff auf Ihre AWS Ressourcen gewähren](#).

Note

Security Lake unterstützt die kontoübergreifende Datenfreigabe von Lake Formation Version 1 nicht. Sie müssen Lake Formation Cross-account Data Sharing auf Version 2 oder Version 3 aktualisieren. Die Schritte zum Aktualisieren der kontoübergreifenden Versionseinstellungen über die AWS Lake Formation Konsole oder die AWS CLI finden Sie unter [So aktivieren Sie die neue Version](#) im AWS Lake Formation Entwicklerhandbuch.

Console

1. Öffnen Sie die Security Lake-Konsole unter <https://console.aws.amazon.com/securitylake/>.
Melden Sie sich mit dem delegierten Administratorkonto an.
2. Wählen Sie mithilfe der AWS-Region Auswahl in der oberen rechten Ecke der Seite die Region aus, in der Sie den Abonnenten erstellen möchten.
3. Wählen Sie im Navigationsbereich Abonnenten aus.
4. Wählen Sie auf der Seite Abonnenten die Option Abonnent erstellen aus.
5. Geben Sie für Abonnentendetails einen Abonnentennamen und optional eine Beschreibung ein.

Die Region wird automatisch so ausgefüllt, wie Sie sie aktuell ausgewählt haben, AWS-Region und kann nicht geändert werden.

6. Wählen Sie für Protokoll- und Ereignisquellen aus, welche Quellen Security Lake bei der Rückgabe von Abfrageergebnissen einbeziehen soll.
7. Wählen Sie als Datenzugriffsmethode Lake Formation aus, um den Abfragezugriff für den Abonnenten zu erstellen.
8. Geben Sie für Abonnentenanmeldedaten die AWS-Konto ID und die [externe ID](#) des Abonnenten an.
9. (Optional) Geben Sie für Stichwörter bis zu 50 Stichwörter ein, die dem Abonnenten zugewiesen werden sollen.

Ein Tag ist eine Bezeichnung, die Sie definieren und bestimmten Ressourcentypen AWS zuweisen können. Jedes Tag besteht aus einem erforderlichen Tag-Schlüssel und einem optionalen Tag-Wert. Mithilfe von Tags können Sie Ressourcen auf unterschiedliche Weise identifizieren, kategorisieren und verwalten. Weitere Informationen hierzu finden Sie unter [Markieren von Amazon Security Lake-Ressourcen](#).

10. Wählen Sie Erstellen.

API

Verwenden Sie die Security Lake-API, um programmgesteuert einen Abonnenten mit Abfragezugriff zu erstellen. [CreateSubscriber](#) Wenn Sie AWS Command Line Interface (AWS CLI) verwenden, führen Sie den Befehl [create-subscriber](#) aus.

Verwenden Sie in Ihrer Anfrage diese Parameter, um die folgenden Einstellungen für den Abonnenten anzugeben:

- Legen Sie für `accessTypes` die Option `LAKEFORMATION` fest.
- Geben Sie für `sources` jede Quelle an, die Security Lake bei der Rückgabe von Abfrageergebnissen einbeziehen soll.
- Geben Sie für `subscriberIdentity` die AWS Identität und die externe ID an, die der Abonnent zur Abfrage von Quelldaten verwendet.

Im folgenden Beispiel wird ein Abonnent mit Abfragezugriff in der aktuellen AWS Region für die angegebene Abonnenten-Identität erstellt. Dieses Beispiel ist für Linux, macOS oder Unix formatiert und verwendet den umgekehrten Schrägstrich (`\`) zur Verbesserung der Lesbarkeit.

```
$ aws securitylake create-subscriber \  
--subscriber-identity {"accountID": 129345678912,"externalId": 123456789012} \  
--sources [{"awsLogSource": {"sourceName": VPC_FLOW, sourceVersion": 2.0}}] \  
--subscriber-name subscriber name \  
--access-types LAKEFORMATION
```

Einrichtung der kontenübergreifenden gemeinsamen Nutzung von Tabellen (Abonnentenschritt)

Security Lake verwendet die kontenübergreifende Tabellenfreigabe von Lake Formation, um den Zugriff auf Abonnentenabfragen zu unterstützen. Wenn Sie einen Abonnenten mit Abfragezugriff in der Security Lake-Konsole, API oder AWS CLI erstellen, gibt Security Lake Informationen über die entsprechenden Lake Formation-Tabellen an den Abonnenten weiter, indem es eine [Ressourcenfreigabe](#) in AWS Resource Access Manager (AWS RAM) erstellt.

Wenn Sie bestimmte Arten von Änderungen an einem Abonnenten mit Abfragezugriff vornehmen, erstellt Security Lake eine neue Ressourcenfreigabe. Weitere Informationen finden Sie unter [Einen Abonnenten mit Abfragezugriff bearbeiten](#).

Der Abonnent sollte die folgenden Schritte ausführen, um Daten aus Ihren Lake Formation-Tabellen zu nutzen:

1. Die Ressourcenfreigabe akzeptieren — Der Abonnent muss die Ressourcenfreigabe akzeptieren, die den `resourceShareArn` und enthält und der generiert wird `resourceShareName`, wenn Sie den Abonnenten erstellen oder bearbeiten. Wählen Sie eine der folgenden Zugriffsmethoden:
 - Informationen zu Konsole und AWS CLI finden Sie unter [Eine Einladung zur gemeinsamen Nutzung einer Ressource annehmen von AWS RAM](#).
 - Rufen Sie für API die [GetResourceShareInvitations](#)API auf. Filtern Sie nach `resourceShareArn` und `resourceShareName`, um die richtige Ressourcenfreigabe zu finden. Nehmen Sie die Einladung mit der [AcceptResourceShareInvitation](#)API an.

Die Einladung zur gemeinsamen Nutzung von Ressourcen läuft in 12 Stunden ab. Sie müssen die Einladung also innerhalb von 12 Stunden validieren und annehmen. Wenn die Einladung abläuft, wird sie weiterhin in einem bestimmten PENDING Status angezeigt, aber wenn Sie sie annehmen, erhalten Sie keinen Zugriff auf die gemeinsam genutzten Ressourcen. Wenn mehr als 12 Stunden vergangen sind, löschen Sie den Lake Formation Formation-Abonnenten und erstellen Sie den Abonnenten neu, um eine neue Resource Share-Einladung zu erhalten.

2. Einen Ressourcenlink zu gemeinsam genutzten Tabellen erstellen — Der Abonnent muss entweder AWS Lake Formation (bei Verwendung der Konsole) oder AWS Glue (bei Verwendung von API/AWS CLI) einen Ressourcenlink zu den gemeinsam genutzten Lake Formation-Tabellen erstellen. Dieser Ressourcenlink verweist das Konto des Abonnenten auf die gemeinsam genutzten Tabellen. Wählen Sie eine der folgenden Zugriffsmethoden:
 - Informationen zur Konsole und AWS CLI finden Sie unter [Erstellen eines Ressourcenlinks zu einer gemeinsam genutzten Datenkatalogtabelle](#) im AWS Lake Formation Entwicklerhandbuch.
 - Rufen Sie für API die AWS Glue [CreateTable](#)API auf. Wir empfehlen Abonnenten, mit der [CreateDatabase](#)API auch eine eigene Datenbank zum Speichern von Ressourcenlink-Tabellen zu erstellen.
3. Fragen Sie die gemeinsam genutzten Tabellen ab — Dienste wie Amazon Athena können direkt auf die Tabellen verweisen, und neue Daten, die Security Lake sammelt, stehen automatisch für Abfragen zur Verfügung. Abfragen werden beim Abonnenten ausgeführt AWS-Konto, und die durch Abfragen entstehenden Kosten werden dem Abonnenten in Rechnung gestellt. Sie können den Lesezugriff auf Ressourcen in Ihrem eigenen Security Lake-Konto kontrollieren.

Weitere Informationen zur Gewährung kontenübergreifender Berechtigungen finden Sie unter [Kontenübergreifender Datenaustausch in Lake Formation](#) im AWS Lake Formation Entwicklerhandbuch.

Einen Abonnenten mit Abfragezugriff bearbeiten

Security Lake unterstützt Änderungen an einem Abonnenten mit Abfragezugriff. Sie können den Namen, die Beschreibung, die externe ID, den Prinzipal (AWS-Konto ID) und die Protokollquellen, die der Abonnent nutzen kann, bearbeiten. Wählen Sie Ihre bevorzugte Methode und folgen Sie den Schritten zum Bearbeiten eines Abonnenten mit Abfragezugriff in der aktuellen Version AWS-Region.

Note

Security Lake unterstützt die kontoübergreifende Datenfreigabe von Lake Formation Version 1 nicht. Sie müssen Lake Formation Cross-account Data Sharing auf Version 2 oder Version 3 aktualisieren. Die Schritte zum Aktualisieren der kontoübergreifenden Versionseinstellungen über die AWS Lake Formation Konsole oder die AWS CLI finden Sie unter [So aktivieren Sie die neue Version](#) im AWS Lake Formation Entwicklerhandbuch.

Console

Basierend auf den Details, die Sie bearbeiten möchten, folgen Sie nur den Schritten, die für diese Aktion vorgesehen sind.

Um den Namen des Abonnenten zu bearbeiten

1. Öffnen Sie die Security Lake-Konsole unter <https://console.aws.amazon.com/securitylake/>.

Melden Sie sich mit dem delegierten Administratorkonto an.

2. Wählen Sie mithilfe der AWS-Region Auswahl in der oberen rechten Ecke der Seite die Region aus, in der Sie die Abonnentendetails bearbeiten möchten.
3. Wählen Sie im Navigationsbereich Abonnenten aus.
4. Verwenden Sie auf der Abonnentenseite das Optionsfeld, um den Abonnenten auszuwählen, den Sie bearbeiten möchten. Die Datenzugriffsmethode für den ausgewählten Abonnenten muss LAKEFORMATION sein.
5. Wählen Sie Bearbeiten aus.
6. Geben Sie den neuen Abonnentennamen ein und wählen Sie Speichern.

Um die Beschreibung des Abonnenten zu bearbeiten

1. Öffnen Sie die Security Lake-Konsole unter <https://console.aws.amazon.com/securitylake/>.

Melden Sie sich mit dem delegierten Administratorkonto an.

2. Wählen Sie mithilfe der AWS-Region Auswahl in der oberen rechten Ecke der Seite die Region aus, in der Sie den Abonnenten bearbeiten möchten.
3. Wählen Sie im Navigationsbereich Abonnenten aus.
4. Verwenden Sie auf der Abonnentenseite das Optionsfeld, um den Abonnenten auszuwählen, den Sie bearbeiten möchten. Die Datenzugriffsmethode für den ausgewählten Abonnenten muss LAKEFORMATION sein.
5. Wählen Sie Bearbeiten aus.
6. Geben Sie die neue Beschreibung für den Abonnenten ein und wählen Sie Speichern.

Um die externe ID zu bearbeiten

1. Öffnen Sie die Security Lake-Konsole unter <https://console.aws.amazon.com/securitylake/>.

Melden Sie sich mit dem delegierten Administratorkonto an.

2. Wählen Sie mithilfe der AWS-Region Auswahl in der oberen rechten Ecke der Seite die Region aus, in der Sie die Abonnentendetails bearbeiten möchten.
3. Wählen Sie im Navigationsbereich Abonnenten aus.
4. Verwenden Sie auf der Abonnentenseite das Optionsfeld, um den Abonnenten auszuwählen, den Sie bearbeiten möchten. Die Datenzugriffsmethode für den ausgewählten Abonnenten muss LAKEFORMATION sein.
5. Wählen Sie Bearbeiten aus.
6. Geben Sie die neue externe ID ein, die der Abonnent angegeben hat, und wählen Sie Speichern.

Durch das Speichern der neuen externen ID wird automatisch die vorherige AWS RAM Ressourcenfreigabe entfernt und eine neue Ressourcenfreigabe für den Abonnenten erstellt.

7. Der Abonnent muss die neue Ressourcenfreigabe akzeptieren, indem er Schritt 1 unter [ausführt Einrichtung der kontenübergreifenden gemeinsamen Nutzung von Tabellen](#)

[\(Abonnentenschritt\)](#). Stellen Sie sicher, dass der Amazon-Ressourcenname (ARN), der in den Abonentendetails angezeigt wird, mit dem in der Lake Formation Formation-Konsole übereinstimmt. Der Ressourcenlink zu den gemeinsam genutzten Tabellen bleibt unverändert, sodass der Abonnent keinen neuen Ressourcenlink erstellen muss.

Um den Prinzipal (AWS-Konto ID) zu bearbeiten

1. Öffnen Sie die Security Lake-Konsole unter <https://console.aws.amazon.com/securitylake/>.

Melden Sie sich mit dem delegierten Administratorkonto an.

2. Wählen Sie mithilfe der AWS-Region Auswahl in der oberen rechten Ecke der Seite die Region aus, in der Sie die Abonentendetails bearbeiten möchten.
3. Wählen Sie im Navigationsbereich Abonnenten aus.
4. Verwenden Sie auf der Abonentenseite das Optionsfeld, um den Abonnenten auszuwählen, den Sie bearbeiten möchten. Die Datenzugriffsmethode für den ausgewählten Abonnenten muss LAKEFORMATION sein.
5. Wählen Sie Bearbeiten aus.
6. Geben Sie die neue AWS-Konto ID des Abonnenten ein und wählen Sie Speichern.

Durch das Speichern der neuen Konto-ID wird automatisch die vorherige AWS RAM Ressourcenfreigabe entfernt, sodass der vorherige Prinzipal die Protokoll- und Ereignisquellen nicht nutzen kann. Security Lake erstellt eine neue Ressourcenfreigabe.

7. Unter Verwendung der Anmeldeinformationen des neuen Prinzipals muss der Abonnent die neue Ressourcenfreigabe akzeptieren und einen Ressourcenlink zu den gemeinsam genutzten Tabellen erstellen. Dadurch erhält der neue Principal Zugriff auf die gemeinsam genutzten Ressourcen. Anweisungen finden Sie in den Schritten 1 und 2 unter [Einrichtung der kontenübergreifenden gemeinsamen Nutzung von Tabellen \(Abonnentenschritt\)](#). Stellen Sie sicher, dass der ARN, der in den Abonentendetails angezeigt wird, mit dem in der Lake Formation Formation-Konsole übereinstimmt.

Um Protokoll- und Ereignisquellen zu bearbeiten

1. Öffnen Sie die Security Lake-Konsole unter <https://console.aws.amazon.com/securitylake/>.

Melden Sie sich mit dem delegierten Administratorkonto an.

2. Wählen Sie mithilfe der AWS-Region Auswahl in der oberen rechten Ecke der Seite die Region aus, in der Sie die Abonentendetails bearbeiten möchten.
3. Wählen Sie im Navigationsbereich Abonnenten aus.
4. Verwenden Sie auf der Abonentenseite das Optionsfeld, um den Abonnenten auszuwählen, den Sie bearbeiten möchten. Die Datenzugriffsmethode für den ausgewählten Abonnenten muss LAKEFORMATION sein.
5. Wählen Sie Bearbeiten aus.
6. Wählen Sie vorhandene Quellen ab oder wählen Sie Quellen aus, die Sie hinzufügen möchten. Wenn Sie die Auswahl einer Quelle aufheben, sind von Ihrer Seite keine weiteren Maßnahmen erforderlich. Wenn Sie sich dafür entscheiden, eine Quelle hinzuzufügen, wird keine neue Einladung zur gemeinsamen Nutzung einer Ressource erstellt. Security Lake aktualisiert jedoch die gemeinsam genutzten Lake Formation-Tabellen auf der Grundlage der hinzugefügten Quellen. Der Abonnent muss einen Ressourcenlink zu den aktualisierten gemeinsamen Tabellen erstellen, damit er die Quelldaten abfragen kann. Anweisungen finden Sie in Schritt 2 unter [Einrichtung der kontenübergreifenden gemeinsamen Nutzung von Tabellen \(Abonentenschritt\)](#).
7. Wählen Sie Speichern.

API

Um einen Abonnenten mit Abfragezugriff programmgesteuert zu bearbeiten, verwenden Sie den [UpdateSubscriber](#)Betrieb der Security Lake-API. Wenn Sie AWS Command Line Interface (AWS CLI) verwenden, führen Sie den Befehl [update-subscriber](#) aus. Verwenden Sie in Ihrer Anfrage die unterstützten Parameter, um die folgenden Einstellungen für den Abonnenten anzugeben:

- Geben Sie für `subscriberName` den neuen Abonentennamen an.
- Geben Sie für `subscriberDescription` die neue Beschreibung an.
- Geben Sie für `subscriberIdentity` den Prinzipal (AWS-Konto ID) und die externe ID an, die der Abonnent zur Abfrage von Quelldaten verwenden wird. Sie müssen sowohl den Prinzipal als auch die externe ID angeben. Wenn Sie möchten, dass einer dieser Werte unverändert bleibt, geben Sie den aktuellen Wert ein.
- Nur externe ID aktualisieren — Diese Aktion entfernt die vorherige AWS RAM Ressourcenfreigabe und erstellt eine neue Ressourcenfreigabe für den Abonnenten.

Der Abonnent muss die neue Ressourcenfreigabe akzeptieren, indem er Schritt 1 unter [ausführt Einrichtung der kontenübergreifenden gemeinsamen Nutzung von Tabellen \(Abonnentenschritt\)](#). Der Ressourcenlink zu den gemeinsam genutzten Tabellen bleibt unverändert, sodass der Abonnent keinen neuen Ressourcenlink erstellen muss.

- Nur Hauptbenutzer aktualisieren — Durch diese Aktion wird die vorherige AWS RAM Ressourcenfreigabe entfernt, sodass der vorherige Prinzipal die Protokoll- und Ereignisquellen nicht nutzen kann. Security Lake erstellt eine neue Ressourcenfreigabe. Unter Verwendung der Anmeldeinformationen des neuen Prinzipals muss der Abonnent die neue Ressourcenfreigabe akzeptieren und einen Ressourcenlink zu den gemeinsam genutzten Tabellen erstellen. Dadurch erhält der neue Principal Zugriff auf die gemeinsam genutzten Ressourcen. Anweisungen finden Sie in den Schritten 1 und 2 unter [Einrichtung der kontenübergreifenden gemeinsamen Nutzung von Tabellen \(Abonnentenschritt\)](#).

Um die externe ID und den Prinzipal zu aktualisieren, folgen Sie den Schritten 1 und 2 unter [Einrichtung der kontenübergreifenden gemeinsamen Nutzung von Tabellen \(Abonnentenschritt\)](#).

- Entfernen Sie zum sources Beispiel vorhandene Quellen oder geben Sie Quellen an, die Sie hinzufügen möchten. Wenn Sie eine Quelle entfernen, sind keine weiteren Maßnahmen Ihrerseits erforderlich. Wenn Sie eine Quelle hinzufügen, wird keine neue Einladung zur gemeinsamen Nutzung von Ressourcen erstellt. Security Lake aktualisiert jedoch die gemeinsam genutzten Lake Formation-Tabellen auf der Grundlage der hinzugefügten Quellen. Der Abonnent muss einen Ressourcenlink zu den aktualisierten gemeinsamen Tabellen erstellen, damit er die Quelldaten abfragen kann. Anweisungen finden Sie in Schritt 2 unter [Einrichtung der kontenübergreifenden gemeinsamen Nutzung von Tabellen \(Abonnentenschritt\)](#).

Security-Lake-Abfragen

Sie können die Daten abfragen, die Security Lake in AWS Lake Formation Datenbanken und Tabellen speichert. Sie können auch Abonnenten von Drittanbietern in der Security-Lake-Konsole, API oder erstellen AWS CLI. Abonnenten von Drittanbietern können auch Lake-Formation-Daten aus den von Ihnen angegebenen Quellen abfragen.

Der Lake-Formation-Data-Lake-Administrator muss der IAM-Identität, die die Daten abfragt, SELECT Berechtigungen für die relevanten Datenbanken und Tabellen erteilen. Ein Subscriber muss auch in Security Lake erstellt werden, bevor er Daten abfragen kann. Weitere Informationen zum Erstellen eines Abonnenten mit Abfragezugriff finden Sie unter [Verwaltung des Abfragezugriffs für Security Lake-Abonnenten](#).

Themen

- [Security Lake-Abfragen für AWS Quellversion 1 \(OCSF 1.0.0-rc.2\)](#)
- [Security Lake-Abfragen für AWS Quellversion 2 \(OCSF 1.1.0\)](#)

Security Lake-Abfragen für AWS Quellversion 1 (OCSF 1.0.0-rc.2)

Der folgende Abschnitt enthält Anleitungen zum Abfragen von Daten aus Security Lake und enthält einige Abfragebeispiele für nativ AWS unterstützte Quellen. Diese Abfragen dienen zum Abrufen von Daten in einem bestimmten Bereich. AWS-Region In diesen Beispielen wird us-east-1 (US East (Nord-Virginia)) verwendet. Darüber hinaus verwenden die Beispielabfragen einen LIMIT 25 Parameter, der bis zu 25 Datensätze zurückgibt. Sie können diesen Parameter weglassen oder ihn nach Ihren Wünschen anpassen. Weitere Beispiele finden Sie im [GitHub Verzeichnis Amazon Security Lake OCSF Queries](#).

Quelltabelle für das Protokoll

Wenn Sie Security Lake-Daten abfragen, müssen Sie den Namen der Lake Formation-Tabelle angeben, in der sich die Daten befinden.

```
SELECT *  
FROM  
amazon_security_lake_glue_db_DB_Region.amazon_security_lake_table_DB_Region_SECURITY_LAKE_TABL
```

```
WHERE eventDay BETWEEN cast(date_format(current_timestamp - INTERVAL '7' day, '%Y%m%d%H') as varchar) and cast(date_format(current_timestamp - INTERVAL '0' day, '%Y%m%d%H') as varchar)
LIMIT 25
```

Zu den allgemeinen Werten für die Protokollquelltable gehören die folgenden:

- `cloud_trail_mgmt_1_0`— AWS CloudTrail Verwaltungsereignisse
- `lambda_execution_1_0`— CloudTrail Datenereignisse für Lambda
- `s3_data_1_0`— CloudTrail Datenereignisse für S3
- `route53_1_0`— Amazon Route 53-Resolver-Abfrageprotokolle
- `sh_findings_1_0`— Ergebnisse AWS Security Hub
- `vpc_flow_1_0`— Flussprotokolle von Amazon Virtual Private Cloud (Amazon VPC)

Beispiel: Alle Security Hub Hub-Ergebnisse in der Tabelle `sh_findings_1_0` aus der Region `us-east-1`

```
SELECT *
FROM
amazon_security_lake_glue_db_us_east_1.amazon_security_lake_table_us_east_1_sh_findings_1_0
WHERE eventDay BETWEEN cast(date_format(current_timestamp - INTERVAL '7' day, '%Y%m%d%H') as varchar) and cast(date_format(current_timestamp - INTERVAL '0' day, '%Y%m%d%H') as varchar)
LIMIT 25
```

Datenbank-Region

Wenn Sie Security Lake-Daten abfragen, müssen Sie den Namen der Datenbankregion angeben, aus der Sie die Daten abfragen. Eine vollständige Liste der Datenbankregionen, in denen Security Lake derzeit verfügbar ist, finden Sie unter [Amazon Security Lake-Endpoints](#).

Beispiel: AWS CloudTrail Aktivitäten von der Quell-IP auflisten

Das folgende Beispiel listet alle CloudTrail Aktivitäten von der Quell-IP 192.0.2.1 auf, die nach 20230301 (01. März 2023) aufgezeichnet wurden, in der Tabelle `cloud_trail_mgmt_1_0` von `us-east-1`. DB_Region

```
SELECT *
  FROM
amazon_security_lake_glue_db_us_east_1.amazon_security_lake_table_us_east_1_cloud_trail_mgmt_1
  WHERE eventDay > '20230301' AND src_endpoint.ip = '192.0.2.1'
  ORDER BY time desc
  LIMIT 25
```

Datum der Partition

Durch die Partitionierung Ihrer Daten können Sie die Menge der bei jeder Abfrage gescannten Daten einschränken und so die Leistung verbessern und die Kosten senken. Security Lake implementiert die Partitionierung durch eventDay Parameterregion, undaccountid. eventDayPartitionen verwenden das FormatYYYYMMDD.

Dies ist eine Beispielabfrage, die die eventDay Partition verwendet:

```
SELECT *
  FROM
amazon_security_lake_glue_db_us_east_1.amazon_security_lake_table_us_east_1_cloud_trail_mgmt_1
  WHERE eventDay > '20230301'
  AND src_endpoint.ip = '192.0.2.1'
  ORDER BY time desc
```

Zu den allgemeinen Werten für eventDay gehören die folgenden:

Ereignisse, die im letzten Jahr eingetreten sind

```
> cast(date_format(current_timestamp - INTERVAL '1' year, '%Y%m%d%H') as
varchar)
```

Ereignisse, die im letzten Monat eingetreten sind

```
> cast(date_format(current_timestamp - INTERVAL '1' month, '%Y%m%d%H')
as varchar)
```

Ereignisse der letzten 30 Tage

```
> cast(date_format(current_timestamp - INTERVAL '30' day, '%Y%m%d%H') as
varchar)
```

Ereignisse der letzten 12 Stunden

```
> cast(date_format(current_timestamp - INTERVAL '12' hour, '%Y%m%d%H')
as varchar)
```

Ereignisse, die in den letzten 5 Minuten eingetreten sind

```
> cast(date_format(current_timestamp - INTERVAL '5' minute, '%Y%m%d%H')
as varchar)
```

Ereignisse, die vor 7 bis 14 Tagen eingetreten sind

```
BETWEEN cast(date_format(current_timestamp - INTERVAL '14' day, '%Y%m%d
%H') as varchar) and cast(date_format(current_timestamp - INTERVAL '7'
day, '%Y%m%d%H') as varchar)
```

Ereignisse, die an oder nach einem bestimmten Datum auftreten

```
>= '20230301'
```

Beispiel: Liste aller CloudTrail Aktivitäten von der Quell-IP **192.0.2.1** am oder nach dem 1. März 2023 in der Tabelle **cloud_trail_mgmt_1_0**

```
SELECT *
FROM
amazon_security_lake_glue_db_us_east_1.amazon_security_lake_table_us_east_1_cloud_trail_mgmt_1_0
WHERE eventDay >= '20230301'
AND src_endpoint.ip = '192.0.2.1'
ORDER BY time desc
LIMIT 25
```

Beispiel: Liste aller CloudTrail Aktivitäten von der Quell-IP **192.0.2.1** in den letzten 30 Tagen in der Tabelle **cloud_trail_mgmt_1_0**

```
SELECT *
FROM
amazon_security_lake_glue_db_us_east_1.amazon_security_lake_table_us_east_1_cloud_trail_mgmt_1_0
WHERE eventDay > cast(date_format(current_timestamp - INTERVAL '30' day, '%Y%m%d
%H') as varchar)
AND src_endpoint.ip = '192.0.2.1'
```

```
ORDER BY time desc
LIMIT 25
```

Beispielabfragen für CloudTrail Daten

AWS CloudTrail verfolgt Benutzeraktivitäten und API-Nutzung in AWS-Services. Abonnenten können CloudTrail Daten abfragen, um die folgenden Arten von Informationen zu erhalten:

Hier sind einige Beispiele für CloudTrail Datenabfragen:

Unautorisierte Versuche gegen AWS-Services in den letzten 7 Tagen

```
SELECT
    time,
    api.service.name,
    api.operation,
    api.response.error,
    api.response.message,
    unmapped['responseElements'],
    cloud.region,
    actor.user.uuid,
    src_endpoint.ip,
    http_request.user_agent
FROM
    amazon_security_lake_glue_db_us_east_1.amazon_security_lake_table_us_east_1_cloud_trail_mgmt_1
WHERE eventDay BETWEEN cast(date_format(current_timestamp - INTERVAL '7' day, '%Y%m%d%H') as varchar) and cast(date_format(current_timestamp - INTERVAL '0' day, '%Y%m%d%H') as varchar)
AND api.response.error in (
    'Client.UnauthorizedOperation',
    'Client.InvalidPermission.NotFound',
    'Client.OperationNotPermitted',
    'AccessDenied')
ORDER BY time desc
LIMIT 25
```

Liste aller CloudTrail Aktivitäten von der Quell-IP **192.0.2.1** in den letzten 7 Tagen

```
SELECT
    api.request.uid,
    time,
```

```

    api.service.name,
    api.operation,
    cloud.region,
    actor.user.uuid,
    src_endpoint.ip,
    http_request.user_agent
FROM
amazon_security_lake_glue_db_us_east_1.amazon_security_lake_table_us_east_1_cloud_trail_mgmt_1
WHERE eventDay BETWEEN cast(date_format(current_timestamp - INTERVAL '7' day, '%Y%m%d%H') as varchar) and cast(date_format(current_timestamp - INTERVAL '0' day, '%Y%m%d%H') as varchar)
AND src_endpoint.ip = '127.0.0.1.'
ORDER BY time desc
LIMIT 25

```

Liste aller IAM-Aktivitäten in den letzten 7 Tagen

```

SELECT *
FROM
amazon_security_lake_glue_db_us_east_1.amazon_security_lake_table_us_east_1_cloud_trail_mgmt_1
WHERE eventDay BETWEEN cast(date_format(current_timestamp - INTERVAL '7' day, '%Y%m%d%H') as varchar) and cast(date_format(current_timestamp - INTERVAL '0' day, '%Y%m%d%H') as varchar)
AND api.service.name = 'iam.amazonaws.com'
ORDER BY time desc
LIMIT 25

```

Instanzen, in denen die Anmeldeinformationen in den letzten 7 Tagen verwendet **AIDACKCEVSQ6C2EXAMPLE** wurden

```

SELECT
    actor.user.uid,
    actor.user.uuid,
    actor.user.account_uid,
    cloud.region
FROM
amazon_security_lake_glue_db_us_east_1.amazon_security_lake_table_us_east_1_cloud_trail_mgmt_1
WHERE eventDay BETWEEN cast(date_format(current_timestamp - INTERVAL '7' day, '%Y%m%d%H') as varchar) and cast(date_format(current_timestamp - INTERVAL '0' day, '%Y%m%d%H') as varchar)
AND actor.user.credential_uid = 'AIDACKCEVSQ6C2EXAMPLE'
LIMIT 25

```

Liste der fehlgeschlagenen CloudTrail Datensätze der letzten 7 Tage

```

SELECT
    actor.user.uid,
    actor.user.uuid,
    actor.user.account_uid,
    cloud.region
FROM
amazon_security_lake_glue_db_us_east_1.amazon_security_lake_table_us_east_1_cloud_trail_mgmt_1
    WHERE status='failed' and eventDay BETWEEN cast(date_format(current_timestamp -
INTERVAL '7' day, '%Y%m%d%H') as varchar) and cast(date_format(current_timestamp -
INTERVAL '0' day, '%Y%m%d%H') as varchar)
    ORDER BY time DESC
    LIMIT 25

```

Beispielabfragen für Route 53-Resolver-Abfrageprotokolle

Die Amazon Route 53-Resolver-Abfrageprotokolle verfolgen DNS-Abfragen, die von Ressourcen in Ihrer Amazon VPC gestellt wurden. Abonnenten können die Route 53-Resolver-Abfrageprotokolle abfragen, um die folgenden Arten von Informationen zu erhalten:

Im Folgenden finden Sie einige Beispielabfragen von Route 53-Resolver-Abfrageprotokollen:

Liste der DNS-Abfragen CloudTrail der letzten 7 Tage

```

SELECT
    time,
    src_endpoint.instance_uid,
    src_endpoint.ip,
    src_endpoint.port,
    query.hostname,
    rcode
FROM
amazon_security_lake_glue_db_us_east_1.amazon_security_lake_table_us_east_1_route53_1_0
    WHERE eventDay BETWEEN cast(date_format(current_timestamp - INTERVAL '7' day, '%Y%m
%d%H') as varchar) and cast(date_format(current_timestamp - INTERVAL '0' day, '%Y%m%d
%H') as varchar)
    ORDER BY time DESC
    LIMIT 25

```

Liste der DNS-Abfragen, die **s3.amazonaws.com** in den letzten 7 Tagen übereinstimmen

```
SELECT
    time,
    src_endpoint.instance_uid,
    src_endpoint.ip,
    src_endpoint.port,
    query.hostname,
    rcode,
    answers
FROM
amazon_security_lake_glue_db_us_east_1.amazon_security_lake_table_us_east_1_route53_1_0
WHERE query.hostname LIKE 's3.amazonaws.com.' and eventDay BETWEEN
cast(date_format(current_timestamp - INTERVAL '7' day, '%Y%m%d%H') as varchar) and
cast(date_format(current_timestamp - INTERVAL '0' day, '%Y%m%d%H') as varchar)
ORDER BY time DESC
LIMIT 25
```

Liste der DNS-Abfragen, die in den letzten 7 Tagen nicht gelöst wurden

```
SELECT
    time,
    src_endpoint.instance_uid,
    src_endpoint.ip,
    src_endpoint.port,
    query.hostname,
    rcode,
    answers
FROM
amazon_security_lake_glue_db_us_east_1.amazon_security_lake_table_us_east_1_route53_1_0
WHERE cardinality(answers) = 0 and eventDay BETWEEN
cast(date_format(current_timestamp - INTERVAL '7' day, '%Y%m%d%H') as varchar) and
cast(date_format(current_timestamp - INTERVAL '0' day, '%Y%m%d%H') as varchar)
LIMIT 25
```

Liste der DNS-Abfragen, die **192.0.2.1** in den letzten 7 Tagen behoben wurden

```
SELECT
    time,
    src_endpoint.instance_uid,
    src_endpoint.ip,
    src_endpoint.port,
    query.hostname,
    rcode,
```

```

    answer.rdata
FROM
amazon_security_lake_glue_db_us_east_1.amazon_security_lake_table_us_east_1_route53_1_0
CROSS JOIN UNNEST(answers) as st(answer)
WHERE answer.rdata='192.0.2.1' and eventDay BETWEEN
cast(date_format(current_timestamp - INTERVAL '7' day, '%Y%m%d%H') as varchar) and
cast(date_format(current_timestamp - INTERVAL '0' day, '%Y%m%d%H') as varchar)
LIMIT 25

```

Beispielabfragen für Security Hub Hub-Ergebnisse

Security Hub bietet Ihnen einen umfassenden Überblick über Ihren Sicherheitsstatus AWS und hilft Ihnen dabei, Ihre Umgebung anhand von Industriestandards und Best Practices zu überprüfen. Security Hub erstellt Ergebnisse für Sicherheitsüberprüfungen und erhält Ergebnisse von Diensten Dritter.

Hier sind einige Beispielabfragen zu Ergebnissen von Security Hub:

Neue Ergebnisse mit einem Schweregrad größer oder gleich **MEDIUM** in den letzten 7 Tagen

```

SELECT
    time,
    finding,
    severity
FROM
amazon_security_lake_glue_db_us_east_1.amazon_security_lake_table_us_east_1_sh_findings_1_0_fi
WHERE eventDay BETWEEN cast(date_format(current_timestamp - INTERVAL '7' day, '%Y%m
%d%H') as varchar) and cast(date_format(current_timestamp - INTERVAL '0' day, '%Y%m%d
%H') as varchar)
AND severity_id >= 3
AND state_id = 1
ORDER BY time DESC
LIMIT 25

```

Doppelte Befunde in den letzten 7 Tagen

```

SELECT
    finding.uid,
    MAX(time) AS time,
    ARBITRARY(region) AS region,
    ARBITRARY(accountid) AS accountid,

```

```

    ARBITRARY(finding) AS finding,
    ARBITRARY(vulnerabilities) AS vulnerabilities
FROM
    amazon_security_lake_glue_db_us_east_1.amazon_security_lake_table_us_east_1_sh_findings_1_0
WHERE eventDay BETWEEN cast(date_format(current_timestamp - INTERVAL '7' day, '%Y%m%d
%H') as varchar) and cast(date_format(current_timestamp - INTERVAL '0' day, '%Y%m%d%H')
    as varchar)
GROUP BY finding.uid
LIMIT 25

```

Alle nicht informativen Ergebnisse der letzten 7 Tage

```

SELECT
    time,
    finding.title,
    finding,
    severity
FROM
    amazon_security_lake_glue_db_us_east_1.amazon_security_lake_table_us_east_1_sh_findings_1_0
WHERE severity != 'Informational' and eventDay BETWEEN
    cast(date_format(current_timestamp - INTERVAL '7' day, '%Y%m%d%H') as varchar) and
    cast(date_format(current_timestamp - INTERVAL '0' day, '%Y%m%d%H') as varchar)
LIMIT 25

```

Ergebnisse, bei denen es sich bei der Ressource um einen Amazon S3 S3-Bucket handelt (keine Zeitbeschränkung)

```

SELECT *
FROM
    amazon_security_lake_glue_db_us_east_1.amazon_security_lake_table_us_east_1_sh_findings_1_0
WHERE any_match(resources, element -> element.type = 'AwsS3Bucket')
LIMIT 25

```

Ergebnisse mit einem CVSS-Wert (Common Vulnerability Scoring System) von mehr als 1 (ohne Zeitbeschränkung)

```

SELECT *
FROM
    amazon_security_lake_glue_db_us_east_1.amazon_security_lake_table_us_east_1_sh_findings_1_0
WHERE any_match(vulnerabilities, element -> element.cve.cvss.base_score > 1.0)
LIMIT 25

```

Ergebnisse, die mit Common Vulnerabilities and Exposures (CVE) übereinstimmen **CVE-0000-0000** (keine zeitliche Beschränkung)

```
SELECT *
  FROM
amazon_security_lake_glue_db_us_east_1.amazon_security_lake_table_us_east_1_sh_findings_1_0
 WHERE any_match(vulnerabilities, element -> element.cve.uid = 'CVE-0000-0000')
 LIMIT 25
```

Anzahl der Produkte, die in den letzten 7 Tagen Ergebnisse von Security Hub gesendet haben

```
SELECT
  metadata.product.feature.name,
  count(*)
  FROM
amazon_security_lake_glue_db_us_east_1.amazon_security_lake_table_us_east_1_sh_findings_1_0
 WHERE eventDay BETWEEN cast(date_format(current_timestamp - INTERVAL '7' day, '%Y%m
%d%H') as varchar) and cast(date_format(current_timestamp - INTERVAL '0' day, '%Y%m%d
%H') as varchar)
 GROUP BY metadata.product.feature.name
 ORDER BY metadata.product.feature.name DESC
 LIMIT 25
```

Anzahl der Ressourcentypen in den Ergebnissen der letzten 7 Tage

```
SELECT
  count(*),
  resource.type
  FROM
amazon_security_lake_glue_db_us_east_1.amazon_security_lake_table_us_east_1_sh_findings_1_0
   CROSS JOIN UNNEST(resources) as st(resource)
 WHERE eventDay BETWEEN cast(date_format(current_timestamp - INTERVAL '7' day, '%Y%m
%d%H') as varchar) and cast(date_format(current_timestamp - INTERVAL '0' day, '%Y%m%d
%H') as varchar)
 GROUP BY resource.type
 LIMIT 25
```

Anfällige Pakete aufgrund von Ergebnissen der letzten 7 Tage

```
SELECT
  vulnerability
```

```

FROM
amazon_security_lake_glue_db_us_east_1.amazon_security_lake_table_us_east_1_sh_findings_1_0,
UNNEST(vulnerabilities) as t(vulnerability)
WHERE vulnerabilities is not null
LIMIT 25

```

Ergebnisse, die sich in den letzten 7 Tagen geändert haben

```

SELECT
  finding.uid,
  finding.created_time,
  finding.first_seen_time,
  finding.last_seen_time,
  finding.modified_time,
  finding.title,
  state
FROM
amazon_security_lake_glue_db_us_east_1.amazon_security_lake_table_us_east_1_sh_findings_1_0
WHERE eventDay BETWEEN cast(date_format(current_timestamp - INTERVAL '7' day, '%Y%m%d%H') as varchar) and cast(date_format(current_timestamp - INTERVAL '0' day, '%Y%m%d%H') as varchar)
LIMIT 25

```

Beispielabfragen für Amazon VPC Flow Logs

Amazon Virtual Private Cloud (Amazon VPC) bietet Details zum IP-Verkehr zu und von Netzwerkschnittstellen in Ihrer VPC.

