



Entwicklerhandbuch

AWS Lake Formation



AWS Lake Formation: Entwicklerhandbuch

Copyright © 2026 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 AWS Lake Formation?	1
Merkmale der Lake Formation	2
Datenaufnahme und -verwaltung	2
Sicherheitsmanagement	3
Ihre Daten zum Datenkatalog hinzufügen	5
Funktionsweise	6
Workflow zur Verwaltung von Berechtigungen in Lake Formation	7
Berechtigungen für Metadaten	8
Verwaltung des Speicherzugriffs	12
Kontoübergreifender Datenaustausch in Lake Formation	13
Lake Formation komponenten	14
Lake Formation Formation-Konsole	14
Lake Formation API und Befehlszeilenschnittstelle	15
Andere AWS Dienste	15
Terminologie der Lake Formation	15
Datensee	15
Datenzugriff	16
Hybrider Zugriffsmodus	16
Blueprint	16
Workflow	16
Data Catalog	17
Zugrundeliegende Daten	17
Auftraggeber	17
Data Lake-Administrator	17
AWS Serviceintegrationen mit Lake Formation	18
Zusätzliche Ressourcen zur Lake Formation	20
Blogs	20
Technische Vorträge und Webinare	21
Moderne Architektur	21
Daten-Mesh-Ressourcen	21
Leitfäden mit bewährten Verfahren	21
Erste Schritte mit Lake Formation	21
Erste Schritte	23
Erledigen Sie die Aufgaben zur AWS Erstkonfiguration	23

Melde dich an für ein AWS-Konto	23
Erstellen eines Benutzers mit Administratorzugriff	24
Erteilen programmgesteuerten Zugriffs	25
Richten AWS Lake Formation	28
Lake Formation Formation-Ressourcen mithilfe einer CloudFormation Vorlage einrichten	28
Erstellen Sie einen Data Lake-Administrator	30
Ändern Sie das Standardberechtigungsmodell oder verwenden Sie den hybriden Zugriffsmodus	35
Benutzern von Lake Formation Berechtigungen zuweisen	36
Konfigurieren Sie einen Amazon S3 S3-Standort für Ihren Data Lake	38
(Optional) Einstellungen für die externe Datenfilterung	39
(Optional) Gewähren Sie Zugriff auf den Datenkatalog-Verschlüsselungsschlüssel	40
(Optional) Erstellen Sie eine IAM-Rolle für Workflows	40
Aktualisierung der AWS Glue Datenberechtigungen auf das Lake Formation Formation- Modell	42
Über Standardberechtigungen	43
Listet die vorhandenen Berechtigungen auf	45
Lake Formation Formation-Berechtigungen einrichten	47
Erteilen Sie Benutzern IAM-Berechtigungen	48
Wechseln Sie zum Lake Formation Formation-Berechtigungsmodell	48
Schritt 5: Sichern Sie sich neue Datenkatalog-Ressourcen	52
Schritt 6: Geben Sie Benutzern eine neue IAM-Richtlinie	53
Schritt 7: Bereinigen vorhandener IAM-Richtlinien	54
Einrichtung von Amazon VPC-Endpunkten (AWS PrivateLink)	54
Überlegungen zu Lake Formation VPC-Endpunkten	55
Erstellen eines VPC-Schnittstellen-Endpunkts für Lake Formation	55
Erstellen einer VPC-Endpunktrichtlinie für Lake Formation	56
Lernprogramme	58
Einen Data Lake aus einer AWS CloudTrail Quelle erstellen	59
Zielgruppe	61
Voraussetzungen	61
Schritt 1: Erstellen Sie einen Data Analyst-Benutzer	62
Schritt 2: Fügen Sie der Workflow-Rolle Berechtigungen zum Lesen von AWS CloudTrail Protokollen hinzu	63
Schritt 3: Erstellen Sie einen Amazon S3 S3-Bucket für den Data Lake	63
Schritt 4: Registrieren Sie einen Amazon S3 S3-Pfad	64

Schritt 5: Erteilen Sie Berechtigungen für den Datenspeicherort	64
Schritt 6: Erstellen Sie eine Datenbank im Datenkatalog	65
Schritt 7: Erteilen Sie Datenberechtigungen	65
Schritt 8: Verwenden Sie einen Blueprint, um einen Workflow zu erstellen	66
Schritt 9: Führen Sie den Workflow aus	67
Schritt 10: Gewähren Sie SELECT für die Tabellen	68
Schritt 11: Fragen Sie den Data Lake ab mit Amazon Athena	69
Einen Data Lake aus einer JDBC-Quelle erstellen	70
Zielgruppe	71
Voraussetzungen	71
Schritt 1: Erstellen Sie einen Data Analyst-Benutzer	72
Schritt 2: Erstellen Sie eine Verbindung in AWS Glue	73
Schritt 3: Erstellen Sie einen Amazon S3 S3-Bucket für den Data Lake	74
Schritt 4: Registrieren Sie einen Amazon S3 S3-Pfad	74
Schritt 5: Erteilen Sie Berechtigungen für den Datenspeicherort	75
Schritt 6: Erstellen Sie eine Datenbank im Datenkatalog	75
Schritt 7: Erteilen Sie Datenberechtigungen	75
Schritt 8: Verwenden Sie einen Blueprint, um einen Workflow zu erstellen	76
Schritt 9: Führen Sie den Workflow aus	78
Schritt 10: Gewähren Sie SELECT für die Tabellen	79
Schritt 11: Fragen Sie den Data Lake ab mit Amazon Athena	79
Schritt 12: Fragen Sie die Daten im Data Lake mit Amazon Redshift Spectrum ab	80
Schritt 13: Erteilen oder Widerrufen Lake Formation Formation-Berechtigungen mithilfe von Amazon Redshift Spectrum	85
Berechtigungen für offene Tabellenformate in Lake Formation einrichten	85
Zielgruppe	86
Voraussetzungen	86
Schritt 1: Stellen Sie Ihre Ressourcen bereit	88
Schritt 2: Richten Sie Berechtigungen für eine Iceberg-Tabelle ein	89
Schritt 3: Richten Sie Berechtigungen für eine Hudi-Tabelle ein	96
Schritt 4: Richten Sie Berechtigungen für eine Delta Lake-Tabelle ein	99
Schritt 5: Ressourcen bereinigen AWS	101
Verwaltung eines Data Lakes mithilfe einer tagbasierten Zugriffskontrolle	102
Zielgruppe	103
Voraussetzungen	105
Schritt 1: Stellen Sie Ihre Ressourcen bereit	105

Schritt 2: Registrieren Sie Ihren Datenstandort, erstellen Sie eine LF-Tag-Ontologie und gewähren Sie Berechtigungen	106
Schritt 3: Lake Formation Formation-Datenbanken erstellen	110
Schritt 4: Erteilen Sie Tabellenberechtigungen	120
Schritt 5: Führen Sie eine Abfrage in Amazon Athena aus, um die Berechtigungen zu überprüfen	122
Schritt 6: Ressourcen AWS bereinigen	123
Sicherung von Data Lakes mit Zugriffskontrolle auf Zeilenebene	124
Zielgruppe	124
Voraussetzungen	125
Schritt 1: Stellen Sie Ihre Ressourcen bereit	126
Schritt 2: Abfrage ohne Datenfilter	127
Schritt 3: Richten Sie Datenfilter ein und gewähren Sie Berechtigungen	129
Schritt 4: Abfrage mit Datenfiltern	131
Schritt 5: AWS Ressourcen bereinigen	133
Teilen Sie Ihre Daten sicher mit Lake Formation	133
Zielgruppe	134
Lake Formation Formation-Einstellungen konfigurieren	135
Schritt 1: Stellen Sie Ihre Ressourcen mithilfe von AWS CloudFormation Vorlagen bereit	138
Schritt 2: Voraussetzungen für die gemeinsame Nutzung von Konten bei Lake Formation ...	140
Schritt 3: Implementieren Sie die kontenübergreifende gemeinsame Nutzung mithilfe der tagbasierten Zugriffskontrollmethode	143
Schritt 4: Implementieren Sie die benannte Ressourcenmethode	149
Schritt 5: AWS Ressourcen bereinigen	154
Gemeinsame Nutzung von Datenkatalogressourcen mit externen Benutzern AWS-Konten mithilfe einer detaillierten Zugriffskontrolle	154
Zielgruppe	156
Voraussetzungen	156
Schritt 1: Stellen Sie einen detaillierten Zugriff auf ein anderes Konto bereit	157
Schritt 2: Bieten Sie einem Benutzer im selben Konto differenzierten Zugriff	159
Einsteigen in die Genehmigungen von Lake Formation	161
Überblick über die Genehmigungen für Lake Formation	163
Methoden für eine differenzierte Zugriffskontrolle	165
Zugriffskontrolle für Metadaten	168
Zugrundeliegende Datenzugriffskontrolle	173
Referenz zu Personas und IAM-Berechtigungen in Lake Formation	179

AWS Lake Formation Personas	179
AWS verwaltete Richtlinien für Lake Formation	181
Personas hat Berechtigungen vorgeschlagen	190
Ändern der Standardeinstellungen für Ihren Data Lake	201
Implizite Lake Formation Formation-Berechtigungen	204
Referenz zu den Genehmigungen von Lake Formation	206
Lake Formation Formation-Berechtigungen pro Ressourcentyp	206
Lake Formation erteilt und widerruft AWS CLI Befehle	209
Lake-Formation-Berechtigungen	214
Integration von IAM Identity Center	230
Voraussetzungen für die Integration von IAM Identity Center mit Lake Formation	231
Lake Formation mit dem IAM Identity Center verbinden	235
Aktualisierung der IAM Identity Center-Integration	238
Löschen einer Lake Formation Formation-Verbindung mit IAM Identity Center	240
Benutzern und Gruppen Berechtigungen gewähren	240
Einbeziehen des IAM Identity Center-Benutzerkontextes in die Protokolle CloudTrail	244
Hinzufügen eines Amazon S3 S3-Standorts zu Ihrem Data Lake	246
Anforderungen für Rollen, die zur Registrierung von Standorten verwendet werden	247
Registrierung eines Amazon S3 S3-Standorts	255
Registrierung eines verschlüsselten Amazon S3 S3-Standorts	259
Registrierung eines Amazon S3 S3-Standorts in einem anderen AWS Konto	264
AWS Kontoübergreifende Registrierung eines verschlüsselten Amazon S3 S3-Standorts	267
Abmeldung eines Amazon S3 S3-Standorts	272
Hybrider Zugriffsmodus	272
Allgemeine Anwendungsfälle im hybriden Zugriffsmodus	274
So funktioniert der hybride Zugriffsmodus	276
Einrichtung des hybriden Zugriffsmodus — häufig vorkommende Szenarien	278
Prinzipale und Ressourcen aus dem Hybridzugriffsmodus entfernen	301
Prinzipale und Ressourcen im Hybridzugriffsmodus anzeigen	302
Weitere Ressourcen	303
Objekte erstellen in AWS Glue Data Catalog	303
Einen Katalog erstellen	304
Erstellen einer Datenbank	305
Erstellen von Tabellen	306
Ansichten des Gebäudedatenkatalogs	315
Daten mithilfe von Workflows importieren	364

Entwürfe und Arbeitsabläufe	365
Einen Workflow erstellen	366
Einen Workflow ausführen	371
Hinzufügen Ihrer Daten zum Datenkatalog	373
Katalogverbund	375
Funktionen von Catalog Federation	375
Föderiere dich zu Snowflake	376
Föderiere dich zu Databricks	384
Aufnehmen von Amazon-Redshift-Daten in den Datenkatalog	393
Wichtigste Vorteile	395
Rollen und Zuständigkeiten	396
Voraussetzungen	397
Erstellen von Amazon Redshift Redshift-Verbundkatalogen	403
Katalogobjekte anzeigen	413
Aktualisierung eines Verbundkatalogs	415
Zugreifen auf einen gemeinsam genutzten Verbundkatalog	417
Löschen eines Verbundkatalogs	422
Verbundkataloge abfragen	423
Weitere Ressourcen	424
Zusammenführung mit externen Datenquellen	424
Workflow	425
Voraussetzungen	426
Einen Verbundkatalog erstellen	430
Katalogobjekte anzeigen	436
Löschen eines Verbundkatalogs	438
Verbundkataloge abfragen	439
Weitere Ressourcen	439
Erstellen eines Amazon S3 S3-Tabellenkatalogs im Datenkatalog	439
So funktioniert die Integration von Data Catalog und Lake Formation	440
Voraussetzungen	441
Aktivierung der Amazon S3 S3-Tabellenintegration	444
Erstellen von Datenbanken und Tabellen	447
Registrierung eines Amazon S3 S3-Tabellen-Buckets in einem anderen AWS Konto	450
Gewähren von Berechtigungen	453
Einen verwalteten Amazon Redshift Redshift-Katalog erstellen	456
Verwaltung von Berechtigungen für Daten in einem Amazon Redshift Redshift-Datashare	462

Voraussetzungen	463
Berechtigungen für Amazon Redshift Redshift-Datenfreigaben einrichten	464
Abfragen verbundener Datenbanken	468
Verwaltung von Berechtigungen für Datensätze, die externe Metastores verwenden	469
Workflow	472
Voraussetzungen	473
Den Datenkatalog mit einem externen Hive-Metastore verbinden	475
Weitere Ressourcen	479
Verwaltung von Lake Formation Formation-Berechtigungen	480
Erteilung von Berechtigungen zum Speicherort von Daten	480
Erteilen von Datenspeicherberechtigungen (dasselbe Konto)	481
Erteilen von Datenstandortberechtigungen (externes Konto)	484
Erteilen von Berechtigungen für einen Datenstandort, der mit Ihrem Konto geteilt wird	487
Erteilen von Datenberechtigungen	488
Für die Erteilung von Lake Formation Formation-Berechtigungen sind IAM-Berechtigungen erforderlich	490
Verwendung der Methode für benannte Ressourcen	493
Tag-basierte Zugriffskontrolle	521
Erteilen von Data Lake-Berechtigungen mithilfe der LF-TBAC-Methode	583
Attributbasierte Zugriffskontrolle	591
Beispielszenario für Berechtigungen	595
Datenfilterung und Sicherheit auf Zellebene	597
Datenfilter	599
PartiQL-Unterstützung in Zeilenfilterausdrücken	603
Erforderliche Berechtigungen für das Abfragen von Tabellen mit Filterung auf Zellenebene	606
Datenfilter verwalten	606
Datenbank- und Tabellenberechtigungen anzeigen	622
Widerrufen von Berechtigungen mithilfe der Konsole	627
Kontoübergreifender Datenaustausch	627
Voraussetzungen	631
Aktualisierung der Versionseinstellungen für die kontenübergreifende gemeinsame Nutzung von Daten	635
Gemeinsame Nutzung von Datenkatalogtabellen und Datenbanken für mehrere AWS-Konten IAM-Prinzipale von externen Konten aus	642
Erteilen von Berechtigungen für eine Datenbank oder Tabelle, die mit Ihrem Konto geteilt wird	648

Erteilen von Ressourcenverknüpfungsberechtigungen	650
Zugreifen auf die zugrunde liegenden Daten einer gemeinsam genutzten Tabelle	653
Kontoübergreifende Protokollierung CloudTrail	655
Verwaltung kontenübergreifender Berechtigungen sowohl AWS Glue mit Lake Formation als auch mit Lake Formation	660
Alle kontenübergreifenden Zuschüsse mithilfe des GetResourceShares API-Vorgangs anzeigen	663
Zugreifen auf und Anzeigen von gemeinsam genutzten Datenkatalogtabellen und Datenbanken	664
Annahme einer Einladung AWS RAM zur gemeinsamen Nutzung von Ressourcen	666
Tabellen und Datenbanken des gemeinsamen Datenkatalogs anzeigen	668
Ressourcenlinks erstellen	670
Wie funktionieren Ressourcenlinks	671
Einen Ressourcenlink zu einer gemeinsam genutzten Tabelle erstellen	673
Einen Ressourcenlink zu einer gemeinsam genutzten Datenbank erstellen	677
Umgang mit Ressourcenlinks in AWS Glue APIs	681
Regionsübergreifender Zugriff auf Tabellen	686
Arbeitsabläufe	687
Einrichtung des regionsübergreifenden Tabellenzugriffs	691
Sicherheit	695
Datenschutz	695
Verschlüsselung im Ruhezustand	697
Sicherheit der Infrastruktur	697
Serviceübergreifende Confused-Deputy-Prävention	698
Anmeldung bei Sicherheitsereignissen AWS Lake Formation	699
Integration mit Lake Formation	701
Verwenden der Anwendungsintegration von Lake Formation	701
So funktioniert die Anwendungsintegration von Lake Formation	702
Rollen und Verantwortlichkeiten bei der Anwendungsintegration von Lake Formation	704
Lake FormationWorkflow für API-Operationen zur Anwendungsintegration	705
Registrierung einer Query-Engine eines Drittanbieters	708
Aktivierung von Berechtigungen für eine Abfrage-Engine eines Drittanbieters zum Aufrufen von API-Operationen für die Anwendungsintegration	709
Anwendungsintegration für vollständigen Tabellenzugriff	714
Zusammenarbeit mit anderen AWS Diensten	717
Amazon Athena	721

Support für Transaktionstabellenformate	723
Weitere Ressourcen	726
Amazon Redshift Spectrum	726
Support für Transaktionstabellentypen	727
Weitere Ressourcen	728
AWS Glue	729
Support für Transaktionstabellentypen	730
Weitere Ressourcen	731
Amazon EMR	731
Support für Transaktionstabellenformate	732
Weitere Ressourcen	733
Schnell	733
Weitere Ressourcen	734
AWS CloudTrail See	734
Protokollieren AWS Lake Formation Formation-API-Aufrufen mit AWS CloudTrail	735
Informationen Lake Formation in CloudTrail	735
Lake Formation Formation-Ereignisse verstehen	736
Bewährte Methoden, Überlegungen und Einschränkungen von Lake Formation	739
Bewährte Methoden und Überlegungen für den kontenübergreifenden Datenaustausch	739
Einschränkungen für dienstbezogene Rollen	742
Regionsübergreifende Beschränkungen des Datenzugriffs	743
Überlegungen und Einschränkungen im Datenkatalog	743
Einschränkungen bei der Datenfilterung	745
Hinweise und Einschränkungen für die Filterung auf Spaltenebene	745
Einschränkungen bei der Filterung auf Zellebene	747
Überlegungen und Einschränkungen des hybriden Zugriffsmodus	749
Einschränkungen beim Einbringen von Amazon Redshift Data Warehouse-Daten in die AWS Glue Data Catalog	750
Einschränkungen bei der Integration von S3-Tabellen	752
Überlegungen und Einschränkungen beim Datenaustausch im Hive-Metadatenpeicher	753
Einschränkungen beim Datenaustausch mit Amazon Redshift	755
Einschränkungen bei der IAM Identity Center-Integration	756
Bewährte Methoden und Überlegungen zur Tag-basierten Zugriffskontrolle von Lake Formation	757
Überlegungen zur attributbasierten Zugriffskontrolle, Einschränkungen und unterstützte Regionen	761

Fehlerbehebung bei der Lake Formation	762
Allgemeine Problembehebung	762
Fehler: Unzureichende Lake Formation Formation-Berechtigungen für <Amazon S3 location>	762
Fehler: „Unzureichende Verschlüsselungsschlüsselberechtigungen für die Glue-API“	763
Meine Amazon Athena oder Amazon Redshift Redshift-Abfrage, die Manifeste verwendet, schlägt fehl	763
Fehler: „Unzureichende Lake Formation Formation-Berechtigungen: Erforderlich, Tag im Katalog erstellen“	763
Fehler beim Löschen ungültiger Data Lake-Administratoren	763
Problembehandlung beim kontoübergreifenden Zugriff	763
Ich habe eine kontoübergreifende Lake Formation Formation-Genehmigung erteilt, aber der Empfänger kann die Ressource nicht sehen	764
Principals im Empfängerkonto können die Datenkatalogressource sehen, aber nicht auf die zugrunde liegenden Daten zugreifen	765
Fehler: „Die Zuordnung ist fehlgeschlagen, weil der Anrufer nicht autorisiert war“ beim Annehmen einer AWS RAM Einladung zur gemeinsamen Nutzung von Ressourcen	765
Fehler: „Nicht berechtigt, Berechtigungen für die Ressource zu erteilen“	766
Fehler: „Zugriff zum Abrufen von AWS Unternehmensinformationen verweigert“	766
Fehler: „Organisation <organization-ID>nicht gefunden“	766
Fehler: „Unzureichende Lake Formation Formation-Berechtigungen: Unzulässige Kombination“	766
ConcurrentModificationException bei grant/revoke Anfragen an externe Konten	766
Fehler bei der Verwendung von Amazon EMR für den Zugriff auf kontoübergreifende Daten	767
Problembehandlung bei Blueprints und Workflows	768
<role-ARN>Mein Blueprint schlug fehl mit der Meldung „User: <user-ARN>is not authorized to perform: iam: PassRole on resource:“	768
<role-ARN>Mein Workflow ist mit „User: <user-ARN>is not authorized to perform: iam: PassRole on resource:“ fehlgeschlagen	769
Ein Crawler in meinem Workflow ist mit der Meldung „Die Ressource ist nicht vorhanden oder der Anforderer ist nicht berechtigt, auf die angeforderten Berechtigungen zuzugreifen“ fehlgeschlagen	769
Ein Crawler in meinem Workflow ist mit der Meldung „Beim Aufrufen der CreateTable Operation... ist ein Fehler aufgetreten (AccessDeniedException)“ fehlgeschlagen	769
Bekannte Probleme für AWS Lake Formation	769

Einschränkung beim Filtern von Tabellenmetadaten	770
Problem beim Umbenennen einer ausgeschlossenen Spalte	771
Problem beim Löschen von Spalten in CSV-Tabellen	771
Tabellenpartitionen müssen unter einem gemeinsamen Pfad hinzugefügt werden	771
Problem beim Erstellen einer Datenbank während der Workflow-Erstellung	772
Problem beim Löschen und erneuten Erstellen eines Benutzers	772
Bei API-Vorgängen für den Datenkatalog wird der Wert für den IsRegisteredWithLakeFormation Parameter nicht aktualisiert	772
Lake Formation Formation-Operationen unterstützen AWS Glue Schema Registry nicht	773
Die Fehlermeldung wurde aktualisiert	773
Lake Formation API	774
Berechtigungen	775
— Operationen —	775
— Datentypen —	775
Data Lake-Einstellungen	776
— Operationen —	776
— Datentypen —	776
IAM-Identity-Center-Integration	776
— Operationen —	776
— Datentypen —	776
Hybrider Zugriffsmodus	777
— Operationen —	777
— Datentypen —	775
Verkauf von Zugangsdaten	777
— Operationen —	777
— Datentypen —	778
Tagging	778
— Operationen —	778
— Datentypen —	779
Datenfilter APIs	779
— Operationen —	779
— Datentypen —	779
Gängige Datentypen	780
ErrorDetail	780
Zeichenfolgemuster	780
Unterstützte Regionen	782

Allgemeine Verfügbarkeit	782
AWS GovCloud (US)	782
Transaktionen und Speicheroptimierung	782
Dokumentverlauf	785
AWS Glossar	802
.....	dccciiii

Was ist AWS Lake Formation?

Willkommen im AWS Lake Formation Entwicklerhandbuch.

AWS Lake Formation hilft Ihnen dabei, Daten für Analysen und maschinelles Lernen zentral zu verwalten, zu sichern und weltweit auszutauschen. Mit Lake Formation können Sie eine detaillierte Zugriffskontrolle für Ihre Data Lake-Daten auf Amazon Simple Storage Service (Amazon S3) und deren Metadaten verwalten. AWS Glue Data Catalog

Lake Formation bietet ein eigenes Berechtigungsmodell, das das IAM-Berechtigungsmodell erweitert. Das Lake Formation Formation-Berechtigungsmodell ermöglicht einen detaillierten Zugriff auf Daten, die in Data Lakes gespeichert sind, sowie auf externe Datenquellen wie Amazon Redshift Data Warehouses, Amazon DynamoDB Datenbanken und Datenquellen von Drittanbietern über einen einfachen Gewährungs- oder Widerrufmechanismus, der einem relationalen Datenbankmanagementsystem (RDBMS) ähnelt. Lake Formation Formation-Berechtigungen werden mithilfe detaillierter Kontrollen auf Spalten-, Zeilen- und Zellenebene in allen AWS Analyse- und Machine-Learning-Diensten, einschließlich Amazon Athena, Amazon Redshift Spectrum Amazon Quick, Amazon EMR und, durchgesetzt. AWS Glue

Mit dem Lake Formation Formation-Hybridzugriffsmodus für AWS Glue Data Catalog (Data Catalog) können Sie die katalogisierten Daten sichern und darauf zugreifen, indem Sie sowohl Lake Formation Formation-Berechtigungen als auch IAM-Berechtigungsrichtlinien für Amazon S3 und AWS Glue Aktionen verwenden. Im hybriden Zugriffsmodus können Datenadministratoren Lake Formation Formation-Berechtigungen selektiv und inkrementell integrieren und sich dabei jeweils auf einen Data Lake-Anwendungsfall konzentrieren.

Lake Formation ermöglicht es Ihnen auch AWS-Konten, Daten intern und extern zwischen mehreren AWS Organisationen oder direkt mit IAM-Prinzipalen in einem anderen Konto zu teilen, was einen detaillierten Zugriff auf die Datenkatalog-Metadaten und die zugrunde liegenden Daten bietet.

Themen

- [Merkmale der Lake Formation](#)
- [AWS Lake Formation: Funktionsweise](#)
- [Lake Formation komponenten](#)
- [Terminologie der Lake Formation](#)
- [AWS Serviceintegrationen mit Lake Formation](#)

- [Zusätzliche Ressourcen zur Lake Formation](#)
- [Erste Schritte mit Lake Formation](#)

Merkmale der Lake Formation

Lake Formation hilft Ihnen dabei, Datensilos aufzubrechen und verschiedene Arten strukturierter und unstrukturierter Daten in einem zentralen Repository zu kombinieren. Identifizieren Sie zunächst bestehende Datenspeicher in Amazon S3 oder relationalen und NoSQL-Datenbanken und verschieben Sie die Daten in Ihren Data Lake. Dann crawlen, katalogisieren und bereiten Sie die Daten für Analysen vor. Bieten Sie Ihren Benutzern als Nächstes sicheren Self-Service-Zugriff auf die Daten über die Analysedienste ihrer Wahl.

Sie können die Lake Formation Formation-Konsole verwenden, um mehrstufige Verbundkataloge im Datenkatalog zu erstellen und Daten in Amazon S3-Datenseen und Amazon Redshift Redshift-Data Warehouses zu vereinheitlichen. Sie können auch Daten aus Ihren Betriebsdatenbanken und Datenquellen von Drittanbietern wie Google BigQuery, MySQL usw. integrieren. Amazon DynamoDB Der Datenkatalog bietet ein zentrales Metadaten-Repository, das die Verwaltung und Erkennung von Daten in unterschiedlichen Systemen erleichtert.

Weitere Informationen finden Sie unter [Bringen Sie Ihre Daten in die AWS Glue Data Catalog](#).

Themen

- [Datenaufnahme und -verwaltung](#)
- [Sicherheitsmanagement](#)
- [Ihre Daten zum Datenkatalog hinzufügen](#)

Datenaufnahme und -verwaltung

Importieren Sie Daten aus Datenbanken, die sich bereits in AWS

Nachdem Sie angegeben haben, wo sich Ihre vorhandenen Datenbanken befinden, und Ihre Zugangsdaten angegeben haben, liest Lake Formation die Daten und ihre Metadaten (Schema), um den Inhalt der Datenquelle zu verstehen. Anschließend importiert es die Daten in Ihren neuen Data Lake und zeichnet die Metadaten in einem zentralen Katalog auf. Mit Lake Formation können Sie Daten aus MySQL-, PostgreSQL-, SQL Server-, MariaDB- und Oracle-Datenbanken importieren, die in Amazon RDS laufen oder in Amazon EC2 gehostet werden. Sowohl das Laden von Massendaten als auch das inkrementelle Laden von Daten werden unterstützt.

Importieren Sie Daten aus anderen externen Quellen

Sie können Lake Formation verwenden, um Daten aus lokalen Datenbanken zu verschieben, indem Sie eine Verbindung mit Java Database Connectivity (JDBC) herstellen. Identifizieren Sie Ihre Zielquellen und geben Sie die Zugangsdaten in der Konsole ein, und Lake Formation liest und lädt Ihre Daten in den Data Lake. Um Daten aus anderen als den oben aufgeführten Datenbanken zu importieren, können Sie benutzerdefinierte ETL-Jobs mit erstellen AWS Glue.

Katalogisieren und beschriften Sie Ihre Daten

Sie können AWS Glue Crawler verwenden, um Ihre Daten in Amazon S3 zu lesen und das Datenbank- und Tabellenschema zu extrahieren und diese Daten in einem durchsuchbaren Datenkatalog zu speichern. Verwenden Sie dann Lake Formation [Tag-basierte Zugangskontrolle von Lake Formation](#) (TBAC), um Berechtigungen für Datenbanken, Tabellen und Spalten zu verwalten. Weitere Informationen zum Hinzufügen von Tabellen zum Datenkatalog finden Sie unter [Objekte erstellen in AWS Glue Data Catalog](#)

Sicherheitsmanagement

Definieren und verwalten Sie Zugriffskontrollen

Lake Formation bietet einen zentralen Ort für die Verwaltung der Zugriffskontrollen für Daten in Ihrem Data Lake. Sie können Sicherheitsrichtlinien definieren, die den Zugriff auf Daten auf Datenbank-, Tabellen-, Spalten-, Zeilen- und Zellenebene einschränken. Diese Richtlinien gelten für IAM-Benutzer und -Rollen sowie für Benutzer und Gruppen, wenn der Verbund über einen externen Identitätsanbieter erfolgt. Sie können detaillierte Kontrollen verwenden, um auf Daten zuzugreifen, die von Lake Formation in Amazon Redshift Spectrum, Athena, AWS Glue ETL und Amazon EMR for Apache Spark gesichert wurden. Achten Sie bei der Erstellung von IAM-Identitäten darauf, dass Sie sich an die Best Practices für IAM halten. Weitere Informationen finden Sie unter [Bewährte Sicherheitsmethoden](#) im IAM-Benutzerhandbuch.

Hybrider Zugriffsmodus

Der hybride Zugriffsmodus von Lake Formation bietet die Flexibilität, Lake Formation Formation-Berechtigungen für Datenbanken und Tabellen in Ihrem Datenkatalog selektiv zu aktivieren. Mit dem Hybridzugriffsmodus verfügen Sie jetzt über einen inkrementellen Pfad, mit dem Sie Lake Formation Formation-Berechtigungen für eine bestimmte Gruppe von Benutzern festlegen können, ohne die Berechtigungsrichtlinien anderer vorhandener Benutzer oder Workloads zu unterbrechen. Weitere Informationen finden Sie unter [Hybrider Zugriffsmodus](#).

Implementieren Sie die Auditprotokollierung

Lake Formation bietet umfassende Auditprotokolle CloudTrail zur Überwachung des Zugriffs und zum Nachweis der Einhaltung zentral definierter Richtlinien. Sie können den Datenzugriffsverlauf für alle Analyse- und Machine-Learning-Dienste überprüfen, die die Daten in Ihrem Data Lake über Lake Formation lesen. Auf diese Weise können Sie sehen, welche Benutzer oder Rollen versucht haben, mit welchen Diensten und wann auf welche Daten zuzugreifen. Sie können auf die Audit-Logs genauso zugreifen wie auf alle anderen CloudTrail Logs über die CloudTrail APIs AND-Konsole. Weitere Informationen zu CloudTrail Protokollen finden Sie unter [Protokollieren AWS Lake Formation Formation-API-Aufrufen mit AWS CloudTrail](#).

Sicherheit auf Zeilen- und Zellenebene

Lake Formation bietet Datenfilter, mit denen Sie den Zugriff auf eine Kombination aus Spalten und Zeilen einschränken können. Verwenden Sie Sicherheit auf Zeilen- und Zellenebene, um sensible Daten wie personenbezogene Daten (PII) zu schützen. Weitere Informationen zur Sicherheit auf Zeilenebene finden Sie unter [Datenfilterung und Sicherheit auf Zellebene in Lake Formation](#)

Tag-basierte Zugriffskontrolle

Verwenden Sie die [attributbasierte Zugriffskontrolle](#) von Lake Formation, um Hunderte oder sogar Tausende von Datenberechtigungen zu verwalten, indem Sie benutzerdefinierte Labels, sogenannte LF-Tags, erstellen. Sie können jetzt LF-Tags definieren und sie an Datenbanken, Tabellen oder Spalten anhängen. Anschließend können Sie den kontrollierten Zugriff auf die Dienste für Analytik, maschinelles Lernen (ML) und Extrahieren, Transformieren und Laden (ETL) gemeinsam nutzen. LF-Tags stellen sicher, dass die Datenverwaltung einfach skaliert werden kann, indem die Richtliniendefinitionen von Tausenden von Ressourcen durch einige wenige logische Tags ersetzt werden. Lake Formation bietet eine textbasierte Suche über diese Metadaten, sodass Ihre Benutzer schnell die Daten finden können, die sie analysieren müssen.

Attributbasierte Zugriffskontrolle

Verwenden Sie die [attributbasierte Zugriffskontrolle, um Zugriff auf Datenkatalogobjekte](#) zu gewähren. Die attributbasierte Zugriffskontrolle (ABAC) ist eine Autorisierungsstrategie, bei der Berechtigungen auf der Grundlage von Attributen definiert werden. AWS nennt diese Attribute Tags. Sie können ABAC verwenden, um Principals innerhalb desselben Kontos oder in einem anderen Konto Zugriff auf die Datenkatalogressourcen zu gewähren. Jeder IAM-Prinzipal mit passenden Schlüsseln und Werten für das IAM-Tag oder das Sitzungs-Tag erhält Zugriff auf die Ressource. Sie müssen über erteilbare Berechtigungen für die Ressourcen verfügen, um diese Berechtigungen gewähren zu können.

Kontoübergreifender Zugriff

Die Berechtigungsverwaltungsfunktionen von Lake Formation vereinfachen die Sicherung und Verwaltung verteilter Data Lakes über mehrere AWS Konten hinweg durch einen zentralen Ansatz, der eine detaillierte Zugriffskontrolle für den Data Catalog und die Amazon S3 S3-Standorte ermöglicht. Weitere Informationen finden Sie unter [Kontoübergreifender Datenaustausch in Lake Formation](#).

Ihre Daten zum Datenkatalog hinzufügen

Die Verbundfunktion ermöglicht es Ihnen, Verbundkataloge zu erstellen und Berechtigungen für Datensätze einzurichten, die in verschiedenen Datenquellen wie Amazon Redshift gespeichert sind, ohne Daten oder Metadaten in Amazon S3 oder zu migrieren. AWS Glue Data Catalog Sie können die folgenden Methoden verwenden, um Daten abzurufen und Berechtigungen für externe Datensätze in Lake Formation zu verwalten:

Weitere Informationen finden Sie unter [Bringen Ihrer Daten in die AWS Glue Data Catalog](#).

- Daten aus Amazon Redshift Redshift-Data Warehouses in den AWS Glue Data Catalog — Registrieren Sie einen vorhandenen [Amazon Redshift Redshift-Namespace](#) oder einen Cluster mit dem Datenkatalog und erstellen Sie einen mehrstufigen Verbundkatalog im Datenkatalog.

Sie können mit jeder beliebigen Abfrage-Engine, die mit der OpenAPI-Spezifikation des Apache Iceberg REST-Katalogs kompatibel ist, wie Amazon EMR Serverless und Amazon Athena, auf Ihre Daten zugreifen.

Weitere Informationen finden Sie unter [Überführung Amazon Redshift Redshift-Daten in die AWS Glue Data Catalog](#).

- Aus externen Datenquellen mit dem Datenkatalog verbinden — Verbinden Sie den Datenkatalog mithilfe von AWS Glue Verbindungen mit externen Datenquellen und erstellen Sie Verbundkataloge, um Zugriffsberechtigungen für Datensätze mithilfe von Lake Formation zentral zu verwalten. Eine Migration von Metadaten in den Datenkatalog ist nicht erforderlich.

Weitere Informationen finden Sie unter [Zusammenführung mit externen Datenquellen in der AWS Glue Data Catalog](#).

- Integration von Amazon S3 Table Buckets mit Data Catalog — Sie können Amazon S3 S3-Tabellen als Datenkatalogobjekte veröffentlichen und katalogisieren und den Katalog als Lake Formation Formation-Datenspeicherort registrieren, entweder über die Lake Formation Formation-Konsole oder mithilfe AWS Glue APIs von.

Weitere Informationen finden Sie unter [Erstellen eines Amazon S3 Tables-Katalogs in AWS Glue Data Catalog](#).

- Kataloge zur Verwaltung von Amazon Redshift Redshift-Tabellen im Datenkatalog erstellen — Möglicherweise haben Sie derzeit weder einen Amazon Redshift Redshift-Producer-Cluster noch einen Amazon Redshift Redshift-Datashare verfügbar, möchten aber Amazon Redshift Redshift-Tabellen mithilfe von Data Catalog erstellen und verwalten. Sie können damit beginnen, einen AWS Glue verwalteten Katalog mithilfe der `glue:CreateCatalog` API oder der AWS Lake Formation Konsole zu erstellen, indem Sie den Katalogtyp auf `Managed` und `Catalog source` als `Redshift` festlegen.

Weitere Informationen finden Sie unter [Erstellen eines verwalteten Amazon Redshift Redshift-Katalogs in der AWS Glue Data Catalog](#).

- Integration von Lake Formation mit Amazon Redshift Redshift-Datenfreigabe — Verwenden Sie Lake Formation, um Zugriffsberechtigungen für [Amazon Redshift Redshift-Datenfreigaben](#) auf Datenbank-, Tabellen-, Spalten- und Zeilenebene zentral zu verwalten und den Benutzerzugriff auf Objekte innerhalb eines Datashare einzuschränken.
- Datenkatalog mit externen Metastores verbinden — Stellen Sie eine Verbindung AWS Glue Data Catalog zu externen Metastores her, um mithilfe von Lake Formation Zugriffsberechtigungen für Datensätze in Amazon S3 zu verwalten. Eine Migration von Metadaten in den Datenkatalog ist nicht erforderlich.

Weitere Informationen finden Sie unter [Verwaltung von Berechtigungen für Datensätze, die externe Metastores verwenden](#).

- Integration von Lake Formation mit AWS Data Exchange — Lake Formation unterstützt die Lizenzierung des Zugriffs auf Ihre Daten über AWS Data Exchange. Wenn Sie daran interessiert sind, Ihre Lake Formation Formation-Daten zu lizenzieren, finden Sie weitere Informationen unter [Was ist AWS Data Exchange](#) im AWS Data Exchange Benutzerhandbuch enthalten.

AWS Lake Formation: Funktionsweise

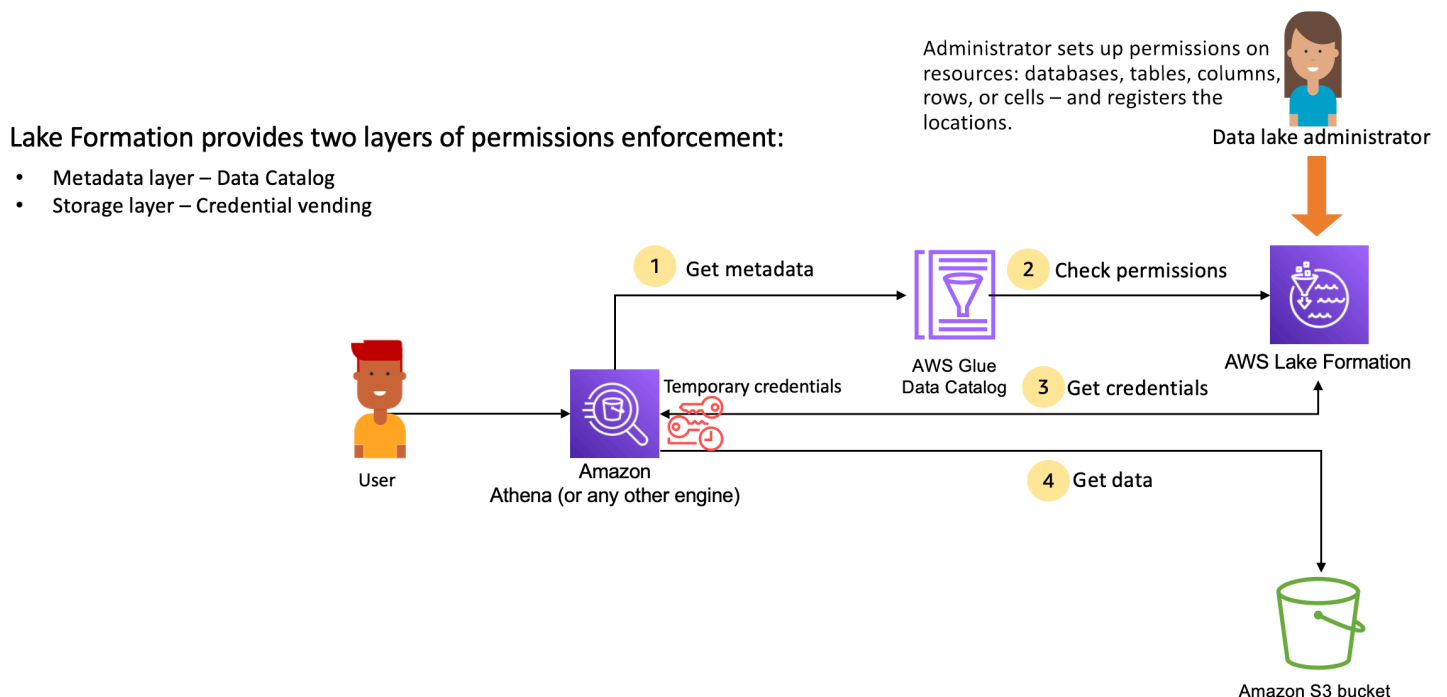
AWS Lake Formation bietet ein RDBMS-Berechtigungsmodell (Relational Database Management System), um Zugriff auf Datenkatalogressourcen wie Datenbanken, Tabellen und Spalten mit zugrunde liegenden Daten in Amazon S3 zu gewähren oder zu entziehen. Die einfach zu verwaltenden Lake Formation Formation-Berechtigungen ersetzen die komplexen Amazon S3 S3-Bucket-Richtlinien und die entsprechenden IAM-Richtlinien.

In Lake Formation können Sie Berechtigungen auf zwei Ebenen implementieren:

- Erzwingen von Berechtigungen auf Metadatenebene für Datenkatalogressourcen wie Datenbanken und Tabellen
- Verwaltung von Speicherzugriffsberechtigungen für die zugrunde liegenden Daten, die in Amazon S3 gespeichert sind, im Auftrag integrierter Engines

Workflow zur Verwaltung von Berechtigungen in Lake Formation

Lake Formation lässt sich in Analyse-Engines integrieren, um Amazon S3 S3-Datenspeicher und Metadatenobjekte abzufragen, die bei Lake Formation registriert sind. Das folgende Diagramm zeigt, wie die Rechteverwaltung in Lake Formation funktioniert.



Wichtige Schritte zur Verwaltung von Berechtigungen bei Lake Formation

Bevor Lake Formation Zugriffskontrollen für Daten in Ihrem Data Lake bereitstellen kann, richtet ein [Data Lake-Administrator](#) oder ein Benutzer mit Administratorberechtigungen individuelle Benutzerrichtlinien für Datenkatalogtabellen ein, um den Zugriff auf Datenkatalogtabellen mithilfe von Lake Formation Formations-Berechtigungen zuzulassen oder zu verweigern.

Anschließend erteilt entweder der Data Lake-Administrator oder ein vom Administrator delegierter Benutzer Lake Formation-Berechtigungen für Benutzer in den Data Catalog-Datenbanken und -Tabellen und registriert den Amazon S3 S3-Speicherort der Tabelle bei Lake Formation.

1. **Metadaten abrufen** — Ein Principal (Benutzer) sendet eine Abfrage oder ein ETL-Skript an eine [integrierte Analyse-Engine](#) wie Amazon Athena AWS Glue, Amazon EMR oder Amazon Redshift Spectrum. Die integrierte Analyse-Engine identifiziert die Tabelle, die angefordert wird, und sendet eine Anfrage nach Metadaten an den Datenkatalog.
2. **Berechtigungen überprüfen** — Der Datenkatalog überprüft die Benutzerberechtigungen mit Lake Formation. Wenn der Benutzer berechtigt ist, auf die Tabelle zuzugreifen, gibt er die Metadaten, die der Benutzer sehen darf, an die Engine zurück.
3. **Anmeldeinformationen abrufen** — Der Datenkatalog teilt der Engine mit, ob die Tabelle von Lake Formation verwaltet wird oder nicht. Wenn die zugrunde liegenden Daten bei Lake Formation registriert sind, fordert die Analyse-Engine Lake Formation auf, Datenzugriff zu gewähren, indem temporärer Zugriff gewährt wird.
4. **Daten abrufen** — Wenn der Benutzer berechtigt ist, auf die Tabelle zuzugreifen, bietet Lake Formation temporären Zugriff auf die integrierte Analyse-Engine. Mithilfe des temporären Zugriffs ruft die Analyse-Engine die Daten von Amazon S3 ab und führt die erforderlichen Filter wie Spalten-, Zeilen- oder Zellenfilterung durch. Wenn die Engine die Ausführung des Jobs beendet hat, gibt sie die Ergebnisse an den Benutzer zurück. Dieser Vorgang wird als Verkauf von [Anmeldeinformationen bezeichnet](#).

Wenn die Tabelle nicht von Lake Formation verwaltet wird, erfolgt der zweite Aufruf von der Analyse-Engine direkt an Amazon S3. Die betreffende Amazon S3 S3-Bucket-Richtlinie und die IAM-Benutzerrichtlinie werden im Hinblick auf den Datenzugriff bewertet.

Wenn Sie IAM-Richtlinien verwenden, stellen Sie sicher, dass Sie die bewährten IAM-Methoden befolgen. Weitere Informationen finden Sie unter [Bewährte Methoden für die Sicherheit in IAM](#) im IAM-Benutzerhandbuch.

Themen

- [Berechtigungen für Metadaten](#)
- [Verwaltung des Speicherzugriffs](#)
- [Kontoübergreifender Datenaustausch in Lake Formation](#)

Berechtigungen für Metadaten

Lake Formation bietet Autorisierung und Zugriffskontrolle für den Datenkatalog. Wenn eine IAM-Rolle von einem beliebigen System aus einen Datenkatalog-API-Aufruf durchführt, überprüft der

Datenkatalog die Datenberechtigungen des Benutzers und gibt nur die Metadaten zurück, für die der Benutzer Zugriffsberechtigungen besitzt. Wenn eine IAM-Rolle beispielsweise Zugriff auf nur eine Tabelle innerhalb einer Datenbank hat und ein Dienst oder ein Benutzer davon ausgeht, dass die Rolle den `GetTables` Vorgang ausführt, enthält die Antwort unabhängig von der Anzahl der Tabellen in der Datenbank nur die eine Tabelle.

Standardeinstellungen — **IAMAllowedPrincipal** Gruppenberechtigungen

AWS Lake Formation, legt standardmäßig Berechtigungen für alle Datenbanken und Tabellen einer virtuellen Gruppe mit dem Namen `festIAMAllowedPrincipal`. Diese Gruppe ist einzigartig und nur innerhalb von Lake Formation sichtbar. Die `IAMAllowedPrincipal` Gruppe umfasst alle IAM-Prinzipale, die über IAM-Prinzipal- und AWS Glue Ressourcenrichtlinien Zugriff auf Datenkatalogressourcen haben. Wenn diese Berechtigungen für eine Datenbank oder Tabelle vorhanden sind, erhalten alle Prinzipale Zugriff auf die Datenbank oder Tabelle.

Wenn Sie detailliertere Berechtigungen für eine Datenbank oder Tabelle bereitstellen möchten, entfernen Sie die `IAMAllowedPrincipal` Berechtigung und Lake Formation setzt alle anderen Richtlinien durch, die mit dieser Datenbank oder Tabelle verknüpft sind. Wenn es beispielsweise eine Richtlinie gibt, die es Benutzer A erlaubt, mit `DESCRIBE` Berechtigungen auf Datenbank A zuzugreifen, und diese mit allen Berechtigungen `IAMAllowedPrincipal` vorhanden ist, führt Benutzer A weiterhin alle anderen Aktionen aus, bis die `IAMAllowedPrincipal` Berechtigung widerrufen wird.

Darüber hinaus verfügt die `IAMAllowedPrincipal` Gruppe standardmäßig über Berechtigungen für alle neuen Datenbanken und Tabellen, wenn diese erstellt werden. Es gibt zwei Konfigurationen, die dieses Verhalten steuern. Die erste ist auf Konto- und Regionsebene, sodass dies für neu erstellte Datenbanken möglich ist, und die zweite auf Datenbankebene. Informationen zum Ändern der Standardeinstellung finden Sie unter [Ändern Sie das Standardberechtigungsmodell oder verwenden Sie den hybriden Zugriffsmodus](#)

Gewähren von Berechtigungen

Data Lake-Administratoren können Prinzipalen Datenkatalogberechtigungen gewähren, sodass die Prinzipale Datenbanken und Tabellen erstellen und verwalten und auf die zugrunde liegenden Daten zugreifen können.

Berechtigungen auf Datenbank- und Tabellenebene

Wenn Sie innerhalb von Lake Formation Berechtigungen gewähren, muss der Gewährer den Principal angeben, für den Berechtigungen erteilt werden sollen, für welche Ressourcen

Berechtigungen erteilt werden sollen und für welche Aktionen der Empfänger Zugriff haben soll. Bei den meisten Ressourcen innerhalb von Lake Formation sind die Hauptliste und die Ressourcen für die Erteilung von Berechtigungen ähnlich, aber die Aktionen, die ein Empfänger ausführen kann, unterscheiden sich je nach Ressourcentyp. Beispielsweise sind für Tabellen SELECT Berechtigungen zum Lesen der Tabellen verfügbar, für Datenbanken jedoch keine SELECT Berechtigungen. Die CREATE_TABLE Berechtigung ist für Datenbanken zulässig, nicht jedoch für Tabellen.

Sie können AWS Lake Formation Berechtigungen auf zwei Arten gewähren:

- [Methode für benannte Ressourcen](#) — Ermöglicht es Ihnen, Datenbank- und Tabellennamen auszuwählen und Benutzern gleichzeitig Berechtigungen zu gewähren.
- [LF-Tag-basierte Zugriffskontrolle \(LF-TBAC\)](#) — Benutzer erstellen LF-Tags, ordnen sie Datenkatalogressourcen zu, gewähren Berechtigungen für LF-Tags, ordnen einzelnen Benutzern Berechtigungen zu und schreiben Describe LF-Berechtigungsrichtlinien mithilfe von LF-Tags für verschiedene Benutzer. Solche LF-Tag-based Richtlinien gelten für alle Datenkatalogressourcen, die mit diesen LF-Tag-Werten verknüpft sind.

 Note

LF-Tags gibt es nur bei Lake Formation. Sie sind nur in Lake Formation sichtbar und sollten nicht mit AWS Resource-Tags verwechselt werden.

LF-TBAC ist eine Funktion, mit der Benutzer Ressourcen in benutzerdefinierte Kategorien von LF-Tags gruppieren und Berechtigungen auf diese Ressourcengruppen anwenden können. Daher ist dies der beste Weg, um Berechtigungen für eine große Anzahl von Datenkatalogressourcen zu skalieren.

Weitere Informationen finden Sie unter [Tag-basierte Zugangskontrolle von Lake Formation](#).

Wenn Sie einem Prinzipal Berechtigungen gewähren, bewertet Lake Formation die Berechtigungen als Zusammenfassung aller Richtlinien für diesen Benutzer. Wenn Sie beispielsweise zwei Richtlinien für eine Tabelle für einen Prinzipal haben, wobei eine Richtlinie über die benannte Ressourcenmethode Berechtigungen für die Spalten col1, col2 und col3 gewährt und die andere Richtlinie Col5 und col6 über LF-Tags Berechtigungen für dieselbe Tabelle und denselben Principal gewährt, sind die effektiven Berechtigungen eine Vereinigung der Berechtigungen, nämlich col1, col2, col3, col5 und col6. Dazu gehören auch Datenfilter und Zeilen.

Berechtigungen zum Speicherort von Daten

Datenstandortberechtigungen bieten Benutzern ohne Administratorrechte die Möglichkeit, Datenbanken und Tabellen an bestimmten Amazon S3 S3-Standorten zu erstellen. Wenn ein Benutzer versucht, eine Datenbank oder eine Tabelle an einem Ort zu erstellen, zu dessen Erstellung er nicht berechtigt ist, schlägt die Erstellungsaufgabe fehl. Auf diese Weise wird verhindert, dass Benutzer Tabellen an beliebigen Stellen innerhalb des Data Lake erstellen, und ermöglicht die Kontrolle darüber, wo diese Benutzer Daten lesen und schreiben können. Beim Erstellen von Tabellen am Amazon S3 S3-Speicherort innerhalb der Datenbank, in der sie erstellt werden, besteht eine implizite Berechtigung. Weitere Informationen finden Sie unter [Erteilung von Berechtigungen zum Speicherort von Daten](#).

Tabellen- und Datenbankberechtigungen erstellen

Benutzer ohne Administratorrechte sind standardmäßig nicht berechtigt, Datenbanken oder Tabellen innerhalb einer Datenbank zu erstellen. Die Datenbankerstellung wird auf Kontoebene mithilfe der Lake Formation Formation-Einstellungen gesteuert, sodass nur autorisierte Prinzipale Datenbanken erstellen können. Weitere Informationen finden Sie unter [Erstellen einer Datenbank](#). Um eine Tabelle zu erstellen, benötigt ein Principal CREATE_TABLE Berechtigungen für die Datenbank, in der die Tabelle erstellt wird. Weitere Informationen finden Sie unter [Erstellen von Tabellen](#).

Implizite und explizite Berechtigungen

Lake Formation bietet implizite Berechtigungen, abhängig von der Persona und den Aktionen, die die Persona ausführt. Beispielsweise erhalten Data Lake-Administratoren automatisch DESCRIBE Berechtigungen für alle Ressourcen im Datenkatalog, Datenspeicherberechtigungen für alle Standorte, Berechtigungen zum Erstellen von Datenbanken und Tabellen an allen Speicherorten sowie Grant Revoke Berechtigungen für jede Ressource. Datenbankersteller erhalten automatisch alle Datenbankberechtigungen für die von ihnen erstellten Datenbanken, und Tabellenersteller erhalten alle Berechtigungen für die von ihnen erstellten Tabellen. Weitere Informationen finden Sie unter [Implizite Lake Formation Formation-Berechtigungen](#).

Erteilbare Berechtigungen

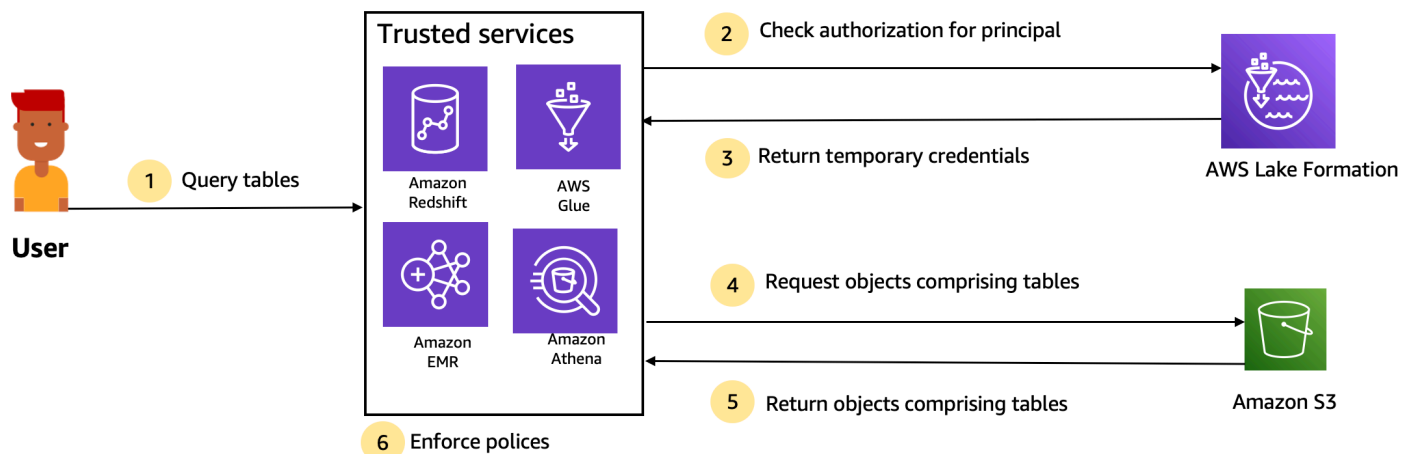
Data Lake-Administratoren können die Verwaltung von Berechtigungen an Benutzer ohne Administratorrechte delegieren, indem sie erteilbare Berechtigungen bereitstellen. Wenn einem Prinzipal erteilbare Berechtigungen für eine Ressource und eine Reihe von Berechtigungen zugewiesen werden, erhält dieser Principal die Möglichkeit, anderen Prinzipalen Berechtigungen für diese Ressource zu erteilen.

Verwaltung des Speicherzugriffs

Lake Formation verwendet die [Verkaufsfunktion für Anmeldeinformationen](#), um temporären Zugriff auf Amazon S3 S3-Daten zu ermöglichen. Der Verkauf von Anmeldeinformationen oder Token-Verkauf ist ein gängiges Muster, bei dem Benutzern, Diensten oder einer anderen Entität temporäre Anmeldeinformationen zur Verfügung gestellt werden, um kurzfristigen Zugriff auf eine Ressource zu gewähren.

Lake Formation nutzt dieses Muster, um kurzfristigen Zugriff auf AWS Analysedienste wie Athena zu ermöglichen, um im Namen des anrufenden Principals auf Daten zuzugreifen. Bei der Erteilung von Berechtigungen müssen Benutzer ihre Amazon S3-Bucket-Richtlinien oder IAM-Richtlinien nicht aktualisieren und benötigen keinen direkten Zugriff auf Amazon S3.

Das folgende Diagramm zeigt, wie Lake Formation temporären Zugriff auf registrierte Standorte bietet:



Trusted services enforce AWS Lake Formation policies (distributed enforcement with fail close).

1. Ein Principal (Benutzer) gibt über einen vertrauenswürdigen integrierten Service wie Athena, Amazon EMR, Redshift Spectrum oder eine Anfrage nach Daten für eine Tabelle ein. AWS Glue
2. Der integrierte Dienst prüft, ob die Tabelle und die angeforderten Spalten von Lake Formation autorisiert wurden, und trifft eine Autorisierungsfeststellung. Wenn der Benutzer nicht autorisiert ist, verweigert Lake Formation den Zugriff auf Daten und die Abfrage schlägt fehl.
3. Nachdem die Autorisierung erfolgreich war und die Speicherautorisierung für die Tabelle und den Benutzer aktiviert wurde, ruft der integrierte Dienst temporäre Anmeldeinformationen von Lake Formation ab, um auf die Daten zuzugreifen.
4. Der integrierte Service verwendet die temporären Anmeldeinformationen von Lake Formation, um Objekte von Amazon S3 anzufordern.

5. Amazon S3 stellt die Amazon S3 S3-Objekte für den integrierten Service bereit. Die Amazon S3 S3-Objekte enthalten alle Daten aus der Tabelle.
6. Der integrierte Service sorgt für die erforderliche Durchsetzung der Lake Formation Richtlinien, wie z. B. die Filterung auf Spalten-, Zeilen- und/oder Zellenebene. Der integrierte Dienst verarbeitet die Abfragen und gibt die Ergebnisse an den Benutzer zurück.

Aktivieren Sie die Durchsetzung von Berechtigungen auf Speicherebene für Datenkatalogtabellen

Standardmäßig ist die Durchsetzung auf Speicherebene für Tabellen im Datenkatalog nicht aktiviert. Um die Durchsetzung auf Speicherebene zu aktivieren, müssen Sie den Amazon S3 S3-Standort Ihrer Quelldaten bei Lake Formation registrieren und eine IAM-Rolle angeben. Berechtigungen auf Speicherebene werden für alle Tabellen mit demselben Tabellenspeicherpfad oder Präfix des Amazon S3 S3-Standorts aktiviert.

Wenn ein integrierter Dienst im Namen eines Benutzers Zugriff auf den Datenstandort anfordert, übernimmt der Lake Formation Formation-Dienst diese Rolle und gibt die Anmeldeinformationen mit eingeschränkten Berechtigungen für die Ressource an den angeforderten Dienst zurück, sodass der Datenzugriff erfolgen kann. Die registrierte IAM-Rolle muss über den gesamten erforderlichen Zugriff auf den Amazon S3 S3-Standort verfügen, einschließlich der AWS KMS Schlüssel.

Weitere Informationen finden Sie unter [Registrierung eines Amazon S3 S3-Standorts](#).

Unterstützte Dienste AWS

AWS Analysedienste wie Athena, Redshift Spectrum, Amazon EMR, AWS Glue Amazon Quick, und Amazon SageMaker AI lassen sich mithilfe der AWS Lake Formation Credential Vending-API-Operationen in Lake Formation integrieren. Eine vollständige Liste der AWS Dienste, die in Lake Formation integriert sind, sowie die Granularitätsstufen und Tabellenformate, die sie unterstützen, finden [Zusammenarbeit mit anderen AWS Diensten](#) Sie unter.

Kontoübergreifender Datenaustausch in Lake Formation

Mit Lake Formation können Sie Datenkatalogressourcen (Datenbanken und Tabellen) innerhalb eines AWS Kontos und kontenübergreifend in einem einfachen Setup mithilfe der benannten Ressourcenmethode oder LF-Tags gemeinsam nutzen. Sie können eine gesamte Datenbank oder ausgewählte Tabellen aus einer Datenbank für beliebige IAM-Prinzipale (IAM-Rollen und -Benutzer) in einem Konto, für andere AWS Konten auf Kontoebene oder direkt für IAM-Prinzipale in einem anderen Konto gemeinsam nutzen.

Sie können Datenkatalogtabellen auch mit Datenfiltern gemeinsam nutzen, um den Zugriff auf die Details auf Zeilen- und Zellenebene einzuschränken. Lake Formation verwendet AWS Resource Access Manager (AWS RAM), um die Erteilung von Berechtigungen zwischen Konten zu erleichtern. Wenn eine Ressource von zwei Konten gemeinsam genutzt wird, werden Einladungen an das Empfängerkonto AWS RAM gesendet. Wenn ein Benutzer eine Einladung zum AWS RAM Teilen annimmt, AWS RAM gewährt er Lake Formation die erforderlichen Berechtigungen, um die Datenkatalogressourcen verfügbar zu haben, und aktiviert die Durchsetzung der Speicherebene. Weitere Informationen finden Sie unter [Kontoübergreifender Datenaustausch in Lake Formation](#).

Wenn der Data Lake-Administrator des Empfängerkontos die AWS RAM Freigabe akzeptiert, sind die gemeinsam genutzten Ressourcen im Empfängerkonto verfügbar. Der Data Lake-Administrator erteilt zusätzlichen IAM-Prinzipalen im Empfängerkonto weitere Lake Formation Formation-Berechtigungen für die gemeinsam genutzte Ressource, sofern der Administrator über GRANTABLE Berechtigungen für die gemeinsam genutzte Ressource verfügt.

Die Principals können die gemeinsam genutzten Ressourcen jedoch nicht mit Athena oder Redshift Spectrum ohne Ressourcenlink abfragen. Ein Ressourcenlink ist eine Entität im Datenkatalog und ähnelt einem Linux-Symlink-Konzept.

Der Data Lake-Administrator des Empfängerkontos erstellt einen Ressourcenlink auf der gemeinsam genutzten Ressource. Der Administrator erteilt weiteren Benutzern `Describe` Berechtigungen für den Ressourcenlink mit den erforderlichen Berechtigungen für die ursprüngliche gemeinsam genutzte Ressource. Ein Benutzer im Empfängerkonto kann dann den Ressourcenlink verwenden, um die gemeinsam genutzte Ressource mithilfe von Athena und Redshift Spectrum abzufragen. Weitere Informationen zu Ressourcenlinks finden Sie unter [Ressourcenlinks erstellen](#).

Lake Formation komponenten

AWS Lake Formation stützt sich bei der Erstellung und Verwaltung Ihres Data Lakes auf das Zusammenspiel mehrerer Komponenten.

Lake Formation Formation-Konsole

Sie verwenden die Lake Formation Formation-Konsole, um Ihren Data Lake zu definieren und zu verwalten und Lake Formation Formation-Berechtigungen zu erteilen und zu widerrufen. Sie können Blueprints auf der Konsole verwenden, um Daten zu erkennen, zu bereinigen, zu transformieren und aufzunehmen. Sie können den Zugriff auf die Konsole auch für einzelne Lake Formation Formation-Benutzer aktivieren oder deaktivieren.

Lake Formation API und Befehlszeilenschnittstelle

Lake Formation bietet API-Operationen über mehrere sprachspezifische SDKs und die AWS Command Line Interface (AWS CLI). Die Lake Formation API funktioniert in Verbindung mit dem AWS Glue API. Die Lake Formation API konzentriert sich hauptsächlich auf die Verwaltung von Lake Formation-Berechtigungen, während die AWS Glue API bietet eine Datenkatalog-API und eine verwaltete Infrastruktur für die Definition, Planung und Ausführung von ETL-Vorgängen für Ihre Daten.

Für Informationen über AWS Glue API finden Sie im [AWS Glue Entwicklerhandbuch](#). Informationen zur Verwendung von finden Sie in der [AWS CLI Befehlsreferenz](#). AWS CLI

Andere AWS Dienste

Lake Formation nutzt die folgenden Dienste:

- [AWS Glue](#) zur Orchestrierung von Jobs und Crawlern zur Transformation von Daten mithilfe der AWS Glue transformiert.
- [IAM](#) erteilt den Prinzipalen von Lake Formation Berechtigungsrichtlinien. Das Lake Formation-Berechtigungsmodell erweitert das IAM-Berechtigungsmodell, um Ihren Data Lake zu sichern.

Terminologie der Lake Formation

Im Folgenden sind einige wichtige Begriffe aufgeführt, denen Sie in diesem Handbuch begegnen werden.

Datensee

Der Data Lake sind Ihre persistenten Daten, die in Amazon S3 gespeichert und von Lake Formation mithilfe eines Datenkatalogs verwaltet werden. Ein Data Lake speichert in der Regel Folgendes:

- Strukturierte und unstrukturierte Daten
- Rohdaten und transformierte Daten

Damit sich ein Amazon S3 S3-Pfad innerhalb eines Data Lake befindet, muss er bei Lake Formation registriert sein.

Datenzugriff

Lake Formation bietet sicheren und detaillierten Zugriff auf Daten durch ein neues Modell zur Gewährung und Widerruf von Berechtigungen, das die AWS Identity and Access Management (IAM) -Richtlinien erweitert.

Analysten und Datenwissenschaftler können das gesamte Portfolio an AWS Analyse- und Machine-Learning-Diensten wie Amazon Athena nutzen, um auf die Daten zuzugreifen. Die konfigurierten Sicherheitsrichtlinien von Lake Formation stellen sicher, dass Benutzer nur auf die Daten zugreifen können, für die sie autorisiert sind.

Hybrider Zugriffsmodus

Im Hybrid-Zugriffsmodus können Sie die katalogisierten Daten sichern und darauf zugreifen, indem Sie sowohl Lake Formation Formation-Berechtigungen als auch IAM- und Amazon S3 S3-Berechtigungen verwenden. Der hybride Zugriffsmodus ermöglicht es Datenadministratoren, Lake Formation Formation-Berechtigungen selektiv und inkrementell zu integrieren und sich dabei jeweils auf einen Data Lake-Anwendungsfall zu konzentrieren.

Blueprint

Ein Blueprint ist eine Datenverwaltungsvorlage, mit der Sie Daten einfach in einen Data Lake aufnehmen können. Lake Formation bietet mehrere Blueprints, jeweils für einen vordefinierten Quelltyp, z. B. eine relationale Datenbank oder AWS CloudTrail Protokolle. Aus einem Blueprint können Sie einen Workflow erstellen. Workflows bestehen aus AWS Glue Crawlern, Jobs und Triggern, die generiert werden, um das Laden und Aktualisieren von Daten zu orchestrieren. Blueprints verwenden die Datenquelle, das Datenziel und den Zeitplan als Eingabe für die Konfiguration des Workflows.

Workflow

Ein Workflow ist ein Container für eine Reihe verwandter AWS Glue Jobs, Crawler und Trigger. Sie erstellen den Workflow in Lake Formation und er wird ausgeführt in AWS Glue Dienst. Lake Formation kann den Status eines Workflows als eine Einheit verfolgen.

Wenn Sie einen Workflow definieren, wählen Sie den Blueprint aus, auf dem er basiert. Anschließend können Sie Workflows nach Bedarf oder nach einem Zeitplan ausführen.

Workflows, die Sie in Lake Formation erstellen, sind sichtbar in AWS Glue Konsole als gerichteter azyklischer Graph (DAG). Mithilfe der DAG können Sie den Fortschritt des Workflows verfolgen und Problembhebungen durchführen.

Data Catalog

Der Datenkatalog ist Ihr persistenter Metadatenpeicher. Es handelt sich um einen verwalteten Dienst, mit dem Sie Metadaten in der AWS Cloud genauso speichern, kommentieren und teilen können, wie Sie es in einem Apache Hive-Metastore tun würden. Es bietet ein einheitliches Repository, in dem unterschiedliche Systeme Metadaten speichern und finden können, um Daten in Datensilos zu verfolgen, und diese Metadaten dann zur Abfrage und Transformation der Daten verwenden können. Lake Formation verwendet die AWS Glue Datenkatalog zum Speichern von Metadaten über Data Lakes, Datenquellen, Transformationen und Ziele.

Metadaten zu Datenquellen und Zielen liegen in Form von Datenbanken und Tabellen vor. In Tabellen werden Schemainformationen, Standortinformationen und mehr gespeichert. Datenbanken sind Sammlungen von Tabellen. Lake Formation bietet eine Hierarchie von Berechtigungen zur Steuerung des Zugriffs auf Datenbanken und Tabellen im Datenkatalog.

Jedes AWS Konto hat einen Datenkatalog pro AWS Region.

Zugrundeliegende Daten

Zugrundeliegende Daten beziehen sich auf die Quelldaten oder Daten innerhalb der Data Lakes, auf die Datenkatalogtabellen verweisen.

Auftraggeber

Ein Principal ist ein AWS Identity and Access Management (IAM-) Benutzer oder eine Rolle oder ein Active Directory-Benutzer.

Data Lake-Administrator

Ein Data Lake-Administrator ist ein Principal, der jedem Prinzipal (auch sich selbst) alle Berechtigungen für jede Datenkatalogressource oder jeden Datenspeicherort erteilen kann. Benennen Sie einen Data Lake-Administrator als ersten Benutzer des Datenkatalogs. Dieser Benutzer kann dann anderen Prinzipalen detailliertere Berechtigungen für Ressourcen gewähren.

Note

IAM-Administratorbenutzer — Benutzer mit der AdministratorAccess AWS verwalteten Richtlinie — sind nicht automatisch Data Lake-Administratoren. Beispielsweise können sie Lake Formation Formation-Berechtigungen für Katalogobjekte nur gewähren, wenn ihnen die entsprechenden Berechtigungen erteilt wurden. Sie können jedoch die Lake Formation Formation-Konsole oder die API verwenden, um sich als Data Lake-Administratoren zu bezeichnen.

Informationen zu den Funktionen eines Data Lake-Administrators finden Sie unter [Implizite Lake Formation Formation-Berechtigungen](#). Informationen zur Benennung eines Benutzers als Data Lake-Administrator finden Sie unter [Erstellen Sie einen Data Lake-Administrator](#).

AWS Serviceintegrationen mit Lake Formation

Sie können Lake Formation verwenden, um Zugriffsberechtigungen auf Datenbank-, Tabellen- und Spaltenebene für in Amazon S3 gespeicherte Daten zu verwalten. Nachdem Ihre Daten bei Lake Formation registriert wurden, können Sie AWS Analysedienste wie Amazon Athena AWS Glue, Amazon Redshift Spectrum und Amazon EMR verwenden, um die Daten abzufragen. Die folgenden AWS Dienste sind in Lake Formation Formation-Berechtigungen integriert AWS Lake Formation und respektieren diese.

AWS Dienst	Integrationsdetails
AWS Glue	Referenzthema: Verwenden mit AWS Lake Formation AWS Glue AWS Glue und Lake Formation teilen sich denselben Datenkatalog. Für Konsolenoperationen (z. B. das Anzeigen einer Tabellenliste) und alle API-Operationen können AWS Glue Benutzer nur auf die Datenbanken und Tabellen zugreifen, für die sie Lake Formation Formation-Berechtigungen haben.
Amazon Athena	Referenzthema: Verwendung AWS Lake Formation mit Amazon Athena Verwenden Sie Lake Formation, um Berechtigungen zum Lesen von Daten in Amazon S3 zuzulassen oder zu verweigern. Wenn

AWS Dienst	Integrationsdetails
	Amazon Athena Benutzer den AWS Glue Katalog im Abfrage-Editor auswählen, können sie nur die Datenbanken, Tabellen und Spalten abfragen, für die sie Lake Formation Formation-Berechtigungen haben. Abfragen, die Manifeste verwenden, werden nicht unterstützt. Derzeit unterstützt Lake Formation die Verwaltung von Berechtigungen für Schreiboperationen wie VACUUMMERGE, UPDATE und OPTIMIZE für Tabellen in Open Table Formats nicht. Neben Principals, die sich über AWS Identity and Access Management (IAM) bei Athena authentifizieren, unterstützt Lake Formation Athena-Benutzer, die sich über den JDBC- oder ODBC-Treiber verbinden und sich über SAML authentifizieren. Zu den unterstützten SAML-Anbietern gehören Okta und Microsoft Active Directory Federation Service (AD FS).
Amazon Redshift Spectrum	Referenzthema: Verwendung AWS Lake Formation mit Amazon Redshift Spectrum Wenn Amazon Redshift Redshift-Benutzer ein externes Schema für eine Datenbank in der erstellen AWS Glue Data Catalog, können sie nur die Tabellen und Spalten in diesem Schema abfragen, für die sie Lake Formation Formation-Berechtigungen haben.
Amazon Quick Enterprise Edition	Referenz: Verwendung mit Quick AWS Lake Formation Wenn ein Amazon Quick Enterprise Edition-Benutzer einen Datensatz an einem Amazon S3 S3-Standort abfragt, muss der Benutzer über die Lake Formation SELECT Formation-Berechtigung für die Daten verfügen.

AWS Dienst	Integrationsdetails
Amazon EMR	Referenz: Verwendung AWS Lake Formation mit Amazon EMR Sie können Lake Formation Formation-Berechtigungen integrieren, wenn Sie einen Amazon EMR-Cluster mit einer Runtime-Rolle erstellen. Eine Runtime-Rolle ist eine IAM-Rolle, die Sie Amazon EMR-Aufrufen oder -Abfragen zuordnen. Amazon EMR verwendet diese Rolle dann für den Zugriff auf Ressourcen. AWS

Lake Formation arbeitet auch mit [AWS Key Management Service](#)(AWS KMS), damit Sie diese integrierten Dienste zum Verschlüsseln und Entschlüsseln von Daten an Amazon Simple Storage Service (Amazon S3) -Standorten einfacher einrichten können.

Zusätzliche Ressourcen zur Lake Formation

Für weitere Informationen zu empfehlen wir Ihnen AWS Lake Formation, sich anhand der folgenden Ressourcen weiter mit den in diesem Handbuch vorgestellten Konzepten vertraut zu machen:

Themen

- [Blogs](#)
- [Technische Vorträge und Webinare](#)
- [Moderne Architektur](#)
- [Daten-Mesh-Ressourcen](#)
- [Leitfäden mit bewährten Verfahren](#)

Blogs

- [AWS Lake Formation Jahresrückblick 2022](#)
- [Hochgradig belastbare moderne Datenarchitektur für mehrere Regionen](#)
- [Kontoübergreifende gemeinsame Nutzung mithilfe von LF-Tags zur direkten Steuerung von IAM-Prinzipalen](#)
- [Inventar-Dashboard für Lake Formation Formation-Berechtigungen](#)

- [Ereignisgesteuertes Datennetz](#)

Technische Vorträge und Webinare

- re:Invent 2020 — [Data Lakes: Einfach erstellen, sichern und](#) mit anderen teilen AWS Lake Formation
- re:Invent 2022 — [Aufbau und Betrieb eines Datalakes](#) auf Amazon S3
- AWS Summit SF 2022 — Eine moderne [Datenarchitektur verstehen und umsetzen](#)
- AWS Summit ATL 2022 — [Moderne Data Lakes mit AWS Lake Formation Amazon Redshift und AWS Glue](#)
- AWS Summit ANZ 2022 — [Data Lakes, Seehäuser und Data Mesh: was, warum und wie?](#)
- AWS Online Tech Talks — [Vereinfachung von Berechtigungen und Verwaltung in Ihrem Data Lake](#)

Moderne Architektur

- [Moderne Architekturmuster](#)

Daten-Mesh-Ressourcen

- [Erstellen Sie mithilfe von AWS Lake Formation Tag-basierter Zugriffskontrolle eine moderne Datenarchitektur und ein massstabsgerechtes Datenmaschenmuster](#)
- [Wie JPMorgan Chase eine Data-Mesh-Architektur entwickelte, um einen erheblichen Mehrwert für die Verbesserung seiner Unternehmensdatenplattform zu erzielen](#)
- [Erstellen Sie ein Datennetz auf AWS](#)

Leitfäden mit bewährten Verfahren

- [AWS Lake Formation Leitfäden zu bewährten Verfahren](#)

Erste Schritte mit Lake Formation

Wir empfehlen Ihnen, dass Sie mit den folgenden Abschnitten beginnen:

- [AWS Lake Formation: Funktionsweise](#)— Erfahren Sie mehr über die grundlegende Terminologie und das Zusammenspiel der verschiedenen Komponenten.
- [Erste Schritte mit Lake Formation](#)— Informieren Sie sich über die Voraussetzungen und erledigen Sie wichtige Einrichtungsaufgaben.
- [AWS Lake Formation Tutorials](#)— Folgen Sie den step-by-step Tutorials, um zu lernen, wie Sie Lake Formation verwenden.
- [Sicherheit in AWS Lake Formation](#)— Erfahren Sie, wie Sie dazu beitragen können, den Zugriff auf Daten in Lake Formation zu sichern.

Erste Schritte mit Lake Formation

Wenn Sie sich noch nicht angemeldet haben AWS oder Hilfe beim Einstieg benötigen, sollten Sie unbedingt die folgenden Aufgaben ausführen.

Themen

- [Erledigen Sie die Aufgaben zur AWS Erstkonfiguration](#)
- [Richten AWS Lake Formation](#)
- [AWS GlueDatenberechtigungen für das AWS Lake Formation Modell aktualisieren](#)
- [AWS Lake Formation und Schnittstellen-VPC-Endpunkte \(\)AWS PrivateLink](#)

Erledigen Sie die Aufgaben zur AWS Erstkonfiguration

Um AWS Lake Formation zu nutzen, müssen Sie zuerst die folgenden Schritte ausführen:

Topics

- [Melde dich an für ein AWS-Konto](#)
- [Erstellen eines Benutzers mit Administratorzugriff](#)
- [Erteilen programmgesteuerten Zugriffs](#)

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/die-Anmeldung>.
2. Folgen Sie den Online-Anweisungen.

Während der Anmeldung erhalten Sie einen Telefonanruf oder eine Textnachricht und müssen 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. Als bewährte Sicherheitsmethode weisen Sie einem Benutzer Administratorzugriff zu und verwenden Sie nur den Root-Benutzer, um [Aufgaben auszuführen, die Root-Benutzerzugriff erfordern](#).

AWS sendet Ihnen nach Abschluss des Anmeldevorgangs eine Bestätigungs-E-Mail. Du kannst jederzeit deine aktuellen Kontoaktivitäten einsehen und dein Konto verwalten, indem du zu <https://aws.amazon.com/> gehst und Mein Konto auswählst.

Erstellen eines Benutzers 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-Managementkonsole](#) 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 eines Benutzers 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 Administratorbenutzer im IAM Identity Center Benutzerzugriff.

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

Anmelden als Administratorbenutzer

- 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 Access-Portal](#).

Weiteren Benutzern Zugriff zuweisen

1. Erstellen Sie im IAM-Identity-Center einen Berechtigungssatz, der den bewährten Vorgehensweisen für die Anwendung von geringsten Berechtigungen folgt.

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

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

Eine genaue Anleitung finden Sie unter [Gruppen hinzufügen](#) im AWS IAM Identity Center - Benutzerhandbuch.

Erteilen programmgesteuerten Zugriffs

Benutzer benötigen programmatischen Zugriff, wenn sie mit AWS außerhalb des Interagierens möchten. AWS-Managementkonsole Die Art und Weise, wie programmatischer Zugriff gewährt wird, hängt vom Benutzertyp ab, der zugreift. AWS

Um Benutzern programmgesteuerten Zugriff zu gewähren, wählen Sie eine der folgenden Optionen.

Welcher Benutzer benötigt programmgesteuerten Zugriff?	Bis	Von
IAM	(Empfohlen) Verwenden Sie Konsolenanmeldeinformationen als temporäre Anmeldeinformationen, um programmatische Anfragen an AWS CLI	Befolgen Sie die Anweisungen für die Schnittstelle, die Sie verwenden möchten.

Welcher Benutzer benötigt programmgesteuerten Zugriff?	Bis	Von
	AWS SDKs, oder zu signieren . AWS APIs	• Informationen zum AWS CLI finden Sie unter Anmeldung für AWS lokale Entwicklung im AWS Command Line Interface Benutzerhandbuch. • Weitere Informationen finden Sie unter Anmeldung für AWS lokale Entwicklung im Referenzhandbuch AWS SDKs und im Tools-Referenzhandbuch. AWS SDKs
Mitarbeiteridentität (Benutzer, die in IAM Identity Center verwaltet werden)	Verwenden Sie temporäre Anmeldeinformationen, um programmatische Anfragen an das AWS CLI AWS SDKs, oder AWS APIs zu signieren.	Befolgen Sie die Anweisungen für die Schnittstelle, die Sie verwenden möchten. • Informationen zu den AWS CLI finden Sie unter Konfiguration der AWS CLI zur Verwendung AWS IAM Identity Center im AWS Command Line Interface Benutzerhandbuch. • Informationen zu AWS SDKs Tools und AWS APIs finden Sie unter IAM Identity Center-Authentifizierung im Referenzhandbuch AWS SDKs und im Tools-Referenzhandbuch.

Welcher Benutzer benötigt programmgesteuerten Zugriff?	Bis	Von
IAM	Verwenden Sie temporäre Anmeldeinformationen, um programmatische Anfragen an das AWS CLI AWS SDKs, oder zu signieren. AWS APIs	Folgen Sie den Anweisungen unter Verwenden temporärer Anmeldeinformationen mit AWS Ressourcen im IAM-Benutzerhandbuch.
IAM	(Nicht empfohlen) Verwenden Sie langfristige Anmeldeinformationen, um programmatische Anfragen an das AWS CLI AWS SDKs, oder zu signieren. AWS APIs	Befolgen Sie die Anweisungen für die Schnittstelle, die Sie verwenden möchten. • Informationen dazu AWS CLI finden Sie unter Authentifizierung mithilfe von IAM-Benutzeranmeldinformationen im AWS Command Line Interface Benutzerhandbuch. • Informationen zu AWS SDKs und Tools finden Sie unter Authentifizieren mit langfristigen Anmeldeinformationen im Referenzhandbuch AWS SDKs und im Tools-Referenzhandbuch. • Weitere Informationen finden Sie unter Verwaltung von Zugriffsschlüsseln für IAM-Benutzer im IAM-Benutzerhandbuch. AWS APIs

Richten AWS Lake Formation

In den folgenden Abschnitten finden Sie Informationen zur erstmaligen Einrichtung von Lake Formation. Nicht alle Themen in diesem Abschnitt sind erforderlich, um Lake Formation nutzen zu können. Sie können die Anweisungen verwenden, um das Lake Formation Formation-Berechtigungsmodell einzurichten, um Ihre vorhandenen AWS Glue Data Catalog Objekte und Datenspeicherorte in Amazon Simple Storage Service (Amazon S3) zu verwalten.

1. [Erstellen Sie einen Data Lake-Administrator](#)
2. [Ändern Sie das Standardberechtigungsmodell oder verwenden Sie den hybriden Zugriffsmodus](#)
3. [the section called “Konfigurieren Sie einen Amazon S3 S3-Standort für Ihren Data Lake”](#)
4. [the section called “Benutzern von Lake Formation Berechtigungen zuweisen”](#)
5. [the section called “Integration von IAM Identity Center”](#)
6. [the section called “\(Optional\) Einstellungen für die externe Datenfilterung”](#)
7. [the section called “\(Optional\) Gewähren Sie Zugriff auf den Datenkatalog-Verschlüsselungsschlüssel”](#)
8. [\(Optional\) Erstellen Sie eine IAM-Rolle für Workflows](#)

In diesem Abschnitt erfahren Sie, wie Sie Lake Formation Formation-Ressourcen auf zwei verschiedene Arten einrichten:

- Verwenden einer AWS CloudFormation Vorlage
- Verwenden der Lake Formation Formation-Konsole

Um Lake Formation mit der AWS Konsole einzurichten, gehen Sie zu [Erstellen Sie einen Data Lake-Administrator](#).

Lake Formation Formation-Ressourcen mithilfe einer CloudFormation Vorlage einrichten

Note

Der CloudFormation Stack führt die Schritte 1 bis 6 der oben genannten Schritte aus, mit Ausnahme der Schritte 2 und 5. Führen Sie [Ändern Sie das Standardberechtigungsmodell](#)

oder verwenden Sie den hybriden Zugriffsmodus es the section called “Integration von IAM Identity Center” manuell von der Lake Formation Formation-Konsole aus.

1. Melden Sie sich bei der AWS CloudFormation Konsole unter <https://console.aws.amazon.com/cloudformation> als IAM-Administrator in der Region USA Ost (Nord-Virginia) an.
2. Wählen Sie Launch Stack.
3. Wählen Sie auf dem Bildschirm „Stack erstellen“ die Option „Weiter“.
4. Geben Sie einen Stack-Namen ein.
5. Geben Sie für DatalakeAdminName und DatalakeAdminPassword Ihren Benutzernamen und Ihr Passwort für den Data Lake-Admin-Benutzer ein.
6. Geben Sie für DatalakeUser1Name und DatalakeUser1Password Ihren Benutzernamen und Ihr Passwort für den Data Lake Analyst-Benutzer ein.
7. Geben Sie für DataLakeBucketName Ihren neuen Bucket-Namen ein, der erstellt werden soll.
8. Wählen Sie Weiter aus.
9. Wählen Sie I acknowledge that CloudFormation might create IAM resources with custom names auf der nächsten Seite Weiter aus.
10. Überprüfen Sie die Details auf der letzten Seite und wählen Sie Ich bestätige, dass AWS CloudFormation möglicherweise IAM-Ressourcen erstellt werden.
11. Wählen Sie Erstellen aus.

Die Erstellung des Stacks kann bis zu zwei Minuten dauern.

Bereinigen von Ressourcen

Wenn Sie die CloudFormation Stack-Ressourcen bereinigen möchten:

1. Deregistrieren Sie den Amazon S3 S3-Bucket, den Ihr Stack erstellt und als Data Lake-Standort registriert hat.
2. Löschen Sie den CloudFormation Stack. Dadurch werden alle vom Stack erstellten Ressourcen gelöscht.

Erstellen Sie einen Data Lake-Administrator

Data Lake-Administratoren sind zunächst die einzigen AWS Identity and Access Management (IAM-) Benutzer oder Rollen, die Lake Formation Formation-Berechtigungen für Datenspeicherorte und Datenkatalogressourcen jedem Prinzipal (einschließlich sich selbst) gewähren können. Weitere Informationen zu den Funktionen von Data Lake-Administratoren finden Sie unter [Implizite Lake Formation Formation-Berechtigungen](#). Standardmäßig können Sie mit Lake Formation bis zu 30 Data Lake-Administratoren einrichten.

Sie können einen Data Lake-Administrator mithilfe der Lake Formation Formation-Konsole oder mithilfe der PutDataLakeSettings Lake Formation Formation-API erstellen.

Die folgenden Berechtigungen sind erforderlich, um einen Data Lake-Administrator zu erstellen. Der Administrator Benutzer verfügt implizit über diese Berechtigungen.

- `lakeformation:PutDataLakeSettings`
- `lakeformation:GetDataLakeSettings`

Wenn Sie einem Benutzer die AWSLakeFormationDataAdmin Richtlinie gewähren, kann dieser Benutzer keine weiteren Lake Formation-Administratorbenutzer erstellen.

Um einen Data Lake-Administrator (Konsole) zu erstellen

1. Wenn der Benutzer, der Data Lake-Administrator werden soll, noch nicht existiert, verwenden Sie die IAM-Konsole, um ihn zu erstellen. Wählen Sie andernfalls einen vorhandenen Benutzer aus, der der Data Lake-Administrator werden soll.

Note

Es wird empfohlen, keinen IAM-Administratorbenutzer (Benutzer mit der AdministratorAccess AWS verwalteten Richtlinie) als Data Lake-Administrator auszuwählen.

Ordnen Sie dem Benutzer die folgenden AWS verwalteten Richtlinien zu:

Richtlinien	Obligatorisch?	Hinweise
<code>AWSLakeFormationDataAdmin</code>	zwingend erforderlich	Grundlegende Data Lake-Administrator berechtigungen. Diese AWS verwaltet e Richtlinie enthält eine ausdrückliche Ablehnung des Lake Formation Formation-API-Vorgangs, wodurch Benutzer <code>PutDataLakeSetting</code> daran gehindert werden, neue Data Lake-Administratoren zu erstellen.
<code>AWSGlueConsoleFullAccess</code> , <code>CloudWatchLogsReadOnlyAccess</code>	Optional	Fügen Sie diese Richtlinien hinzu, wenn der Data Lake-Administrator Probleme mit Workflows beheben soll, die anhand von Lake Formation -Blueprints erstellt wurden. Diese Richtlinien ermöglichen es dem Data Lake-Administrator, Informationen zur Fehlerbehebung in der AWS Glue Konsole und der Amazon CloudWatch Logs Konsole einzusehen. Informationen zu Workflows finden Sie unter the section called “Daten mithilfe von Workflows importieren” .
<code>AWSLakeFormationCrossAccountManager</code>	Optional	Fügen Sie diese Richtlinie hinzu, damit der Data Lake-Administrator kontoübergreifende Berechtigungen für Datenkatalogressourcen gewähren und widerrufen kann. Weitere Informationen finden Sie unter Kontoübergreifender Datenaustausch in Lake Formation .

Richtlinien	Obligatorisch?	Hinweise
AmazonAthenaFullAccess	Optional	Fügen Sie diese Richtlinie an, wenn der Data Lake-Administrator Abfragen in Amazon Athena ausführen wird.

2. Fügen Sie die folgende Inline-Richtlinie an, die dem Data Lake-Administrator die Berechtigung erteilt, die mit dem Service verknüpfte Lake Formation Formation-Rolle zu erstellen. Ein empfohlener Name für die Richtlinie lautet `LakeFormationSLR`.

Die serviceverknüpfte Rolle ermöglicht es dem Data Lake-Administrator, Amazon S3 S3-Standorte einfacher bei Lake Formation zu registrieren. Weitere Informationen zur dienstbezogenen Rolle Lake Formation finden Sie unter [the section called “Verwenden von servicegebundenen Rollen”](#).

Important

Ersetzen Sie den Text in allen folgenden Richtlinien `<account-id>` durch eine gültige AWS Kontonummer.

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Action": "iam:CreateServiceLinkedRole",
      "Resource": "*",
      "Condition": {
        "StringEquals": {
          "iam:AWSServiceName": "lakeformation.amazonaws.com"
        }
      }
    },
    {
      "Effect": "Allow",
      "Action": [
        "iam:PutRolePolicy"
      ],
```

```

        "Resource": "arn:aws:iam::<account-id>:role/aws-service-role/
lakeformation.amazonaws.com/AWSServiceRoleForLakeFormationDataAccess"
    }
]
}

```

3. (Optional) Fügen Sie dem Benutzer die folgende PassRole Inline-Richtlinie hinzu. Diese Richtlinie ermöglicht es dem Data Lake-Administrator, Workflows zu erstellen und auszuführen. Die `iam:PassRole` Berechtigung ermöglicht es dem Workflow, die Rolle `LakeFormationWorkflowRole` zum Erstellen von Crawlern und Jobs zu übernehmen und die Rolle den erstellten Crawlern und Jobs zuzuweisen. Ein empfohlener Name für die Richtlinie lautet `UserPassRole`.

Important

`<account-id>` Durch eine gültige AWS Kontonummer ersetzen.

JSON

```

{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Sid": "PassRolePermissions",
      "Effect": "Allow",
      "Action": [
        "iam:PassRole"
      ],
      "Resource": [
        "arn:aws:iam::111122223333:role/LakeFormationWorkflowRole"
      ]
    }
  ]
}

```

4. (Optional) Fügen Sie diese zusätzliche Inline-Richtlinie bei, wenn Ihr Konto kontoübergreifende Lake Formation Formations-Berechtigungen gewährt oder erhält. Diese Richtlinie ermöglicht es dem Data Lake-Administrator, Einladungen zur gemeinsamen Nutzung von Ressourcen anzuzeigen und anzunehmen AWS Resource Access Manager (AWS RAM). Außerdem

beinhaltet die Richtlinie für Data Lake-Administratoren im AWS Organizations Verwaltungskonto die Erlaubnis, Organisationen kontenübergreifende Zuschüsse zu gewähren. Weitere Informationen finden Sie unter [Kontoübergreifender Datenaustausch in Lake Formation](#).

Ein empfohlener Name für die Richtlinie lautet `RAMAccess`.

JSON

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Action": [
        "ram:AcceptResourceShareInvitation",
        "ram:RejectResourceShareInvitation",
        "ec2:DescribeAvailabilityZones",
        "ram:EnableSharingWithAwsOrganization"
      ],
      "Resource": "*"
    }
  ]
}
```

5. Öffnen Sie die AWS Lake Formation Konsole unter <https://console.aws.amazon.com/lakeformation/> und melden Sie sich als Administratorbenutzer an, den Sie in der benutzerverwalteten Richtlinie erstellt haben, [Erstellen eines Benutzers mit Administratorzugriff](#) oder als AdministratorAccess Benutzer mit AWS benutzerverwalteter Richtlinie.
6. Wenn das Fenster Welcome to Lake Formation angezeigt wird, wählen Sie den IAM-Benutzer aus, den Sie in Schritt 1 erstellt oder ausgewählt haben, und klicken Sie dann auf Get started.
7. Wenn das Fenster Willkommen bei Lake Formation nicht angezeigt wird, führen Sie die folgenden Schritte aus, um einen Lake Formation-Administrator zu konfigurieren.
 - a. Wählen Sie im Navigationsbereich unter Administration die Option Administrative Rollen und Aufgaben aus. Wählen Sie auf der Konsolenseite im Abschnitt Data Lake-Administratoren die Option Hinzufügen aus.
 - b. Wählen Sie im Dialogfeld Administratoren hinzufügen unter Zugriffstyp die Option Data Lake-Administrator aus.

- c. Wählen Sie für IAM-Benutzer und -Rollen den IAM-Benutzer aus, den Sie in Schritt 1 erstellt oder ausgewählt haben, und klicken Sie dann auf Speichern.

Ändern Sie das Standardberechtigungsmodell oder verwenden Sie den hybriden Zugriffsmodus

Lake Formation beginnt damit, dass die Einstellungen „Nur IAM-Zugriffskontrolle verwenden“ aktiviert sind, um die Kompatibilität mit dem vorhandenen AWS Glue Data Catalog Verhalten zu gewährleisten. Mit diesen Einstellungen können Sie den Zugriff auf Ihre Daten im Data Lake und dessen Metadaten über IAM-Richtlinien und Amazon S3 S3-Bucket-Richtlinien verwalten.

Um den Übergang von Data Lake-Berechtigungen von einem IAM- und Amazon S3 S3-Modell zu Lake Formation Formation-Berechtigungen zu vereinfachen, empfehlen wir Ihnen, den hybriden Zugriffsmodus für Data Catalog zu verwenden. Mit dem Hybridzugriffsmodus haben Sie einen inkrementellen Pfad, über den Sie Lake Formation Formation-Berechtigungen für eine bestimmte Gruppe von Benutzern aktivieren können, ohne andere bestehende Benutzer oder Workloads zu unterbrechen.

Weitere Informationen finden Sie unter [Hybrider Zugriffsmodus](#).

Deaktivieren Sie die Standardeinstellungen, um alle vorhandenen Benutzer einer Tabelle in einem einzigen Schritt nach Lake Formation zu verschieben.

Important

Wenn Sie bereits AWS Glue Data Catalog Datenbanken und Tabellen haben, folgen Sie nicht den Anweisungen in diesem Abschnitt. Folgen Sie stattdessen den Anweisungen in [the section called “Aktualisierung der AWS Glue Datenberechtigungen auf das Lake Formation Formation-Modell”](#).

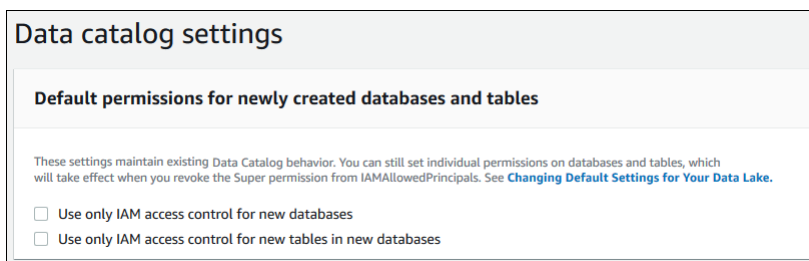
Warning

Wenn Sie über eine Automatisierung verfügen, die Datenbanken und Tabellen im Datenkatalog erstellt, können die folgenden Schritte dazu führen, dass die Automatisierungs- und Downstream-Jobs zum Extrahieren, Transformieren und Laden (ETL) fehlschlagen. Fahren Sie erst fort, nachdem Sie entweder Ihre vorhandenen Prozesse geändert oder den erforderlichen Prinzipalen explizite Lake Formation Formation-Berechtigungen erteilt haben.

Informationen zu den Berechtigungen für Lake Formation finden Sie unter [the section called “Referenz zu den Genehmigungen von Lake Formation”](#).

So ändern Sie die Standardeinstellungen für den Datenkatalog

1. Fahren Sie in der Lake Formation Formation-Konsole unter fort <https://console.aws.amazon.com/lakeformation/>. Stellen Sie sicher, dass Sie als der Administratorbenutzer, den Sie in der verwalteten Richtlinie erstellt haben, [Erstellen eines Benutzers mit Administratorzugriff](#) oder als Benutzer mit der AdministratorAccess AWS verwalteten Richtlinie angemeldet sind.
2. Ändern Sie die Datenkatalogeinstellungen:
 - a. Wählen Sie im Navigationsbereich unter Verwaltung die Option Datenkatalogeinstellungen aus.
 - b. Deaktivieren Sie beide Kontrollkästchen und wählen Sie Speichern.



3. Widerrufen Sie IAMAllowedPrincipals die Erlaubnis für Datenbankersteller.
 - a. Wählen Sie im Navigationsbereich unter Administration die Option Administrative Rollen und Aufgaben aus.
 - b. Wählen Sie auf der Konsole für Administratorrollen und -aufgaben im Abschnitt Datenbankersteller die IAMAllowedPrincipals Gruppe aus und klicken Sie auf Widerrufen.

Das Dialogfeld „Berechtigungen widerrufen“ wird angezeigt, in dem angegeben wird, dass die IAMAllowedPrincipals Person über die Berechtigung „Datenbank erstellen“ verfügt.

- c. Wählen Sie „Widerrufen“.

Benutzern von Lake Formation Berechtigungen zuweisen

Erstellen Sie einen Benutzer, der Zugriff auf den Data Lake in haben soll AWS Lake Formation. Dieser Benutzer verfügt über die geringsten Rechte, um den Data Lake abzufragen.

Weitere Informationen zum Erstellen von Benutzern oder Gruppen finden Sie unter [IAM-Identitäten im IAM-Benutzerhandbuch](#).

So weisen Sie einem Benutzer ohne Administratorrechte Berechtigungen für den Zugriff auf Lake Formation Daten zu

1. Öffnen Sie die IAM-Konsole unter <https://console.aws.amazon.com/iam> und melden Sie sich als Administratorbenutzer an, den Sie in der verwalteten Richtlinie erstellt haben, [Erstellen eines Benutzers mit Administratorzugriff](#) oder als Benutzer mit der AdministratorAccess AWS verwalteten Richtlinie.
2. Wählen Sie Benutzer oder Benutzergruppen aus.
3. Wählen Sie in der Liste den Namen des Benutzers oder der Gruppe, in die eine Richtlinie eingebettet werden soll.

Wählen Sie Berechtigungen.

4. Wählen Sie „Berechtigungen hinzufügen“ und anschließend „Richtlinien direkt anhängen“. Geben Sie Athena in das Textfeld Richtlinien filtern ein. Markieren Sie in der Ergebnisliste das Kästchen für AmazonAthenaFullAccess.
5. Wählen Sie die Schaltfläche Richtlinie erstellen. Wählen Sie auf der Seite Richtlinie erstellen die Registerkarte JSON aus. Kopieren Sie den folgenden Code und fügen Sie ihn in den Richtlinien-Editor ein.