Hier sind einige Beispielabfragen von Amazon VPC Flow Logs:

Insbesondere der Verkehr AWS-Regionen der letzten 7 Tage

```

SELECT *
FROM
amazon_security_lake_glue_db_us_east_1.amazon_security_lake_table_us_east_1_vpc_flow_1_0
WHERE eventDay BETWEEN cast(date_format(current_timestamp - INTERVAL '7' day, '%Y%m%d%H') as varchar) and cast(date_format(current_timestamp - INTERVAL '0' day, '%Y%m%d%H') as varchar)
AND region in ('us-east-1','us-east-2','us-west-2')
LIMIT 25

```

Liste der Aktivitäten von Quell-IP **192.0.2.1** und Quellport **22** in den letzten 7 Tagen

```

SELECT *
  FROM
amazon_security_lake_glue_db_us_east_1.amazon_security_lake_table_us_east_1_vpc_flow_1_0
  WHERE eventDay BETWEEN cast(date_format(current_timestamp - INTERVAL '7' day, '%Y%m
%d%H') as varchar) and cast(date_format(current_timestamp - INTERVAL '0' day, '%Y%m%d
%H') as varchar)
    AND src_endpoint.ip = '192.0.2.1'
    AND src_endpoint.port = 22
  LIMIT 25

```

Anzahl der unterschiedlichen Ziel-IP-Adressen in den letzten 7 Tagen

```

SELECT
  COUNT(DISTINCT dst_endpoint.ip)
  FROM
amazon_security_lake_glue_db_us_east_1.amazon_security_lake_table_us_east_1_vpc_flow_1_0
  WHERE eventDay BETWEEN cast(date_format(current_timestamp - INTERVAL '7' day, '%Y%m
%d%H') as varchar) and cast(date_format(current_timestamp - INTERVAL '0' day, '%Y%m%d
%H') as varchar)
  LIMIT 25

```

Datenverkehr, der in den letzten 7 Tagen von 198.51.100.0/24 stammt

```

SELECT *
  FROM
amazon_security_lake_glue_db_us_east_1.amazon_security_lake_table_us_east_1_vpc_flow_1_0
  WHERE eventDay BETWEEN cast(date_format(current_timestamp - INTERVAL '7' day, '%Y%m
%d%H') as varchar) and cast(date_format(current_timestamp - INTERVAL '0' day, '%Y%m%d
%H') as varchar)
    AND split_part(src_endpoint.ip, '.', 1)='198'AND split_part(src_endpoint.ip, '.',
2)='51'
  LIMIT 25

```

Gesamter HTTPS-Traffic der letzten 7 Tage

```

SELECT
  dst_endpoint.ip as dst,
  src_endpoint.ip as src,
  traffic.packets

```

```
FROM
amazon_security_lake_glue_db_us_east_1.amazon_security_lake_table_us_east_1_vpc_flow_1_0
WHERE eventDay BETWEEN cast(date_format(current_timestamp - INTERVAL '7' day, '%Y%m
%d%H') as varchar) and cast(date_format(current_timestamp - INTERVAL '0' day, '%Y%m%d
%H') as varchar)
AND dst_endpoint.port = 443
GROUP BY
dst_endpoint.ip,
traffic.packets,
src_endpoint.ip
ORDER BY traffic.packets DESC
LIMIT 25
```

Sortiert nach Paketanzahl für Verbindungen, die **443** in den letzten 7 Tagen für den Port bestimmt sind

```
SELECT
traffic.packets,
dst_endpoint.ip
FROM
amazon_security_lake_glue_db_us_east_1.amazon_security_lake_table_us_east_1_vpc_flow_1_0
WHERE eventDay BETWEEN cast(date_format(current_timestamp - INTERVAL '7' day, '%Y%m
%d%H') as varchar) and cast(date_format(current_timestamp - INTERVAL '0' day, '%Y%m%d
%H') as varchar)
AND dst_endpoint.port = 443
GROUP BY
traffic.packets,
dst_endpoint.ip
ORDER BY traffic.packets DESC
LIMIT 25
```

Gesamter Verkehr zwischen IP **192.0.2.1** und **192.0.2.2** in den letzten 7 Tagen

```
SELECT
start_time,
end_time,
src_endpoint.interface_uid,
connection_info.direction,
src_endpoint.ip,
dst_endpoint.ip,
src_endpoint.port,
dst_endpoint.port,
traffic.packets,
```

```

    traffic.bytes
FROM
amazon_security_lake_glue_db_us_east_1.amazon_security_lake_table_us_east_1_vpc_flow_1_0
WHERE eventDay BETWEEN cast(date_format(current_timestamp - INTERVAL '7' day, '%Y%m
%d%H') as varchar) and cast(date_format(current_timestamp - INTERVAL '0' day, '%Y%m%d
%H') as varchar)
AND(
    src_endpoint.ip = '192.0.2.1'
    AND dst_endpoint.ip = '192.0.2.2')
OR (
    src_endpoint.ip = '192.0.2.2'
    AND dst_endpoint.ip = '192.0.2.1')
ORDER BY start_time ASC
LIMIT 25

```

Gesamter eingehender Verkehr der letzten 7 Tage

```

SELECT *
FROM
amazon_security_lake_glue_db_us_east_1.amazon_security_lake_table_us_east_1_vpc_flow_1_0
WHERE eventDay BETWEEN cast(date_format(current_timestamp - INTERVAL '7' day, '%Y%m
%d%H') as varchar) and cast(date_format(current_timestamp - INTERVAL '0' day, '%Y%m%d
%H') as varchar)
AND connection_info.direction = 'ingress'
LIMIT 25

```

Gesamter ausgehender Verkehr der letzten 7 Tage

```

SELECT *
FROM
amazon_security_lake_glue_db_us_east_1.amazon_security_lake_table_us_east_1_vpc_flow_1_0
WHERE eventDay BETWEEN cast(date_format(current_timestamp - INTERVAL '7' day, '%Y%m
%d%H') as varchar) and cast(date_format(current_timestamp - INTERVAL '0' day, '%Y%m%d
%H') as varchar)
AND connection_info.direction = 'egress'
LIMIT 25

```

Der gesamte abgelehnte Verkehr der letzten 7 Tage

```

SELECT *

```

```
FROM
amazon_security_lake_glue_db_us_east_1.amazon_security_lake_table_us_east_1_vpc_flow_1_0
WHERE eventDay BETWEEN cast(date_format(current_timestamp - INTERVAL '7' day, '%Y%m%d%H') as varchar) and cast(date_format(current_timestamp - INTERVAL '0' day, '%Y%m%d%H') as varchar)
AND type_uid = 400105
LIMIT 25
```

Security Lake-Abfragen für AWS Quellversion 2 (OCSF 1.1.0)

Sie können die Daten abfragen, die Security Lake in AWS Lake Formation Datenbanken und Tabellen speichert. Sie können auch Abonnenten von Drittanbietern in der Security Lake-Konsole, API oder erstellen AWS CLI. Abonnenten von Drittanbietern können Lake Formation Formation-Daten auch aus den von Ihnen angegebenen Quellen abfragen.

Der Lake Formation Data Lake-Administrator muss der IAM-Identität, die die Daten abfragt, SELECT Berechtigungen für die entsprechenden Datenbanken und Tabellen gewähren. Ein Abonnent muss auch in Security Lake erstellt werden, bevor er Daten abfragen kann. Weitere Informationen zum Erstellen eines Abonnenten mit Abfragezugriff finden Sie unter [Verwaltung des Abfragezugriffs für Security Lake-Abbonenten](#).

Der folgende Abschnitt enthält Anleitungen zum Abfragen von Daten aus Security Lake und enthält einige Abfragebeispiele für nativ unterstützte Quellen AWS . Diese Abfragen dienen zum Abrufen von Daten in einem bestimmten Bereich. AWS-Region In diesen Beispielen wird us-east-1 (US East (Nord-Virginia)) verwendet. Darüber hinaus verwenden die Beispielabfragen einen LIMIT 25 Parameter, der bis zu 25 Datensätze zurückgibt. Sie können diesen Parameter weglassen oder ihn nach Ihren Wünschen anpassen. Weitere Beispiele finden Sie im [GitHub Verzeichnis Amazon Security Lake OCSF Queries](#).

Protokollquelltablelle

Wenn Sie Security Lake-Daten abfragen, müssen Sie den Namen der Lake Formation-Tabelle angeben, in der sich die Daten befinden.

```
SELECT *
FROM
"amazon_security_lake_glue_db_DB_Region"."amazon_security_lake_table_DB_Region_SECURITY_LAKE_T
WHERE time_dt BETWEEN CURRENT_TIMESTAMP - INTERVAL '7' DAY AND CURRENT_TIMESTAMP
LIMIT 25
```

Zu den allgemeinen Werten für die Protokollquellentabelle gehören die folgenden:

- `cloud_trail_mgmt_2_0`— AWS CloudTrail Verwaltungsereignisse
- `lambda_execution_2_0`— CloudTrail Datenereignisse für Lambda
- `s3_data_2_0`— CloudTrail Datenereignisse für S3
- `route53_2_0`— Amazon Route 53-Resolver-Abfrageprotokolle
- `sh_findings_2_0`— Ergebnisse AWS Security Hub
- `vpc_flow_2_0`— Flussprotokolle von Amazon Virtual Private Cloud (Amazon VPC)
- `eks_audit_2_0`— Auditprotokolle von Amazon Elastic Kubernetes Service (Amazon EKS)
- `waf_2_0`— v2-Protokolle AWS WAF

Beispiel: Alle Security Hub Hub-Ergebnisse in der Tabelle `sh_findings_2_0` aus der Region `us-east-1`

```
SELECT *
  FROM
    "amazon_security_lake_glue_db_us_east_1"."amazon_security_lake_table_us_east_1_sh_findings_2_0"
  WHERE time_dt BETWEEN CURRENT_TIMESTAMP - INTERVAL '7' DAY AND CURRENT_TIMESTAMP
 LIMIT 25
```

Datenbank-Region

Wenn Sie Security Lake-Daten abfragen, müssen Sie den Namen der Datenbankregion angeben, aus der Sie die Daten abfragen. Eine vollständige Liste der Datenbankregionen, in denen Security Lake derzeit verfügbar ist, finden Sie unter [Amazon Security Lake-Endpoints](#).

Beispiel: Amazon Virtual Private Cloud Cloud-Aktivitäten anhand der Quell-IP auflisten

Das folgende Beispiel listet alle Amazon VPC-Aktivitäten von der Quell-IP 192.0.2.1 auf, die nach 20230301 (01. März 2023) aufgezeichnet wurden, in der Tabelle `vpc_flow_2_0` von `us-west-2`. DB_Region

```
SELECT *
  FROM
    "amazon_security_lake_glue_db_us_east_1"."amazon_security_lake_table_us_east_1_vpc_flow_2_0"
  WHERE time_dt > TIMESTAMP '2023-03-01'
  AND src_endpoint.ip = '192.0.2.1'
```

```
ORDER BY time_dt desc
LIMIT 25
```

Datum der Partition

Durch die Partitionierung Ihrer Daten können Sie die Menge der bei jeder Abfrage gescannten Daten einschränken und so die Leistung verbessern und die Kosten senken. Partitionen funktionieren in Security Lake 2.0 etwas anders als in Security Lake 1.0. Security Lake implementiert jetzt die Partitionierung über `time_dtregion`, und `accountid`. In Security Lake 1.0 wurde dagegen die Partitionierung durch Parameter `eventDayregion`, und `accountid` implementiert.

Bei der Abfrage `time_dt` werden automatisch die Datumspartitionen von S3 abgerufen und sie können wie jedes zeitbasierte Feld in Athena abgefragt werden.

Dies ist eine Beispielabfrage, bei der die `time_dt` Partition verwendet wird, um die Logs nach dem Zeitpunkt 01. März 2023 abzufragen:

```
SELECT *
FROM
  "amazon_security_lake_glue_db_us_east_1"."amazon_security_lake_table_us_east_1_vpc_flow_2_0"
WHERE time_dt > TIMESTAMP '2023-03-01'
AND src_endpoint.ip = '192.0.2.1'
ORDER BY time desc
LIMIT 25
```

Zu den gängigen Werten für `time_dt` gehören die folgenden:

Ereignisse, die im letzten Jahr eingetreten sind

```
WHERE time_dt > CURRENT_TIMESTAMP - INTERVAL '1' YEAR
```

Ereignisse, die im letzten Monat eingetreten sind

```
WHERE time_dt > CURRENT_TIMESTAMP - INTERVAL '1' MONTH
```

Ereignisse der letzten 30 Tage

```
WHERE time_dt > CURRENT_TIMESTAMP - INTERVAL '30' DAY
```

Ereignisse der letzten 12 Stunden

```
WHERE time_dt > CURRENT_TIMESTAMP - INTERVAL '12' HOUR
```

Ereignisse der letzten 5 Minuten

```
WHERE time_dt > CURRENT_TIMESTAMP - INTERVAL '5' MINUTE
```

Ereignisse, die vor 7 bis 14 Tagen aufgetreten sind

```
WHERE time_dt BETWEEN CURRENT_TIMESTAMP - INTERVAL '14' DAY AND
CURRENT_TIMESTAMP - INTERVAL '7' DAY
```

Ereignisse, die an oder nach einem bestimmten Datum auftreten

```
WHERE time_dt >= TIMESTAMP '2023-03-01'
```

Beispiel: Liste aller CloudTrail Aktivitäten von der Quell-IP **192.0.2.1** am oder nach dem 1. März 2023 in der Tabelle **cloud_trail_mgmt_1_0**

```
SELECT *
FROM
amazon_security_lake_glue_db_us_east_1.amazon_security_lake_table_us_east_1_cloud_trail_mgmt_1_0
WHERE eventDay >= '20230301'
AND src_endpoint.ip = '192.0.2.1'
ORDER BY time desc
LIMIT 25
```

Beispiel: Liste aller CloudTrail Aktivitäten von der Quell-IP **192.0.2.1** in den letzten 30 Tagen in der Tabelle **cloud_trail_mgmt_1_0**

```
SELECT *
FROM
amazon_security_lake_glue_db_us_east_1.amazon_security_lake_table_us_east_1_cloud_trail_mgmt_1_0
WHERE eventDay > cast(date_format(current_timestamp - INTERVAL '30' day, '%Y%m%d
%H') as varchar)
AND src_endpoint.ip = '192.0.2.1'
ORDER BY time desc
LIMIT 25
```

Security Lake-Observables abfragen

Observables ist eine neue Funktion, die jetzt in Security Lake 2.0 verfügbar ist. Das beobachtbare Objekt ist ein Pivot-Element, das verwandte Informationen enthält, die sich an vielen Stellen des Ereignisses befinden. Durch die Abfrage von Observablen können Benutzer umfassende Sicherheitsinformationen aus ihren Datensätzen ableiten.

Indem Sie bestimmte Elemente innerhalb von Observables abfragen, können Sie die Datensätze auf Dinge wie bestimmte Benutzernamen, Ressourcen-UIDs, IPs, Hashes und andere IOC-Informationen beschränken

Dies ist eine Beispielabfrage, bei der das Observables-Array verwendet wird, um die Protokolle in den VPC Flow- und Route53-Tabellen abzufragen, die den IP-Wert '172.01.02.03' enthalten

```
WITH a AS
  (SELECT
    time_dt,
    observable.name,
    observable.value
  FROM
    "amazon_security_lake_glue_db_us_east_1"."amazon_security_lake_table_us_east_1_vpc_flow_2_0",
    UNNEST(observables) AS t(observable)
  WHERE time_dt BETWEEN CURRENT_TIMESTAMP - INTERVAL '7' DAY AND CURRENT_TIMESTAMP
  AND observable.value='172.01.02.03'
  AND observable.name='src_endpoint.ip'),
b as
  (SELECT
    time_dt,
    observable.name,
    observable.value
  FROM
    "amazon_security_lake_glue_db_us_east_1"."amazon_security_lake_table_us_east_1_route53_2_0",
    UNNEST(observables) AS t(observable)
  WHERE time_dt BETWEEN CURRENT_TIMESTAMP - INTERVAL '7' DAY AND CURRENT_TIMESTAMP
  AND observable.value='172.01.02.03'
  AND observable.name='src_endpoint.ip')
SELECT * FROM a
LEFT JOIN b ON a.value=b.value and a.name=b.name
LIMIT 25
```

Abfragen nach Daten CloudTrail

AWS CloudTrail verfolgt Benutzeraktivitäten und API-Nutzung in AWS-Services. Abonnenten können CloudTrail Daten abfragen, um die folgenden Arten von Informationen zu erhalten:

Hier sind einige Beispiele für CloudTrail Datenabfragen:

Unautorisierte Versuche gegen AWS-Services in den letzten 7 Tagen

```
SELECT
```

```
time_dt,  
api.service.name,  
api.operation,  
api.response.error,  
api.response.message,  
api.response.data,  
cloud.region,  
actor.user.uid,  
src_endpoint.ip,  
http_request.user_agent  
FROM  
"amazon_security_lake_glue_db_us_east_1"."amazon_security_lake_table_us_east_1_cloud_trail_mgm  
WHERE time_dt BETWEEN CURRENT_TIMESTAMP - INTERVAL '7' DAY AND CURRENT_TIMESTAMP  
AND api.response.error in (  
  'Client.UnauthorizedOperation',  
  'Client.InvalidPermission.NotFound',  
  'Client.OperationNotPermitted',  
  'AccessDenied')  
ORDER BY time desc  
LIMIT 25
```

Liste aller CloudTrail Aktivitäten von der Quell-IP **192.0.2.1** in den letzten 7 Tagen

```
SELECT  
  api.request.uid,  
  time_dt,  
  api.service.name,  
  api.operation,  
  cloud.region,  
  actor.user.uid,  
  src_endpoint.ip,  
  http_request.user_agent  
FROM  
"amazon_security_lake_glue_db_us_east_1"."amazon_security_lake_table_us_east_1_cloud_trail_mgm  
WHERE time_dt BETWEEN CURRENT_TIMESTAMP - INTERVAL '7' DAY AND CURRENT_TIMESTAMP  
AND src_endpoint.ip = '192.0.2.1.'  
ORDER BY time desc  
LIMIT 25
```

Liste aller IAM-Aktivitäten in den letzten 7 Tagen

```
SELECT *
```

```
FROM
```

```
  "amazon_security_lake_glue_db_us_east_1"."amazon_security_lake_table_us_east_1_cloud_trail_mgm
WHERE time_dt BETWEEN CURRENT_TIMESTAMP - INTERVAL '7' DAY AND CURRENT_TIMESTAMP
AND api.service.name = 'iam.amazonaws.com'
ORDER BY time desc
LIMIT 25
```

Instanzen, in denen die Anmeldeinformationen in den letzten 7 Tagen verwendet
AIDACKCEVSQ6C2EXAMPLE wurden

```
SELECT
```

```
  actor.user.uid,
  actor.user.uid_alt,
  actor.user.account.uid,
  cloud.region
```

```
FROM
```

```
  "amazon_security_lake_glue_db_us_east_1"."amazon_security_lake_table_us_east_1_cloud_trail_mgm
WHERE time_dt BETWEEN CURRENT_TIMESTAMP - INTERVAL '7' DAY AND CURRENT_TIMESTAMP
AND actor.user.credential_uid = 'AIDACKCEVSQ6C2EXAMPLE'
LIMIT 25
```

Liste der fehlgeschlagenen CloudTrail Datensätze der letzten 7 Tage

```
SELECT
```

```
  actor.user.uid,
  actor.user.uid_alt,
  actor.user.account.uid,
  cloud.region
```

```
FROM
```

```
  "amazon_security_lake_glue_db_us_east_1"."amazon_security_lake_table_us_east_1_cloud_trail_mgm
WHERE status='failed' and time_dt BETWEEN CURRENT_TIMESTAMP - INTERVAL '7' DAY AND
  CURRENT_TIMESTAMP
ORDER BY time DESC
LIMIT 25
```

Abfragen für Route 53-Resolver-Abfrageprotokolle

Die Amazon Route 53-Resolver-Abfrageprotokolle verfolgen DNS-Abfragen, die von Ressourcen in Ihrer Amazon VPC gestellt wurden. Abonnenten können die Route 53-Resolver-Abfrageprotokolle abfragen, um die folgenden Arten von Informationen zu erhalten:

Im Folgenden finden Sie einige Beispielabfragen für Route 53-Resolver-Abfrageprotokolle:

Liste der DNS-Abfragen der letzten CloudTrail 7 Tage

```
SELECT
    time_dt,
    src_endpoint.instance_uid,
    src_endpoint.ip,
    src_endpoint.port,
    query.hostname,
    rcode
FROM
    "amazon_security_lake_glue_db_us_east_1"."amazon_security_lake_table_us_east_1_route53_2_0"
WHERE time_dt BETWEEN CURRENT_TIMESTAMP - INTERVAL '7' DAY AND CURRENT_TIMESTAMP
ORDER BY time DESC
LIMIT 25
```

Liste der DNS-Abfragen, die **s3.amazonaws.com** in den letzten 7 Tagen übereinstimmten

```
SELECT
    time_dt,
    src_endpoint.instance_uid,
    src_endpoint.ip,
    src_endpoint.port,
    query.hostname,
    rcode,
    answers
FROM
    "amazon_security_lake_glue_db_us_east_1"."amazon_security_lake_table_us_east_1_route53_2_0"
WHERE query.hostname LIKE 's3.amazonaws.com.' and time_dt BETWEEN CURRENT_TIMESTAMP -
    INTERVAL '7' DAY AND CURRENT_TIMESTAMP
ORDER BY time DESC
LIMIT 25
```

Liste der DNS-Abfragen, die in den letzten 7 Tagen nicht gelöst wurden

```
SELECT
    time_dt,
    src_endpoint.instance_uid,
    src_endpoint.ip,
    src_endpoint.port,
    query.hostname,
    rcode,
    answers
```

```

FROM
  "amazon_security_lake_glue_db_us_east_1"."amazon_security_lake_table_us_east_1_route53_2_0"
WHERE cardinality(answers) = 0 and time_dt BETWEEN CURRENT_TIMESTAMP - INTERVAL '7' DAY
  AND CURRENT_TIMESTAMP
LIMIT 25

```

Liste der DNS-Abfragen, die **192.0.2.1** in den letzten 7 Tagen behoben wurden

```

SELECT
  time_dt,
  src_endpoint.instance_uid,
  src_endpoint.ip,
  src_endpoint.port,
  query.hostname,
  rcode,
  answer.rdata
FROM
  "amazon_security_lake_glue_db_us_east_1"."amazon_security_lake_table_us_east_1_route53_2_0",
  UNNEST(answers) as st(answer)
WHERE answer.rdata='192.0.2.1'
AND time_dt BETWEEN CURRENT_TIMESTAMP - INTERVAL '7' DAY AND CURRENT_TIMESTAMP
LIMIT 25

```

Abfragen zu Ergebnissen von Security Hub

Security Hub bietet Ihnen einen umfassenden Überblick über Ihren Sicherheitsstatus AWS und hilft Ihnen dabei, Ihre Umgebung anhand von Industriestandards und Best Practices zu überprüfen. Security Hub erstellt Ergebnisse für Sicherheitsüberprüfungen und erhält Ergebnisse von Diensten Dritter.

Hier sind einige Beispielabfragen zu Ergebnissen von Security Hub:

Neue Ergebnisse mit einem Schweregrad größer oder gleich **MEDIUM** in den letzten 7 Tagen

```

SELECT
  time_dt,
  finding_info,
  severity_id,
  status
FROM
  "amazon_security_lake_glue_db_us_east_1"."amazon_security_lake_table_us_east_1_sh_findings_2_0"
WHERE time_dt BETWEEN CURRENT_TIMESTAMP - INTERVAL '7' DAY AND CURRENT_TIMESTAMP

```

```

AND severity_id >= 3
AND status = 'New'
ORDER BY time DESC
LIMIT 25

```

Doppelte Befunde in den letzten 7 Tagen

```

SELECT
  finding_info.uid,
  MAX(time_dt) AS time,
  ARBITRARY(region) AS region,
  ARBITRARY(accountid) AS accountid,
  ARBITRARY(finding_info) AS finding,
  ARBITRARY(vulnerabilities) AS vulnerabilities
FROM
  "amazon_security_lake_glue_db_us_east_1"."amazon_security_lake_table_us_east_1_sh_findings_2_0
WHERE time_dt BETWEEN CURRENT_TIMESTAMP - INTERVAL '7' DAY AND CURRENT_TIMESTAMP
GROUP BY finding_info.uid
LIMIT 25

```

Alle nicht informativen Ergebnisse der letzten 7 Tage

```

SELECT
  time_dt,
  finding_info.title,
  finding_info,
  severity
FROM
  "amazon_security_lake_glue_db_us_east_1"."amazon_security_lake_table_us_east_1_sh_findings_2_0
WHERE severity != 'Informational' and time_dt BETWEEN CURRENT_TIMESTAMP - INTERVAL '7'
  DAY AND CURRENT_TIMESTAMP
LIMIT 25

```

Ergebnisse, bei denen es sich bei der Ressource um einen Amazon S3 S3-Bucket handelt (keine Zeitbeschränkung)

```

SELECT *
FROM
  "amazon_security_lake_glue_db_us_east_1"."amazon_security_lake_table_us_east_1_sh_findings_2_0
WHERE any_match(resources, element -> element.type = 'AwsS3Bucket')
LIMIT 25

```

Ergebnisse mit einem CVSS-Wert (Common Vulnerability Scoring System) von mehr als **1** (ohne Zeitbeschränkung)

```
SELECT
  DISTINCT finding_info.uid
  time_dt,
  metadata,
  finding_info,
  vulnerabilities,
  resource
FROM
  "amazon_security_lake_glue_db_us_east_1"."amazon_security_lake_table_us_east_1_sh_findings_2_0
UNNEST(vulnerabilities) AS t(vulnerability),
UNNEST(vulnerability.cve.cvss) AS t(cvs)
WHERE cvs.base_score > 1.0
AND vulnerabilities is NOT NULL
LIMIT 25
```

Ergebnisse, die mit Common Vulnerabilities and Exposures (CVE) übereinstimmen **CVE-0000-0000** (keine zeitliche Beschränkung)

```
SELECT *
FROM
  "amazon_security_lake_glue_db_us_east_1"."amazon_security_lake_table_us_east_1_sh_findings_2_0
WHERE any_match(vulnerabilities, element -> element.cve.uid = 'CVE-0000-0000')
LIMIT 25
```

Anzahl der Produkte, die in den letzten 7 Tagen Ergebnisse von Security Hub gesendet haben

```
SELECT
  metadata.product.name,
  count(*)
FROM
  "amazon_security_lake_glue_db_us_east_1"."amazon_security_lake_table_us_east_1_sh_findings_2_0
WHERE time_dt BETWEEN CURRENT_TIMESTAMP - INTERVAL '7' DAY AND CURRENT_TIMESTAMP
GROUP BY metadata.product.name
ORDER BY metadata.product.name DESC
LIMIT 25
```

Anzahl der Ressourcentypen in den Ergebnissen der letzten 7 Tage

```
SELECT
```

```
count(*) AS "Total",
resource.type
FROM
"amazon_security_lake_glue_db_us_east_1"."amazon_security_lake_table_us_east_1_sh_findings_2_0
WHERE time_dt BETWEEN CURRENT_TIMESTAMP - INTERVAL '7' DAY AND CURRENT_TIMESTAMP
GROUP BY resource.type
ORDER BY count(*) DESC
LIMIT 25
```

Anfällige Pakete aufgrund von Ergebnissen der letzten 7 Tage

```
SELECT
vulnerabilities
FROM
"amazon_security_lake_glue_db_us_east_1"."amazon_security_lake_table_us_east_1_sh_findings_2_0
WHERE time_dt BETWEEN CURRENT_TIMESTAMP - INTERVAL '7' DAY AND CURRENT_TIMESTAMP
AND vulnerabilities is NOT NULL
LIMIT 25
```

Ergebnisse, die sich in den letzten 7 Tagen geändert haben

```
SELECT
status,
finding_info.title,
finding_info.created_time_dt,
finding_info,
finding_info.uid,
finding_info.first_seen_time_dt,
finding_info.last_seen_time_dt,
finding_info.modified_time_dt
FROM
"amazon_security_lake_glue_db_us_east_1"."amazon_security_lake_table_us_east_1_sh_findings_2_0
WHERE time_dt BETWEEN CURRENT_TIMESTAMP - INTERVAL '7' DAY AND CURRENT_TIMESTAMP
LIMIT 25
```

Abfragen für Amazon-VPC-Flow-Protokolle

Amazon Virtual Private Cloud (Amazon VPC) bietet Details zum IP-Verkehr zu und von Netzwerkschnittstellen in Ihrer VPC.

Hier sind einige Beispielabfragen für Amazon VPC Flow Logs:

Insbesondere der Verkehr AWS-Regionen der letzten 7 Tage

```
SELECT *
  FROM
    "amazon_security_lake_glue_db_us_east_1"."amazon_security_lake_table_us_east_1_vpc_flow_2_0"
WHERE time_dt BETWEEN CURRENT_TIMESTAMP - INTERVAL '7' DAY AND CURRENT_TIMESTAMP
AND region in ('us-east-1','us-east-2','us-west-2')
LIMIT 25
```

Liste der Aktivitäten von Quell-IP **192.0.2.1** und Quellport **22** in den letzten 7 Tagen

```
SELECT *
  FROM
    "amazon_security_lake_glue_db_us_east_1"."amazon_security_lake_table_us_east_1_vpc_flow_2_0"
WHERE time_dt BETWEEN CURRENT_TIMESTAMP - INTERVAL '7' DAY AND CURRENT_TIMESTAMP
AND src_endpoint.ip = '192.0.2.1'
AND src_endpoint.port = 22
LIMIT 25
```

Anzahl der unterschiedlichen Ziel-IP-Adressen in den letzten 7 Tagen

```
SELECT
  COUNT(DISTINCT dst_endpoint.ip) AS "Total"
  FROM
    "amazon_security_lake_glue_db_us_east_1"."amazon_security_lake_table_us_east_1_vpc_flow_2_0"
WHERE time_dt BETWEEN CURRENT_TIMESTAMP - INTERVAL '7' DAY AND CURRENT_TIMESTAMP
LIMIT 25
```

Datenverkehr, der in den letzten 7 Tagen von 198.51.100.0/24 stammt

```
SELECT *
  FROM
    "amazon_security_lake_glue_db_us_east_1"."amazon_security_lake_table_us_east_1_vpc_flow_2_0"
WHERE time_dt BETWEEN CURRENT_TIMESTAMP - INTERVAL '7' DAY AND CURRENT_TIMESTAMP
AND split_part(src_endpoint.ip, '.', 1)='198'AND split_part(src_endpoint.ip, '.', 2)='51'
LIMIT 25
```

Gesamter HTTPS-Verkehr der letzten 7 Tage

```
SELECT
  dst_endpoint.ip as dst,
  src_endpoint.ip as src,
```

```
    traffic.packets
FROM
    "amazon_security_lake_glue_db_us_east_1"."amazon_security_lake_table_us_east_1_vpc_flow_2_0"
WHERE time_dt BETWEEN CURRENT_TIMESTAMP - INTERVAL '7' DAY AND CURRENT_TIMESTAMP
AND dst_endpoint.port = 443
GROUP BY
    dst_endpoint.ip,
    traffic.packets,
    src_endpoint.ip
ORDER BY traffic.packets DESC
LIMIT 25
```

Sortiert nach Paketanzahl für Verbindungen, die **443** in den letzten 7 Tagen für den Port bestimmt sind

```
SELECT
    traffic.packets,
    dst_endpoint.ip
FROM
    "amazon_security_lake_glue_db_us_east_1"."amazon_security_lake_table_us_east_1_vpc_flow_2_0"
WHERE time_dt BETWEEN CURRENT_TIMESTAMP - INTERVAL '7' DAY AND CURRENT_TIMESTAMP
AND dst_endpoint.port = 443
GROUP BY
    traffic.packets,
    dst_endpoint.ip
ORDER BY traffic.packets DESC
LIMIT 25
```

Gesamter Verkehr zwischen IP **192.0.2.1** und **192.0.2.2** in den letzten 7 Tagen

```
SELECT
    start_time_dt,
    end_time_dt,
    src_endpoint.interface_uid,
    connection_info.direction,
    src_endpoint.ip,
    dst_endpoint.ip,
    src_endpoint.port,
    dst_endpoint.port,
    traffic.packets,
    traffic.bytes
FROM
    "amazon_security_lake_glue_db_us_east_1"."amazon_security_lake_table_us_east_1_vpc_flow_2_0"
```

```
WHERE time_dt BETWEEN CURRENT_TIMESTAMP - INTERVAL '7' DAY AND CURRENT_TIMESTAMP
AND(
    src_endpoint.ip = '192.0.2.1'
AND dst_endpoint.ip = '192.0.2.2')
OR (
    src_endpoint.ip = '192.0.2.2'
AND dst_endpoint.ip = '192.0.2.1')
ORDER BY start_time_dt ASC
LIMIT 25
```

Der gesamte eingehende Verkehr der letzten 7 Tage

```
SELECT *
FROM
    "amazon_security_lake_glue_db_us_east_1"."amazon_security_lake_table_us_east_1_vpc_flow_2_0"
WHERE time_dt BETWEEN CURRENT_TIMESTAMP - INTERVAL '7' DAY AND CURRENT_TIMESTAMP
AND connection_info.direction = 'Inbound'
LIMIT 25
```

Gesamter ausgehender Verkehr der letzten 7 Tage

```
SELECT *
FROM
    "amazon_security_lake_glue_db_us_east_1"."amazon_security_lake_table_us_east_1_vpc_flow_2_0"
WHERE time_dt BETWEEN CURRENT_TIMESTAMP - INTERVAL '7' DAY AND CURRENT_TIMESTAMP
AND connection_info.direction = 'Outbound'
LIMIT 25
```

Der gesamte abgelehnte Verkehr der letzten 7 Tage

```
SELECT *
FROM
    "amazon_security_lake_glue_db_us_east_1"."amazon_security_lake_table_us_east_1_vpc_flow_2_0"
WHERE time_dt BETWEEN CURRENT_TIMESTAMP - INTERVAL '7' DAY AND CURRENT_TIMESTAMP
AND action = 'Denied'
LIMIT 25
```

Abfragen für Amazon EKS-Auditprotokolle

Amazon EKS-Protokolle verfolgen Aktivitäten auf der Kontrollebene und stellen Prüf- und Diagnoseprotokolle direkt von der Amazon EKS-Steuerebene in CloudWatch Logs in Ihrem Konto

zur Verfügung. Diese Protokolle erleichtern Ihnen die Absicherung und Ausführung Ihrer Cluster. Abonnenten können EKS-Protokolle abfragen, um die folgenden Arten von Informationen zu erhalten.