JSON

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Action": [
        "lakeformation:GetDataAccess",
        "glue:GetTable",
        "glue:GetTables",
        "glue:SearchTables",
        "glue:GetDatabase",
        "glue:GetDatabases",
        "glue:GetPartitions",
        "lakeformation:GetResourceLFTags",
        "lakeformation:ListLFTags",
```

```

        "lakeformation:GetLFTag",
        "lakeformation:SearchTablesByLFTags",
        "lakeformation:SearchDatabasesByLFTags"
    ],
    "Resource": "*"
}
]
}

```

6. Klicken Sie unten auf die Schaltfläche Weiter, bis Sie die Seite „Richtlinie überprüfen“ sehen. Geben Sie einen Namen für die Richtlinie ein, DataLakeUserBasic z. B. Wählen Sie Richtlinie erstellen und schließen Sie dann die Registerkarte Richtlinien oder das Browserfenster.

Konfigurieren Sie einen Amazon S3 S3-Standort für Ihren Data Lake

Um Lake Formation zur Verwaltung und Sicherung der Daten in Ihrem Data Lake zu verwenden, müssen Sie zunächst einen Amazon S3 S3-Standort registrieren. Wenn Sie einen Standort registrieren, werden dieser Amazon S3 S3-Pfad und alle Ordner unter diesem Pfad registriert, sodass Lake Formation Berechtigungen auf Speicherebene erzwingen kann. Wenn der Benutzer Daten von einer integrierten Engine wie Amazon Athena anfordert, bietet Lake Formation Datenzugriff, anstatt die Benutzerberechtigungen zu verwenden.

Wenn Sie einen Standort registrieren, geben Sie eine IAM-Rolle an, die read/write Berechtigungen für diesen Standort gewährt. Lake Formation übernimmt diese Rolle bei der Bereitstellung temporärer Anmeldeinformationen für integrierte AWS Dienste, die Zugriff auf Daten am registrierten Amazon S3 S3-Standort anfordern. Sie können entweder die serviceverknüpfte Rolle (SLR) von Lake Formation angeben oder Ihre eigene Rolle erstellen.

Verwenden Sie eine benutzerdefinierte Rolle in den folgenden Situationen:

- Sie planen, Metriken in Amazon CloudWatch Logs zu veröffentlichen. Die benutzerdefinierte Rolle muss zusätzlich zu den SLR-Berechtigungen eine Richtlinie für das Hinzufügen von CloudWatch Protokollen in Logs und das Veröffentlichen von Metriken enthalten. Ein Beispiel für eine Inline-Richtlinie, die die erforderlichen CloudWatch Berechtigungen gewährt, finden Sie unter [Anforderungen für Rollen, die zur Registrierung von Standorten verwendet werden](#)
- Der Amazon S3 S3-Standort ist in einem anderen Konto vorhanden. Details hierzu finden Sie unter [the section called “Registrierung eines Amazon S3 S3-Standorts in einem anderen AWS Konto”](#).
- Der Amazon S3 S3-Standort enthält Daten, die mit einem verschlüsselt sind Von AWS verwalteter Schlüssel. Details dazu finden Sie unter [Registrierung eines verschlüsselten Amazon S3 S3-](#)

Standorts und AWS Kontoübergreifende Registrierung eines verschlüsselten Amazon S3 S3-Standorts.

- Sie planen, mit Amazon EMR auf den Amazon S3-Standort zuzugreifen. Weitere Informationen zu den Rollenanforderungen finden Sie unter [IAM-Rollen für Lake Formation](#) im Amazon EMR Management Guide.

Die Rolle, die Sie wählen, muss über die erforderlichen Berechtigungen verfügen, wie unter beschrieben. [Anforderungen für Rollen, die zur Registrierung von Standorten verwendet werden](#) Anweisungen zur Registrierung eines Amazon S3 S3-Standorts finden Sie unter [Hinzufügen eines Amazon S3 S3-Standorts zu Ihrem Data Lake](#).

(Optional) Einstellungen für die externe Datenfilterung

Wenn Sie beabsichtigen, Daten in Ihrem Data Lake mithilfe von Abfrage-Engines von Drittanbietern zu analysieren und zu verarbeiten, müssen Sie sich dafür entscheiden, externen Engines den Zugriff auf von Lake Formation verwaltete Daten zu ermöglichen. Wenn Sie sich nicht anmelden, können externe Engines nicht auf Daten an Amazon S3 S3-Standorten zugreifen, die bei Lake Formation registriert sind.

Lake Formation unterstützt Berechtigungen auf Spaltenebene, um den Zugriff auf bestimmte Spalten in einer Tabelle einzuschränken. Integrierte Analysedienste wie Amazon Athena Amazon Redshift Spectrum und Amazon EMR rufen ungefilterte Tabellenmetadaten aus dem ab. AWS Glue Data Catalog Das eigentliche Filtern von Spalten in Abfrageantworten liegt in der Verantwortung des integrierten Dienstes. Es liegt in der Verantwortung der Drittanbieteradministratoren, mit Berechtigungen ordnungsgemäß umzugehen, um unbefugten Zugriff auf Daten zu verhindern.

So stimmen Sie zu, dass Drittanbieter-Engines auf Daten zugreifen und diese filtern können (Konsole)

1. Fahren Sie in der Lake Formation Formation-Konsole unter fort <https://console.aws.amazon.com/lakeformation/>. Stellen Sie sicher, dass Sie als Principal angemeldet sind, der über die IAM-Berechtigung für den Lake Formation PutDataLakeSettings API-Vorgang verfügt. Der IAM-Administratorbenutzer, den Sie erstellt haben, [Melde dich an für ein AWS-Konto](#) verfügt über diese Berechtigung.
2. Wählen Sie im Navigationsbereich unter Administration die Option Anwendungsintegrationseinstellungen aus.
3. Gehen Sie auf der Seite mit den Einstellungen für die Anwendungsintegration wie folgt vor:

- a. Markieren Sie das Kästchen Erlauben Sie externen Engines, Daten an Amazon S3 S3-Standorten zu filtern, die bei Lake Formation registriert sind.
- b. Geben Sie Sitzungs-Tag-Werte ein, die für Engines von Drittanbietern definiert sind.
- c. Geben Sie als AWS Konto das Konto ein IDs, IDs von dem aus Engines von Drittanbietern auf Standorte zugreifen können, die bei Lake Formation registriert sind. Drücken Sie nach jeder Konto-ID die Eingabetaste.
- d. Wählen Sie Speichern.

Informationen dazu, wie externe Engines ohne Überprüfung des Sitzungs-Tags auf Daten zugreifen können, finden Sie unter [Anwendungsintegration für vollständigen Tabellenzugriff](#)

(Optional) Gewähren Sie Zugriff auf den Datenkatalog-Verschlüsselungsschlüssel

Wenn der verschlüsselt AWS Glue Data Catalog ist, gewähren Sie allen Prinzipalen, die Lake Formation-Berechtigungen für Data Catalog-Datenbanken und -Tabellen gewähren müssen, AWS Identity and Access Management (IAM) -Berechtigungen für den AWS KMS Schlüssel.

Weitere Informationen finden Sie im AWS Key Management Service -Entwicklerhandbuch.

(Optional) Erstellen Sie eine IAM-Rolle für Workflows

Mit AWS Lake Formation können Sie Ihre Daten mithilfe von Workflows importieren, die von AWS Glue Crawlern ausgeführt werden. Ein Workflow definiert die Datenquelle und den Zeitplan für den Import von Daten in Ihren Data Lake. Mithilfe der von Lake Formation bereitgestellten Blueprints oder Vorlagen können Sie ganz einfach Workflows definieren.

Wenn Sie einen Workflow erstellen, müssen Sie ihm eine AWS Identity and Access Management (IAM-) Rolle zuweisen, die Lake Formation die erforderlichen Berechtigungen zum Ingestieren der Daten gewährt.

Das folgende Verfahren setzt Vertrautheit mit IAM voraus.

Um eine IAM-Rolle für Workflows zu erstellen

1. Öffnen Sie die IAM-Konsole unter <https://console.aws.amazon.com/iam> und melden Sie sich als der Administratorbenutzer an, den Sie in der verwalteten Richtlinie erstellt haben, [Erstellen eines](#)

[Benutzers mit Administratorzugriff](#) oder als Benutzer mit der AdministratorAccess AWS verwalteten Richtlinie.

2. Wählen Sie im Navigationsbereich Rollen und anschließend Rolle erstellen aus.
3. Wählen Sie auf der Seite Rolle erstellen die Option AWS Service und dann Glue aus. Wählen Sie Weiter aus.
4. Suchen Sie auf der Seite „Berechtigungen hinzufügen“ nach der AWSGlueServiceRoleverwalteten Richtlinie und aktivieren Sie das Kontrollkästchen neben dem Richtlinienamen in der Liste. Schließen Sie dann den Assistenten zum Erstellen von Rollen ab und geben Sie der Rolle einen Namen `LFWorkflowRole`. Um den Vorgang abzuschließen, wählen Sie Create role (Rolle erstellen).
5. Gehen Sie zurück zur Rollenseite `LFWorkflowRole`, suchen Sie nach dem Rollennamen und wählen Sie ihn aus.
6. Wählen Sie auf der Seite mit der Rollenzusammenfassung unter dem Tab Berechtigungen die Option Inline-Richtlinie erstellen aus. Navigieren Sie auf dem Bildschirm „Richtlinie erstellen“ zur Registerkarte JSON und fügen Sie die folgende Inline-Richtlinie hinzu. Ein empfohlener Name für die Richtlinie lautet `LakeFormationWorkflow`.

 Important

Ersetzen Sie den Text in der folgenden Richtlinie `<account-id>` durch eine gültige AWS-Konto Zahl.

JSON

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Action": [
        "lakeformation:GetDataAccess",
        "lakeformation:GrantPermissions"
      ],
      "Resource": "*"
    }
  ]
}
```

```
        "Effect": "Allow",
        "Action": ["iam:PassRole"],
        "Resource": [
            "arn:aws:iam::111122223333:role/LakeFormationWorkflowRole"
        ]
    }
}
```

Im Folgenden finden Sie eine kurze Beschreibung der Berechtigungen in dieser Richtlinie:

- `lakeformation:GetDataAccess` ermöglicht es Aufträgen, die durch den Workflow erstellt wurden, an den Zielspeicherort zu schreiben.
 - `lakeformation:GrantPermission` ermöglicht es dem Workflow, die `SELECT` Berechtigung für Zieltabellen zu erteilen.
 - `iam:PassRole` ermöglicht es dem Service, die Rolle beim `LakeFormationWorkflowRole` Erstellen von Crawlern und Jobs (Instanzen von Workflows) zu übernehmen und die Rolle den erstellten Crawlern und Jobs zuzuweisen.
7. Stellen Sie sicher, dass der Rolle `LakeFormationWorkflowRole` zwei Richtlinien zugeordnet sind.
 8. Wenn Sie Daten aufnehmen, die sich außerhalb des Data Lake-Speicherorts befinden, fügen Sie eine Inline-Richtlinie hinzu, die Berechtigungen zum Lesen der Quelldaten gewährt.

AWS GlueDatenberechtigungen für das AWS Lake Formation Modell aktualisieren

AWS Lake Formation Berechtigungen ermöglichen eine detaillierte Zugriffskontrolle für Daten in Ihrem Data Lake. Sie können das Lake Formation Formation-Berechtigungsmodell verwenden, um Ihre vorhandenen AWS Glue Data Catalog Objekte und Datenspeicherorte in Amazon Simple Storage Service (Amazon S3) zu verwalten.

Das Lake Formation Formation-Berechtigungsmodell verwendet grobkörnige AWS Identity and Access Management (IAM) Berechtigungen für den Zugriff auf API-Dienste. Lake Formation verwendet [Datenfilterung und Sicherheit auf Zellebene in Lake Formation](#) Funktionen, um den Tabellenzugriff auf Spalten-, Zeilen- und Zellenebene für Benutzer und ihre Anwendungen

einzuschränken. Im Vergleich dazu gewährt das AWS Glue Modell den Datenzugriff über [identitätsbasierte und ressourcenbasierte IAM-Richtlinien](#).

Folgen Sie den Schritten in dieser Anleitung, um den Wechsel vorzunehmen.

Weitere Informationen finden Sie unter [Überblick über die Genehmigungen für Lake Formation](#).

Über Standardberechtigungen

Um die Abwärtskompatibilität mit AWS Glue zu gewährleisten, AWS Lake Formation wird der IAMAllowedPrincipals Gruppe standardmäßig die Super Berechtigung für alle vorhandenen AWS Glue Datenkatalogressourcen und die Super Berechtigung für neue Datenkatalogressourcen erteilt, wenn die Einstellungen Nur IAM-Zugriffssteuerung verwenden aktiviert sind. Dadurch wird der Zugriff auf Datenkatalogressourcen und Amazon S3 S3-Standorte ausschließlich durch AWS Identity and Access Management (IAM-) Richtlinien gesteuert. Die IAMAllowedPrincipals Gruppe umfasst alle IAM-Benutzer und -Rollen, denen aufgrund Ihrer IAM-Richtlinien Zugriff auf Ihre Datenkatalogobjekte gewährt wird. Die Super Berechtigung ermöglicht es einem Prinzipal, jeden unterstützten Lake Formation Formation-Vorgang in der Datenbank oder Tabelle auszuführen, für die sie erteilt wurde.

Sie können beginnen, Lake Formation zur Verwaltung des Zugriffs auf Ihre Daten zu verwenden, indem Sie die Standorte vorhandener Datenkatalogressourcen in Lake Formation registrieren oder den Hybridzugriffsmodus verwenden. Wenn Sie den Amazon S3 S3-Standort im Hybridzugriffsmodus registrieren, können Sie Lake Formation Formation-Berechtigungen aktivieren, indem Sie Prinzipale für Datenbanken und Tabellen unter diesem Standort auswählen.

Um den Übergang von Data Lake-Berechtigungen von einem IAM- und Amazon S3 S3-Modell zu Lake Formation Formation-Berechtigungen zu vereinfachen, empfehlen wir Ihnen, den hybriden Zugriffsmodus für Data Catalog zu verwenden. Mit dem Hybridzugriffsmodus haben Sie einen inkrementellen Pfad, über den Sie Lake Formation Formation-Berechtigungen für eine bestimmte Gruppe von Benutzern aktivieren können, ohne andere bestehende Benutzer oder Workloads zu unterbrechen.

Weitere Informationen finden Sie unter [Hybrider Zugriffsmodus](#).

Deaktivieren Sie die Standardeinstellungen für den Datenkatalog, um alle vorhandenen Benutzer einer Tabelle in einem einzigen Schritt nach Lake Formation zu verschieben.

Um mit der Verwendung von Lake Formation Formation-Berechtigungen mit Ihren vorhandenen AWS Glue Data Catalog-Datenbanken und -Tabellen zu beginnen, müssen Sie wie folgt vorgehen:

1. Ermitteln Sie die vorhandenen IAM-Berechtigungen Ihrer Benutzer für jede Datenbank und Tabelle.
2. Replizieren Sie diese Berechtigungen in Lake Formation.
3. Für jeden Amazon S3 S3-Standort, der Daten enthält:
 - a. Widerrufen Sie der IAMAllowedPrincipals Gruppe die Super Erlaubnis für jede Datenkatalogressource, die auf diesen Speicherort verweist.
 - b. Registrieren Sie den Standort bei Lake Formation.
4. Bereinigen Sie bestehende, fein abgestufte IAM-Richtlinien für die Zugriffskontrolle.

Important

Um während der Umstellung Ihres Datenkatalogs neue Benutzer hinzuzufügen, müssen Sie wie bisher detaillierte AWS Glue Berechtigungen in IAM einrichten. Sie müssen diese Berechtigungen auch in Lake Formation replizieren, wie in diesem Abschnitt beschrieben. Wenn neue Benutzer über die in diesem Handbuch beschriebenen groben IAM-Richtlinien verfügen, können sie alle Datenbanken oder Tabellen auflisten, denen die entsprechenden Berechtigungen erteilt wurden. Super IAMAllowedPrincipals Sie können auch die Metadaten für diese Ressourcen einsehen.

Folgen Sie den Schritten in diesem Abschnitt, um auf das Lake Formation Formation-Berechtigungsmodell umzusteigen.

Themen

- [Schritt 1: Listet die vorhandenen Berechtigungen der Benutzer und Rollen auf](#)
- [Schritt 2: Richten Sie entsprechende Lake Formation Formation-Berechtigungen ein](#)
- [Schritt 3: Erteilen Sie Benutzern IAM-Berechtigungen zur Verwendung von Lake Formation](#)
- [Schritt 4: Stellen Sie Ihre Datenspeicher auf das Lake Formation Formation-Berechtigungsmodell um](#)
- [Schritt 5: Sichern Sie sich neue Datenkatalog-Ressourcen](#)
- [Schritt 6: Geben Sie Benutzern eine neue IAM-Richtlinie für den future Zugriff auf Data Lake](#)
- [Schritt 7: Bereinigen vorhandener IAM-Richtlinien](#)

Schritt 1: Listet die vorhandenen Berechtigungen der Benutzer und Rollen auf

Um mit der Verwendung von AWS Lake Formation Berechtigungen für Ihre vorhandenen AWS Glue Datenbanken und Tabellen zu beginnen, müssen Sie zunächst die vorhandenen Berechtigungen Ihrer Benutzer ermitteln.

Important

Bevor Sie beginnen, stellen Sie sicher, dass Sie die Aufgaben unter abgeschlossen haben [Erste Schritte](#).

Themen

- [Verwenden des API-Vorgangs](#)
- [Mit dem AWS-Managementkonsole](#)
- [Verwenden AWS CloudTrail](#)

Verwenden des API-Vorgangs

Verwenden Sie den [ListPoliciesGrantingServiceAccess](#) API-Vorgang AWS Identity and Access Management (IAM), um die IAM-Richtlinien zu ermitteln, die jedem Prinzipal (Benutzer oder Rolle) zugewiesen sind. Anhand der in den Ergebnissen zurückgegebenen Richtlinien können Sie die IAM-Berechtigungen ermitteln, die dem Prinzipal gewährt werden. Sie müssen die API für jeden Prinzipal separat aufrufen.

Example

Im folgenden AWS CLI Beispiel werden die dem Benutzer `glue_user1` zugewiesenen Richtlinien zurückgegeben.

```
aws iam list-policies-granting-service-access --arn arn:aws:iam::111122223333:user/glue_user1 --service-namespaces glue
```

Der Befehl gibt Ergebnisse zurück, die den folgenden ähneln.

```
{
  "PoliciesGrantingServiceAccess": [
```

```
{
  "ServiceNamespace": "glue",
  "Policies": [
    {
      "PolicyType": "INLINE",
      "PolicyName": "GlueUserBasic",
      "EntityName": "glue_user1",
      "EntityType": "USER"
    },
    {
      "PolicyType": "MANAGED",
      "PolicyArn": "arn:aws:iam::aws:policy/AmazonAthenaFullAccess",
      "PolicyName": "AmazonAthenaFullAccess"
    }
  ]
},
{
  "IsTruncated": false
}
```

Mit dem AWS-Managementkonsole

Sie können diese Informationen auch auf der AWS Identity and Access Management (IAM-) Konsole auf der Registerkarte Access Advisor auf der Seite mit der Benutzer- oder Rollenübersicht einsehen:

1. Öffnen Sie unter <https://console.aws.amazon.com/iam/> die IAM-Konsole.
2. Klicken Sie im Navigationsbereich auf Users (Benutzer) oder Roles (Rollen).
3. Wählen Sie einen Namen in der Liste aus, um die zugehörige Übersichtsseite zu öffnen, und wählen Sie die Registerkarte Access Advisor.
4. Untersuchen Sie die einzelnen Richtlinien, um die Kombination von Datenbanken, Tabellen und Aktionen zu ermitteln, für die jeder Benutzer über Berechtigungen verfügt.

Denken Sie daran, während dieses Vorgangs zusätzlich zu den Benutzern auch Rollen zu überprüfen, da Ihre Datenverarbeitungsaufträge möglicherweise Rollen für den Datenzugriff übernehmen.

Verwenden AWS CloudTrail

Eine andere Möglichkeit, Ihre vorhandenen Berechtigungen zu ermitteln, besteht darin, nach AWS Glue API-Aufrufen zu suchen, bei denen das `additionalEventData` Feld der Protokolle einen

`insufficientLakeFormationPermissions` Eintrag enthält. AWS CloudTrail Dieser Eintrag listet die Datenbank und Tabelle auf, für die der Benutzer Lake Formation Formation-Berechtigungen benötigt, um dieselbe Aktion auszuführen.

Da es sich um Datenzugriffsprotokolle handelt, kann nicht garantiert werden, dass sie eine umfassende Liste der Benutzer und ihrer Berechtigungen erstellen. Wir empfehlen, einen großen Zeitraum zu wählen, um die meisten Datenzugriffsmuster Ihrer Benutzer zu erfassen, z. B. mehrere Wochen oder Monate.

Weitere Informationen finden Sie im AWS CloudTrail Benutzerhandbuch unter [Ereignisse mit CloudTrail Ereignisverlauf anzeigen](#).

Als Nächstes können Sie Lake Formation Formation-Berechtigungen so einrichten, dass sie den AWS Glue Berechtigungen entsprechen. Siehe [Schritt 2: Richten Sie entsprechende Lake Formation Formation-Berechtigungen ein](#).

Schritt 2: Richten Sie entsprechende Lake Formation Formation-Berechtigungen ein

Erteilen Sie anhand der in gesammelten Informationen AWS Lake Formation Berechtigungen [Schritt 1: Listet die vorhandenen Berechtigungen der Benutzer und Rollen auf](#), die den AWS Glue Berechtigungen entsprechen. Verwenden Sie eine der folgenden Methoden, um die Erteilung der Genehmigungen vorzunehmen:

- Verwenden Sie die Lake Formation Formation-Konsole oder die AWS CLI.

Siehe [the section called “Erteilen von Datenberechtigungen”](#).

- Verwenden Sie die `GrantPermissions` oder `BatchGrantPermissions` API-Operationen.

Siehe [Genehmigungen APIs](#).

Weitere Informationen finden Sie unter [Überblick über die Genehmigungen für Lake Formation](#).

Nachdem Sie die Lake Formation Formation-Berechtigungen eingerichtet haben, fahren Sie mit fort [Schritt 3: Erteilen Sie Benutzern IAM-Berechtigungen zur Verwendung von Lake Formation](#).

Schritt 3: Erteilen Sie Benutzern IAM-Berechtigungen zur Verwendung von Lake Formation

Um das AWS Lake Formation Berechtigungsmodell verwenden zu können, müssen Principals über AWS Identity and Access Management (IAM-) Berechtigungen für die Lake Formation verfügen. APIs

Erstellen Sie die folgende Richtlinie in IAM und fügen Sie sie jedem Benutzer hinzu, der Zugriff auf Ihren Data Lake benötigt. Speichern Sie die Richtlinie unter dem Namen `LakeFormationDataAccess`.

JSON

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Sid": "LakeFormationDataAccess",
      "Effect": "Allow",
      "Action": [
        "lakeformation:GetDataAccess"
      ],
      "Resource": "*"
    }
  ]
}
```

Als Nächstes führen Sie ein Upgrade auf Lake Formation Formation-Berechtigungen für jeweils einen Datenstandort durch. Siehe [Schritt 4: Stellen Sie Ihre Datenspeicher auf das Lake Formation Formation-Berechtigungsmodell um](#).

Schritt 4: Stellen Sie Ihre Datenspeicher auf das Lake Formation Formation-Berechtigungsmodell um

Ein Upgrade auf Lake Formation ermöglicht jeweils einen Datenstandort. Wiederholen Sie dazu den gesamten Abschnitt, bis Sie alle Amazon Simple Storage Service (Amazon S3) -Pfade registriert haben, auf die in Ihrem Datenkatalog verwiesen wird.

Themen

- [Überprüfen Sie die Berechtigungen von Lake Formation](#)
- [Sichern Sie vorhandene Datenkatalog-Ressourcen](#)
- [Aktivieren Sie die Lake Formation Formation-Berechtigungen für Ihren Amazon S3 S3-Standort](#)

Überprüfen Sie die Berechtigungen von Lake Formation

Führen Sie vor der Registrierung eines Standorts einen Bestätigungsschritt durch, um sicherzustellen, dass die richtigen Principals über die erforderlichen Lake Formation Formation-Berechtigungen verfügen und dass Principals, die diese nicht haben sollten, keine Lake Formation Formation-Berechtigungen erteilt werden. Identifizieren Sie mithilfe des Lake Formation GetEffectivePermissionsForPath Formation-API-Vorgangs die Data Catalog-Ressourcen, die auf den Amazon S3 S3-Standort verweisen, zusammen mit den Principals, die über Berechtigungen für diese Ressourcen verfügen.

Das folgende AWS CLI Beispiel gibt die Data Catalog-Datenbanken und -Tabellen zurück, die auf den Amazon S3 S3-Bucket verweisenproducts.

```
aws lakeformation get-effective-permissions-for-path --resource-arn
arn:aws:s3:::products --profile datalake_admin
```

Beachten Sie die profile Option. Es wird empfohlen, den Befehl als Data Lake-Administrator auszuführen.

Im Folgenden finden Sie einen Auszug aus den zurückgegebenen Ergebnissen.

```
{
  "PermissionsWithGrantOption": [
    "SELECT"
  ],
  "Resource": {
    "TableWithColumns": {
      "Name": "inventory_product",
      "ColumnWildcard": {},
      "DatabaseName": "inventory"
    }
  },
  "Permissions": [
    "SELECT"
  ],
}
```

```
"Principal": {
  "DataLakePrincipalIdentifier": "arn:aws:iam::111122223333:user/
datalake_user1",
  "DataLakePrincipalType": "IAM_USER"
},...
```

Important

Wenn Ihr AWS Glue Datenkatalog verschlüsselt ist, werden nur Datenbanken und Tabellen `GetEffectivePermissionsForPath` zurückgegeben, die nach der allgemeinen Verfügbarkeit von Lake Formation erstellt oder geändert wurden.

Sichern Sie vorhandene Datenkatalog-Ressourcen

Widerrufen Sie als Nächstes die Super Berechtigung für jede Tabelle und Datenbank, die Sie für den Standort identifiziert haben. `IAMAllowedPrincipals`

Warning

Wenn Sie über eine Automatisierung verfügen, die Datenbanken und Tabellen im Datenkatalog erstellt, können die folgenden Schritte dazu führen, dass die Automatisierungs- und Downstream-Jobs zum Extrahieren, Transformieren und Laden (ETL) fehlschlagen. Fahren Sie erst fort, nachdem Sie entweder Ihre vorhandenen Prozesse geändert oder den erforderlichen Prinzipalen explizite Lake Formation Formation-Berechtigungen erteilt haben. Informationen zu den Berechtigungen für Lake Formation finden Sie unter [the section called “Referenz zu den Genehmigungen von Lake Formation”](#).

Um von einer Tabelle **Super** aus **IAMAllowedPrincipals** zu widerrufen

1. Öffnen Sie die AWS Lake Formation Konsole unter <https://console.aws.amazon.com/lakeformation/>. Melden Sie sich als Data Lake-Administrator an.
2. Wählen Sie im Navigationsbereich Tables (Tabellen) aus.
3. Wählen Sie auf der Seite Tabellen das Optionsfeld neben der gewünschten Tabelle aus.
4. Wählen Sie im Menü Aktionen die Option Widerrufen aus.

5. Scrollen Sie im Dialogfeld Berechtigungen widerrufen in der Liste der IAM-Benutzer und -Rollen nach unten zur Überschrift Gruppe und wählen Sie IAMAllowedPrincipals aus.
6. Stellen Sie sicher, dass unter Tabellenberechtigungen die Option Super ausgewählt ist, und wählen Sie dann Revoke aus.

Um von einer Datenbank **Super** aus **IAMAllowedPrincipals** zu widerrufen

1. Öffnen Sie die AWS Lake Formation Konsole unter <https://console.aws.amazon.com/lakeformation/>. Melden Sie sich als Data Lake-Administrator an.
2. Wählen Sie im Navigationsbereich Datenbanken aus.
3. Wählen Sie auf der Seite Datenbanken das Optionsfeld neben der gewünschten Datenbank aus.
4. Wählen Sie im Menü Actions die Option Edit.
5. Deaktivieren Sie auf der Seite Datenbank bearbeiten die Option Nur IAM-Zugriffskontrolle für neue Tabellen in dieser Datenbank verwenden, und wählen Sie dann Speichern aus.
6. Vergewissern Sie sich auf der Seite Datenbanken, dass die Datenbank weiterhin ausgewählt ist, und wählen Sie dann im Menü Aktionen die Option Widerrufen aus.
7. Scrollen Sie im Dialogfeld Berechtigungen widerrufen in der Liste der IAM-Benutzer und -Rollen nach unten zur Überschrift Gruppe und wählen Sie IAMAllowedPrincipals aus.
8. Stellen Sie sicher, dass unter Datenbankberechtigungen die Option Super ausgewählt ist, und wählen Sie dann Revoke aus.

Aktivieren Sie die Lake Formation Formation-Berechtigungen für Ihren Amazon S3 S3-Standort

Als Nächstes registrieren Sie den Amazon S3 S3-Standort bei Lake Formation. Dazu können Sie den unter beschriebenen Prozess verwenden [Hinzufügen eines Amazon S3 S3-Standorts zu Ihrem Data Lake](#). Oder verwenden Sie den RegisterResource API-Vorgang wie unter beschrieben [Verkauf von Zugangsdaten APIs](#).

 Note

Wenn ein übergeordneter Standort registriert ist, müssen Sie keine untergeordneten Standorte registrieren.

Nachdem Sie diese Schritte abgeschlossen und getestet haben, ob Ihre Benutzer auf ihre Daten zugreifen können, haben Sie erfolgreich auf Lake Formation Formations-Berechtigungen aktualisiert. Fahren Sie mit dem nächsten Schritt fort, [Schritt 5: Sichern Sie sich neue Datenkatalog-Ressourcen](#).

Schritt 5: Sichern Sie sich neue Datenkatalog-Ressourcen

Sichern Sie als Nächstes alle neuen Datenkatalogressourcen, indem Sie die Standardeinstellungen für den Datenkatalog ändern. Deaktivieren Sie die Optionen, um die Zugriffskontrolle nur AWS Identity and Access Management (IAM) für neue Datenbanken und Tabellen zu verwenden.

Warning

Wenn Sie über eine Automatisierung verfügen, die Datenbanken und Tabellen im Datenkatalog erstellt, können die folgenden Schritte dazu führen, dass die Automatisierungs- und Downstream-Jobs zum Extrahieren, Transformieren und Laden (ETL) fehlschlagen. Fahren Sie erst fort, nachdem Sie entweder Ihre vorhandenen Prozesse geändert oder den erforderlichen Prinzipalen explizite Lake Formation Formations-Berechtigungen erteilt haben. Informationen zu den Berechtigungen für Lake Formation finden Sie unter [the section called "Referenz zu den Genehmigungen von Lake Formation"](#).

So ändern Sie die Standardeinstellungen für den Datenkatalog

1. Öffnen Sie die AWS Lake Formation Konsole unter <https://console.aws.amazon.com/lakeformation/>. Melden Sie sich als IAM-Administratorbenutzer an (der Benutzer Administrator oder ein anderer Benutzer mit der AdministratorAccess AWS verwalteten Richtlinie).
2. Wählen Sie im Navigationsbereich Settings (Einstellungen).
3. Deaktivieren Sie auf der Seite mit den Datenkatalogeinstellungen beide Kontrollkästchen und wählen Sie dann Speichern aus.

Der nächste Schritt besteht darin, Benutzern in future Zugriff auf weitere Datenbanken oder Tabellen zu gewähren. Siehe [Schritt 6: Geben Sie Benutzern eine neue IAM-Richtlinie für den future Zugriff auf Data Lake](#).

Schritt 6: Geben Sie Benutzern eine neue IAM-Richtlinie für den future Zugriff auf Data Lake

Um Ihren Benutzern in future Zugriff auf weitere Data Catalog-Datenbanken oder -Tabellen zu gewähren, müssen Sie ihnen die folgende grobkörnige Inline-Richtlinie AWS Identity and Access Management (IAM) zur Verfügung stellen. Speichern Sie die Richtlinie unter dem Namen `GlueFullReadAccess`.

Important

Wenn Sie diese Richtlinie an einen Benutzer anhängen, bevor Sie den Zugriff `IAMAllowedPrincipals` auf jede Datenbank und Tabelle in Ihrem Datenkatalog widerrufen`Super`, kann dieser Benutzer alle Metadaten für jede Ressource einsehen, für die der Zugriff gewährt wurde. `Super IAMAllowedPrincipals`

JSON

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Sid": "GlueFullReadAccess",
      "Effect": "Allow",
      "Action": [
        "lakeformation:GetDataAccess",
        "glue:GetTable",
        "glue:GetTables",
        "glue:SearchTables",
        "glue:GetDatabase",
        "glue:GetDatabases",
        "glue:GetPartitions"
      ],
      "Resource": "*"
    }
  ]
}
```

 Note

Die in diesem und den vorherigen Schritten festgelegten Inline-Richtlinien enthalten minimale IAM-Berechtigungen. Richtlinienvorschläge für Data Lake-Administratoren, Datenanalysten und andere Personen finden Sie unter [the section called “Referenz zu Personas und IAM-Berechtigungen in Lake Formation”](#)

Fahren Sie als Nächstes fort mit [Schritt 7: Bereinigen vorhandener IAM-Richtlinien](#)

Schritt 7: Bereinigen vorhandener IAM-Richtlinien

Nachdem Sie die AWS Lake Formation Berechtigungen eingerichtet und die Richtlinien für die grobkörnige Zugriffskontrolle AWS Identity and Access Management (IAM) erstellt und angehängt haben, führen Sie den folgenden letzten Schritt aus:

- Entfernen Sie die alten detaillierten IAM-Richtlinien für die [Zugriffskontrolle, die Sie in Lake Formation repliziert](#) haben, aus Benutzern, Gruppen und Rollen.

Auf diese Weise stellen Sie sicher, dass diese Principals keinen direkten Zugriff mehr auf die Daten in Amazon Simple Storage Service (Amazon S3) haben. Anschließend können Sie den Data Lake-Zugriff für diese Principals vollständig über Lake Formation verwalten.

AWS Lake Formation und Schnittstellen-VPC-Endpunkte (AWS PrivateLink)

Amazon VPC ist ein AWS Service, mit dem Sie AWS Ressourcen in einem von Ihnen definierten virtuellen Netzwerk starten können. Mit einer VPC haben Sie die Kontrolle über Ihre Netzwerkeinstellungen, wie IP-Adressbereich, Subnetze, Routing-Tabellen und Netzwerk-Gateways.

Wenn Sie Amazon Virtual Private Cloud (Amazon VPC) zum Hosten Ihrer AWS Ressourcen verwenden, können Sie eine private Verbindung zwischen Ihrer VPC und Lake Formation herstellen. Sie verwenden diese Verbindung, damit Lake Formation mit den Ressourcen in Ihrer VPC kommunizieren kann, ohne das öffentliche Internet nutzen zu müssen.

Sie können eine private Verbindung zwischen Ihrer VPC herstellen und AWS Lake Formation einen VPC-Schnittstellen-Endpunkt erstellen. Schnittstellenendpunkte werden mit einer Technologie

betrieben [AWS PrivateLink](#), mit der Sie privat auf Lake Formation zugreifen können, APIs ohne ein Internet-Gateway, ein NAT-Gerät, eine VPN-Verbindung oder eine Direct Connect Verbindung benötigen. Instances in Ihrer VPC benötigen keine öffentlichen IP-Adressen, um mit Lake Formation APIs zu kommunizieren. Der Verkehr zwischen Ihrer VPC und Lake Formation verlässt das Amazon-Netzwerk nicht.

Jeder Schnittstellenendpunkt wird durch eine oder mehrere [Elastic-Netzwerk-Schnittstellen](#) in Ihren Subnetzen dargestellt.

Weitere Informationen finden Sie unter [Schnittstellen-VPC-Endpunkte \(AWS PrivateLink\)](#) im Amazon-VPC-Benutzerhandbuch.

Überlegungen zu Lake Formation VPC-Endpunkten

Bevor Sie einen Schnittstellen-VPC-Endpunkt für Lake Formation einrichten, stellen Sie sicher, dass Sie die [Eigenschaften und Einschränkungen der Schnittstellenendpunkte](#) im Amazon VPC-Benutzerhandbuch lesen.

Lake Formation unterstützt Aufrufe aller API-Aktionen von Ihrer VPC aus. Sie können Lake Formation mit VPC-Endpunkten in allen verwenden AWS-Regionen , die sowohl Lake Formation- als auch Amazon VPC-Endpoints unterstützen.

Erstellen eines VPC-Schnittstellen-Endpunkts für Lake Formation

Sie können einen VPC-Endpunkt für den Lake Formation Service entweder mit der Amazon VPC-Konsole oder mit AWS Command Line Interface ()AWS CLI erstellen. Weitere Informationen finden Sie unter [Erstellung eines Schnittstellenendpunkts](#) im Benutzerhandbuch für Amazon VPC.

Erstellen Sie einen VPC-Endpunkt für Lake Formation mit dem folgenden Dienstnamen:

- `com.amazonaws. region`. Informationen zum See

Wenn Sie privates DNS für den Endpunkt aktivieren, können Sie API-Anfragen an Lake Formation stellen, indem Sie den Standard-DNS-Namen für die Region verwenden, `lakeformation.us-east-1.amazonaws.com` z. B.

Weitere Informationen finden Sie unter [Zugriff auf einen Service über einen Schnittstellenendpunkt](#) im Benutzerhandbuch für Amazon VPC.

Erstellen einer VPC-Endpunktrichtlinie für Lake Formation

Lake Formation unterstützt VPC-Endpunktrichtlinien. Eine Endpunktrichtlinie ist eine ressourcenbasierte Richtlinie, die Sie an einen VPC-Endpunkt anhängen, um zu steuern, welche AWS Principals den Endpunkt für den Zugriff auf einen Service verwenden können. AWS

Sie können Ihrem VPC-Endpunkt eine Endpunktrichtlinie hinzufügen, die den Zugriff auf Lake Formation steuert. Die Richtlinie gibt die folgenden Informationen an:

- Prinzipal, der die Aktionen ausführen kann.
- Aktionen, die ausgeführt werden können
- Die Ressourcen, für die Aktionen ausgeführt werden können.

Weitere Informationen finden Sie unter [Steuerung des Zugriffs auf Services mit VPC-Endpunkten](#) im Amazon-VPC-Benutzerhandbuch.

Beispiel: VPC-Endpunktrichtlinie für Lake Formation Formation-Aktionen

Die folgende Beispiel-VPC-Endpunktrichtlinie für Lake Formation ermöglicht den Verkauf von Anmeldeinformationen mithilfe von Lake Formation Formation-Berechtigungen. Sie können diese Richtlinie verwenden, um Abfragen mit Lake Formation Formation-Berechtigungen von einem Amazon Redshift Redshift-Cluster oder einem Amazon EMR Cluster in einem privaten Subnetz auszuführen.

```
{
  "Statement": [
    {
      "Effect": "Allow",
      "Action": "lakeformation:GetDataAccess",
      "Resource": "*",
      "Principal": "*"
    }
  ]
}
```

Note

Wenn Sie beim Erstellen eines Endpunkts keine Richtlinie anhängen, wird eine Standardrichtlinie angehängt, die vollen Zugriff auf den Service ermöglicht.

Weitere Informationen finden Sie in den folgenden Themen in der Amazon VPC-Dokumentation:

- [Was ist Amazon VPC?](#)
- [Erstellen Sie einen Schnittstellen-Endpunkt](#)
- [VPC-Endpunktrichtlinien verwenden](#)

AWS Lake Formation Tutorials

Die folgenden Tutorials sind in drei Abschnitte gegliedert und enthalten step-by-step Anweisungen zum Aufbau eines Data Lakes, zum Ingestieren von Daten, zum Teilen und Sichern von Data Lakes mithilfe von AWS Lake Formation:

1. Einen Data Lake erstellen und Daten aufnehmen: Erfahren Sie, wie Sie einen Data Lake erstellen und mithilfe von Blueprints Ihre Daten verschieben, speichern, katalogisieren, bereinigen und organisieren. Sie werden auch lernen, verwaltete Tabellen einzurichten. Eine verwaltete Tabelle ist ein neuer Amazon S3 S3-Tabellentyp, der atomare, konsistente, isolierte und dauerhafte Transaktionen (ACID) unterstützt.

Bevor Sie beginnen, stellen Sie sicher, dass Sie die unter aufgeführten Schritte abgeschlossen haben [Erste Schritte mit Lake Formation](#).

- [Einen Data Lake aus einer AWS CloudTrail Quelle erstellen](#)

Erstellen und laden Sie Ihren ersten Data Lake, indem Sie Ihre eigenen CloudTrail Logs als Datenquelle verwenden.

- [Erstellen eines Data Lakes aus einer JDBC-Quelle in Lake Formation](#)

Erstellen Sie einen Data Lake, indem Sie einen Ihrer auf JDBC zugänglichen Datenspeicher, z. B. eine relationale Datenbank, als Datenquelle verwenden.

2. Sicherung von Data Lakes: Erfahren Sie, wie Sie mithilfe von Tag-basierten Zugriffskontrollen und Zugriffskontrollen auf Zeilenebene den Zugriff auf Ihre Data Lakes effektiv sichern und verwalten können.

- [Berechtigungen für Open-Table-Speicherformate in Lake Formation einrichten](#)

Dieses Tutorial zeigt, wie Sie Berechtigungen für Open-Source-Transaktionstabellenformate (Apache Iceberg-, Apache Hudi- und Delta Lake-Tabellen der Linux Foundation) in Lake Formation einrichten.

- [Verwaltung eines Data Lakes mithilfe der Tag-basierten Zugriffskontrolle von Lake Formation](#)

Erfahren Sie, wie Sie den Zugriff auf die Daten in einem Data Lake mithilfe der tagbasierten Zugriffskontrolle in Lake Formation verwalten.

- [Sicherung von Data Lakes mit Zugriffskontrolle auf Zeilenebene](#)

Erfahren Sie, wie Sie Berechtigungen auf Zeilenebene einrichten, mit denen Sie den Zugriff auf bestimmte Zeilen auf der Grundlage von Datenkonformitäts- und Governance-Richtlinien in Lake Formation einschränken können.

3. Gemeinsame Nutzung von Daten: Erfahren Sie, wie Sie Ihre Daten AWS-Konten mithilfe von Tag-Based Access Control (TBAC) sicher teilen und detaillierte Berechtigungen für gemeinsam genutzte Datensätze verwalten können. AWS-Konten

- [Gemeinsame Nutzung eines Data Lakes mithilfe von Tag-basierter Zugriffskontrolle von Lake Formation und benannten Ressourcen](#)

In diesem Tutorial erfahren Sie, wie Sie Ihre Daten AWS-Konten mithilfe von Lake Formation sicher teilen können.

- [Gemeinsame Nutzung eines Data Lakes mithilfe der feinkörnigen Zugriffskontrolle von Lake Formation](#)

In diesem Tutorial erfahren Sie, wie Sie mithilfe von Lake Formation schnell und einfach Datensätze gemeinsam nutzen können, wenn Sie mehrere AWS-Konten mit AWS Organizations verwalten.

Themen

- [Einen Data Lake aus einer AWS CloudTrail Quelle erstellen](#)
- [Erstellen eines Data Lakes aus einer JDBC-Quelle in Lake Formation](#)
- [Berechtigungen für Open-Table-Speicherformate in Lake Formation einrichten](#)
- [Verwaltung eines Data Lakes mithilfe der Tag-basierten Zugriffskontrolle von Lake Formation](#)
- [Sicherung von Data Lakes mit Zugriffskontrolle auf Zeilenebene](#)
- [Gemeinsame Nutzung eines Data Lakes mithilfe von Tag-basierter Zugriffskontrolle von Lake Formation und benannten Ressourcen](#)
- [Gemeinsame Nutzung eines Data Lakes mithilfe der feinkörnigen Zugriffskontrolle von Lake Formation](#)

Einen Data Lake aus einer AWS CloudTrail Quelle erstellen

Dieses Tutorial führt Sie durch die Aktionen, die Sie in der Lake Formation Konsole ausführen müssen, um Ihren ersten Data Lake aus einer AWS CloudTrail Quelle zu erstellen und zu laden.

Allgemeine Schritte zum Erstellen eines Data Lakes

1. Registrieren Sie einen Amazon Simple Storage Service (Amazon S3) -Pfad als Data Lake.
2. Erteilen Sie Lake Formation die Berechtigungen, in den Datenkatalog und in Amazon S3 S3-Standorte im Data Lake zu schreiben.
3. Erstellen Sie eine Datenbank, um die Metadatentabellen im Datenkatalog zu organisieren.
4. Verwenden Sie einen Blueprint, um einen Workflow zu erstellen. Führen Sie den Workflow aus, um Daten aus einer Datenquelle aufzunehmen.
5. Richten Sie Ihre Lake Formation Formation-Berechtigungen so ein, dass andere Personen Daten im Datenkatalog und im Data Lake verwalten können.
6. Richten Sie Amazon Athena so ein, dass die Daten, die Sie in Ihren Amazon S3 S3-Data Lake importiert haben, abgefragt werden.
7. Richten Sie Amazon Redshift Spectrum für einige Datenspeichertypen so ein, dass die Daten abgefragt werden, die Sie in Ihren Amazon S3 S3-Data Lake importiert haben.

Topics

- [Zielgruppe](#)
- [Voraussetzungen](#)
- [Schritt 1: Erstellen Sie einen Data Analyst-Benutzer](#)
- [Schritt 2: Fügen Sie der Workflow-Rolle Berechtigungen zum Lesen von AWS CloudTrail Protokollen hinzu](#)
- [Schritt 3: Erstellen Sie einen Amazon S3 S3-Bucket für den Data Lake](#)
- [Schritt 4: Registrieren Sie einen Amazon S3 S3-Pfad](#)
- [Schritt 5: Erteilen Sie Berechtigungen für den Datenspeicherort](#)
- [Schritt 6: Erstellen Sie eine Datenbank im Datenkatalog](#)
- [Schritt 7: Erteilen Sie Datenberechtigungen](#)
- [Schritt 8: Verwenden Sie einen Blueprint, um einen Workflow zu erstellen](#)
- [Schritt 9: Führen Sie den Workflow aus](#)
- [Schritt 10: Gewähren Sie SELECT für die Tabellen](#)
- [Schritt 11: Fragen Sie den Data Lake ab mit Amazon Athena](#)

Zielgruppe

In der folgenden Tabelle sind die Rollen aufgeführt, die in diesem Tutorial verwendet wurden, um einen Data Lake zu erstellen.

Zielgruppe

Rolle	Description
IAM-Administrator	Hat die AWS verwaltete Richtlinie:AdministratorAccess. Kann IAM-Rollen und Amazon S3 S3-Buckets erstellen.
Data-Lake-Administrator	Benutzer, der auf den Datenkatalog zugreifen, Datenbanken erstellen und anderen Benutzern Lake Formation Formation-Berechtigungen gewähren kann. Hat weniger IAM-Berechtigungen als der IAM-Administrator, reicht aber aus, um den Data Lake zu verwalten.
Datenanalyst	Benutzer, der Abfragen für den Data Lake ausführen kann. Hat nur genügend Berechtigungen, um Abfragen auszuführen.
Workflow-Rolle	Rolle mit den erforderlichen IAM-Richtlinien zur Ausführung eines Workflows. Weitere Informationen finden Sie unter (Optional) Erstellen Sie eine IAM-Rolle für Workflows .

Voraussetzungen

Bevor Sie beginnen:

- Stellen Sie sicher, dass Sie die Aufgaben in [Richten AWS Lake Formation](#) abgeschlossen haben.
- Informieren Sie sich über den Speicherort Ihrer CloudTrail Protokolle.
- Athena verlangt von der Datenanalyst-Persona, dass sie vor der Verwendung von Athena einen Amazon S3 S3-Bucket zum Speichern von Abfrageergebnissen erstellt.

Vertrautheit mit AWS Identity and Access Management (IAM) wird vorausgesetzt. Informationen zu IAM finden Sie im [IAM-Benutzerhandbuch](#).

Schritt 1: Erstellen Sie einen Data Analyst-Benutzer

Dieser Benutzer verfügt über die Mindestberechtigungen, um den Data Lake abzufragen.

1. Öffnen Sie unter <https://console.aws.amazon.com/iam> die IAM-Konsole. Melden Sie sich als der Administratorbenutzer an, den Sie in der verwalteten Richtlinie erstellt haben, [Erstellen eines Benutzers mit Administratorzugriff](#) oder als Benutzer mit der AdministratorAccess AWS verwalteten Richtlinie.
2. Erstellen Sie einen Benutzer `datalake_user` mit dem Namen mit den folgenden Einstellungen:
 - AWS-Managementkonsole Zugriff aktivieren.
 - Legen Sie ein Passwort fest und fordern Sie kein Zurücksetzen des Passworts an.
 - Hängen Sie die AmazonAthenaFullAccess AWS verwaltete Richtlinie an.
 - Fügen Sie die folgende Inline-Richtlinie an. Speichern Sie die Richtlinie unter dem Namen `DatalakeUserBasic`.

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Action": [
        "lakeformation:GetDataAccess",
        "glue:GetTable",
        "glue:GetTables",
        "glue:SearchTables",
        "glue:GetDatabase",
        "glue:GetDatabases",
        "glue:GetPartitions",
        "lakeformation:GetResourceLFTags",
        "lakeformation:ListLFTags",
        "lakeformation:GetLFTag",
        "lakeformation:SearchTablesByLFTags",
        "lakeformation:SearchDatabasesByLFTags"
      ],
      "Resource": "*"
    }
  ]
}
```



```
}
```

Schritt 2: Fügen Sie der Workflow-Rolle Berechtigungen zum Lesen von AWS CloudTrail Protokollen hinzu

1. Fügen Sie der Rolle die folgende Inline-Richtlinie hinzu `LakeFormationWorkflowRole`. Die Richtlinie gewährt die Erlaubnis, Ihre AWS CloudTrail Protokolle zu lesen. Speichern Sie die Richtlinie unter dem Namen `DataLakeGetCloudTrail`.

Weitere Informationen zum Erstellen der `LakeFormationWorkflowRole`-Rolle finden Sie unter [\(Optional\) Erstellen Sie eine IAM-Rolle für Workflows](#).

Important

<your-s3-cloudtrail-bucket> Ersetzen Sie durch den Amazon S3 S3-Speicherort Ihrer CloudTrail Daten.

JSON

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Action": "s3:GetObject",
      "Resource": ["arn:aws:s3:::<your-s3-cloudtrail-bucket>/*"]
    }
  ]
}
```

2. Stellen Sie sicher, dass der Rolle drei Richtlinien zugeordnet sind.

Schritt 3: Erstellen Sie einen Amazon S3 S3-Bucket für den Data Lake

Erstellen Sie den Amazon S3 S3-Bucket, der der Stammspeicherort Ihres Data Lakes sein soll.

1. Öffnen Sie die Amazon S3 S3-Konsole unter <https://console.aws.amazon.com/s3/> und melden Sie sich als der Administratorbenutzer an, den Sie erstellt haben [Erstellen eines Benutzers mit Administratorzugriff](#).
2. Wählen Sie Create Bucket und erstellen Sie mithilfe des Assistenten einen Bucket mit dem `<yourName>` Namen `<yourName>-datalake-cloudtrail`, der Ihren Vor- und Nachnamen enthält. Beispiel: `jdoe-datalake-cloudtrail`.

Eine ausführliche Anleitung zur Erstellung eines Amazon S3 S3-Buckets finden Sie unter [Bucket erstellen](#).

Schritt 4: Registrieren Sie einen Amazon S3 S3-Pfad

Registrieren Sie einen Amazon S3 S3-Pfad als Stammverzeichnis Ihres Data Lakes.

1. Öffnen Sie die Lake Formation Formation-Konsole unter <https://console.aws.amazon.com/lakeformation/>. Melden Sie sich als Data Lake-Administrator an.
2. Wählen Sie im Navigationsbereich unter Registrieren und aufnehmen die Option Data Lake-Standorte aus.
3. Wählen Sie Speicherort registrieren und dann Durchsuchen aus.
4. Wählen Sie den `<yourName>-datalake-cloudtrail` Bucket aus, den Sie zuvor erstellt haben, akzeptieren Sie die Standard-IAM-Rolle `AWSServiceRoleForLakeFormationDataAccess` und wählen Sie dann Standort registrieren aus.

Weitere Informationen zur Registrierung von Standorten finden Sie unter [Hinzufügen eines Amazon S3 S3-Standorts zu Ihrem Data Lake](#).

Schritt 5: Erteilen Sie Berechtigungen für den Datenspeicherort

Prinzipale müssen über Datenspeicherberechtigungen für einen Data Lake-Standort verfügen, um Datenkatalogtabellen oder Datenbanken zu erstellen, die auf diesen Speicherort verweisen. Sie müssen der IAM-Rolle für Workflows Datenspeicherberechtigungen erteilen, damit der Workflow in das Datenaufnahmeziel schreiben kann.

1. Wählen Sie im Navigationsbereich unter Berechtigungen die Option Datenspeicherorte aus.

2. Wählen Sie Grant aus, und treffen Sie im Dialogfeld Berechtigungen gewähren die folgenden Auswahlen:
 - a. Wählen Sie für IAM-Benutzer und -Rollen die Option. `LakeFormationWorkflowRole`
 - b. Wählen Sie für Speicherorte Ihren `<yourName>-datalake-cloudtrail` Bucket aus.
3. Wählen Sie Grant (Erteilen).

Weitere Informationen zu Berechtigungen für Datenspeicherorte finden Sie unter [Underlying data access control](#).

Schritt 6: Erstellen Sie eine Datenbank im Datenkatalog

Metadatentabellen im Lake Formation Data Catalog werden in einer Datenbank gespeichert.

1. Wählen Sie im Navigationsbereich unter Datenkatalog die Option Datenbanken aus.
2. Wählen Sie Datenbank erstellen aus, und geben Sie unter Datenbankdetails den Namen `einlakeformation_cloudtrail`.
3. Lassen Sie die anderen Felder leer und wählen Sie Datenbank erstellen aus.

Schritt 7: Erteilen Sie Datenberechtigungen

Sie müssen Berechtigungen zum Erstellen von Metadatentabellen im Datenkatalog erteilen. Da der Workflow mit der Rolle ausgeführt wird `LakeFormationWorkflowRole`, müssen Sie der Rolle diese Berechtigungen erteilen.

1. Wählen Sie in der Lake Formation Formation-Konsole im Navigationsbereich unter Datenkatalog die Option Datenbanken aus.
2. Wählen Sie die `lakeformation_cloudtrail` Datenbank aus und wählen Sie dann in der Dropdownliste Aktionen unter der Überschrift Berechtigungen die Option Grant aus.
3. Treffen Sie im Dialogfeld „Datenberechtigungen gewähren“ die folgenden Optionen:
 - a. Wählen Sie unter Principals für IAM-Benutzer und -Rollen die Option aus. `LakeFormationWorkflowRole`
 - b. Wählen Sie unter LF-Tags or catalog resources (LF-Tags oder Katalogressourcen) die Option Named Data Catalog resources (Benannte Datenkatalogressourcen).

- c. Bei Datenbanken sollten Sie sehen, dass die `lakeformation_cloudtrail` Datenbank bereits hinzugefügt wurde.
 - d. Wählen Sie unter Datenbankberechtigungen die Optionen Tabelle erstellen, Ändern und Löschen aus, und deaktivieren Sie Super, falls diese Option ausgewählt ist.
4. Wählen Sie Grant (Erteilen).

Weitere Informationen zur Erteilung von Lake Formation Formation-Berechtigungen finden Sie unter [Verwaltung von Lake Formation Formation-Berechtigungen](#).

Schritt 8: Verwenden Sie einen Blueprint, um einen Workflow zu erstellen

Um die CloudTrail Protokolle zu lesen, ihre Struktur zu verstehen und die entsprechenden Tabellen im Datenkatalog zu erstellen, müssen wir einen Workflow einrichten, der aus AWS Glue Crawlern, Jobs, Triggern und Workflows besteht. Die Blueprints von Lake Formation vereinfachen diesen Prozess.

Der Workflow generiert die Jobs, Crawler und Trigger, die Daten erkennen und in Ihren Data Lake aufnehmen. Sie erstellen einen Workflow, der auf einem der vordefinierten Lake Formation-Blueprints basiert.

1. Wählen Sie in der Lake Formation Formation-Konsole im Navigationsbereich unter Ingestion die Option Blueprints aus, und wählen Sie dann Blueprint verwenden aus.
2. Wählen Sie auf der Seite Blueprint verwenden unter Blueprint-Typ die Option aus. AWS CloudTrail
3. Wählen Sie unter Quelle importieren eine CloudTrail Quelle und ein Startdatum aus.
4. Geben Sie unter Importziel die folgenden Parameter an:

Zieldatenbank	<code>lakeformation_cloudtrail</code>
Zielspeicherort	<code>s3://<yourName> -datalake-cloudtrail</code>
Data format (Datenformat)	Parquet

5. Wählen Sie für die Importhäufigkeit die Option Bei Bedarf ausführen aus.
6. Geben Sie unter Importoptionen die folgenden Parameter an:

Name des Workflows	lakeformationcloudtrailtest
IAM role (IAM-Rolle)	LakeFormationWorkflowRole
Tabellenpräfix	cloudtrailtest

Note

Muss in Kleinbuchstaben geschrieben werden.

- Wählen Sie Create und warten Sie, bis die Konsole meldet, dass der Workflow erfolgreich erstellt wurde.

Tip

Haben Sie die folgende Fehlermeldung erhalten?

User: arn:aws:iam::<account-id>:user/<datalake_administrator_user> is not authorized to perform: iam:PassRole on resource:arn:aws:iam::<account-id>:role/LakeFormationWorkflowRole...

Falls ja, überprüfen Sie, ob Sie die Inline-Richtlinie für den Data Lake-Administratorbenutzer durch eine gültige AWS Kontonummer ersetzt <account-id> haben.

Schritt 9: Führen Sie den Workflow aus

Da Sie angegeben haben, dass es sich um einen Workflow handelt run-on-demand, müssen Sie den Workflow manuell starten.

- Wählen Sie auf der Seite Blueprints den Workflow aus lakeformationcloudtrailtest, und klicken Sie im Menü Aktionen auf Start.

Während der Ausführung des Workflows können Sie seinen Fortschritt in der Spalte Status der letzten Ausführung einsehen. Wählen Sie gelegentlich die Schaltfläche „Aktualisieren“.

Der Status wechselt von LÄUFT zu Wird erkannt, importiert und ist ABGESCHLOSSEN.

Wenn der Workflow abgeschlossen ist:

- Der Datenkatalog wird neue Metadatentabellen enthalten.
- Ihre CloudTrail Protokolle werden in den Data Lake aufgenommen.

Wenn der Workflow fehlschlägt, gehen Sie wie folgt vor:

- a. Wählen Sie den Workflow aus, und klicken Sie im Menü Aktionen auf Diagramm anzeigen.

Der Workflow wird in der AWS Glue Konsole geöffnet.

- b. Wählen Sie den Workflow aus und gehen Sie auf die Registerkarte History (Verlauf).
- c. Wählen Sie unter Verlauf den letzten Lauf aus und klicken Sie auf Laufdetails anzeigen.
- d. Wählen Sie im dynamischen (Laufzeit-) Diagramm einen fehlgeschlagenen Job oder Crawler aus und überprüfen Sie die Fehlermeldung. Fehlgeschlagene Knoten sind entweder rot oder gelb.

Schritt 10: Gewähren Sie SELECT für die Tabellen

Sie müssen die SELECT Berechtigung für die neuen Datenkatalogtabellen erteilen, damit der Datenanalyst die Daten abfragen kann, auf die die Tabellen verweisen.

Note

Ein Workflow erteilt dem Benutzer, der ihn ausgeführt hat, automatisch die SELECT Berechtigung für die Tabellen, die er erstellt hat. Da der Data Lake-Administrator diesen Workflow ausgeführt hat, müssen Sie ihn SELECT dem Datenanalysten erteilen.

1. Wählen Sie in der Lake Formation Konsole im Navigationsbereich unter Datenkatalog die Option Datenbanken aus.
2. Wählen Sie die `lakeformation_cloudtrail` Datenbank aus und wählen Sie dann in der Dropdownliste Aktionen unter der Überschrift Berechtigungen die Option Grant aus.
3. Treffen Sie im Dialogfeld „Datenberechtigungen gewähren“ die folgenden Optionen:

- a. Wählen Sie unter Principals für IAM-Benutzer und -Rollen die Option aus. `datalake_user`
 - b. Wählen Sie unter LF-Tags oder Katalogressourcen die Option Benannte Datenkatalogressourcen aus.
 - c. Für Datenbanken sollte die `lakeformation_cloudtrail` Datenbank bereits ausgewählt sein.
 - d. Wählen Sie für Tabellen die Option `cloudtrailtest-cloudtrail`.
 - e. Wählen Sie unter Tabellen- und Spaltenberechtigungen die Option Auswählen aus.
4. Wählen Sie Grant (Erteilen).

Der nächste Schritt wird als Datenanalyst ausgeführt.

Schritt 11: Fragen Sie den Data Lake ab mit Amazon Athena

Verwenden Sie die Amazon Athena Konsole, um die CloudTrail Daten in Ihrem Data Lake abzufragen.

1. Öffnen Sie die Athena-Konsole unter <https://console.aws.amazon.com/athena/> und melden Sie sich als Datenanalyst, Benutzer `datalake_user` an.
2. Falls erforderlich, wählen Sie Get Started, um zum Athena-Abfrage-Editor zu gelangen.
3. Wählen Sie für Datenquelle `AwsDataCatalog` aus.
4. Wählen Sie unter Database (Datenbank) Option `lakeformation_cloudtrail` aus.

Die Tabellenliste wird aufgefüllt.

5. Wählen Sie im Überlaufmenü (3 horizontal angeordnete Punkte) neben der Tabelle **`cloudtrailtest-cloudtrail`** die Option Tabellenvorschau und anschließend Ausführen aus.

Die Abfrage wird ausgeführt und zeigt 10 Datenzeilen an.

Wenn Sie Athena noch nicht verwendet haben, müssen Sie zunächst einen Amazon S3 S3-Standort in der Athena-Konsole zum Speichern der Abfrageergebnisse konfigurieren. Sie `datalake_user` müssen über die erforderlichen Berechtigungen für den Zugriff auf den von Ihnen Amazon S3 S3-Bucket verfügen.

 Note

Nachdem Sie das Tutorial abgeschlossen haben, gewähren Sie den Prinzipalen in Ihrer Organisation Datenberechtigungen und Datenspeicherberechtigungen.

Erstellen eines Data Lakes aus einer JDBC-Quelle in Lake Formation

Dieses Tutorial führt Sie durch die Schritte, die Sie auf der AWS Lake Formation Konsole ausführen müssen, um mithilfe von Lake Formation Ihren ersten Data Lake aus einer JDBC-Quelle zu erstellen und zu laden.

Themen

- [Zielgruppe](#)
- [Voraussetzungen für das JDBC-Tutorial](#)
- [Schritt 1: Erstellen Sie einen Data Analyst-Benutzer](#)
- [Schritt 2: Erstellen Sie eine Verbindung in AWS Glue](#)
- [Schritt 3: Erstellen Sie einen Amazon S3 S3-Bucket für den Data Lake](#)
- [Schritt 4: Registrieren Sie einen Amazon S3 S3-Pfad](#)
- [Schritt 5: Erteilen Sie Berechtigungen für den Datenspeicherort](#)
- [Schritt 6: Erstellen Sie eine Datenbank im Datenkatalog](#)
- [Schritt 7: Erteilen Sie Datenberechtigungen](#)
- [Schritt 8: Verwenden Sie einen Blueprint, um einen Workflow zu erstellen](#)
- [Schritt 9: Führen Sie den Workflow aus](#)
- [Schritt 10: Gewähren Sie SELECT für die Tabellen](#)
- [Schritt 11: Fragen Sie den Data Lake ab mit Amazon Athena](#)
- [Schritt 12: Fragen Sie die Daten im Data Lake mit Amazon Redshift Spectrum ab](#)
- [Schritt 13: Erteilen oder Widerrufen Lake Formation Formation-Berechtigungen mithilfe von Amazon Redshift Spectrum](#)

Zielgruppe

In der folgenden Tabelle sind die Rollen aufgeführt, die in diesem [AWS Lake Formation JDBC-Tutorial](#) verwendet werden.

Rolle	Description
IAM-Administrator	Ein Benutzer, der AWS Identity and Access Management (IAM) -Benutzer und -Rollen sowie Amazon Simple Storage Service (Amazon S3) -Buckets erstellen kann. Hat die AdministratorAccess AWS verwaltete Richtlinie.
Data Lake-Administrator	Ein Benutzer, der auf den Datenkatalog zugreifen, Datenbanken erstellen und anderen Benutzern Lake Formation Formation-Berechtigungen gewähren kann. Hat weniger IAM-Berechtigungen als der IAM-Administrator, reicht aber aus, um den Data Lake zu verwalten .
Datenanalyst	Ein Benutzer, der Abfragen für den Data Lake ausführen kann. Hat nur genügend Berechtigungen, um Abfragen auszuführen.
Workflow-Rolle	Eine Rolle mit den erforderlichen IAM-Richtlinien zur Ausführung eines Workflows.

Informationen zu den Voraussetzungen für das Abschließen des Tutorials finden Sie unter [Voraussetzungen für das JDBC-Tutorial](#).

Voraussetzungen für das JDBC-Tutorial

Bevor Sie mit dem [AWS Lake Formation JDBC-Tutorial](#) beginnen, stellen Sie sicher, dass Sie Folgendes getan haben:

- Führen Sie die Aufgaben unter [Erste Schritte mit Lake Formation](#).

- Entscheiden Sie sich für einen JDBC-zugänglichen Datenspeicher, den Sie für das Tutorial verwenden möchten.
- Sammeln Sie die Informationen, die zum Herstellen einer AWS Glue Verbindung des Typs JDBC erforderlich sind. Dieses Datenkatalogobjekt enthält die URL zum Datenspeicher, Anmeldeinformationen und zusätzliche VPC-spezifische Konfigurationsinformationen, falls der Datenspeicher in einer Amazon Virtual Private Cloud (Amazon VPC) erstellt wurde. Weitere Informationen finden Sie unter [Definieren von Verbindungen im AWS Glue Datenkatalog im Entwicklerhandbuch](#).AWS Glue

In der Anleitung wird davon ausgegangen, dass Sie mit AWS Identity and Access Management (IAM) vertraut sind. Informationen zu IAM finden Sie im [IAM-Benutzerhandbuch](#).

Um zu beginnen, fahren Sie mit fort. [the section called “Schritt 1: Erstellen Sie einen Data Analyst-Benutzer”](#)

Schritt 1: Erstellen Sie einen Data Analyst-Benutzer

In diesem Schritt erstellen Sie einen AWS Identity and Access Management (IAM-) Benutzer, der als Datenanalyst für Ihren Data Lake in fungiert. AWS Lake Formation

Dieser Benutzer verfügt über die Mindestberechtigungen, um den Data Lake abzufragen.

1. Öffnen Sie unter <https://console.aws.amazon.com/iam> die IAM-Konsole. Melden Sie sich als der Administratorbenutzer an, den Sie in der verwalteten Richtlinie erstellt haben, [Erstellen eines Benutzers mit Administratorzugriff](#) oder als Benutzer mit der AdministratorAccess AWS verwalteten Richtlinie.
2. Erstellen Sie einen Benutzer `dataLake_user` mit dem Namen mit den folgenden Einstellungen:
 - AWS-Managementkonsole Zugriff aktivieren.
 - Legen Sie ein Passwort fest und fordern Sie kein Zurücksetzen des Passworts an.
 - Hängen Sie die `AmazonAthenaFullAccess` AWS verwaltete Richtlinie an.
 - Fügen Sie die folgende Inline-Richtlinie an. Speichern Sie die Richtlinie unter dem Namen `DataLakeUserBasic`.

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

```

```
{
  "Effect": "Allow",
  "Action": [
    "lakeformation:GetDataAccess",
    "glue:GetTable",
    "glue:GetTables",
    "glue:SearchTables",
    "glue:GetDatabase",
    "glue:GetDatabases",
    "glue:GetPartitions",
    "lakeformation:GetResourceLFTags",
    "lakeformation:ListLFTags",
    "lakeformation:GetLFTag",
    "lakeformation:SearchTablesByLFTags",
    "lakeformation:SearchDatabasesByLFTags"
  ],
  "Resource": "*"
}
```

Schritt 2: Erstellen Sie eine Verbindung in AWS Glue

Note

Überspringen Sie diesen Schritt, wenn Sie bereits eine AWS Glue Verbindung zu Ihrer JDBC-Datenquelle haben.

AWS Lake Formation greift über eine Verbindung auf JDBC-Datenquellen zu. AWS Glue Eine Verbindung ist ein Datenkatalogobjekt, das alle Informationen enthält, die für die Verbindung mit der Datenquelle erforderlich sind. Sie können mit der AWS Glue Konsole eine Verbindung herstellen.

So stellen Sie eine Verbindung her

1. Öffnen Sie AWS Glue die Konsole unter <https://console.aws.amazon.com/glue/> und melden Sie sich als der Administratorbenutzer an, den Sie erstellt haben [Erstellen eines Benutzers mit Administratorzugriff](#).
2. Wählen Sie im Navigationsbereich unter Data catalog die Option Connections (Verbindungen) aus.

3. Wählen Sie auf der Seite Connectors die Option Verbindung erstellen aus.
4. Wählen Sie auf der Seite Datenquelle auswählen die Option JDBC als Verbindungstyp aus. Klicken Sie anschließend auf Weiter.
5. Fahren Sie mit dem Verbindungsassistenten fort und speichern Sie die Verbindung.

Informationen zum Erstellen einer Verbindung finden Sie unter [AWS Glue JDBC-Verbindungseigenschaften](#) im AWS Glue Entwicklerhandbuch.

Schritt 3: Erstellen Sie einen Amazon S3 S3-Bucket für den Data Lake

In diesem Schritt erstellen Sie den Amazon Simple Storage Service (Amazon S3) -Bucket, der als Stammverzeichnis Ihres Data Lake dienen soll.

1. Öffnen Sie die Amazon S3 S3-Konsole unter <https://console.aws.amazon.com/s3/> und melden Sie sich als der Administratorbenutzer an, den Sie erstellt haben [Erstellen eines Benutzers mit Administratorzugriff](#).
2. Wählen Sie Create Bucket und erstellen Sie mithilfe des Assistenten einen Bucket mit dem `<yourName>` Namen `<yourName>-datalake-tutorial`, der Ihren Vor- und Nachnamen enthält. Beispiel: `jdoe-datalake-tutorial`.

Eine ausführliche Anleitung zur Erstellung eines Amazon S3 S3-Buckets finden Sie unter [Wie erstelle ich einen S3-Bucket?](#) im Amazon Simple Storage Service-Benutzerhandbuch.

Schritt 4: Registrieren Sie einen Amazon S3 S3-Pfad

In diesem Schritt registrieren Sie einen Amazon Simple Storage Service (Amazon S3) -Pfad als Stammverzeichnis Ihres Data Lakes.

1. Öffnen Sie die Lake Formation Formation-Konsole unter <https://console.aws.amazon.com/lakeformation/>. Melden Sie sich als Data Lake-Administrator an.
2. Wählen Sie im Navigationsbereich unter Verwaltung die Option Data Lake-Standorte aus.
3. Wählen Sie Speicherort registrieren und dann Durchsuchen aus.
4. Wählen Sie den `<yourName>-datalake-tutorial` Bucket aus, den Sie zuvor erstellt haben, akzeptieren Sie die Standard-IAM-Rolle `AWSServiceRoleForLakeFormationDataAccess` und wählen Sie dann Standort registrieren aus.

Weitere Informationen zur Registrierung von Standorten finden Sie unter [Hinzufügen eines Amazon S3 S3-Standorts zu Ihrem Data Lake](#).

Schritt 5: Erteilen Sie Berechtigungen für den Datenspeicherort

Prinzipale müssen über Datenstandortberechtigungen für einen Data Lake-Standort verfügen, um Datenkatalogtabellen oder Datenbanken zu erstellen, die auf diesen Speicherort verweisen. Sie müssen der IAM-Rolle für Workflows Datenspeicherberechtigungen erteilen, damit der Workflow in das Datenaufnahmeziel schreiben kann.

1. Wählen Sie in der Lake Formation Formation-Konsole im Navigationsbereich unter Berechtigungen die Option Datenspeicherorte aus.
2. Wählen Sie Grant aus, und gehen Sie im Dialogfeld Berechtigungen gewähren wie folgt vor:
 - a. Wählen Sie für IAM-Benutzer und -Rollen die Option `LakeFormationWorkflowRole`.
 - b. Wählen Sie für Speicherorte Ihren `<yourName>-datalake-tutorial` Bucket aus.
3. Wählen Sie Grant (Erteilen).

Weitere Informationen zu Berechtigungen für Datenspeicherorte finden Sie unter [Underlying data access control](#).

Schritt 6: Erstellen Sie eine Datenbank im Datenkatalog

Metadatentabellen im Lake Formation Data Catalog werden in einer Datenbank gespeichert.

1. Wählen Sie in der Lake Formation Formation-Konsole im Navigationsbereich unter Datenkatalog die Option Datenbanken aus.
2. Wählen Sie Datenbank erstellen aus, und geben Sie unter Datenbankdetails den Namen `enlakeformation_tutorial`.
3. Lassen Sie die anderen Felder leer und wählen Sie Datenbank erstellen aus.

Schritt 7: Erteilen Sie Datenberechtigungen

Sie müssen Berechtigungen zum Erstellen von Metadatentabellen im Datenkatalog erteilen. Da der Workflow mit der Rolle ausgeführt wird `LakeFormationWorkflowRole`, müssen Sie der Rolle diese Berechtigungen gewähren.

1. Wählen Sie in der Lake Formation Formation-Konsole im Navigationsbereich unter Berechtigungen die Option Data Lake-Berechtigungen aus.
2. Wählen Sie Grant aus, und gehen Sie im Dialogfeld Datenberechtigungen gewähren wie folgt vor:
 - a. Wählen Sie unter Principals für IAM-Benutzer und -Rollen die Option aus.
LakeFormationWorkflowRole
 - b. Wählen Sie unter LF-Tags oder Katalogressourcen die Option Benannte Datenkatalogressourcen aus.
 - c. Wählen Sie für Datenbanken die Datenbank aus, die Sie zuvor erstellt haben.
lakeformation_tutorial
 - d. Wählen Sie unter Datenbankberechtigungen die Optionen Tabelle erstellen, Ändern und Löschen aus, und deaktivieren Sie Super, falls diese Option ausgewählt ist.
3. Wählen Sie Grant (Erteilen).

Weitere Informationen zur Erteilung von Lake Formation Formation-Berechtigungen finden Sie unter [Überblick über die Genehmigungen für Lake Formation](#).

Schritt 8: Verwenden Sie einen Blueprint, um einen Workflow zu erstellen

Der AWS Lake Formation Workflow generiert die AWS Glue Jobs, Crawler und Trigger, die Daten erkennen und in Ihren Data Lake aufnehmen. Sie erstellen einen Workflow, der auf einem der vordefinierten Lake Formation-Blueprints basiert.

1. Wählen Sie in der Lake Formation Formation-Konsole im Navigationsbereich Blueprints und dann Blueprint verwenden aus.
2. Wählen Sie auf der Seite Blueprint verwenden unter Blueprint-Typ die Option Datenbank-Snapshot aus.
3. Wählen Sie unter Importquelle für Datenbankverbindung die Verbindung aus, die Sie gerade erstellt habendatalake-tutorial, oder wählen Sie eine bestehende Verbindung für Ihre Datenquelle aus.
4. Geben Sie im Formular `<database>/<schema>/<table>` unter Quelldatenpfad den Pfad ein, aus dem Daten aufgenommen werden sollen.

Sie können den Platzhalter Prozent (%) durch Schema oder Tabelle ersetzen. Geben Sie für Datenbanken, die Schemas unterstützen, `<database>/<schema>/%` ein, um alle darin

enthaltenen Tabellen abzugleichen. *<schema>* *<database>* Oracle Database und MySQL unterstützen kein Schema im Pfad. Geben Sie stattdessen *<database>* /% ein. Für Oracle Database *<database>* ist dies der Systembezeichner (SID).

Wenn eine Oracle-Datenbank beispielsweise die SID `hatorc1`, geben Sie ein, dass sie allen Tabellen `orc1/%` entspricht, auf die der in der JDCB-Verbindung angegebene Benutzer Zugriff hat.

Important

Bitte beachten Sie die Groß- und Kleinschreibung.

5. Geben Sie unter Importziel die folgenden Parameter an:

Zielfdatenbank	lakeformation_tutorial
Zielspeicherort	s3:// <i><yourName></i> -datalake-tutorial
Data format (Datenformat)	(Wählen Sie Parquet oder CSV)

6. Wählen Sie für die Importhäufigkeit die Option Bei Bedarf ausführen aus.
7. Geben Sie unter Importoptionen die folgenden Parameter an:

Name des Workflows	lakeformationjdbctest
IAM role (IAM-Rolle)	LakeFormationWorkflowRole
Tabellenpräfix	jdbctest

Note

Muss in Kleinbuchstaben geschrieben werden.

8. Wählen Sie Create und warten Sie, bis die Konsole meldet, dass der Workflow erfolgreich erstellt wurde.

 Tip

Haben Sie die folgende Fehlermeldung erhalten?

```
User: arn:aws:iam::<account-id>:user/<datalake_administrator_user> is not authorized to
perform: iam:PassRole on resource:arn:aws:iam::<account-id>:role/
LakeFormationWorkflowRole...
```

Falls ja, überprüfen Sie, ob Sie `<account-id>` in der Inline-Richtlinie für den Data Lake-Administratorbenutzer eine gültige AWS Kontonummer eingegeben haben.

Schritt 9: Führen Sie den Workflow aus

Da Sie angegeben haben, dass es sich um einen Workflow handelt run-on-demand, müssen Sie den Workflow manuell in starten AWS Lake Formation.

1. Wählen Sie in der Lake Formation Konsole auf der Seite Blueprints den Workflow `lakeformationjdbctest` aus.
2. Wählen Sie Aktionen und dann Start aus.
3. Während der Ausführung des Workflows können Sie seinen Fortschritt in der Spalte Status der letzten Ausführung anzeigen. Wählen Sie gelegentlich die Schaltfläche „Aktualisieren“.

Der Status wechselt von LÄUFT zu Wird erkannt, importiert und ist ABGESCHLOSSEN.

Wenn der Workflow abgeschlossen ist:

- Der Datenkatalog enthält neue Metadatentabellen.
- Ihre Daten werden in den Data Lake aufgenommen.

Wenn der Workflow fehlschlägt, gehen Sie wie folgt vor:

- a. Wählen Sie den Workflow aus. Wählen Sie Aktionen und dann Diagramm anzeigen aus.

Der Workflow wird in der AWS Glue Konsole geöffnet.

- b. Wählen Sie den Workflow und dann die Registerkarte Verlauf aus.
- c. Wählen Sie den letzten Lauf aus und wählen Sie Laufdetails anzeigen.

- d. Wählen Sie im dynamischen (Laufzeit-) Diagramm einen fehlgeschlagenen Job oder Crawler aus und überprüfen Sie die Fehlermeldung. Fehlgeschlagene Knoten sind entweder rot oder gelb.

Schritt 10: Gewähren Sie SELECT für die Tabellen

Sie müssen die SELECT Berechtigung für die neuen Datenkatalogtabellen erteilen, AWS Lake Formation damit der Datenanalyst die Daten abfragen kann, auf die die Tabellen verweisen.

Note

Ein Workflow erteilt dem Benutzer, der ihn ausgeführt hat, automatisch die SELECT Berechtigung für die Tabellen, die er erstellt hat. Da der Data Lake-Administrator diesen Workflow ausgeführt hat, müssen Sie ihn SELECT dem Datenanalysten erteilen.

1. Wählen Sie in der Lake Formation Konsole im Navigationsbereich unter Berechtigungen die Option Data Lake-Berechtigungen aus.
2. Wählen Sie Grant aus, und gehen Sie im Dialogfeld Datenberechtigungen gewähren wie folgt vor:
 - a. Wählen Sie unter Principals für IAM-Benutzer und -Rollen die Option aus. `datalake_user`
 - b. Wählen Sie unter LF-Tags oder Katalogressourcen die Option Benannte Datenkatalogressourcen aus.
 - c. Wählen Sie für Datenbanken die Option. `lakeformation_tutorial`

Die Tabellenliste wird aufgefüllt.

 - d. Wählen Sie für Tabellen eine oder mehrere Tabellen aus Ihrer Datenquelle aus.
 - e. Wählen Sie unter Tabellen- und Spaltenberechtigungen die Option Auswählen aus.
3. Wählen Sie Grant (Erteilen).

Der nächste Schritt wird als Datenanalyst ausgeführt.

Schritt 11: Fragen Sie den Data Lake ab mit Amazon Athena

Verwenden Sie die Amazon Athena Konsole, um die Daten in Ihrem Data Lake abzufragen.

1. Öffnen Sie die Athena-Konsole unter <https://console.aws.amazon.com/athena/> und melden Sie sich als Datenanalyst-Benutzer `data_lake_user` an.
2. Falls erforderlich, wählen Sie Get Started, um zum Athena-Abfrage-Editor zu gelangen.
3. Wählen Sie für Datenquelle `AwsDataCatalog` aus.
4. Wählen Sie unter Database (Datenbank) Option `lakeformation_tutorial` aus.

Die Tabellenliste wird aufgefüllt.

5. Wählen Sie im Popupmenü neben einer der Tabellen die Option Tabellenvorschau aus.

Die Abfrage wird ausgeführt und zeigt 10 Datenzeilen an.

Schritt 12: Fragen Sie die Daten im Data Lake mit Amazon Redshift Spectrum ab

Sie können Amazon Redshift Spectrum so einrichten, dass die Daten abgefragt werden, die Sie in Ihren Amazon Simple Storage Service (Amazon S3) Data Lake importiert haben. Erstellen Sie zunächst eine AWS Identity and Access Management (IAM-) Rolle, die zum Starten des Amazon Redshift Redshift-Clusters und zum Abfragen der Amazon S3 S3-Daten verwendet wird. Erteilen Sie dieser Rolle anschließend die `Select` Berechtigungen für die Tabellen, die Sie abfragen möchten. Erteilen Sie dem Benutzer anschließend Berechtigungen zur Verwendung des Amazon Redshift Redshift-Abfrage-Editors. Erstellen Sie abschließend einen Amazon Redshift Redshift-Cluster und führen Sie Abfragen aus.

Sie erstellen den Cluster als Administrator und fragen den Cluster als Datenanalyst ab.

Weitere Informationen zu Amazon Redshift Spectrum finden Sie unter [Verwenden von Amazon Redshift Spectrum zur Abfrage externer Daten](#) im Amazon Redshift Database Developer Guide.

So richten Sie Berechtigungen für die Ausführung von Amazon Redshift Redshift-Abfragen ein

1. Öffnen Sie unter <https://console.aws.amazon.com/iam/> die IAM-Konsole. Melden Sie sich als der Administratorbenutzer an, den Sie in [Erstellen eines Benutzers mit Administratorzugriff](#) (Benutzername `Administrator`) erstellt haben, oder als Benutzer mit der `AdministratorAccess` AWS verwalteten Richtlinie.
2. Wählen Sie im Navigationsbereich Policies aus.

Wenn Sie zum ersten Mal Policies (Richtlinien) auswählen, erscheint die Seite Welcome to Managed Policies (Willkommen bei verwalteten Richtlinien). Wählen Sie Get Started.

3. Wählen Sie Richtlinie erstellen aus.
4. Wählen Sie den Tab JSON.
5. Fügen Sie das folgende JSON-Richtliniendokument ein.

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Action": [
        "lakeformation:GetDataAccess",
        "glue:GetTable",
        "glue:GetTables",
        "glue:SearchTables",
        "glue:GetDatabase",
        "glue:GetDatabases",
        "glue:GetPartitions",
        "lakeformation:GetResourceLFTags",
        "lakeformation:ListLFTags",
        "lakeformation:GetLFTag",
        "lakeformation:SearchTablesByLFTags",
        "lakeformation:SearchDatabasesByLFTags"
      ],
      "Resource": "*"
    }
  ]
}
```

6. Wählen Sie, wenn Sie fertig sind, Review (Überprüfen) aus. Die Richtlinienvvalidierung meldet mögliche Syntaxfehler.
7. Geben Sie auf der Seite „Richtlinie überprüfen“ den Namen **RedshiftLakeFormationPolicy** für die Richtlinie ein, die Sie erstellen. (Optional) Geben Sie eine Beschreibung ein. Überprüfen Sie unter Summary die Richtlinienzusammenfassung, um die Berechtigungen einzusehen, die von Ihrer Richtlinie gewährt werden. Wählen Sie dann Create policy aus, um Ihre Eingaben zu speichern.
8. Klicken Sie im Navigationsbereich der IAM-Konsole auf Rollen, und wählen Sie dann Rolle erstellen.

9. Wählen Sie für Select trusted entity (Vertrauenswürdige Entität auswählen) die Option AWS - Dienst.
10. Wählen Sie den Amazon-Redshift-Service aus, um diese Rolle anzunehmen.
11. Wählen Sie den Anwendungsfall Redshift Customizable (Durch Redshift anpassbar) für Ihren Service aus. Wählen Sie dann Next: Permissions.
12. Suchen Sie nach der Berechtigungsrichtlinie, die Sie erstellt haben `RedshiftLakeFormationPolicy`, und aktivieren Sie das Kontrollkästchen neben dem Richtliniennamen in der Liste.
13. Wählen Sie Next: Tags (Weiter: Tags) aus.
14. Klicken Sie auf Weiter: Prüfen.
15. Geben Sie für Role name (Rollenname) den Namen **RedshiftLakeFormationRole** ein.
16. (Optional) Geben Sie im Feld Role description (Rollenbeschreibung) eine Beschreibung für die neue Rolle ein.
17. Prüfen Sie die Rolle und klicken Sie dann auf Create Role (Rolle erstellen).

Um **Select** Berechtigungen für die Tabelle zu erteilen, die in der Lake Formation Formation-Datenbank abgefragt werden soll

1. Öffnen Sie die Lake Formation Formation-Konsole unter <https://console.aws.amazon.com/lakeformation/>. Melden Sie sich als Data Lake-Administrator an.
2. Wählen Sie im Navigationsbereich unter Berechtigungen die Option Data Lake-Berechtigungen und dann Grant aus.
3. Geben Sie die folgenden Informationen ein:
 - Wählen Sie für IAM-Benutzer und -Rollen die von Ihnen erstellte IAM-Rolle aus. `RedshiftLakeFormationRole` Wenn Sie den Amazon Redshift Query Editor ausführen, verwendet dieser die IAM-Rolle, um die erforderlichen Berechtigungen für die Daten zu erhalten.
 - Wählen Sie unter Database (Datenbank) Option `lakeformation_tutorial` aus.

Die Tabellenliste wird aufgefüllt.
 - Wählen Sie für Tabelle eine Tabelle in der abzufragenden Datenquelle aus.
 - Wählen Sie die Berechtigung Tabelle auswählen.
4. Wählen Sie Grant (Erteilen).

So richten Sie Amazon Redshift Spectrum ein und führen Abfragen aus

1. Öffnen Sie die Amazon Redshift Redshift-Konsole unter <https://console.aws.amazon.com/redshift>. Melden Sie sich als Benutzer Administrator an.
2. Wählen Sie Cluster erstellen.
3. Geben Sie auf der Seite Cluster erstellen `redshift-lakeformation-demo` die Cluster-ID ein.
4. Wählen Sie für den Knotentyp `dc2.large` aus.
5. Scrollen Sie nach unten und geben Sie unter Datenbankkonfigurationen die folgenden Parameter ein, oder akzeptieren Sie sie:
 - Admin-Benutzername: `awsuser`
 - Admin-Benutzerpasswort: (*Choose a password*)
6. Erweitern Sie Cluster-Berechtigungen und wählen Sie für Verfügbare IAM-Rollen die Option `RedshiftLakeFormationRole`. Wählen Sie dann Add IAM role (IAM-Rolle hinzufügen) aus.
7. Wenn Sie einen anderen Port als den Standardwert 5439 verwenden müssen, deaktivieren Sie neben Zusätzliche Konfigurationen die Option Standardwerte verwenden. Erweitern Sie den Abschnitt für Datenbankkonfigurationen und geben Sie eine neue Datenbankportnummer ein.
8. Wählen Sie Cluster erstellen.

Die Cluster-Seite wird geladen.

9. Warten Sie, bis der Cluster-Status „Verfügbar“ lautet. Wählen Sie regelmäßig das Aktualisierungssymbol.
10. Erteilen Sie dem Datenanalysten die Erlaubnis, Abfragen für den Cluster auszuführen. Führen Sie dazu die folgenden Schritte aus:
 - a. Öffnen Sie die IAM-Konsole unter <https://console.aws.amazon.com/iam/> und melden Sie sich als Administrator Benutzer an.
 - b. Wählen Sie im Navigationsbereich Benutzer aus und fügen Sie dem Benutzer `datalake_user` die folgenden verwalteten Richtlinien hinzu.
 - `AmazonRedshiftQueryEditor`
 - `AmazonRedshiftReadOnlyAccess`
11. Melden Sie sich von der Amazon Redshift Redshift-Konsole ab und melden Sie sich erneut als Benutzer `datalake_user` an.

- Wählen Sie in der linken vertikalen Werkzeugleiste das EDITOR-Symbol, um den Abfrage-Editor zu öffnen und eine Verbindung zum Cluster herzustellen. Wenn das Dialogfeld Mit Datenbank Connect angezeigt wird, wählen Sie den Clusternamen `redshift-lakeformation-demo` und geben Sie den Datenbanknamen `dev`, den Benutzernamen und das Passwort ein `awsuser`, das Sie erstellt haben. Wählen Sie dann Connect to database (Verbindung zur Datenbank herstellen) aus.

 Note

Wenn Sie nicht zur Eingabe von Verbindungsparametern aufgefordert werden und bereits ein anderer Cluster im Abfrage-Editor ausgewählt ist, wählen Sie Verbindung ändern, um das Dialogfeld Mit Datenbank Connect zu öffnen.

- Geben Sie im Textfeld Neue Abfrage 1 die folgende Anweisung ein und führen Sie sie aus, um die Datenbank `lakeformation_tutorial` in Lake Formation dem Amazon Redshift Redshift-Schemanamen zuzuordnen: `redshift_jdbc`

 Important

`<account-id>` Ersetzen Sie es durch eine gültige AWS Kontonummer und `<region>` einen gültigen AWS Regionsnamen (z. B. `us-east-1`).

```
create external schema if not exists redshift_jdbc from DATA CATALOG
  database 'lakeformation_tutorial' iam_role 'arn:aws:iam::<account-id>:role/
  RedshiftLakeFormationRole' region '<region>';
```

- Wählen Sie in der Schemaliste unter Schema auswählen die Option `redshift_jdbc` aus.

Die Tabellenliste wird aufgefüllt. Der Abfrage-Editor zeigt nur die Tabellen an, für die Ihnen Lake Formation Data Lake-Berechtigungen erteilt wurden.

- Wählen Sie im Popupmenü neben einem Tabellennamen die Option Datenvorschau aus.

Amazon Redshift gibt die ersten 10 Zeilen zurück.

Sie können jetzt Abfragen für die Tabellen und Spalten ausführen, für die Sie Berechtigungen haben.

Schritt 13: Erteilen oder Widerrufen Lake Formation Formation-Berechtigungen mithilfe von Amazon Redshift Spectrum

Amazon Redshift unterstützt die Möglichkeit, Lake Formation Formation-Berechtigungen für Datenbanken und Tabellen mithilfe modifizierter SQL-Anweisungen zu gewähren und zu widerrufen. Diese Aussagen ähneln den bestehenden Amazon Redshift Redshift-Aussagen. Weitere Informationen finden Sie unter [GRANT](#) und [REVOKE](#) im Amazon Redshift Database Developer Guide.

Berechtigungen für Open-Table-Speicherformate in Lake Formation einrichten

AWS Lake Formation unterstützt die Verwaltung von Zugriffsberechtigungen für Open Table Formats (OTFs) wie [Apache Iceberg](#), [Apache Hudi](#) und [Linux](#) Foundation Delta Lake. In diesem Tutorial erfahren Sie, wie Sie Iceberg, Hudi und Delta Lake mit [Symlink-Manifesttabellen](#) in der AWS Glue Data Catalog Verwendung erstellen AWS Glue, detaillierte Berechtigungen mit Lake Formation einrichten und Daten mit Amazon Athena abfragen.

Note

AWS Analytics-Services unterstützen nicht alle Transaktionstabellenformate. Weitere Informationen finden Sie unter [Zusammenarbeit mit anderen AWS Diensten](#). In diesem Tutorial wird das manuelle Erstellen einer neuen Datenbank und einer Tabelle im Datenkatalog ausschließlich mithilfe von AWS Glue Jobs behandelt.

Dieses Tutorial enthält eine AWS CloudFormation Vorlage für die schnelle Einrichtung. Sie können es überprüfen und an Ihre Bedürfnisse anpassen.

Themen

- [Zielgruppe](#)
- [Voraussetzungen](#)
- [Schritt 1: Stellen Sie Ihre Ressourcen bereit](#)
- [Schritt 2: Richten Sie Berechtigungen für eine Iceberg-Tabelle ein](#)
- [Schritt 3: Richten Sie Berechtigungen für eine Hudi-Tabelle ein](#)
- [Schritt 4: Richten Sie Berechtigungen für eine Delta Lake-Tabelle ein](#)

- [Schritt 5: Ressourcen bereinigen AWS](#)

Zielgruppe

Dieses Tutorial richtet sich an IAM-Administratoren, Data Lake-Administratoren und Geschäftsanalysten. In der folgenden Tabelle sind die Rollen aufgeführt, die in diesem Tutorial zum Erstellen einer gesteuerten Tabelle mit Lake Formation verwendet wurden.

Rolle	Description
IAM-Administrator	Ein Benutzer, der IAM-Benutzer und -Rollen sowie Amazon S3 S3-Buckets erstellen kann. Hat die AdministratorAccess AWS verwaltete Richtlinie.
Data Lake-Administrator	Ein Benutzer, der auf den Datenkatalog zugreifen, Datenbanken erstellen und anderen Benutzern Lake Formation Berechtigungen gewähren kann. Hat weniger IAM-Berechtigungen als der IAM-Administrator, reicht aber aus, um den Data Lake zu verwalten.
Geschäftsanalyst	Ein Benutzer, der Abfragen für den Data Lake ausführen kann. Hat Berechtigungen zum Ausführen von Abfragen.

Voraussetzungen

Bevor Sie mit diesem Tutorial beginnen, benötigen Sie eine AWS-Konto, mit der Sie sich als Benutzer mit den richtigen Berechtigungen anmelden können. Weitere Informationen erhalten Sie unter [Melde dich an für ein AWS-Konto](#) und [Erstellen eines Benutzers mit Administratorzugriff](#).

In der Anleitung wird davon ausgegangen, dass Sie mit IAM-Rollen und -Richtlinien vertraut sind. Informationen zu IAM finden Sie im [IAM-Benutzerhandbuch](#).

Sie müssen die folgenden AWS Ressourcen einrichten, um dieses Tutorial abschließen zu können:

- Data Lake-Administratorbenutzer
- Data Lake-Einstellungen für Lake Formation
- Amazon Athena Athena-Engine Version 3

Um einen Data Lake-Administrator zu erstellen

1. Melden Sie sich <https://console.aws.amazon.com/lakeformation/> als Administratorbenutzer bei der Lake Formation Formation-Konsole an. Für dieses Tutorial werden Sie Ressourcen in der Region USA Ost (Nord-Virginia) erstellen.
2. Wählen Sie in der Lake Formation Formation-Konsole im Navigationsbereich unter Berechtigungen die Option Administrative Rollen und Aufgaben aus.
3. Wählen Sie unter Data Lake-Administratoren die Option Administratoren auswählen aus.
4. Wählen Sie im Popup-Fenster Data Lake-Administratoren verwalten unter IAM-Benutzer und -Rollen die Option IAM-Admin-Benutzer aus.
5. Wählen Sie Speichern.

Um die Data Lake-Einstellungen zu aktivieren

1. Öffnen Sie die Lake Formation Formation-Konsole unter <https://console.aws.amazon.com/lakeformation/>. Wählen Sie im Navigationsbereich unter Datenkatalog die Option Einstellungen aus. Deaktivieren Sie Folgendes:
 - Verwenden Sie nur die IAM-Zugriffskontrolle für neue Datenbanken.
 - Verwenden Sie nur die IAM-Zugriffskontrolle für neue Tabellen in neuen Datenbanken.
2. Wählen Sie unter Einstellungen für kontenübergreifende Versionen Version Version 3 als kontoübergreifende Version aus.
3. Wählen Sie Speichern.

Um die Amazon Athena Athena-Engine auf Version 3 zu aktualisieren

1. Öffnen Sie die Athena-Konsole unter <https://console.aws.amazon.com/athena/>
2. Wählen Sie die Arbeitsgruppe und anschließend die primäre Arbeitsgruppe aus.
3. Stellen Sie sicher, dass für die Arbeitsgruppe mindestens Version 3 installiert ist. Ist dies nicht der Fall, bearbeiten Sie die Arbeitsgruppe, wählen Sie Manuell für die Upgrade-Abfrage-Engine und wählen Sie Version 3.

4. Wählen Sie Änderungen speichern aus.

Schritt 1: Stellen Sie Ihre Ressourcen bereit

In diesem Abschnitt erfahren Sie, wie Sie die AWS Ressourcen mithilfe einer CloudFormation Vorlage einrichten.

Um Ihre Ressourcen mithilfe einer CloudFormation Vorlage zu erstellen

1. Melden Sie sich bei der AWS CloudFormation Konsole unter <https://console.aws.amazon.com/cloudformation> als IAM-Administrator in der Region USA Ost (Nord-Virginia) an.
2. [Wählen Sie Launch Stack.](#)
3. Wählen Sie auf dem Bildschirm „Stack erstellen“ die Option „Weiter“.
4. Geben Sie einen Stack-Namen ein.
5. Wählen Sie Weiter aus.
6. Wählen Sie auf der nächsten Seite Weiter.
7. Überprüfen Sie die Details auf der letzten Seite und wählen Sie Ich bestätige, dass AWS CloudFormation möglicherweise IAM-Ressourcen erstellt werden.
8. Wählen Sie Erstellen aus.

Die Erstellung des Stacks kann bis zu zwei Minuten dauern.

Durch das Starten des Cloud-Formation-Stacks werden die folgenden Ressourcen erstellt:

- If-otf-datalake-123456789012 — Amazon S3 S3-Bucket zum Speichern von Daten

Note

Die Konto-ID, die an den Amazon S3 S3-Bucket-Namen angehängt wird, wird durch Ihre Konto-ID ersetzt.

- If-otf-tutorial-123456789012 — Amazon S3 S3-Bucket zum Speichern von Abfrageergebnissen und Jobskripten AWS Glue
- AWS Glue Ificebergdb — Eisberg-Datenbank
- Ifhudidb — AWS Glue Hudi-Datenbank
- Ifdeltadb — AWS Glue Delta-Datenbank

- `native-iceberg-create` — AWS Glue Job, der eine Eisberg-Tabelle im Datenkatalog erstellt
- `native-hudi-create` — AWS Glue Job, der eine Hudi-Tabelle im Datenkatalog erstellt
- `native-delta-create` — AWS Glue Job, der eine Delta-Tabelle im Datenkatalog erstellt
- `LF-OTF-GlueServiceRole` — IAM-Rolle, an die Sie übergeben, AWS Glue um die Jobs auszuführen. Dieser Rolle sind die erforderlichen Richtlinien für den Zugriff auf Ressourcen wie Data Catalog, Amazon S3 S3-Bucket usw. zugeordnet.
- `LF-OTF-RegisterRole` — IAM-Rolle zur Registrierung des Amazon S3 S3-Standorts bei Lake Formation. Diese Rolle wurde mit `LF-Data-Lake-Storage-Policy` der Rolle verknüpft.
- `lf-consumer-analystuser` — IAM-Benutzer zur Abfrage der Daten mit Athena
- `lf-consumer-analystuser-credentials` — Passwort für den Data Analyst-Benutzer, gespeichert in AWS Secrets Manager

Nachdem die Stack-Erstellung abgeschlossen ist, navigieren Sie zur Registerkarte „Ausgabe“ und notieren Sie sich die Werte für:

- `AthenaQueryResultLocation` — Amazon S3 S3-Standort für die Athena-Abfrageausgabe
- `BusinessAnalystUserCredentials` — Passwort für den Data Analyst-Benutzer

Um den Passwortwert abzurufen:

1. Wählen Sie den `lf-consumer-analystuser-credentials` Wert aus, indem Sie zur Secrets Manager Manager-Konsole navigieren.
2. Wählen Sie im Bereich Secret value (Secret-Wert) die Option Retrieve secret value (Secret-Wert abrufen).
3. Notieren Sie sich den geheimen Wert für das Passwort.

Schritt 2: Richten Sie Berechtigungen für eine Iceberg-Tabelle ein

In diesem Abschnitt erfahren Sie, wie Sie eine Iceberg-Tabelle in Amazon Athena erstellen AWS Glue Data Catalog, Datenberechtigungen einrichten und Daten mit Amazon Athena abfragen. AWS Lake Formation

So erstellen Sie eine Iceberg-Tabelle

In diesem Schritt führen Sie einen AWS Glue Job aus, der eine Iceberg-Transaktionstabelle im Datenkatalog erstellt.

1. Öffnen Sie die AWS Glue Konsole <https://console.aws.amazon.com/glue/> in der Region USA Ost (Nord-Virginia) als Data Lake-Administratorbenutzer.
2. Wählen Sie im linken Navigationsbereich Jobs aus.
3. Wählen Sie `native-iceberg-create`.

The screenshot shows the AWS Glue console interface. The top section is titled 'Create job' with an 'Info' link and a 'Create' button. It offers six options for creating a job: 'Visual with a source and target' (selected), 'Visual with a blank canvas', 'Spark script editor', 'Python Shell script editor', 'Jupyter Notebook', and 'Ray script editor' (marked 'New'). Below these options, the 'Source' and 'Target' are both set to 'Amazon S3'. The 'Source' is described as 'JSON, CSV, or Parquet files stored in S3.' and the 'Target' as 'S3 bucket by specifying a bucket path as the data target.'

The bottom section is titled 'Your jobs (24)' with an 'Info' link. It includes a search bar and a table of jobs. The 'native-iceberg-create' job is selected. An 'Actions' menu is open, showing options: 'Edit job', 'Clone job', 'Schedule job', 'Delete job(s)', and 'Reset job bookmark'.

	Job name	Type	Last modified	
☐	native-delta-create	Glue ETL	2/24/2023, 9:22:31 AM	
☒	native-iceberg-create	Glue ETL	2/24/2023, 9:22:31 AM	3.0
☐	native-hudi-create	Glue ETL	2/24/2023, 9:22:30 AM	3.0

4. Wählen Sie unter Aktionen die Option Job bearbeiten aus.
5. Erweitern Sie unter Jobdetails die Option Erweiterte Eigenschaften und aktivieren Sie das Kästchen neben Als Hive-Metastore verwenden AWS Glue Data Catalog , um die Tabellenmetadaten in der hinzuzufügen. AWS Glue Data Catalog Dies wird AWS Glue Data Catalog als Metastore für die im Job verwendeten Datenkatalogressourcen angegeben und ermöglicht, dass Lake Formation Formation-Berechtigungen später auf die Katalogressourcen angewendet werden.
6. Wählen Sie Speichern.
7. Klicken Sie auf Ausführen. Sie können den Status des Jobs anzeigen, während er ausgeführt wird.

Weitere Informationen zu AWS Glue Jobs finden Sie im AWS Glue Developer Guide unter [Arbeiten mit Jobs auf der AWS Glue Konsole](#).

Dieser Job erstellt eine `product` in der `lficebergdb` Datenbank benannte Iceberg-Tabelle. Überprüfen Sie die Produkttabelle in der Lake Formation Formation-Konsole.

Um den Datenstandort bei Lake Formation zu registrieren

Als Nächstes registrieren Sie den Amazon S3 S3-Pfad als Standort Ihres Data Lakes.

1. Öffnen Sie die Lake Formation Formation-Konsole unter <https://console.aws.amazon.com/lakeformation/> als Data Lake-Administratorbenutzer.
2. Wählen Sie im Navigationsbereich unter Registrieren und aufnehmen die Option Datenspeicherort aus.
3. Wählen Sie oben rechts in der Konsole die Option Speicherort registrieren aus.
4. Geben Sie auf der Seite Speicherort registrieren Folgendes ein:
 - Amazon S3 S3-Pfad — Wählen Sie Durchsuchen und wählen Sie aus `lf-otf-datalake-123456789012`. Klicken Sie auf den Rechtspfeil (>) neben dem Amazon S3 S3-Stammverzeichnis, um zum `s3/buckets/lf-otf-datalake-123456789012/transactionaldata/native-iceberg` Speicherort zu navigieren.
 - IAM-Rolle — Wählen Sie `LF-OTF-RegisterRole` als IAM-Rolle aus.
 - Wählen Sie Standort registrieren.

Register location

Amazon S3 location

Register an Amazon S3 path as the storage location for your data lake.

Amazon S3 path

Choose an Amazon S3 path for your data lake.

s3://lf-otf-datalake- /transactionaldata/native-iceberg

Browse

Review location permissions - strongly recommended

Registering the selected location may result in your users gaining access to data already at that location. Before registering a location, we recommend that you review existing location permissions on resources in that location.

Review location permissions

IAM role

To add or update data, Lake Formation needs read/write access to the chosen Amazon S3 path. Choose a role that you know has permission to do this, or choose the **AWSServiceRoleForLakeFormationDataAccess** service-linked role. When you register the first Amazon S3 path, the service-linked role and a new inline policy are created on your behalf. Lake Formation adds the first path to the inline policy and attaches it to the service-linked role. When you register subsequent paths, Lake Formation adds the path to the existing policy.

LF-OTF-GlueServiceRole ▼

☐ **Enable Catalog Federation**

Lake Formation will only assume a role to access a registered location when accessing a table under a federated database

Cancel

Register location

Weitere Informationen zur Registrierung eines Datenstandorts bei Lake Formation finden Sie unter [Hinzufügen eines Amazon S3 S3-Standorts zu Ihrem Data Lake](#).

Um Lake Formation Formation-Berechtigungen für die Iceberg-Tabelle zu erteilen

In diesem Schritt erteilen wir dem Business Analyst-Benutzer Data Lake-Berechtigungen.

1. Wählen Sie unter Data Lake-Berechtigungen die Option Grant aus.
2. Wählen Sie auf dem Bildschirm Datenberechtigungen gewähren die Option IAM-Benutzer und -Rollen aus.
3. Wählen Sie lf-consumer-analystuser aus dem Drop-down-Menü aus.

Principals

☒ **IAM users and roles**
Users or roles from this AWS account.

☐ **SAML users and groups**
SAML users and group or QuickSight ARNs.

☐ **External accounts**
AWS account, AWS organization or IAM principal outside of this account

IAM users and roles

Add one or more IAM users or roles.

Choose IAM principals to add ▼

lf-consumer-analystuser X
User

4. Wählen Sie Benannte Datenkatalogressource aus.
5. Wählen Sie für Datenbankenlficebergdb.
6. Wählen Sie für Tabellenproduct.

LF-Tags or catalog resources

☐ Resources matched by LF-Tags (recommended)
Manage permissions indirectly for resources or data matched by a specific set of LF-Tags.

☒ Named data catalog resources
Manager permissions for specific databases or tables, in addition to fine-grained data access.

Databases

Select one or more databases.

Choose databases ▼

Load more

lficebergdb ✕

Tables - optional

Select one or more tables.