Hier sind einige Beispielabfragen für Amazon EKS-Audit-Logs:

Anfragen an eine bestimmte URL in den letzten 7 Tagen

```
SELECT
    time_dt,
    actor.user.name,
    http_request.url.path,
    activity_name
FROM
    "amazon_security_lake_glue_db_us_east_1"."amazon_security_lake_table_us_east_1_eks_audit_2_0"
WHERE time_dt BETWEEN CURRENT_TIMESTAMP - INTERVAL '7' DAY AND CURRENT_TIMESTAMP
AND activity_name = 'get'
and http_request.url.path = '/apis/coordination.k8s.io/v1/'
LIMIT 25
```

Aktualisiere Anfragen von '10.0.97.167' in den letzten 7 Tagen

```
SELECT
    activity_name,
    time_dt,
    api.request,
    http_request.url.path,
    src_endpoint.ip,
    resources
FROM
    "amazon_security_lake_glue_db_us_east_1"."amazon_security_lake_table_us_east_1_eks_audit_2_0"
WHERE time_dt BETWEEN CURRENT_TIMESTAMP - INTERVAL '7' DAY AND CURRENT_TIMESTAMP
AND src_endpoint.ip = '10.0.97.167'
AND activity_name = 'Update'
LIMIT 25
```

Anfragen und Antworten im Zusammenhang mit der Ressource 'kube-controller-manager' in den letzten 7 Tagen

```
SELECT
    activity_name,
    time_dt,
    api.request,
```

```
    api.response,  
    resource.name  
FROM  
  "amazon_security_lake_glue_db_us_east_1"."amazon_security_lake_table_us_east_1_eks_audit_2_0",  
UNNEST(resources) AS t(resource)  
WHERE time_dt BETWEEN CURRENT_TIMESTAMP - INTERVAL '7' DAY AND CURRENT_TIMESTAMP  
AND resource.name = 'kube-controller-manager'  
LIMIT 25
```

Abfragen für v2-Protokolle AWS WAF

AWS WAF ist eine Firewall für Webanwendungen, mit der Sie Webanfragen überwachen können, die Ihre Endbenutzer an Ihre Anwendungen senden, und den Zugriff auf Ihre Inhalte kontrollieren können.

Hier sind einige Beispiele für Abfragen für AWS WAF v2-Logs:

Anfragen von einer bestimmten Quell-IP in den letzten 7 Tagen posten

```
SELECT  
  time_dt,  
  activity_name,  
  src_endpoint.ip,  
  http_request.url.path,  
  http_request.url.hostname,  
  http_request.http_method,  
  http_request.http_headers  
FROM  
  "amazon_security_lake_glue_db_us_east_1"."amazon_security_lake_table_us_east_1_waf_2_0"  
WHERE time_dt BETWEEN CURRENT_TIMESTAMP - INTERVAL '7' DAY AND CURRENT_TIMESTAMP  
AND src_endpoint.ip = '100.123.123.123'  
AND activity_name = 'Post'  
LIMIT 25
```

Anfragen, die in den letzten 7 Tagen einem Firewalltyp MANAGED_RULE_GROUP entsprachen

```
SELECT  
  time_dt,  
  activity_name,  
  src_endpoint.ip,  
  http_request.url.path,  
  http_request.url.hostname,
```

```
    http_request.http_method,  
    firewall_rule.uid,  
    firewall_rule.type,  
    firewall_rule.condition,  
    firewall_rule.match_location,  
    firewall_rule.match_details,  
    firewall_rule.rate_limit  
FROM  
    "amazon_security_lake_glue_db_us_east_1"."amazon_security_lake_table_us_east_1_waf_2_0"  
WHERE time_dt BETWEEN CURRENT_TIMESTAMP - INTERVAL '7' DAY AND CURRENT_TIMESTAMP  
AND firewall_rule.type = 'MANAGED_RULE_GROUP'  
LIMIT 25
```

Anfragen, die in den letzten 7 Tagen mit einem REGEX in einer Firewallregel übereinstimmen

```
SELECT  
    time_dt,  
    activity_name,  
    src_endpoint.ip,  
    http_request.url.path,  
    http_request.url.hostname,  
    http_request.http_method,  
    firewall_rule.uid,  
    firewall_rule.type,  
    firewall_rule.condition,  
    firewall_rule.match_location,  
    firewall_rule.match_details,  
    firewall_rule.rate_limit  
FROM  
    "amazon_security_lake_glue_db_us_east_1"."amazon_security_lake_table_us_east_1_waf_2_0"  
WHERE time_dt BETWEEN CURRENT_TIMESTAMP - INTERVAL '7' DAY AND CURRENT_TIMESTAMP  
AND firewall_rule.condition = 'REGEX'  
LIMIT 25
```

Das Abrufen von Anfragen nach AWS Anmeldeinformationen, die in den letzten 7 Tagen die AWS WAF Regel ausgelöst haben, wurde verweigert

```
SELECT  
    time_dt,  
    activity_name,  
    action,  
    src_endpoint.ip,  
    http_request.url.path,
```

```
    http_request.url.hostname,  
    http_request.http_method,  
    firewall_rule.uid,  
    firewall_rule.type  
FROM  
    "amazon_security_lake_glue_db_us_east_1"."amazon_security_lake_table_us_east_1_waf_2_0"  
WHERE time_dt BETWEEN CURRENT_TIMESTAMP - INTERVAL '7' DAY AND CURRENT_TIMESTAMP  
AND http_request.url.path = '/.aws/credentials'  
AND action = 'Denied'  
LIMIT 25
```

Ruft Anfragen nach AWS Zugangsdaten ab, gruppiert nach Ländern der letzten 7 Tage

```
SELECT count(*) as Total,  
    src_endpoint.location.country AS Country,  
    activity_name,  
    action,  
    src_endpoint.ip,  
    http_request.url.path,  
    http_request.url.hostname,  
    http_request.http_method  
FROM  
    "amazon_security_lake_glue_db_us_east_1"."amazon_security_lake_table_us_east_1_waf_2_0"  
WHERE time_dt BETWEEN CURRENT_TIMESTAMP - INTERVAL '7' DAY  
    AND CURRENT_TIMESTAMP  
    AND activity_name = 'Get'  
    AND http_request.url.path = '/.aws/credentials'  
GROUP BY src_endpoint.location.country,  
    activity_name,  
    action,  
    src_endpoint.ip,  
    http_request.url.path,  
    http_request.url.hostname,  
    http_request.http_method
```

Lebenszyklusmanagement in Security Lake

Sie können Security Lake so anpassen, dass Daten AWS-Regionen für den von Ihnen gewünschten Zeitraum in Ihrer bevorzugten Umgebung gespeichert werden. Lifecycle Management kann Ihnen dabei helfen, unterschiedliche Compliance-Anforderungen zu erfüllen.

Verwaltung der Aufbewahrung

Um Ihre Daten so zu verwalten, dass sie kostengünstig gespeichert werden, können Sie Aufbewahrungseinstellungen für die Daten konfigurieren. Da Security Lake Ihre Daten als Objekte in Amazon Simple Storage Service (Amazon S3) -Buckets speichert, entsprechen die Aufbewahrungseinstellungen einer Amazon S3-Lifecycle-Konfiguration. Durch die Konfiguration dieser Einstellungen können Sie Ihre bevorzugte Amazon S3 S3-Speicherklasse und den Zeitraum angeben, für den S3-Objekte in dieser Speicherklasse verbleiben sollen, bevor sie in eine andere Speicherklasse wechseln oder ablaufen. Weitere Informationen zu Amazon S3 Lifecycle-Konfigurationen finden Sie unter [Verwaltung Ihres Speicherlebenszyklus](#) im Amazon Simple Storage Service-Benutzerhandbuch.

In Security Lake geben Sie Aufbewahrungseinstellungen auf Regionsebene an. Sie könnten sich beispielsweise dafür entscheiden, alle S3-Objekte in einer bestimmten Speicherklasse AWS-Region auf die S3-Standard-IA-Speicherklasse 30 Tage nach dem Schreiben in den Data Lake umzustellen. Die standardmäßige Amazon S3 S3-Speicherklasse ist S3 Standard.

Important

Security Lake unterstützt Amazon S3 Object Lock nicht. Wenn die Data Lake-Buckets erstellt werden, ist S3 Object Lock standardmäßig deaktiviert. Wenn Sie S3 Object Lock mit dem standardmäßigen Aufbewahrungsmodus aktivieren, wird die Übermittlung von normalisierten Protokolldaten an den Data Lake unterbrochen.

Konfiguration der Aufbewahrungseinstellungen bei der Aktivierung von Security Lake

Folgen Sie diesen Anweisungen, um die Aufbewahrungseinstellungen für eine oder mehrere Regionen zu konfigurieren, wenn Sie bei Security Lake einsteigen. Wenn Sie keine

Aufbewahrungseinstellungen konfigurieren, verwendet Security Lake die Standardeinstellungen für eine Amazon S3 Lifecycle-Konfiguration — speichern Sie die Daten auf unbestimmte Zeit mit der Speicherklasse S3 Standard.

Console

1. [Öffnen Sie die Security Lake-Konsole unter https://console.aws.amazon.com/securitylake/](https://console.aws.amazon.com/securitylake/).
2. Wenn Sie Schritt 2: Definieren Sie das Zielziel des Onboarding-Workflows erreicht haben, wählen Sie unter Speicherklassen auswählen die Option Übergang hinzufügen aus. Wählen Sie dann die Amazon S3 S3-Speicherklasse aus, auf die Sie S3-Objekte umstellen möchten. (Die nicht aufgeführte Standardspeicherklasse ist S3 Standard.) Geben Sie außerdem einen Aufbewahrungszeitraum (in Tagen) für diese Speicherklasse an. Um Objekte nach dieser Zeit in eine andere Speicherklasse umzuwandeln, wählen Sie Übergang hinzufügen und geben Sie die Einstellungen für die nachfolgende Speicherklasse und den Aufbewahrungszeitraum ein.
3. Um anzugeben, wann S3-Objekte ablaufen sollen, wählen Sie Übergang hinzufügen. Wählen Sie dann für die Speicherklasse die Option Expire aus. Geben Sie für den Aufbewahrungszeitraum die Gesamtzahl der Tage ein, an denen Sie Objekte nach der Erstellung der Objekte in Amazon S3 unter Verwendung einer beliebigen Speicherklasse speichern möchten. Wenn dieser Zeitraum endet, laufen Objekte ab und Amazon S3 löscht sie.
4. Wenn Sie fertig sind, wählen Sie Next (Weiter) aus.

Ihre Änderungen gelten für alle Regionen, in denen Sie Security Lake bei früheren Onboarding-Schritten aktiviert haben.

API

Verwenden Sie die Security Lake-API, um die Aufbewahrungseinstellungen beim Onboarding in Security Lake programmgesteuert [CreateDataLake](#) zu konfigurieren. Wenn Sie den verwenden, führen Sie den AWS CLI Befehl aus. [create-data-lake](#) Geben Sie die gewünschten Aufbewahrungseinstellungen in den `lifecycleConfiguration` Parametern wie folgt an:

- Geben Sie für die Gesamtzahl der Tage (`days`) `antransitions`, an denen Sie S3-Objekte in einer bestimmten Amazon S3 S3-Speicherklasse (`storageClass`) speichern möchten.
- Geben Sie für die Gesamtzahl der Tage `anexpiration`, an denen Sie Objekte in Amazon S3 speichern möchten, und verwenden Sie dabei eine beliebige Speicherklasse, nachdem Objekte erstellt wurden. Wenn dieser Zeitraum endet, laufen Objekte ab und Amazon S3 löscht sie.

Security Lake wendet die Einstellungen auf die Region an, die Sie im `region` Feld des `configurations` Objekts angeben.

Der folgende Befehl aktiviert beispielsweise Security Lake in der `us-east-1` Region. In dieser Region laufen Objekte nach 365 Tagen ab und Objekte werden nach 60 Tagen in die Speicherklasse `ONEZONE_IA` S3 überführt. Dieses Beispiel ist für Linux, macOS oder Unix formatiert und verwendet den umgekehrten Schrägstrich (`\`) zur Verbesserung der Lesbarkeit.

```
$ aws securitylake create-data-lake \  
--configurations '[{"encryptionConfiguration":  
{"kmsKeyId": "S3_MANAGED_KEY", "region": "us-east-1", "lifecycleConfiguration":  
{"expiration": {"days": 365}, "transitions":  
[{"days": 60, "storageClass": "ONEZONE_IA"}]}]'] \  
--meta-store-manager-role-arn "arn:aws:securitylake:ap-  
northeast-2:123456789012:data-lake/default"
```

Aufbewahrungseinstellungen werden aktualisiert

Folgen Sie diesen Anweisungen, um die Aufbewahrungseinstellungen für eine oder mehrere Regionen zu aktualisieren, nachdem Sie Security Lake aktiviert haben.

Console

1. Öffnen Sie die Security Lake-Konsole unter <https://console.aws.amazon.com/securitylake/>.
2. Wählen Sie im Navigationsbereich Regionen
3. Wählen Sie eine Region aus und klicken Sie dann auf Bearbeiten.
4. Geben Sie im Abschnitt Speicherklassen auswählen die gewünschten Einstellungen ein. Wählen Sie als Speicherklasse die Amazon S3 S3-Speicherklasse aus, auf die Sie S3-Objekte umstellen möchten. (Die nicht aufgeführte Standardspeicherklasse ist S3 Standard.) Geben Sie als Aufbewahrungszeitraum die Anzahl der Tage ein, für die Sie Objekte in dieser Speicherklasse speichern möchten. Sie können mehrere Übergänge angeben.

Um auch anzugeben, wann S3-Objekte ablaufen sollen, wählen Sie `Expire` für die Speicherklasse. Geben Sie dann als Aufbewahrungszeitraum die Gesamtzahl der Tage ein, an denen Sie Objekte nach der Erstellung der Objekte in Amazon S3 unter Verwendung einer beliebigen Speicherklasse speichern möchten. Wenn dieser Zeitraum endet, laufen Objekte ab und Amazon S3 löscht sie.

5. Wählen Sie `Save` (Speichern) aus, wenn Sie fertig sind.

API

Um die Aufbewahrungseinstellungen programmgesteuert zu aktualisieren, verwenden Sie den [UpdateDataLake](#) Betrieb der Security Lake-API. Wenn Sie sie verwenden AWS CLI, führen Sie den Befehl aus. [update-data-lake](#) Verwenden Sie in Ihrer Anfrage den `lifecycleConfiguration` Parameter, um die neuen Einstellungen anzugeben:

- Um die Übergangseinstellungen zu ändern, verwenden Sie die `transitions` Parameter, um jeden neuen Zeitraum in Tagen (`days`) anzugeben, in dem Sie S3-Objekte in einer bestimmten Amazon S3 S3-Speicherklasse (`storageClass`) speichern möchten.
- Um die gesamte Aufbewahrungsdauer zu ändern, verwenden Sie den `expiration` Parameter, um die Gesamtzahl der Tage anzugeben, an denen Sie S3-Objekte nach der Erstellung der Objekte unter Verwendung einer beliebigen Speicherklasse speichern möchten. Wenn diese Aufbewahrungsfrist endet, laufen Objekte ab und Amazon S3 löscht sie.

Security Lake wendet die Einstellungen auf die Region an, die Sie im `region` Feld des `configurations` Objekts angeben.

Mit dem folgenden AWS CLI Befehl werden beispielsweise die Datenablaufeinstellungen und die Einstellungen für den Speicherübergang für die `us-east-1` Region aktualisiert. In dieser Region laufen Objekte nach 500 Tagen ab und Objekte werden nach 30 Tagen in die Speicherklasse `ONEZONE_IA` S3 überführt. Dieses Beispiel ist für Linux, macOS oder Unix formatiert und verwendet den umgekehrten Schrägstrich (`\`) zur Verbesserung der Lesbarkeit.

```
$ aws securitylake update-data-lake \  
--configurations '[{"encryptionConfiguration":  
  {"kmsKeyId":"S3_MANAGED_KEY"},"region":"us-east-1","lifecycleConfiguration":  
  {"expiration":{"days":500},"transitions":  
  [{"days":30,"storageClass":"ONEZONE_IA"}]}]' \  
--meta-store-manager-role-arn "arn:aws:securitylake:ap-  
northeast-2:123456789012:data-lake/default"
```

Regionen zusammenfassen

Eine Rollup-Region konsolidiert Daten aus einer oder mehreren beitragenden Regionen. Dies kann Ihnen helfen, die regionalen Datenkonformitätsanforderungen zu erfüllen.

Anweisungen zur Konfiguration von Rollup-Regionen finden Sie unter. [Konfiguration von Rollup-Regionen](#)

Offenes Cybersecurity Schema Framework (OCSF)

Was ist OCSF?

Das [Open Cybersecurity Schema Framework \(OCSF\)](#) ist eine gemeinsame Open-Source-Initiative von AWS führenden Partnern in der Cybersicherheitsbranche. OCSF bietet ein Standardschema für allgemeine Sicherheitsereignisse, definiert Versionierungskriterien, um die Schemaentwicklung zu erleichtern, und beinhaltet einen Selbstverwaltungsprozess für Hersteller und Nutzer von Sicherheitsprotokollen. Der öffentliche Quellcode für OCSF wird auf [GitHub](#) gehostet.

Security Lake konvertiert automatisch Protokolle und Ereignisse, die von nativ unterstützten Systemen stammen, in das OCSF-Schema AWS-Services. Nach der Konvertierung in OCSF speichert Security Lake die Daten in einem Amazon Simple Storage Service (Amazon S3) -Bucket (ein Bucket pro Bucket AWS-Region) in Ihrem AWS-Konto. Protokolle und Ereignisse, die aus benutzerdefinierten Quellen in Security Lake geschrieben werden, müssen dem OCSF-Schema und einem Apache Parquet-Format entsprechen. Abonnenten können die Protokolle und Ereignisse als generische Parquet-Datensätze behandeln oder die OCSF-Schema-Ereignisklasse anwenden, um die in einem Datensatz enthaltenen Informationen genauer zu interpretieren.

OCSF-Ereignisklassen

Protokolle und Ereignisse aus einer bestimmten Security [Lake-Quelle](#) entsprechen einer bestimmten in OCSF definierten Ereignisklasse. DNS-Aktivität, SSH-Aktivität und Authentifizierung sind Beispiele für [Ereignisklassen in](#) OCSF. Sie können angeben, welcher Ereignisklasse eine bestimmte Quelle entspricht.

Identifizierung der OCSF-Quelle

OCSF verwendet eine Vielzahl von Feldern, anhand derer Sie ermitteln können, woher ein bestimmter Satz von Protokollen oder Ereignissen stammt. Dies sind die Werte der entsprechenden Felder AWS-Services, die in Security Lake nativ als Quellen unterstützt werden.

The OCSF source identification for AWS log sources (Version 1) are listed in the following table.

Quelle	metadata. product.name	metadata. produkt.H erstellername	metadata. product.f eature.name	Klassenname	Metadaten .Version
CloudTrail Lambda-Da tenereignisse	CloudTrai l	AWS	Data	API Activity	1.0.0-rc. 2
CloudTrai l Ereigniss e für das Management	CloudTrai l	AWS	Managemen t	API Activity, Authentic ation oder Account Change	1.0.0-rc. 2
CloudTrail S3-Datene reignisse	CloudTrai l	AWS	Data	API Activity	1.0.0-rc. 2
Route 53	Route 53	AWS	Resolver Query Logs	DNS Activity	1.0.0-rc. 2
Security Hub	Security Hub	AWS	Entsprich t dem Security Hub ProductNa me _Hub-Wert	Security Finding	1.0.0-rc. 2
VPC Flow Logs	Amazon VPC	AWS	Flowlogs	Network Activity	1.0.0-rc. 2

The OCSF source identification for AWS log sources (Version 2) are listed in the following table.

Quelle	metadata. product.name	metadata. produkt.H erstellername	metadata. product.f eature.name	Klassenname	Metadaten .Version
CloudTrail Lambda-Da tenereignisse	CloudTrai l	AWS	Data	API Activity	1.1.0
CloudTrai l Ereigniss e für das Management	CloudTrai l	AWS	Managemen t	API Activity, Authentic ation oder Account Change	1.1.0
CloudTrail S3-Datene reignisse	CloudTrai l	AWS	Data	API Activity	1.1.0
Route 53	Route 53	AWS	Resolver Query Logs	DNS Activity	1.1.0
Security Hub	Entspricht dem Wert des AWS Security Finding Format (ASFF) ProductNa me	Entspricht dem AWS Wert des Security Finding Format (ASFF) CompanyNa me	Entsprich t dem featureNa me Wert aus ASFF ProductFi elds	Vulnerabi lity Finding, Complianc e Finding, or Detection Finding	1.1.0
VPC Flow Logs	Amazon VPC	AWS	Flowlogs	Network Activity	1.1.0

Quelle	metadata. product.name	metadata. produkt.H erstellername	metadata. product.f eature.name	Klassenname	Metadaten .Version
EKS-Prüfprotokolle	Amazon EKS	AWS	Elastic Kubernete s Service	API Activity	1.1.0
AWS WAF v2-Protokolle	AWS WAF	AWS	–	HTTP Activity	1.1.0

Integrationen mit Security Lake

Amazon Security Lake lässt sich in andere Produkte AWS-Services und Produkte von Drittanbietern integrieren. Integrationen können Daten als Quelle an Security Lake senden oder als Abonnent Daten in Security Lake nutzen. In den folgenden Themen wird erklärt, welche Produkte AWS-Services und Produkte von Drittanbietern in Security Lake integriert werden können.

Themen

- [AWS-Service Integrationen mit Security Lake](#)
- [Integrationen von Drittanbietern mit Security Lake](#)

AWS-Service Integrationen mit Security Lake

Amazon Security Lake lässt sich mit anderen integrieren AWS-Services. Ein Service kann entweder als Quellintegration, Abonnentenintegration oder als beides betrieben werden.

Quellintegrationen haben die folgenden Eigenschaften:

- Daten an Security Lake senden
- Daten kommen im [Offenes Cybersecurity Schema Framework \(OCSF\)](#) Schema an
- Daten kommen im Apache Parquet-Format an

Abonnentenintegrationen haben die folgenden Eigenschaften: Sie können Quelldaten aus Security Lake an einem HTTPS-Endpunkt oder einer Amazon Simple Queue Service (Amazon SQS) - Warteschlange lesen oder Quelldaten direkt abfragen von AWS Lake Formation

Im folgenden Abschnitt wird erklärt, in welche AWS-Services Security Lake integriert werden kann und wie die einzelnen Integrationen funktionieren.

Integration mit AWS AppFabric

Integrationstyp: Quelle

[AWS AppFabric](#) ist ein No-Code-Service, der Software-as-a-Service (SaaS) -Anwendungen in Ihrem Unternehmen verbindet, sodass IT- und Sicherheitsteams Anwendungen mithilfe eines Standardschemas und eines zentralen Repositorys verwalten und sichern können.

Wie erhält AppFabric Security Lake die Ergebnisse

Sie können AppFabric Audit-Protokolldaten an Security Lake senden, indem Sie Amazon Kinesis Data Firehose als Ziel auswählen und Kinesis Data Firehose so konfigurieren, dass Daten im OCSF-Schema und im Apache Parquet-Format an Security Lake gesendet werden.

Voraussetzungen

Bevor Sie AppFabric Audit-Logs an Security Lake senden können, müssen Sie Ihre normalisierten OCSF-Audit-Logs in einen Kinesis Data Firehose Firehose-Stream ausgeben. Anschließend können Sie Kinesis Data Firehose so konfigurieren, dass die Ausgabe an Ihren Security Lake Amazon S3 S3-Bucket gesendet wird. Weitere Informationen finden [Sie unter Wählen Sie Amazon S3 für Ihr Ziel](#) im Amazon Kinesis Developer Guide.

Senden Sie Ihre AppFabric Ergebnisse an Security Lake

Um AppFabric Auditprotokolle an Security Lake zu senden, nachdem Sie die oben genannten Voraussetzungen erfüllt haben, müssen Sie beide Dienste aktivieren und AppFabric als benutzerdefinierte Quelle in Security Lake hinzufügen. Anweisungen zum Hinzufügen einer benutzerdefinierten Quelle finden Sie unter [Sammeln von Daten aus benutzerdefinierten Quellen](#).

Beenden Sie den Empfang von AppFabric Protokollen in Security Lake

Um den Empfang von AppFabric Auditprotokollen zu beenden, können Sie die Security Lake-Konsole, die Security Lake-API oder AWS CLI das Löschen AppFabric als benutzerdefinierte Quelle verwenden. Anweisungen finden Sie unter [Löschen einer benutzerdefinierten Quelle](#).

Integration mit Amazon Detective

Integrationstyp: Abonnent

[Amazon Detective](#) hilft Ihnen, die Ursache von Sicherheitserkenntnissen oder verdächtigen Aktivitäten zu analysieren, zu untersuchen und schnell zu identifizieren. Detective sammelt automatisch Protokolldaten von Ihren AWS Ressourcen. Es verwendet dann Machine Learning, statistische Analysen und die Diagrammtheorie, um Visualisierungen zu erstellen, mit denen Sie effektive Sicherheitsuntersuchungen schneller und effizienter durchführen können. Detective bietet vordefinierte Datenaggregationen, Übersichten und Kontexte, mit denen Sie Art und Ausmaß möglicher Sicherheitsprobleme schnell analysieren und feststellen können.

Wenn Sie Security Lake und Detective integrieren, können Sie die von Security Lake gespeicherten Rohprotokolldaten von Detective abfragen. Weitere Informationen finden Sie unter [Integration mit Amazon Security Lake](#).

Integration mit Amazon OpenSearch Service

Integrationstyp: Abonnent

[Amazon OpenSearch Service](#) ist ein verwalteter Service, der die Bereitstellung, den Betrieb und die Skalierung von OpenSearch Service-Clustern in der erleichtert AWS Cloud. Wenn Sie OpenSearch Service Ingestion verwenden, um Daten in Ihren OpenSearch Service Service-Cluster aufzunehmen, können Sie schneller Erkenntnisse für zeitkritische Sicherheitsuntersuchungen gewinnen. Sie können schnell auf Sicherheitsvorfälle reagieren und so Ihre geschäftskritischen Daten und Systeme schützen.

OpenSearch Service-Dashboard

Nachdem Sie OpenSearch Service in Security Lake integriert haben, können Sie Security Lake so konfigurieren, dass Sicherheitsdaten aus verschiedenen Quellen über serverlose OpenSearch Service Ingestion an Service OpenSearch Service gesendet werden. Weitere Informationen zur Konfiguration von OpenSearch Service Ingest für die Verarbeitung von Sicherheitsdaten finden Sie unter [Generieren von Sicherheitsinformationen aus Amazon Security Lake-Daten mithilfe von Amazon OpenSearch Service](#) Ingestion.

Nachdem OpenSearch Service Ingestion mit dem Schreiben Ihrer Daten in Ihre Service Service-Domain beginnt. OpenSearch Um die Daten mithilfe der vorgefertigten Dashboards zu visualisieren, navigieren Sie zu den Dashboards und wählen Sie eines der installierten Dashboards aus.

Integration mit Amazon QuickSight

Integrationstyp: Abonnent

[Amazon QuickSight](#) ist ein Business Intelligence (BI) -Service auf Cloud-Ebene, mit dem Sie den Menschen, mit denen Sie zusammenarbeiten, easy-to-understand Erkenntnisse liefern können, egal wo sie sich befinden. Amazon QuickSight stellt eine Verbindung zu Ihren Daten in der Cloud her und kombiniert Daten aus vielen verschiedenen Quellen. Amazon QuickSight bietet Entscheidungsträgern die Möglichkeit, Informationen in einer interaktiven visuellen Umgebung zu erkunden und zu interpretieren. Sie haben von jedem Gerät in Ihrem Netzwerk und von mobilen Geräten aus sicheren Zugriff auf Dashboards.

QuickSight Amazon-Dashboard

Um Ihre Amazon Security Lake-Daten in Amazon zu visualisieren QuickSight, die erforderlichen AWS Objekte zu erstellen und grundlegende Datenquellen, Datensätze, Analysen, Dashboards und Benutzergruppen in QuickSight Bezug auf Security Lake für Amazon bereitzustellen. Eine ausführliche Anleitung finden Sie unter [Integration mit Amazon QuickSight](#).

Integration mit Amazon SageMaker

Integrationstyp: Abonnent

[Amazon SageMaker](#) ist ein vollständig verwalteter Service für maschinelles Lernen (ML). Mit Security Lake können Datenwissenschaftler und Entwickler schnell und zuverlässig ML-Modelle erstellen, trainieren und in einer produktionsbereiten, gehosteten Umgebung einsetzen. Es bietet eine Benutzeroberfläche für die Ausführung von ML-Workflows, sodass SageMaker ML-Tools in mehreren integrierten Entwicklungsumgebungen (IDEs) verfügbar sind.

SageMaker Einblicke

Mit SageMaker Studio können Sie Erkenntnisse zum maschinellen Lernen für Security Lake generieren. SageMaker Studio ist eine webintegrierte Entwicklungsumgebung (IDE) für maschinelles Lernen, die Tools für Datenwissenschaftler zur Vorbereitung, Erstellung, Schulung und Bereitstellung von Modellen für maschinelles Lernen bereitstellt. Mit dieser Lösung können Sie schnell einen Basissatz von Python-Notebooks bereitstellen, der sich auf die AWS Security Hub Ergebnisse in Security Lake konzentriert. Dieser kann auch erweitert werden, um andere AWS Quellen oder benutzerdefinierte Datenquellen in Security Lake zu integrieren. Weitere Informationen finden Sie unter [Generieren von Erkenntnissen zum maschinellen Lernen für Amazon Security Lake-Daten mithilfe von Amazon SageMaker](#).

Integration mit Amazon Bedrock

[Amazon Bedrock](#) ist ein vollständig verwalteter Service, der Ihnen leistungsstarke Foundation-Modelle (FMs) von führenden KI-Startups und Amazon über eine einheitliche API zur Verfügung stellt. Mit der serverlosen Erfahrung von Amazon Bedrock können Sie schnell loslegen, Foundation-Modelle privat mit Ihren eigenen Daten anpassen und sie mithilfe von AWS Tools einfach und sicher in Ihre Anwendungen integrieren und bereitstellen, ohne eine Infrastruktur verwalten zu müssen.

Generative KI

Sie können die generativen KI-Funktionen von Amazon Bedrock und die Eingabe in natürlicher Sprache in SageMaker Studio verwenden, um Daten in Security Lake zu analysieren und darauf hinzuarbeiten, das Risiko Ihres Unternehmens zu reduzieren und Ihre Sicherheitslage zu verbessern. Sie können den Zeitaufwand für die Durchführung einer Untersuchung reduzieren, indem Sie automatisch die entsprechenden Datenquellen identifizieren, SQL-Abfragen generieren und aufrufen und Daten aus Ihrer Untersuchung visualisieren. Weitere Informationen finden Sie unter [Generieren von KI-gestützten Erkenntnissen für Amazon Security Lake mithilfe von Amazon SageMaker Studio und Amazon Bedrock](#).

Integration mit AWS Security Hub

Integrationstyp: Quelle

[AWS Security Hub](#) bietet Ihnen einen umfassenden Überblick über Ihren Sicherheitsstatus AWS und hilft Ihnen dabei, Ihre Umgebung anhand von Industriestandards und Best Practices zu überprüfen. Security Hub sammelt Sicherheitsdaten von Across AWS-Konten, Services und unterstützten Produkten von Drittanbietern und hilft Ihnen dabei, Ihre Sicherheitstrends zu analysieren und die Sicherheitsprobleme mit der höchsten Priorität zu identifizieren.

Wenn Sie Security Hub aktivieren und Security Hub-Ergebnisse als Quelle in Security Lake hinzufügen, beginnt Security Hub, neue Ergebnisse und Aktualisierungen vorhandener Ergebnisse an Security Lake zu senden.

Wie Security Lake die Ergebnisse von Security Hub erhält

Im Security Hub werden Sicherheitsprobleme als Erkenntnisse verfolgt. Einige Ergebnisse stammen aus Problemen, die von anderen AWS Diensten oder von Drittanbietern entdeckt wurden. Security Hub generiert auch seine eigenen Ergebnisse, indem es automatisierte und kontinuierliche Sicherheitsprüfungen anhand von Regeln durchführt. Die Regeln werden durch Sicherheitskontrollen repräsentiert.

Alle Erkenntnisse in Security Hub verwenden ein Standard-JSON-Format, das so genannte [AWS - Security Finding Format \(ASFF\)](#).

Security Lake erhält die Ergebnisse von Security Hub und wandelt sie in die [Offenes Cybersecurity Schema Framework \(OCSF\)](#) um.

Senden Sie Ihre Security Hub Hub-Ergebnisse an Security Lake

Um Security Hub Hub-Ergebnisse an Security Lake zu senden, müssen Sie beide Dienste aktivieren und Security Hub Hub-Ergebnisse als Quelle in Security Lake hinzufügen. Anweisungen zum Hinzufügen einer AWS Quelle finden Sie unter [Eine als Quelle hinzufügen AWS-Service](#).

Wenn Sie möchten, dass Security Hub [Kontrollergebnisse](#) generiert und an Security Lake sendet, müssen Sie die entsprechenden Sicherheitsstandards aktivieren und die Ressourcenaufzeichnung auf regionaler Basis in aktivieren AWS Config. Weitere Informationen finden Sie unter [Aktivierung und Konfiguration AWS Config](#) im AWS Security Hub Benutzerhandbuch.

Beenden Sie den Empfang von Security Hub Hub-Ergebnissen in Security Lake

Um keine Security Hub Hub-Ergebnisse mehr zu erhalten, können Sie die Security Hub Hub-Konsole, die Security Hub Hub-API oder verwenden AWS CLI.

Weitere Informationen finden Sie unter [Deaktivieren und Aktivieren des Ergebnisflusses aus einer Integration \(Konsole\)](#) oder [Deaktivieren des Ergebnisflusses aus einer Integration \(Security Hub Hub-API, AWS-CLI\)](#) im AWS Security Hub Benutzerhandbuch.

Integrationen von Drittanbietern mit Security Lake

Amazon Security Lake lässt sich in mehrere Drittanbieter integrieren. Ein Anbieter kann eine Quellintegration, eine Abonnentenintegration oder eine Serviceintegration anbieten. Anbieter können einen oder mehrere Integrationstypen anbieten.

Quellintegrationen haben die folgenden Eigenschaften:

- Daten an Security Lake senden
- Die Daten kommen im Apache Parquet-Format an
- Daten kommen im [Offenes Cybersecurity Schema Framework \(OCSF\)](#) Schema an

Abonnentenintegrationen haben die folgenden Eigenschaften:

- Lesen Sie Quelldaten aus Security Lake an einem HTTPS-Endpunkt oder einer Amazon Simple Queue Service (Amazon SQS) -Warteschlange oder durch direkte Abfrage von Quelldaten von AWS Lake Formation
- Kann Daten im Apache Parquet-Format lesen

- Kann Daten im OCSF-Schema lesen

Serviceintegrationen können Ihnen bei der Implementierung von Security Lake und anderen Programmen AWS-Services in Ihrem Unternehmen helfen. Sie können auch Unterstützung bei Berichten, Analysen und anderen Anwendungsfällen bieten.

Informationen zur Suche nach einem bestimmten Partneranbieter finden Sie im [Partner Solutions Finder](#). Um ein Drittanbieterprodukt zu erwerben, besuchen Sie den [AWS Marketplace](#).

Um als Partnerintegration hinzugefügt zu werden oder ein Security Lake-Partner zu werden, senden Sie eine E-Mail an <securitylake-partners@amazon.com>.

Wenn Sie Integrationen von Drittanbietern verwenden, die Ergebnisse an senden AWS Security Hub, können Sie diese Ergebnisse auch in Security Lake überprüfen, sofern die Security Hub Hub-Integration für Security Lake aktiviert ist. Anweisungen zur Aktivierung der Integration finden Sie unter [Integration mit AWS Security Hub](#). Eine Liste der Integrationen von Drittanbietern, die Ergebnisse an Security Hub senden, finden Sie im AWS Security Hub Benutzerhandbuch unter [Verfügbare Produktintegrationen von Drittanbietern](#).

Bevor Sie Ihre Abonnenten einrichten, überprüfen Sie, ob Ihr Abonnent das OCSF-Protokoll unterstützt. Die neuesten Informationen finden Sie in der Dokumentation Ihres Abonnenten.

Integration abfragen

Sie können die Daten abfragen, die Security Lake in AWS Lake Formation Datenbanken und Tabellen speichert. Sie können auch Abonnenten von Drittanbietern in der Security Lake-Konsole, API oder erstellen AWS Command Line Interface.

Der Lake Formation Data Lake-Administrator muss der IAM-Identität, die die Daten abfragt, SELECT Berechtigungen für die entsprechenden Datenbanken und Tabellen gewähren. Sie müssen einen Abonnenten in Security Lake erstellen, bevor Sie Daten abfragen können. Weitere Informationen zum Erstellen eines Abonnenten mit Abfragezugriff finden Sie unter [Verwaltung des Abfragezugriffs für Security Lake-Abonnenten](#).

Sie können die Abfrageintegration mit Security Lake für die folgenden Drittanbieter konfigurieren.

- Cribl – Search
- Palo Alto Networks – XSOAR
- IBM – QRadar

- Query.AI – Query Federated Search
- SOC Prime
- Tego Cyber

Accenture – MxDR

Integrationstyp: Abonent, Dienst

Accenture's Die MxDR-Integration mit Security Lake ermöglicht die Erfassung von Protokollen und Ereignissen in Echtzeit, die verwaltete Erkennung von Anomalien, die Suche nach Bedrohungen und Sicherheitsoperationen. Dies unterstützt Analysen und Managed Detection and Response (MDR).

Die Integration als Service Accenture kann Ihnen auch bei der Implementierung von Security Lake in Ihrem Unternehmen helfen.

[Dokumentation zur Integration](#)

Aqua Security

Art der Integration: Quelle

Aqua Security kann als benutzerdefinierte Quelle hinzugefügt werden, um Audit-Ereignisse an Security Lake zu senden. Die Prüfereignisse werden in das OCSF-Schema und das Parquet-Format konvertiert.

[Dokumentation zur Integration](#)

Barracuda – Email Protection

Art der Integration: Quelle

Barracuda Email Protection kann Ereignisse an Security Lake senden, wenn neue Phishing-E-Mail-Angriffe erkannt werden. Sie können diese Ereignisse zusammen mit anderen Sicherheitsdaten in Ihrem Data Lake empfangen.