Choose tables ▼

Load more

product ✕

Data filters - optional

Select one or more data filters.

Choose data filters ▼

Load more

Create new

[Manage data filters](#) 

7. Als Nächstes können Sie spaltenbasierten Zugriff gewähren, indem Sie Spalten angeben.
 - a. Wählen Sie unter Tabellenberechtigungen die Option Auswählen aus.
 - b. Wählen Sie unter Datenberechtigungen die Option Spaltenbasierter Zugriff und dann Spalten einbeziehen aus.
 - c. Wählen Sie product_nameprice, und category Spalten aus.
 - d. Wählen Sie Grant (Erteilen).

Table permissions

Table permissions
Choose specific access permissions to grant.

☒ Select

☐ Insert

☐ Delete

☐ Describe

☐ Alter

☐ Drop

☐ Super
This permission is the union of all the individual permissions to the left, and supersedes them.

Grantable permissions
Choose the permission that may be granted to others.

☐ Select

☐ Insert

☐ Delete

☐ Describe

☐ Alter

☐ Drop

☐ Super
This permission allows the principal to grant any of the permissions to the left, and supersedes those grantable permissions.

Data permissions

☐ All data access
Grant access to all data without any restrictions.

☒ Column-based access
Grant data access to specific columns only.

Choose permission filter
Choose whether to include or exclude columns.

☒ Include columns
Grant permissions to access specific columns.

☐ Exclude columns
Grant permissions to access all but specific columns.

Select columns

Choose one or more columns ▼

product_name
string

price
bigint

category
string

CancelGrant

Um die Iceberg-Tabelle mit Athena abzufragen

Jetzt können Sie mit der Abfrage der Iceberg-Tabelle beginnen, die Sie mit Athena erstellt haben. Wenn Sie zum ersten Mal Abfragen in Athena ausführen, müssen Sie einen Speicherort für Abfrageergebnisse konfigurieren. Weitere Informationen finden Sie unter [Angaben eines Speicherorts für Abfrageergebnisse](#).

1. Melden Sie sich als Data Lake-Administratorbenutzer ab und melden Sie sich mit dem zuvor `lf-consumer-analystuser` in der CloudFormation Ausgabe angegebenen Kennwort als Benutzer in der Region USA Ost (Nord-Virginia) an.
2. Öffnen Sie die Athena-Konsole unter <https://console.aws.amazon.com/athena/>.
3. Wählen Sie Einstellungen und anschließend Verwalten aus.
4. Geben Sie im Feld Speicherort des Abfrageergebnisses den Pfad zu dem Bucket ein, den Sie in CloudFormation Ausgaben erstellt haben. Kopieren Sie den Wert von **AthenaQueryResultLocation** (`s3://lf-otf-tutorial-123456789012/athena-results/`) und wählen Sie Speichern.
5. Führen Sie die folgende Abfrage aus, um eine Vorschau von 10 in der Iceberg-Tabelle gespeicherten Datensätzen anzuzeigen:

```
select * from lficebergdb.product limit 10;
```

Weitere Informationen zum Abfragen von Iceberg-Tabellen mit Athena finden Sie unter [Abfragen von Iceberg-Tabellen](#) im Amazon Athena Athena-Benutzerhandbuch.

Schritt 3: Richten Sie Berechtigungen für eine Hudi-Tabelle ein

In diesem Abschnitt erfahren Sie, wie Sie eine Hudi-Tabelle in Amazon Athena erstellen AWS Glue Data Catalog, Datenberechtigungen einrichten und Daten mit Amazon Athena abfragen. AWS Lake Formation

Um eine Hudi-Tabelle zu erstellen

In diesem Schritt führen Sie einen AWS Glue Job aus, der eine Hudi-Transaktionstabelle im Datenkatalog erstellt.

1. Melden Sie sich bei der AWS Glue Konsole <https://console.aws.amazon.com/glue/> in der Region USA Ost (Nord-Virginia) an
als Data Lake-Administratorbenutzer.
2. Wählen Sie im linken Navigationsbereich Jobs aus.
3. Wählen Sie `native-hudi-create`.
4. Wählen Sie unter Aktionen die Option Job bearbeiten aus.

5. Erweitern Sie unter Jobdetails die Option Erweiterte Eigenschaften und aktivieren Sie das Kästchen neben Als Hive-Metastore verwenden AWS Glue Data Catalog , um die Tabellenmetadaten in der hinzuzufügen. AWS Glue Data Catalog Dies wird AWS Glue Data Catalog als Metastore für die im Job verwendeten Datenkatalogressourcen angegeben und ermöglicht, dass Lake Formation Formation-Berechtigungen später auf die Katalogressourcen angewendet werden.
6. Wählen Sie Speichern.
7. Klicken Sie auf Ausführen. Sie können den Status des Jobs anzeigen, während er ausgeführt wird.

Weitere Informationen zu AWS Glue Jobs finden Sie im AWS Glue Developer Guide unter [Arbeiten mit Jobs auf der AWS Glue Konsole](#).

Dieser Job erstellt eine Hudi-Tabelle (cow) in der Datenbank:lfhudidb. Überprüfen Sie die product Tabelle in der Lake Formation Formation-Konsole.

Um den Datenstandort bei Lake Formation zu registrieren

Als Nächstes registrieren Sie einen Amazon S3 S3-Pfad als Stammverzeichnis Ihres Data Lakes.

1. Melden Sie sich <https://console.aws.amazon.com/lakeformation/> als Data Lake-Administratorbenutzer bei der Lake Formation Formation-Konsole an.
2. Wählen Sie im Navigationsbereich unter Registrieren und aufnehmen die Option Datenspeicherort aus.
3. Wählen Sie oben rechts in der Konsole die Option Speicherort registrieren aus.
4. Geben Sie auf der Seite Speicherort registrieren Folgendes ein:
 - Amazon S3 S3-Pfad — Wählen Sie Durchsuchen und wählen Sie aus lf-otf-datalake-123456789012. Klicken Sie auf den Rechtspfeil (>) neben dem Amazon S3 S3-Stammverzeichnis, um zum s3/buckets/lf-otf-datalake-123456789012/transactionaldata/native-hudi Speicherort zu navigieren.
 - IAM-Rolle — Wählen Sie LF-OTF-RegisterRole als IAM-Rolle aus.
 - Wählen Sie Standort registrieren.

Um Data Lake-Berechtigungen für die Hudi-Tabelle zu gewähren

In diesem Schritt gewähren wir dem Business Analyst-Benutzer Data-Lake-Berechtigungen.

1. Wählen Sie unter Data Lake-Berechtigungen die Option Grant aus.
2. Wählen Sie auf dem Bildschirm Datenberechtigungen gewähren die Option IAM-Benutzer und -Rollen aus.
3. `lf-consumer-analystuser` aus dem Drop-down-Menü.
4. Wählen Sie Benannte Datenkatalogressource aus.
5. Wählen Sie für Datenbanken `lfhudidb`.
6. Wählen Sie für Tabellen `product`.
7. Als Nächstes können Sie spaltenbasierten Zugriff gewähren, indem Sie Spalten angeben.
 - a. Wählen Sie unter Tabellenberechtigungen die Option Auswählen aus.
 - b. Wählen Sie unter Datenberechtigungen die Option Spaltenbasierter Zugriff und dann Spalten einbeziehen aus.
 - c. Wählen Sie `product_nameprice`, und `category` Spalten aus.
 - d. Wählen Sie Grant (Erteilen).

Um die Hudi-Tabelle mit Athena abzufragen

Beginnen Sie nun mit der Abfrage der Hudi-Tabelle, die Sie mit Athena erstellt haben.

Wenn Sie zum ersten Mal Abfragen in Athena ausführen, müssen Sie einen Speicherort für Abfrageergebnisse konfigurieren. Weitere Informationen finden Sie unter [Angaben eines Speicherorts für Abfrageergebnisse](#).

1. Melden Sie sich als Data Lake-Administratorbenutzer ab und melden Sie sich mit dem zuvor `lf-consumer-analystuser` in der CloudFormation Ausgabe angegebenen Kennwort als Benutzer in der Region USA Ost (Nord-Virginia) an.
2. Öffnen Sie die Athena-Konsole unter <https://console.aws.amazon.com/athena/>.
3. Wählen Sie Einstellungen und anschließend Verwalten aus.
4. Geben Sie im Feld Speicherort des Abfrageergebnisses den Pfad zu dem Bucket ein, den Sie in CloudFormation Ausgaben erstellt haben. Kopieren Sie den Wert von **AthenaQueryResultLocation** (`s3://lf-otf-tutorial-123456789012/athena-results/`) und speichern Sie.
5. Führen Sie die folgende Abfrage aus, um eine Vorschau von 10 in der Hudi-Tabelle gespeicherten Datensätzen anzuzeigen:

```
select * from lfhudidb.product limit 10;
```

Weitere Informationen zum Abfragen von Hudi-Tabellen finden Sie im Abschnitt [Abfragen von Hudi-Tabellen](#) im Amazon Athena Athena-Benutzerhandbuch.

Schritt 4: Richten Sie Berechtigungen für eine Delta Lake-Tabelle ein

In diesem Abschnitt erfahren Sie, wie Sie eine Delta Lake-Tabelle mit einer Symmlink-Manifestdatei in der erstellen AWS Glue Data Catalog, Datenberechtigungen in Amazon Athena einrichten AWS Lake Formation und Daten mit Amazon Athena abfragen.

So erstellen Sie eine Delta Lake-Tabelle

In diesem Schritt führen Sie einen AWS Glue Job aus, der eine Delta Lake-Transaktionstabelle im Datenkatalog erstellt.

1. Melden Sie sich bei der AWS Glue Konsole <https://console.aws.amazon.com/glue/> in der Region USA Ost (Nord-Virginia) an
als Data Lake-Administratorbenutzer.
2. Wählen Sie im linken Navigationsbereich Jobs aus.
3. Wählen Sie `native-delta-create`.
4. Wählen Sie unter Aktionen die Option Job bearbeiten aus.
5. Erweitern Sie unter Jobdetails die Option Erweiterte Eigenschaften und aktivieren Sie das Kästchen neben Als Hive-Metastore verwenden AWS Glue Data Catalog , um die Tabellenmetadaten in der hinzuzufügen. AWS Glue Data Catalog Dies wird AWS Glue Data Catalog als Metastore für die im Job verwendeten Datenkatalogressourcen angegeben und ermöglicht, dass Lake Formation Formation-Berechtigungen später auf die Katalogressourcen angewendet werden.
6. Wählen Sie Speichern.
7. Wählen Sie unter Aktionen die Option Ausführen aus.

Dieser Job erstellt eine Delta Lake-Tabelle mit dem Namen `product` in der `lfdeltadb` Datenbank. Überprüfen Sie die `product` Tabelle in der Lake Formation Formation-Konsole.

Um den Datenstandort bei Lake Formation zu registrieren

Als Nächstes registrieren Sie den Amazon S3 S3-Pfad als Stammverzeichnis Ihres Data Lakes.

1. Öffnen Sie die Lake Formation Konsole <https://console.aws.amazon.com/lakeformation/> beim Data Lake-Administratorbenutzer.
2. Wählen Sie im Navigationsbereich unter Registrieren und aufnehmen die Option Datenstandort aus.
3. Wählen Sie oben rechts in der Konsole die Option Speicherort registrieren aus.
4. Geben Sie auf der Seite Speicherort registrieren Folgendes ein:
 - Amazon S3 S3-Pfad — Wählen Sie Durchsuchen und wählen Sie aus `lf-otf-datalake-123456789012`. Klicken Sie auf den Rechtspfeil (>) neben dem Amazon S3 S3-Stammverzeichnis, um zum `s3/buckets/lf-otf-datalake-123456789012/transactionaldata/native-delta` Speicherort zu navigieren.
 - IAM-Rolle — Wählen Sie `LF-OTF-RegisterRole` als IAM-Rolle aus.
 - Wählen Sie Standort registrieren.

Um Data Lake-Berechtigungen für die Delta Lake-Tabelle zu erteilen

In diesem Schritt erteilen wir dem Business Analyst-Benutzer Data-Lake-Berechtigungen.

1. Wählen Sie unter Data Lake-Berechtigungen die Option Grant aus.
2. Wählen Sie auf dem Bildschirm Datenberechtigungen gewähren die Option IAM-Benutzer und -Rollen aus.
3. `lf-consumer-analystuser` aus dem Drop-down-Menü.
4. Wählen Sie Benannte Datenkatalogressource aus.
5. Wählen Sie für Datenbanken `lfdeltadb`.
6. Wählen Sie für Tabellen `product`.
7. Als Nächstes können Sie spaltenbasierten Zugriff gewähren, indem Sie Spalten angeben.
 - a. Wählen Sie unter Tabellenberechtigungen die Option Auswählen aus.
 - b. Wählen Sie unter Datenberechtigungen die Option Spaltenbasierter Zugriff und dann Spalten einbeziehen aus.
 - c. Wählen Sie `product_nameprice`, und `category` Spalten aus.

- d. Wählen Sie Grant (Erteilen).

Um die Delta Lake-Tabelle mit Athena abzufragen

Beginnen Sie nun mit der Abfrage der Delta Lake-Tabelle, die Sie mit Athena erstellt haben.

Wenn Sie zum ersten Mal Abfragen in Athena ausführen, müssen Sie einen Speicherort für Abfrageergebnisse konfigurieren. Weitere Informationen finden Sie unter [Angaben eines Speicherorts für Abfrageergebnisse](#).

1. Melden Sie sich als Data Lake-Administratorbenutzer ab und melden Sie sich mit dem zuvor BusinessAnalystUser in der CloudFormation Ausgabe angegebenen Kennwort in der Region USA Ost (Nord-Virginia) an.
2. Öffnen Sie die Athena-Konsole unter <https://console.aws.amazon.com/athena/>.
3. Wählen Sie Einstellungen und anschließend Verwalten aus.
4. Geben Sie im Feld Speicherort des Abfrageergebnisses den Pfad zu dem Bucket ein, den Sie in CloudFormation Ausgaben erstellt haben. Kopieren Sie den Wert von **AthenaQueryResultLocation** (s3://lf-otf-tutorial-123456789012/athena-results/) und speichern Sie.
5. Führen Sie die folgende Abfrage aus, um eine Vorschau von 10 in der Delta Lake-Tabelle gespeicherten Datensätzen anzuzeigen:

```
select * from lfdeltadb.product limit 10;
```

Weitere Informationen zur Abfrage von Delta Lake-Tabellen finden Sie im Abschnitt [Abfragen von Delta Lake-Tabellen](#) im Amazon Athena Athena-Benutzerhandbuch.

Schritt 5: Ressourcen bereinigen AWS

So bereinigen Sie Ressourcen

Um zu verhindern, dass Ihnen unerwünschte Kosten entstehen AWS-Konto, löschen Sie die AWS Ressourcen, die Sie für dieses Tutorial verwendet haben.

1. Melden Sie sich als CloudFormation IAM-Administrator bei der Konsole unter <https://console.aws.amazon.com/cloudformation> an.

2. [Löschen Sie den Cloud Formation Stack](#). Die von Ihnen erstellten Tabellen werden automatisch mit dem Stack gelöscht.

Verwaltung eines Data Lakes mithilfe der Tag-basierten Zugriffskontrolle von Lake Formation

Tausende von Kunden bauen darauf Data Lakes im Petabyte-Bereich auf. AWS Viele dieser Kunden nutzen die Möglichkeit AWS Lake Formation , ihre Data Lakes einfach aufzubauen und unternehmensweit gemeinsam zu nutzen. Angesichts der steigenden Anzahl von Tabellen und Benutzern suchen Data Stewards und Administratoren nach Möglichkeiten, Berechtigungen für Data Lakes einfach und skalierbar zu verwalten. Lake Formation Tag-Based Access Control (LF-TBAC) löst dieses Problem, indem Data Stewards ermöglicht wird, LF-Tags (basierend auf ihrer Datenklassifizierung und Ontologie) zu erstellen, die dann an Ressourcen angehängt werden können.

LF-TBAC ist eine Autorisierungsstrategie, die Berechtigungen auf der Grundlage von Attributen definiert. In Lake Formation werden diese Attribute als LF-Tags bezeichnet. Sie können LF-Tags an Datenkatalogressourcen und Lake Formation-Prinzipale anhängen. Data Lake-Administratoren können mithilfe von LF-Tags Berechtigungen für Lake Formation-Prinzipale zuweisen und widerrufen. Weitere Informationen dazu finden Sie unter [Tag-basierte Zugangskontrolle von Lake Formation](#)

In diesem Tutorial wird gezeigt, wie Sie mithilfe eines AWS öffentlichen Datensatzes eine auf Lake Formation-Tags basierende Zugriffskontrollrichtlinie erstellen. Darüber hinaus wird gezeigt, wie Tabellen, Datenbanken und Spalten abgefragt werden, denen auf Lake Formation-Tags basierende Zugriffsrichtlinien zugeordnet sind.

Sie können LF-TBAC für die folgenden Anwendungsfälle verwenden:

- Sie haben eine große Anzahl von Tabellen und Prinzipalen, auf die der Data Lake-Administrator Zugriff gewähren muss
- Sie möchten Ihre Daten auf der Grundlage einer Ontologie klassifizieren und auf der Grundlage der Klassifizierung Berechtigungen gewähren
- Der Data Lake-Administrator möchte Berechtigungen dynamisch, also lose gekoppelt, zuweisen

Im Folgenden sind die allgemeinen Schritte zur Konfiguration von Berechtigungen mithilfe von LF-TBAC aufgeführt:

1. Der Data Steward definiert die Tag-Ontologie mit zwei LF-Tags: und. Confidential Sensitive Für Daten mit gelten strengere Confidential=True Zugriffskontrollen. Daten mit Sensitive=True erfordern eine spezifische Analyse durch den Analysten.
2. Der Data Steward weist dem Dateningenieur verschiedene Berechtigungsstufen zu, um Tabellen mit unterschiedlichen LF-Tags zu erstellen.
3. Der Dateningenieur erstellt zwei Datenbanken: und. tag_database col_tag_database Alle Tabellen in tag_database sind mit konfiguriert Confidential=True. Alle Tabellen in der col_tag_database sind mit konfiguriert Confidential=False. Einige Spalten der Tabelle in col_tag_database sind Sensitive=True für spezielle Analyseanforderungen mit gekennzeichnet.
4. Der Dateningenieur erteilt dem Analysten Leseberechtigungen für Tabellen mit bestimmten Ausdrucksbedingungen Confidential=True und Confidential=False, Sensitive=True.
5. Mit dieser Konfiguration kann sich der Datenanalyst darauf konzentrieren, Analysen mit den richtigen Daten durchzuführen.

Themen

- [Zielgruppe](#)
- [Voraussetzungen](#)
- [Schritt 1: Stellen Sie Ihre Ressourcen bereit](#)
- [Schritt 2: Registrieren Sie Ihren Datenstandort, erstellen Sie eine LF-Tag-Ontologie und gewähren Sie Berechtigungen](#)
- [Schritt 3: Lake Formation Formation-Datenbanken erstellen](#)
- [Schritt 4: Erteilen Sie Tabellenberechtigungen](#)
- [Schritt 5: Führen Sie eine Abfrage in Amazon Athena aus, um die Berechtigungen zu überprüfen](#)
- [Schritt 6: Ressourcen AWS bereinigen](#)

Zielgruppe

Dieses Tutorial richtet sich an Datenverwalter, Dateningenieure und Datenanalysten. Wenn es um die Verwaltung AWS Glue Data Catalog und Verwaltung von Berechtigungen in Lake Formation geht, haben die Data Stewards innerhalb der produzierenden Konten die funktionale Verantwortung, basierend auf den Funktionen, die sie unterstützen, und können verschiedenen Verbrauchern, externen Organisationen und Konten Zugriff gewähren.

In der folgenden Tabelle sind die Rollen aufgeführt, die in diesem Tutorial verwendet werden:

Rolle	Description
Datenverwalter (Administrator)	Der <code>lf-data-steward</code> Benutzer hat folgenden Zugriff: • Lesezugriff auf alle Ressourcen im Datenkatalog • Kann LF-Tags erstellen und sie der Rolle des Dateningenieurs zuordnen, um anderen Prinzipalen Berechtigungen zu erteilen
Dateningenieur	<code>lf-data-engineer</code> Der Benutzer hat folgenden Zugriff: • Vollständiger Lese-, Schreib- und Aktualisierungszugriff auf alle Ressourcen im Datenkatalog • Berechtigungen zum Speicherort von Daten im Data Lake • Kann LF-Tags zuordnen und eine Verbindung zum Datenkatalog herstellen • Kann LF-Tags an Ressourcen anhängen, was den Zugriff auf Prinzipale auf der Grundlage von Richtlinien ermöglicht, die von Data Stewards erstellt wurden
Datenanalyst	Der <code>lf-data-analyst</code> Benutzer hat folgenden Zugriff: • Präziser Zugriff auf Ressourcen, die von Tag-basierten Zugriffsrichtlinien von Lake Formation gemeinsam genutzt werden

Voraussetzungen

Bevor Sie mit diesem Tutorial beginnen, benötigen Sie eine AWS-Konto , mit der Sie sich als Administratorbenutzer mit den richtigen Berechtigungen anmelden können. Weitere Informationen finden Sie unter [Erledigen Sie die Aufgaben zur AWS Erstkonfiguration](#).

In der Anleitung wird davon ausgegangen, dass Sie mit IAM vertraut sind. Informationen zu IAM finden Sie im [IAM-Benutzerhandbuch](#).

Schritt 1: Stellen Sie Ihre Ressourcen bereit

Dieses Tutorial enthält eine AWS CloudFormation Vorlage für eine schnelle Einrichtung. Sie können es überprüfen und an Ihre Bedürfnisse anpassen. Die Vorlage erstellt drei verschiedene Rollen (aufgeführt unter [Zielgruppe](#)), um diese Übung durchzuführen, und kopiert den nyc-taxi-data Datensatz in Ihren lokalen Amazon S3 S3-Bucket.

- Ein Amazon S3 S3-Bucket
- Die entsprechenden Lake Formation Formation-Einstellungen
- Die entsprechenden Amazon EC2 EC2-Ressourcen
- Drei IAM-Rollen mit Anmeldeinformationen

Erstellen Sie Ihre Ressourcen

1. Melden Sie sich bei der AWS CloudFormation Konsole unter <https://console.aws.amazon.com/cloudformation> in der Region USA Ost (Nord-Virginia) an.
2. Wählen Sie [Launch Stack](#).
3. Wählen Sie Weiter aus.
4. Geben Sie im Abschnitt Benutzerkonfiguration das Passwort für drei Rollen ein: DataStewardUserPassword, DataEngineerUserPassword und DataAnalystUserPassword.
5. Überprüfen Sie die Details auf der letzten Seite und wählen Sie Ich bestätige, dass AWS CloudFormation möglicherweise IAM-Ressourcen erstellt werden.
6. Wählen Sie Erstellen aus.

Die Erstellung des Stacks kann bis zu fünf Minuten dauern.

 Note

Nachdem Sie das Tutorial abgeschlossen haben, möchten Sie möglicherweise den Stack löschen, CloudFormation um zu vermeiden, dass weiterhin Gebühren anfallen. Stellen Sie sicher, dass die Ressourcen im Ereignisstatus für den Stack erfolgreich gelöscht wurden.

Schritt 2: Registrieren Sie Ihren Datenstandort, erstellen Sie eine LF-Tag-Ontologie und gewähren Sie Berechtigungen

In diesem Schritt definiert der Data Steward-Benutzer die Tag-Ontologie mit zwei LF-Tags: `Confidential` und `Sensitive` und gibt bestimmten IAM-Prinzipalen die Möglichkeit, neu erstellte LF-Tags an Ressourcen anzuhängen.

Registrieren Sie einen Datenstandort und definieren Sie die LF-Tag-Ontologie

1. Führen Sie den ersten Schritt als Data Steward-Benutzer (`lf-data-steward`) aus, um die Daten in Amazon S3 und den Datenkatalog in Lake Formation zu überprüfen.
 - a. Melden Sie sich bei der Lake Formation Konsole unter <https://console.aws.amazon.com/lakeformation/> als `lf-data-steward` mit dem Passwort an, das Sie bei der Bereitstellung des CloudFormation Stacks verwendet haben.
 - b. Wählen Sie im Navigationsbereich unter Berechtigungen die Option Administrative Rollen und Aufgaben aus.
 - c. Wählen Sie im Abschnitt Data Lake-Administratoren die Option Hinzufügen aus.
 - d. Wählen Sie auf der Seite Administrator hinzufügen für IAM-Benutzer und -Rollen den Benutzer `lf-data-steward` aus.
 - e. Wählen Sie Speichern, um es `lf-data-steward` als Lake Formation-Administrator hinzuzufügen.
2. Aktualisieren Sie als Nächstes die Datenkatalogeinstellungen, sodass anstelle der IAM-basierten Zugriffskontrolle die Lake Formation Berechtigung zur Steuerung der Katalogressourcen verwendet wird.
 - a. Wählen Sie im Navigationsbereich unter Verwaltung die Option Datenkatalogeinstellungen aus.
 - b. Deaktivieren Sie die Option Nur IAM-Zugriffskontrolle für neue Datenbanken verwenden.

- c. Deaktivieren Sie die Option Nur IAM-Zugriffskontrolle für neue Tabellen in neuen Datenbanken verwenden.
 - d. Klicken Sie auf Speichern.
3. Als Nächstes registrieren Sie den Datenstandort für den Data Lake.
 - a. Wählen Sie im Navigationsbereich unter Administration die Option Data Lake-Standorte aus.
 - b. Wählen Sie Standort registrieren aus.
 - c. Geben Sie auf der Seite Speicherort registrieren für den Amazon S3 S3-Pfad ein `s3://lf-tagbased-demo-Account-ID`.
 - d. Lassen Sie für die IAM-Rolle den Standardwert `AWSServiceRoleForLakeFormationDataAccess` unverändert.
 - e. Wählen Sie Lake Formation als Berechtigungsmodus.
 - f. Wählen Sie Standort registrieren.
4. Als Nächstes erstellen Sie die Ontologie, indem Sie ein LF-Tag definieren.
 - a. Wählen Sie im Navigationsbereich unter Berechtigungen die Option LF-Tags und Berechtigungen aus. .
 - b. Wählen Sie LF-Tag hinzufügen.
 - c. Geben Sie für Key (Schlüssel) `Confidential` ein.
 - d. Fügen Sie für Werte und hinzu `True`. `False`
 - e. Wählen Sie „LF-Tag hinzufügen“.
 - f. Wiederholen Sie die Schritte, um das LF-Tag `Sensitive` mit dem Wert zu erstellen. `True`

Sie haben alle erforderlichen LF-Tags für diese Übung erstellt.

Erteilen Sie IAM-Benutzern Berechtigungen

1. Geben Sie als Nächstes bestimmten IAM-Prinzipalen die Möglichkeit, neu erstellte LF-Tags an Ressourcen anzuhängen.
 - a. Wählen Sie im Navigationsbereich unter Berechtigungen die Option LF-Tags und Berechtigungen aus.
 - b. Wählen Sie im Abschnitt LF-Tag-Berechtigungen die Option Berechtigungen gewähren aus.
 - c. Wählen Sie als Berechtigungstyp die Option LF-Tag-Schlüsselwertpaar-Berechtigungen aus.

- d. Wählen Sie IAM-Benutzer und -Rollen aus.
 - e. Suchen Sie für IAM-Benutzer und -Rollen nach der Rolle und wählen Sie sie aus. `lf-data-engineer`
 - f. Fügen Sie im Abschnitt LF-Tags den Schlüssel `Confidential` mit den Werten `True` und `False` den mit dem key `Sensitive` Wert hinzu. `True`
 - g. Wählen Sie unter Berechtigungen die Option `Describe and Associate` für Berechtigungen und Gewährbare Berechtigungen aus.
 - h. Wählen Sie `Grant` (Erteilen).
2. Erteilen Sie als Nächstes Berechtigungen `lf-data-engineer` zum Erstellen von Datenbanken in unserem Datenkatalog und im zugrunde liegenden Amazon S3 S3-Bucket, der von erstellt wurde AWS CloudFormation.
- a. Wählen Sie im Navigationsbereich unter Administration die Option Administrative Rollen und Aufgaben aus.
 - b. Wählen Sie im Abschnitt Datenbankersteller die Option `Grant` aus.
 - c. Wählen Sie für IAM-Benutzer und -Rollen die `lf-data-engineer` Rolle aus.
 - d. Wählen Sie für Katalogberechtigungen die Option `Datenbank erstellen` aus.
 - e. Wählen Sie `Grant` (Erteilen).
3. Als Nächstes gewähren Sie dem `lf-data-engineer` Benutzer Berechtigungen für den Amazon S3 S3-Bucket(`s3://lf-tagbased-demo-Account-ID`).
- a. Wählen Sie im Navigationsbereich unter Berechtigungen die Option Datenspeicherorte aus.
 - b. Wählen Sie `Grant` (Erteilen).
 - c. Wählen Sie `Mein Konto` aus.
 - d. Wählen Sie für IAM-Benutzer und -Rollen die `lf-data-engineer` Rolle aus.
 - e. Geben Sie für Speicherorte den Amazon S3 S3-Bucket ein, der mit der CloudFormation Vorlage erstellt wurde(`s3://lf-tagbased-demo-Account-ID`).
 - f. Wählen Sie `Grant` (Erteilen).
4. Als Nächstes `lf-data-engineer` gewähren Sie erteilbare Berechtigungen für Ressourcen, die mit dem LF-Tag-Ausdruck verknüpft sind. `Confidential=True`
- a. Wählen Sie im Navigationsbereich unter Berechtigungen die Option `Data Lake-Berechtigungen` aus.
 - b. Wählen Sie `Grant` (Erteilen).

- c. Wählen Sie IAM-Benutzer und -Rollen aus.
 - d. Wählen Sie die Rolle `lf-data-engineer` aus.
 - e. Wählen Sie im Abschnitt LF-Tags oder Katalogressourcen die Option Ressourcen aus, denen LF-Tags zugeordnet sind.
 - f. Wählen Sie LF-Tag-Schlüssel-Wert-Paar hinzufügen.
 - g. Fügen Sie den Schlüssel `Confidential` mit den Werten hinzu. `True`
 - h. Wählen Sie im Abschnitt Datenbankberechtigungen für Datenbankberechtigungen und Grantable Permissions die Option Describe aus.
 - i. Wählen Sie im Abschnitt Tabellenberechtigungen sowohl für Tabellenberechtigungen als auch für Grantable-Berechtigungen die Optionen Beschreiben, Auswählen und Ändern aus.
 - j. Wählen Sie Grant (Erteilen).
5. Erteilen Sie als Nächstes `lf-data-engineer` erteilbare Berechtigungen für Ressourcen, die mit dem LF-Tag-Ausdruck verknüpft sind. `Confidential=False`
- a. Wählen Sie im Navigationsbereich unter Berechtigungen die Option Data Lake-Berechtigungen aus.
 - b. Wählen Sie Grant (Erteilen).
 - c. Wählen Sie IAM-Benutzer und -Rollen aus.
 - d. Wählen Sie die Rolle `lf-data-engineer` aus.
 - e. Wählen Sie Ressourcen aus, denen LF-Tags zugeordnet sind.
 - f. Wählen Sie LF-Tag hinzufügen.
 - g. Fügen Sie den Schlüssel `Confidential` mit dem Wert hinzu. `False`
 - h. Wählen Sie im Abschnitt Datenbankberechtigungen für Datenbankberechtigungen und Grantable Permissions die Option Describe aus.
 - i. Wählen Sie im Abschnitt Tabellen- und Spaltenberechtigungen nichts aus.
 - j. Wählen Sie Grant (Erteilen).
6. Als Nächstes `lf-data-engineer` gewähren wir erteilbare Berechtigungen für Ressourcen, die den LF-Tag-Schlüssel-Wert-Paaren und zugeordnet sind. `Confidential=False`
`Sensitive=True`
- a. Wählen Sie im Navigationsbereich unter Berechtigungen die Option Datenberechtigungen aus.

- c. Wählen Sie IAM-Benutzer und -Rollen aus.
- d. Wählen Sie die Rolle `lf-data-engineer` aus.
- e. Wählen Sie im Abschnitt LF-Tags oder Katalogressourcen die Option Ressourcen aus, denen LF-Tags zugeordnet sind.
- f. Wählen Sie LF-Tag hinzufügen.
- g. Fügen Sie den Schlüssel `Confidential` mit dem Wert hinzu. `False`
- h. Wählen Sie „LF-Tag-Schlüssel-Wert-Paar hinzufügen“.
- i. Fügen Sie den Schlüssel `Sensitive` mit dem Wert hinzu. `True`
- j. Wählen Sie im Abschnitt Datenbankberechtigungen für Datenbankberechtigungen und Grantable Permissions die Option Describe aus.
- k. Wählen Sie im Abschnitt Tabellenberechtigungen sowohl für Tabellenberechtigungen als auch für Grantable-Berechtigungen die Optionen Beschreiben, Auswählen und Ändern aus.
- l. Wählen Sie Grant (Erteilen).

Schritt 3: Lake Formation Formation-Datenbanken erstellen

In diesem Schritt erstellen Sie zwei Datenbanken und fügen den Datenbanken und bestimmten Spalten zu Testzwecken LF-Tags hinzu.

Erstellen Sie Ihre Datenbanken und Tabellen für den Zugriff auf Datenbankebene

1. Erstellen Sie zunächst die Datenbank `tag_database` und die Tabelle und fügen Sie die entsprechenden `source_data` LF-Tags hinzu.
 - a. Wählen Sie in der Lake Formation Formation-Konsole (<https://console.aws.amazon.com/lakeformation/>) unter Datenkatalog die Option Datenbanken aus.
 - b. Wählen Sie Datenbank erstellen aus.
 - c. Geben Sie unter Name `tag_database` ein.
 - d. Geben Sie für Standort den Amazon S3 S3-Standort ein, der mit der CloudFormation Vorlage erstellt wurde(`s3://lf-tagbased-demo-Account-ID/tag_database/`).
 - e. Deaktivieren Sie die Option Nur IAM-Zugriffskontrolle für neue Tabellen in dieser Datenbank verwenden.
 - f. Wählen Sie Datenbank erstellen aus.

~~2. Erstellen Sie als Nächstes eine neue Tabelle darin. tag_database~~

- a. Wählen Sie auf der Seite Datenbanken die Datenbank `austag_database`.
- b. Wählen Sie Tabellen anzeigen und klicken Sie auf Tabelle erstellen.
- c. Geben Sie unter Name `source_data` ein.
- d. Für Datenbank wählen Sie die `tag_database`-Datenbank aus.
- e. Wählen Sie als Tabellenformat die Option `AWS Glue Standardtabelle` aus.
- f. Wählen Sie für Daten befinden sich in die Option `Angegebener Pfad in meinem Konto` aus.
- g. Geben Sie unter Pfad einschließen den Pfad ein, der von der CloudFormation Vorlage `tag_database` erstellt wurde(`s3://lf-tagbased-demo`*Account-ID*/`tag_database/`).
- h. Wählen Sie als Datenformat die Option `CSV` aus.
- i. Geben Sie unter Schema hochladen das folgende JSON-Array mit Spaltenstruktur ein, um ein Schema zu erstellen:

```
[
  {
    "Name": "vendorid",
    "Type": "string"
  },
  {
    "Name": "lpep_pickup_datetime",
    "Type": "string"
  },
  {
    "Name": "lpep_dropoff_datetime",
    "Type": "string"
  },
  {
    "Name": "store_and_fwd_flag",
    "Type": "string"
  },
  {
    "Name": "ratecodeid",
    "Type": "string"
  },
  {
    "Name": "pulocationid",
```

```
        "Type": "string"
    },
    {
        "Name": "dolocationid",
        "Type": "string"
    },
    {
        "Name": "passenger_count",
        "Type": "string"
    },
    {
        "Name": "trip_distance",
       Type": "string"
    },
    {
        "Name": "fare_amount",
        "Type": "string"
    },
    {
        "Name": "extra",
        "Type": "string"
    },
    {
        "Name": "mta_tax",
        "Type": "string"
    },
    {
        "Name": "tip_amount",
        "Type": "string"
    },
    {
        "Name": "tolls_amount",
        "Type": "string"
    },
    {
```

```
        "Name": "ehail_fee",
        "Type": "string"
    },
    {
        "Name": "improvement_surcharge",
        "Type": "string"
    },
    {
        "Name": "total_amount",
        "Type": "string"
    },
    {
        "Name": "payment_type",
        "Type": "string"
    }
]
```

- j. Klicken Sie auf Upload. Nach dem Hochladen des Schemas sollte das Tabellenschema wie im folgenden Screenshot aussehen:

#	Column Name	▼	Data type
1	vendorid		string
2	lpep_pickup_datetime		string
3	lpep_dropoff_datetime		string
4	store_and_fwd_flag		string
5	ratecodeid		string
6	pulocationid		string
7	dolocationid		string
8	passenger_count		string
9	trip_distance		string
10	fare_amount		string
11	extra		string
12	mta_tax		string
13	tip_amount		string
14	tolls_amount		string
15	ehail_fee		string
16	improvement_surcharge		string
17	total_amount		string
18	payment_type		string

- k. Wählen Sie Absenden aus.
3. Als Nächstes hängen Sie LF-Tags auf Datenbankebene an.
 - a. Suchen Sie auf der Seite Datenbanken nach und wählen Sie es aus. `tag_database`
 - b. Wählen Sie im Menü Aktionen die Option LF-Tags bearbeiten aus.
 - c. Wählen Sie „Neues LF-Tag zuweisen“.
 - d. Wählen Sie unter Zugewiesene Schlüssel den `Confidential` LF-Tag aus, den Sie zuvor erstellt haben.
 - e. Wählen Sie für Werte die Option. `True`
 - f. Wählen Sie Speichern.

Damit ist die LF-Tag-Zuweisung zur `tag_database`-Datenbank abgeschlossen.

Erstellen Sie Ihre Datenbank und Tabelle für den Zugriff auf Spaltenebene

Wiederholen Sie die folgenden Schritte, um die Datenbank `col_tag_database` und die Tabelle `source_data_col_lvl1` zu erstellen und LF-Tags auf Spaltenebene anzuhängen.

1. Wählen Sie auf der Seite Datenbanken die Option Datenbank erstellen aus.
2. Geben Sie unter Name `col_tag_database` ein.
3. Geben Sie für Standort den Amazon S3 S3-Standort ein, der mit der CloudFormation Vorlage erstellt wurde(`s3://lf-tagbased-demo-Account-ID/col_tag_database/`).
4. Deaktivieren Sie die Option Nur IAM-Zugriffskontrolle für neue Tabellen in dieser Datenbank verwenden.
5. Wählen Sie Datenbank erstellen aus.
6. Wählen Sie auf der Seite Datenbanken Ihre neue Datenbank aus. (`col_tag_database`)
7. Wählen Sie Tabellen anzeigen und klicken Sie auf Tabelle erstellen.
8. Geben Sie unter Name `source_data_col_lvl1` ein.
9. Wählen Sie unter Datenbank Ihre neue Datenbank aus(`col_tag_database`).
10. Wählen Sie als Tabellenformat die Option AWS Glue Standardtabelle aus.
11. Wählen Sie für Daten befinden sich in die Option Angegebener Pfad in meinem Konto aus.
12. Geben Sie den Amazon S3 S3-Pfad für ein `col_tag_database`(`s3://lf-tagbased-demo-Account-ID/col_tag_database/`).

13. Wählen Sie für Datenformat die Option CSV.
14. Geben Sie Upload schema unter das folgende JSON-Schema ein:

```
[
  {
    "Name": "vendorid",
    "Type": "string"
  },
  {
    "Name": "lpep_pickup_datetime",
    "Type": "string"
  },
  {
    "Name": "lpep_dropoff_datetime",
    "Type": "string"
  },
  {
    "Name": "store_and_fwd_flag",
    "Type": "string"
  },
  {
    "Name": "ratecodeid",
    "Type": "string"
  },
  {
    "Name": "pulocationid",
    "Type": "string"
  },
  {
    "Name": "dolocationid",
    "Type": "string"
  }
]
```

```
    },  
    {  
      "Name": "passenger_count",  
      "Type": "string"  
    },  
    {  
      "Name": "trip_distance",  
      "Type": "string"  
    },  
    {  
      "Name": "fare_amount",  
      "Type": "string"  
    },  
    {  
      "Name": "extra",  
      "Type": "string"  
    },  
    {  
      "Name": "mta_tax",  
      "Type": "string"  
    },  
    {  
      "Name": "tip_amount",  
      "Type": "string"  
    },  
    {  
      "Name": "tolls_amount",  
      "Type": "string"
```

```
    },  
    {  
      "Name": "ehail_fee",  
      "Type": "string"  
    },  
    {  
      "Name": "improvement_surcharge",  
      "Type": "string"  
    },  
    {  
      "Name": "total_amount",  
      "Type": "string"  
    },  
    {  
      "Name": "payment_type",  
      "Type": "string"  
    }  
  ]  
}
```

15. Wählen Sie Upload. Nach dem Hochladen des Schemas sollte das Tabellenschema wie im folgenden Screenshot aussehen.

#	Column Name	▼	Data type
1	vendorid		string
2	lpep_pickup_datetime		string
3	lpep_dropoff_datetime		string
4	store_and_fwd_flag		string
5	ratecodeid		string
6	pulocationid		string
7	dolocationid		string
8	passenger_count		string
9	trip_distance		string
10	fare_amount		string
11	extra		string
12	mta_tax		string
13	tip_amount		string
14	tolls_amount		string
15	ehail_fee		string
16	improvement_surcharge		string
17	total_amount		string
18	payment_type		string

16. Wählen Sie Submit, um die Erstellung der Tabelle abzuschließen.
17. Ordnen Sie nun das Sensitive=True LF-Tag den Spalten vendorid und zu. fare_amount
 - a. Wählen Sie auf der Seite Tabellen die Tabelle aus, die Sie erstellt haben.
(source_data_col_lvl1)
 - b. Wählen Sie im Menü Aktionen die Option Schema aus.
 - c. Wählen Sie die Spalte aus vendorid und klicken Sie auf LF-Tags bearbeiten.
 - d. Wählen Sie für Zugewiesene Schlüssel die Option Sensitiv aus.
 - e. Wählen Sie für Werte die Option True aus.
 - f. Wählen Sie Speichern.
18. Ordnen Sie als Nächstes das Confidential=False LF-Tag zu. col_tag_database
Dies ist erforderlich lf-data-analyst, um die Datenbank beschreiben zu können, col_tag_database wenn Sie von dort aus angemeldet sind. Amazon Athena
 - a. Suchen Sie auf der Seite Datenbanken nach und wählen Sie col_tag_database.
 - b. Wählen Sie im Menü Aktionen die Option LF-Tags bearbeiten aus.
 - c. Wählen Sie „Neues LF-Tag zuweisen“.
 - d. Wählen Sie unter Zugewiesene Schlüssel den Confidential LF-Tag aus, den Sie zuvor erstellt haben.
 - e. Wählen Sie für Werte die Option. False
 - f. Wählen Sie Speichern.

Schritt 4: Erteilen Sie Tabellenberechtigungen

Erteilen Sie Datenanalysten Berechtigungen für die Nutzung der Datenbanken tag_database und der Tabelle col_tag_database mithilfe von LF-Tags Confidential und Sensitive

1. Gehen Sie wie folgt vor, um dem lf-data-analyst Benutzer Berechtigungen für die Objekte zu erteilen, die mit dem LF-Tag Confidential=True (Database:TAG_Database) verknüpft sind, sodass er über die Datenbank und Berechtigungen für Tabellen verfügt. Describe Select
 - a. Melden Sie sich bei der Lake Formation Konsole unter <https://console.aws.amazon.com/lakeformation/> als lf-data-engineer.
 - b. Wählen Sie unter Berechtigungen die Option Data Lake-Berechtigungen aus.

- c. Wählen Sie Grant (Erteilen).
 - d. Wählen Sie unter Principals die Option IAM-Benutzer und -Rollen aus.
 - e. Wählen Sie für IAM-Benutzer und -Rollen die Option. `lf-data-analyst`
 - f. Wählen Sie unter LF-Tags oder Katalogressourcen die Option Ressourcen aus, denen LF-Tags zugeordnet sind.
 - g. Wählen Sie LF-Tag hinzufügen.
 - h. Wählen Sie für Schlüssel die Option. `Confidential`
 - i. Wählen Sie für Werte die Option `True`.
 - j. Wählen Sie für Datenbankberechtigungen die Option `Describe`.
 - k. Wählen Sie für Tabellenberechtigungen die Option `Select and Describe` aus.
 - l. Wählen Sie Grant (Erteilen).
2. Wiederholen Sie anschließend die Schritte, um Datenanalysten Berechtigungen für den LF-Tag-Ausdruck für zu erteilen. `Confidential=False` Dieses LF-Tag wird zur Beschreibung der Tabelle `col_tag_database` und der Tabelle verwendet, `source_data_col_lvl` wenn Sie über Amazon Athena `lf-data-analyst` angemeldet sind.
 - a. Melden Sie sich bei der Lake Formation Konsole unter <https://console.aws.amazon.com/lakeformation/> als `lf-data-engineer`.
 - b. Wählen Sie auf der Seite Datenbanken die Datenbank `col_tag_database`.
 - c. Wählen Sie Aktion und Grant aus.
 - d. Wählen Sie unter Principals die Option IAM-Benutzer und -Rollen aus.
 - e. Wählen Sie für IAM-Benutzer und -Rollen die Option. `lf-data-analyst`
 - f. Wählen Sie Ressourcen aus, denen LF-Tags zugeordnet sind.
 - g. Wählen Sie LF-Tag hinzufügen.
 - h. Wählen Sie für Schlüssel die Option. `Confidential`
 - i. Wählen Sie für Werte die Option `False`.
 - j. Wählen Sie für Datenbankberechtigungen die Option `Describe`.
 - k. Wählen Sie für Tabellenberechtigungen nichts aus.
 - l. Wählen Sie Grant (Erteilen).
3. Wiederholen Sie anschließend die Schritte, um Datenanalysten Berechtigungen für den LF-Tag-Ausdruck für `Confidential=False` und zu erteilen. `Sensitive=True` Dieses LF-Tag

wird zur Beschreibung der `col_tag_database` und der Tabelle `source_data_col_lvl1` (auf Spaltenebene) verwendet, wenn Sie über Amazon Athena angemeldet sind. `lf-data-analyst`

- a. Melden Sie sich bei der Lake Formation Konsole unter <https://console.aws.amazon.com/lakeformation/> als `lf-data-engineer`.
- b. Wählen Sie auf der Seite Datenbanken die Datenbank `col_tag_database`.
- c. Wählen Sie Aktion und Grant aus.
- d. Wählen Sie unter Principals die Option IAM-Benutzer und -Rollen aus.
- e. Wählen Sie für IAM-Benutzer und -Rollen die Option `lf-data-analyst`.
- f. Wählen Sie Ressourcen aus, denen LF-Tags zugeordnet sind.
- g. Wählen Sie LF-Tag hinzufügen.
- h. Wählen Sie für Schlüssel die Option `Confidential`.
- i. Wählen Sie für Werte die Option `False`.
- j. Wählen Sie LF-Tag hinzufügen.
- k. Wählen Sie für Schlüssel die Option `Sensitive`.
- l. Wählen Sie für Werte die Option `True`.
- m. Wählen Sie für Datenbankberechtigungen die Option `Describe`.
- n. Wählen Sie für Tabellenberechtigungen die Option `Select` und `Describe`.
- o. Wählen Sie Grant (Erteilen).

Schritt 5: Führen Sie eine Abfrage in Amazon Athena aus, um die Berechtigungen zu überprüfen

Verwenden Sie für diesen Schritt Amazon Athena, um `SELECT` Abfragen für die beiden Tabellen (`source_data` und `source_data_col_lvl1`) auszuführen. Verwenden Sie den Amazon S3 S3-Pfad als Speicherort für die Abfrageergebnisse (`s3://lf-tagbased-demo-Account-ID/athena-results/`).

1. Melden Sie sich bei der Athena-Konsole unter <https://console.aws.amazon.com/athena/> als `lf-data-analyst` an.
2. Wählen Sie im Athena-Abfrage-Editor `tag_database` im linken Bereich.
3. Wählen Sie das Symbol für zusätzliche Menüoptionen (drei vertikale Punkte) neben `source_data` und wählen Sie „Tabellenvorschau“.

4. Wählen Sie Abfrage ausführen.

Die Ausführung der Abfrage sollte einige Minuten dauern. Die Abfrage zeigt alle Spalten in der Ausgabe an, da das LF-Tag auf Datenbankebene verknüpft ist und die `source_data` Tabelle das automatisch LF-tag von der Datenbank übernommen hat. `tag_database`

5. Führen Sie eine weitere Abfrage mit `col_tag_database` und aus. `source_data_col_lvl1`

Die zweite Abfrage gibt die beiden Spalten zurück, die als `Non-Confidential` und `gezeichnet` wurden `Sensitive`.

6. Sie können auch überprüfen, ob das Verhalten der Tag-basierten Zugriffsrichtlinie von Lake Formation in Spalten angezeigt wird, für die Sie keine Richtlinienberechtigungen haben. Wenn eine Spalte ohne Tags aus der Tabelle ausgewählt wird `source_data_col_lvl1`, gibt Athena einen Fehler zurück. Sie können beispielsweise die folgende Abfrage ausführen, um Spalten ohne Tags auszuwählen: `geolocationid`

```
SELECT geolocationid FROM "col_tag_database"."source_data_col_lvl1" limit 10;
```

Schritt 6: Ressourcen AWS bereinigen

Um zu verhindern, dass Ihnen unerwünschte Kosten entstehen AWS-Konto, können Sie die AWS Ressourcen löschen, die Sie für dieses Tutorial verwendet haben.

1. Melden Sie sich bei der Lake Formation Console an `lf-data-engineer` und löschen Sie die Datenbanken `tag_database` und `col_tag_database`.
2. Melden Sie sich als Nächstes an `lf-data-steward` und bereinigen Sie alle LF-Tag-Berechtigungen, Datenberechtigungen und Datenspeicherberechtigungen, die oben gewährt wurden und gewährt `lf-data-engineer` wurden. `lf-data-analyst`.
3. Melden Sie sich bei der Amazon S3-Konsole als Kontoinhaber mit den IAM-Anmeldeinformationen an, die Sie für die Bereitstellung des CloudFormation Stacks verwendet haben.
4. Löschen Sie die folgenden Buckets:
 - `lf-tagbased-demo-accesslogs-acct-id`
 - `lf-tagbased-demo-acct-id`

5. Melden Sie sich unter <https://console.aws.amazon.com/cloudformation> bei der CloudFormation Konsole an und löschen Sie den von Ihnen erstellten Stack. Warten Sie, bis sich der Stack-Status auf ändert. DELETE_COMPLETE

Sicherung von Data Lakes mit Zugriffskontrolle auf Zeilenebene

AWS Lake Formation Mit Berechtigungen auf Zeilenebene können Sie auf der Grundlage von Datenkonformitäts- und Governance-Richtlinien Zugriff auf bestimmte Zeilen in einer Tabelle gewähren. Wenn Sie über große Tabellen verfügen, in denen Milliarden von Datensätzen gespeichert werden, benötigen Sie eine Möglichkeit, verschiedenen Benutzern und Teams den Zugriff nur auf die Daten zu ermöglichen, die sie sehen dürfen. Die Zugriffskontrolle auf Zeilenebene ist eine einfache und leistungsstarke Methode, um Daten zu schützen und Benutzern gleichzeitig Zugriff auf die Daten zu gewähren, die sie für ihre Arbeit benötigen. Lake Formation bietet zentralisierte Audits und Compliance-Berichte, indem ermittelt wird, welche Principals wann und über welche Dienste auf welche Daten zugegriffen haben.

In diesem Tutorial erfahren Sie, wie Zugriffskontrollen auf Zeilenebene in Lake Formation funktionieren und wie Sie sie einrichten.

Dieses Tutorial enthält eine AWS CloudFormation Vorlage für die schnelle Einrichtung der erforderlichen Ressourcen. Sie können es überprüfen und an Ihre Bedürfnisse anpassen.

Themen

- [Zielgruppe](#)
- [Voraussetzungen](#)
- [Schritt 1: Stellen Sie Ihre Ressourcen bereit](#)
- [Schritt 2: Abfrage ohne Datenfilter](#)
- [Schritt 3: Richten Sie Datenfilter ein und gewähren Sie Berechtigungen](#)
- [Schritt 4: Abfrage mit Datenfiltern](#)
- [Schritt 5: AWS Ressourcen bereinigen](#)

Zielgruppe

Dieses Tutorial richtet sich an Datenverwalter, Dateningenieure und Datenanalysten. In der folgenden Tabelle sind die Rollen und Verantwortlichkeiten eines Datenbesitzers und eines Datenkonsumenten aufgeführt.

Rolle	Beschreibung
IAM-Administrator	Ein Benutzer, der Benutzer und Rollen sowie Amazon Simple Storage Service (Amazon S3) -Buckets erstellen kann. Hat die AdministratorAccess AWS verwaltete Richtlinie.
Data Lake-Administrator	Ein Benutzer, der für die Einrichtung des Data Lakes, die Erstellung von Datenfiltern und die Erteilung von Berechtigungen für Datenanalysten verantwortlich ist.
Datenanalyst	Ein Benutzer, der Abfragen für den Data Lake ausführen kann. Datenanalysten mit Wohnsitz in verschiedenen Ländern (für unseren Anwendungsfall in den USA und Japan) können nur Produktbewertungen von Kunden in ihrem eigenen Land analysieren und sollten aus Compliance-Gründen keine Kundendaten in anderen Ländern sehen können.

Voraussetzungen

Bevor Sie mit diesem Tutorial beginnen, benötigen Sie eine AWS-Konto , mit der Sie sich als Administratorbenutzer mit den richtigen Berechtigungen anmelden können. Weitere Informationen finden Sie unter [Erledigen Sie die Aufgaben zur AWS Erstkonfiguration](#).

In der Anleitung wird davon ausgegangen, dass Sie mit IAM vertraut sind. Informationen zu IAM finden Sie im [IAM-Benutzerhandbuch](#).

Lake Formation Formation-Einstellungen ändern

Important

Bevor Sie die CloudFormation Vorlage starten, deaktivieren Sie die Option Nur IAM-Zugriffskontrolle für neue Datenbanken/Tabellen in Lake Formation verwenden, indem Sie die folgenden Schritte ausführen:

1. Melden Sie sich in der Region USA Ost (Nord-Virginia) oder USA West (Oregon) bei <https://console.aws.amazon.com/lakeformation/> der Lake Formation Konsole an.
2. Wählen Sie unter Datenkatalog die Option Einstellungen aus.
3. Deaktivieren Sie die Optionen Nur IAM-Zugriffskontrolle für neue Datenbanken verwenden und Nur IAM-Zugriffskontrolle für neue Tabellen in neuen Datenbanken verwenden.
4. Wählen Sie Save (Speichern) aus.

Schritt 1: Stellen Sie Ihre Ressourcen bereit

Dieses Tutorial enthält eine CloudFormation Vorlage für eine schnelle Einrichtung. Sie können es überprüfen und an Ihre Bedürfnisse anpassen. Die CloudFormation Vorlage generiert die folgenden Ressourcen:

- Benutzer und Richtlinien für:
 - DataLakeAdmin
 - DataAnalystUSA
 - DataAnalystJP
- Lake Formation Data Lake-Einstellungen und Berechtigungen
- Eine Lambda-Funktion (für Lambda-gestützte CloudFormation benutzerdefinierte Ressourcen), die verwendet wird, um Beispieldatendateien aus dem öffentlichen Amazon S3 S3-Bucket in Ihren Amazon S3-Bucket zu kopieren
- Ein Amazon S3 S3-Bucket, der als unser Data Lake dient
- Eine AWS Glue Data Catalog Datenbank, eine Tabelle und eine Partition

Erstellen Sie Ihre Ressourcen

Gehen Sie wie folgt vor, um Ihre Ressourcen mithilfe der CloudFormation Vorlage zu erstellen.

1. Melden Sie sich bei der CloudFormation Konsole unter <https://console.aws.amazon.com/cloudformation> in der Region USA Ost (Nord-Virginia) an.
2. Wählen Sie [Launch Stack](#).
3. Wählen Sie auf dem Bildschirm „Stack erstellen“ die Option „Weiter“.
4. Geben Sie einen Stack-Namen ein.

5. Geben Sie für `DatalakeAdminUserName` und `DatalakeAdminUserPassword` Ihren IAM-Benutzernamen und Ihr Passwort für den Data Lake-Admin-Benutzer ein.
6. Geben Sie für `DataAnalystUsUserName` und `DataAnalystUsUserPassword` den gewünschten Benutzernamen und das Passwort für den Data Analyst-Benutzer, der für den US-Marketplace verantwortlich ist, den gewünschten Benutzernamen und das Passwort ein.
7. Geben Sie für `DataAnalystJpUserName` und `DataAnalystJpUserPassword` den gewünschten Benutzernamen und das Passwort für den Data Analyst-Benutzer, der für den japanischen Marketplace zuständig ist, den gewünschten Benutzernamen und das Passwort ein.
8. Geben Sie für `DataLakeBucketName` den Namen Ihres Daten-Buckets ein.
9. Für `DatabaseName` und `TableName` belassen Sie die Standardeinstellung.
10. Wählen Sie Weiter
11. Wählen Sie auf der nächsten Seite Weiter aus.
12. Überprüfen Sie die Details auf der letzten Seite und wählen Sie Ich bestätige, dass CloudFormation möglicherweise IAM-Ressourcen erstellt werden.
13. Wählen Sie Create (Erstellen) aus.

Die Erstellung des Stacks kann eine Minute dauern.

Schritt 2: Abfrage ohne Datenfilter

Nachdem Sie die Umgebung eingerichtet haben, können Sie die Tabelle mit den Produktbewertungen abfragen. Fragen Sie zunächst die Tabelle ohne Zugriffskontrollen auf Zeilenebene ab, um sicherzustellen, dass Sie die Daten sehen können. Wenn Sie Abfragen zum ersten Mal in Amazon Athena ausführen, müssen Sie den Speicherort der Abfrageergebnisse konfigurieren.

Fragen Sie die Tabelle ohne Zugriffskontrolle auf Zeilenebene ab

1. Melden Sie sich an Athena Konsolen Sie <https://console.aws.amazon.com/athena/> als `DatalakeAdmin` Benutzer und führen Sie die folgende Abfrage aus:

```
SELECT *  
FROM lakeformation_tutorial_row_security.amazon_reviews  
LIMIT 10
```

Der folgende Screenshot zeigt das Abfrageergebnis. Diese Tabelle hat nur eine Partition `product_category=Video`, sodass jeder Datensatz ein Bewertungskommentar für ein Videoprodukt ist.

Query:

```
1 SELECT *
2 FROM lakeformation_tutorial_row_security.amazon_reviews
3 LIMIT 10
```

Run query **Save as** **Create** (Run time: 12.62 seconds, Data scanned: 64.57 MB) **Format query** **Clear**

Use Ctrl + Enter to run query, Ctrl + Space to autocomplete

Athena engine version 2 [Release versions](#)

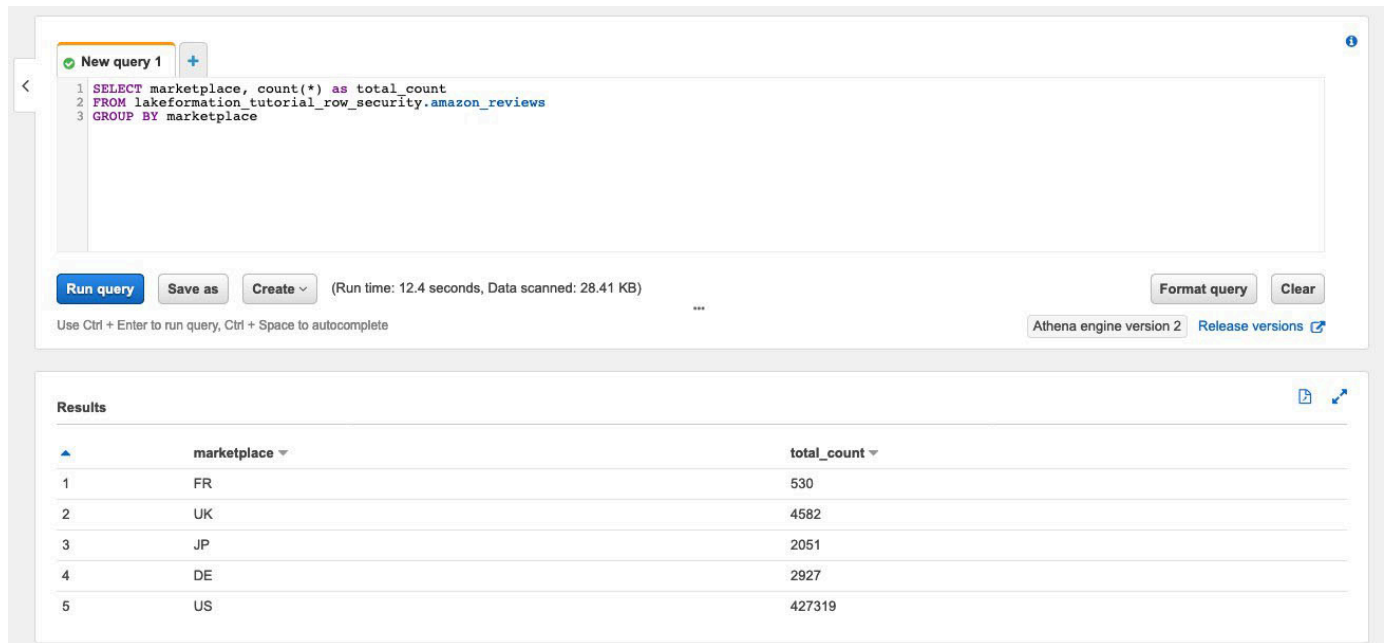
Results

	marketplace	customer_id	review_id	product_id	product_parent	product_title	star_rating	helpful_votes	total_votes	vine
1	US	22066705	R3HZYXMJ5HEXIG	6304878621	928670802	The Thin Blue Line 3 [VHS]	5	0	0	N
2	US	20838467	RJC8PH4K3DVQB	630335663X	577032943	Covert Bailey: Fit Or Fat for the 90's [VHS]	1	0	0	N
3	US	15338666	R1OH4581ARVWNX	6300269434	266152594	Young Man With a Horn [VHS]	1	0	2	N
4	US	7080939	R3TWQ5OT8KW0E8	B000EKCQMQ	345913478	Madeline in London (Told By Christopher Plummer)	5	0	0	N
5	US	30548191	R3BK9ULGX82VG0	078311317X	38445970	2 Days in the Valley (Widescreen Edition) [VHS]	5	0	0	N
6	US	16052189	R1LV7NN89A38YT	6302862833	924318070	Zoltz [VHS]	4	0	0	N
7	US	43430756	R2IJAELO3PXEYM	B00027VBBJ	51076382	Party Crasher	1	1	1	N
8	US	43539164	R3TNQJ9JANR9Q5	6303205542	69262780	Frugal Gourmet: Spanish Kitchen [VHS]	5	0	0	N
9	US	21187650	R2AVXCQOLI53IC	6302606713	934453987	Live [VHS]	5	0	0	N
10	US	7080939	RC71NIBDHR9KA	B00007ELHT	498552125	Golden Rules of Growing Up [VHS]	5	0	0	N

- Führen Sie als Nächstes eine Aggregationsabfrage aus, um die Gesamtzahl der Datensätze pro marketplace Datensatz abzurufen.

```
SELECT marketplace, count(*) as total_count
FROM lakeformation_tutorial_row_security.amazon_reviews
GROUP BY marketplace
```

Der folgende Screenshot zeigt das Abfrageergebnis. Die marketplace Spalte hat fünf verschiedene Werte. In den nachfolgenden Schritten richten Sie zeilenbasierte Filter mithilfe der marketplace Spalte ein.



The screenshot shows the AWS Lake Formation console interface. At the top, there is a text area for a SQL query labeled "New query 1". The query is:

```
1 SELECT marketplace, count(*) as total_count
2 FROM lakeformation_tutorial_row_security.amazon_reviews
3 GROUP BY marketplace
```

Below the query area, there are buttons for "Run query", "Save as", and "Create". To the right of these buttons, it says "(Run time: 12.4 seconds, Data scanned: 28.41 KB)". Further right are buttons for "Format query" and "Clear". Below these buttons, a small text says "Use Ctrl + Enter to run query, Ctrl + Space to autocomplete". On the far right, it says "Athena engine version 2" with a link to "Release versions".

Below the query area, there is a section titled "Results" which contains a table with two columns: "marketplace" and "total_count". The table has five rows of data:

	marketplace	total_count
1	FR	530
2	UK	4582
3	JP	2051
4	DE	2927
5	US	427319

Schritt 3: Richten Sie Datenfilter ein und gewähren Sie Berechtigungen

In diesem Tutorial werden zwei Datenanalysten verwendet: einer ist für den US-Markt zuständig, der andere für den japanischen Markt. Jeder Analyst verwendet Athena, um Kundenrezensionen nur für seinen spezifischen Marketplace zu analysieren. Erstellen Sie zwei verschiedene Datenfilter, einen für den Analysten, der für den US-Markt verantwortlich ist, und einen weiteren für den, der für den japanischen Markt verantwortlich ist. Erteilen Sie den Analysten anschließend ihre jeweiligen Berechtigungen.

Erstellen Sie Datenfilter und gewähren Sie Berechtigungen

1. Erstellen Sie einen Filter, um den Zugriff auf die US marketplace Daten einzuschränken.
 - a. Melden Sie sich als DataLakeAdmin Benutzer bei der Lake Formation Formation-Konsole <https://console.aws.amazon.com/lakeformation/> in der Region USA Ost (Nord-Virginia) an.
 - b. Wählen Sie Datenfilter.
 - c. Wählen Sie Neuen Filter erstellen.
 - d. Geben Sie als Datenfiltername einamazon_reviews_US.
 - e. Wählen Sie für Zieldatenbank die Datenbank auslakeformation_tutorial_row_security.
 - f. Wählen Sie für Zieltabelle die Tabelle ausamazon_reviews.

- g. Behalten Sie für den Zugriff auf Spaltenebene die Standardeinstellung bei.
 - h. Geben Sie für Zeilenfilterausdruck den Wert ein. `marketplace= 'US'`
 - i. Wählen Sie Create Filter) (Filter erstellen.
2. Erstellen Sie einen Filter, um den Zugriff auf die japanischen marketplace Daten einzuschränken.
 - a. Wählen Sie auf der Seite Datenfilter die Option Neuen Filter erstellen aus.
 - b. Geben Sie als Datenfiltername den Wert ein `amazon_reviews_JP`.
 - c. Wählen Sie für Zieldatenbank die Datenbank `auslakeformation_tutorial_row_security`.
 - d. Wählen Sie für Target-Tabelle die Tabelle `amazon_reviews`.
 - e. Behalten Sie für den Zugriff auf Spaltenebene die Standardeinstellung bei.
 - f. Geben Sie für Zeilenfilterausdruck den Wert ein. `marketplace= 'JP'`
 - g. Wählen Sie Create Filter) (Filter erstellen.
3. Erteilen Sie als Nächstes den Datenanalysten, die diese Datenfilter verwenden, Berechtigungen. Gehen Sie wie folgt vor, um dem US-Datenanalysten Berechtigungen zu erteilen (DataAnalystUS):
 - a. Wählen Sie unter Berechtigungen die Option Data Lake-Berechtigungen aus.
 - b. Wählen Sie unter Datenberechtigung die Option Erteilen aus.
 - c. Wählen Sie für Principals die Option IAM-Benutzer und -Rollen und anschließend die Rolle aus. `DataAnalystUS`
 - d. Wählen Sie für LF-Tags oder Katalogressourcen die Option Benannte Datenkatalogressourcen aus.
 - e. Wählen Sie unter Database (Datenbank) Option `lakeformation_tutorial_row_security` aus.
 - f. Wählen Sie für Tabellen optional die Option. `amazon_reviews`
 - g. Für Datenfilter — optional — wählen Sie. `amazon_reviews_US`
 - h. Wählen Sie für Datenfilterberechtigungen die Option Auswählen aus.
 - i. Wählen Sie Grant (Erteilen).
4. Gehen Sie wie folgt vor, um dem japanischen Datenanalysten (DataAnalystJP) Berechtigungen zu erteilen:

- a. Wählen Sie unter Berechtigungen die Option Data Lake-Berechtigungen aus.
- b. Wählen Sie unter Datenberechtigung die Option Erteilen aus.
- c. Wählen Sie für Principals die Option IAM-Benutzer und -Rollen und anschließend die Rolle aus. DataAnalystJP
- d. Wählen Sie für LF-Tags oder Katalogressourcen die Option Benannte Datenkatalogressourcen aus.
- e. Wählen Sie unter Database (Datenbank) Option lakeformation_tutorial_row_security aus.
- f. Wählen Sie für Tabellen optional die Option. amazon_reviews
- g. Für Datenfilter — optional — wählen Sie. amazon_reviews_JP
- h. Wählen Sie für Datenfilterberechtigungen die Option Auswählen aus.
- i. Wählen Sie Grant (Erteilen).

Schritt 4: Abfrage mit Datenfiltern

Führen Sie anhand der Datenfilter, die der Tabelle mit den Produktbewertungen beigelegt sind, einige Abfragen durch, um zu sehen, wie Berechtigungen von Lake Formation durchgesetzt werden.

1. Melden Sie sich <https://console.aws.amazon.com/athena/> als DataAnalystUS Benutzer bei der Athena-Konsole an.
2. Führen Sie die folgende Abfrage aus, um einige Datensätze abzurufen, die anhand der von uns definierten Berechtigungen auf Zeilenebene gefiltert werden:

```
SELECT *  
FROM lakeformation_tutorial_row_security.amazon_reviews  
LIMIT 10
```

Der folgende Screenshot zeigt das Abfrageergebnis.

The screenshot shows the AWS Athena console interface. At the top, there's a query editor with a SQL query: `SELECT * FROM lakeformation_tutorial_row_security.amazon_reviews LIMIT 10`. Below the editor are buttons for 'Run query', 'Save as', and 'Create'. A status bar indicates '(Run time: 11.9 seconds, Data scanned: 0 KB)'. To the right are 'Format query' and 'Clear' buttons. Below the query editor, the 'Results' section displays a table with 12 columns: marketplace, customer_id, review_id, product_id, product_parent, product_title, star_rating, helpful_votes, total_votes, vine, verified_purchase, and review_text. The table contains 10 rows of data, all with 'US' in the marketplace column.

	marketplace	customer_id	review_id	product_id	product_parent	product_title	star_rating	helpful_votes	total_votes	vine	verified_purchase	review_text
1	US	43836277	R2NUBTUO60VYU	B00068S41I	653409458	The Notebook [VHS]	4	0	0	N	Y	KI
2	US	20261976	R2QTOLZUQERU5B	6303060013	176265879	American Cyborg: Steel Warrior [VHS]	5	0	1	N	Y	it
3	US	15947067	R1PHKR75RKZNSU	6303927319	850909689	Biography - Darryl Zanuck [VHS]	5	0	0	N	N	G
4	US	19288153	R1BL2WVE5X34UN	6304032153	479446069	Timon & Pumbaa: Quit Buggin Me [VHS]	5	0	0	N	N	FI
5	US	19712967	R2DKOCIBS5FSP7	0784017743	35164822	Denise Austin - Hit the Spot: Arms & Bust [VHS]	5	0	0	N	Y	G
6	US	51047097	R2XF5HQATT4IVR	0793960142	233936597	I Love Lucy - Lucy's Italian Movie/Ballet [VHS]	5	0	0	N	N	FI
7	US	43836277	R2NUBTUO60VYU	B00068S41I	653409458	The Notebook [VHS]	4	0	0	N	Y	KI
8	US	51047097	R1C0H0G6NATZXO	6304872585	233936597	I Love Lucy: Lucy Meets Superman/Freez [VHS]	5	0	1	N	N	FI
9	US	42808630	R2HXW7UD4IGZLN	6303060013	176265879	American Cyborg: Steel Warrior [VHS]	5	0	1	N	Y	M
10	US	11682952	R18IURLUPYI4DP	6302993717	42308924	Songs of Christmas [VHS]	1	0	0	N	Y	R

- Führen Sie auf ähnliche Weise eine Abfrage aus, um die Gesamtzahl der Datensätze pro Marketplace zu zählen.

```
SELECT marketplace , count ( * ) as total_count
FROM lakeformation_tutorial_row_security .amazon_reviews
GROUP BY marketplace
```

Das Abfrageergebnis zeigt nur die marketplace US in den Ergebnissen. Dies liegt daran, dass der Benutzer nur Zeilen sehen darf, in denen der marketplace Spaltenwert gleich ist US.

- Wechseln Sie zum DataAnalystJP Benutzer und führen Sie dieselbe Abfrage aus.

```
SELECT *
FROM lakeformation_tutorial_row_security.amazon_reviews
LIMIT 10
```

Das Abfrageergebnis zeigt, dass nur die Datensätze zu den gehören JP marketplace.

- Führen Sie die Abfrage aus, um die Gesamtzahl der Datensätze pro zu zählen marketplace.

```
SELECT marketplace, count(*) as total_count
FROM lakeformation_tutorial_row_security.amazon_reviews
GROUP BY marketplace
```

Das Abfrageergebnis zeigt nur die Zeile, die zu der gehört JPmarketplace.

Schritt 5: AWS Ressourcen bereinigen

Bereinigen von -Ressourcen

Um zu verhindern, dass Ihnen unerwünschte Kosten entstehen AWS-Konto, können Sie die AWS Ressourcen löschen, die Sie für dieses Tutorial verwendet haben.

- [Löschen Sie den Cloud-Formation-Stack.](#)

Gemeinsame Nutzung eines Data Lakes mithilfe von Tag-basierter Zugriffskontrolle von Lake Formation und benannten Ressourcen

Dieses Tutorial zeigt, wie Sie konfigurieren können AWS Lake Formation , um Daten, die in einem Data Lake gespeichert sind, sicher mit mehreren Unternehmen, Organisationen oder Geschäftseinheiten gemeinsam zu nutzen, ohne die gesamte Datenbank kopieren zu müssen. Es gibt zwei Möglichkeiten, Ihre Datenbanken und Tabellen mithilfe der kontenübergreifenden Zugriffskontrolle AWS-Konto von Lake Formation gemeinsam mit anderen zu nutzen:

- Tag-basierte Zugriffskontrolle von Lake Formation (empfohlen)

Die tagbasierte Zugriffskontrolle von Lake Formation ist eine Autorisierungsstrategie, die Berechtigungen auf der Grundlage von Attributen definiert. In Lake Formation werden diese Attribute LF-Tags genannt. Weitere Informationen finden Sie unter [Verwaltung eines Data Lakes mithilfe der Tag-basierten Zugriffskontrolle von Lake Formation.](#)

- Lake Formation benannte Ressourcen

Die Methode Lake Formation Named Resource ist eine Autorisierungsstrategie, die Berechtigungen für Ressourcen definiert. Zu den Ressourcen gehören Datenbanken, Tabellen und Spalten. Data Lake-Administratoren können Berechtigungen für Lake Formation Formation-Ressourcen zuweisen und widerrufen. Weitere Informationen finden Sie unter [Kontoübergreifender Datenaustausch in Lake Formation.](#)

Wir empfehlen die Verwendung benannter Ressourcen, wenn der Data Lake-Administrator es vorzieht, einzelnen Ressourcen explizit Berechtigungen zu gewähren. Wenn Sie die benannte Ressourcenmethode verwenden, um einem externen Konto Lake Formation-Berechtigungen für

eine Datenkatalogressource zu gewähren, verwendet Lake Formation AWS Resource Access Manager (AWS RAM), um die Ressource gemeinsam zu nutzen.

Themen

- [Zielgruppe](#)
- [Konfigurieren Sie die Lake Formation Data Catalog-Einstellungen im Produzentenkonto](#)
- [Schritt 1: Stellen Sie Ihre Ressourcen mithilfe von AWS CloudFormation Vorlagen bereit](#)
- [Schritt 2: Voraussetzungen für die gemeinsame Nutzung von Konten bei Lake Formation](#)
- [Schritt 3: Implementieren Sie die kontenübergreifende gemeinsame Nutzung mithilfe der tagbasierten Zugriffskontrollmethode](#)
- [Schritt 4: Implementieren Sie die benannte Ressourcenmethode](#)
- [Schritt 5: AWS Ressourcen bereinigen](#)

Zielgruppe

Dieses Tutorial richtet sich an Datenverwalter, Dateningenieure und Datenanalysten. Wenn es um die gemeinsame Nutzung von Datenkatalogtabellen von Lake Formation AWS Glue und die Verwaltung von Berechtigungen in Lake Formation geht, haben die Data Stewards innerhalb der produzierenden Konten die funktionale Verantwortung, basierend auf den Funktionen, die sie unterstützen, und können verschiedenen Verbrauchern, externen Organisationen und Konten Zugriff gewähren. In der folgenden Tabelle sind die Rollen aufgeführt, die in diesem Tutorial verwendet werden:

Rolle	Description
DataLakeAdminProducer	Der Data Lake-Admin-IAM-Benutzer hat folgenden Zugriff: • Vollständiger Lese-, Schreib- und Aktualisierungszugriff auf alle Ressourcen im Datenkatalog • Fähigkeit, Ressourcen Berechtigungen zu erteilen • Kann Ressourcenlinks für die gemeinsam genutzte Tabelle erstellen

Rolle	Description
	• Kann LF-Tags an Ressourcen anhängen, was den Zugriff auf Prinzipale auf der Grundlage von Richtlinien ermöglicht, die von Data Stewards erstellt wurden
DataLakeAdminConsumer	Der Data Lake-Admin-IAM-Benutzer hat folgenden Zugriff: • Vollständiger Lese-, Schreib- und Aktualisierungszugriff auf alle Ressourcen im Datenkatalog • Fähigkeit, Ressourcen Berechtigungen zu erteilen • Kann Ressourcenlinks für die gemeinsam genutzte Tabelle erstellen • Kann LF-Tags an Ressourcen anhängen, was den Zugriff auf Prinzipale auf der Grundlage von Richtlinien ermöglicht, die von Data Stewards erstellt wurden
DataAnalyst	Der DataAnalyst Benutzer hat folgenden Zugriff: • Detaillierter Zugriff auf Ressourcen, die von Tag-basierten Zugriffsrichtlinien von Lake Formation oder mithilfe der Methode für benannte Ressourcen gemeinsam genutzt werden

Konfigurieren Sie die Lake Formation Data Catalog-Einstellungen im Produzentenkonto

Bevor Sie mit diesem Tutorial beginnen, benötigen Sie eine AWS-Konto , mit der Sie sich als Administratorbenutzer mit den richtigen Berechtigungen anmelden können. Weitere Informationen finden Sie unter [Erledigen Sie die Aufgaben zur AWS Erstkonfiguration](#).

In der Anleitung wird davon ausgegangen, dass Sie mit IAM vertraut sind. Informationen zu IAM finden Sie im [IAM-Benutzerhandbuch](#).

Konfigurieren Sie die Lake Formation Data Catalog-Einstellungen im Produzentenkonto

 Note

In diesem Tutorial wird das Konto, das die Quelltablette enthält, als Produzentenkonto bezeichnet, und das Konto, das Zugriff auf die Quelltablette benötigt, wird als Verbraucherkonto bezeichnet.

Lake Formation bietet ein eigenes Genehmigungsverwaltungsmodell. Um die Abwärtskompatibilität mit dem IAM-Berechtigungsmodell aufrechtzuerhalten, wird der Gruppe `IAMAllowedPrincipals` die `Super` Berechtigung standardmäßig für alle vorhandenen AWS Glue Data Catalog Ressourcen erteilt. Außerdem sind die Einstellungen für die Zugriffskontrolle „Nur IAM verwenden“ für neue Datenkatalogressourcen aktiviert. In diesem Tutorial wird eine feinkörnige Zugriffskontrolle mithilfe Lake Formation Formation-Berechtigungen und IAM-Richtlinien für eine grobe Zugriffskontrolle verwendet. Details dazu finden Sie unter [Methoden für eine differenzierte Zugriffskontrolle](#). Bevor Sie eine AWS CloudFormation Vorlage für eine schnelle Einrichtung verwenden, müssen Sie daher die Lake Formation Data Catalog-Einstellungen im Producer-Konto ändern.

 Important

Diese Einstellung wirkt sich auf alle neu erstellten Datenbanken und Tabellen aus. Wir empfehlen daher dringend, dieses Tutorial in einem Konto zu absolvieren, das nicht zur Produktion verwendet wird, oder mit einem neuen Konto. Wenn Sie ein gemeinsames Konto verwenden (z. B. das Entwicklungskonto Ihres Unternehmens), stellen Sie außerdem sicher, dass sich dies nicht auf andere Ressourcen auswirkt. Wenn Sie es vorziehen, die Standardsicherheitseinstellungen beizubehalten, müssen Sie bei der gemeinsamen Nutzung von `IAMAllowedPrincipals` Ressourcen für andere Konten einen zusätzlichen Schritt ausführen, in dem Sie die Standard-Superberechtigung für die Datenbank oder Tabelle entziehen. Wir besprechen die Details später in diesem Tutorial.

Gehen Sie wie folgt vor, um die Lake Formation Data Catalog-Einstellungen im Producer-Konto zu konfigurieren:

1. Melden Sie sich AWS-Managementkonsole mit dem Producer-Konto als Admin-Benutzer oder als Benutzer mit Lake Formation PutDataLakeSettings API-Berechtigung an.
2. Wählen Sie in der Lake Formation Formation-Konsole im Navigationsbereich unter Datenkatalog die Option Einstellungen aus.
3. Deaktivieren Sie „Nur IAM-Zugriffskontrolle für neue Datenbanken verwenden“ und „Nur IAM-Zugriffskontrolle für neue Tabellen in neuen Datenbanken verwenden“

Wählen Sie Speichern.

AWS Lake Formation > Data catalog settings

Data catalog settings

Default permissions for newly created databases and tables

These settings maintain existing AWS Glue Data Catalog behavior. You can still set individual permissions on databases and tables, which will take effect when you revoke the Super permission from IAMAllowedPrincipals. See [Changing Default Settings for Your Data Lake](#).

☐ Use only IAM access control for new databases

☐ Use only IAM access control for new tables in new databases

Default permissions for AWS CloudTrail

These settings specify the information being shown in AWS CloudTrail.

Resource owners

Enter resource owners you wish to share your CloudTrail access details with.

Enter one or more AWS account IDs. Press Enter after each ID.

Cancel

Save

Darüber hinaus können Sie **IAMAllowedPrincipals** unter Administratorrollen und -aufgaben die **CREATE_DATABASE** Berechtigungen für Datenbankersteller entfernen. Nur dann können Sie mithilfe von Lake Formation Formation-Berechtigungen steuern, wer eine neue Datenbank erstellen kann.

Schritt 1: Stellen Sie Ihre Ressourcen mithilfe von AWS CloudFormation Vorlagen bereit

Die CloudFormation Vorlage für das Produzentenkonto generiert die folgenden Ressourcen:

- Ein Amazon S3 S3-Bucket, der als Data Lake dient.
- Eine Lambda-Funktion (für CloudFormation Lambda-gestützte benutzerdefinierte Ressourcen). Wir verwenden die Funktion, um Beispieldatendateien aus dem öffentlichen Amazon S3 S3-Bucket in Ihren Amazon S3-Bucket zu kopieren.
- IAM-Benutzer und -Richtlinien: DataLakeAdminProducer.
- Die entsprechenden Lake Formation Formation-Einstellungen und -Berechtigungen, einschließlich:
 - Definieren des Lake Formation Data Lake-Administrators im Producer-Konto
 - Registrierung eines Amazon S3 S3-Buckets als Lake Formation Data Lake-Standort (Produzentenkonto)
- Eine AWS Glue Data Catalog Datenbank, eine Tabelle und eine Partition. Da es zwei Optionen für die gemeinsame Nutzung von Ressourcen gibt AWS-Konten, erstellt diese Vorlage zwei separate Gruppen von Datenbank und Tabelle.

Die CloudFormation Vorlage für das Verbraucherkonto generiert die folgenden Ressourcen:

- IAM-Benutzer und -Richtlinien:
 - DataLakeAdminConsumer
 - DataAnalyst
- Eine AWS Glue Data Catalog Datenbank. Diese Datenbank dient zum Erstellen von Ressourcenlinks zu gemeinsam genutzten Ressourcen.

Erstellen Sie Ihre Ressourcen im Produzentenkonto

1. Melden Sie sich bei der AWS CloudFormation Konsole unter <https://console.aws.amazon.com/cloudformation> in der Region USA Ost (Nord-Virginia) an.
2. Wählen Sie [Launch Stack](#).
3. Wählen Sie Weiter aus.
4. Geben Sie unter Stackname einen Stacknamen ein, z. stack-producer B.

5. Geben Sie im Abschnitt Benutzerkonfiguration den Benutzernamen und das Passwort für `ProducerDataLakeAdminUserName` und `einProducerDataLakeAdminUserPassword`.
6. Geben Sie für `DataLakeBucketName` den Namen Ihres Data Lake-Buckets ein. Dieser Name muss weltweit eindeutig sein.
7. Behalten Sie für `DatabaseName` und `TableName` die Standardwerte bei.
8. Wählen Sie Weiter aus.
9. Wählen Sie auf der nächsten Seite Weiter aus.
10. Überprüfen Sie die Details auf der letzten Seite und wählen Sie Ich bestätige, dass AWS CloudFormation möglicherweise IAM-Ressourcen erstellt werden.
11. Wählen Sie Erstellen aus.

Die Erstellung des Stacks kann bis zu einer Minute dauern.

Erstellen Sie Ihre Ressourcen im Kundenkonto

1. Melden Sie sich bei der AWS CloudFormation Konsole unter <https://console.aws.amazon.com/cloudformation> in der Region USA Ost (Nord-Virginia) an.
2. Wählen Sie [Launch Stack](#).
3. Wählen Sie Weiter aus.
4. Geben Sie unter Stackname einen Stacknamen ein, z. `stack-consumer B`.
5. Geben Sie im Abschnitt Benutzerkonfiguration den Benutzernamen und das Passwort für `ConsumerDataLakeAdminUserName` und `einConsumerDataLakeAdminUserPassword`.
6. Geben Sie für `DataAnalystUserName` und `DataAnalystUserPassword` den gewünschten Benutzernamen und das Kennwort für den IAM-Benutzer von Data Analyst ein.
7. Geben Sie für `DataLakeBucketName` den Namen Ihres Data Lake-Buckets ein. Dieser Name muss weltweit eindeutig sein.
8. Behalten Sie im Feld `DatabaseName` die Standardwerte bei.
9. Geben Sie für `AthenaQueryResultS3BucketName` den Namen des Amazon S3 S3-Buckets ein, in dem die Amazon Athena Athena-Abfrageergebnisse gespeichert werden. Wenn Sie noch keinen haben, [erstellen Sie einen Amazon S3 S3-Bucket](#).
10. Wählen Sie Weiter aus.
11. Wählen Sie auf der nächsten Seite Weiter aus.

12. Überprüfen Sie die Details auf der letzten Seite und wählen Sie Ich bestätige, dass AWS CloudFormation möglicherweise IAM-Ressourcen erstellt werden.
13. Wählen Sie Erstellen aus.

Die Erstellung des Stacks kann bis zu einer Minute dauern.

 Note

Löschen Sie nach Abschluss des Tutorials den Stack CloudFormation , um Gebühren zu vermeiden. Stellen Sie sicher, dass die Ressourcen im Ereignisstatus für den Stack erfolgreich gelöscht wurden.

Schritt 2: Voraussetzungen für die gemeinsame Nutzung von Konten bei Lake Formation

Bevor Ressourcen mit Lake Formation gemeinsam genutzt werden können, müssen Voraussetzungen sowohl für die tagbasierte Zugriffskontrollmethode als auch für die benannte Ressourcenmethode erfüllt sein.

Erfüllen Sie die Voraussetzungen für die tagbasierte Zugriffskontrolle und die kontenübergreifende gemeinsame Nutzung von Daten

- Weitere Informationen zu den Anforderungen für die kontenübergreifende gemeinsame Nutzung von Daten finden Sie im [Voraussetzungen](#) Abschnitt des Kapitels zur kontenübergreifenden Datenfreigabe.

Um Datenkatalogressourcen mit Version 3 oder höher der Einstellungen für die kontenübergreifende Version gemeinsam nutzen zu können, benötigt der Gewährer die in der AWS verwalteten Richtlinie `AWSLakeFormationCrossAccountManager` definierten IAM-Berechtigungen in Ihrem Konto.

Wenn Sie Version 1 oder Version 2 der Einstellungen für die kontenübergreifende Version verwenden, müssen Sie der Datenkatalog-Ressourcenrichtlinie im Produzentenkonto das folgende JSON Berechtigungsobjekt hinzufügen, bevor Sie die tagbasierte Zugriffssteuerungsmethode verwenden können, um kontenübergreifenden Zugriff auf Ressourcen zu gewähren. Dadurch erhält das Verbraucherkonto die Erlaubnis, auf den Datenkatalog zuzugreifen, wenn dies `glue:EvaluatedByLakeFormationTags` zutrifft. Diese

Bedingung gilt auch für Ressourcen, für die Sie die Erlaubnis erteilt haben, Lake Formation Formation-Berechtigungs-Tags für das Konto des Verbrauchers zu verwenden. Diese Richtlinie ist für jede Richtlinie erforderlich AWS-Konto , für die Sie Berechtigungen erteilen.

Die folgende Richtlinie muss sich in einem Statement Element befinden. Wir besprechen die vollständige IAM-Richtlinie im nächsten Abschnitt.

```
{
  "Effect": "Allow",
  "Action": [
    "glue:*"
  ],
  "Principal": {
    "AWS": [
      "consumer-account-id"
    ]
  },
  "Resource": [
    "arn:aws:glue:region:account-id:table/*",
    "arn:aws:glue:region:account-id:database/*",
    "arn:aws:glue:region:account-id:catalog"
  ],
  "Condition": {
    "Bool": {
      "glue:EvaluatedByLakeFormationTags": true
    }
  }
}
```

Vollständige Voraussetzungen für die kontenübergreifende gemeinsame Nutzung der Methode „Benannte Ressourcen“

1. Wenn es in Ihrem Konto keine Datenkatalog-Ressourcenrichtlinie gibt, werden die von Ihnen gewährten kontoübergreifenden Zuschüsse von Lake Formation wie gewohnt durchgeführt. Wenn jedoch eine Datenkatalog-Ressourcenrichtlinie existiert, müssen Sie dieser die folgende Erklärung hinzufügen, damit Ihre kontoübergreifenden Zuschüsse erfolgreich sind, wenn sie mit der benannten Ressourcenmethode gewährt werden. Wenn Sie nur die benannte Ressourcenmethode oder nur die tagbasierte Zugriffskontrollmethode verwenden möchten,

können Sie diesen Schritt überspringen. In diesem Tutorial evaluieren wir beide Methoden und müssen die folgende Richtlinie hinzufügen.

Die folgende Richtlinie muss sich in einem Statement Element befinden. Wir besprechen die vollständige IAM-Richtlinie im nächsten Abschnitt.

```
{
    "Effect": "Allow",
    "Action": [
        "glue:ShareResource"
    ],
    "Principal": {
        "Service": "ram.amazonaws.com"
    },
    "Resource": [
        "arn:aws:glue:region:account-id:table/*/*",
        "arn:aws:glue:region:account-id:database/*",
        "arn:aws:glue:region:account-id:catalog"
    ]
}
```

2. Fügen Sie als Nächstes die AWS Glue Data Catalog Ressourcenrichtlinie mithilfe von AWS Command Line Interface (AWS CLI) hinzu.

Wenn Sie kontenübergreifende Berechtigungen sowohl mithilfe der tagbasierten Zugriffskontrollmethode als auch der benannten Ressourcenmethode gewähren, müssen Sie das `EnableHybrid` Argument auf „true“ setzen, wenn Sie die vorherigen Richtlinien hinzufügen. Weil diese Option derzeit nicht auf der Konsole unterstützt wird und Sie die `glue:PutResourcePolicy` API und verwenden müssen. AWS CLI

Erstellen Sie zunächst ein Richtlinienokument (z. B. `policy.json`) und fügen Sie die beiden vorherigen Richtlinien hinzu. *consumer-account-id* Ersetzen Sie es durch die Angabe *account ID* des AWS-Konto Empfängers des Zuschusses, *region* durch die Region des Datenkatalogs, die die Datenbanken und Tabellen enthält, für die Sie Berechtigungen gewähren, und *account-id* durch die AWS-Konto Producer-ID.

Geben Sie den folgenden AWS CLI Befehl ein. *glue-resource-policy* Ersetzen Sie durch die richtigen Werte (z. B. `file: //policy.json`).


```
aws glue put-resource-policy --policy-in-json glue-resource-policy --enable-hybrid  
TRUE
```

Weitere Informationen finden Sie unter [put-resource-policy](#).

Schritt 3: Implementieren Sie die kontenübergreifende gemeinsame Nutzung mithilfe der tagbasierten Zugriffskontrollmethode

In diesem Abschnitt führen wir Sie durch die folgenden allgemeinen Schritte:

1. Definieren Sie ein LF-Tag.
2. Weisen Sie der Zielressource das LF-Tag zu.
3. Erteilen Sie dem Verbraucherkonto LF-Tag-Berechtigungen.
4. Erteilen Sie dem Verbraucherkonto Datenberechtigungen.
5. Widerrufen Sie optional die IAMAllowedPrincipals Berechtigungen für die Datenbank, Tabellen und Spalten.
6. Erstellen Sie einen Ressourcenlink zu der gemeinsam genutzten Tabelle.
7. Erstellen Sie ein LF-Tag und weisen Sie es der Zieldatenbank zu.
8. Erteilen Sie dem Verbraucherkonto LF-Tag-Datenberechtigungen.

Definieren Sie ein LF-Tag

Note

Wenn Sie mit Ihrem Produzentenkonto angemeldet sind, melden Sie sich ab, bevor Sie die folgenden Schritte ausführen.

1. Melden Sie sich als Data Lake-Administrator unter beim Produzentenkonto an <https://console.aws.amazon.com/lakeformation/>. Verwenden Sie die Producer-Kontonummer, den IAM-Benutzernamen (die Standardeinstellung ist `DataLakeAdminProducer`) und das Passwort, die Sie bei der CloudFormation Stack-Erstellung angegeben haben.

2. Wählen Sie in der Lake Formation Formation-Konsole (<https://console.aws.amazon.com/lakeformation/>) im Navigationsbereich unter Berechtigungen die Optionen LF-Tags and Permissions aus.
3. Wählen Sie „LF-Tag hinzufügen“.

Weisen Sie der Zielressource das LF-Tag zu

Weisen Sie der Zielressource das LF-Tag zu und gewähren Sie einem anderen Konto Datenberechtigungen

Als Data Lake-Administrator können Sie Tags an Ressourcen anhängen. Wenn Sie beabsichtigen, eine separate Rolle zu verwenden, müssen Sie der separaten Rolle möglicherweise Berechtigungen zum Beschreiben und Anhängen erteilen.

1. Wählen Sie im Navigationsbereich unter Datenkatalog die Option Datenbanken aus.
2. Wählen Sie die Zieldatenbank aus (`lakeformation_tutorial_cross_account_database_tbac`) und klicken Sie im Menü Aktionen auf LF-Tags bearbeiten.

In diesem Tutorial weisen Sie einer Datenbank ein LF-Tag zu, Sie können aber auch Tabellen und Spalten LF-Tags zuweisen.

3. Wählen Sie Neues LF-Tag zuweisen.
4. Fügen Sie den Schlüssel `Confidentiality` und den Wert hinzu. `public`
5. Wählen Sie Speichern.

Erteilen Sie dem Kundenkonto die LF-Tag-Erlaubnis

Erteilen Sie dem Verbraucherkonto, das sich immer noch im Herstellerkonto befindet, Berechtigungen für den Zugriff auf das LF-Tag.

1. Wählen Sie im Navigationsbereich unter Berechtigungen die Option LF-Tags und Berechtigungen aus.
2. Wählen Sie die Registerkarte LF-Tags und wählen Sie den Schlüssel und die Werte des LF-Tags aus, das mit dem Kundenkonto geteilt wird (Schlüssel und Wert). **Confidentiality** `public`
3. Klicken Sie auf Gewähren von Berechtigungen aus.
4. Wählen Sie als Berechtigungstyp die Option LF-Tag-Schlüssel-Wert-Paar-Berechtigungen aus.

5. Wählen Sie für Principals die Option Externe Konten aus.
6. Geben Sie die AWS-Konto Ziel-ID ein.

AWS-Konten innerhalb derselben Organisation werden automatisch angezeigt. Andernfalls müssen Sie die AWS-Konto ID manuell eingeben.

7. Wählen Sie unter Berechtigungen die Option Describe aus.

Dies sind die Berechtigungen, die dem Verbraucherkonto erteilt wurden. Erteilbare Berechtigungen sind Berechtigungen, die das Verbraucherkonto anderen Prinzipalen gewähren kann.

8. Wählen Sie Grant (Erteilen).

Zu diesem Zeitpunkt sollte der Data Lake-Administrator in der Lage sein, das Policy-Tag, das über die Lake Formation Formation-Konsole des Verbraucherkontos gemeinsam genutzt wird, unter Berechtigungen, LF-Tags und Berechtigungen zu finden.

Erteilen Sie dem Verbraucherkonto eine Datenberechtigung

Wir werden nun Datenzugriff auf das Verbraucherkonto gewähren, indem wir einen LF-Tag-Ausdruck angeben und dem Verbraucherkonto Zugriff auf alle Tabellen oder Datenbanken gewähren, die dem Ausdruck entsprechen..

1. Wählen Sie im Navigationsbereich unter Berechtigungen und Data Lake-Berechtigungen die Option Grant aus.
2. Wählen Sie für Principals die Option Externe Konten aus und geben Sie die AWS-Konto Ziel-ID ein.
3. Wählen Sie für LF-Tags oder Katalogressourcen den Schlüssel und die Werte des LF-Tags aus, das mit dem Kundenkonto geteilt wird (Schlüssel und Wert). **Confidentiality** public
4. Wählen Sie für Berechtigungen unter Ressourcen, denen LF-Tags zugeordnet sind (empfohlen) die Option LF-Tag hinzufügen aus.
5. Wählen Sie den Schlüssel und den Wert des Tags aus, das mit dem Kundenkonto geteilt wird (Schlüssel Confidentiality und Wert). public
6. Wählen Sie für Datenbankberechtigungen unter Datenbankberechtigungen die Option Beschreiben aus, um Zugriffsberechtigungen auf Datenbankebene zu gewähren.
7. Der Data Lake-Administrator für Verbraucher sollte das Policy-Tag, das über das Verbraucherkonto geteilt wird, in der Lake Formation Formation-Konsole unter Berechtigungen

<https://console.aws.amazon.com/lakeformation/>, Administratorrollen und Aufgaben, LF-Tags finden können.

8. Wählen Sie unter Erteilbare Berechtigungen die Option Beschreiben aus, damit das Verbraucherkonto seinen Benutzern Berechtigungen auf Datenbankebene gewähren kann.
9. Wählen Sie für Tabellen- und Spaltenberechtigungen unter Tabellenberechtigungen die Option Auswählen und Beschreiben aus.
10. Wählen Sie unter Erteilbare Berechtigungen die Option Auswählen und Beschreiben aus.
11. Wählen Sie Grant (Erteilen).

Widerrufen Sie die Berechtigung für **IAMAllowedPrincipals** die Datenbank, Tabellen und Spalten (optional).

Ganz am Anfang dieses Tutorials haben Sie die Lake Formation Data Catalog-Einstellungen geändert. Wenn Sie diesen Teil übersprungen haben, ist dieser Schritt erforderlich. Wenn Sie Ihre Lake Formation Data Catalog-Einstellungen geändert haben, können Sie diesen Schritt überspringen.

In diesem Schritt müssen wir die standardmäßige Super-Berechtigung für die Datenbank oder Tabelle widerrufen. IAMAllowedPrincipals Details dazu finden Sie unter [Schritt 4: Stellen Sie Ihre Datenspeicher auf das Lake Formation Formation-Berechtigungsmodell um](#).

Bevor Sie die Genehmigung für widerrufenIAMAllowedPrincipals, stellen Sie sicher, dass Sie bestehenden IAM-Prinzipalen die erforderliche Genehmigung über Lake Formation erteilt haben. Dies umfasst drei Schritte:

1. Fügen Sie dem IAM-Zielbenutzer oder der Zielrolle mit der GetDataAccess Aktion Lake Formation (mit IAM-Richtlinie) eine IAM-Berechtigung hinzu.
2. Erteilen Sie dem Ziel-IAM-Benutzer oder der Zielrolle Lake Formation Formation-Datenberechtigungen (ändern, auswählen usw.).
3. Widerrufen Sie anschließend die Berechtigungen fürIAMAllowedPrincipals. Andernfalls können bestehende IAM-Prinzipale nach dem Widerruf der Berechtigungen für IAMAllowedPrincipals möglicherweise nicht mehr auf die Zieldatenbank oder den Datenkatalog zugreifen.

Der Widerruf der Super-Berechtigung für IAMAllowedPrincipals ist erforderlich, wenn Sie das Lake Formation Formation-Berechtigungsmodell (anstelle des IAM-Richtlinienmodells) anwenden möchten, um den Benutzerzugriff innerhalb eines einzelnen Kontos oder zwischen mehreren Konten mithilfe des Lake Formation Formation-Berechtigungsmodells zu verwalten.

Sie müssen die Erlaubnis `IAMAllowedPrincipals` für andere Tabellen nicht widerrufen, für die Sie das traditionelle IAM-Richtlinienmodell beibehalten möchten.

Zu diesem Zeitpunkt sollte der Data Lake-Administrator des Verbraucherkontos in der Lage sein, die Datenbank und die Tabelle, die über das Verbraucherkonto gemeinsam genutzt werden <https://console.aws.amazon.com/lakeformation/>, in der Lake Formation Konsole unter Data Catalog unter Datenbanken zu finden. Falls nicht, überprüfen Sie, ob die folgenden Komponenten ordnungsgemäß konfiguriert sind:

1. Den Zieldatenbanken und -tabellen werden das richtige Policy-Tag und die richtigen Werte zugewiesen.
2. Dem Verbraucherkonto werden die richtigen Tagberechtigungen und Datenberechtigungen zugewiesen.
3. Widerrufen Sie die Standard-Superberechtigung für die Datenbank oder Tabelle.
`IAMAllowedPrincipals`

Erstellen Sie einen Ressourcenlink zu der gemeinsam genutzten Tabelle

Wenn eine Ressource von mehreren Konten gemeinsam genutzt wird und die gemeinsam genutzten Ressourcen nicht in den Datenkatalog der Verbraucherkonten aufgenommen werden. Um sie verfügbar zu machen und die zugrunde liegenden Daten einer gemeinsam genutzten Tabelle mithilfe von Diensten wie Athena abzufragen, müssen wir einen Ressourcenlink zu der gemeinsam genutzten Tabelle erstellen. Ein Ressourcenlink ist ein Datenkatalog-Objekt, bei dem es sich um einen Link zu einer lokalen oder gemeinsam genutzten Datenbank oder Tabelle handelt. Details hierzu finden Sie unter [Ressourcenlinks erstellen](#). Durch das Erstellen einer Ressourcenverknüpfung können Sie:

- Weisen Sie einer Datenbank oder Tabelle einen anderen Namen zu, der Ihren Richtlinien zur Benennung von Ressourcen im Datenkatalog entspricht.
- Verwenden Sie Dienste wie Athena und Redshift Spectrum, um gemeinsam genutzte Datenbanken oder Tabellen abzufragen.

Gehen Sie wie folgt vor, um einen Ressourcenlink zu erstellen:

1. Wenn Sie in Ihrem Kundenkonto angemeldet sind, melden Sie sich ab.
2. Melden Sie sich als Data Lake-Administrator für das Verbraucherkonto an. Verwenden Sie die Benutzerkonto-ID, den IAM-Benutzernamen (Standard `DatalakeAdminConsumer`) und das Passwort, die Sie bei der CloudFormation Stack-Erstellung angegeben haben.

3. Wählen Sie in der Lake Formation Formation-Konsole (<https://console.aws.amazon.com/lakeformation/>) im Navigationsbereich unter Datenkatalog, Datenbanken die gemeinsam genutzte Datenbank `auslakeformation_tutorial_cross_account_database_tbac`.

Wenn Sie die Datenbank nicht sehen, wiederholen Sie die vorherigen Schritte, um zu überprüfen, ob alles richtig konfiguriert ist.