[Dokumentation zur Integration](#)

Booz Allen Hamilton

Art der Integration: Dienst

Als Serviceintegration Booz Allen Hamilton verwendet es einen datengesteuerten Ansatz zur Cybersicherheit, indem Daten und Analysen mit dem Security Lake-Dienst zusammengeführt werden.

[Link zum Partner](#)

Bosch Software and Digital Solutions – AIShield

Integrationstyp: Quelle

AIShieldpowered by Bosch bietet durch die Integration mit Security Lake automatisierte Schwachstellenanalysen und Endpunktschutz für KI-Assets.

[Dokumentation zur Integration](#)

ChaosSearch

Integrationstyp: Abonnent

ChaosSearchbietet Benutzern mit offenen APIs wie Elasticsearch und SQL oder mit den nativ enthaltenen Kibana- und Superset-Benutzeroberflächen Datenzugriff mit mehreren Modellen. Sie können Ihre Security Lake-Daten ChaosSearch ohne Aufbewahrungsbeschränkungen nutzen, um sie zu überwachen, zu warnen und nach Bedrohungen zu suchen. Dies hilft Ihnen, den komplexen Sicherheitsumgebungen und den anhaltenden Bedrohungen von heute zu begegnen.

[Dokumentation zur Integration](#)

Cisco Security – Secure Firewall

Art der Integration: Quelle

Durch die Integration Cisco Secure Firewall mit Security Lake können Sie Firewall-Protokolle strukturiert und skalierbar speichern. Der EnCore-Client von Cisco streamt Firewall-Protokolle vom Firewall Management Center, führt eine Schemakonvertierung in das OCSF-Schema durch und speichert sie in Security Lake.

[Dokumentation zur Integration](#)

Claroty – xDome

Art der Integration: Quelle

Claroty xDomesendet in Netzwerken erkannte Warnmeldungen mit minimaler Konfiguration an Security Lake. Flexible und schnelle Bereitstellungsoptionen tragen xDome zum Schutz erweiterter Ressourcen des Internet der Dinge (XIoT) — bestehend aus IoT-, IIoT- und BMS-Ressourcen — in Ihrem Netzwerk bei und erkennen gleichzeitig automatisch Frühindikatoren für Bedrohungen.

[Dokumentation zur Integration](#)

CMD Solutions

Art der Integration: Dienst

CMD Solutionshilft Unternehmen, ihre Agilität zu erhöhen, indem sie Sicherheit frühzeitig und kontinuierlich durch Entwurfs-, Automatisierungs- und kontinuierliche Sicherheitsprozesse integrieren. Die Integration als Service CMD Solutions kann Ihnen bei der Implementierung von Security Lake in Ihrem Unternehmen helfen.

[Link zum Partner](#)

Confluent – Amazon S3 Sink Connector

Integrationstyp: Quelle

Confluentverbindet, konfiguriert und orchestriert automatisch Datenintegrationen mit vollständig verwalteten, vorgefertigten Konnektoren. Auf diese Confluent S3 Sink Connector Weise können Sie Rohdaten in großem Umfang im nativen Parkett-Format in Security Lake speichern.

[Dokumentation zur Integration](#)

Contrast Security

Art der Integration: Quelle

Partnerprodukt für die Integration: Contrast Assess

Contrast Security Assessist ein IAST-Tool, das die Erkennung von Sicherheitslücken in Web-Apps, APIs und Microservices in Echtzeit ermöglicht. Assess lässt sich in Security Lake integrieren und bietet so einen zentralen Überblick über all Ihre Workloads.

[Dokumentation zur Integration](#)

Cribl – Search

Integrationstyp: Abonntent

Sie können es verwenden Cribl Search, um nach Security Lake-Daten zu suchen.

[Dokumentation zur Integration](#)

Cribl – Stream

Art der Integration: Quelle

Sie können Cribl Stream es verwenden, um Daten aus allen Cribl unterstützten Drittanbieterquellen im OCSF-Schema an Security Lake zu senden.

[Dokumentation zur Integration](#)

CrowdStrike – Falcon Data Replicator

Art der Integration: Quelle

Diese Integration ruft Daten CrowdStrike Falcon Data Replicator auf kontinuierlicher Streaming-Basis ab, wandelt die Daten in ein OCSF-Schema um und sendet sie an Security Lake.

[Dokumentation zur Integration](#)

CyberArk – Unified Identify Security Platform

Art der Integration: Quelle

CyberArk Audit Adapter, eine AWS Lambda Funktion, sammelt Sicherheitsereignisse von Security Lake CyberArk Identity Security Platform und sendet die Daten im OCSF-Schema an Security Lake.

[Dokumentation zur Integration](#)

Cyber Security Cloud – Cloud Fastener

Integrationstyp: Abonntent

CloudFastener nutzt Security Lake, um die Konsolidierung von Sicherheitsdaten aus Ihren Cloud-Umgebungen zu vereinfachen.

[Dokumentation zur Integration](#)

DataBahn

Art der Integration: Quelle

Zentralisieren Sie Ihre Sicherheitsdaten in Security Lake mithilfe von DataBahn's Security Data Fabric.

[Integrationsdokumentation \(melden Sie sich im DataBahn Portal an, um die Dokumentation zu lesen\)](#)

Darktrace – Cyber AI Loop

Integrationstyp: Quelle

Die Darktrace Integration mit Security Lake erweitert Security Lake um das Potenzial des Darktrace Selbstlernens. Erkenntnisse aus Cyber AI Loop können mit anderen Datenströmen und Elementen des Sicherheitsstapels Ihres Unternehmens korreliert werden. Die Integration protokolliert Darktrace Modellverletzungen als Sicherheitserkenntnisse.

[Integrationsdokumentation \(melden Sie sich im Darktrace Portal an, um die Dokumentation zu lesen\)](#)

Datadog

Integrationstyp: Abonnent

Datadog Cloud SIEMerkennt Bedrohungen für Ihre Cloud-Umgebung in Echtzeit, einschließlich Daten in Security Lake, DevOps und vereint Sicherheitsteams auf einer Plattform.

[Dokumentation zur Integration](#)

Deloitte – MXDR Cyber Analytics and AI Engine (CAE)

Integrationstyp: Abonnent, Dienst

Deloitte MXDR CAEhilft Ihnen dabei, Ihre standardisierten Sicherheitsdaten schnell zu speichern, zu analysieren und zu visualisieren. Die CAE-Suite mit maßgeschneiderten Analyse-, KI- und ML-Funktionen liefert automatisch umsetzbare Erkenntnisse auf der Grundlage von Modellen, die auf den OCSF-formatierten Daten in Security Lake basieren.

Die Integration als Service Deloitte kann Ihnen auch bei der Implementierung von Security Lake in Ihrem Unternehmen helfen.

[Dokumentation zur Integration](#)

Devo

Integrationstyp: Abonnent

Der Devo Collector für AWS unterstützt die Aufnahme aus Security Lake. Diese Integration kann Ihnen helfen, eine Vielzahl von Sicherheitsanwendungsfällen zu analysieren und zu behandeln, z. B. bei der Erkennung von Bedrohungen, der Untersuchung und der Reaktion auf Vorfälle.

[Dokumentation zur Integration](#)

DXC – SecMon

Integrationstyp: Abonnent, Dienst

DXC SecMonsammelt Sicherheitsereignisse aus Security Lake und überwacht sie, um potenzielle Sicherheitsbedrohungen zu erkennen und davor zu warnen. Dies hilft Unternehmen dabei, ihre Sicherheitslage besser zu verstehen und Bedrohungen proaktiv zu erkennen und darauf zu reagieren.

Die Integration als Service DXC kann Ihnen auch bei der Implementierung von Security Lake in Ihrem Unternehmen helfen.

[Dokumentation zur Integration](#)

Eviden— Alsaac (früherAtos)

Art der Integration: Abonnent

Die Alsaac MDR Plattform verwendet VPC Flow Logs, die in das OCSF-Schema in Security Lake aufgenommen wurden, und verwendet KI-Modelle zur Erkennung von Bedrohungen.

[Dokumentation zur Integration](#)

ExtraHop – Reveal(x) 360

Art der Integration: Quelle

Sie können Ihre Workload- und Anwendungssicherheit verbessern, indem Sie Netzwerkdaten, einschließlich der Erkennung von IOCs, vonExtraHop Reveal(x) 360, bis Security Lake in das OCSF-Schema integrieren

[Dokumentation zur Integration](#)

Falcosidekick

Art der Integration: Quelle

Falcosidekick sammelt Falco-Ereignisse und sendet sie an Security Lake. Diese Integration exportiert Sicherheitsereignisse mithilfe des OCSF-Schemas.

[Dokumentation zur Integration](#)

Fortinet - Cloud Native Firewall

Art der Integration: Quelle

Wenn Sie FortiGate CNF-Instances in erstellen AWS, können Sie Amazon Security Lake als Ziel für die Protokollausgabe angeben.

[Dokumentation zur Integration](#)

Gigamon – Application Metadata Intelligence

Art der Integration: Quelle

Gigamon Application Metadata Intelligence (AMI) stattet Ihre Tools für Observability, SIEM und Netzwerkleistungsüberwachung mit wichtigen Metadatenattributen aus. Dies trägt zu einer besseren Transparenz der Anwendungen bei, sodass Sie Leistungsengpässe, Qualitätsprobleme und potenzielle Netzwerksicherheitsrisiken erkennen können.

[Dokumentation zur Integration](#)

Hoop Cyber

Art der Integration: Dienst

Hoop Cyber FastStart umfasst eine Datenquellenbewertung, Priorisierung und Integration von Datenquellen und unterstützt Kunden bei der Abfrage ihrer Daten mit den vorhandenen Tools und Integrationen, die über Security Lake angeboten werden.

[Link zum Partner](#)

IBM – QRadar

Integrationstyp: Abonnent

IBM Security QRadar SIEM with UAXintegriert Security Lake mit einer Analyseplattform, die Bedrohungen in Hybrid-Clouds identifiziert und verhindert. Diese Integration unterstützt sowohl den Datenzugriff als auch den Abfragezugriff.

[Integrationsdokumentation zur Nutzung von AWS CloudTrail Protokollen](#)

[Integrationsdokumentation zur Verwendung von Amazon Athena für Abfragen](#)

Infosys

Art der Integration: Service

Infosys hilft Ihnen dabei, Ihre Security Lake-Implementierung an Ihre Unternehmensanforderungen anzupassen, und bietet maßgeschneiderte Einblicke.

[Link zum Partner](#)

Insbuilt

Art der Integration: Service

Insbuilt ist auf Cloud-Beratungsdienste spezialisiert und kann Ihnen helfen, zu verstehen, wie Sie Security Lake in Ihrem Unternehmen implementieren können.

[Link zum Partner](#)

Kyndryl – AIOps

Integrationstyp: Abonnent, Dienst

Kyndryl lässt sich in Security Lake integrieren, um die Interoperabilität von Cyberdaten, Bedrohungsinformationen und KI-gestützten Analysen zu gewährleisten. Als Abonnent für Datenzugriff nimmt er AWS CloudTrail Verwaltungsereignisse von Security Lake zu Analyse Zwecken auf.

Die Integration als Service Kyndryl kann Ihnen auch bei der Implementierung von Security Lake in Ihrem Unternehmen helfen.

[Dokumentation zur Integration](#)

Lacework – Polygraph

Art der Integration: Quelle

Lacework Polygraph® Data Platform lässt sich in Security Lake als Datenquelle integrieren und bietet Sicherheitsinformationen zu Sicherheitslücken, Fehlkonfigurationen sowie bekannten und unbekanntem Bedrohungen in Ihrer AWS Umgebung.

[Dokumentation zur Integration](#)

Laminar

Art der Integration: Quelle

Laminar sendet Datensicherheitsereignisse im OCSF-Schema an Security Lake und stellt sie so für zusätzliche Analyse-Anwendungsfälle zur Verfügung, z. B. für die Reaktion auf Vorfälle und Untersuchungen.

[Dokumentation zur Integration](#)

MegazoneCloud

Art der Integration: Dienst

MegazoneCloud ist auf Cloud-Beratungsdienste spezialisiert und kann Ihnen helfen, zu verstehen, wie Sie Security Lake in Ihrem Unternehmen implementieren können. Wir verbinden Security Lake mit integrierten ISV-Lösungen, um maßgeschneiderte Aufgaben zu erstellen und maßgeschneiderte Einblicke in Bezug auf Kundenbedürfnisse zu gewinnen.

[Dokumentation zur Integration](#)

Monad

Art der Integration: Quelle

Monad wandelt Ihre Daten automatisch in das OCSF-Schema um und sendet sie an Ihren Security Lake Data Lake.

[Dokumentation zur Integration](#)

NETSCOUT – Omnis Cyber Intelligence

Art der Integration: Quelle

Durch die Integration mit Security Lake NETSCOUT wird es zu einer maßgeschneiderten Quelle für Sicherheitserkenntnisse und detaillierte Sicherheitseinblicke in das Geschehen in Ihrem Unternehmen, wie z. B. Cyberbedrohungen, Sicherheitsrisiken und Veränderungen der Angriffsoberfläche. Diese Ergebnisse werden von NETSCOUT CyberStreams und im Kundenkonto generiert und Omnis Cyber Intelligence dann im OCSF-Schema an Security Lake gesendet. Die aufgenommenen Daten erfüllen auch andere Anforderungen und bewährte Verfahren für eine Security Lake-Quelle, einschließlich Format, Schema, Partitionierung und leistungsbezogener Aspekte.

[Dokumentation zur Integration](#)

Netskope – CloudExchange

Art der Integration: Quelle

Netskope hilft Ihnen dabei, Ihre Sicherheitslage zu stärken, indem sicherheitsrelevante Protokolle und Bedrohungsinformationen mit Security Lake geteilt werden. Netskope Die Ergebnisse werden mit einem CloudExchange Plugin an Security Lake gesendet, das als Docker-basierte Umgebung innerhalb AWS oder in einem lokalen Rechenzentrum gestartet werden kann.

[Dokumentation zur Integration](#)

New Relic ONE

Integrationstyp: Abonnent

New Relic ONE ist eine Lambda-basierte Abonnementanwendung. Es wird in Ihrem Konto bereitgestellt, von Amazon SQS ausgelöst und sendet Daten New Relic mithilfe von New Relic Lizenzschlüsseln

[Dokumentation zur Integration](#)

Okta – Workforce Identity Cloud

Art der Integration: Quelle

Oktasendet Identitätsprotokolle im OCSF-Schema über eine EventBridge Amazon-Integration an Security Lake. Okta System LogsDas OCSF-Schema hilft Sicherheits- und Datenwissenschaftlerteams dabei, Sicherheitsereignisse anhand eines Open-Source-Standards abzufragen. Durch die Generierung standardisierter OCSF-Protokolle von Okta können Sie Auditaktivitäten durchführen und Berichte zu Authentifizierung, Autorisierung, Kontoänderungen und Entitätsänderungen anhand eines konsistenten Schemas erstellen.

[Dokumentation zur Integration](#)

[AWS CloudFormation Vorlage zum Hinzufügen Okta als benutzerdefinierte Quelle in Security Lake](#)

Orca – Cloud Security Platform

Integrationstyp: Quelle

Die Orca agentenlose Cloud-Sicherheitsplattform lässt sich in Security Lake AWS integrieren, indem sie Cloud Detection and Response (CDR) -Ereignisse im OCSF-Schema sendet.

[Integrationsdokumentation \(melden Sie sich im Orca Portal an, um die Dokumentation zu lesen\)](#)

Palo Alto Networks – Prisma Cloud

Integrationstyp: Quelle

Palo Alto Networks Prisma Cloudaggregiert Daten zur Schwachstellenerkennung auf allen VMs in Ihren cloudnativen Umgebungen und sendet sie an Security Lake.

[Dokumentation zur Integration](#)

Palo Alto Networks – XSOAR

Art der Integration: Abonnent

Palo Alto Networks XSOARhat eine Abonnentenintegration mit XSOAR und Security Lake entwickelt.

[Dokumentation zur Integration](#)

Panther

Integrationstyp: Abonnent

Pantherunterstützt die Erfassung von Security Lake-Protokollen zur Verwendung bei der Suche und Erkennung.

[Dokumentation zur Integration](#)

Ping Identity – PingOne

Art der Integration: Quelle

PingOnesendet Benachrichtigungen über Kontoänderungen im OCSF-Schema und im Parquet-Format an Security Lake, sodass Sie Kontoänderungen erkennen und darauf reagieren können.

[Dokumentation zur Integration](#)

PwC – Fusion center

Integrationstyp: Abonnent, Dienst

PwC bietet Wissen und Expertise, um Kunden bei der Implementierung eines Fusion Centers zu unterstützen, das ihren individuellen Bedürfnissen entspricht. Ein auf Amazon Security Lake aufgebautes Fusion Center bietet die Möglichkeit, Daten aus einer Vielzahl von Quellen zu kombinieren, um eine zentralisierte Ansicht nahezu in Echtzeit zu erstellen.

[Dokumentation zur Integration](#)

Query.AI – Query Federated Search

Integrationstyp: Abonnent

Query Federated Searchkann jede Security Lake-Tabelle direkt über Amazon Athena abfragen, um die Reaktion auf Vorfälle, Untersuchungen, die Bedrohungssuche und die allgemeine Suche über eine Vielzahl von Observables, Ereignissen und Objekten im OCSF-Schema zu unterstützen.

[Dokumentation zur Integration](#)

Rapid7 – InsightIDR

Integrationstyp: Abonnent

InsightIDR, die Rapid7 SIEM/XDR-Lösung, kann Protokolle in Security Lake aufnehmen, um Bedrohungen zu erkennen und verdächtige Aktivitäten zu untersuchen.

[Dokumentation zur Integration](#)

RipJar – Labyrinth for Threat Investigations

Integrationstyp: Abonnent

Labyrinth for Threat Investigations bietet einen unternehmensweiten Ansatz für die Erkundung von Bedrohungen in großem Maßstab auf der Grundlage von Datenfusion mit detaillierter Sicherheit, anpassbaren Workflows und Berichten.

[Dokumentation zur Integration](#)

Sailpoint

Art der Integration: Quelle

Partnerprodukt für die Integration: SailPoint IdentityNow

Diese Integration ermöglicht es Kunden, Ereignisdaten aus zu transformierenSailPoint IdentityNow. Die Integration soll einen automatisierten Prozess zur Übertragung von IdentityNow Benutzeraktivitäten und Governance-Ereignissen in Security Lake ermöglichen, um so die Erkenntnisse aus Produkten zur Überwachung von Sicherheitsvorfällen und Ereignissen zu verbessern.

[Dokumentation zur Integration](#)

Securonix

Integrationstyp: Abonnent

Securonix Next-Gen SIEM lässt sich in Security Lake integrieren, sodass Sicherheitsteams Daten schneller aufnehmen und ihre Erkennungs- und Reaktionsmöglichkeiten erweitern können.

[Dokumentation zur Integration](#)

SentinelOne

Integrationstyp: Abonnent

Die SentinelOne Singularity™ XDR Plattform erweitert die Erkennung und Reaktion in Echtzeit auf Endpunkt-, Identitäts- und Cloud-Workloads, die auf lokalen und öffentlichen Cloud-Infrastrukturen

ausgeführt werden, darunter Amazon Elastic Compute Cloud (Amazon EC2), Amazon Elastic Container Service (Amazon ECS) und Amazon Elastic Kubernetes Service (Amazon EKS).

[Integrationsdokumentation \(melden Sie sich im SentinelOne Portal an, um die Dokumentation zu lesen\)](#)

Sentra – Data Lifecycle Security Platform

Integrationstyp: Quelle

Ruft nach der Bereitstellung der Sentra Scan-Infrastruktur in Ihrem Konto die Sentra Ergebnisse ab und nimmt sie in Ihr SaaS auf. Bei diesen Ergebnissen handelt es sich um Metadaten, die Sentra gespeichert und später zur Abfrage im OCSF-Schema an Security Lake gestreamt werden.

[Dokumentation zur Integration](#)

SOC Prime

Integrationstyp: Abonnent

SOC Prime lässt sich über Amazon OpenSearch Service und Amazon Athena in Security Lake integrieren, um intelligente Datenorchestrierung und Bedrohungssuche auf der Grundlage von Zero-Trust-Meilensteinen zu erleichtern. SOC Prime ermöglicht Sicherheitsteams, die Sichtbarkeit von Bedrohungen zu erhöhen und Vorfälle zu untersuchen, ohne dass eine überwältigende Menge an Warnmeldungen erforderlich ist. Mit wiederverwendbaren Regeln und Abfragen, die im OCSF-Schema automatisch in Athena und OpenSearch Service konvertiert werden können, können Sie Entwicklungszeit sparen.

[Dokumentation zur Integration](#)

Splunk

Integrationstyp: Abonnent

Das Splunk AWS Add-On für Amazon Web Services (AWS) unterstützt die Aufnahme aus Security Lake. Diese Integration hilft Ihnen, die Erkennung, Untersuchung und Reaktion von Bedrohungen zu beschleunigen, indem Sie Daten im OCSF-Schema von Security Lake abonnieren.

[Dokumentation zur Integration](#)

Stellar Cyber

Integrationstyp: Abonnent

Stellar Cyber verwendet Protokolle von Security Lake und fügt die Datensätze dem Stellar Cyber Data Lake hinzu. Dieser Connector verwendet das OCSF-Schema.

[Dokumentation zur Integration](#)

Sumo Logic

Integrationstyp: Abonnent

Sumo Logic nutzt Daten aus Security Lake und bietet umfassende Transparenz in AWS lokalen und Hybrid-Cloud-Umgebungen. Sumo Logic bietet Sicherheitsteams umfassende Transparenz, Automatisierung und Bedrohungsüberwachung für all ihre Sicherheitstools.

[Dokumentation zur Integration](#)

Swimlane – Turbine

Integrationstyp: Abonnent

Swimlane nimmt Daten aus Security Lake in das OCSF-Schema auf und sendet die Daten über Low-Code-Playbooks und Fallmanagement, um eine schnellere Erkennung, Untersuchung und Reaktion auf Vorfälle zu ermöglichen.

[Integrationsdokumentation \(melden Sie sich im Swimlane Portal an, um die Dokumentation zu lesen\)](#)

Sysdig Secure

Integrationstyp: Quelle

Sysdig Secure's Die Cloud-native Application Protection Platform (CNAPP) sendet Sicherheitsereignisse an Security Lake, um den Überblick zu maximieren, die Ermittlungen zu optimieren und die Einhaltung von Vorschriften zu vereinfachen.

[Dokumentation zur Integration](#)

Talon

Art der Integration: Quelle

Partnerprodukt für die Integration: Talon Enterprise Browser

Talon's Enterprise Browser, eine sichere und isolierte browserbasierte Endpunktumgebung, sendet Talon Zugriffs-, Datenschutz-, SaaS-Aktionen und Sicherheitsereignisse an Security Lake und bietet so Transparenz und Optionen zur Korrelation von Ereignissen für Erkennung, Forensik und Ermittlungen.

[Integrationsdokumentation \(melden Sie sich im Talon Portal an, um die Dokumentation zu lesen\)](#)

Tanium

Integrationstyp: Quelle

Tanium Unified Cloud Endpoint Detection, Management, and SecurityDie Plattform stellt Security Lake Inventardaten im OCSF-Schema zur Verfügung.

[Dokumentation zur Integration](#)

TCS

Art der Integration: Dienst

Das TCS AWS Business Unit bietet Innovation, Erfahrung und Talent. Diese Integration basiert auf einem Jahrzehnt gemeinsamer Wertschöpfung, fundiertem Branchenwissen, technologischer Expertise und umfassender Erfahrung in der Umsetzung. Die Integration als Service TCS kann Ihnen bei der Implementierung von Security Lake in Ihrem Unternehmen helfen.

[Dokumentation zur Integration](#)

Tego Cyber

Integrationstyp: Abonnent

Tego Cyberlässt sich in Security Lake integrieren, sodass Sie potenzielle Sicherheitsbedrohungen schnell erkennen und untersuchen können. Durch die Korrelation verschiedener Bedrohungsindikatoren über umfangreiche Zeiträume und Protokollquellen hinweg deckt Tego Cyber versteckte Bedrohungen auf. Die Plattform ist mit stark kontextbezogenen Bedrohungsinformationen angereichert, die Präzision und Einblicke in die Erkennung und Untersuchung von Bedrohungen bieten.

[Dokumentation zur Integration](#)

Tines – No-code security automation

Integrationstyp: Abonnent

Tines No-code security automation hilft Ihnen, genauere Entscheidungen zu treffen, indem es Sicherheitsdaten nutzt, die in Security Lake zentralisiert sind.

[Dokumentation zur Integration](#)

Torq – Enterprise Security Automation Platform

Integrationstyp: Quelle, Abonnent

Torq lässt sich sowohl als benutzerdefinierte Quelle als auch als Abonnent nahtlos in Security Lake integrieren. Torq hilft Ihnen bei der Implementierung von Automatisierung und Orchestrierung auf Unternehmensebene mit einer einfachen No-Code-Plattform.

[Dokumentation zur Integration](#)

Trellix – XDR

Integrationstyp: Quelle, Abonnent

Trellix XDR unterstützt als offene XDR-Plattform die Security Lake-Integration. Trellix XDR kann Daten im OCSF-Schema für Anwendungsfälle im Bereich Sicherheitsanalysen nutzen. Sie können Ihren Security Lake-Data Lake auch um mehr als 1.000 Quellen für Sicherheitsereignisse erweitern. Trellix XDR Auf diese Weise können Sie die Erkennungs- und Reaktionsmöglichkeiten für Ihre AWS Umgebung erweitern. Die aufgenommenen Daten werden mit anderen Sicherheitsrisiken korreliert, sodass Sie über die notwendigen Spielregeln verfügen, um rechtzeitig auf ein Risiko reagieren zu können.

[Dokumentation zur Integration](#)

Trend Micro – CloudOne

Art der Integration: Quelle

Trend Micro CloudOne Workload Security sendet die folgenden Informationen von Ihren Amazon Elastic Compute Cloud (EC2) -Instances an Security Lake:

- Aktivität der DNS-Abfrage
- Dateiaktivität
- Netzwerkaktivität
- Aktivität verarbeiten
- Aktivität „Registry Value“
- Aktivität des Benutzerkontos

[Dokumentation zur Integration](#)

Uptycs – Uptycs XDR

Art der Integration: Quelle

Uptycssendet eine Fülle von Daten im OCSF-Schema von lokalen und Cloud-Ressourcen an Security Lake. Zu den Daten gehören die Erkennung verhaltensbedingter Bedrohungen von Endpunkten und Cloud-Workloads, die Erkennung von Anomalien, Richtlinienverstöße, riskante Richtlinien, Fehlkonfigurationen und Sicherheitslücken.

[Dokumentation zur Integration](#)

Vectra AI – Vectra Detect for AWS

Art der Integration: Quelle

Mithilfe dieser Vectra Detect for AWS Option können Sie mithilfe einer speziellen AWS CloudFormation Vorlage hochwertige Warnmeldungen als benutzerdefinierte Quelle an Security Lake senden.

[Dokumentation zur Integration](#)

VMware Aria Automation for Secure Clouds

Art der Integration: Quelle

Mit dieser Integration können Sie Cloud-Fehlkonfigurationen erkennen und sie zur erweiterten Analyse an Security Lake senden.

[Dokumentation zur Integration](#)

Wazuh

Integrationstyp: Abonnent

Wazuh zielt darauf ab, Benutzerdaten sicher zu handhaben, Abfragezugriff für jede Quelle bereitzustellen und die Abfragekosten zu optimieren.

[Dokumentation zur Integration](#)

Wipro

Integrationstyp: Quelle, Dienst

Diese Integration ermöglicht es Ihnen, Daten von der Wipro Cloud Application Risk Governance (CARG) Plattform zu sammeln, um einen einheitlichen Überblick über Ihre Cloud-Anwendungen und den Compliance-Status im gesamten Unternehmen zu erhalten.

Die Integration als Service Wipro kann Ihnen auch bei der Implementierung von Security Lake in Ihrem Unternehmen helfen.

[Dokumentation zur Integration](#)

Wiz – CNAPP

Art der Integration: Quelle

Die Integration zwischen Wiz und Security Lake erleichtert die Erfassung von Cloud-Sicherheitsdaten in einem einzigen Sicherheitsdatensee, indem das OCSF-Schema genutzt wird, ein Open-Source-Standard, der für den erweiterbaren und normalisierten Austausch von Sicherheitsdaten entwickelt wurde.

[Integrationsdokumentation \(melden Sie sich im Wiz Portal an, um die Dokumentation zu lesen\)](#)

Zscaler – Zscaler Posture Control

Integrationstyp: Quelle

Zscaler Posture Control™, eine Cloud-native Anwendungsschutzplattform, sendet Sicherheitsergebnisse im OCSF-Schema an Security Lake.

[Dokumentation zur Integration](#)

Sicherheit in Amazon Security Lake

Die Sicherheit in der Cloud hat bei AWS höchste Priorität. Als AWS-Kunde profitieren Sie von Rechenzentren und Netzwerkarchitekturen, die eingerichtet wurden, um die Anforderungen der anspruchsvollsten Organisationen in puncto Sicherheit zu erfüllen.

Sicherheit ist eine übergreifende Verantwortlichkeit zwischen AWS und Ihnen. Das [Modell der geteilten Verantwortung](#) beschreibt dies als Sicherheit der Cloud selbst und als Sicherheit in der Cloud:

- Sicherheit der Cloud – AWS ist dafür verantwortlich, die Infrastruktur zu schützen, mit der AWS-Services in der AWS Cloud ausgeführt werden. AWS stellt Ihnen außerdem Services bereit, die Sie sicher nutzen können. Auditoren von Drittanbietern testen und überprüfen die Effektivität unserer Sicherheitsmaßnahmen im Rahmen der [AWS-Compliance-Programme](#) regelmäßig. Informationen zu den Compliance-Programmen, die für Amazon Security Lake gelten, finden Sie unter [AWSServices in Scope by Compliance Program AWS](#).
- Sicherheit in der Cloud – Ihr Verantwortungsumfang wird durch den AWS-Service bestimmt, den Sie verwenden. Sie sind auch für andere Faktoren verantwortlich, etwa für die Vertraulichkeit Ihrer Daten, für die Anforderungen Ihres Unternehmens und für die geltenden Gesetze und Vorschriften.

Diese Dokumentation hilft Ihnen zu verstehen, wie Sie das Modell der geteilten Verantwortung bei der Verwendung von Security Lake anwenden können. Die folgenden Themen zeigen Ihnen, wie Sie Security Lake konfigurieren, um Ihre Sicherheits- und Compliance-Ziele zu erreichen. Sie lernen auch, wie Sie andere AWS Dienste nutzen können, die Ihnen helfen, Ihre Security Lake-Ressourcen zu überwachen und zu sichern.

Themen

- [Identitäts- und Zugriffsmanagement für Amazon Security Lake](#)
- [Datenschutz in Amazon Security Lake](#)
- [Konformitätsprüfung für Amazon Security Lake](#)
- [Bewährte Sicherheitsmethoden für Security Lake](#)
- [Resilienz im Amazon Security Lake](#)
- [Infrastruktursicherheit in Amazon Security Lake](#)
- [Konfigurations- und Schwachstellenanalyse in Security Lake](#)

- [Überwachen Sie](#)

Identitäts- und Zugriffsmanagement für Amazon Security Lake

AWS Identity and Access Management (IAM) hilft einem Administrator AWS-Service , den Zugriff auf Ressourcen sicher zu AWS kontrollieren. IAM-Administratoren kontrollieren, wer authentifiziert (angemeldet) und autorisiert werden kann (über Berechtigungen verfügt), um Security Lake-Ressourcen zu verwenden. IAM ist ein Programm AWS-Service , das Sie ohne zusätzliche Kosten nutzen können.

Themen

- [Zielgruppe](#)
- [Authentifizierung mit Identitäten](#)
- [Verwalten des Zugriffs mit Richtlinien](#)
- [So funktioniert Amazon Security Lake mit IAM](#)
- [Beispiele für identitätsbasierte Richtlinien für Amazon Security Lake](#)
- [AWS verwaltete Richtlinien für Amazon Security Lake](#)
- [Servicebezogene Rolle für Amazon Security Lake](#)

Zielgruppe

Wie Sie AWS Identity and Access Management (IAM) verwenden, hängt von der Arbeit ab, die Sie in Security Lake ausführen.

Dienstbenutzer — Wenn Sie den Security Lake-Dienst für Ihre Arbeit verwenden, stellt Ihnen Ihr Administrator die Anmeldeinformationen und Berechtigungen zur Verfügung, die Sie benötigen. Wenn Sie für Ihre Arbeit mehr Security Lake-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 auf eine Funktion in Security Lake nicht zugreifen können, finden Sie weitere Informationen unter [Fehlerbehebung bei Identität und Zugriff auf Amazon Security Lake](#).

Serviceadministrator — Wenn Sie in Ihrem Unternehmen für die Security Lake-Ressourcen verantwortlich sind, haben Sie wahrscheinlich vollen Zugriff auf Security Lake. Es ist Ihre Aufgabe, zu bestimmen, auf welche Funktionen und Ressourcen von Security Lake 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 mit Security Lake nutzen kann, finden Sie unter [So funktioniert Amazon Security Lake mit IAM](#).

IAM-Administrator — Wenn Sie ein IAM-Administrator sind, möchten Sie vielleicht mehr darüber erfahren, wie Sie Richtlinien schreiben können, um den Zugriff auf Security Lake zu verwalten. Beispiele für identitätsbasierte Security Lake-Richtlinien, die Sie in IAM verwenden können, finden Sie unter [Beispiele für identitätsbasierte Richtlinien für Amazon Security Lake](#)

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 zugreifen, AWS stellt es ein Software Development Kit (SDK) und eine Befehlszeilenschnittstelle (CLI) bereit, um Ihre Anfragen mithilfe Ihrer Anmeldeinformationen kryptografisch zu signieren. 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 zum Unterschied zwischen Rollen und ressourcenbasierten Richtlinien für den kontoübergreifenden Zugriff finden Sie unter [Kontoübergreifender Ressourcenzugriff in IAM im IAM-Benutzerhandbuch](#).
- **Serviceübergreifender Zugriff** — Einige verwenden Funktionen in anderen. AWS-Services 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, kombiniert 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) in festlegen. AWS Organizations AWS Organizations ist ein Dienst zur Gruppierung und zentralen Verwaltung mehrerer Objekte 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](#).

So funktioniert Amazon Security Lake mit IAM

Bevor Sie IAM verwenden, um den Zugriff auf Security Lake zu verwalten, sollten Sie sich darüber informieren, welche IAM-Funktionen für die Verwendung mit Security Lake verfügbar sind.

IAM-Funktionen, die Sie mit Amazon Security Lake verwenden können

IAM-Feature	Security Lake-Unterstützung
Identitätsbasierte Richtlinien	Ja
Ressourcenbasierte Richtlinien	Ja
Richtlinienaktionen	Ja
Richtlinienressourcen	Ja
Bedingungsschlüssel für die Richtlinie	Ja
ACLs	Nein
ABAC (Tags in Richtlinien)	Ja
Temporäre Anmeldeinformationen	Ja
Hauptberechtigungen	Ja
Servicerollen	Nein
Serviceverknüpfte Rollen	Ja

Einen allgemeinen Überblick darüber, wie Security Lake 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 Security Lake

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.

Security Lake unterstützt identitätsbasierte Richtlinien. Weitere Informationen finden Sie unter [Beispiele für identitätsbasierte Richtlinien für Amazon Security Lake](#).

Ressourcenbasierte Richtlinien innerhalb von Security Lake

Unterstützt ressourcenbasierte Richtlinien Ja

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 Prinzipalidentität (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 [Kontenübergreifender Ressourcenzugriff in IAM](#) im IAM-Benutzerhandbuch.

Der Security Lake-Service erstellt ressourcenbasierte Richtlinien für die Amazon S3 S3-Buckets, in denen Ihre Daten gespeichert werden. Sie fügen diese ressourcenbasierten Richtlinien nicht Ihren S3-Buckets hinzu. Security Lake erstellt diese Richtlinien automatisch in Ihrem Namen.