4. Wählen Sie „Tabellen anzeigen“.
5. Wählen Sie die gemeinsam genutzte Tabelle `amazon_reviews_table_tbac`.
6. Wählen Sie im Menü Aktionen die Option Ressourcenlink erstellen aus.
7. Geben Sie unter Name des Ressourcenlinks einen Namen ein (für dieses Tutorial, `amazon_reviews_table_tbac_resource_link`).
8. Wählen Sie unter Datenbank die Datenbank aus, in der der Ressourcenlink erstellt wurde (für diesen Beitrag hat der CloudFormation n-Stack die Datenbank `lakeformation_tutorial_cross_account_database_consumer`).
9. Wählen Sie Erstellen aus.

Der Ressourcenlink wird unter Datenkatalog, Tabellen angezeigt.

Erstellen Sie ein LF-Tag und weisen Sie es der Zieldatenbank zu

Lake Formation-Tags befinden sich im selben Datenkatalog wie die Ressourcen. Das bedeutet, dass im Produzentenkonto erstellte Tags nicht verwendet werden können, wenn Zugriff auf die Ressourcenlinks im Verbraucherkonto gewährt wird. Sie müssen einen separaten Satz von LF-Tags im Verbraucherkonto erstellen, um die auf LF-Tags basierende Zugriffskontrolle bei der gemeinsamen Nutzung der Ressourcenlinks im Verbraucherkonto verwenden zu können.

1. Definieren Sie das LF-Tag im Verbraucherkonto. Für dieses Tutorial verwenden wir Schlüssel `Division` und Werte `salesmarketing`, und `analyst`
2. Weisen Sie der Datenbank, in der der Ressourcenlink erstellt wird `lakeformation_tutorial_cross_account_database_consumer`, `analyst` den LF-Tag-Schlüssel `Division` und den Wert zu.

Erteilen Sie dem Verbraucher die Erlaubnis für LF-Tag-Daten

Erteilen Sie dem Verbraucher als letzten Schritt die Genehmigung für LF-Tag-Daten.

1. Wählen Sie im Navigationsbereich unter Berechtigungen, Data Lake-Berechtigungen die Option Grant aus.
2. Wählen Sie für Principals die Option IAM-Benutzer und -Rollen und dann den Benutzer aus. `DataAnalyst`
3. Wählen Sie für LF-Tags oder Katalogressourcen die Option Ressourcen, denen LF-Tags zugeordnet sind (empfohlen) aus.
4. Wählen Sie „Key Division“ und „Value Analyst“.
5. Wählen Sie für Datenbankberechtigungen unter Datenbankberechtigungen die Option Describe aus.
6. Wählen Sie für Tabellen- und Spaltenberechtigungen unter Tabellenberechtigungen die Option Auswählen und Beschreiben aus.
7. Wählen Sie Grant (Erteilen).
8. Wiederholen Sie diese Schritte für den Benutzer `DataAnalyst`, wobei sich der LF-Tag-Schlüssel `Confidentiality` und der Wert befinden. `public`

Zu diesem Zeitpunkt sollte der Data Analyst-Benutzer im Kundenkonto in der Lage sein, die Datenbank und den Ressourcenlink zu finden und die gemeinsam genutzte Tabelle über die Athena-Konsole unter <https://console.aws.amazon.com/athena/> abzufragen. Falls nicht, überprüfen Sie, ob die folgenden Komponenten ordnungsgemäß konfiguriert sind:

- Der Ressourcenlink wird für die gemeinsam genutzte Tabelle erstellt
- Sie haben dem Benutzer Zugriff auf das vom Producer-Konto gemeinsam genutzte LF-Tag gewährt
- Sie haben dem Benutzer Zugriff auf das LF-Tag gewährt, das dem Ressourcenlink und der Datenbank zugeordnet ist, in der der Ressourcenlink erstellt wurde
- Überprüfen Sie, ob Sie dem Ressourcenlink und der Datenbank, in der der Ressourcenlink erstellt wurde, das richtige LF-Tag zugewiesen haben

Schritt 4: Implementieren Sie die benannte Ressourcenmethode

Um die Methode „Named Resource“ zu verwenden, führen wir Sie durch die folgenden allgemeinen Schritte:

1. Widerrufen Sie optional die Zugriffsrechte für `IAMAllowedPrincipals` die Datenbank, Tabellen und Spalten.

2. Erteilen Sie dem Kundenkonto die Datenberechtigung.
3. Akzeptieren Sie eine gemeinsame Nutzung einer Ressource von AWS Resource Access Manager.
4. Erstellen Sie einen Ressourcenlink für die gemeinsam genutzte Tabelle.
5. Erteilen Sie dem Verbraucher die Datenberechtigung für die gemeinsam genutzte Tabelle.
6. Erteilen Sie dem Verbraucher die Datenberechtigung für den Ressourcenlink.

Widerrufen Sie **IAMAllowedPrincipals** die Berechtigung für die Datenbank, Tabellen und Spalten (optional)

- Ganz am Anfang dieses Tutorials haben wir die Einstellungen für den Lake Formation Data Catalog geändert. Wenn Sie diesen Teil übersprungen haben, ist dieser Schritt erforderlich. Anweisungen finden Sie im optionalen Schritt im vorherigen Abschnitt.

Erteilen Sie dem Kundenkonto die Datenberechtigung

1.

 Note

Wenn Sie als anderer Benutzer beim Produzentenkonto angemeldet sind, melden Sie sich zuerst ab.

Melden Sie sich <https://console.aws.amazon.com/lakeformation/> mit dem Data Lake-Administrator des Producer-Kontos bei der Lake Formation Formation-Konsole an. Verwenden Sie AWS-Konto dabei die ID, den IAM-Benutzernamen (Standard ist `DataLakeAdminProducer`) und das Passwort, die bei der CloudFormation Stack-Erstellung angegeben wurden.

2. Wählen Sie auf der Seite Berechtigungen unter Data Lake-Berechtigungen die Option Grant aus.
3. Wählen Sie unter Principals die Option Externe Konten aus und geben Sie eine AWS-Konto IDs oder mehrere AWS Organisationen IDs ein. Weitere Informationen finden Sie unter: [AWS Organizations](#).

Organizations, zu denen das Produzentenkonto gehört und zu AWS-Konten derselben Organisation gehört, werden automatisch angezeigt. Andernfalls geben Sie die Konto- oder Organisations-ID manuell ein.

4. Wählen Sie für LF-Tags oder Katalogressourcen. `Named data catalog resources`

5. Wählen Sie unter Datenbanken die Datenbank aus.
`lakeformation_tutorial_cross_account_database_named_resource`
6. Wählen Sie LF-Tag hinzufügen.
7. Wählen Sie unter Tabellen die Option Alle Tabellen aus.
8. Wählen Sie für Tabellenspaltenberechtigungen die Option Auswählen und unter Tabellenberechtigungen die Option Beschreiben aus.
9. Wählen Sie unter Erteilbare Berechtigungen die Option Auswählen und beschreiben aus.
10. Wählen Sie optional für Datenberechtigungen die Option Einfacher spaltenbasierter Zugriff aus, wenn eine Berechtigungsverwaltung auf Spaltenebene erforderlich ist.
11. Wählen Sie Grant (Erteilen).

Wenn Sie die Berechtigung für nicht widerrufen haben **IAMAllowedPrincipals**, wird die Fehlermeldung „Berechtigungen nicht erteilt“ angezeigt. Zu diesem Zeitpunkt sollten Sie unter Berechtigungen, Datenberechtigungen die Zieltabelle sehen, AWS RAM über die für das Verbraucherkonto freigegeben wurde.

Akzeptieren Sie eine gemeinsame Nutzung einer Ressource von AWS RAM

 Note

Dieser Schritt ist nur für die gemeinsame Nutzung AWS-Konto auf der Grundlage von Organisationen erforderlich, nicht für die gemeinsame Nutzung innerhalb einer Organisation.

1. Melden Sie sich mit dem Data Lake-Administrator des Verbraucherkontos <https://console.aws.amazon.com/connect/> mit dem IAM-Benutzernamen (Standard ist `DatalakeAdminConsumer`) und dem Passwort, das Sie bei der Stack-Erstellung angegeben haben, bei der AWS CloudFormation Konsole an.
2. Wählen Sie auf der AWS RAM Konsole im Navigationsbereich unter Für mich freigegeben, Ressourcenfreigaben die gemeinsam genutzte Lake Formation Formation-Ressource aus. Der Status sollte „Ausstehend“ lauten.
3. Wählen Sie Aktion und Grant aus.
4. Bestätigen Sie die Ressourcendetails und wählen Sie „Ressourcenfreigabe akzeptieren“.

Zu diesem Zeitpunkt sollte der Data Lake-Administrator des Benutzerkontos in der Lage sein, die gemeinsam genutzte Ressource in der Lake Formation Formation-Konsole (<https://console.aws.amazon.com/lakeformation/>) unter Datenkatalog, Datenbanken zu finden.

Erstellen Sie einen Ressourcenlink für die gemeinsam genutzte Tabelle

- Folgen Sie den Anweisungen in [Schritt 3: Implementieren Sie die kontenübergreifende gemeinsame Nutzung mithilfe der tagbasierten Zugriffskontrollmethode](#) (Schritt 6), um einen Ressourcenlink für eine gemeinsam genutzte Tabelle zu erstellen. Benennen Sie den Ressourcenlink `amazon_reviews_table_named_resource_resource_link`. Erstellen Sie den Ressourcenlink in der Datenbank `lakeformation_tutorial_cross_account_database_consumer`.

Erteilen Sie dem Benutzer die Datenberechtigung für die gemeinsam genutzte Tabelle

Gehen Sie wie folgt vor, um dem Verbraucher die Datenberechtigung für die gemeinsam genutzte Tabelle zu erteilen:

1. Wählen Sie auf der Lake Formationconsole (<https://console.aws.amazon.com/lakeformation/>) unter Berechtigungen und Data Lake-Berechtigungen die Option Grant aus.
2. Wählen Sie für Principals die Option IAM-Benutzer und -Rollen und dann den Benutzer aus. `DataAnalyst`
3. Wählen Sie für LF-Tags oder Katalogressourcen die Option Benannte Datenkatalogressourcen aus.
4. Wählen Sie unter Datenbanken die Datenbank aus. `lakeformation_tutorial_cross_account_database_named_resource` Wenn Sie die Datenbank nicht in der Dropdownliste sehen, wählen Sie Mehr laden aus.
5. Wählen Sie unter Tabellen die Tabelle `amazon_reviews_table_named_resource`.
6. Wählen Sie für Tabellen- und Spaltenberechtigungen unter Tabellenberechtigungen die Option Auswählen und Beschreiben aus.
7. Wählen Sie Grant (Erteilen).

Erteilen Sie dem Verbraucher die Datenberechtigung für den Ressourcenlink

Sie müssen dem Data Lake-Benutzer nicht nur die Berechtigung für den Zugriff auf die gemeinsam genutzte Tabelle gewähren, sondern auch dem Data Lake-Benutzer die Berechtigung für den Zugriff auf den Ressourcenlink erteilen.

1. Wählen Sie in der Lake Formation Formation-Konsole (<https://console.aws.amazon.com/lakeformation/>) unter Berechtigungen, Data Lake-Berechtigungen die Option Grant aus.
2. Wählen Sie für Principals die Option IAM-Benutzer und -Rollen und dann den Benutzer aus.
`DataAnalyst`
3. Wählen Sie für LF-Tags oder Katalogressourcen die Option Benannte Datenkatalogressourcen aus.
4. Wählen Sie unter Datenbanken die Datenbank aus.
`lakeformation_tutorial_cross_account_database_consumer` Wenn Sie die Datenbank nicht in der Dropdownliste sehen, wählen Sie Mehr laden aus.
5. Wählen Sie unter Tabellen die Tabelle
`ausamazon_reviews_table_named_resource_resource_link`.
6. Wählen Sie für Berechtigungen für Ressourcenlinks die Option Beschreiben unter Berechtigungen für Ressourcenlinks aus.
7. Wählen Sie Grant (Erteilen).

Zu diesem Zeitpunkt sollte der Data Analyst-Benutzer im Verbraucherkonto in der Lage sein, die Datenbank und den Ressourcenlink zu finden und die gemeinsam genutzte Tabelle über die Athena-Konsole abzufragen.

Falls nicht, überprüfen Sie, ob die folgenden Komponenten ordnungsgemäß konfiguriert sind:

- Der Ressourcenlink wird für die gemeinsam genutzte Tabelle erstellt
- Sie haben dem Benutzer Zugriff auf die vom Producer-Konto gemeinsam genutzte Tabelle gewährt
- Sie haben dem Benutzer Zugriff auf den Ressourcenlink und die Datenbank gewährt, für die der Ressourcenlink erstellt wurde

Schritt 5: AWS Ressourcen bereinigen

Um zu verhindern, dass Ihnen unerwünschte Kosten entstehen AWS-Konto, können Sie die AWS Ressourcen löschen, die Sie für dieses Tutorial verwendet haben.

1. Melden Sie sich <https://console.aws.amazon.com/lakeformation/> mit dem Produzentenkonto bei der Lake Formation Formation-Konsole an und löschen oder ändern Sie Folgendes:
 - AWS Resource Access Manager gemeinsame Nutzung von Ressourcen
 - Lake Formation Stichworte
 - CloudFormation stapeln
 - Lake Formation Formation-Einstellungen
 - AWS Glue Data Catalog
2. Melden Sie sich <https://console.aws.amazon.com/lakeformation/> mit dem Kundenkonto bei der Lake Formation Formation-Konsole an und löschen oder ändern Sie Folgendes:
 - Lake Formation Stichworte
 - CloudFormation stapeln

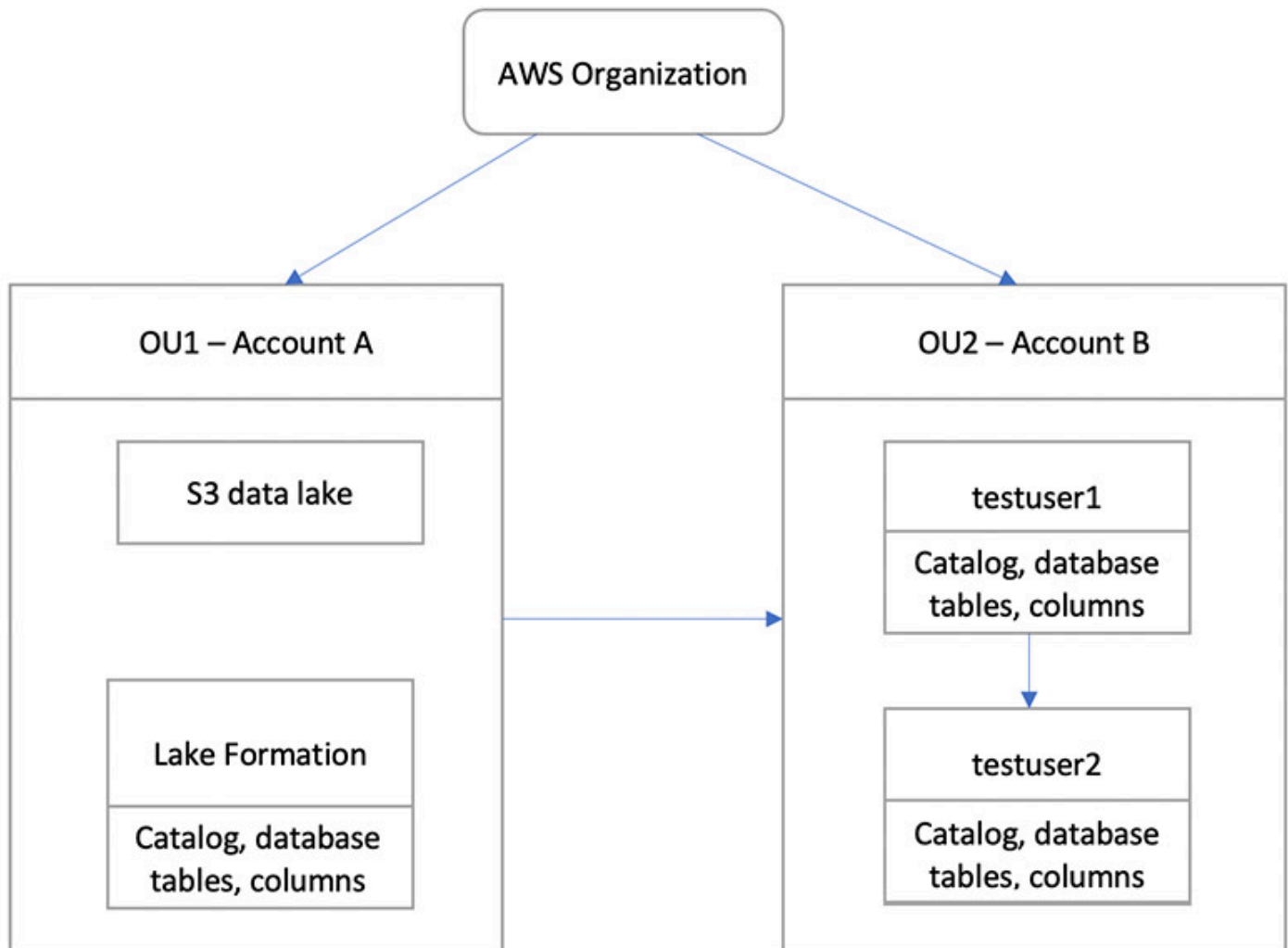
Gemeinsame Nutzung eines Data Lakes mithilfe der feinkörnigen Zugriffskontrolle von Lake Formation

Dieses Tutorial enthält step-by-step Anweisungen, wie Sie mithilfe von Lake Formation schnell und einfach Datensätze gemeinsam nutzen können, wenn Sie mehrere AWS-Konten mit AWS Organizations verwalten. Sie definieren detaillierte Berechtigungen, um den Zugriff auf sensible Daten zu kontrollieren.

Die folgenden Verfahren zeigen auch, wie ein Data Lake-Administrator von Konto A differenzierten Zugriff für Konto B bereitstellen kann und wie ein Benutzer in Konto B, der als Data Steward fungiert, anderen Benutzern in seinem Konto differenzierten Zugriff auf die gemeinsam genutzte Tabelle gewähren kann. Data Stewards in jedem Konto können den Zugriff unabhängig voneinander an ihre eigenen Benutzer delegieren, sodass jedes Team oder jeder Geschäftsbereich (LOB) Autonomie erhält.

Der Anwendungsfall geht davon aus, dass Sie Ihre verwenden, um Ihre AWS Organizations zu verwalten. AWS-Konten Der Benutzer von Konto A in einer Organisationseinheit (OU1) gewährt

Benutzern von Konto B in Zugriff OU2. Sie können denselben Ansatz verwenden, wenn Sie Organizations nicht verwenden, z. B. wenn Sie nur wenige Konten haben. Das folgende Diagramm veranschaulicht die detaillierte Zugriffskontrolle von Datensätzen in einem Data Lake. Der Data Lake ist in Konto A verfügbar. Der Data Lake-Administrator von Konto A bietet detaillierten Zugriff auf Konto B. Das Diagramm zeigt auch, dass ein Benutzer von Konto B einem anderen Benutzer in Konto B Zugriff auf die Data-Lake-Tabelle von Konto A auf Spaltenebene gewährt.



Themen

- [Zielgruppe](#)
- [Voraussetzungen](#)
- [Schritt 1: Stellen Sie einen detaillierten Zugriff auf ein anderes Konto bereit](#)
- [Schritt 2: Bieten Sie einem Benutzer im selben Konto differenzierten Zugriff](#)

Zielgruppe

Dieses Tutorial richtet sich an Datenverwalter, Dateningenieure und Datenanalysten. In der folgenden Tabelle sind die Rollen aufgeführt, die in diesem Tutorial verwendet werden:

Rolle	Beschreibung
IAM-Administrator	Benutzer, der über die AWS verwaltete Richtlinie verfügt: <code>AdministratorAccess</code> .
Data Lake-Administrator	Benutzer, dem die Rolle „AWS Verwaltete Richtlinie:“ <code>AWSLakeFormationDataAdmin</code> zugewiesen ist.
Datenanalyst	Benutzer, dem die AWS verwaltete Richtlinie: <code>AmazonAthenaFullAccess</code> angehängt ist.

Voraussetzungen

Bevor Sie mit diesem Tutorial beginnen, benötigen Sie eine AWS-Konto , mit der Sie sich als Administratorbenutzer mit den richtigen Berechtigungen anmelden können. Weitere Informationen finden Sie unter [Erledigen Sie die Aufgaben zur AWS Erstkonfiguration](#).

In der Anleitung wird davon ausgegangen, dass Sie mit IAM vertraut sind. Informationen zu IAM finden Sie im [IAM-Benutzerhandbuch](#).

Für dieses Tutorial benötigen Sie die folgenden Ressourcen:

- Zwei Organisationseinheiten:
 - OU1 — Enthält Konto A
 - OU2 — Enthält Konto B
- Ein Amazon S3 S3-Data-Lake-Standort (Bucket) in Konto A.
- Ein Data Lake-Administratorbenutzer in Konto A. Sie können einen Data Lake-Administrator mithilfe der Lake Formation Formation-Konsole (<https://console.aws.amazon.com/lakeformation/>) oder mithilfe der `PutDataLakeSettings` Lake Formation Formation-API erstellen.
- Lake Formation ist in Konto A konfiguriert, und der Amazon S3 S3-Data-Lake-Standort, der bei Lake Formation in Konto A registriert ist.

- Zwei Benutzer in Konto B mit den folgenden IAM-verwalteten Richtlinien:
 - testuser1 — hat die AWS verwalteten Richtlinien angehängt. `AWSLakeFormationDataAdmin`
 - testuser2 — Die verwaltete Richtlinie ist AWS angehängt. `AmazonAthenaFullAccess`
- Eine Datenbank-Testdb in der Lake Formation Formation-Datenbank für Account B.

Schritt 1: Stellen Sie einen detaillierten Zugriff auf ein anderes Konto bereit

Erfahren Sie, wie ein Data Lake-Administrator von Konto A differenzierten Zugriff für Konto B bereitstellt.

Gewähren Sie einem anderen Konto differenzierten Zugriff

1. Melden Sie sich AWS-Managementkonsole <https://console.aws.amazon.com/connect/> bei Konto A als Data Lake-Administrator an.
2. Öffnen Sie die Lake Formation Formation-Konsole (<https://console.aws.amazon.com/lakeformation/>) und wählen Sie Get started.
3. wählen Sie im Navigationsbereich Datenbanken aus.
4. Wählen Sie Create database (Datenbank erstellen) aus.
5. Wählen Sie im Abschnitt Datenbankdetails die Option Datenbank aus.
6. Geben Sie unter Name einen Namen ein (für dieses Tutorial verwenden wir `samp1edb01`).
7. Stellen Sie sicher, dass die Option Nur IAM-Zugriffskontrolle für neue Tabellen in dieser Datenbank verwenden nicht ausgewählt ist. Wenn diese Option nicht ausgewählt ist, können wir den Zugriff von Lake Formation aus kontrollieren.
8. Wählen Sie Datenbank erstellen aus.
9. Wählen Sie auf der Seite Datenbanken Ihre Datenbank `samp1edb01` aus.
10. Wählen Sie im Menü Aktionen die Option Grant aus.
11. Wählen Sie im Abschnitt Berechtigungen gewähren die Option Externes Konto aus.
12. Geben Sie für AWS-Konto ID oder AWS Organisations-ID die Konto-ID für Konto B unter ein OU2.
13. Wählen Sie für Tabelle die Tabelle aus, auf die Konto B Zugriff haben soll (für diesen Beitrag verwenden wir `Tabelleacc_a_area`). Optional können Sie Zugriff auf Spalten in der Tabelle gewähren, was wir in diesem Beitrag tun.
14. Wählen Sie unter Spalten einbeziehen die Spalten aus, auf die Konto B Zugriff haben soll (für diesen Beitrag gewähren wir Berechtigungen für Typ, Namen und Identifikatoren).

15. Wählen Sie für Spalten die Option Spalten einbeziehen aus.
16. Wählen Sie für Tabellenberechtigungen die Option Auswählen aus.
17. Wählen Sie für Erteilbare Berechtigungen die Option Auswählen aus. Erteilbare Berechtigungen sind erforderlich, damit Administratorbenutzer in Konto B anderen Benutzern in Konto B Berechtigungen gewähren können.
18. Wählen Sie Grant (Erteilen).
19. Wählen Sie im Navigationsbereich Tables (Tabellen) aus.
20. Im Abschnitt AWS-Konten und AWS Organisationen mit Zugriff wurde möglicherweise eine aktive Verbindung angezeigt.

Erstellen Sie einen Ressourcenlink

Integrierte Dienste wie Amazon Athena können nicht direkt kontenübergreifend auf Datenbanken oder Tabellen zugreifen. Daher müssen Sie einen Ressourcenlink erstellen, damit Athena auf Ressourcenlinks in Ihrem Konto zu Datenbanken und Tabellen in anderen Konten zugreifen kann. Erstellen Sie einen Ressourcenlink zur Tabelle (acc_a_area), damit Benutzer von Account B ihre Daten mit Athena abfragen können.

1. Melden Sie sich in der AWS Konsole unter <https://console.aws.amazon.com/connect/> in Konto B an alstestuser1.
2. Wählen Sie in der Lake Formation Formation-Konsole (<https://console.aws.amazon.com/lakeformation/>) im Navigationsbereich die Option Tabellen aus. Sie sollten die Tabellen sehen, auf die Konto A Zugriff gewährt hat.
3. Wählen Sie die acc_a_area Tabelle aus.
4. Wählen Sie im Menü Aktionen die Option Ressourcenlink erstellen aus.
5. Geben Sie unter Name des Ressourcenlinks einen Namen ein (für dieses Tutorial, acc_a_area_r1).
6. Wählen Sie für Datenbank Ihre Datenbank (testdb) aus.
7. Wählen Sie Create (Erstellen) aus.
8. Wählen Sie im Navigationsbereich Tables (Tabellen) aus.
9. Wählen Sie die acc_b_area_r1 Tabelle aus.
10. Wählen Sie im Menü Aktionen die Option Daten anzeigen aus.

Sie werden zur Athena-Konsole weitergeleitet, wo Sie die Datenbank und die Tabelle sehen sollten.

Sie können jetzt eine Abfrage in der Tabelle ausführen, um den Spaltenwert zu ermitteln, auf den testuser1 von Konto B aus Zugriff gewährt wurde.

Schritt 2: Bieten Sie einem Benutzer im selben Konto differenzierten Zugriff

In diesem Abschnitt wird gezeigt, wie ein Benutzer in Konto B (testuser1), der als Datenverwalter fungiert, einem anderen Benutzer desselben Kontos (testuser2) differenzierten Zugriff auf den Spaltennamen in der gemeinsam genutzten Tabelle gewährt. `aac_b_area_r1`

Gewähren Sie einem Benutzer im selben Konto differenzierten Zugriff

1. Melden Sie sich bei der AWS Konsole unter Konto B <https://console.aws.amazon.com/connect/> an als. testuser1
2. Wählen Sie in der Lake Formation Konsole im Navigationsbereich die Option Tabellen aus.

Sie können über den zugehörigen Ressourcenlink Berechtigungen für eine Tabelle gewähren. Wählen Sie dazu auf der Seite Tabellen den Ressourcenlink `acc_b_area_r1` und dann im Menü Aktionen die Option Auf Ziel gewähren aus.

3. Wählen Sie im Abschnitt Berechtigungen gewähren die Option Mein Konto aus.
4. Wählen Sie für IAM-Benutzer und -Rollen den Benutzer testuser2 aus.
5. Wählen Sie für Spalte den Spaltennamen aus.
6. Wählen Sie für Tabellenberechtigungen die Option Auswählen aus.
7. Wählen Sie Grant (Erteilen).

Wenn Sie einen Ressourcenlink erstellen, können nur Sie ihn anzeigen und darauf zugreifen. Um anderen Benutzern in Ihrem Konto den Zugriff auf den Ressourcenlink zu ermöglichen, müssen Sie Berechtigungen für den Ressourcenlink selbst erteilen. Sie müssen DESCRIBE - oder DROP-Berechtigungen erteilen. Wählen Sie auf der Seite Tabellen erneut Ihre Tabelle aus und klicken Sie im Menü Aktionen auf Grant.

8. Wählen Sie im Abschnitt Berechtigungen gewähren die Option Mein Konto aus.
9. Wählen Sie für IAM-Benutzer und -Rollen den Benutzer testuser2 aus.

10. Wählen Sie für Resource Link Permissions die Option Describe aus.
11. Wählen Sie Grant (Erteilen).
12. Melden Sie sich in der AWS Konsole mit Konto B als antestuser2.

Auf der Athena-Konsole (<https://console.aws.amazon.com/athena/>) sollten Sie die Datenbank und die Tabelle `acc_b_area_r1` sehen. Sie können jetzt eine Abfrage in der Tabelle ausführen, um den Spaltenwert zu sehen, auf den Sie Zugriff `testuser2` haben.

Einsteigen in die Genehmigungen von Lake Formation

AWS Lake Formation verwendet den AWS Glue Data Catalog (Datenkatalog), um Metadaten für die Amazon S3 S3-Data Lakes und externe Datenquellen wie Amazon Redshift in Form von Katalogen, Datenbanken und Tabellen zu speichern. Die Metadaten im Datenkatalog sind in einer dreistufigen Datenhierarchie organisiert, die Kataloge, Datenbanken und Tabellen umfasst. Es organisiert Daten aus verschiedenen Quellen in logischen Containern, den sogenannten Katalogen. Datenbanken sind Sammlungen von Tabellen. Der Datenkatalog enthält auch Ressourcenlinks, d. h. Links zu gemeinsam genutzten Datenbanken und Tabellen in externen Konten, die für den kontenübergreifenden Zugriff auf Daten im Data Lake verwendet werden. Jedes AWS Konto hat einen Datenkatalog pro AWS Region.

Lake Formation bietet ein Rechtemodell für relationale Datenbankverwaltungssysteme (RDBMS), mit dem Sie Zugriff auf Kataloge, Datenbanken, Tabellen und Spalten im Datenkatalog mit zugrunde liegenden Daten in Amazon S3 gewähren oder entziehen können.

Bevor Sie sich mit den Einzelheiten des Lake Formation Formation-Genehmigungsmodells vertraut machen, sollten Sie sich die folgenden Hintergrundinformationen ansehen:

- Von Lake Formation verwaltete Data Lakes befinden sich an bestimmten Orten in Amazon Simple Storage Service (Amazon S3). Der Datenkatalog enthält auch Katalogobjekte. Jeder Katalog stellt Daten aus Quellen wie Amazon Redshift Data Warehouses, Amazon DynamoDB Datenbanken und Datenquellen von Drittanbietern wie Snowflake, MySQL und über 30 externen Datenquellen dar, die über föderierte Konnektoren integriert sind.
- Lake Formation unterhält einen Datenkatalog, der Metadaten zu Quelldaten enthält, die in Ihre Data Lakes importiert werden sollen, wie Daten in Protokollen und relationalen Datenbanken, und zu Daten in Ihren Data Lakes in Amazon S3. Der Datenkatalog enthält auch Metadaten zu Daten aus anderen externen Datenquellen als Amazon S3. Die Metadaten sind in Katalogen, Datenbanken und Tabellen organisiert. Metadatentabellen enthalten Schema, Speicherort, Partitionierung und andere Informationen zu den Daten, die sie repräsentieren. Metadatendatenbanken sind Sammlungen von Tabellen.
- Der Lake Formation Data Catalog ist derselbe Datenkatalog, der von verwendet wird AWS Glue. Sie können AWS Glue Crawler verwenden, um Datenkatalogtabellen zu erstellen, und Sie können Aufträge zum AWS Glue Extrahieren, Transformieren und Laden (ETL) verwenden, um die zugrunde liegenden Daten in Ihren Data Lakes aufzufüllen.

- Die Kataloge, Datenbanken und Tabellen im Datenkatalog werden als Datenkatalogressourcen bezeichnet. Tabellen im Datenkatalog werden als Metadatentabellen bezeichnet, um sie von Tabellen in Datenquellen oder tabellarischen Daten in Amazon S3 zu unterscheiden. Die Daten, auf die die Metadatentabellen in Amazon S3 oder in Datenquellen verweisen, werden als Basisdaten bezeichnet.
- Ein Principal ist ein Benutzer oder eine Rolle, ein Amazon Quick-Benutzer oder eine Gruppe, ein Benutzer oder eine Gruppe, die sich über einen SAML-Anbieter bei Lake Formation authentifiziert, oder für die kontoübergreifende Zugriffskontrolle eine AWS Konto-ID, Organisations-ID oder Organisationseinheit-ID.
- AWS GlueCrawler erstellen Metadatentabellen, aber Sie können Metadatentabellen auch manuell mit der Lake Formation Formation-Konsole, der API oder der AWS Command Line Interface (AWS CLI) erstellen. Beim Erstellen einer Metadatentabelle müssen Sie einen Speicherort angeben. Wenn Sie eine Datenbank erstellen, ist der Speicherort optional. Tabellenspeicherorte können Amazon S3 S3-Standorte oder Datenquellenstandorte wie eine Amazon Relational Database Service (Amazon RDS) -Datenbank sein. Datenbankstandorte sind immer Amazon S3 S3-Standorte.
- Dienste, die in Lake Formation integriert sind, wie Amazon Athena und Amazon Redshift, können auf den Datenkatalog zugreifen, um Metadaten abzurufen und die Autorisierung für laufende Abfragen zu überprüfen. Eine vollständige Liste der integrierten Dienste finden Sie unter. [AWS Serviceintegrationen mit Lake Formation](#)

Topics

- [Überblick über die Genehmigungen für Lake Formation](#)
- [Referenz zu Personas und IAM-Berechtigungen in Lake Formation](#)
- [Ändern der Standardeinstellungen für Ihren Data Lake](#)
- [Implizite Lake Formation Formation-Berechtigungen](#)
- [Referenz zu den Genehmigungen von Lake Formation](#)
- [Integration von IAM Identity Center](#)
- [Hinzufügen eines Amazon S3 S3-Standorts zu Ihrem Data Lake](#)
- [Hybrider Zugriffsmodus](#)
- [Objekte erstellen in AWS Glue Data Catalog](#)
- [Daten mithilfe von Workflows in Lake Formation importieren](#)

Überblick über die Genehmigungen für Lake Formation

Es gibt zwei Haupttypen von Berechtigungen in AWS Lake Formation:

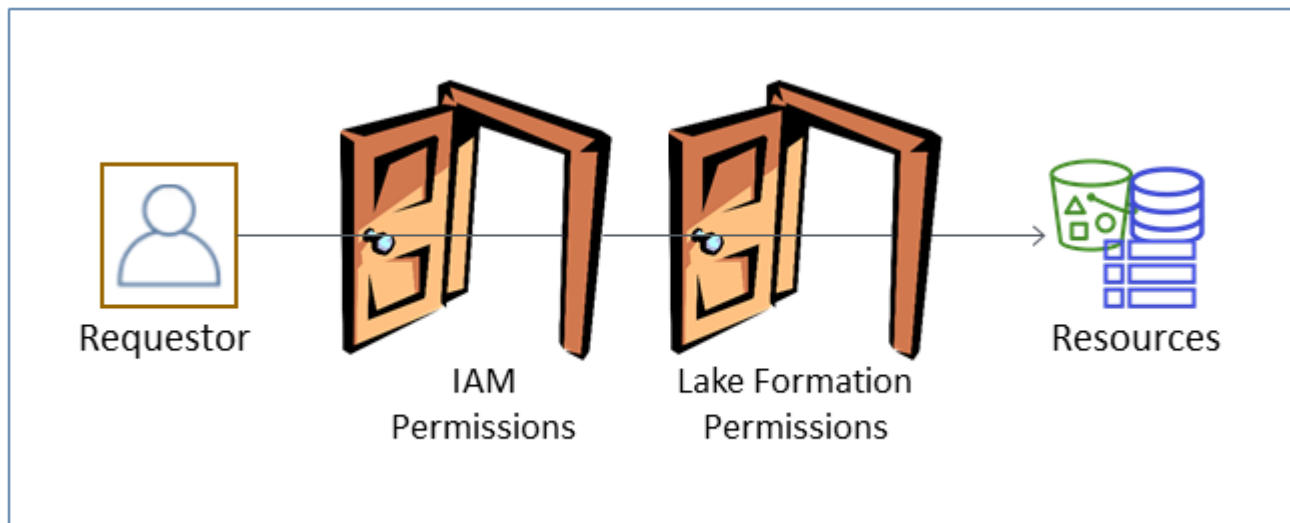
- Zugriff auf Metadaten — Berechtigungen für Datenkatalogressourcen (Datenkatalog-Berechtigungen).

Diese Berechtigungen ermöglichen es Prinzipalen, Metadatendatenbanken und Tabellen im Datenkatalog zu erstellen, zu lesen, zu aktualisieren und zu löschen.

- Zugrundeliegender Datenzugriff — Berechtigungen für Standorte in Amazon Simple Storage Service (Amazon S3) (Datenzugriffsberechtigungen und Datenstandortberechtigungen).
 - Data Lake-Berechtigungen ermöglichen es Prinzipalen, Daten zu lesen und an zugrunde liegende Amazon S3 S3-Standorte zu schreiben — Daten, auf die von Data Catalog-Ressourcen verwiesen wird.
 - Datenstandortberechtigungen ermöglichen es Prinzipalen, Metadatendatenbanken und Tabellen zu erstellen und zu ändern, die auf bestimmte Amazon S3 S3-Standorte verweisen.

Für beide Gebiete verwendet Lake Formation eine Kombination aus Lake Formation Formation-Berechtigungen und AWS Identity and Access Management (IAM) -Berechtigungen. Das IAM-Berechtigungsmodell besteht aus IAM-Richtlinien. Das Lake Formation Formation-Berechtigungsmodell ist als GRANT/REVOKE Befehle im DBMS-Stil implementiert, wie z. `Grant SELECT on tableName to userName`

Wenn ein Principal eine Anfrage für den Zugriff auf Datenkatalogressourcen oder zugrunde liegende Daten stellt, muss er die Berechtigungsprüfungen sowohl von IAM als auch von Lake Formation bestehen, damit die Anfrage erfolgreich ist.



Lake Formation Formations-Berechtigungen kontrollieren den Zugriff auf Datenkatalogressourcen, Amazon S3 S3-Standorte und die zugrunde liegenden Daten an diesen Standorten. IAM-Berechtigungen kontrollieren den Zugriff auf die Lake Formation AWS Glue APIs und die Ressourcen. Obwohl Sie möglicherweise über die Lake Formation Formations-Berechtigung zum Erstellen einer Metadaten-tabelle im Datenkatalog (`CREATE_TABLE`) verfügen, schlägt Ihr Vorgang fehl, wenn Sie nicht über die IAM-Berechtigung für die `glue:CreateTable` API verfügen. (Warum eine `glue`: Erlaubnis? Weil Lake Formation den AWS Glue Datenkatalog verwendet.)

Note

Genehmigungen für Lake Formation gelten nur in der Region, in der sie erteilt wurden.

AWS Lake Formation erfordert, dass jeder Prinzipal (Benutzer oder Rolle) autorisiert ist, Aktionen auf von Lake Formation verwalteten Ressourcen durchzuführen. Einem Principal werden die erforderlichen Autorisierungen vom Data Lake-Administrator oder einem anderen Principal mit den Berechtigungen zur Erteilung von Lake Formation Formations-Berechtigungen erteilt.

Wenn Sie einem Principal eine Lake Formation Formations-Genehmigung erteilen, können Sie optional die Möglichkeit gewähren, diese Berechtigung an einen anderen Principal weiterzugeben.

Sie können die Lake Formation Formations-API, die AWS Command Line Interface (AWS CLI) oder die Seiten Datenberechtigungen und Datenspeicherorte der Lake Formation-Konsole verwenden, um Lake Formation-Berechtigungen zu erteilen oder zu widerrufen.

Methoden für eine differenzierte Zugriffskontrolle

Bei einem Data Lake besteht das Ziel in einer differenzierten Zugriffskontrolle für Daten. In Lake Formation bedeutet dies eine detaillierte Zugriffskontrolle auf Datenkatalogressourcen und Amazon S3 S3-Standorte. Sie können eine detaillierte Zugriffskontrolle mit einer der folgenden Methoden erreichen.

Methode	Genehmigungen für Lake Formation	IAM-Berechtigungen	Kommentare
Methode 1	Öffnen	Feinkörnig	Dies ist die Standardmethode für die Abwärtskompatibilität mit. AWS Glue • Offen bedeutet, dass die Sonderberechtigung der Gruppe gewährt Super wird <code>IAMAllowedPrincipals</code> , die automatisch erstellt <code>IAMAllowedPrincipals</code> wird und alle IAM-Benutzer und -Rollen einschließt, denen aufgrund Ihrer IAM-Richtlinien Zugriff auf Ihre Datenkatalogressourcen gewährt wird. Die Super Berechtigung ermöglicht es einem Prinzipal, jeden unterstützten Lake Formation Vorgang in der Datenbank oder Tabelle durchzuführen, für die sie erteilt wurde. Dadurch wird der Zugriff auf Datenkatalogressourcen und Amazon S3 S3-Standorte ausschließlich durch IAM-Richtlinien gesteuert. Weitere Informationen erhalten Sie unter Ändern der Standardereinstellungen für Ihren Data Lake und AWS Glue Datenberechtigungen für das AWS Lake Formation Modell aktualisieren.

Methode	Genehmigungen für Lake Formation	IAM-Berechtigungen	Kommentare
			• Feinkörnig bedeutet, dass IAM-Richtlinien den gesamten Zugriff auf Datenkatalogressourcen und auf einzelne Amazon S3 S3-Buckets steuern. In der Lake-Formation-Konsole wird diese Methode als Nur IAM-Zugriffskontrolle verwenden angezeigt.

Methode	Genehmigungen für Lake Formation	IAM-Berechtigungen	Kommentare
Methode 2	Fein abgestuft	Grobkörnig	Dies ist die empfohlene Methode. • Detaillierter Zugriff bedeutet, dass einzelnen Prinzipalen eingeschränkte Lake Formation Berechtigungen für Datenkatalogressourcen, Amazon S3 S3-Standorte und die zugrunde liegenden Daten an diesen Standorten gewährt werden. • Grobkörnig bedeutet umfassendere Berechtigungen für einzelne Operationen und für den Zugriff auf Amazon S3 S3-Standorte. Eine grobe IAM-Richtlinie könnte beispielsweise beinhalten <code>"glue: *"</code>, Lake Formation Berechtigungen zu überlassen <code>"glue:CreateTables"</code>, um zu kontrollieren, ob ein Principal Katalogobjekte erstellen kann oder nicht. <code>"glue:Create*"</code> Das bedeutet auch, den Prinzipalen Zugriff auf die Informationen zu gewähren APIs, die sie für ihre Arbeit benötigen, aber andere Ressourcen zu sperren. APIs Sie könnten beispielsweise eine IAM-Richtlinie erstellen, die es einem Prinzipal ermöglicht, Datenkatalogressourcen zu erstellen und Workflows zu erstellen und auszuführen, die Erstellung von AWS Glue Verbindungen oder benutzerdefinierten Funktionen jedoch nicht

Methode	Genehmigungen für Lake Formation	IAM-Berechtigungen	Kommentare
			ermöglicht. Die Beispiele finden Sie weiter unten in diesem Abschnitt.

Important

Achten Sie auf Folgendes:

- Standardmäßig sind in Lake Formation die Einstellungen Nur IAM-Zugriffskontrolle verwenden aktiviert, um die Kompatibilität mit dem bestehenden AWS Glue Datenkatalogverhalten zu gewährleisten. Wir empfehlen, dass Sie diese Einstellungen deaktivieren, nachdem Sie zur Verwendung von Lake Formation Formation-Berechtigungen übergegangen sind. Weitere Informationen finden Sie unter [Ändern der Standardeinstellungen für Ihren Data Lake](#).
- Data Lake-Administratoren und Datenbankersteller verfügen über implizite Lake Formation Formation-Berechtigungen, die Sie verstehen müssen. Weitere Informationen finden Sie unter [Implizite Lake Formation Formation-Berechtigungen](#).

Zugriffskontrolle für Metadaten

Bei der Zugriffskontrolle für Datenkatalogressourcen wird in der folgenden Diskussion von einer detaillierten Zugriffskontrolle mit Lake Formation Formation-Berechtigungen und einer groben Zugriffskontrolle mit IAM-Richtlinien ausgegangen.

Es gibt zwei unterschiedliche Methoden, um Lake Formation Formation-Berechtigungen für Datenkatalogressourcen zu gewähren:

- Zugriffskontrolle für benannte Ressourcen — Mit dieser Methode gewähren Sie Berechtigungen für bestimmte Datenbanken oder Tabellen, indem Sie Datenbank- oder Tabellennamen angeben. Die Zuschüsse haben die folgende Form:

Erteilen Sie Principals Berechtigungen für Ressourcen [mit Grant-Option].

Mit der Option „Gewähren“ können Sie dem Empfänger gestatten, die Berechtigungen anderen Prinzipalen zu gewähren.

- **Tag-basierte Zugriffskontrolle** — Mit dieser Methode weisen Sie Datenkatalogdatenbanken, Tabellen und Spalten ein oder mehrere LF-Tags zu und gewähren Prinzipalen Berechtigungen für ein oder mehrere LF-Tags. Jedes LF-Tag ist ein Schlüssel-Wert-Paar, wie z. `department=sales`. Ein Principal mit LF-Tags, die den LF-Tags auf einer Datenkatalogressource entsprechen, kann auf diese Ressource zugreifen. Diese Methode wird für Data Lakes mit einer großen Anzahl von Datenbanken und Tabellen empfohlen. Sie wird ausführlich in [erklärt Tag-basierte Zugangskontrolle von Lake Formation](#).

Die Berechtigungen, die ein Principal für eine Ressource hat, sind die Vereinigung der Berechtigungen, die durch beide Methoden gewährt wurden.

In der folgenden Tabelle sind die verfügbaren Lake Formation-Berechtigungen für Datenkatalogressourcen zusammengefasst. Die Spaltenüberschriften geben die Ressource an, für die die Berechtigung erteilt wurde.

Katalog	Datenbank	Tabelle
CREATE_DATABASE	CREATE_TABLE	ALTER
	ALTER	DROP
	DROP	DESCRIBE
	DESCRIBE	SELECT*
		INSERT*
		DELETE*

Die CREATE_TABLE Berechtigung wird beispielsweise für eine Datenbank erteilt. Das bedeutet, dass der Prinzipal Tabellen in dieser Datenbank erstellen darf.

Die mit einem Sternchen (*) markierten Berechtigungen werden für Datenkatalogressourcen gewährt, sie gelten jedoch für die zugrunde liegenden Daten. Die DROP Berechtigung für eine Metadatatabelle ermöglicht es Ihnen beispielsweise, die Tabelle aus dem Datenkatalog zu löschen.

Die für dieselbe Tabelle erteilte DELETE Berechtigung ermöglicht es Ihnen jedoch, die der Tabelle zugrunde liegenden Daten in Amazon S3 zu löschen, indem Sie beispielsweise eine DELETE SQL-Anweisung verwenden. Mit diesen Berechtigungen können Sie die Tabelle auch auf der Lake Formation Formation-Konsole anzeigen und Informationen über die Tabelle mit der AWS Glue API abrufen. Somit DELETE sind SELECT/INSERT, und sowohl Datenkatalogberechtigungen als auch Datenzugriffsberechtigungen.

Wenn Sie für eine Tabelle gewähren SELECT, können Sie einen Filter hinzufügen, der eine oder mehrere Spalten ein- oder ausschließt. Dies ermöglicht eine detaillierte Zugriffskontrolle auf die Spalten der Metadaten-Tabelle und schränkt die Spalten ein, die Benutzer integrierter Dienste bei der Ausführung von Abfragen sehen können. Diese Funktion ist nicht nur bei Verwendung von IAM-Richtlinien verfügbar.

Es gibt auch eine spezielle Genehmigung mit dem Namen Super. Die Super Berechtigung ermöglicht es einem Prinzipal, jeden unterstützten Lake Formation Formation-Vorgang in der Datenbank oder Tabelle auszuführen, für die sie erteilt wurde. Diese Genehmigung kann mit den anderen Lake Formation Formation-Berechtigungen koexistieren. Sie können beispielsweise Super SELECT, und INSERT für eine Metadaten-Tabelle gewähren. Der Principal kann alle unterstützten Aktionen für die Tabelle ausführen, und wenn Sie sie widerrufen Super, bleiben die INSERT Berechtigungen SELECT und erhalten.

Einzelheiten zu den einzelnen Berechtigungen finden Sie unter [Referenz zu den Genehmigungen von Lake Formation](#).

Important

Um eine von einem anderen Benutzer erstellte Datenkatalog-Tabelle anzeigen zu können, muss Ihnen mindestens eine Lake Formation Formation-Berechtigung für die Tabelle erteilt worden sein. Wenn Ihnen mindestens eine Berechtigung für die Tabelle erteilt wurde, können Sie auch die Datenbank sehen, die die Tabelle enthält.

Sie können Datenkatalogberechtigungen mithilfe der Lake Formation Formation-Konsole, der API oder der AWS Command Line Interface (AWS CLI) gewähren oder widerrufen. Im Folgenden finden Sie ein Beispiel für einen AWS CLI Befehl, der dem Benutzer die `datalake_user1` Berechtigung erteilt, Tabellen in der `retail` Datenbank zu erstellen.

```
aws lakeformation grant-permissions --principal  
DataLakePrincipalIdentifier=arn:aws:iam::111122223333:user/datalake_user1
```

```
--permissions "CREATE_TABLE" --resource '{ "Database": {"Name":"retail"} }'
```

Im Folgenden finden Sie ein Beispiel für eine grobkörnige IAM-Richtlinie für die Zugriffskontrolle, die die detaillierte Zugriffskontrolle durch Lake Formation Formation-Berechtigungen ergänzt. Sie ermöglicht alle Operationen an jeder Metadaten-Datenbank oder -Tabelle.

JSON

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Action": [
        "glue:*Database*",
        "glue:*Table*",
        "glue:*Partition*"
      ],
      "Resource": "*"
    }
  ]
}
```

Das nächste Beispiel ist ebenfalls grobkörnig, aber etwas restriktiver. Es ermöglicht schreibgeschützte Operationen für alle Metadatenbanken und Tabellen im Datenkatalog im angegebenen Konto und in der angegebenen Region.

JSON

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Action": [
        "glue:GetTables",
        "glue:SearchTables",
        "glue:GetTable",
        "glue:GetDatabase",
        "glue:GetDatabases"
      ]
    }
  ]
}
```

```

    ],
    "Resource": "arn:aws:glue:us-east-1:111122223333:*"
  }
]
}

```

Vergleichen Sie diese Richtlinien mit der folgenden Richtlinie, die eine IAM-basierte, detaillierte Zugriffskontrolle implementiert. Sie gewährt Berechtigungen nur für eine Teilmenge von Tabellen in der CRM-Metadatenbank (Customer Relationship Management) im angegebenen Konto und in der angegebenen Region.

JSON

```

{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Action": [
        "glue:GetTables",
        "glue:SearchTables",
        "glue:GetTable",
        "glue:GetDatabase",
        "glue:GetDatabases"
      ],
      "Resource": [
        "arn:aws:glue:us-east-1:111122223333:catalog",
        "arn:aws:glue:us-east-1:111122223333:database/CRM",
        "arn:aws:glue:us-east-1:111122223333:table/CRM/P*"
      ]
    }
  ]
}

```

Weitere Beispiele für grobe Richtlinien zur Zugriffskontrolle finden Sie unter [Referenz zu Personas und IAM-Berechtigungen in Lake Formation](#)

Zugrundeliegende Datenzugriffskontrolle

Wenn ein integrierter AWS Service Zugriff auf Daten an einem Amazon S3 S3-Standort anfordert, der zugriffskontrolliert wird AWS Lake Formation, stellt Lake Formation temporäre Anmeldeinformationen für den Zugriff auf die Daten bereit.

Damit Lake Formation den Zugriff auf die zugrunde liegenden Daten an einem Amazon S3 S3-Standort kontrollieren kann, registrieren Sie diesen Standort bei Lake Formation.

Nachdem Sie einen Amazon S3 S3-Standort registriert haben, können Sie damit beginnen, die folgenden Lake Formation Formation-Berechtigungen zu gewähren:

- Datenzugriffsberechtigungen (SELECTINSERT, und für Datenkatalogtabellen, die DELETE) auf diesen Speicherort verweisen.
- Berechtigungen zum Speicherort von Daten an diesem Standort.

Die Datenstandortberechtigungen von Lake Formation steuern die Fähigkeit, Datenkatalogressourcen zu erstellen, die auf bestimmte Amazon S3 S3-Standorte verweisen. Datenstandortberechtigungen bieten eine zusätzliche Sicherheitsebene für Standorte innerhalb des Data Lake. Wenn Sie einem Prinzipal die ALTER Berechtigung CREATE_TABLE oder erteilen, gewähren Sie auch Datenstandortberechtigungen, um die Speicherorte einzuschränken, für die der Prinzipal Metadatentabellen erstellen oder ändern kann.