Eine Beispielressource ist ein S3-Bucket mit dem Amazon-Ressourcennamen (ARN) `vonarn:aws:s3:::aws-security-data-lake-{region}-{bucket-identifizier}`. In diesem Beispiel `region` handelt es sich um eine spezifische AWS-Region Zeichenfolge, für die Sie Security Lake aktiviert haben, und um `bucket-identifizier` eine regional eindeutige alphanumerische Zeichenfolge, die Security Lake dem Bucket zuweist. Security Lake erstellt den S3-Bucket, um Daten aus dieser Region zu speichern. Die Ressourcenrichtlinie definiert, welche Principals Aktionen auf dem Bucket ausführen können. Hier ist ein Beispiel für eine ressourcenbasierte Richtlinie (Bucket-Richtlinie), die Security Lake an den Bucket anhängt:

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Deny",
      "Principal": {
        "AWS": "*"
      },
      "Action": "s3:*",
      "Resource": [
        "arn:aws:s3:::aws-security-data-lake-{region}-{bucket-identifizier}/*",
        "arn:aws:s3:::aws-security-data-lake-{region}-{bucket-identifizier}"
      ],
      "Condition": {
        "Bool": {
          "aws:SecureTransport": "false"
        }
      }
    },
  ],
}
```

```
"Sid": "PutSecurityLakeObject",
"Effect": "Allow",
"Principal": {
  "Service": "securitylake.amazonaws.com"
},
"Action": "s3:PutObject",
"Resource": [
  "arn:aws:s3::aws-security-data-lake-{region}-{bucket-identifier}/*",
  "arn:aws:s3::aws-security-data-lake-{region}-{bucket-identifier}"
],
"Condition": {
  "StringEquals": {
    "aws:SourceAccount": "{DA-AccountID}",
    "s3:x-amz-acl": "bucket-owner-full-control"
  },
  "ArnLike": {
    "aws:SourceArn": "arn:aws:securitylake:us-east-1:{DA-AccountID}:*"
  }
}
}
```

Weitere Informationen zu ressourcenbasierten Richtlinien finden Sie unter [Identitätsbasierte Richtlinien und ressourcenbasierte Richtlinien](#) im IAM-Benutzerhandbuch.

Richtlinienaktionen für Security Lake

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 keinen passenden API-Vorgang 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 Security Lake-Aktionen finden Sie unter [Von Amazon Security Lake definierte Aktionen](#) in der Service Authorization Reference.

Richtlinienaktionen in Security Lake verwenden vor der Aktion das folgende Präfix:

```
securitylake
```

Um einem Benutzer beispielsweise die Erlaubnis zu erteilen, auf Informationen über einen bestimmten Abonnenten zuzugreifen, nehmen Sie die `securitylake:GetSubscriber` Aktion in die diesem Benutzer zugewiesene Richtlinie auf. Richtlinienanweisungen müssen entweder ein `Action` oder ein `NotAction`-Element enthalten. Security Lake definiert eigene Aktionen, die Aufgaben beschreiben, die Sie mit diesem Dienst ausführen können.

Um mehrere Aktionen in einer einzigen Anweisung anzugeben, trennen Sie sie mit Kommata:

```
"Action": [  
  "securitylake:action1",  
  "securitylake:action2"  
]
```

Beispiele für identitätsbasierte Security Lake-Richtlinien finden Sie unter [Beispiele für identitätsbasierte Richtlinien für Amazon Security Lake](#)

Richtlinienressourcen für Security Lake

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` 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": "*" 
```

Security Lake definiert die folgenden Ressourcentypen: Abonment und die Data Lake-Konfiguration für einen AWS-Konto bestimmten AWS-Region. Sie können diese Ressourcentypen mithilfe von ARNs in Richtlinien angeben.

Eine Liste der Security Lake-Ressourcentypen und der jeweiligen ARN-Syntax finden Sie unter [Von Amazon Security Lake definierte Ressourcentypen](#) in der Service Authorization Reference. Informationen darüber, welche Aktionen Sie für jeden Ressourcentyp angeben können, finden Sie unter [Von Amazon Security Lake definierte Aktionen](#) in der Service Authorization Reference.

Beispiele für identitätsbasierte Security Lake-Richtlinien finden Sie unter. [Beispiele für identitätsbasierte Richtlinien für Amazon Security Lake](#)

Bedingungsschlüssel für Richtlinien für Security Lake

Unterstützt servicespezifische Richtlinienbedingungsschlüssel	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 `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, AWS 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.

Eine Liste der Security Lake-Bedingungsschlüssel finden Sie unter [Bedingungsschlüssel für Amazon Security Lake](#) in der Service Authorization Reference. Informationen zu den Aktionen und Ressourcen, mit denen Sie einen Bedingungsschlüssel verwenden können, finden Sie unter [Von Amazon Security Lake definierte Aktionen](#) in der Service Authorization Reference. Beispiele für Richtlinien, die Bedingungsschlüssel verwenden, finden Sie unter [Beispiele für identitätsbasierte Richtlinien für Amazon Security Lake](#).

Zugriffskontrolllisten (ACLs) in Security Lake

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.

Security Lake unterstützt keine ACLs, was bedeutet, dass Sie einer Security Lake-Ressource keine ACL zuordnen können.

Attributbasierte Zugriffskontrolle (ABAC) mit Security Lake

Unterstützt ABAC (Tags in Richtlinien)

Ja

Die attributbasierte Zugriffskontrolle (ABAC) ist eine Autorisierungsstrategie, bei der Berechtigungen basierend auf Attributen definiert werden. In werden AWS 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 Tags an Security Lake-Ressourcen — Abonnenten und die Data Lake-Konfiguration für eine einzelne Person — anhängen. AWS-Konto AWS-Regionen Sie können den Zugriff auf diese Arten von Ressourcen auch steuern, indem Sie Tag-Informationen im Condition Element einer Richtlinie angeben. Informationen zum Markieren von Security Lake-Ressourcen finden Sie unter [Markieren von Amazon Security Lake-Ressourcen](#). Ein Beispiel für eine identitätsbasierte Richtlinie, die den Zugriff auf eine Ressource anhand der Tags für diese Ressource steuert, finden Sie unter [Beispiele für identitätsbasierte Richtlinien für Amazon Security Lake](#)

Temporäre Anmeldeinformationen mit Security Lake verwenden

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](#).

Security Lake unterstützt die Verwendung temporärer Anmeldeinformationen.

Zugriffssitzungen für Security Lake weiterleiten

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](#).

Für einige Security Lake-Aktionen sind Berechtigungen für zusätzliche, abhängige Aktionen in anderen AWS-Services erforderlich. Eine Liste dieser Aktionen finden Sie unter [Von Amazon Security Lake definierte Aktionen](#) in der Service Authorization Reference.

Service rollen für Security Lake

Unterstützt Service rollen	Nein
----------------------------	------

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.

Security Lake übernimmt oder verwendet keine Servicerollen. Verwandte Dienste wie Amazon und Amazon EventBridge S3 übernehmen jedoch Servicerollen AWS Lambda, wenn Sie Security Lake verwenden. Um Aktionen in Ihrem Namen durchzuführen, verwendet Security Lake eine dienstbezogene Rolle.

 Warning

Das Ändern der Berechtigungen für eine Servicerolle kann zu Betriebsproblemen bei Ihrer Nutzung von Security Lake führen. Bearbeiten Sie Servicerollen nur, wenn Security Lake Sie dazu anleitet.

Dienstbezogene Rollen für Security Lake

Unterstützt serviceverknüpfte Rollen	Ja
--------------------------------------	----

Eine dienstverknüpfte 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. 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.

Security Lake verwendet eine mit dem Dienst verknüpfte IAM-Rolle mit dem Namen.

`AWSServiceRoleForAmazonSecurityLake` Die dienstbezogene Rolle Security Lake gewährt Berechtigungen zum Betrieb eines Security Data Lake-Dienstes im Namen von Kunden. Bei dieser serviceverknüpften Rolle handelt es sich um eine IAM-Rolle, die direkt mit Security Lake verknüpft ist. Sie ist von Security Lake vordefiniert und umfasst alle Berechtigungen, die Security Lake benötigt, um andere in AWS-Services Ihrem Namen anzurufen. Security Lake verwendet diese dienstbezogene Rolle überall dort, AWS-Regionen wo Security Lake verfügbar ist.

Einzelheiten zur Erstellung oder Verwaltung der dienstbezogenen Security Lake-Rolle finden Sie unter [Servicebezogene Rolle für Amazon Security Lake](#)

Beispiele für identitätsbasierte Richtlinien für Amazon Security Lake

Standardmäßig sind Benutzer und Rollen nicht berechtigt, Security Lake-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 den von Security Lake definierten Aktionen und Ressourcentypen, einschließlich des Formats der ARNs für jeden Ressourcentyp, finden Sie unter [Aktionen, Ressourcen und Bedingungsschlüssel für Amazon Security Lake](#) in der Service Authorization Reference.

Themen

- [Bewährte Methoden für Richtlinien](#)
- [Verwenden der Security Lake-Konsole](#)
- [Beispiel: Erteilen der Berechtigung zur Anzeige der eigenen Berechtigungen für Benutzer](#)
- [Beispiel: Erlauben Sie dem Organisationsverwaltungskonto, einen delegierten Administrator zu benennen und zu entfernen](#)
- [Beispiel: Erlauben Sie Benutzern, Abonnenten anhand von Stichwörtern zu bewerten](#)

Bewährte Methoden für Richtlinien

Identitätsbasierte Richtlinien legen fest, ob jemand Security Lake-Ressourcen in Ihrem Konto erstellen, darauf zugreifen oder sie löschen kann. Dies kann zusätzliche Kosten für Ihr verursachen AWS-Konto. Befolgen Sie beim Erstellen oder Bearbeiten identitätsbasierter Richtlinien die folgenden Anleitungen und Empfehlungen:

- Erste Schritte mit AWS verwalteten Richtlinien und Umstellung auf Berechtigungen mit den geringsten Rechten — Um Ihren Benutzern und Workloads zunächst Berechtigungen zu gewähren, verwenden Sie die AWS verwalteten Richtlinien, die Berechtigungen für viele gängige Anwendungsfälle 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.

Verwenden der Security Lake-Konsole

Um auf die Amazon Security Lake-Konsole zugreifen zu können, benötigen Sie einen Mindestsatz an Berechtigungen. Diese Berechtigungen müssen es Ihnen ermöglichen, Details zu den Security Lake-Ressourcen in Ihrem aufzulisten und einzusehen 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.

Um sicherzustellen, dass Benutzer und Rollen die Security Lake-Konsole verwenden können, erstellen Sie IAM-Richtlinien, die ihnen Konsolenzugriff gewähren. Weitere Informationen finden Sie unter [IAM-Identitäten](#) im IAM-Benutzerhandbuch.

Wenn Sie eine Richtlinie erstellen, die es Benutzern oder Rollen ermöglicht, die Security Lake-Konsole zu verwenden, stellen Sie sicher, dass die Richtlinie die entsprechenden Aktionen für die Ressourcen enthält, auf die diese Benutzer oder Rollen auf der Konsole zugreifen müssen. Andernfalls können sie nicht zu diesen Ressourcen navigieren oder Details zu diesen Ressourcen auf der Konsole anzeigen.

Um beispielsweise mithilfe der Konsole eine benutzerdefinierte Quelle hinzuzufügen, muss ein Benutzer berechtigt sein, die folgenden Aktionen auszuführen:

- `glue:CreateCrawler`
- `glue:CreateDatabase`
- `glue:CreateTable`
- `glue:StartCrawlerSchedule`
- `iam:GetRole`
- `iam:PutRolePolicy`
- `iam>DeleteRolePolicy`
- `iam:PassRole`
- `lakeformation:RegisterResource`
- `lakeformation:GrantPermissions`
- `s3:ListBucket`

- s3:PutObject

Beispiel: Erteilen 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": "*"
    }
  ]
}
```

}

Beispiel: Erlauben Sie dem Organisationsverwaltungskonto, einen delegierten Administrator zu benennen und zu entfernen

Dieses Beispiel zeigt, wie Sie eine Richtlinie erstellen könnten, die es einem Benutzer eines AWS Organizations Verwaltungskontos ermöglicht, den delegierten Security Lake-Administrator für seine Organisation zu bestimmen und zu entfernen.

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Action": [
        "securitylake:RegisterDataLakeDelegatedAdministrator",
        "securitylake:DeregisterDataLakeDelegatedAdministrator"
      ],
      "Resource": "arn:aws:securitylake:*:*:*"
    }
  ]
}
```

Beispiel: Erlauben Sie Benutzern, Abonnenten anhand von Stichwörtern zu bewerten

In identitätsbasierten Richtlinien können Sie Bedingungen verwenden, um den Zugriff auf Security Lake-Ressourcen anhand von Stichwörtern zu steuern. Dieses Beispiel zeigt, wie Sie eine Richtlinie erstellen könnten, die es einem Benutzer ermöglicht, Abonnenten mithilfe der Security Lake-Konsole oder der Security Lake-API zu überprüfen. Die Erlaubnis wird jedoch nur erteilt, wenn der Wert für das Owner Tag für einen Abonnenten der Benutzername des Benutzers ist.

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Sid": "ReviewSubscriberDetailsIfOwner",
      "Effect": "Allow",
      "Action": "securitylake:GetSubscriber",
      "Resource": "arn:aws:securitylake:*:*:subscriber/*",
      "Condition": {
        "StringEquals": {"aws:ResourceTag/Owner": "${aws:username}"}
      }
    }
  ]
}
```

```
    }
  },
  {
    "Sid": "ListSubscribersIfOwner",
    "Effect": "Allow",
    "Action": "securitylake:ListSubscribers",
    "Resource": "*",
    "Condition": {
      "StringEquals": {"aws:ResourceTag/Owner": "${aws:username}"}
    }
  }
]
```

Wenn in diesem Beispiel ein Benutzer, der den Benutzernamen hat, `richard-roe` versucht, die Daten einzelner Abonnenten zu überprüfen, muss der Abonnent mit `Owner=richard-roe` oder `markiert werdenowner=richard-roe`. Andernfalls wird dem Benutzer der Zugriff verweigert. Der Tag-Schlüssel `Owner` der Bedingung stimmt sowohl mit `Owner` als auch mit `owner` überein, da die Namen von Bedingungsschlüsseln nicht zwischen Groß- und Kleinschreibung unterscheiden. Weitere Informationen zur Verwendung von Bedingungsschlüsseln finden Sie unter [IAM-JSON-Richtlinienelemente: Bedingung](#) im IAM-Benutzerhandbuch. Informationen zum Taggen von Security Lake-Ressourcen finden Sie unter [Markieren von Amazon Security Lake-Ressourcen](#)

AWS verwaltete Richtlinien für Amazon Security Lake

Eine AWS verwaltete Richtlinie ist eine eigenständige Richtlinie, die von erstellt und verwaltet wird AWS. AWS Verwaltete Richtlinien sind so konzipiert, dass sie Berechtigungen für viele gängige Anwendungsfälle bereitstellen, sodass Sie damit beginnen können, Benutzern, Gruppen und Rollen Berechtigungen zuzuweisen.

Beachten Sie, dass AWS verwaltete Richtlinien für Ihre speziellen Anwendungsfälle möglicherweise keine Berechtigungen mit den geringsten Rechten gewähren, da sie für alle AWS Kunden verfügbar sind. Wir empfehlen Ihnen, die Berechtigungen weiter zu reduzieren, indem Sie [kundenverwaltete Richtlinien](#) definieren, die speziell auf Ihre Anwendungsfälle zugeschnitten sind.

Sie können die in AWS verwalteten Richtlinien definierten Berechtigungen nicht ändern. Wenn die in einer AWS verwalteten Richtlinie definierten Berechtigungen AWS aktualisiert werden, wirkt sich das

Update auf alle Prinzidentitäten (Benutzer, Gruppen und Rollen) aus, denen die Richtlinie zugeordnet ist. AWS aktualisiert eine AWS verwaltete Richtlinie höchstwahrscheinlich, wenn eine neue Richtlinie eingeführt AWS-Service wird oder neue API-Operationen für bestehende Dienste verfügbar werden.

Weitere Informationen finden Sie unter [Von AWS verwaltete Richtlinien](#) im IAM-Benutzerhandbuch.

AWS verwaltete Richtlinie: AmazonSecurityLakeMetastoreManager

Amazon Security Lake verwendet eine AWS Lambda Funktion zur Verwaltung von Metadaten in Ihrem Data Lake. Mithilfe dieser Funktion kann Security Lake Amazon Simple Storage Service (Amazon S3) -Partitionen, die Ihre Daten und Datendateien enthalten, in den AWS Glue Datenkatalogtabellen indizieren. Diese verwaltete Richtlinie enthält alle Berechtigungen für die Lambda-Funktion, um die S3-Partitionen und Datendateien in den AWS Glue Tabellen zu indizieren.

Details zu Berechtigungen

Diese Richtlinie umfasst die folgenden Berechtigungen:

- `logs`— Ermöglicht Prinzipalen, die Ausgabe der Lambda-Funktion in Amazon CloudWatch Logs zu protokollieren.
- `glue`— Ermöglicht Prinzipalen, bestimmte Schreibaktionen für AWS Glue Datenkatalogtabellen durchzuführen. Auf diese Weise können AWS Glue Crawler auch Partitionen in Ihren Daten identifizieren.
- `sqs`— Ermöglicht Principals, spezifische Lese- und Schreibaktionen für Amazon SQS SQS-Warteschlangen durchzuführen, die Ereignisbenachrichtigungen senden, wenn Objekte zu Ihrem Data Lake hinzugefügt oder aktualisiert werden.
- `s3`— Ermöglicht Prinzipalen, bestimmte Lese- und Schreibaktionen für den Amazon S3 S3-Bucket durchzuführen, der Ihre Daten enthält.

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Sid": "AllowWriteLambdaLogs",
      "Effect": "Allow",
      "Action": [
        "logs:CreateLogStream",
```

```

    "logs:PutLogEvents",
    "logs:CreateLogGroup"
  ],
  "Resource": [
    "arn:aws:logs:*:*:log-group:/aws/lambda/AmazonSecurityLake*",
    "arn:aws:logs:*:*:/aws/lambda/AmazonSecurityLake*"
  ],
  "Condition": {
    "StringEquals": {
      "aws:ResourceAccount": "${aws:PrincipalAccount}"
    }
  }
},
{
  "Sid": "AllowGlueManage",
  "Effect": "Allow",
  "Action": [
    "glue:CreatePartition",
    "glue:BatchCreatePartition",
    "glue:GetTable",
    "glue:UpdateTable"
  ],
  "Resource": [
    "arn:aws:glue:*:*:table/amazon_security_lake_glue_db*/**",
    "arn:aws:glue:*:*:database/amazon_security_lake_glue_db*",
    "arn:aws:glue:*:*:catalog"
  ],
  "Condition": {
    "StringEquals": {
      "aws:ResourceAccount": "${aws:PrincipalAccount}"
    }
  }
},
{
  "Sid": "AllowToReadFromSqs",
  "Effect": "Allow",
  "Action": [
    "sqs:ReceiveMessage",
    "sqs>DeleteMessage",
    "sqs:GetQueueAttributes"
  ],
  "Resource": [
    "arn:aws:sqs:*:*:AmazonSecurityLake*"
  ],

```

```
    "Condition": {
      "StringEquals": {
        "aws:ResourceAccount": "${aws:PrincipalAccount}"
      }
    }
  },
  {
    "Sid": "AllowMetaDataReadWrite",
    "Effect": "Allow",
    "Action": [
      "s3:ListBucket",
      "s3:PutObject",
      "s3:GetObject"
    ],
    "Resource": [
      "arn:aws:s3:::aws-security-data-lake*"
    ],
    "Condition": {
      "StringEquals": {
        "aws:ResourceAccount": "${aws:PrincipalAccount}"
      }
    }
  },
  {
    "Sid": "AllowMetaDataCleanup",
    "Effect": "Allow",
    "Action": [
      "s3:DeleteObject"
    ],
    "Resource": [
      "arn:aws:s3:::aws-security-data-lake*/metadata/*.avro",
      "arn:aws:s3:::aws-security-data-lake*/metadata/*.metadata.json"
    ],
    "Condition": {
      "StringEquals": {
        "aws:ResourceAccount": "${aws:PrincipalAccount}"
      }
    }
  }
]
```

AWS verwaltete Richtlinie: AmazonSecurityLakePermissionsBoundary

Amazon Security Lake erstellt IAM-Rollen für benutzerdefinierte Drittanbieterquellen, um Daten in den Data Lake zu schreiben, und für benutzerdefinierte Drittanbieter-Abonnenten, um Daten aus dem Data Lake zu nutzen, und verwendet diese Richtlinie bei der Erstellung dieser Rollen, um die Grenze ihrer Berechtigungen zu definieren. Sie müssen keine Maßnahmen ergreifen, um diese Richtlinie zu verwenden. Wenn der Data Lake mit einem vom Kunden verwalteten AWS KMS Schlüssel verschlüsselt ist `kms:Decrypt` und `kms:GenerateDataKey` Berechtigungen hinzugefügt werden.

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Sid": "AllowActionsForSecurityLake",
      "Effect": "Allow",
      "Action": [
        "s3:GetObject",
        "s3:GetObjectVersion",
        "s3:ListBucket",
        "s3:ListBucketVersions",
        "s3:PutObject",
        "s3:GetBucketLocation",
        "kms:Decrypt",
        "kms:GenerateDataKey",
        "sqs:ReceiveMessage",
        "sqs:ChangeMessageVisibility",
        "sqs>DeleteMessage",
        "sqs:GetQueueUrl",
        "sqs:SendMessage",
        "sqs:GetQueueAttributes",
        "sqs:ListQueues"
      ],
      "Resource": "*"
    },
    {
      "Sid": "DenyActionsForSecurityLake",
      "Effect": "Deny",
      "NotAction": [
        "s3:GetObject",
        "s3:GetObjectVersion",
        "s3:ListBucket",
        "s3:ListBucketVersions",
        "s3:PutObject",

```

```

        "s3:GetBucketLocation",
        "kms:Decrypt",
        "kms:GenerateDataKey",
        "sqs:ReceiveMessage",
        "sqs:ChangeMessageVisibility",
        "sqs>DeleteMessage",
        "sqs:GetQueueUrl",
        "sqs:SendMessage",
        "sqs:GetQueueAttributes",
        "sqs:ListQueues"
    ],
    "Resource": "*"
},
{
    "Sid": "DenyActionsNotOnSecurityLakeBucket",
    "Effect": "Deny",
    "Action": [
        "s3:GetObject",
        "s3:GetObjectVersion",
        "s3:ListBucket",
        "s3:ListBucketVersions",
        "s3:PutObject",
        "s3:GetBucketLocation"
    ],
    "NotResource": [
        "arn:aws:s3:::aws-security-data-lake*"
    ]
},
{
    "Sid": "DenyActionsNotOnSecurityLakeSQS",
    "Effect": "Deny",
    "Action": [
        "sqs:ReceiveMessage",
        "sqs:ChangeMessageVisibility",
        "sqs>DeleteMessage",
        "sqs:GetQueueUrl",
        "sqs:SendMessage",
        "sqs:GetQueueAttributes",
        "sqs:ListQueues"
    ],
    "NotResource": "arn:aws:sqs:*:*:AmazonSecurityLake*"
},
{
    "Sid": "DenyActionsNotOnSecurityLakeKMSS3SQS",

```

```

    "Effect": "Deny",
    "Action": [
      "kms:Decrypt",
      "kms:GenerateDataKey"
    ],
    "Resource": "*",
    "Condition": {
      "StringNotLike": {
        "kms:ViaService": [
          "s3.*.amazonaws.com",
          "sqs.*.amazonaws.com"
        ]
      }
    }
  },
  {
    "Sid": "DenyActionsNotOnSecurityLakeKMSForS3",
    "Effect": "Deny",
    "Action": [
      "kms:Decrypt",
      "kms:GenerateDataKey"
    ],
    "Resource": "*",
    "Condition": {
      "Null": {
        "kms:EncryptionContext:aws:s3:arn": "false"
      },
      "StringNotLikeIfExists": {
        "kms:EncryptionContext:aws:s3:arn": [
          "arn:aws:s3:::aws-security-data-lake*"
        ]
      }
    }
  },
  {
    "Sid": "DenyActionsNotOnSecurityLakeKMSForS3SQS",
    "Effect": "Deny",
    "Action": [
      "kms:Decrypt",
      "kms:GenerateDataKey"
    ],
    "Resource": "*",
    "Condition": {
      "Null": {

```

```
    "kms:EncryptionContext:aws:sqs:arn": "false"
  },
  "StringNotLikeIfExists": {
    "kms:EncryptionContext:aws:sqs:arn": [
      "arn:aws:sqs:*:*:AmazonSecurityLake*"
    ]
  }
}
```

AWS verwaltete Richtlinie: AmazonSecurityLakeAdministrator

Sie können die `AmazonSecurityLakeAdministrator` Richtlinie einem Principal zuordnen, bevor dieser Amazon Security Lake für sein Konto aktiviert. Diese Richtlinie gewährt Administratorberechtigungen, die einem Principal vollen Zugriff auf alle Security Lake-Aktionen gewähren. Der Principal kann sich dann in Security Lake einbinden und anschließend Quellen und Abonnenten in Security Lake konfigurieren.

Diese Richtlinie umfasst die Aktionen, die Security Lake-Administratoren über Security Lake für andere AWS Dienste ausführen können.

Die `AmazonSecurityLakeAdministrator` Richtlinie unterstützt nicht die Erstellung von Dienstprogrammrollen, die Security Lake benötigt, um die regionsübergreifende Amazon S3 S3-Replikation zu verwalten, neue Datenpartitionen in zu registrieren AWS Glue, einen Glue-Crawler für Daten auszuführen, die zu benutzerdefinierten Quellen hinzugefügt wurden, oder zur Benachrichtigung von HTTPS-Endpunktabonnenten über neue Daten. Sie können diese Rollen im Voraus erstellen, wie unter beschrieben. [Erste Schritte mit Amazon Security Lake](#)

Zusätzlich zur `AmazonSecurityLakeAdministrator` verwalteten Richtlinie benötigt Security Lake `lakeformation:PutDataLakeSettings` Berechtigungen für Onboarding- und Konfigurationsfunktionen. `PutDataLakeSetting` ermöglicht die Einrichtung eines IAM-Prinzips als Administrator für alle regionalen Lake Formation Formation-Ressourcen im Konto. Mit dieser Rolle müssen `iam:CreateRole` permission auch `AmazonSecurityLakeAdministrator` Richtlinien verknüpft sein.

Lake Formation-Administratoren haben vollen Zugriff auf die Lake Formation Formation-Konsole und kontrollieren die anfängliche Datenkonfiguration und die Zugriffsberechtigungen. Security Lake weist den Principal, der Security Lake aktiviert, und die `AmazonSecurityLakeMetaStoreManager` Rolle

(oder eine andere angegebene Rolle) als Lake Formation-Administratoren zu, sodass sie Tabellen erstellen, das Tabellenschema aktualisieren, neue Partitionen registrieren und Berechtigungen für Tabellen konfigurieren können. Sie müssen die folgenden Berechtigungen in die Richtlinie für den Security Lake-Administratorbenutzer oder die Rolle des Security Lake-Administrators aufnehmen:

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Sid": "AllowPutLakeFormationSettings",
      "Effect": "Allow",
      "Action": "lakeformation:PutDatalakeSettings",
      "Resource": "*",
      "Condition": {
        "ForAnyValue:StringEquals": {
          "aws:CalledVia": "securitylake.amazonaws.com"
        }
      }
    }
  ]
}
```

Details zu Berechtigungen

Diese Richtlinie umfasst die folgenden Berechtigungen.

- **securitylake**— Ermöglicht Prinzipalen vollen Zugriff auf alle Security Lake-Aktionen.
- **organizations**— Ermöglicht Prinzipalen, Informationen von AWS Organizations über die Konten in einer Organisation abzurufen. Wenn ein Konto zu einer Organisation gehört, ermöglichen diese Berechtigungen der Security Lake-Konsole, Kontonamen und Kontonummern anzuzeigen.
- **iam**— Ermöglicht Prinzipalen das Erstellen von dienstbezogenen Rollen für Security Lake und AWS Lake Formation Amazon EventBridge, als erforderlichen Schritt bei der Aktivierung dieser Dienste. Ermöglicht auch die Erstellung und Bearbeitung von Richtlinien für Abonnenten- und benutzerdefinierte Quellrollen, wobei die Berechtigungen für diese Rollen auf das beschränkt sind, was in der `AmazonSecurityLakePermissionsBoundary` Richtlinie zulässig ist.
- **ram**— Ermöglicht Prinzipalen die Konfiguration des Lake Formation basierten Abfragezugriffs von Abonnenten auf Security Lake-Quellen.

- `s3`— Ermöglicht Prinzipalen, Security Lake-Buckets zu erstellen und zu verwalten und den Inhalt dieser Buckets zu lesen.
- `lambda`— Ermöglicht Prinzipalen die Verwaltung der zur Aktualisierung Lambda verwendeten AWS Glue Tabellenpartitionen nach der AWS Quellenzustellung und der regionsübergreifenden Replikation.
- `glue`— Ermöglicht Prinzipalen die Erstellung und Verwaltung der Security Lake-Datenbank und -Tabellen.
- `lakeformation`— Ermöglicht Prinzipalen die Verwaltung von Lake Formation Berechtigungen für Security Lake-Tabellen.
- `events`— Ermöglicht Prinzipalen die Verwaltung von Regeln, mit denen Abonnenten über neue Daten in Security Lake-Quellen informiert werden.
- `sqs`— Ermöglicht Prinzipalen das Erstellen und Verwalten von Amazon SQS Warteschlangen, mit denen Abonnenten über neue Daten in Security Lake-Quellen informiert werden.
- `kms`— Ermöglicht Prinzipalen, Security Lake Zugriff auf das Schreiben von Daten mithilfe eines vom Kunden verwalteten Schlüssels zu gewähren.
- `secretsmanager`— Ermöglicht Prinzipalen die Verwaltung von Geheimnissen, die zur Benachrichtigung von Abonnenten über neue Daten in Security Lake-Quellen über HTTPS-Endpunkte verwendet werden.

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Sid": "AllowActionsWithAnyResource",
      "Effect": "Allow",
      "Action": [
        "securitylake:*",
        "organizations:DescribeOrganization",
        "organizations:ListDelegatedServicesForAccount",
        "organizations:ListAccounts",
        "iam:ListRoles",
        "ram:GetResourceShareAssociations"
      ],
      "Resource": "*"
    },
    {
      "Sid": "AllowActionsWithAnyResourceViaSecurityLake",
```

```
"Effect": "Allow",
"Action": [
  "glue:CreateCrawler",
  "glue:StopCrawlerSchedule",
  "lambda:CreateEventSourceMapping",
  "lakeformation:GrantPermissions",
  "lakeformation:ListPermissions",
  "lakeformation:RegisterResource",
  "lakeformation:RevokePermissions",
  "lakeformation:GetDataLakeSettings",
  "events:ListConnections",
  "events:ListApiDestinations",
  "iam:GetRole",
  "iam:ListAttachedRolePolicies",
  "kms:DescribeKey"
],
"Resource": "*",
"Condition": {
  "ForAnyValue:StringEquals": {
    "aws:CalledVia": "securitylake.amazonaws.com"
  }
}
},
{
  "Sid": "AllowManagingSecurityLakeS3Buckets",
  "Effect": "Allow",
  "Action": [
    "s3:CreateBucket",
    "s3:PutBucketPolicy",
    "s3:PutBucketPublicAccessBlock",
    "s3:PutBucketNotification",
    "s3:PutBucketTagging",
    "s3:PutEncryptionConfiguration",
    "s3:PutBucketVersioning",
    "s3:PutReplicationConfiguration",
    "s3:PutLifecycleConfiguration",
    "s3:ListBucket",
    "s3:PutObject",
    "s3:GetBucketNotification"
  ],
  "Resource": "arn:aws:s3:::aws-security-data-lake*",
  "Condition": {
    "ForAnyValue:StringEquals": {
      "aws:CalledVia": "securitylake.amazonaws.com"
    }
  }
}
```

```
    }
  }
},
{
  "Sid": "AllowLambdaCreateFunction",
  "Effect": "Allow",
  "Action": [
    "lambda:CreateFunction"
  ],
  "Resource": [
    "arn:aws:lambda:*:*:function:SecurityLake_Glue_Partition_Updater_Lambda*",
    "arn:aws:lambda:*:*:function:AmazonSecurityLake*"
  ],
  "Condition": {
    "ForAnyValue:StringEquals": {
      "aws:CalledVia": "securitylake.amazonaws.com"
    }
  }
},
{
  "Sid": "AllowLambdaAddPermission",
  "Effect": "Allow",
  "Action": [
    "lambda:AddPermission"
  ],
  "Resource": [
    "arn:aws:lambda:*:*:function:SecurityLake_Glue_Partition_Updater_Lambda*",
    "arn:aws:lambda:*:*:function:AmazonSecurityLake*"
  ],
  "Condition": {
    "ForAnyValue:StringEquals": {
      "aws:CalledVia": "securitylake.amazonaws.com"
    },
    "StringEquals": {
      "lambda:Principal": "securitylake.amazonaws.com"
    }
  }
},
{
  "Sid": "AllowGlueActions",
  "Effect": "Allow",
  "Action": [
    "glue:CreateDatabase",
    "glue:GetDatabase",
```

```

    "glue:CreateTable",
    "glue:GetTable"
  ],
  "Resource": [
    "arn:aws:glue:*:*:catalog",
    "arn:aws:glue:*:*:database/amazon_security_lake_glue_db*",
    "arn:aws:glue:*:*:table/amazon_security_lake_glue_db*/*"
  ],
  "Condition": {
    "ForAnyValue:StringEquals": {
      "aws:CalledVia": "securitylake.amazonaws.com"
    }
  }
},
{
  "Sid": "AllowEventBridgeActions",
  "Effect": "Allow",
  "Action": [
    "events:PutTargets",
    "events:PutRule",
    "events:DescribeRule",
    "events:CreateApiDestination",
    "events:CreateConnection",
    "events:UpdateConnection",
    "events:UpdateApiDestination",
    "events>DeleteConnection",
    "events>DeleteApiDestination",
    "events:ListTargetsByRule",
    "events:RemoveTargets",
    "events>DeleteRule"
  ],
  "Resource": [
    "arn:aws:events:*:*:rule/AmazonSecurityLake*",
    "arn:aws:events:*:*:rule/SecurityLake*",
    "arn:aws:events:*:*:api-destination/AmazonSecurityLake*",
    "arn:aws:events:*:*:connection/AmazonSecurityLake*"
  ],
  "Condition": {
    "ForAnyValue:StringEquals": {
      "aws:CalledVia": "securitylake.amazonaws.com"
    }
  }
}
},
{

```

```

    "Sid": "AllowSQSActions",
    "Effect": "Allow",
    "Action": [
      "sqs:CreateQueue",
      "sqs:SetQueueAttributes",
      "sqs:GetQueueURL",
      "sqs:AddPermission",
      "sqs:GetQueueAttributes",
      "sqs>DeleteQueue"
    ],
    "Resource": [
      "arn:aws:sqs:*:*:SecurityLake*",
      "arn:aws:sqs:*:*:AmazonSecurityLake*"
    ],
    "Condition": {
      "ForAnyValue:StringEquals": {
        "aws:CalledVia": "securitylake.amazonaws.com"
      }
    }
  },
  {
    "Sid": "AllowKmsCmkGrantForSecurityLake",
    "Effect": "Allow",
    "Action": "kms:CreateGrant",
    "Resource": "arn:aws:kms:*:*:key/*",
    "Condition": {
      "ForAnyValue:StringEquals": {
        "aws:CalledVia": "securitylake.amazonaws.com"
      },
      "StringLike": {
        "kms:EncryptionContext:aws:s3:arn": "arn:aws:s3:::aws-security-data-lake*"
      },
      "ForAllValues:StringEquals": {
        "kms:GrantOperations": [
          "GenerateDataKey",
          "RetireGrant",
          "Decrypt"
        ]
      }
    }
  },
  {
    "Sid": "AllowEnablingQueryBasedSubscribers",
    "Effect": "Allow",

```

```

"Action": [
  "ram:CreateResourceShare",
  "ram:AssociateResourceShare"
],
"Resource": "*",
"Condition": {
  "StringLikeIfExists": {
    "ram:ResourceArn": [
      "arn:aws:glue:*:*:catalog",
      "arn:aws:glue:*:*:database/amazon_security_lake_glue_db*",
      "arn:aws:glue:*:*:table/amazon_security_lake_glue_db*/*"
    ]
  },
  "ForAnyValue:StringEquals": {
    "aws:CalledVia": "securitylake.amazonaws.com"
  }
}
},
{
  "Sid": "AllowConfiguringQueryBasedSubscribers",
  "Effect": "Allow",
  "Action": [
    "ram:UpdateResourceShare",
    "ram:GetResourceShares",
    "ram:DisassociateResourceShare",
    "ram>DeleteResourceShare"
  ],
  "Resource": "*",
  "Condition": {
    "StringLike": {
      "ram:ResourceShareName": "LakeFormation*"
    },
    "ForAnyValue:StringEquals": {
      "aws:CalledVia": "securitylake.amazonaws.com"
    }
  }
},
{
  "Sid": "AllowConfiguringCredentialsForSubscriberNotification",
  "Effect": "Allow",
  "Action": [
    "secretsmanager:CreateSecret",
    "secretsmanager:GetSecretValue",
    "secretsmanager:PutSecretValue"
  ]
}

```

```

    ],
    "Resource": "arn:aws:secretsmanager:*:*:secret:events!connection/
AmazonSecurityLake-*",
    "Condition": {
      "ForAnyValue:StringEquals": {
        "aws:CalledVia": "securitylake.amazonaws.com"
      }
    }
  },
  {
    "Sid": "AllowPassRoleForUpdatingGluePartitionsSecLakeArn",
    "Effect": "Allow",
    "Action": "iam:PassRole",
    "Resource": [
      "arn:aws:iam:*:*:role/service-role/AmazonSecurityLakeMetaStoreManager",
      "arn:aws:iam:*:*:role/service-role/AmazonSecurityLakeMetaStoreManagerV2"
    ],
    "Condition": {
      "StringEquals": {
        "iam:PassedToService": "lambda.amazonaws.com"
      },
      "StringLike": {
        "iam:AssociatedResourceARN": "arn:aws:securitylake:*:*:data-lake/default"
      }
    }
  },
  {
    "Sid": "AllowPassRoleForUpdatingGluePartitionsLambdaArn",
    "Effect": "Allow",
    "Action": "iam:PassRole",
    "Resource": [
      "arn:aws:iam:*:*:role/service-role/AmazonSecurityLakeMetaStoreManager",
      "arn:aws:iam:*:*:role/service-role/AmazonSecurityLakeMetaStoreManagerV2"
    ],
    "Condition": {
      "StringEquals": {
        "iam:PassedToService": "lambda.amazonaws.com"
      },
      "StringLike": {
        "iam:AssociatedResourceARN": [
          "arn:aws:lambda:*:*:function:SecurityLake_Glue_Partition_Updater_Lambda*",
          "arn:aws:lambda:*:*:function:AmazonSecurityLake*"
        ]
      }
    }
  },

```

```

    "ForAnyValue:StringEquals": {
      "aws:CalledVia": "securitylake.amazonaws.com"
    }
  },
  {
    "Sid": "AllowPassRoleForCrossRegionReplicationSecLakeArn",
    "Effect": "Allow",
    "Action": "iam:PassRole",
    "Resource": "arn:aws:iam::*:role/service-role/AmazonSecurityLakeS3ReplicationRole",
    "Condition": {
      "StringEquals": {
        "iam:PassedToService": "s3.amazonaws.com"
      },
      "StringLike": {
        "iam:AssociatedResourceARN": "arn:aws:securitylake:*:*:data-lake/default"
      }
    }
  },
  {
    "Sid": "AllowPassRoleForCrossRegionReplicationS3Arn",
    "Effect": "Allow",
    "Action": "iam:PassRole",
    "Resource": "arn:aws:iam::*:role/service-role/AmazonSecurityLakeS3ReplicationRole",
    "Condition": {
      "StringEquals": {
        "iam:PassedToService": "s3.amazonaws.com"
      },
      "StringLike": {
        "iam:AssociatedResourceARN": "arn:aws:s3:::aws-security-data-lake*"
      },
      "ForAnyValue:StringEquals": {
        "aws:CalledVia": "securitylake.amazonaws.com"
      }
    }
  },
  {
    "Sid": "AllowPassRoleForCustomSourceCrawlerSecLakeArn",
    "Effect": "Allow",
    "Action": "iam:PassRole",
    "Resource": "arn:aws:iam::*:role/service-role/
AmazonSecurityLakeCustomDataGlueCrawler*",
    "Condition": {
      "StringEquals": {

```

```

        "iam:PassedToService": "glue.amazonaws.com"
    },
    "StringLike": {
        "iam:AssociatedResourceARN": "arn:aws:securitylake:*:*:data-lake/default"
    }
}
},
{
    "Sid": "AllowPassRoleForCustomSourceCrawlerGlueArn",
    "Effect": "Allow",
    "Action": "iam:PassRole",
    "Resource": "arn:aws:iam:*:*:role/service-role/
AmazonSecurityLakeCustomDataGlueCrawler*",
    "Condition": {
        "StringEquals": {
            "iam:PassedToService": "glue.amazonaws.com"
        },
        "ForAnyValue:StringEquals": {
            "aws:CalledVia": "securitylake.amazonaws.com"
        }
    }
},
{
    "Sid": "AllowPassRoleForSubscriberNotificationSecLakeArn",
    "Effect": "Allow",
    "Action": "iam:PassRole",
    "Resource": "arn:aws:iam:*:*:role/service-role/
AmazonSecurityLakeSubscriberEventBridge",
    "Condition": {
        "StringEquals": {
            "iam:PassedToService": "events.amazonaws.com"
        },
        "StringLike": {
            "iam:AssociatedResourceARN": "arn:aws:securitylake:*:*:subscriber/*"
        }
    }
},
{
    "Sid": "AllowPassRoleForSubscriberNotificationEventsArn",
    "Effect": "Allow",
    "Action": "iam:PassRole",
    "Resource": "arn:aws:iam:*:*:role/service-role/
AmazonSecurityLakeSubscriberEventBridge",
    "Condition": {

```

```

    "StringEquals": {
      "iam:PassedToService": "events.amazonaws.com"
    },
    "StringLike": {
      "iam:AssociatedResourceARN": "arn:aws:events:*:*:rule/AmazonSecurityLake*"
    },
    "ForAnyValue:StringEquals": {
      "aws:CalledVia": "securitylake.amazonaws.com"
    }
  }
},
{
  "Sid": "AllowOnboardingToSecurityLakeDependencies",
  "Effect": "Allow",
  "Action": "iam:CreateServiceLinkedRole",
  "Resource": [
    "arn:aws:iam:*:*:role/aws-service-role/securitylake.amazonaws.com/
AWSServiceRoleForSecurityLake",
    "arn:aws:iam:*:*:role/aws-service-role/lakeformation.amazonaws.com/
AWSServiceRoleForLakeFormationDataAccess",
    "arn:aws:iam:*:*:role/aws-service-role/apidestinations.events.amazonaws.com/
AWSServiceRoleForAmazonEventBridgeApiDestinations"
  ],
  "Condition": {
    "StringLike": {
      "iam:AWSServiceName": [
        "securitylake.amazonaws.com",
        "lakeformation.amazonaws.com",
        "apidestinations.events.amazonaws.com"
      ]
    }
  }
},
{
  "Sid": "AllowRolePolicyActionsforSubscribersandSources",
  "Effect": "Allow",
  "Action": [
    "iam:CreateRole",
    "iam:PutRolePolicy",
    "iam>DeleteRolePolicy"
  ],
  "Resource": "arn:aws:iam:*:*:role/AmazonSecurityLake*",
  "Condition": {
    "StringEquals": {

```

```

    "iam:PermissionsBoundary": "arn:aws:iam::aws:policy/
AmazonSecurityLakePermissionsBoundary"
  },
  "ForAnyValue:StringEquals": {
    "aws:CalledVia": "securitylake.amazonaws.com"
  }
}
},
{
  "Sid": "AllowRegisterS3LocationInLakeFormation",
  "Effect": "Allow",
  "Action": [
    "iam:PutRolePolicy",
    "iam:GetRolePolicy"
  ],
  "Resource": "arn:aws:iam::*:role/aws-service-role/lakeformation.amazonaws.com/
AWSServiceRoleForLakeFormationDataAccess",
  "Condition": {
    "ForAnyValue:StringEquals": {
      "aws:CalledVia": "securitylake.amazonaws.com"
    }
  }
},
{
  "Sid": "AllowIAMActionsByResource",
  "Effect": "Allow",
  "Action": [
    "iam:ListRolePolicies",
    "iam>DeleteRole"
  ],
  "Resource": "arn:aws:iam::*:role/AmazonSecurityLake*",
  "Condition": {
    "ForAnyValue:StringEquals": {
      "aws:CalledVia": "securitylake.amazonaws.com"
    }
  }
},
{
  "Sid": "S3ReadAccessToSecurityLakes",
  "Effect": "Allow",
  "Action": [
    "s3:Get*",
    "s3:List*"
  ],
}

```

```

    "Resource": "arn:aws:s3:::aws-security-data-lake-*"
  },
  {
    "Sid": "S3ReadAccessToSecurityLakeMetastoreObject",
    "Effect": "Allow",
    "Action": [
      "s3:GetObject",
      "s3:GetObjectVersion"
    ],
    "Resource": "arn:aws:s3:::security-lake-meta-store-manager-*"
  },
  {
    "Sid": "S3ResourcelessReadOnly",
    "Effect": "Allow",
    "Action": [
      "s3:GetAccountPublicAccessBlock",
      "s3:ListAccessPoints",
      "s3:ListAllMyBuckets"
    ],
    "Resource": "*"
  }
]
}

```

AWS verwaltete Richtlinie: SecurityLakeServiceLinkedRole

Sie können die `SecurityLakeServiceLinkedRole` verwaltete Richtlinie nicht an Ihre IAM-Entitäten anhängen. Diese Richtlinie ist einer dienstbezogenen Rolle zugeordnet, die es Security Lake ermöglicht, Aktionen in Ihrem Namen durchzuführen. Weitere Informationen finden Sie unter [Servicebezogene Rolle für Amazon Security Lake](#).

AWS verwaltete Richtlinie: Rolle AWS GlueService

Die `AWS GlueServiceRole` verwaltete Richtlinie ruft den AWS Glue Crawler auf und ermöglicht AWS Glue das Crawlen benutzerdefinierter Quelldaten und das Identifizieren von Partitionsmetadaten. Diese Metadaten sind erforderlich, um Tabellen im Datenkatalog zu erstellen und zu aktualisieren.

Weitere Informationen finden Sie unter [Sammeln von Daten aus benutzerdefinierten Quellen](#).

Security Lake aktualisiert AWS verwaltete Richtlinien

Sehen Sie sich Details zu Aktualisierungen der AWS verwalteten Richtlinien für Security Lake an, seit dieser Dienst begonnen hat, diese Änderungen zu verfolgen. Wenn Sie automatische Benachrichtigungen über Änderungen an dieser Seite erhalten möchten, abonnieren Sie den RSS-Feed auf der Seite mit dem Verlauf der Security Lake-Dokumente.

Änderung	Beschreibung	Datum
Serviceverknüpfte Rolle für Amazon Security Lake — Aktualisierung der vorhandenen Berechtigungen für serviceverknüpfte Rollen	Wir haben der AWS verwalteten Richtlinie für die SecurityLakeServiceLinkedRole Richtlinie AWS WAF Aktionen hinzugefügt. Die zusätzlichen Aktionen ermöglichen es Security Lake, AWS WAF Protokolle zu sammeln, wenn es als Protokollquelle in Security Lake aktiviert ist.	22. Mai 2024
AmazonSecurityLake PermissionsBoundary – Aktualisierung auf eine bestehende Richtlinie	Security Lake hat der Richtlinie SID-Aktionen hinzugefügt.	13. Mai 2024
AmazonSecurityLake MetastoreManager – Aktualisierung auf eine bestehende Richtlinie	Security Lake hat die Richtlinie aktualisiert und nun eine Aktion zur Bereinigung von Metadaten hinzugefügt, mit der Sie die Metadaten in Ihrem Data Lake löschen können.	27. März 2024
AmazonSecurityLakeAdministrator – Aktualisierung auf eine bestehende Richtlinie	Security Lake hat die Richtlinie aktualisiert, um die neue AmazonSecurityLakeMetastoreManagerV2 Rolle zuzulassen iam:PassRole und ermöglicht es	23. Februar 2024

Änderung	Beschreibung	Datum
	Security Lake, Data Lake-Komponenten bereitzustellen oder zu aktualisieren.	
AmazonSecurityLakeMetastoreManager – Neue Richtlinie.	Security Lake hat eine neue verwaltete Richtlinie hinzugefügt, die Security Lake Berechtigungen zur Verwaltung von Metadaten in Ihrem Data Lake gewährt.	23. Januar 2024
AmazonSecurityLakeAdministrator – Neue Richtlinie.	Security Lake hat eine neue verwaltete Richtlinie hinzugefügt, die einem Principal vollen Zugriff auf alle Security Lake-Aktionen gewährt.	30. Mai 2023
Security Lake hat begonnen, Änderungen zu verfolgen	Security Lake begann, Änderungen an seinen AWS verwalteten Richtlinien nachzuverfolgen.	29. November 2022

Servicebezogene Rolle für Amazon Security Lake

Security Lake verwendet eine [dienstverknüpfte AWS Identity and Access Management \(IAM\) Rolle](#) mit dem Namen `AWSServiceRoleForSecurityLake`. Bei dieser serviceverknüpften Rolle handelt es sich um eine IAM-Rolle, die direkt mit Security Lake verknüpft ist. Sie ist von Security Lake vordefiniert und umfasst alle Berechtigungen, die Security Lake benötigt, um andere in AWS-Services Ihrem Namen anzurufen und den Security Data Lake-Dienst zu betreiben. Security Lake verwendet diese dienstbezogene Rolle überall dort, AWS-Regionen wo Security Lake verfügbar ist.

Durch die dienstbezogene Rolle müssen die erforderlichen Berechtigungen bei der Einrichtung von Security Lake nicht mehr manuell hinzugefügt werden. Security Lake definiert die Berechtigungen dieser dienstbezogenen Rolle, und sofern nicht anders definiert, kann nur Security Lake die Rolle übernehmen. Die definierten Berechtigungen umfassen die Vertrauens- und Berechtigungsrichtlinie. Diese Berechtigungsrichtlinie kann keinen anderen IAM-Entitäten zugewiesen werden.

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 Rollenberechtigung](#) im IAM-Benutzerhandbuch. Sie können eine dienstverknüpfte Rolle erst löschen, nachdem Sie die zugehörigen Ressourcen gelöscht haben. Dies schützt Ihre -Ressourcen, da Sie nicht versehentlich die Berechtigung für den Zugriff auf die Ressourcen entfernen können.

Informationen zu anderen Services, die serviceorientierte Rollen unterstützen, finden Sie unter [AWS services that work with IAM](#) (-Services, die mit IAM funktionieren). Suchen Sie nach den Services, für die Yes (Ja) in der Spalte Service-linked roles (Serviceorientierte Rollen) angegeben ist. Wählen Sie Ja mit einem Link, um die Dokumentation der dienstbezogenen Rolle für diesen Dienst zu lesen.

Themen

- [Berechtigungen für dienstbezogene Rollen für Security Lake](#)
- [Die serviceverknüpfte Security Lake-Rolle wird erstellt](#)
- [Bearbeitung der serviceverknüpften Rolle in Security Lake](#)
- [Löschen der serviceverknüpften Rolle in Security Lake](#)
- [Wird AWS-Regionen für die serviceverknüpfte Security Lake-Rolle unterstützt](#)

Berechtigungen für dienstbezogene Rollen für Security Lake

Security Lake verwendet die angegebene dienstverknüpfte Rolle.

`AWSServiceRoleForSecurityLake` Diese dienstbezogene Rolle vertraut darauf, dass der `securitylake.amazonaws.com` Dienst die Rolle übernimmt. Weitere Informationen zu AWS verwalteten Richtlinien für Amazon Security Lake finden Sie unter [Richtlinien für Amazon Security Lake AWS verwalten](#).

Die Berechtigungsrichtlinie für die Rolle, bei der es sich um eine AWS verwaltete Richtlinie mit dem Namen `SecurityLakeServiceLinkedRole`, ermöglicht es Security Lake, den Security Data Lake zu erstellen und zu betreiben. Sie ermöglicht es Security Lake auch, Aufgaben wie die folgenden für die angegebenen Ressourcen auszuführen:

- Verwenden Sie AWS Organizations Aktionen, um Informationen über verknüpfte Konten abzurufen
- Verwenden Sie Amazon Elastic Compute Cloud (Amazon EC2), um Informationen über Amazon VPC Flow Logs abzurufen
- Verwenden Sie AWS CloudTrail Aktionen, um Informationen über die serviceverknüpfte Rolle abzurufen

- Verwenden Sie AWS WAF Aktionen zum Sammeln von AWS WAF Protokollen, wenn es als Protokollquelle in Security Lake aktiviert ist
- Verwenden Sie LogDelivery Action, um ein Abonnement für die AWS WAF Protokollzustellung zu erstellen oder zu löschen.

Die Rolle ist mit der folgenden Berechtigungsrichtlinie konfiguriert:

```
{
  "Version": "2012-10-17",
  "Statement": [{
    "Sid": "OrganizationsPolicies",
    "Effect": "Allow",
    "Action": [
      "organizations:ListAccounts",
      "organizations:DescribeOrganization"
    ],
    "Resource": [
      "*"
    ]
  },
  {
    "Sid": "DescribeOrgAccounts",
    "Effect": "Allow",
    "Action": [
      "organizations:DescribeAccount"
    ],
    "Resource": [
      "arn:aws:organizations::*:account/o-*/*"
    ]
  },
  {
    "Sid": "AllowManagementOfServiceLinkedChannel",
    "Effect": "Allow",
    "Action": [
      "cloudtrail:CreateServiceLinkedChannel",
      "cloudtrail>DeleteServiceLinkedChannel",
      "cloudtrail:GetServiceLinkedChannel",
      "cloudtrail:UpdateServiceLinkedChannel"
    ],
    "Resource": "arn:aws:cloudtrail:*:*:channel/aws-service-channel/security-
lake/*"
  },
  ],
}
```

```
{
  "Sid": "AllowListServiceLinkedChannel",
  "Effect": "Allow",
  "Action": [
    "cloudtrail:ListServiceLinkedChannels"
  ],
  "Resource": "*"
},
{
  "Sid": "DescribeAnyVpc",
  "Effect": "Allow",
  "Action": [
    "ec2:DescribeVpcs"
  ],
  "Resource": "*"
},
{
  "Sid": "ListDelegatedAdmins",
  "Effect": "Allow",
  "Action": [
    "organizations:ListDelegatedAdministrators"
  ],
  "Resource": "*",
  "Condition": {
    "StringEquals": {
      "organizations:ServicePrincipal": "securitylake.amazonaws.com"
    }
  }
},
{
  "Sid": "AllowWafLoggingConfiguration",
  "Effect": "Allow",
  "Action": [
    "wafv2:PutLoggingConfiguration",
    "wafv2:GetLoggingConfiguration",
    "wafv2:ListLoggingConfigurations",
    "wafv2>DeleteLoggingConfiguration"
  ],
  "Resource": "*",
  "Condition": {
    "StringEquals": {
      "wafv2:LogScope": "SecurityLake"
    }
  }
}
```

```

    },
    {
      "Sid": "AllowPutLoggingConfiguration",
      "Effect": "Allow",
      "Action": [
        "wafv2:PutLoggingConfiguration"
      ],
      "Resource": "*",
      "Condition": {
        "ArnLike": {
          "wafv2:LogDestinationResource": "arn:aws:s3:::aws-waf-logs-
security-lake-*"
        }
      }
    },
    {
      "Sid": "ListWebACLs",
      "Effect": "Allow",
      "Action": [
        "wafv2:ListWebACLs"
      ],
      "Resource": "*"
    },
    {
      "Sid": "LogDelivery",
      "Effect": "Allow",
      "Action": [
        "logs:CreateLogDelivery",
        "logs>DeleteLogDelivery"
      ],
      "Resource": "*",
      "Condition": {
        "ForAnyValue:StringEquals": {
          "aws:CalledVia": [
            "wafv2.amazonaws.com"
          ]
        }
      }
    }
  ]
}

```

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 Rollenberechtigung](#) im IAM-Benutzerhandbuch.

Die serviceverknüpfte Security Lake-Rolle wird erstellt

Sie müssen die `AWSServiceRoleForSecurityLake` dienstverknüpfte Rolle für Security Lake nicht manuell erstellen. Wenn Sie Security Lake für Sie aktivieren AWS-Konto, erstellt Security Lake automatisch die serviceverknüpfte Rolle für Sie.

Bearbeitung der serviceverknüpften Rolle in Security Lake

In Security Lake können Sie die `AWSServiceRoleForSecurityLake` dienstverknüpfte Rolle nicht bearbeiten. Nachdem eine dienstverknüpfte Rolle erstellt wurde, können Sie den Namen der Rolle nicht mehr ändern, da verschiedene Entitäten möglicherweise auf die Rolle verweisen. Sie können jedoch die Beschreibung der Rolle mit IAM bearbeiten. Weitere Informationen finden Sie unter [Bearbeiten einer serviceverknüpften Rolle](#) im IAM-Benutzerhandbuch.

Löschen der serviceverknüpften Rolle in Security Lake

Sie können die dienstverknüpfte Rolle nicht aus Security Lake löschen. Stattdessen können Sie die dienstverknüpfte Rolle aus der IAM-Konsole, API oder löschen. AWS CLI Weitere Informationen finden Sie unter [Löschen einer serviceverknüpften Rolle](#) im IAM-Benutzerhandbuch.

Bevor Sie die dienstverknüpfte Rolle löschen können, müssen Sie zunächst bestätigen, dass die Rolle keine aktiven Sitzungen hat, und alle Ressourcen entfernen, die `AWSServiceRoleForSecurityLake` sie verwendet.

Note

Wenn Security Lake die `AWSServiceRoleForSecurityLake` Rolle verwendet, wenn Sie versuchen, die Ressourcen zu löschen, schlägt das Löschen möglicherweise fehl. Warten Sie in diesem Fall einige Minuten und führen Sie den Vorgang dann erneut aus.

Wenn Sie die `AWSServiceRoleForSecurityLake` dienstverknüpfte Rolle löschen und sie erneut erstellen müssen, können Sie sie erneut erstellen, indem Sie Security Lake für Ihr Konto aktivieren. Wenn Sie Security Lake erneut aktivieren, erstellt Security Lake die dienstverknüpfte Rolle automatisch erneut für Sie.

Wird AWS-Regionen für die serviceverknüpfte Security Lake-Rolle unterstützt

Security Lake unterstützt die Verwendung der `AWSServiceRoleForSecurityLake` dienstbezogenen Rolle in allen Bereichen, in AWS-Regionen denen Security Lake verfügbar ist. Eine Liste der Regionen, in denen Security Lake derzeit verfügbar ist, finden Sie unter [Amazon Security Lake e-](#).

Datenschutz in Amazon Security Lake

Das AWS [Modell](#) der mit gilt für den Datenschutz in Amazon Security Lake. 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 Security Lake oder anderen Geräten arbeiten und die Konsole, die API oder SDKs 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.

Verschlüsselung im Ruhezustand

Amazon Security Lake speichert Ihre Daten im Ruhezustand sicher mithilfe von AWS Verschlüsselungslösungen. Unformatierte Sicherheitsprotokoll- und Ereignisdaten werden in einem Amazon Simple Storage Service (Amazon S3) -Bucket mit mehreren Mandanten in einem Konto gespeichert, das von Security Lake verwaltet wird. Security Lake verschlüsselt diese Rohdaten mit einem [AWS eigenen Schlüssel](#) von AWS Key Management Service (AWS KMS). AWS Eigene Schlüssel sind eine Sammlung von AWS KMS Schlüsseln, die ein AWS Dienst — in diesem Fall Security Lake — besitzt und verwaltet, sodass sie in mehreren Konten verwendet werden können.

AWS

Security Lake führt ETL-Jobs (Extrahieren, Transformieren und Laden) für rohe Protokoll- und Ereignisdaten aus. Die verarbeiteten Daten bleiben im Security Lake-Dienstkonto verschlüsselt.

Nach Abschluss der ETL-Jobs erstellt Security Lake S3-Buckets mit einem Mandanten in Ihrem Konto (ein Bucket für jeden Bucket AWS-Region, in dem Sie Security Lake aktiviert haben). Daten werden nur vorübergehend im Multi-Tenant-S3-Bucket gespeichert, bis Security Lake die Daten zuverlässig an die Single-Tenant-S3-Buckets liefern kann. Die Single-Tenant-Buckets beinhalten eine ressourcenbasierte Richtlinie, die Security Lake die Erlaubnis erteilt, Protokoll- und Ereignisdaten in die Buckets zu schreiben. [Um Daten in Ihrem S3-Bucket zu verschlüsseln, können Sie entweder einen von S3 verwalteten Verschlüsselungsschlüssel oder einen vom Kunden verwalteten Schlüssel \(von\) wählen.](#) AWS KMS Beide Optionen verwenden symmetrische Verschlüsselung.

Verwenden Sie einen KMS-Schlüssel für die Verschlüsselung Ihrer Daten

Standardmäßig werden die von Security Lake an Ihren S3-Bucket übermittelten Daten durch serverseitige Amazon-Verschlüsselung mit von Amazon S3 [verwalteten Verschlüsselungsschlüsseln \(SSE-S3\)](#) verschlüsselt. Um eine Sicherheitsebene bereitzustellen, die Sie direkt verwalten, können Sie stattdessen [serverseitige Verschlüsselung mit AWS KMS Schlüsseln \(SSE-KMS\)](#) für Ihre Security Lake-Daten verwenden.

SSE-KMS wird in der Security Lake-Konsole nicht unterstützt. Um SSE-KMS mit der Security Lake API oder CLI zu verwenden, [erstellen Sie zunächst einen KMS-Schlüssel](#) oder verwenden einen vorhandenen Schlüssel. Sie fügen dem Schlüssel eine Richtlinie hinzu, die festlegt, welche Benutzer den Schlüssel zum Verschlüsseln und Entschlüsseln von Security Lake-Daten verwenden können.

Wenn Sie einen vom Kunden verwalteten Schlüssel verwenden, um Daten zu verschlüsseln, die in Ihren S3-Bucket geschrieben werden, können Sie keinen Schlüssel für mehrere Regionen wählen. Für vom Kunden verwaltete Schlüssel gewährt Security Lake in Ihrem Namen einen [Zuschuss](#), indem es eine `CreateGrant` Anfrage an sendet. AWS KMS Grants in AWS KMS werden verwendet, um Security Lake Zugriff auf einen KMS-Schlüssel in einem Kundenkonto zu gewähren.

Security Lake benötigt den Grant, um Ihren vom Kunden verwalteten Schlüssel für die folgenden internen Operationen zu verwenden:

- Senden Sie `GenerateDataKey` Anfragen AWS KMS zur Generierung von Datenschlüsseln, die mit Ihrem vom Kunden verwalteten Schlüssel verschlüsselt sind.
- Senden Sie `RetireGrant` Anfragen an AWS KMS. Wenn Sie Ihren Data Lake aktualisieren, ermöglicht dieser Vorgang die Außerbetriebnahme des Zuschusses, der dem AWS KMS KMS-Schlüssel für die ETL-Verarbeitung hinzugefügt wurde.

Security Lake benötigt keine `Decrypt` Berechtigungen. Wenn autorisierte Benutzer des Schlüssels Security Lake-Daten lesen, verwaltet S3 die Entschlüsselung, und die autorisierten Benutzer können Daten in unverschlüsselter Form lesen. Ein Abonnent benötigt jedoch `Decrypt` Berechtigungen, um Quelldaten nutzen zu können. Weitere Informationen zu Abonnentenberechtigungen finden Sie unter [Verwaltung des Datenzugriffs für Security Lake-Abonnenten](#).

Wenn Sie einen vorhandenen KMS-Schlüssel zum Verschlüsseln von Security Lake-Daten verwenden möchten, müssen Sie die Schlüsselrichtlinie für den KMS-Schlüssel ändern. Die Schlüsselrichtlinie muss es der IAM-Rolle, die dem Data Lake-Standort Lake Formation zugeordnet ist, ermöglichen, den KMS-Schlüssel zum Entschlüsseln der Daten zu verwenden. Anweisungen dazu, wie Sie die Schlüsselrichtlinie für einen KMS-Schlüssel ändern können, finden Sie unter [Ändern einer Schlüsselrichtlinie](#) im AWS Key Management Service Entwicklerhandbuch.

Ihr KMS-Schlüssel kann Zuschussanfragen annehmen, sodass Security Lake auf den Schlüssel zugreifen kann, wenn Sie eine Schlüsselrichtlinie erstellen oder eine vorhandene Schlüsselrichtlinie mit den entsprechenden Berechtigungen verwenden. Anweisungen zum Erstellen einer Schlüsselrichtlinie finden Sie unter [Erstellen einer Schlüsselrichtlinie](#) im AWS Key Management Service Entwicklerhandbuch.

Fügen Sie Ihrem KMS-Schlüssel die folgende Schlüsselrichtlinie hinzu:

```
{
  "Sid": "Allow use of the key",
  "Effect": "Allow",
  "Principal": {"AWS": "arn:aws:iam::111122223333:role/ExampleRole"},
  "Action": [
    "kms:CreateGrant",
    "kms:DescribeKey",
    "kms:GenerateDataKey"
  ],
  "Resource": "*"
}
```

Erforderliche IAM-Berechtigungen bei Verwendung eines vom Kunden verwalteten Schlüssels

Im Abschnitt [Erste Schritte: Voraussetzungen](#) finden Sie einen Überblick über die IAM-Rollen, die Sie für die Verwendung von Security Lake erstellen müssen.

Wenn Sie eine benutzerdefinierte Quelle oder einen Abonnenten hinzufügen, erstellt Security Lake IAM-Rollen in Ihrem Konto. Diese Rollen sind für die gemeinsame Nutzung mit anderen IAM-Identitäten vorgesehen. Sie ermöglichen es einer benutzerdefinierten Quelle, Daten in den Data Lake zu schreiben, und einem Abonnenten, Daten aus dem Data Lake zu nutzen. Eine AWS verwaltete Richtlinie namens `AmazonSecurityLakePermissionsBoundary` legt die Berechtigungsgrenzen für diese Rollen fest.

Verschlüsseln von Amazon SQS SQS-Warteschlangen

Wenn Sie Ihren Data Lake erstellen, erstellt Security Lake zwei unverschlüsselte Amazon Simple Queue Service (Amazon SQS) -Warteschlangen im delegierten Security Lake-Administratorkonto. Sie sollten diese Warteschlangen verschlüsseln, um Ihre Daten zu schützen. Die von Amazon Simple Queue Service bereitgestellte standardmäßige serverseitige Verschlüsselung (SSE) ist nicht ausreichend. Sie müssen in AWS Key Management Service (AWS KMS) einen vom Kunden verwalteten Schlüssel erstellen, um die Warteschlangen zu verschlüsseln, und dann dem Amazon S3-Serviceprinzipal die Rechte zur Arbeit mit den verschlüsselten Warteschlangen gewähren. Anweisungen zur Erteilung dieser Berechtigungen finden Sie unter [Warum werden Amazon S3 S3-Ereignisbenachrichtigungen nicht an eine Amazon SQS SQS-Warteschlange gesendet, die serverseitige Verschlüsselung verwendet?](#) im AWS Knowledge Center.

Da Security Lake früher AWS Lambda ETL-Jobs (Extrahieren, Übertragen und Laden) für Ihre Daten unterstützt, müssen Sie Lambda auch Berechtigungen zur Verwaltung von Nachrichten in Ihren Amazon SQS SQS-Warteschlangen erteilen. Weitere Informationen finden Sie unter [Berechtigungen für Ausführungsrollen im Entwicklerhandbuch](#).AWS Lambda

Verschlüsselung während der Übertragung

Security Lake verschlüsselt alle Daten, die zwischen AWS Diensten übertragen werden. Security Lake schützt Daten während der Übertragung zum und vom Dienst, indem alle Daten zwischen Netzwerken automatisch mit dem Verschlüsselungsprotokoll Transport Layer Security (TLS) 1.2 verschlüsselt werden. Direkte HTTPS-Anfragen, die an die Security Lake-APIs gesendet werden, werden mithilfe des [AWS Signature Version 4-Algorithmus](#) signiert, um eine sichere Verbindung herzustellen.

Abmeldung von der Verwendung Ihrer Daten zur Serviceverbesserung

Sie können sich dafür entscheiden, die Verwendung Ihrer Daten zur Entwicklung und Verbesserung von Security Lake und anderen AWS Sicherheitsdiensten abzulehnen, indem Sie die AWS Organizations Opt-Out-Richtlinie verwenden. Sie können sich auch dann abmelden, wenn Security Lake derzeit keine derartigen Daten sammelt. Weitere Informationen zur Deaktivierung finden Sie in den [Opt-Out-Richtlinien für KI-Services](#) im Benutzerhandbuch für AWS Organizations .

Derzeit sammelt Security Lake keine Sicherheitsdaten, die es in Ihrem Namen verarbeitet, oder Sicherheitsdaten, die Sie in Ihren von diesem Dienst erstellten Sicherheitsdatensee hochladen. Um den Security Lake-Dienst und die Funktionen anderer AWS Sicherheitsdienste weiterzuentwickeln und zu verbessern, kann Security Lake in future solche Daten erheben, einschließlich Daten, die Sie aus Datenquellen Dritter hochladen. Wir werden diese Seite aktualisieren, wenn Security Lake beabsichtigt, solche Daten zu sammeln, und beschreiben, wie dies funktionieren wird. Sie haben weiterhin die Möglichkeit, sich jederzeit abzumelden.

Note

Damit Sie die Opt-Out-Richtlinie nutzen können, müssen Ihre AWS Konten zentral von verwaltet werden AWS Organizations. Wenn Sie noch keine Organisation für Ihre AWS Konten erstellt haben, finden Sie [weitere Informationen unter Organisation erstellen und verwalten](#) im AWS Organizations Benutzerhandbuch.

Opt-Out hat folgende Auswirkungen:

- Security Lake löscht die Daten, die es vor Ihrer Abmeldung gesammelt und gespeichert hat (falls vorhanden).
- Nach Ihrer Abmeldung sammelt oder speichert Security Lake diese Daten nicht mehr.

Konformitätsprüfung für Amazon Security Lake

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 Bereitstellungslaufplänen 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.

Bewährte Sicherheitsmethoden für Security Lake

Sehen Sie sich die folgenden bewährten Methoden für die Arbeit mit Amazon Security Lake an.

Gewähren Sie Security Lake-Benutzern die geringstmöglichen Berechtigungen

Folgen Sie dem Prinzip der geringsten Rechte, indem Sie Ihren AWS Identity and Access Management (IAM-) Benutzern, Benutzergruppen und Rollen die Mindestanzahl an Zugriffsrichtlinienberechtigungen gewähren. Sie können beispielsweise einem IAM-Benutzer erlauben, eine Liste von Protokollquellen in Security Lake einzusehen, aber keine Quellen oder Abonnenten zu erstellen. Weitere Informationen finden Sie unter [Beispiele für identitätsbasierte Richtlinien für Amazon Security Lake](#)

Sie können es auch verwenden AWS CloudTrail, um die API-Nutzung in Security Lake zu verfolgen. CloudTrail stellt eine Aufzeichnung der API-Aktionen bereit, die von einem Benutzer, einer Gruppe

oder Rolle in Security Lake ausgeführt wurden. Weitere Informationen finden Sie unter [Protokollieren von Amazon Security Lake-API-Aufrufen mit AWS CloudTrail](#).

Sehen Sie sich die Übersichtsseite an

Die Übersichtsseite der Security Lake-Konsole bietet einen Überblick über die Probleme der letzten 14 Tage, die sich auf den Security Lake-Service und die Amazon S3-Buckets auswirken, in denen Ihre Daten gespeichert sind. Sie können diese Probleme weiter untersuchen, um mögliche sicherheitsrelevante Auswirkungen zu minimieren.

In Security Hub integrieren

Integrieren Sie Security Lake und erhalten AWS Security Hub Sie die Ergebnisse des Security Hubs in Security Lake. Security Hub generiert Erkenntnisse aus vielen verschiedenen Integrationen AWS-Services und Integrationen von Drittanbietern. Wenn Sie die Ergebnisse von Security Hub erhalten, können Sie sich einen Überblick über Ihren Compliance-Status verschaffen und feststellen, ob Sie die bewährten AWS Sicherheitsmethoden einhalten.

Weitere Informationen finden Sie unter [Integration mit AWS Security Hub](#).

Achten Sie auf Security Lake-Ereignisse

Sie können Security Lake mithilfe von CloudWatch Amazon-Metriken überwachen. CloudWatch sammelt jede Minute Rohdaten von Security Lake und verarbeitet sie zu Metriken. Sie können Alarme einrichten, die Benachrichtigungen auslösen, wenn Messwerte bestimmte Schwellenwerte erreichen.

Weitere Informationen finden Sie unter [CloudWatch-Metriken Amazon Security Lake Lake Lake Lake Lake Lake](#).

Resilienz im Amazon Security Lake

Die globale AWS-Infrastruktur ist um AWS-Regionen und Availability Zones herum aufgebaut. AWS-Regionen bieten mehrere physisch getrennte und isolierte Availability Zones, die mit einem Netzwerk mit geringer Latenz, hohem Durchsatz und hoher Redundanz verbunden sind. Diese Availability Zones bieten Ihnen eine effektive Methode zum Entwerfen und Betreiben von Anwendungen und Datenbanken. Availability Zones sind besser hoch verfügbar, fehlertoleranter und skalierbarer als herkömmliche Infrastrukturen mit einem oder mehreren Rechenzentren.

Die Verfügbarkeit von Security Lake hängt von der Verfügbarkeit in der Region ab. Die Verteilung auf mehrere Availability Zones hilft dem Service, Ausfälle in jeder einzelnen Availability Zone zu tolerieren.

Die Verfügbarkeit der Security Lake-Datenebene ist nicht an die Verfügbarkeit einer Region gebunden. Die Verfügbarkeit der Security Lake-Kontrollebene ist jedoch eng mit der Verfügbarkeit in der Region USA Ost (Nord-Virginia) verknüpft.

Weitere Informationen über AWS-Regionen und Availability Zones finden Sie unter [AWS Globale Infrastruktur](#).

Zusätzlich zur AWS globalen Infrastruktur bietet Security Lake, in dem Daten durch Amazon Simple Storage Service (Amazon S3) gesichert werden, mehrere Funktionen zur Unterstützung Ihrer Datenausfallsicherheit und Backup-Anforderungen.

Konfiguration des Lebenszyklus

Eine Lebenszyklus-Konfiguration besteht aus einer Reihe von Regeln, mit denen Aktionen definiert werden, die Amazon S3 auf eine Gruppe von Objekten anwendet. Mithilfe der Konfigurationsregeln für den Lebenszyklus können Sie Amazon S3 anweisen, Objekte in kostengünstigere Speicherklassen zu übergeben bzw. zu archivieren oder zu löschen. Weitere Informationen finden Sie unter [Managing your storage lifecycle \(Verwaltung des Speicherlebenszyklus\)](#) im Amazon-S3-Benutzerhandbuch.

Versioning

Das Versioning ermöglicht Ihnen, mehrere Versionen eines Objekts im selben Bucket aufzubewahren. Sie können Versioning verwenden, um sämtliche Versionen aller Objekte in Ihrem Amazon S3 Bucket zu speichern, abzurufen oder wiederherzustellen. Mithilfe der Versionierung können Sie sich sowohl nach unbeabsichtigten Benutzeraktionen als auch nach Anwendungsausfällen erholen. Weitere Informationen finden Sie unter [Verwenden der Versionierung in S3-Buckets](#) im Amazon S3 S3-Benutzerhandbuch.

Speicherklassen

Amazon S3 bietet je nach den Anforderungen Ihrer Workload eine Reihe von Speicherklassen an. Die Speicherklassen S3 Standard-IA und S3 One Zone-IA sind für Daten konzipiert, auf die Sie etwa einmal im Monat zugreifen und auf Millisekunden zugreifen müssen. Die Speicherklasse S3 Glacier Instant Retrieval ist für langlebige Archivdaten konzipiert, auf die Sie mit Millisekunden-Zugriff zugreifen, auf den Sie etwa einmal pro Quartal zugreifen. Für Archivdaten, die keinen

sofortigen Zugriff erfordern, wie zum Beispiel Backups, können Sie die Speicherklassen S3 Glacier Flexible Retrieval oder S3 Glacier Deep Archive verwenden. Weitere Informationen finden Sie unter [Verwenden von Amazon S3 S3-Speicherklassen](#) im Amazon S3 S3-Benutzerhandbuch.

Infrastruktursicherheit in Amazon Security Lake

Als verwalteter Service ist Amazon Security Lake durch AWS globale Netzwerksicherheit geschützt. Informationen zu AWS-Sicherheitsdiensten und wie AWS die Infrastruktur schützt, finden Sie unter [AWS Cloud-Sicherheit](#). Informationen zum Entwerfen Ihrer AWS-Umgebung anhand der bewährten Methoden für die Infrastruktursicherheit finden Sie unter [Infrastrukturschutz](#) im Security Pillar AWS Well-Architected Framework.

Sie verwenden AWS veröffentlichte API-Aufrufe, um über das Netzwerk auf Security Lake zuzugreifen. Kunden müssen Folgendes unterstützen:

- Transport Layer Security (TLS). Wir benötigen TLS 1.2 und empfehlen TLS 1.3.
- Verschlüsselungs-Suiten mit Perfect Forward Secrecy (PFS) wie DHE (Ephemeral Diffie-Hellman) oder ECDHE (Elliptic Curve Ephemeral Diffie-Hellman). Die meisten modernen Systemen 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.

Konfigurations- und Schwachstellenanalyse in Security Lake

Konfiguration und IT-Steuerelemente unterliegen der übergreifenden Verantwortlichkeit von AWS und Ihnen, unserem Kunden. Weitere Informationen finden Sie unter [AWS Modell der übergreifenden Verantwortlichkeit](#).

Überwachen Sie

Amazon Lake AWS CloudTrail AWS-Service Dazu gehören Aktionen von der Security Lake-Konsole und programmatische Aufrufe von Security Lake-API-Vorgängen. Mithilfe der von gesammelten Informationen können Sie feststellen CloudTrail, welche Anfragen an Security Lake gestellt wurden.

3. Wählen Sie auf der Registerkarte Durchsuchen die Option Security Lake aus.
4. Wählen Sie „Quellversionsmetriken pro Konto“ oder „Metriken pro Quellversion“.
5. Wählen Sie eine Metrik aus, um sie im Detail anzuzeigen. Sie können auch Folgendes wählen:
 - Verwenden Sie die Spaltenüberschrift, um die Metriken zu sortieren.
 - Um eine Metriken grafisch darzustellen, müssen Sie einen Metriken grafisch Metriken, um eine Metriken grafisch darzustellen.
 - Um nach Metrik zu filtern, wählen Sie den Metriknamen aus und klicken Sie dann auf Zur Suche hinzufügen.

CloudWatch API

Verwenden Sie die [GetMetricStatistics](#)Aktion, um über die CloudWatch API auf Security Lake-Metriken zuzugreifen.

AWS CLI

Führen Sie den [get-metric-statistics](#)Befehl ausAWS CLI, um mit dem auf Security Lake-Metriken zuzugreifen.

Weitere Informationen zur Überwachung mithilfe von Metriken finden Sie unter [Verwenden von CloudWatch Amazon-Metriken](#) im CloudWatchAmazon-Benutzerhandbuch.

CloudWatchAlarmer für Security Lake-Metriken einrichten

Mit CloudWatch können Sie auch Alarmer für eine Metrik festlegen, die ausgelöst werden, wenn ein Schwellenwert erreicht wird. Sie könnten beispielsweise einen Alarm für die ProcessedSizeMetrik einrichten, sodass Sie benachrichtigt werden, wenn das Datenvolumen aus einer bestimmten Quelle einen bestimmten Schwellenwert überschreitet.

Anweisungen zum Einrichten von Alarmen finden Sie unter [Verwenden von CloudWatch Amazon-Alarmen](#) im CloudWatchAmazon-Benutzerhandbuch.

Protokollieren von Amazon Security Lake-API-Aufrufen mit AWS CloudTrail

Amazon Security Lake lässt sich in einen Dienst integrieren AWS CloudTrail, der eine Aufzeichnung der Aktionen bereitstellt, die von einem Benutzer, einer Rolle oder einem AWS Dienst in Security Lake ausgeführt wurden. CloudTrail erfasst API-Aufrufe für Security Lake als Ereignisse. Zu den erfassten Aufrufen gehören Aufrufe von der Security Lake-Konsole und Codeaufrufe für die Security Lake-API-Operationen. Wenn Sie einen Trail erstellen, können Sie die kontinuierliche Bereitstellung von CloudTrail Ereignissen an einen Amazon S3-Bucket aktivieren, einschließlich Ereignissen für Security Lake. Auch wenn Sie keinen Trail konfigurieren, können Sie die neuesten Ereignisse in der CloudTrail-Konsole in Event history (Ereignisverlauf) anzeigen. Anhand der gesammelten Informationen können Sie ermitteln CloudTrail, welche Anfrage an Security Lake gestellt wurde, die IP-Adresse, von der aus die Anfrage gestellt wurde, wer die Anfrage gestellt hat, wann sie gestellt wurde, und weitere Details.

Weitere Informationen zu CloudTrail finden Sie im [AWS CloudTrail-Benutzerhandbuch](#).

Informationen zu Security Lake in CloudTrail

CloudTrail wird beim Erstellen Ihres Kontos auf AWS-Konto aktiviert. Wenn in Security Lake eine Aktivität stattfindet, wird diese Aktivität zusammen mit anderen AWS Serviceereignissen in der CloudTrail Ereignishistorie in einem Ereignis aufgezeichnet. Sie können die neusten Ereignisse in Ihr(em) AWS-Konto anzeigen, suchen und herunterladen. Weitere Informationen finden Sie unter [Anzeigen von Ereignissen mit dem CloudTrail-Ereignisverlauf](#).

Erstellen Sie einen Pfad, um eine fortlaufende Aufzeichnung der Ereignisse in Ihrem AWS-Konto, einschließlich der Ereignisse für Security Lake, zu erhalten. Ein Trail ermöglicht CloudTrail die Übertragung von Ereignissen als Protokolldateien an einen von Ihnen angegebenen Amazon S3-Bucket. Wenn Sie einen Trail in der Konsole anlegen, gilt dieser für alle AWS-Regionen-Regionen. Der Trail protokolliert Ereignisse aus allen Regionen in der AWS-Partition und stellt die Protokolldateien in dem von Ihnen angegebenen Amazon S3 Bucket bereit. Darüber hinaus können Sie andere AWS-Services konfigurieren, um die in den CloudTrail-Protokollen erfassten Ereignisdaten weiter zu analysieren und entsprechend zu agieren. Weitere Informationen finden Sie unter:

- [Übersicht zum Erstellen eines Trails](#)

- [In CloudTrail unterstützte Services und Integrationen](#)
- [Konfigurieren von Amazon SNS-Benachrichtigungen für CloudTrail](#)
- [Empfangen von CloudTrail-Protokolldateien aus mehreren Regionen](#) und [Empfangen von CloudTrail-Protokolldateien aus mehreren Konten](#)

Security Lake-Aktionen werden von der [Security Lake API-Referenz](#) protokolliert CloudTrail und sind in dieser dokumentiert. Zum Beispiel werden durch Aufrufe der UpdateDataLake-, ListLogSources- und CreateSubscriber-Aktionen Einträge in den CloudTrail-Protokolldateien generiert.

Jeder Ereignis- oder Protokolleintrag enthält Informationen zu dem Benutzer, der die Anforderung generiert hat. Die Identitätsinformationen unterstützen Sie bei der Ermittlung der folgenden Punkte:

- Ob die Anforderung mit Root- oder AWS Identity and Access Management-Benutzeranmeldeinformationen ausgeführt wurde.
- Gibt an, ob die Anforderung mit temporären Sicherheitsanmeldeinformationen für eine Rolle oder einen verbundenen Benutzer gesendet wurde.
- Gibt an, ob die Anforderung aus einem anderen AWS-Service gesendet wurde

Weitere Informationen finden Sie unter [CloudTrail-Element userIdentity](#).

Grundlegendes zu Security Lake-Protokolldateieinträgen

CloudTrail-Protokolldateien können einen oder mehrere Einträge enthalten. Ein Ereignis stellt eine einzelne Anfrage aus einer beliebigen Quelle dar und enthält unter anderem Informationen über die angeforderte Aktion, das Datum und die Uhrzeit der Aktion sowie über die Anfrageparameter. CloudTrail-Protokolleinträge sind kein geordnetes Stacktrace der öffentlichen API-Aufrufe und erscheinen daher nicht in einer bestimmten Reihenfolge.

Das folgende Beispiel zeigt einen CloudTrail Protokolleintrag für die Security GetSubscriber Lake-Aktion.

```
{
  "eventVersion": "1.08",
  "userIdentity": {
    "type": "AssumedRole",
    "principalId": "AIDACKCEVSQ6C2EXAMPLE:user",
```

```
"arn": "arn:aws:sts::123456789012:assumed-role/Admin/user",
"accountId": "123456789012",
"accessKeyId": "AKIAIOSFODNN7EXAMPLE",
"sessionContext": {
  "sessionIssuer": {
    "type": "Role",
    "principalId": "AIDACKCEVSQ6C2EXAMPLE",
    "arn": "arn:aws:iam::123456789012:role/Admin",
    "accountId": "123456789012",
    "userName": "Admin"
  },
  "webIdFederationData": {
  },
  "attributes": {
    "creationDate": "2023-05-30T13:27:19Z",
    "mfaAuthenticated": "false"
  }
}
},
"eventTime": "2023-05-30T17:29:17Z",
"eventSource": "securitylake.amazonaws.com",
"eventName": "GetSubscriber",
"awsRegion": "us-east-1",
"sourceIPAddress": "198.51.100.1",
"userAgent": "console.amazonaws.com",
"requestParameters": {
  "subscriberId": "30ed17a3-0cac-4997-a41f-f5a6bexample"
},
"responseElements": null,
"requestID": "d01f0f32-9ec6-4579-af50-e9f14example",
"eventID": "9c1bff41-0f48-4ee6-921c-ebfd8example",
"readOnly": false,
"eventType": "AwsApiCall",
"managementEvent": true,
"recipientAccountId": "123456789012",
"eventCategory": "Management"
}
```

Markieren von Amazon Security Lake-Ressourcen

Ein Tag ist eine optionale Bezeichnung, die Sie definieren und AWS Ressourcen zuweisen können, einschließlich bestimmter Arten von Amazon-Security-Lake-Ressourcen. Tags können Ihnen helfen, Ressourcen auf unterschiedliche Weise zu identifizieren, zu kategorisieren und zu verwalten, z. B. nach Zweck, Eigentümer, Umgebung oder anderen Kriterien. Sie können beispielsweise Tags verwenden, um Richtlinien anzuwenden, Kosten zuzuweisen, zwischen Ressourcen zu unterscheiden oder Ressourcen zu identifizieren, die bestimmte Compliance-Anforderungen oder -Workflows unterstützen.

Sie können Tags den folgenden Arten von Security-Lake-Ressourcen zuweisen: Abonnenten und die Data-Lake-Konfiguration für Ihr AWS-Konto in einzelnen AWS-Regionen.

Themen

- [Grundlagen der Markierung](#)
- [Verwenden von Tags in IAM-Richtlinien](#)
- [Hinzufügen von Tags zu Amazon Security Lake-Ressourcen](#)
- [Überprüfen von Tags für Amazon Security Lake-Ressourcen](#)
- [Bearbeiten von Tags für Amazon Security Lake-Ressourcen](#)
- [Entfernen von Tags aus Amazon Security Lake-Ressourcen](#)

Grundlagen der Markierung

Eine Ressource kann bis zu 50 Tags enthalten. Jedes Tag besteht aus einem Schlüssel und einem optionalen Wert. Beides können Sie definieren. Ein Tag-Schlüssel ist eine allgemeine Bezeichnung, die als Kategorie für einen spezifischeren Tag-Wert dient. Ein Tag-Wert dient als Bezeichnung für einen Tag-Schlüssel.

Wenn Sie beispielsweise Abonnenten hinzufügen, um Sicherheitsdaten aus verschiedenen Umgebungen zu analysieren (einen Satz von Abonnenten für Cloud-Daten und einen anderen Satz für On-Premises-Daten), können Sie diesen Abonnenten einen `-Environment` Tag-Schlüssel zuweisen. Der zugehörige Tag-Wert kann `Cloud` für Abonnenten gelten, die Daten von analysieren AWS-Services, und `On-Premises` für die anderen.

Beachten Sie beim Definieren und Zuweisen von Tags zu Amazon Security Lake-Ressourcen Folgendes:

- Jede Ressource kann maximal 50 Tags haben.
- Für jede Ressource muss jeder Tag-Schlüssel eindeutig sein und kann nur einen Tag-Wert haben.
- Bei Tag-Schlüsseln und -Werten muss die Groß- und Kleinschreibung beachtet werden. Als bewährte Methode empfehlen wir Ihnen, eine Strategie für die Groß- und Kleinschreibung von Tags zu definieren und diese Strategie konsistent in Ihren -Ressourcen zu implementieren.
- Ein Tag-Schlüssel kann maximal 128 UTF-8-Zeichen enthalten. Ein Tag-Wert kann maximal 256 UTF-8-Zeichen enthalten. Die Zeichen können Buchstaben, Zahlen, Leerzeichen oder die folgenden Symbole sein: `_ . : / = + - @`
- Das `aws :` Präfix ist für die Verwendung durch reserviert AWS. Sie können es nicht in Tag-Schlüsseln oder -Werten verwenden, die Sie definieren. Darüber hinaus können Sie keine Tag-Schlüssel oder -Werte ändern oder entfernen, die dieses Präfix verwenden. Tags mit diesem Präfix werden beim Kontingent von 50 Tags pro Ressource nicht eingerechnet.
- Alle Tags, die Sie zuweisen, sind nur für Ihr AWS-Konto und nur in der verfügbar, AWS-Region in der Sie sie zuweisen.
- Wenn Sie einer Ressource mithilfe von Security Lake Tags zuweisen, werden die Tags nur auf die Ressource angewendet, die direkt in Security Lake in der entsprechenden gespeichert ist AWS-Region. Sie werden nicht auf zugeordnete, unterstützende Ressourcen angewendet, die Security Lake für Sie in anderen erstellt, verwendet oder verwaltet AWS-Services. Wenn Sie beispielsweise Ihrem Data Lake Tags zuweisen, werden die Tags nur auf Ihre Data-Lake-Konfiguration in Security Lake für die angegebene Region angewendet. Sie werden nicht auf den Amazon Simple Storage Service (Amazon S3)-Bucket angewendet, in dem Ihre Protokoll- und Ereignisdaten gespeichert werden. Um einer zugeordneten Ressource auch Tags zuzuweisen, können Sie AWS Resource Groups oder die verwenden AWS-Service , die die Ressource speichert, z. B. Amazon S3 für einen S3-Bucket. Das Zuweisen von Tags zu zugeordneten Ressourcen kann Ihnen helfen, unterstützende Ressourcen für Ihren Data Lake zu identifizieren.
- Wenn Sie eine Ressource löschen, werden alle Tags, die der Ressource zugewiesen sind, ebenfalls gelöscht.

Weitere Einschränkungen, Tipps und bewährte Methoden finden Sie unter [Markieren Ihrer - AWS Ressourcen](#) im Benutzerhandbuch zum Markieren von - AWS Ressourcen.

⚠ Important

Speichern Sie keine vertraulichen oder anderen Arten sensibler Daten in Tags. Auf Tags kann von vielen aus zugegriffen werden AWS-Services, einschließlich AWS Billing and Cost Management. Sie sind nicht für die Verwendung mit sensiblen Daten gedacht.

Um Tags für Security-Lake-Ressourcen hinzuzufügen und zu verwalten, können Sie die Security-Lake-Konsole oder die Security-Lake-API verwenden.

Verwenden von Tags in IAM-Richtlinien

Nachdem Sie mit dem Markieren von Ressourcen begonnen haben, können Sie tagbasierte Berechtigungen auf Ressourcenebene in AWS Identity and Access Management (IAM)-Richtlinien definieren. Durch die Verwendung von Tags auf diese Weise können Sie eine detaillierte Kontrolle darüber implementieren, welche Benutzer und Rollen in Ihrem über die Berechtigung zum Erstellen und Markieren von Ressourcen AWS-Konto verfügen und welche Benutzer und Rollen über die Berechtigung zum Hinzufügen, Bearbeiten und Entfernen von Tags verfügen. Um den Zugriff basierend auf Tags zu steuern, können Sie [tagbezogene Bedingungsschlüssel](#) im [Bedingungelement](#) von IAM-Richtlinien verwenden.

Sie können beispielsweise eine Richtlinie erstellen, die einem Benutzer vollen Zugriff auf alle Amazon Security Lake-Ressourcen ermöglicht, wenn das Owner Tag für die Ressource seinen Benutzernamen angibt:

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Sid": "ModifyResourceIfOwner",
      "Effect": "Allow",
      "Action": "securitylake:*",
      "Resource": "*",
      "Condition": {
        "StringEqualsIgnoreCase": {"aws:ResourceTag/Owner": "${aws:username}"}
      }
    }
  ]
}
```

Wenn Sie Tag-basierte Berechtigungen auf Ressourcenebene definieren, werden die Berechtigungen sofort wirksam. Dies bedeutet, dass Ihre Ressourcen besser geschützt sind, sobald sie erstellt wurden, und Sie schnell damit beginnen können, die Verwendung von Tags für neue Ressourcen zu erzwingen. Mithilfe von Berechtigungen auf Ressourcenebene können Sie auch steuern, welche Tag-Schlüssel und -Werte können mit neuen und vorhandenen Ressourcen verknüpft werden können. Weitere Informationen finden Sie unter [Steuern des Zugriffs auf AWS Ressourcen mithilfe von Tags](#) im IAM-Benutzerhandbuch.

Hinzufügen von Tags zu Amazon Security Lake-Ressourcen

Um einer Amazon Security Lake-Ressource Tags hinzuzufügen, können Sie die Security Lake-Konsole oder die Security Lake-API verwenden.

Important

Das Hinzufügen von Tags zu einer Ressource kann sich auf den Zugriff auf die Ressource auswirken. Bevor Sie einer Ressource ein Tag hinzufügen, überprüfen Sie alle AWS Identity and Access Management (IAM)-Richtlinien, die möglicherweise Tags verwenden, um den Zugriff auf Ressourcen zu steuern.

Console

Wenn Sie Security Lake für einen aktivieren AWS-Region oder einen Abonnenten erstellen, bietet die Security-Lake-Konsole Optionen zum Hinzufügen von Tags zur Ressource – die Data-Lake-Konfiguration für die Region oder den Abonnenten. Folgen Sie den Anweisungen in der Konsole, um der Ressource beim Erstellen der Ressource Tags hinzuzufügen.

Gehen Sie folgendermaßen vor, um einer vorhandenen Ressource mithilfe der Security-Lake-Konsole ein oder mehrere Tags hinzuzufügen.

So fügen Sie einer Ressource einen Tag hinzu

1. Öffnen Sie die Security-Lake-Konsole unter <https://console.aws.amazon.com/securitylake/>.
2. Führen Sie je nach Ressourcentyp, dem Sie ein Tag hinzufügen möchten, einen der folgenden Schritte aus:
 - Wählen Sie für eine Data-Lake-Konfiguration im Navigationsbereich Regionen aus. Wählen Sie dann in der Tabelle Regionen die Region aus.

- Wählen Sie für einen Abonnenten im Navigationsbereich **Subscribers** aus. Wählen Sie dann in der Tabelle **Meine Abonnenten** den Abonnenten aus.

Wenn der Abonnent nicht in der Tabelle angezeigt wird, verwenden Sie die AWS-Region Auswahl in der oberen rechten Ecke der Seite, um die Region auszuwählen, in der Sie den Abonnenten erstellt haben. Die Tabelle listet vorhandene Abonnenten nur für die aktuelle Region auf.

3. Wählen Sie **Bearbeiten** aus.
4. Erweitern Sie den Abschnitt **Tags**. In diesem Abschnitt werden alle Tags aufgeführt, die derzeit der Ressource zugewiesen sind.
5. Klicken Sie im Abschnitt **Tags** auf **Neuen Tag hinzufügen**.
6. Geben Sie im Feld **Schlüssel** den Tag-Schlüssel für das Tag ein, das der Ressource hinzugefügt werden soll. Geben Sie dann im Feld **Wert** optional einen Tag-Wert für den Schlüssel ein.

Ein Tag-Schlüssel kann bis zu 128 Zeichen enthalten. Ein Tag-Wert kann bis zu 256 Zeichen enthalten. Die Zeichen können Buchstaben, Zahlen, Leerzeichen oder die folgenden Symbole sein: `_ . : / = + - @`

7. Um der Ressource ein weiteres Tag hinzuzufügen, wählen Sie **Neues Tag hinzufügen** und wiederholen Sie dann den vorherigen Schritt. Sie können einer Ressource bis zu 50 Tags zuweisen.
8. Wenn Sie mit dem Hinzufügen von Tags fertig sind, wählen Sie **Speichern** aus.

API

Um eine Ressource zu erstellen und ihr programmgesteuert ein oder mehrere Tags hinzuzufügen, verwenden Sie die entsprechende **Create Operation** für den Ressourcentyp, den Sie erstellen möchten:

- **Data-Lake-Konfiguration** – Verwenden Sie die [-CreateDataLake](#) Operation oder, wenn Sie die AWS Command Line Interface (AWS CLI) verwenden, führen Sie den [create-data-lake](#) Befehl aus.
- **Subscriber** – Verwenden Sie die [-CreateSubscriber](#) Operation oder AWS CLI führen Sie bei Verwendung der den Befehl [create-subscriber](#) aus.

Verwenden Sie in Ihrer Anforderung den `tags` Parameter , um den Tag-Schlüssel (`key`) und den optionalen Tag-Wert (`value`) für jedes Tag anzugeben, das der Ressource hinzugefügt werden soll. Der `tags` Parameter gibt ein Array von -Objekten an. Jedes Objekt gibt einen Tag-Schlüssel und den zugehörigen Tag-Wert an.

Um einer vorhandenen Ressource ein oder mehrere Tags hinzuzufügen, verwenden Sie die [-TagResource](#) Operation der Security-Lake-API oder AWS CLI führen Sie bei Verwendung der den Befehl [tag-resource](#) aus. Geben Sie in Ihrer Anfrage den Amazon-Ressourcennamen (ARN) der Ressource an, der Sie ein Tag hinzufügen möchten. Verwenden Sie den `tags` Parameter , um den Tag-Schlüssel (`key`) und den optionalen Tag-Wert (`value`) für jedes hinzuzufügende Tag anzugeben. Wie bei `Create` Operationen und Befehlen gibt der `tags` Parameter ein Array von Objekten, ein Objekt für jeden Tag-Schlüssel und den zugehörigen Tag-Wert an.

Der folgende AWS CLI Befehl fügt beispielsweise dem angegebenen Subscriber einen `Environment` Tag-Schlüssel mit einem `Cloud` Tag-Wert hinzu. Dieses Beispiel ist für Linux, macOS oder Unix formatiert und verwendet den umgekehrten Schrägstrich (`\`) zur Verbesserung der Lesbarkeit.

```
$ aws securitylake tag-resource \  
--resource-arn arn:aws:securitylake:us-  
east-1:123456789012:subscriber/1234abcd-12ab-34cd-56ef-1234567890ab \  
--tags key=Environment,value=Cloud
```

Wobei gilt:

- `resource-arn` gibt den ARN des Abonnenten an, dem ein Tag hinzugefügt werden soll.
- `Environment` ist der Tag-Schlüssel des Tags, das dem Abonnenten hinzugefügt werden soll.
- `Cloud` ist der Tag-Wert für den angegebenen Tag-Schlüssel (`Environment`).

Im folgenden Beispiel fügt der Befehl dem Abonnenten mehrere Tags hinzu.

```
$ aws securitylake tag-resource \  
--resource-arn arn:aws:securitylake:us-  
east-1:123456789012:subscriber/1234abcd-12ab-34cd-56ef-1234567890ab \  
--tags key=Environment,value=Cloud key=CostCenter,value=12345 key=Owner,value=jane-  
doe
```

Für jedes Objekt in einem `key value tagsArray` sind sowohl die Argumente als auch erforderlich. Der Wert für das `value` Argument kann jedoch eine leere Zeichenfolge sein. Wenn

Sie einem Tag-Schlüssel keinen Tag-Wert zuordnen möchten, geben Sie keinen Wert für das `value` Argument an. Der folgende Befehl fügt beispielsweise einen `-Owner` Tag-Schlüssel ohne zugeordneten Tag-Wert hinzu:

```
$ aws securitylake tag-resource \  
--resource-arn arn:aws:securitylake:us-  
east-1:123456789012:subscriber/1234abcd-12ab-34cd-56ef-1234567890ab \  
--tags key=Owner,value=
```

Wenn ein Tagging-Vorgang erfolgreich ist, gibt Security Lake eine leere HTTP 200-Antwort zurück. Andernfalls gibt Security Lake eine HTTP 4xx- oder 500-Antwort zurück, die angibt, warum der Vorgang fehlgeschlagen ist.

Überprüfen von Tags für Amazon Security Lake-Ressourcen

Sie können die Tags (sowohl Tag-Schlüssel als auch Tag-Werte) für eine Amazon-Security-Lake-Ressource mithilfe der Security-Lake-Konsole oder der Security-Lake-API überprüfen.

Console

Gehen Sie wie folgt vor, um die Tags einer Ressource mithilfe der Security-Lake-Konsole zu überprüfen.

So überprüfen Sie die Tags für eine Ressource

1. Öffnen Sie die Security-Lake-Konsole unter <https://console.aws.amazon.com/securitylake/>.
2. Führen Sie je nach Typ der Ressource, deren Tags Sie überprüfen möchten, einen der folgenden Schritte aus:
 - Wählen Sie für eine Data-Lake-Konfiguration im Navigationsbereich Regionen aus. Wählen Sie in der Tabelle Regionen die Region und dann Bearbeiten aus. Erweitern Sie dann den Abschnitt Tags.
 - Wählen Sie für einen Abonnenten im Navigationsbereich Subscribers aus. Wählen Sie dann in der Tabelle Meine Abonnenten den Namen des Abonnenten aus.

Wenn der Abonnent nicht in der Tabelle angezeigt wird, verwenden Sie die AWS-Region Auswahl in der oberen rechten Ecke der Seite, um die Region auszuwählen, in der Sie den Abonnenten erstellt haben. Die Tabelle listet vorhandene Abonnenten nur für die aktuelle Region auf.

Der Abschnitt `Tags` listet alle Tags auf, die derzeit der Ressource zugewiesen sind.

API

Um die Tags für eine vorhandene Ressource programmgesteuert abzurufen und zu überprüfen, verwenden Sie die [ListTagsForResource](#) Operation der Security-Lake-API. Verwenden Sie in Ihrer Anforderung den `resourceArn` Parameter, um den Amazon-Ressourcennamen (ARN) der Ressource anzugeben.

Wenn Sie die AWS Command Line Interface (AWS CLI) verwenden, führen Sie den [list-tags-for-resource](#) Befehl aus und geben Sie mit dem `resource-arn` Parameter den ARN der Ressource an. Beispielsweise:

```
$ aws securitylake list-tags-for-resource --resource-arn arn:aws:securitylake:us-east-1:123456789012:subscriber/1234abcd-12ab-34cd-56ef-1234567890ab
```

Im vorherigen Beispiel ist *arn:aws:securitylake:us-east-1:123456789012:subscriber/1234abcd-12ab-34cd-56ef-1234567890ab* der ARN eines vorhandenen Subscribers.

Wenn der Vorgang erfolgreich ist, gibt Security Lake ein `tagsArray` zurück. Jedes Objekt im Array gibt ein Tag an (sowohl den Tag-Schlüssel als auch den Tag-Wert), das derzeit der Ressource zugewiesen ist. Beispielsweise:

```
{
  "tags": [
    {
      "key": "Environment",
      "value": "Cloud"
    },
    {
      "key": "CostCenter",
      "value": "12345"
    },
    {
      "key": "Owner",
      "value": ""
    }
  ]
}
```

Wobei `Environment`, `CostCenter` und die Tag-Schlüssel `Owner` sind, die der Ressource zugewiesen sind. `Cloud` ist der Tag-Wert, der dem `Environment` Tag-Schlüssel zugeordnet ist. `12345` ist der Tag-Wert, der dem `CostCenter` Tag-Schlüssel zugeordnet ist. Dem `Owner` Tag-Schlüssel ist kein Tag-Wert zugeordnet.

Bearbeiten von Tags für Amazon Security Lake-Ressourcen

Um die Tags (Tag-Schlüssel oder Tag-Werte) für eine Amazon-Security-Lake-Ressource zu bearbeiten, können Sie die Security-Lake-Konsole oder die Security-Lake-API verwenden.

Important

Das Bearbeiten der Tags für eine Ressource kann sich auf den Zugriff auf die Ressource auswirken. Bevor Sie einen Tag-Schlüssel oder -Wert für eine Ressource bearbeiten, überprüfen Sie alle AWS Identity and Access Management (IAM)-Richtlinien, die das Tag verwenden könnten, um den Zugriff auf Ressourcen zu steuern.

Console

Gehen Sie wie folgt vor, um die Tags einer Ressource mithilfe der Security-Lake-Konsole zu bearbeiten.

So bearbeiten Sie die Tags für eine Ressource

1. Öffnen Sie die Security-Lake-Konsole unter <https://console.aws.amazon.com/securitylake/>.
2. Führen Sie je nach Typ der Ressource, deren Tags Sie bearbeiten möchten, einen der folgenden Schritte aus:
 - Wählen Sie für eine Data-Lake-Konfiguration im Navigationsbereich `Regionen` aus. Wählen Sie dann in der Tabelle `Regionen` die `Region` aus.
 - Wählen Sie für einen Abonnenten im Navigationsbereich `Subscribers` aus. Wählen Sie dann in der Tabelle `Meine Abonnenten` den `Abonnenten` aus.

Wenn der Abonnent nicht in der Tabelle angezeigt wird, verwenden Sie die AWS-Region Auswahl in der oberen rechten Ecke der Seite, um die Region auszuwählen, in der Sie den Abonnenten erstellt haben. Die Tabelle listet vorhandene Abonnenten nur für die aktuelle Region auf.

3. Wählen Sie Bearbeiten aus.
4. Erweitern Sie den Abschnitt Tags. Der Abschnitt Tags listet alle Tags auf, die derzeit der Ressource zugewiesen sind.
5. Führen Sie eine der folgenden Aktionen aus:
 - Um einem vorhandenen Tag-Schlüssel einen Tag-Wert hinzuzufügen, geben Sie den Wert in das Feld Wert neben dem Tag-Schlüssel ein.
 - Um einen vorhandenen Tag-Schlüssel zu ändern, wählen Sie neben dem Tag Entfernen aus. Wählen Sie dann Neues Tag hinzufügen aus. Geben Sie im daraufhin angezeigten Feld Schlüssel den neuen Tag-Schlüssel ein. Geben Sie optional einen zugehörigen Tag-Wert in das Feld Wert ein.
 - Um einen vorhandenen Tag-Wert zu ändern, wählen Sie X im Feld Wert, das den Wert enthält. Geben Sie dann den neuen Tag-Wert in das Feld Wert ein.
 - Um einen vorhandenen Tag-Wert zu entfernen, wählen Sie X im Feld Wert, das den Wert enthält.
 - Um ein vorhandenes Tag (sowohl den Tag-Schlüssel als auch den Tag-Wert) zu entfernen, wählen Sie neben dem Tag Entfernen aus.

Eine Ressource kann bis zu 50 Tags enthalten. Ein Tag-Schlüssel kann bis zu 128 Zeichen enthalten. Ein Tag-Wert kann bis zu 256 Zeichen enthalten. Die Zeichen können Buchstaben, Zahlen, Leerzeichen oder die folgenden Symbole sein: `_ . : / = + - @`

6. Wenn Sie mit der Bearbeitung der Tags fertig sind, wählen Sie Speichern aus.

API

Wenn Sie ein Tag für eine Ressource programmgesteuert bearbeiten, überschreiben Sie das vorhandene Tag mit neuen Werten. Daher hängt die beste Methode zum Bearbeiten eines Tags davon ab, ob Sie einen Tag-Schlüssel, einen Tag-Wert oder beides bearbeiten möchten. Um einen Tag-Schlüssel zu bearbeiten, [entfernen Sie das aktuelle Tag](#) und [fügen Sie ein neues Tag](#) hinzu.

Um nur den Tag-Wert zu bearbeiten oder zu entfernen, der einem Tag-Schlüssel zugeordnet ist, überschreiben Sie den vorhandenen Wert mithilfe der [-TagResource](#) Operation der Security-Lake-API. Wenn Sie die AWS Command Line Interface (AWS CLI) verwenden, führen Sie den Befehl [tag-resource](#) aus. Geben Sie in Ihrer Anfrage den Amazon-Ressourcennamen (ARN) der Ressource an, deren Tag-Wert Sie bearbeiten oder entfernen möchten.

Um einen Tag-Wert zu bearbeiten, verwenden Sie den `tags` Parameter, um den Tag-Schlüssel anzugeben, dessen Tag-Wert Sie ändern möchten. Geben Sie auch den neuen Tag-Wert für den Schlüssel an. Mit dem folgenden AWS CLI Befehl wird beispielsweise der Tag-Wert `Cloud On-Premises` für den `Environment` Tag-Schlüssel, der dem angegebenen Subscriber zugewiesen ist, von `in` geändert. Dieses Beispiel ist für Linux, macOS oder Unix formatiert und verwendet den umgekehrten Schrägstrich (`\`) zur Verbesserung der Lesbarkeit.

```
$ aws securitylake tag-resource \  
--resource-arn arn:aws:securitylake:us-east-1:123456789012:subscriber/1234abcd-12ab-34cd-56ef-1234567890ab \  
--tags key=Environment,value=On-Premises
```

Wobei gilt:

- `resource-arn` gibt den ARN des Abonnenten an.
- `Environment` ist der Tag-Schlüssel, der dem zu ändernden Tag-Wert zugeordnet ist.
- `On-Premises` ist der neue Tag-Wert für den angegebenen Tag-Schlüssel (`Environment`).

Um einen Tag-Wert aus einem Tag-Schlüssel zu entfernen, geben Sie keinen Wert für das `value` Argument des Schlüssels im `tags` Parameter an. Beispielsweise:

```
$ aws securitylake tag-resource \  
--resource-arn arn:aws:securitylake:us-east-1:123456789012:subscriber/1234abcd-12ab-34cd-56ef-1234567890ab \  
--tags key=owner,value=
```

Wenn der Vorgang erfolgreich ist, gibt Security Lake eine leere HTTP 200-Antwort zurück. Andernfalls gibt Security Lake eine HTTP 4xx- oder 500-Antwort zurück, die angibt, warum der Vorgang fehlgeschlagen ist.

Entfernen von Tags aus Amazon Security Lake-Ressourcen

Um Tags aus einer Amazon-Security-Lake-Ressource zu entfernen, können Sie die Security-Lake-Konsole oder die Security-Lake-API verwenden.

⚠ Important

Das Entfernen von Tags aus einer Ressource kann sich auf den Zugriff auf die Ressource auswirken. Bevor Sie ein Tag entfernen, überprüfen Sie alle AWS Identity and Access Management (IAM)-Richtlinien, die das Tag verwenden könnten, um den Zugriff auf - Ressourcen zu steuern.

Console

Gehen Sie wie folgt vor, um ein oder mehrere Tags mithilfe der Security-Lake-Konsole aus einer Ressource zu entfernen.

So entfernen Sie ein Tag aus einer Ressource

1. Öffnen Sie die Security-Lake-Konsole unter <https://console.aws.amazon.com/securitylake/>.
2. Führen Sie je nach Ressourcentyp, aus dem Sie ein Tag entfernen möchten, einen der folgenden Schritte aus:
 - Wählen Sie für eine Data-Lake-Konfiguration im Navigationsbereich Regionen aus. Wählen Sie dann in der Tabelle Regionen die Region aus.
 - Wählen Sie für einen Abonnenten im Navigationsbereich Subscribers aus. Wählen Sie dann in der Tabelle Meine Abonnenten den Abonnenten aus.

Wenn der Abonnent nicht in der Tabelle angezeigt wird, verwenden Sie die AWS-Region Auswahl in der oberen rechten Ecke der Seite, um die Region auszuwählen, in der Sie den Abonnenten erstellt haben. Die Tabelle listet vorhandene Abonnenten nur für die aktuelle Region auf.

3. Wählen Sie Bearbeiten aus.
4. Erweitern Sie den Abschnitt Tags. Der Abschnitt Tags listet alle Tags auf, die derzeit der Ressource zugewiesen sind.
5. Führen Sie eine der folgenden Aktionen aus:
 - Um nur den Tag-Wert für ein Tag zu entfernen, wählen Sie X im Feld Wert aus, das den zu entfernenden Wert enthält.
 - Um sowohl den Tag-Schlüssel als auch den Tag-Wert (als Paar) für ein Tag zu entfernen, wählen Sie Entfernen neben dem zu entfernenden Tag aus.

- Um zusätzliche Tags aus der Ressource zu entfernen, wiederholen Sie den vorherigen Schritt für jedes zusätzliche Tag, das entfernt werden soll.
- Wenn Sie mit dem Entfernen von Tags fertig sind, wählen Sie Speichern aus.

API

Um ein oder mehrere Tags programmgesteuert aus einer Ressource zu entfernen, verwenden Sie die [UntagResource](#) Operation der Security-Lake-API. Verwenden Sie in Ihrer Anforderung den `resourceArn` Parameter, um den Amazon-Ressourcennamen (ARN) der Ressource anzugeben, aus der ein Tag entfernt werden soll. Verwenden Sie den `tagKeys` Parameter, um den Tag-Schlüssel des zu entfernenden Tags anzugeben. Um mehrere Tags zu entfernen, fügen Sie den `tagKeys` Parameter und das Argument für jedes zu entfernende Tag an, getrennt durch ein `-`-Zeichen (&), z. B. `tagKeys=key1&tagKeys=key2`. Um nur einen bestimmten Tag-Wert (kein Tag-Schlüssel) aus einer Ressource zu entfernen, [bearbeiten Sie das Tag](#), anstatt das Tag zu entfernen.

Wenn Sie die AWS Command Line Interface (AWS CLI) verwenden, führen Sie den Befehl [untag-resource](#) aus, um ein oder mehrere Tags aus einer Ressource zu entfernen. Geben Sie für den `resource-arn` Parameter den ARN der Ressource an, aus der ein Tag entfernt werden soll. Verwenden Sie den `tag-keys` Parameter, um den Tag-Schlüssel des zu entfernenden Tags anzugeben. Mit dem folgenden Befehl wird beispielsweise das `Environment` Tag (sowohl der Tag-Schlüssel als auch der Tag-Wert) aus dem angegebenen Subscriber entfernt:

```
$ aws securitylake untag-resource \
--resource-arn arn:aws:securitylake:us-
east-1:123456789012:subscriber/1234abcd-12ab-34cd-56ef-1234567890ab \
--tag-keys Environment
```

Gibt den ARN des Abonnenten `resource-arn` an, aus dem ein Tag entfernt werden soll, und `Environment` ist der Tag-Schlüssel des zu entfernenden Tags.

Um mehrere Tags aus einer Ressource zu entfernen, fügen Sie jeden zusätzlichen Tag-Schlüssel als Argument für den Parameter `tag-keys` hinzu. Beispielsweise:

```
$ aws securitylake untag-resource \
--resource-arn arn:aws:securitylake:us-
east-1:123456789012:subscriber/1234abcd-12ab-34cd-56ef-1234567890ab \
--tag-keys Environment Owner
```

Wenn der Vorgang erfolgreich ist, gibt Security Lake eine leere HTTP 200-Antwort zurück. Andernfalls gibt Security Lake eine HTTP 4xx- oder 500-Antwort zurück, die angibt, warum der Vorgang fehlgeschlagen ist.

Problembhebung bei Amazon Security Lake

Lesen Sie die folgenden Themen, falls Sie bei der Verwendung von Security Lake auf Probleme stoßen.

Fehlerbehebung beim Data Lake-Status

Auf der Seite Probleme der Security Lake-Konsole finden Sie eine Zusammenfassung der Probleme, die Ihren Data Lake betreffen. Beispielsweise kann Security Lake die Protokollerfassung für AWS CloudTrail Verwaltungsereignisse nicht aktivieren, wenn Sie keinen CloudTrail Trail für Ihre Organisation erstellt haben. Auf der Seite Probleme werden Probleme behandelt, die in den letzten 14 Tagen aufgetreten sind. Sie können eine Beschreibung der einzelnen Probleme und die vorgeschlagenen Schritte zur Problembhebung einsehen.

Um programmgesteuert auf eine Zusammenfassung der Probleme zuzugreifen, können Sie den [ListDataLakeExceptions](#) Betrieb der Security Lake-API verwenden. Wenn Sie den verwenden AWS CLI, führen Sie den [list-data-lake-exceptions](#) Befehl aus. Für den `regions` Parameter können Sie einen oder mehrere Regioncodes angeben, z. B. für die Region USA Ost (Nord-Virginia), `us-east-1` um sich über die Probleme zu informieren, die diese Regionen betreffen. Wenn Sie den `regions` Parameter nicht angeben, werden Probleme zurückgegeben, die alle Regionen betreffen. Eine Liste der Regioncodes finden Sie unter [Amazon Security Lake-Endpoints](#) in der Allgemeine AWS-Referenz.

Der folgende AWS CLI Befehl listet beispielsweise Probleme auf, die sich auf die `eu-west-3` Regionen `us-east-1` und auswirken. Dieses Beispiel ist für Linux, macOS oder Unix formatiert und verwendet den umgekehrten Schrägstrich (`\`) zur Verbesserung der Lesbarkeit.

```
$ aws securitylake list-data-lake-exceptions \  
--regions "us-east-1" "eu-west-3"
```

Verwenden Sie den [CreateDataLakeExceptionSubscription](#) Betrieb der Security Lake-API, um einen Security Lake-Benutzer über ein Problem oder einen Fehler zu informieren. Der Benutzer kann per E-Mail, Lieferung an eine Amazon Simple Queue Service (Amazon SQS) -Warteschlange, Lieferung an eine AWS Lambda Funktion oder ein anderes unterstütztes Protokoll benachrichtigt werden.

Mit dem folgenden AWS CLI Befehl werden beispielsweise Benachrichtigungen über Security Lake-Ausnahmen per SMS-Versand an das angegebene Konto gesendet. Dieses Beispiel ist für Linux,

macOS oder Unix formatiert und verwendet den umgekehrten Schrägstrich (\) zur Verbesserung der Lesbarkeit.

```
$ aws securitylake create-data-lake-exception-subscription \  
--notification-endpoint "123456789012" \  
--exception-time-to-live 30 \  
--subscription-protocol "sms"
```

Um Details zu einem Ausnahmeabonnement anzuzeigen, können Sie den [GetDataLakeExceptionSubscription](#) Vorgang verwenden. Um ein Ausnahmeabonnement zu aktualisieren, können Sie den [UpdateDataLakeExceptionSubscription](#) Vorgang verwenden. Um ein Ausnahmeabonnement zu löschen und Benachrichtigungen zu beenden, können Sie den [DeleteDataLakeExceptionSubscription](#) Vorgang verwenden.

Behebung von Problemen mit Lake Formation

Verwenden Sie die folgenden Informationen, um häufig auftretende Probleme zu diagnostizieren und zu beheben, die bei der Arbeit mit Security Lake und AWS Lake Formation Datenbanken oder Tabellen auftreten können. Weitere Themen zur Problembehandlung bei Lake Formation finden Sie im Abschnitt [zur Fehlerbehebung](#) im AWS Lake Formation Entwicklerhandbuch.

Die Tabelle wurde nicht gefunden

Möglicherweise wird dieser Fehler angezeigt, wenn Sie versuchen, einen Abonnenten zu erstellen.

Um diesen Fehler zu beheben, stellen Sie sicher, dass Sie bereits Quellen in der Region hinzugefügt haben. Wenn Sie Quellen hinzugefügt haben, als der Security Lake-Dienst in der Vorschauversion war, müssen Sie sie erneut hinzufügen, bevor Sie einen Abonnenten erstellen können. Weitere Informationen zum Hinzufügen von Quellen finden Sie unter [Quellmanagement](#).

400 AccessDenied

Möglicherweise erhalten Sie diesen Fehler, wenn Sie [eine benutzerdefinierte Quelle hinzufügen](#) und die `CreateCustomLogSource` API aufrufen.

Um den Fehler zu beheben, überprüfen Sie Ihre Lake Formation Berechtigungen. Die IAM-Rolle, die die API aufruft, sollte über die Berechtigungen zum Erstellen von Tabellen für die Security Lake-Datenbank verfügen. Weitere Informationen finden Sie unter [Gewähren von](#)

[Datenbankberechtigungen mithilfe der Lake Formation Formation-Konsole und der Methode für benannte Ressourcen](#) im AWS Lake Formation Entwicklerhandbuch.

SYNTAX_ERROR: Zeile 1:8: SELECT * ist für eine Beziehung, die keine Spalten hat, nicht zulässig

Möglicherweise erhalten Sie diesen Fehler, wenn Sie eine Quelltablelle zum ersten Mal in Lake Formation abfragen.

Um den Fehler zu beheben, erteilen Sie der IAM-Rolle, die Sie verwenden, die SELECT Berechtigung, wenn Sie bei Ihrem angemeldet sind. AWS-Konto Anweisungen zum Erteilen SELECT von [Berechtigungen finden Sie unter Erteilen von Tabellenberechtigungen mithilfe der Lake Formation Formation-Konsole und der benannten Ressourcenmethode](#) im AWS Lake Formation Entwicklerhandbuch.

Security Lake konnte den Prinzipal-ARN des Anrufers nicht zum Lake Formation Data Lake Admin hinzufügen. Aktuelle Data Lake-Administratoren schließen möglicherweise ungültige Principals ein, die nicht mehr existieren.

Dieser Fehler wird möglicherweise angezeigt, wenn Sie Security Lake aktivieren oder eine AWS-Service als Protokollquelle hinzufügen.

Gehen Sie wie folgt vor, um den Fehler zu beheben:

1. Öffnen Sie die Lake-Formation-Konsole unter <https://console.aws.amazon.com/lakeformation/>.
2. Melden Sie sich als Administratorbenutzer an.
3. Wählen Sie im Navigationsbereich unter Berechtigungen die Option Administrative Rollen und Aufgaben aus.
4. Wählen Sie im Abschnitt Data Lake-Administratoren die Option Administratoren auswählen aus.
5. Löschen Sie die Hauptbenutzer mit der Bezeichnung Nicht in IAM gefunden, und wählen Sie dann Speichern aus.
6. Führen Sie den Security Lake-Vorgang erneut aus.

Security Lake CreateSubscriber with Lake Formation hat keine neue Einladung zur gemeinsamen Nutzung von RAM-Ressourcen erstellt, um akzeptiert zu werden

Dieser Fehler wird möglicherweise angezeigt, wenn Sie Ressourcen mit [Lake Formation Version 2 oder Version 3 für die kontoübergreifende Datenfreigabe](#) gemeinsam genutzt haben, bevor Sie einen Lake Formation Formation-Abonnenten in Security Lake erstellt haben. Dies liegt daran, dass die kontoübergreifende Nutzung von Lake Formation Version 2 und Version 3 die Anzahl der AWS RAM-Ressourcenfreigaben optimiert, indem mehrere kontoübergreifende Berechtigungsberechtigungen einer AWS RAM-Ressourcenfreigabe zugeordnet werden.

Vergewissern Sie sich, dass der Name der Ressourcenfreigabe die externe ID hat, die Sie bei der Erstellung des Abonnenten angegeben haben, und dass der Resource Share-ARN mit dem ARN in der CreateSubscriber Antwort übereinstimmt.

Problembehandlung bei Abfragen in Amazon Athena

Verwenden Sie die folgenden Informationen, um allgemeine Probleme zu diagnostizieren und zu beheben, die auftreten können, wenn Sie Athena verwenden, um Objekte abzufragen, die in Ihrem Security Lake S3-Bucket gespeichert sind. Weitere Themen zur Athena-Fehlerbehebung finden Sie im Abschnitt [Fehlerbehebung in Athena](#) im Amazon Athena Athena-Benutzerhandbuch.

Beim Abfragen werden keine neuen Objekte im Data Lake zurückgegeben

Ihre Athena-Abfrage gibt möglicherweise keine neuen Objekte in Ihrem Data Lake zurück, selbst wenn der S3-Bucket für Security Lake diese Objekte enthält. Dies kann der Fall sein, wenn Sie Security Lake deaktiviert und dann wieder aktiviert haben. Das hat zur Folge, dass die AWS Glue Partitionen die neuen Objekte möglicherweise nicht richtig registrieren.

Gehen Sie wie folgt vor, um den Fehler zu beheben:

1. Öffnen Sie die AWS Lambda Konsole unter <https://console.aws.amazon.com/lambda/>.
2. Wählen Sie in der Navigationsleiste in der Regionsauswahl die Region aus, in der Security Lake aktiviert ist, die Athena-Abfrage jedoch keine Ergebnisse zurückgibt.
3. *Wählen Sie im Navigationsbereich **Funktionen** und dann die Funktion **SecurityLake_Glue_Partition_Updater_Lambda_region** aus.*

4. Wählen Sie auf der Registerkarte Konfigurationen die Option Trigger aus.
5. Wählen Sie die Option neben der Funktion aus und klicken Sie auf Bearbeiten.
6. Wählen Sie Auslöser aktivieren und dann Speichern aus. Dadurch wird der Funktionsstatus auf Aktiviert gesetzt.

Auf AWS Glue Tabellen kann nicht zugegriffen werden

Ein Abonnent für den Abfragezugriff kann möglicherweise nicht auf AWS Glue Tabellen zugreifen, die Security Lake-Daten enthalten.

Stellen Sie zunächst sicher, dass Sie die unter beschriebenen Schritte befolgt haben [Einrichtung der kontenübergreifenden gemeinsamen Nutzung von Tabellen \(Abonnentenschritt\)](#).

Wenn der Abonnent immer noch keinen Zugriff hat, gehen Sie wie folgt vor:

1. Öffnen Sie die AWS Glue Konsole unter <https://console.aws.amazon.com/glue/>.
2. Wählen Sie im Navigationsbereich Datenkatalog und Katalogeinstellungen aus.
3. Erteilen Sie dem Abonnenten die Erlaubnis, mit einer ressourcenbasierten Richtlinie auf die AWS Glue Tabellen zuzugreifen. Informationen zum Erstellen ressourcenbasierter Richtlinien finden Sie unter [Beispiele für ressourcenbasierte Richtlinien](#) im Entwicklerhandbuch. AWS Glue

Behebung von Problemen mit Organizations

Verwenden Sie die folgenden Informationen, um häufig auftretende Probleme zu diagnostizieren und zu beheben, die bei der Arbeit mit Security Lake und auftreten können AWS Organizations. Weitere Themen zur Problembehandlung für Organizations finden Sie im Abschnitt [Problembehandlung](#) des AWS Organizations Benutzerhandbuchs.

Beim Aufrufen des CreateDataLake Vorgangs ist ein Fehler aufgetreten: Ihr Konto muss das delegierte Administratorkonto für eine Organisation oder ein eigenständiges Konto sein.

[Dieser Fehler kann auftreten, wenn Sie die Organisation löschen, zu der ein delegiertes Administratorkonto gehörte, und dann versuchen, mit diesem Konto Security Lake mithilfe der Security Lake-Konsole oder der CreateData Lake-API einzurichten.](#)

Um den Fehler zu beheben, verwenden Sie ein delegiertes Administratorkonto einer anderen Organisation oder ein eigenständiges Konto.

Fehlerbehebung bei Identität und Zugriff auf Amazon Security Lake

Verwenden Sie die folgenden Informationen, um häufig auftretende Probleme zu diagnostizieren und zu beheben, die bei der Arbeit mit Security Lake und IAM auftreten können.

Ich bin nicht berechtigt, eine Aktion in Security Lake durchzuführen

Wenn Ihnen AWS Management Console mitgeteilt wird, dass Sie nicht berechtigt sind, eine Aktion durchzuführen, müssen Sie sich an Ihren Administrator wenden, um Unterstützung zu erhalten. Ihr Administrator ist die Person, die Ihnen Ihre Anmeldeinformationen zur Verfügung gestellt hat.

Der folgende Beispielfehler tritt auf, wenn der `mateojackson` IAM-Benutzer versucht, die Konsole zu verwenden, um Details zu einem fiktiven Objekt anzuzeigen, `subscriber` aber nicht über die fiktiven `SecurityLake:GetSubscriber` Berechtigungen verfügt.

```
User: arn:aws:iam::123456789012:user/mateojackson is not authorized to perform:
YOURSERVICEPREFIX:GetWidget on resource: my-example-widget
```

In diesem Fall bittet Mateo seinen Administrator, seine Richtlinien zu aktualisieren, damit er mithilfe der Aktion auf die `subscriber` Informationen zugreifen kann. `SecurityLake:GetSubscriber`

Ich bin nicht berechtigt, iam durchzuführen: PassRole

Wenn Sie die Fehlermeldung erhalten, dass Sie nicht autorisiert sind, die `iam:PassRole` Aktion auszuführen, müssen Ihre Richtlinien aktualisiert werden, damit Sie eine Rolle an Security Lake 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 Security Lake auszuführen. Die Aktion erfordert jedoch, dass der Service über Berechtigungen verfügt, die durch eine Servicerolle gewährt werden. Mary besitzt keine Berechtigungen für die Übergabe der Rolle an den Dienst.

```
User: arn:aws:iam::123456789012:user/marymajor is not authorized to perform:  
iam:PassRole
```

In diesem Fall müssen die Richtlinien von Mary aktualisiert werden, um die Aktion `iam:PassRole` ausführen zu können.

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 Security Lake-Ressourcen ermöglichen

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 Security Lake diese Funktionen unterstützt, finden Sie unter [So funktioniert Amazon Security Lake mit IAM](#).
- Informationen dazu, wie Sie Zugriff auf Ihre Ressourcen gewähren können, AWS-Konten die Ihnen gehören, finden Sie im [IAM-Benutzerhandbuch unter Gewähren von Zugriff für 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 im IAM-Benutzerhandbuch unter [Kontenübergreifender Ressourcenzugriff in IAM](#).

So werden die Preise für Security Lake festgelegt

Die Preisgestaltung von Amazon Security Lake basiert auf zwei Dimensionen: Datenaufnahme und Datenkonvertierung. Security Lake arbeitet auch mit anderen zusammen AWS-Services, um Ihre Daten zu speichern und weiterzugeben, und für diese Aktivitäten können separate Gebühren anfallen.

Wenn Sie die Protokollerfassung zum ersten Mal AWS-Konto in einem Programm aktivieren AWS-Region, das Security Lake unterstützt, wird dieses Konto automatisch für eine kostenlose 15-Tage-Testversion von Security Lake registriert. Während der kostenlosen Testversion können für Sie weiterhin Gebühren für andere Dienste anfallen.

Datenaufnahme

Diese Kosten ergeben sich aus der Menge der aufgenommenen AWS CloudTrail Protokolle und anderer AWS-Service Protokolle und Ereignisse (Amazon Route 53-Resolver-Abfrageprotokolle, AWS Security Hub Ergebnisse und Amazon VPC Flow Logs).

Datenkonvertierung

Diese Kosten ergeben sich aus der Menge der AWS-Service Protokolle und Ereignisse, die Security Lake auf das [Offenes Cybersecurity Schema Framework \(OCSF\)](#) Schema normalisiert und in das Apache Parquet-Format konvertiert.

Kosten für damit verbundene Dienstleistungen

Im Folgenden sind einige Kosten aufgeführt, die Ihnen durch andere Kosten AWS-Services für die Speicherung und gemeinsame Nutzung der Daten in Ihrem Security Data Lake entstehen können:

- Amazon S3 — Diese Kosten entstehen durch die Verwaltung von Amazon S3 S3-Buckets in Ihrem Security Lake-Konto, die Speicherung Ihrer Daten dort und die Bewertung und Überwachung Ihres Buckets im Hinblick auf Sicherheit und Zugriffskontrolle. Weitere Informationen finden Sie unter [Amazon S3 – Preise](#).
- Amazon SQS — Diese Kosten entstehen durch die Erstellung einer Amazon SQS SQS-Warteschlange für die Nachrichtenzustellung. Weitere Informationen finden Sie unter [Amazon SQS SQS-Preise](#).
- Amazon EventBridge — Diese Kosten entstehen dadurch, dass Amazon Objektbenachrichtigungen an Abonnementendpunkte EventBridge sendet. Weitere Informationen finden Sie unter [EventBridgeAmazon-Preise](#).

Die Kosten, die einem Abonnenten durch die Abfrage von Daten von Security Lake und das Speichern von Abfrageergebnissen entstehen, gehen zu Lasten des Abonnenten.

Weitere Informationen finden Sie unter [Security Lake-Preise](#).

Überprüfung der Nutzung von Security Lake und der geschätzten Kosten

Auf der Seite Nutzung der Amazon Security Lake-Konsole können Sie Ihre aktuelle Nutzung von Security Lake sowie future Nutzungs- und Kostenschätzungen überprüfen. Wenn Sie derzeit an einer 15-tägigen kostenlosen Testversion teilnehmen, können Sie anhand Ihrer Nutzung während der Testphase Ihre Kosten für die Nutzung von Security Lake nach Ablauf der kostenlosen Testversion abschätzen. Eine Übersicht über die Preise von Security Lake finden Sie unter [So werden die Preise für Security Lake festgelegt](#). Detaillierte Informationen und Kostenbeispiele finden Sie unter [Amazon Security Lake Pricing](#).

In Security Lake werden die geschätzten Nutzungskosten in US-Dollar angegeben und gelten nur für den aktuellen Zeitraum AWS-Region. Die Kosten decken die Nutzung von Security Lake durch alle Konten in Ihrer Organisation ab und beinhalten die Umstellung auf das Open Cybersecurity Schema Framework (OCSF) und das Apache Parquet-Format. Die prognostizierten Kosten beinhalten jedoch keine Kosten für andere Dienste, mit denen Security Lake zusammenarbeitet, wie Amazon Simple Storage Service (Amazon S3) und AWS Glue.

Auf der Seite Nutzung wählen Sie einen Zeitraum aus, für den Nutzungs- und Kostendaten angezeigt werden sollen. Der Standardzeitraum ist der letzte Kalendertag. Sie müssen Security Lake mindestens einen Tag lang genutzt haben, um Kostenprognosen sehen zu können.

Oben auf der Seite werden die voraussichtlichen Kosten für alle Konten angezeigt. Dies sind Ihre voraussichtlichen aktuellen Security Lake-Kosten AWS-Region für die nächsten 30 Kalendertage, basierend auf Ihrer tatsächlichen Nutzung im ausgewählten Zeitraum. Die tatsächliche Nutzung und die prognostizierten Kosten spiegeln alle Konten in Ihrer Organisation wider.

Im Rest der Seite sind die Nutzungs- und Kostendaten wie folgt in zwei Tabellen unterteilt:

- Nutzung und Kosten nach Quelle — Dies ist Ihre aktuelle Nutzung von Security Lake, aufgeschlüsselt nach Datenquelle, sowie die geschätzte Nutzung und Kosten für die nächsten 30 Kalendertage, basierend auf Ihrer tatsächlichen Nutzung im ausgewählten Zeitraum. Die tatsächliche Nutzung, die prognostizierte Nutzung und die prognostizierten Kosten spiegeln alle

Konten in Ihrer Organisation wider. Wenn Sie eine Quelle auswählen, wird ein geteilter Bereich geöffnet, in dem angezeigt wird, welche Konten Protokolle und Ereignisse aus dieser Quelle generiert haben. Für jedes Konto umfasst der geteilte Bereich sowohl die tatsächliche Nutzung aus dieser Quelle als auch die prognostizierte Nutzung und die voraussichtlichen Kosten.

- **Nutzung und Kosten pro Konto** — Dies ist Ihre aktuelle Security Lake-Nutzung, aufgeschlüsselt nach Konten, sowie die geschätzten Nutzung und Kosten für die nächsten 30 Kalendertage, basierend auf Ihrer tatsächlichen Nutzung im ausgewählten Zeitraum. Wenn Sie ein Konto auswählen, wird ein geteilter Bereich geöffnet, in dem die Quellen angezeigt werden, die zur Nutzung dieses Kontos beigetragen haben. Für jede beitragende Quelle enthält der geteilte Bereich sowohl die tatsächliche Nutzung als auch die prognostizierte Nutzung und die Kosten.

Alle unterstützten AWS Datenquellen werden in den obigen Tabellen aufgeführt, auch wenn Sie keine bestimmte Quelle in Security Lake hinzugefügt haben. Wir empfehlen, alle AWS Quellen hinzuzufügen, wenn Sie an der kostenlosen Testversion teilnehmen, um Kostenvoranschläge für Ihre gesamten Protokolle und Ereignisse zu erhalten. Anweisungen zum Hinzufügen einer AWS Quelle finden Sie unter [Erfassung von Daten von AWS-Services](#). Benutzerdefinierte Quellen sind nicht in Nutzungs- oder Kostenberechnungen enthalten.

Gehen Sie wie folgt vor, um Ihre Nutzungs- und Kostendaten in der Security Lake-Konsole zu überprüfen.

Um die Nutzung von Security Lake und die prognostizierten Kosten zu überprüfen (Konsole)

1. Öffnen Sie die Security Lake-Konsole unter <https://console.aws.amazon.com/securitylake/>.
2. Wählen Sie mithilfe der AWS-Region Auswahl in der oberen rechten Ecke der Seite die Region aus, in der Sie Ihre Nutzung und Kosten überprüfen möchten.
3. Wählen Sie im Navigationsbereich Einstellungen und dann Nutzung aus.
4. Wählen Sie den Zeitraum aus, für den Sie Nutzungs- und Kostendaten anzeigen möchten. Die Standardeinstellung ist der letzte Tag.
5. Wählen Sie die Registerkarte Nach Datenquelle oder Nach Konten, um die Nutzung und die Kosten im Detail zu überprüfen.

Amazon Security Lake e-

Eine Liste der unterstützten Regionen und Dienstendpunkte für Security Lake finden Sie unter [Amazon Security Lake-Endpoints](#) in der Allgemeine AWS-Referenz.

Es wird empfohlen, Security Lake zu aktivierenAWS-Regionen. Auf diese Weise können Sie Security Lake verwenden, um unbefugte oder ungewöhnliche Aktivitäten zu erkennen und zu untersuchen, auch in Regionen, die Sie nicht aktiv nutzen.

Deaktivieren von Amazon Security Lake

Wenn Sie Amazon Security Lake deaktivieren, stoppt Security Lake das Sammeln von Protokollen und Ereignissen aus Ihren AWS Quellen. Bestehende Security-Lake-Einstellungen und die Ressourcen, die in Ihrem erstellt wurden, AWS-Konto werden beibehalten. Darüber hinaus bleiben die Daten, die Sie in gespeichert oder in anderen veröffentlicht haben AWS-Services, wie z. B. sensible Daten in AWS Lake Formation Tabellen und AWS CloudTrail Protokollen, verfügbar. Daten, die in Ihrem Amazon Simple Storage Service (Amazon S3)-Bucket gespeichert sind, bleiben gemäß Ihrem [Amazon S3-Speicherlebenszyklus](#) verfügbar.

Wenn Sie Security Lake auf der Seite Einstellungen in der Security-Lake-Konsole deaktivieren, wird die Erfassung von AWS Protokollen und Ereignissen in allen gestoppt, AWS-Regionen in denen Security Lake derzeit aktiviert ist. Sie können die Seite Regionen in der -Konsole verwenden, um die Protokollerfassung in bestimmten Regionen zu beenden. Die Security-Lake-API und beenden AWS CLI auch die Protokollerfassung in den Regionen, die Sie in Ihrer Anforderung angeben.

Wenn Sie die Integration mit verwenden AWS Organizations und Ihr Konto Teil einer Organisation ist, die mehrere Security-Lake-Konten zentral verwaltet, kann nur der delegierte Security-Lake-Administrator Security Lake für sich selbst und für Mitgliedskonten deaktivieren. Wenn Sie jedoch eine Organisation verlassen, wird die Protokollerfassung für ein Mitgliedskonto beendet.

Wenn Sie Security Lake für eine Organisation deaktivieren, wird die Bezeichnung des delegierten Administrators beibehalten, wenn Sie die auf dieser Seite angegebenen Deaktivierungsanweisungen befolgen. Sie müssen den delegierten Administrator nicht erneut benennen, bevor Sie Security Lake erneut aktivieren können.

Bei benutzerdefinierten Quellen müssen Sie beim Deaktivieren von Security Lake jede Quelle außerhalb der Security-Lake-Konsole deaktivieren. Wenn Sie eine Integration nicht deaktivieren, senden Quellintegrationen weiterhin Protokolle an Amazon S3. Darüber hinaus müssen Sie eine Subscriber-Integration deaktivieren, sonst kann der Subscriber weiterhin Daten aus Security Lake verbrauchen. Einzelheiten zum Entfernen einer benutzerdefinierten Quelle oder einer Subscriber-Integration finden Sie in der Dokumentation des jeweiligen Anbieters.

In diesem Thema wird erläutert, wie Sie Security Lake mithilfe der Security-Lake-Konsole, der Security-Lake-API oder deaktivieren AWS CLI.

Console

1. Öffnen Sie die Security-Lake-Konsole unter <https://console.aws.amazon.com/securitylake/>.

2. Klicken Sie im Navigationsbereich unter Settings auf General.
3. Wählen Sie Security Lake deaktivieren aus.
4. Wenn Sie zur Bestätigung aufgefordert werden, geben Sie ein **Disable** und wählen Sie dann Deaktivieren aus.

API

Um Security Lake programmgesteuert zu deaktivieren, verwenden Sie die [DeleteDataLake](#) Operation der Security-Lake-API. Wenn Sie die verwenden AWS CLI, führen Sie den [delete-data-lake](#) Befehl aus. Verwenden Sie in Ihrer Anfrage die `regions` Liste, um den Regionscode für jede Region anzugeben, in der Sie Security Lake deaktivieren möchten. Eine Liste der Regionscodes finden Sie unter [Amazon-Security-Lake-Endpunkte](#) im Allgemeine AWS-Referenz.

Bei einer Security-Lake-Bereitstellung mit kann AWS Organizations nur der delegierte Security-Lake-Administrator für die Organisation Security Lake für Konten in der Organisation deaktivieren.

Mit dem folgenden AWS CLI Befehl wird Security Lake beispielsweise in den `eu-central-1` Regionen `ap-northeast-1` und deaktiviert. Dieses Beispiel ist für Linux, macOS oder Unix formatiert und verwendet den umgekehrten Schrägstrich (`\`) zur Verbesserung der Lesbarkeit.

```
$ aws securitylake delete-data-lake \  
--regions "ap-northeast-1" "eu-central-1"
```

Häufig gestellte Fragen

Security Lake-Update auf die neueste Version von Parquet

Am 20.05.2024 wird Amazon Security Lake auf die neueste Version von Parquet aktualisiert.

Warum macht Security Lake dieses Update?

Im Rahmen der kontinuierlichen Bemühungen von Amazon, unseren Kunden sichere und effiziente Services zu bieten, aktualisiert Security Lake regelmäßig Abhängigkeiten, Bibliotheken, APIs und Tools von Drittanbietern. Security Lake stellt außerdem sicher, dass Kunden die neuesten Erweiterungen aller Standards verwenden, einschließlich der Parquet-Spezifikation.

In seltenen Fällen kann dies zu geringfügigen Änderungen der Art und Weise führen, wie Daten gespeichert und/oder verarbeitet werden. Die Änderungen sind immer abwärtskompatibel mit den etablierten Gemeinschaftsstandards.

Security Lake normalisiert die Sicherheitsprotokolldateien von Kunden in das OCSF-Format und stellt sie in einem abfrageeffizienten Parquet-Format zur Verfügung. Security Lake nimmt diese Änderung vor, um eine reibungslose Einführung des neuesten Parquet-Formats zu gewährleisten. Weitere Informationen finden Sie unter [Parquet-Format](#).

Wo kann ich mehr über die Änderung der Parquet-Spezifikation erfahren?

Weitere Informationen finden Sie unter [Veralteter Zeitstempel ConvertedType](#) im Parquet-Format-Repository. GitHub

Wirkt sich dieses Upgrade auf meine Security Lake-Integrationen aus?

Wenn Sie nur Amazon Athena- oder Apache-Tools (Spark, Hive, Impala, Hadoop) für den Zugriff auf Security Lake-Tabellen verwenden, ändert sich nichts. Die Änderungen im Zusammenhang mit dem Upgrade werden automatisch und transparent von den Client-Tools und APIs verarbeitet.

Wenn Sie andere Client-Tools verwenden, empfiehlt Security Lake, sich mit den neuen Methoden zum Speichern und Behandeln von Datums-/Uhrzeitfeldern vertraut zu machen. In der folgenden Tabelle sind die geringfügigen Unterschiede aufgeführt, die Sie möglicherweise zwischen alten und neuen synthetischen Daten feststellen.

Änderungen der synthetischen Daten

AWS Dienstleistungen	Typ	Aktuell	Neu
Amazon Athena	Datum/Uhrzeit	1970-01-20 03:04:05. 399 000	Keine Änderung
Apache Spark	Datum/Uhrzeit	1970-01-20T 00:04:05.000-03:00	Keine Änderung
PyArrow	Datum/Uhrzeit	1970-01-20 03:04:05	1970-01-20 03:04:05 + 00:00 Die Einführung der UTC-Zeitzone markierung hat sich geändert.

Wie kann ich Änderungen bei der Verarbeitung von Parquetformaten erkennen?

Laden Sie die ZIP-Datei [parquet_format.zip](#) herunter. Die Zip-Datei besteht aus zwei Dateien.

- Synthetische Testdaten, die mit dem alten Framework generiert wurden — `parquet_format_old.parquet`
- Mit dem neuen Framework generierte synthetische Testdaten — `parquet_format_new.parquet`

Testen Sie Ihre Client-Tools und vergleichen Sie die vom alten Framework generierten synthetischen Testdaten mit den vom neuen Framework generierten Daten.

Wenn Sie spürbare Änderungen feststellen, verwenden Sie die Empfehlungen aus der `Changes in synthetic data` Tabelle. Wenn Sie weitere Unterstützung benötigen, wenden Sie sich an den [AWS Support](#).

Dokumentenverlauf für das Amazon Security Lake-Benutzerhandbuch

In der folgenden Tabelle werden die wichtigen Änderungen an der Dokumentation seit der letzten Version von Amazon Security Lake beschrieben. Um Benachrichtigungen über Aktualisierungen dieser Dokumentation zu erhalten, können Sie einen RSS-Feed abonnieren.

Letzte Aktualisierung der Dokumentation: 10. Juni 2024

Änderung	Beschreibung	Datum
Regionale Verfügbarkeit	Security Lake ist jetzt in den Ländern AWS GovCloud (US-Ost) und AWS GovCloud (US-West) verfügbar. AWS-Regionen Eine vollständige Liste der Regionen, in denen Security Lake derzeit verfügbar ist, finden Sie unter Amazon Security Lake-Endpoints in der Allgemeine AWS-Referenz.	10. Juni 2024
Aktualisierung der bestehenden verwalteten Richtlinie	Security Lake hat der AWS verwalteten Richtlinie für die SecurityLakeServiceLinkedRole Richtlinie AWS WAF Aktionen hinzugefügt. Die zusätzlichen Aktionen ermöglichen es Security Lake, AWS WAF Protokolle zu sammeln, wenn es als Protokollquelle in Security Lake aktiviert ist.	22. Mai 2024
Neue AWS Protokollquelle	Security Lake hat AWS-WAF-Protokolle als AWS Protokoll	22. Mai 2024

	quelle hinzugefügt. AWS WAF hilft Ihnen bei der Überwachung von Webanfragen, die Endbenutzer an Anwendungen senden.	
Aktualisierung der bestehenden verwalteten Richtlinie	Security Lake hat der AmazonSecurityLakePermissionsBoundary Richtlinie SID-Aktionen hinzugefügt.	13. Mai 2024
Aktualisierung der bestehenden verwalteten Richtlinie	Security Lake hat die AmazonSecurityLakeMetastoreManager-Richtlinie um eine Aktion zur Bereinigung von Metadaten erweitert, mit der Sie die Metadaten in Ihrem Data Lake löschen können.	27. März 2024
Neue Quellversionen	Aktualisieren Sie Ihre Rollenberechtigungen , um Daten aus den neuen Datenquellenversionen aufzunehmen.	29. Februar 2024
Neue AWS Protokollquelle	Security Lake hat EKS Audit Logs als AWS Protokollquelle hinzugefügt. EKS-Auditprotokolle helfen Ihnen dabei, potenziell verdächtige Aktivitäten in Ihren EKS-Clustern innerhalb des Amazon Elastic Kubernetes Service zu erkennen.	29. Februar 2024

[Aktualisierung der bestehenden verwalteten Richtlinie](#)

Security Lake hat die Richtlinie aktualisiert, um die neue AmazonSecurityLakeMetastoreManagerV2 Rolle zuzulassen iam:PassRole und ermöglicht es Security Lake, Data Lake-Komponenten bereitzustellen oder zu aktualisieren.

23. Februar 2024

[Neue verwaltete Richtlinie](#)

Security Lake hat eine neue [AWS verwaltete Richtlinie](#) hinzugefügt, die AmazonSecurityLakeMetastoreManager Richtlinie. Diese Richtlinie gewährt Security Lake Berechtigungen zur Verwaltung von Metadaten in Ihrem Data Lake.

23. Januar 2024

[Regionale Verfügbarkeit](#)

Security Lake ist jetzt in den folgenden Ländern verfügbar
AWS-Regionen: Asien-Pazifik (Osaka), Kanada (Zentral), Europa (Paris) und Europa (Stockholm). Eine vollständige Liste der Regionen, in denen Security Lake derzeit verfügbar ist, finden Sie unter [Amazon Security Lake-Endpoints](#) in der Allgemeine AWS-Referenz.

26. Oktober 2023

Neue Features	Sie können jetzt bestimmte Einstellungen für Abonnenten mit Abfragezugriff bearbeiten . Sie können den Security Lake-Ressourcen auch Tags für Sie zuweisen AWS-Konto.	20. Juli 2023
Neue verwaltete Richtlinie	Security Lake hat eine neue AWS verwaltete Richtlinie hinzugefügt, die AmazonSecurityLakeAdministrator Richtlinie. Diese Richtlinie gewährt Administratorberechtigungen, die einem Prinzipal vollen Zugriff auf alle Security Lake-Aktionen gewähren.	30. Mai 2023
Allgemeine Verfügbarkeit	Security Lake ist jetzt allgemein verfügbar.	30. Mai 2023
Neues Feature	Security Lake sendet jetzt Metriken an Amazon CloudWatch .	4. Mai 2023
Regionale Verfügbarkeit	Security Lake ist jetzt in den folgenden Ländern verfügbar AWS-Regionen: Asien-Pazifik (Singapur), Europa (London) und Südamerika (São Paulo).	22. März 2023

Neues Feature

Security Lake erstellt jetzt AWS Identity and Access Management (IAM) -Rollen in Ihrem Namen, wenn Sie die Security Lake-Konsole verwenden, um Security Lake zu [aktivieren und zu verwenden](#).

15. Februar 2023

Erstversion

Dies ist die erste Version des Amazon Security Lake-Benutzerhandbuchs.

29. November 2022

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.