Amazon S3 S3-Standorte sind Buckets oder Präfixe unter einem Bucket, aber keine einzelnen Amazon S3 S3-Objekte.

Sie können einem Prinzipal Datenstandortberechtigungen erteilen, indem Sie die Lake Formation Formation-Konsole, die API oder die verwenden AWS CLI. Die allgemeine Form eines Zuschusses lautet wie folgt:

```
grant DATA_LOCATION_ACCESS to principal on S3 location [with grant option]
```

Wenn Sie dies mit einbeziehen `with grant option`, kann der Empfänger die Berechtigungen anderen Schulleitern gewähren.

Denken Sie daran, dass Lake Formation Formation-Berechtigungen immer in Kombination mit AWS Identity and Access Management (IAM-) Berechtigungen für eine detaillierte Zugriffskontrolle funktionieren. Für read/write Berechtigungen für zugrunde liegende Amazon S3 S3-Daten werden IAM-Berechtigungen wie folgt erteilt:

Wenn Sie einen Standort registrieren, geben Sie eine IAM-Rolle an, die Lese-/Schreibberechtigungen für diesen Standort gewährt. Lake Formation übernimmt diese Rolle bei der Bereitstellung temporärer Anmeldeinformationen für integrierte AWS Dienste. Einer typischen Rolle könnte die folgende Richtlinie zugeordnet sein, wobei der registrierte Standort der Bucket `istawsexamplebucket`.

JSON

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Action": [
        "s3:PutObject",
        "s3:GetObject",
        "s3:DeleteObject"
      ],
      "Resource": [
        "arn:aws:s3:::amzn-s3-demo-bucket/*"
      ]
    },
    {
      "Effect": "Allow",
      "Action": [
        "s3:ListBucket"
      ],
      "Resource": [
        "arn:aws:s3:::amzn-s3-demo-bucket"
      ]
    }
  ]
}
```

Lake Formation bietet eine dienstbezogene Rolle, die Sie bei der Registrierung verwenden können, um automatisch solche Richtlinien zu erstellen. Weitere Informationen finden Sie unter [Verwenden von serviceverknüpften Rollen für Lake Formation](#).

Daher gewährt die Registrierung eines Amazon S3 S3-Standorts die erforderlichen `s3`: IAM-Berechtigungen für diesen Standort, wobei die Berechtigungen durch die Rolle festgelegt werden, die für die Registrierung des Standorts verwendet wurde.

 Important

Vermeiden Sie es, einen Amazon S3 S3-Bucket zu registrieren, für den Zahlungen durch den Antragsteller aktiviert ist. Bei Buckets, die bei Lake Formation registriert sind, wird die Rolle, mit der der Bucket registriert wurde, immer als der Anforderer angesehen. Wenn ein anderes AWS Konto auf den Bucket zugreift, wird dem Bucket-Besitzer der Datenzugriff in Rechnung gestellt, sofern die Rolle zu demselben Konto gehört wie der Bucket-Besitzer.

Für read/write den Zugriff auf die zugrunde liegenden Daten benötigen Principals zusätzlich zu den Lake Formation Formation-Berechtigungen auch die `lakeformation:GetDataAccess` IAM-Berechtigung. Mit dieser Berechtigung gewährt Lake Formation die Anforderung von temporären Anmeldeinformationen für den Zugriff auf die Daten.

JSON

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Action": "lakeformation:GetDataAccess",
      "Resource": "*"
    }
  ]
}
```

In der obigen Richtlinie müssen Sie den Resource-Parameter auf `'*` (all) setzen. Die Angabe einer anderen Ressource für diese Berechtigung wird nicht unterstützt. Diese Konfiguration stellt sicher, dass Lake Formation den Datenzugriff in Ihrer gesamten Data-Lake-Umgebung effizient verwalten kann.

 Note

Amazon Athena setzt voraus, dass der Benutzer über die entsprechende `lakeformation:GetDataAccess` Genehmigung verfügt. Für andere integrierte

Dienste ist die entsprechende Ausführungsrolle erforderlich, um über die `lakeformation:GetDataAccess` entsprechende Genehmigung zu verfügen.

Diese Berechtigung ist in den vorgeschlagenen Richtlinien in der enthalten [Referenz zu Personas und IAM-Berechtigungen in Lake Formation](#).

Zusammenfassend lässt sich sagen, dass Lake Formation-Prinzipale die zugrunde liegenden Daten lesen und schreiben können, wobei der Zugriff durch Lake Formation Formation-Berechtigungen gesteuert wird:

- Registrieren Sie die Amazon S3 S3-Standorte, die die Daten enthalten, bei Lake Formation.
- Principals, die Datenkatalogtabellen erstellen, die auf zugrunde liegende Datenspeicherorte verweisen, müssen über Datenstandortberechtigungen verfügen.
- Principals, die zugrunde liegende Daten lesen und schreiben, müssen über Lake Formation Formation-Datenzugriffsberechtigungen für die Datenkatalogtabellen verfügen, die auf die zugrunde liegenden Datenspeicherorte verweisen.
- Principals, die zugrunde liegende Daten lesen und schreiben, müssen über die `lakeformation:GetDataAccess` IAM-Berechtigung verfügen, wenn der zugrunde liegende Datenstandort bei Lake Formation registriert ist.

Note

Das Lake Formation Formation-Berechtigungsmodell verhindert nicht den Zugriff auf Amazon S3 S3-Standorte über die Amazon S3 S3-API oder -Konsole, wenn Sie über IAM- oder Amazon S3 S3-Richtlinien Zugriff darauf haben. Sie können IAM-Richtlinien an Principals anhängen, um diesen Zugriff zu blockieren.

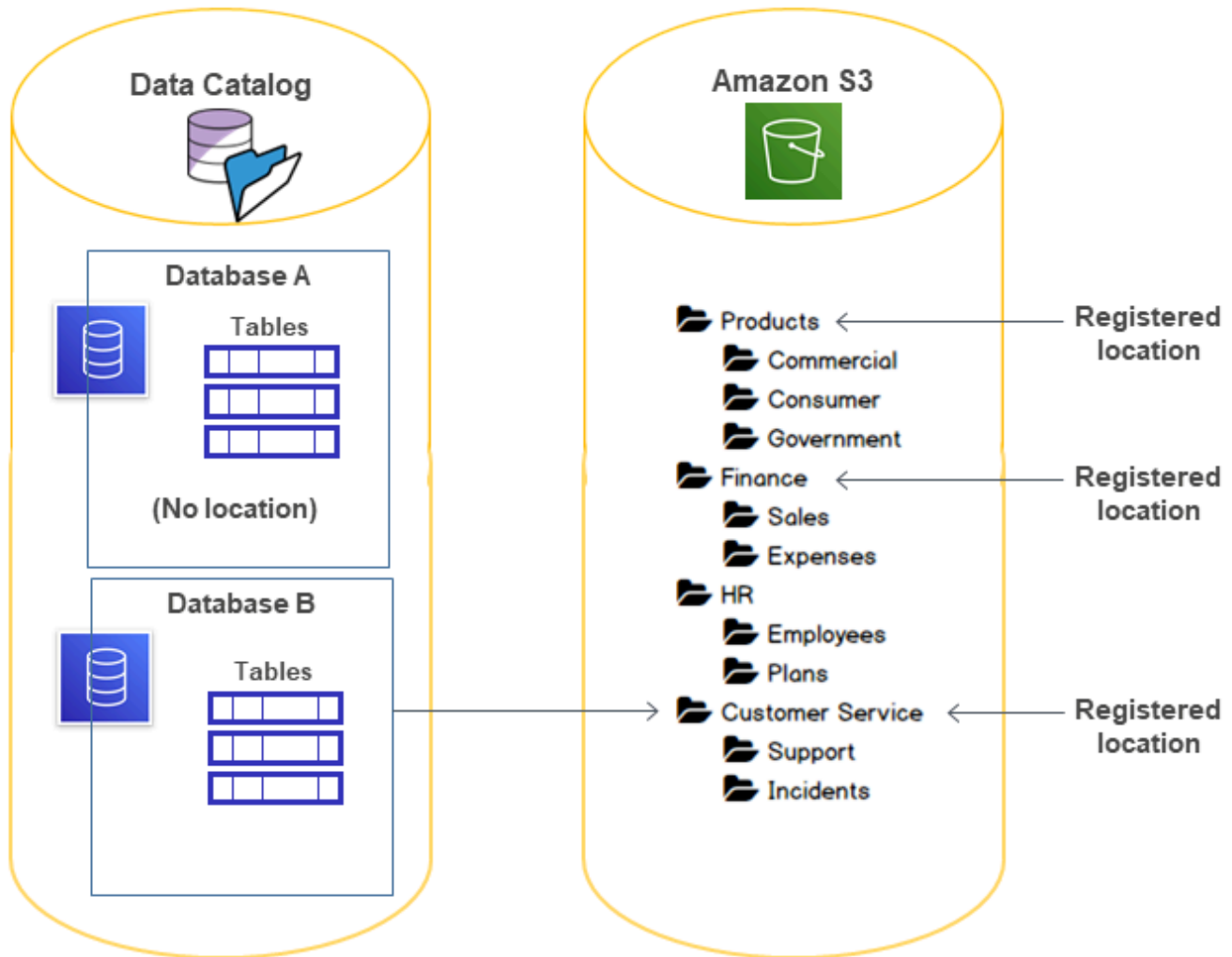
Weitere Informationen zu Berechtigungen für den Speicherort von Daten

Berechtigungen zum Speicherort von Daten bestimmen das Ergebnis von Erstellungs- und Aktualisierungsvorgängen in Datenkatalog-Datenbanken und -Tabellen. Die Regeln lauten wie folgt:

- Ein Principal muss über explizite oder implizite Datenspeicherberechtigungen für einen Amazon S3 S3-Standort verfügen, um eine Datenbank oder Tabelle zu erstellen oder zu aktualisieren, die diesen Speicherort spezifiziert.

- Die ausdrückliche Genehmigung `DATA_LOCATION_ACCESS` wird über die Konsole, die API oder AWS CLI erteilt.
- Implizite Berechtigungen werden erteilt, wenn eine Datenbank über eine Standorteigenschaft verfügt, die auf einen registrierten Speicherort verweist, der Principal über die `CREATE_TABLE` entsprechende Berechtigung für die Datenbank verfügt und der Principal versucht, eine Tabelle an diesem Speicherort oder einem untergeordneten Speicherort zu erstellen.
- Wenn einem Prinzipal Datenstandortberechtigungen für einen Standort erteilt werden, verfügt der Prinzipal über Datenstandortberechtigungen für alle untergeordneten Standorte.
- Ein Prinzipal benötigt keine Datenstandortberechtigungen, um read/write Operationen mit den zugrunde liegenden Daten durchzuführen. Es ist ausreichend, über die `SELECT` oder `INSERT` Datenzugriffsberechtigungen zu verfügen. Berechtigungen zum Speicherort von Daten gelten nur für die Erstellung von Datenkatalogressourcen, die auf den Speicherort verweisen.

Stellen Sie sich das in der folgenden Abbildung gezeigte Szenario vor.



Vorgänge in diesem Diagramm:

- Die Amazon S3 S3-Buckets **Products**, **Finance**, und **Customer Service** sind bei Lake Formation registriert.
- **Database A** hat keine Standorteigenschaft und **Database B** verfügt über eine Standorteigenschaft, die auf den **Customer Service** Bucket verweist.
- Der Benutzer `datalake_user` hat `CREATE_TABLE` in beiden Datenbanken.
- `datalake_user` Dem Benutzer wurden nur Datenspeicherberechtigungen für den **Products** Bucket erteilt.

Im Folgenden sind die Ergebnisse aufgeführt, wenn der Benutzer `datalake_user` versucht, eine Katalogtabelle in einer bestimmten Datenbank an einem bestimmten Speicherort zu erstellen.

Ort, an dem **datalake_user** versucht wird, eine Tabelle zu erstellen

Datenbank und Standort	Erfolgreich oder schlägt fehl	Grund
Datenbank A bei Finance/Sales	Scheitert	Keine Genehmigung zum Speicherort von Daten
Datenbank A bei Products	Ist erfolgreich	Hat die Berechtigung zum Speichern von Daten
Datenbank A unter HR/Plans	Ist erfolgreich	Der Standort ist nicht registriert
Datenbank B unter Customer Service/Incidents	Ist erfolgreich	Die Datenbank hat die Standorteigenschaft unter Customer Service

Weitere Informationen finden Sie hier:

- [Hinzufügen eines Amazon S3 S3-Standorts zu Ihrem Data Lake](#)
- [Referenz zu den Genehmigungen von Lake Formation](#)
- [Referenz zu Personas und IAM-Berechtigungen in Lake Formation](#)

Referenz zu Personas und IAM-Berechtigungen in Lake Formation

In diesem Abschnitt sind einige vorgeschlagene Lake Formation Formation-Personas und ihre empfohlenen AWS Identity and Access Management (IAM-) Berechtigungen aufgeführt. Informationen zu den Berechtigungen für Lake Formation finden Sie unter [the section called “Referenz zu den Genehmigungen von Lake Formation”](#).

AWS Lake Formation Personas

In der folgenden Tabelle sind die vorgeschlagenen AWS Lake Formation Personas aufgeführt.

Lake Formation Personas

Persona	Description
IAM-Administrator (Superuser)	(Erforderlich) Benutzer, der IAM-Benutzer und -Rollen erstellen kann. Hat die <code>AdministratorAccess</code> AWS verwaltete Richtlinie. Hat alle Berechtigungen für alle Lake Formation Formation-Ressourcen. Kann Data Lake-Administratoren hinzufügen. Lake Formation Formation-Berechtigungen können nicht erteilt werden, wenn nicht auch ein Data Lake-Administrator benannt wurde.
Data Lake-Administrator	(Erforderlich) Benutzer, der Amazon S3 S3-Standorte registrieren, auf den Datenkatalog zugreifen, Datenbanken erstellen, Workflows erstellen und ausführen, anderen Benutzern Lake Formation Formation-Berechtigungen gewähren und AWS CloudTrail Protokolle einsehen kann. Hat weniger IAM-Berechtigungen als der IAM-Administrator, reicht aber aus, um den Data Lake zu verwalten. Andere Data Lake-Administratoren können nicht hinzugefügt werden.
Administrator mit Schreibschutz	(Optional) Benutzer, der Prinzipale, Datenkatalogressourcen, Berechtigungen und AWS CloudTrail Protokolle anzeigen kann, ohne über die erforderlichen Berechtigungen für Aktualisierungen zu verfügen.
Dateningenieur	(Optional) Benutzer, der Datenbanken erstellen, Crawler und Workflows erstellen und ausführen und Lake Formation Formation-Berechtigungen für die von den Crawlern und Workflows erstellten Datenkatalogtabellen gewähren kann. Wir empfehlen, dass Sie alle Dateningenieure zu Datenbankersteller machen. Weitere Informationen finden Sie unter Erstellen einer Datenbank .
Datenanalyst	(Optional) Benutzer, der Abfragen für den Data Lake ausführen kann, z. B. mit Amazon Athena. Hat nur genügend Berechtigungen, um Abfragen auszuführen.

Persona	Description
Workflow-Rolle	(Erforderlich) Rolle, die einen Workflow im Namen eines Benutzers ausführt. Sie geben diese Rolle an, wenn Sie einen Workflow aus einem Blueprint erstellen.

Note

In Lake Formation können Data Lake-Administratoren, die nach der Datenbankerstellung hinzugefügt wurden, zwar Berechtigungen gewähren, verfügen aber nicht automatisch über Datenzugriffsberechtigungen wie SELECT oder DESCRIBE. Administratoren, die Datenbanken erstellen, erhalten SUPER Berechtigungen für diese Datenbanken. Dieses Verhalten ist beabsichtigt — zwar können sich alle Administratoren die erforderlichen Berechtigungen selbst gewähren, diese Berechtigungen werden jedoch nicht automatisch auf bereits vorhandene Ressourcen angewendet. Daher müssen sich Administratoren ausdrücklich Zugriff auf Datenbanken gewähren, die existierten, bevor ihnen Administratorrechte zugewiesen wurden.

AWS verwaltete Richtlinien für Lake Formation

Mithilfe von AWS verwalteten Richtlinien und Inline-Richtlinien können Sie die AWS Identity and Access Management (IAM-) Berechtigungen gewähren, die für die Arbeit erforderlich sind. AWS Lake Formation Die folgenden AWS verwalteten Richtlinien sind für Lake Formation verfügbar.

AWS verwaltete Richtlinie: AWSLakeFormationDataAdmin

[AWSLakeFormationDataAdmin](#) Die Richtlinie gewährt administrativen Zugriff auf AWS Lake Formation und damit verbundene Dienste, z. B. AWS Glue die Verwaltung von Data Lakes.

Sie können AWSLakeFormationDataAdmin an Ihre Benutzer, Gruppen und Rollen anfügen.

Berechtigungsdetails

- **CloudTrail**— Ermöglicht Prinzipalen das Einsehen von AWS CloudTrail Protokollen. Dies ist erforderlich, um etwaige Fehler bei der Einrichtung des Data Lake zu überprüfen.
- **Glue**— Ermöglicht Prinzipalen das Anzeigen, Erstellen und Aktualisieren von Metadatatabellen und Datenbanken im Datenkatalog. Dazu gehören API-Operationen, die mit `Get`, `List`, `Create`

UpdateDelete, und Search beginnen. Dies ist erforderlich, um die Metadaten der Data-Lake-Tabellen zu verwalten.

- **IAM**— Ermöglicht Prinzipalen das Abrufen von Informationen über IAM-Benutzer, -Rollen und Richtlinien, die den Rollen zugeordnet sind. Dies ist erforderlich, damit der Datenadministrator die IAM-Benutzer und -Rollen überprüfen und auflisten kann, um Lake Formation Formation-Berechtigungen zu gewähren.
- **Lake Formation**— Gewährt Data Lake-Administratoren die erforderlichen Lake Formation Formation-Berechtigungen zur Verwaltung von Data Lakes.
- **S3**— Ermöglicht Principals das Abrufen von Informationen über Amazon S3 S3-Buckets und deren Standorte, um den Datenstandort für Data Lakes einzurichten.

```
"Statement": [
  {
    "Sid": "AWSLakeFormationDataAdminAllow",
    "Effect": "Allow",
    "Action": [
      "lakeformation:*",
      "cloudtrail:DescribeTrails",
      "cloudtrail:LookupEvents",
      "glue:CreateCatalog",
      "glue:UpdateCatalog",
      "glue>DeleteCatalog",
      "glue:GetCatalog",
      "glue:GetCatalogs",
      "glue:GetDatabase",
      "glue:GetDatabases",
      "glue>CreateDatabase",
      "glue:UpdateDatabase",
      "glue>DeleteDatabase",
      "glue:GetConnections",
      "glue:SearchTables",
      "glue:GetTable",
      "glue:CreateTable",
      "glue:UpdateTable",
      "glue>DeleteTable",
      "glue:GetTableVersions",
      "glue:GetPartitions",
      "glue:GetTables",
      "glue:ListWorkflows",
      "glue:BatchGetWorkflows",
```



```

        "glue:DeleteWorkflow",
        "glue:GetWorkflowRuns",
        "glue:StartWorkflowRun",
        "glue:GetWorkflow",
        "s3:ListBucket",
        "s3:GetBucketLocation",
        "s3:ListAllMyBuckets",
        "s3:GetBucketAcl",
        "iam:ListUsers",
        "iam:ListRoles",
        "iam:GetRole",
        "iam:GetRolePolicy"
    ],
    "Resource": "*"
},
{
    "Sid": "AWSLakeFormationDataAdminDeny",
    "Effect": "Deny",
    "Action": [
        "lakeformation:PutDataLakeSettings"
    ],
    "Resource": "*"
}
]
}

```

Note

Die `AWSLakeFormationDataAdmin` Richtlinie gewährt Data Lake-Administratoren nicht alle erforderlichen Berechtigungen. Zusätzliche Berechtigungen sind erforderlich, um Workflows zu erstellen und auszuführen und Standorte mit der serviceverknüpften Rolle zu registrieren `AWSServiceRoleForLakeFormationDataAccess`. Weitere Informationen erhalten Sie unter [Erstellen Sie einen Data Lake-Administrator](#) und [Verwenden von serviceverknüpften Rollen für Lake Formation](#).

AWS verwaltete Richtlinie: AWSLakeFormationCrossAccountManager

[AWSLakeFormationCrossAccountManager](#) Die Richtlinie ermöglicht den kontenübergreifenden Zugriff auf AWS Glue Ressourcen über Lake Formation und gewährt Lesezugriff auf andere erforderliche Dienste wie AWS Organizations und AWS RAM.

Sie können `AWSLakeFormationCrossAccountManager` an Ihre Benutzer, Gruppen und Rollen anfügen.

Berechtigungsdetails

Diese Richtlinie umfasst die folgenden Berechtigungen.

- `Glue`— Ermöglicht Prinzipalen, die Datenkatalog-Ressourcenrichtlinie für die Zugriffskontrolle festzulegen oder zu löschen.
- `Organizations`— Ermöglicht Prinzipalen das Abrufen von Konto- und Organisationseinheiteninformationen (OU) für eine Organisation.
- `ram:CreateResourceShare`— Ermöglicht Prinzipalen das Erstellen einer Ressourcenfreigabe.
- `ram:UpdateResourceShare`— Ermöglicht Prinzipalen, einige Eigenschaften der angegebenen Ressourcenfreigabe zu ändern.
- `ram>DeleteResourceShare`— Ermöglicht Prinzipalen, die angegebene Ressourcenfreigabe zu löschen.
- `ram:AssociateResourceShare`— Ermöglicht Prinzipalen, die angegebene Liste von Prinzipalen und die Liste der Ressourcen zu einer Ressourcenfreigabe hinzuzufügen.
- `ram:DisassociateResourceShare`— Ermöglicht Prinzipalen, die angegebenen Prinzipale oder Ressourcen von der Teilnahme an der angegebenen Ressourcenfreigabe auszuschließen.
- `ram:GetResourceShares`— Ermöglicht Prinzipalen das Abrufen von Details zu den Ressourcenfreigaben, die Ihnen gehören oder die für Sie gemeinsam genutzt wurden.
- `ram:RequestedResourceType`— Ermöglicht Prinzipalen das Abrufen des Ressourcentyps (Datenbank, Tabelle oder Katalog).
- `AssociateResourceSharePermission`— Ermöglicht Prinzipalen, die AWS RAM Berechtigung für einen Ressourcentyp hinzuzufügen oder zu ersetzen, der in einer Ressourcenfreigabe enthalten ist. Sie können jedem Ressourcentyp in der Ressourcenfreigabe genau eine Berechtigung zuordnen.

JSON

```
{
  "Version": "2012-10-17",
  "Statement": [{
    "Sid": "AllowCreateResourceShare",
    "Effect": "Allow",
    "Action": [
      "ram:CreateResourceShare"
    ],
    "Resource": "*",
    "Condition": {
      "StringLikeIfExists": {
        "ram:RequestedResourceType": [
          "glue:Table",
          "glue:Database",
          "glue:Catalog"
        ]
      }
    }
  },
  {
    "Sid": "AllowManageResourceShare",
    "Effect": "Allow",
    "Action": [
      "ram:UpdateResourceShare",
      "ram:DeleteResourceShare",
      "ram:AssociateResourceShare",
      "ram:DisassociateResourceShare",
      "ram:GetResourceShares"
    ],
    "Resource": "*",
    "Condition": {
      "StringLike": {
        "ram:ResourceShareName": [
          "LakeFormation*"
        ]
      }
    }
  },
  {
    "Sid": "AllowManageResourceSharePermissions",
    "Effect": "Allow",
```

```

        "Action": [
            "ram:AssociateResourceSharePermission"
        ],
        "Resource": "*",
        "Condition": {
            "ArnLike": {
                "ram:PermissionArn": [
                    "arn:aws:ram::aws:permission/AWSRAMLFEnabled*"
                ]
            }
        }
    },
    {
        "Sid": "AllowXAcctManagerPermissions",
        "Effect": "Allow",
        "Action": [
            "glue:PutResourcePolicy",
            "glue>DeleteResourcePolicy",
            "organizations:DescribeOrganization",
            "organizations:DescribeAccount",
            "ram:Get*",
            "ram:List*"
        ],
        "Resource": "*"
    },
    {
        "Sid": "AllowOrganizationsPermissions",
        "Effect": "Allow",
        "Action": [
            "organizations:ListRoots",
            "organizations:ListAccountsForParent",
            "organizations:ListOrganizationalUnitsForParent"
        ],
        "Resource": "*"
    }
]
}

```

AWS verwaltete Richtlinie: AWSGlue ConsoleFullAccess

[AWSGlueConsoleFullAccess](#) Die Richtlinie gewährt vollen Zugriff auf AWS Glue Ressourcen, wenn eine Identität, an die die Richtlinie angehängt ist, die verwendet AWS-Managementkonsole. Wenn Sie die Namenskonvention für Ressourcen befolgen, die in dieser Richtlinie angegeben sind, haben Benutzer alle Konsolenfunktionalitäten. Diese Richtlinie wird in der Regel Benutzern der AWS Glue Konsole zugewiesen.

Darüber hinaus übernehmen AWS Glue und Lake Formation die Servicerolle, `AWSGlueServiceRole` um den Zugriff auf verwandte Dienste zu ermöglichen, darunter Amazon Elastic Compute Cloud (Amazon EC2), Amazon Simple Storage Service (Amazon S3) und Amazon CloudWatch.

AWS managed policy: LakeFormationDataAccessServiceRolePolicy

Diese Richtlinie ist einer dienstbezogenen Rolle mit dem Namen `zugeordnetServiceRoleForLakeFormationDataAccess`, die es dem Service ermöglicht, auf Ihre Anfrage hin Aktionen an Ressourcen durchzuführen. Sie können diese Richtlinie nicht an Ihre IAM-Identitäten anhängen.

Diese Richtlinie ermöglicht es den in Lake Formation integrierten AWS Diensten wie Amazon Athena Amazon Redshift, die serviceverknüpfte Rolle zu verwenden, um Amazon S3 S3-Ressourcen zu ermitteln.

Weitere Informationen finden Sie unter [Verwenden von serviceverknüpften Rollen für Lake Formation](#).

Berechtigungsdetails

Diese Richtlinie umfasst die folgende Berechtigung.

- `s3:ListAllMyBuckets`— Gibt eine Liste aller Buckets zurück, die dem authentifizierten Absender der Anfrage gehören.

JSON

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

```
"Sid": "LakeFormationDataAccessServiceRolePolicy",
"Effect": "Allow",
"Action": [
  "s3:ListAllMyBuckets"
],
"Resource": [
  "arn:aws:s3:::*"
]
}
]
}
```

Lake Formation aktualisiert AWS verwaltete Richtlinien

Sehen Sie sich Details zu Aktualisierungen der AWS verwalteten Richtlinien für Lake Formation an, seit dieser Dienst begonnen hat, diese Änderungen zu verfolgen.

Änderungen	Beschreibung	Date
Die AWSLakeFo rmationCr ossAccountManager Richtlinie von Lake Formation wurde aktualisi ert.	Lake Formation erweiterte die AWSLakeFormationCrossAccoun tManager Richtlinie, indem der StringLike Bedingungsoperator durch den ArnLike Operator ersetzt wurde, der es IAM ermöglicht, die ARN-Formatprüfung durchzuführen.	Januar 2025
Die AWSLakeFo rmationDataAdmin Richtlinie von Lake Formation wurde aktualisi ert.	Lake Formation erweiterte die AWSLakeFormationDataAdmin Richtlini e, indem das folgende AWS Glue Data Catalog CRUD APIs als Teil der Multi-Katalog-Funktion hinzugefügt wurde. • Klebstoff: CreateCatalog • kleben: UpdateCatalog • kleben: DeleteCatalog • kleben: GetCatalog	Dezember 2024

Änderungen	Beschreibung	Date
	• kleben: GetCatalogs Diese verwaltete Richtlinienänderung soll sicherstellen, dass die Lake Formation-Administrator-Persona standardmäßig über IAM-Berechtigungen für diese neuen Operationen verfügt.	
Die AWSLakeFormationCrossAccountManager Richtlinie von Lake Formation wurde aktualisiert.	Lake Formation erweiterte die AWSLakeFormationCrossAccountManager Richtlinie, indem sie der Grundsatzerklärung Sid-Elemente hinzufügte.	März 2024
Die AWSLakeFormationDataAdmin Richtlinie von Lake Formation wurde aktualisiert.	Lake Formation erweiterte die AWSLakeFormationDataAdmin Richtlinie, indem sie der Grundsatzerklärung ein Sid-Element hinzufügte und eine überflüssige Maßnahme entfernte.	März 2024
Die LakeFormationDataAccessServiceRolePolicy Richtlinie von Lake Formation wurde aktualisiert.	Lake Formation erweiterte die LakeFormationDataAccessServiceRolePolicy Richtlinie, indem sie der Grundsatzerklärung ein Sid-Element hinzufügte.	Februar 2024

Änderungen	Beschreibung	Date
Die AWSLakeFormationCrossAccountManager Richtlinie von Lake Formation wurde aktualisiert.	Lake Formation erweiterte die AWSLakeFormationCrossAccountManager Richtlinie um eine neue Berechtigung, um den kontoübergreifenden Datenaustausch im Hybridzugriffsmodus zu ermöglichen.	Oktober 2023
Die AWSLakeFormationCrossAccountManager Richtlinie von Lake Formation wurde aktualisiert.	Lake Formation hat die AWSLakeFormationCrossAccountManager Richtlinie dahingehend erweitert, dass nur eine Ressourcenfreigabe pro Empfängerkonto erstellt wird, wenn die Ressource zum ersten Mal gemeinsam genutzt wird. Alle Ressourcen, die danach mit demselben Konto gemeinsam genutzt werden, werden derselben Ressource zugeordnet.	6. Mai 2022
Lake Formation begann, Veränderungen zu verfolgen.	Lake Formation begann, Änderungen an seinen AWS verwalteten Richtlinien zu verfolgen.	6. Mai 2022

Personas hat Berechtigungen vorgeschlagen

Im Folgenden sind die empfohlenen Berechtigungen für jede Persona aufgeführt. Der IAM-Administrator ist nicht enthalten, da dieser Benutzer über alle Berechtigungen für alle Ressourcen verfügt.

Themen

- [Berechtigungen des Data Lake-Administrators](#)
- [Administratorberechtigungen nur lesen](#)
- [Berechtigungen für Dateningenieure](#)
- [Berechtigungen für Datenanalysten](#)
- [Berechtigungen für Workflow-Rollen](#)

Berechtigungen des Data Lake-Administrators

 **Important**

<account-id> Ersetzen Sie den Text in den folgenden Richtlinien durch eine gültige AWS Kontonummer und *<workflow_role>* durch den Namen einer Rolle, die über Berechtigungen zum Ausführen eines Workflows verfügt, wie unter definiert [Berechtigungen für Workflow-Rollen](#).

Richtlinientyp	Richtlinie
AWS verwaltete Richtlinien	• AWSLakeFormationDataAdmin • LakeFormationDataAccessServiceRolePolicy (Richtlinie für dienstbezogene Rollen) • AWSGlueConsoleFullAccess (Optional) • CloudWatchLogsReadOnlyAccess (Optional) • AWSLakeFormationCrossAccountManager (Optional) • AmazonAthenaFullAccess (Optional) Informationen zu den optionalen AWS verwalteten Richtlinien finden Sie unter the section called “Erstellen Sie einen Data Lake-Administrator”.

Inline-Richtlinie (zur Erstellung der dienstbezogenen Rolle Lake Formation)

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Action": "iam:CreateServiceLinkedRole",
      "Resource": "*",
      "Condition": {
        "StringEquals": {
          "iam:AWSServiceName": "lakeformation.amazonaws.com"
        }
      }
    }
  ]
}
```

Richtlinientyp	Richtlinie
	<pre> } }, { "Effect": "Allow", "Action": ["iam:PutRolePolicy"], "Resource": "arn:aws:iam:: <account-id> :role/aws-service-role/lakeformation.amazonaws.com/AWSServiceRoleForLakeFormationDataAccess" }] } } </pre>
(Optional) Inline-Richtlinie (Passrole-Richtlinie für die Workflow-Rolle). Dies ist nur erforderlich, wenn der Data Lake-Administrator Workflows erstellt und ausführt.	<pre> { "Version": "2012-10-17", "Statement": [{ "Sid": "PassRolePermissions", "Effect": "Allow", "Action": ["iam:PassRole"], "Resource": ["arn:aws:iam:: 111122223333 :role/<workflow_role> "] }] } </pre>

Richtlinientyp	Richtlinie
(Optional) Inline-Richtlinie (wenn Ihr Konto kontoübergreifende Lake Formation-Berechtigungen gewährt oder erhält). Diese Richtlinie dient dazu, Einladungen zur gemeinsamen Nutzung von AWS RAM Ressourcen anzunehmen oder abzulehnen und Organisationen die Erteilung kontoübergreifender Berechtigungen zu ermöglichen. <code>ram:EnableSharingWithAwsOrganization</code> ist nur für Data Lake-Administratoren im AWS Organizations Verwaltungskonto erforderlich.	<pre> { "Version": "2012-10-17", "Statement": [{ "Effect": "Allow", "Action": ["ram:AcceptResourceShareInvitation", "ram:RejectResourceShareInvitation", "ec2:DescribeAvailabilityZones", "ram:EnableSharingWithAwsOrganization"], "Resource": "*" }] }</pre>

Administratorberechtigungen nur lesen

Richtlinientyp	Richtlinie
Inline-Richtlinie (einfach)	<pre> { "Version": "2012-10-17", "Statement": [{ "Effect": "Allow", "Action": ["lakeformation:GetEffectivePermissionsForPath", "lakeformation:ListPermissions", "lakeformation:ListDataCellsFilter", "lakeformation:GetDataCellsFilter", </pre>

Richtlinientyp	Richtlinie
	<pre> "lakeformation:SearchDatabasesByLFTa gs", "lakeformation:SearchTablesByLFTags" , "lakeformation:GetLFTag", "lakeformation:ListLFTags", "lakeformation:GetResourceLFTags", "lakeformation:ListLakeFormationOpti ns", "cloudtrail:DescribeTrails", "cloudtrail:LookupEvents", "glue:GetDatabase", "glue:GetDatabases", "glue:GetConnections", "glue:SearchTables", "glue:GetTable", "glue:GetTableVersions", "glue:GetPartitions", "glue:GetTables", "glue:GetWorkflow", "glue:ListWorkflows", "glue:BatchGetWorkflows", "glue:GetWorkflowRuns", "glue:GetWorkflow", "s3:ListBucket", "s3:GetBucketLocation", "s3:ListAllMyBuckets", "s3:GetBucketAcl", "iam:ListUsers", "iam:ListRoles", "iam:GetRole", "iam:GetRolePolicy"], "Resource": "*" }, { "Effect": "Deny", "Action": ["lakeformation:PutDataLakeSettings"], "Resource": "*" } </pre>

Richtlinientyp	Richtlinie
	<pre>] } </pre>

Berechtigungen für Dateningenieure

Important

Ersetzen Sie den Text in den folgenden Richtlinien `<account-id>` durch eine gültige AWS Kontonummer und `<workflow_role>` durch den Namen der Workflow-Rolle.

Richtlinientyp	Richtlinie
AWS verwaltete Richtlinie	AWSGlueConsoleFullAccess
Inline-Richtlinie (grundlegend)	<pre> { "Version": "2012-10-17", "Statement": [{ "Effect": "Allow", "Action": ["lakeformation:GetDataAccess", "lakeformation:GrantPermissions", "lakeformation:RevokePermissions", "lakeformation:BatchGrantPermissions", "lakeformation:BatchRevokePermissions", "lakeformation:ListPermissions", "lakeformation:AddLFTagsToResource", "lakeformation:RemoveLFTagsFromResource", "lakeformation:GetResourceLFTags", "lakeformation:ListLFTags", "lakeformation:GetLFTag", "lakeformation:SearchTablesByLFTags"] }] } </pre>

Richtlinientyp	Richtlinie
	<pre>"lakeformation:SearchDatabasesByLFTa gs", "lakeformation:GetWorkUnits", "lakeformation:GetWorkUnitResults", "lakeformation:StartQueryPlanning", "lakeformation:GetQueryState", "lakeformation:GetQueryStatistics"], "Resource": "*" }]</pre>
Inline-Richtlinie (für Operationen an kontrollierten Tabellen, einschließlich Operationen innerhalb von Transaktionen)	<pre>{ "Version":"2012-10-17", "Statement": [{ "Effect": "Allow", "Action": ["lakeformation:StartTransaction", "lakeformation:CommitTransaction", "lakeformation:CancelTransaction", "lakeformation:ExtendTransaction", "lakeformation:DescribeTransaction", "lakeformation:ListTransactions", "lakeformation:GetTableObjects", "lakeformation:UpdateTableObjects", "lakeformation>DeleteObjectsOnCancel "], "Resource": "*" }] }</pre>

Richtlinientyp	Richtlinie
Inline-Richtlinie (für die Zugriffskontrolle auf Metadaten mithilfe der Tag-Based Access Control (LF-TBAC) - Methode von Lake Formation)	<pre> { "Version": "2012-10-17", "Statement": [{ "Effect": "Allow", "Action": ["lakeformation:AddLFTagsToResource", "lakeformation:RemoveLFTagsFromResource", "lakeformation:GetResourceLFTags", "lakeformation:ListLFTags", "lakeformation:GetLFTag", "lakeformation:SearchTablesByLFTags", "lakeformation:SearchDatabasesByLFTags"], "Resource": "*" }] }</pre>
Inline-Richtlinie (Passrolle-Richtlinie für die Workflow-Rolle)	<pre> { "Version": "2012-10-17", "Statement": [{ "Sid": "PassRolePermissions", "Effect": "Allow", "Action": ["iam:PassRole"], "Resource": ["arn:aws:iam:: 111122223333 :role/<workflow_role> "] }] }</pre>

Berechtigungen für Datenanalysten

Richtlinientyp	Richtlinie
AWS verwaltete Richtlinie	AmazonAthenaFullAccess
Inline-Richtlinie (grundlegend)	<pre>{ "Version": "2012-10-17", "Statement": [{ "Effect": "Allow", "Action": ["lakeformation:GetDataAccess", "glue:GetTable", "glue:GetTables", "glue:SearchTables", "glue:GetDatabase", "glue:GetDatabases", "glue:GetPartitions", "lakeformation:GetResourceLFTags", "lakeformation:ListLFTags", "lakeformation:GetLFTag", "lakeformation:SearchTablesByLFTags", "lakeformation:SearchDatabasesByLFTags"], "Resource": "*" }] }</pre>
(Optional) Inline-Richtlinie (für Operationen an kontrollierten Tabellen, einschließlich Operationen innerhalb von Transaktionen)	<pre>{ "Version": "2012-10-17", "Statement": [{ "Effect": "Allow", "Action": ["lakeformation:StartTransaction", "lakeformation:CommitTransaction", "lakeformation:CancelTransaction", "lakeformation:ExtendTransaction", </pre>

Richtlinientyp	Richtlinie
	<pre> "lakeformation:DescribeTransaction", "lakeformation:ListTransactions", "lakeformation:GetTableObjects", "lakeformation:UpdateTableObjects", "lakeformation>DeleteObjectsOnCancel "], "Resource": "*" }] } </pre>

Berechtigungen für Workflow-Rollen

Diese Rolle verfügt über die erforderlichen Berechtigungen, um einen Workflow auszuführen. Sie geben eine Rolle mit diesen Berechtigungen an, wenn Sie einen Workflow erstellen.

Important

<region> Ersetzen Sie in den folgenden Richtlinien durch eine gültige AWS Regionskennung (z. B. *us-east-1*), *<account-id>* durch eine gültige AWS Kontonummer, *<workflow_role>* durch den Namen der Workflow-Rolle und *<your-s3-cloudtrail-bucket>* durch den Amazon S3-Pfad zu Ihren AWS CloudTrail Protokollen.

Richtlinientyp	Richtlinie
AWS verwaltete Richtlinie	AWSGlueServiceRole
Inline-Richtlinie (Datenzugriff)	<pre> { "Version": "2012-10-17", "Statement": [{ "Sid": "Lakeformation", "Effect": "Allow", "Action": ["lakeformation:GetDataAccess", </pre>

Richtlinientyp	Richtlinie
	<pre> "lakeformation:GrantPermissions"], "Resource": "*" }] }</pre>
Inline-Richtlinie (Passrolle-Richtlinie für die Workflow-Rolle)	<pre> { "Version": "2012-10-17", "Statement": [{ "Sid": "PassRolePermissions", "Effect": "Allow", "Action": ["iam:PassRole"], "Resource": ["arn:aws:iam:: 111122223333 :role/<workflow_role> "] }] }</pre>
Inline-Richtlinie (für die Aufnahme von Daten außerhalb des Data Lake, AWS CloudTrail z. B. Logs)	<pre> { "Version": "2012-10-17", "Statement": [{ "Effect": "Allow", "Action": ["s3:GetObject", "s3:ListBucket"], "Resource": ["arn:aws:s3::: <your-s3-cloudtrail-bucket> /*"] }] }</pre>

Ändern der Standardeinstellungen für Ihren Data Lake

Um die Abwärtskompatibilität mit zu gewährleisten AWS Glue, AWS Lake Formation verfügt über die folgenden anfänglichen Sicherheitseinstellungen:

- Die `Super` Berechtigung wird der Gruppe `IAMAllowedPrincipals` für alle vorhandenen AWS Glue Datenkatalogressourcen erteilt.
- Die Einstellungen „Nur IAM-Zugriffskontrolle verwenden“ sind für neue Datenkatalogressourcen aktiviert.

Diese Einstellungen bewirken, dass der Zugriff auf Datenkatalogressourcen und Amazon S3 S3-Standorte ausschließlich durch AWS Identity and Access Management (IAM-) Richtlinien gesteuert wird. Individuelle Genehmigungen für Lake Formation sind nicht gültig.

Die `IAMAllowedPrincipals` Gruppe umfasst alle IAM-Benutzer und -Rollen, denen aufgrund Ihrer IAM-Richtlinien Zugriff auf Ihre Datenkatalogressourcen gewährt wird. Die `Super` Berechtigung ermöglicht es einem Prinzipal, jeden unterstützten Lake Formation Formation-Vorgang in der Datenbank oder Tabelle auszuführen, für die sie erteilt wurde.

Gehen Sie wie folgt vor, um die Sicherheitseinstellungen so zu ändern, dass der Zugriff auf Datenkatalogressourcen (Datenbanken und Tabellen) über Lake Formation Formation-Berechtigungen verwaltet wird:

1. Ändern Sie die Standardsicherheitseinstellungen für neue Ressourcen. Detaillierte Anweisungen finden Sie unter [Ändern Sie das Standardberechtigungsmodell oder verwenden Sie den hybriden Zugriffsmodus](#).
2. Ändern Sie die Einstellungen für vorhandene Datenkatalogressourcen. Detaillierte Anweisungen finden Sie unter [AWS Glue Datenberechtigungen für das AWS Lake Formation Modell aktualisieren](#).

Ändern der Standardsicherheitseinstellungen mithilfe des Lake Formation **`PutDataLakeSettings`** API-Vorgangs

Sie können die Standardsicherheitseinstellungen auch mithilfe des Lake Formation [PutDataLakeSettings](#) API-Vorgangs ändern. Diese Aktion verwendet als Argumente eine optionale Katalog-ID und eine [DataLakeSettings](#) Struktur.

Um Metadaten und die zugrundeliegende Datenzugriffskontrolle durch Lake Formation für neue Datenbanken und Tabellen durchzusetzen, codieren Sie die `DataLakeSettings` Struktur wie folgt.

 Note

<AccountID> Ersetzen Sie es durch eine gültige AWS Konto-ID und *<Username>* einen gültigen IAM-Benutzernamen. Sie können mehr als einen Benutzer als Data Lake-Administrator angeben.

```
{
  "DataLakeSettings": {
    "DataLakeAdmins": [
      {
        "DataLakePrincipalIdentifier":
"arn:aws:iam::<AccountId>:user/<Username>"
      }
    ],
    "CreateDatabaseDefaultPermissions": [],
    "CreateTableDefaultPermissions": []
  }
}
```

Sie können die Struktur auch wie folgt codieren. Das Weglassen des `CreateTableDefaultPermissions` Parameters `CreateDatabaseDefaultPermissions` oder entspricht der Übergabe einer leeren Liste.

```
{
  "DataLakeSettings": {
    "DataLakeAdmins": [
      {
        "DataLakePrincipalIdentifier":
"arn:aws:iam::<AccountId>:user/<Username>"
      }
    ]
  }
}
```

Durch diese Aktion werden der IAMAllowedPrincipals Gruppe effektiv alle Lake Formation Formation-Berechtigungen für neue Datenbanken und Tabellen entzogen. Wenn Sie eine Datenbank erstellen, können Sie diese Einstellung überschreiben.

Um Metadaten und die zugrundeliegende Datenzugriffskontrolle nur durch IAM für neue Datenbanken und Tabellen durchzusetzen, codieren Sie die DataLakeSettings Struktur wie folgt.

```
{
  "DataLakeSettings": {
    "DataLakeAdmins": [
      {
        "DataLakePrincipalIdentifier":
"arn:aws:iam::<AccountId>:user/<Username>"
      }
    ],
    "CreateDatabaseDefaultPermissions": [
      {
        "Principal": {
          "DataLakePrincipalIdentifier": "IAM_ALLOWED_PRINCIPALS"
        },
        "Permissions": [
          "ALL"
        ]
      }
    ],
    "CreateTableDefaultPermissions": [
      {
        "Principal": {
          "DataLakePrincipalIdentifier": "IAM_ALLOWED_PRINCIPALS"
        },
        "Permissions": [
          "ALL"
        ]
      }
    ]
  }
}
```

Dadurch erhält die IAMAllowedPrincipals Gruppe Super Lake Formation die Erlaubnis, neue Datenbanken und Tabellen zu verwenden. Wenn Sie eine Datenbank erstellen, können Sie diese Einstellung überschreiben.

 Note

In der vorherigen `DataLakeSettings` Struktur ist der einzig zulässige Wert für `DataLakePrincipalIdentifier` `iam_allowed_principals`, und der einzig zulässige Wert für `Permissions` `all`.

Implizite Lake Formation Formation-Berechtigungen

AWS Lake Formation gewährt Data Lake-Administratoren, Datenbankerstellern und Tabellenerstellern die folgenden impliziten Berechtigungen.

Data Lake-Administratoren

- Sie haben `Describe` Zugriff auf alle Ressourcen im Datenkatalog, mit Ausnahme von Ressourcen, die von einem anderen Konto direkt für einen anderen Principal freigegeben wurden. Dieser Zugriff kann einem Administrator nicht entzogen werden.
- Verfügen Sie überall im Data Lake über Berechtigungen zum Speicherort von Daten.
- Kann jedem Prinzipal (auch sich selbst) Zugriff auf alle Ressourcen im Datenkatalog gewähren oder entziehen. Dieser Zugriff kann einem Administrator nicht entzogen werden.
- Kann Datenbanken im Datenkatalog erstellen.
- Kann einem anderen Benutzer die Erlaubnis erteilen, eine Datenbank zu erstellen.

 Note

Data Lake-Administratoren können Amazon S3 S3-Standorte nur registrieren, wenn sie über die entsprechenden IAM-Berechtigungen verfügen. Die in diesem Handbuch empfohlenen Data Lake-Administratorrichtlinien gewähren diese Berechtigungen. Außerdem verfügen Data Lake-Administratoren nicht über implizite Berechtigungen zum Löschen von Datenbanken oder `alter/drop` Tabellen, die von anderen erstellt wurden. Sie können sich jedoch selbst die entsprechenden Berechtigungen gewähren.

Weitere Informationen zu Data Lake-Administratoren finden Sie unter [Erstellen Sie einen Data Lake-Administrator](#).

Ersteller des Katalogs

- Sie verfügen über alle Katalogberechtigungen für Kataloge, die sie erstellen, verfügen über Berechtigungen für Datenbanken und Tabellen, die sie im Katalog erstellen, und können anderen Hauptbenutzern desselben AWS Kontos die Berechtigung erteilen, Datenbanken und Tabellen im Katalog zu erstellen. Ein Katalogersteller, der auch über die `AWSLakeFormationCrossAccountManager` AWS verwaltete Richtlinie verfügt, kann anderen AWS Konten oder Organisationen Berechtigungen für den Katalog gewähren.

Data Lake-Administratoren können die Lake Formation Formation-Konsole oder die API verwenden, um Katalogersteller zu benennen.



Note

Katalogersteller verfügen nicht implizit über Berechtigungen für Datenbanken und Tabellen, die andere Benutzer im Katalog erstellen.

Weitere Informationen zum Erstellen von Katalogen finden Sie unter [Bringen Sie Ihre Daten in die AWS Glue Data Catalog](#)

Ersteller von Datenbanken

- Sie verfügen über alle Datenbankberechtigungen für Datenbanken, die sie erstellen, verfügen über Berechtigungen für Tabellen, die sie in der Datenbank erstellen, und können anderen Prinzipalen in demselben AWS Konto die Berechtigung erteilen, Tabellen in der Datenbank zu erstellen. Ein Datenbankersteller, der auch über die `AWSLakeFormationCrossAccountManager` AWS verwaltete Richtlinie verfügt, kann anderen AWS Konten oder Organisationen Berechtigungen für die Datenbank gewähren.

Data Lake-Administratoren können die Lake Formation Formation-Konsole oder die API verwenden, um Datenbankersteller zu benennen.



Note

Datenbankersteller verfügen nicht implizit über Berechtigungen für Tabellen, die andere Benutzer in der Datenbank erstellen.

Weitere Informationen finden Sie unter [Erstellen einer Datenbank](#).

Ersteller von Tabellen

- Sie verfügen über alle Berechtigungen für Tabellen, die sie erstellen.
- Kann Prinzipalen im selben AWS Konto Berechtigungen für alle von ihnen erstellten Tabellen gewähren.
- Kann anderen AWS Konten oder Organisationen Berechtigungen für alle von ihnen erstellten Tabellen gewähren, wenn diese über die `AWSLakeFormationCrossAccountManager` AWS verwaltete Richtlinie verfügen.
- Kann die Datenbanken anzeigen, die die von ihnen erstellten Tabellen enthalten.

Referenz zu den Genehmigungen von Lake Formation

Zur Ausführung von AWS Lake Formation Vorgängen benötigen Principals sowohl Lake Formation Formation-Berechtigungen als auch AWS Identity and Access Management (IAM) -Berechtigungen. In der Regel gewähren Sie IAM-Berechtigungen mithilfe von groben Zugriffskontrollrichtlinien, wie unter beschrieben. [the section called “Überblick über die Genehmigungen für Lake Formation”](#) Sie können Lake Formation Formation-Berechtigungen mithilfe der Konsole, der API oder der AWS Command Line Interface (AWS CLI) gewähren.

Informationen zum Erteilen oder Widerrufen Lake Formation Formation-Berechtigungen finden Sie unter [the section called “Erteilen von Datenberechtigungen”](#) und [the section called “Erteilung von Berechtigungen zum Speicherort von Daten”](#).

Note

Die Beispiele in diesem Abschnitt zeigen, wie Prinzipalen im selben AWS Konto Berechtigungen erteilt werden. Beispiele für kontenübergreifende Zuschüsse finden Sie unter [the section called “Kontoübergreifender Datenaustausch”](#)

Lake Formation Formation-Berechtigungen pro Ressourcentyp

Im Folgenden sind die gültigen Lake Formation Formation-Berechtigungen aufgeführt, die für jeden Ressourcentyp verfügbar sind:

Ressource	Berechtigung	
Catalog	ALL(Super), Superuser	
	ALTER	
	CREATE_DATABASE	
	DESCRIBE	
	DROP	
Database	ALL (Super)	
	ALTER	
	CREATE_TABLE	
	DESCRIBE	
	DROP	
Table	ALL (Super)	
	ALTER	
	DELETE	
	DESCRIBE	
	DROP	
	INSERT	
	SELECT	
View	ALL (Super)	
	SELECT	
	DESCRIBE	

Ressource	Berechtigung	
	DROP	
Data Catalog	CREATE_DATABASE	
Amazon S3 location	DATA_LOCATION_ACCESS	
LF-Tags	DROP	
	ALTER	
LF-Tag values	ASSOCIATE	
	DESCRIBE	
	GrantWithLFTagExpression	
LF-Tag policy - Database	ALL (Super)	
	ALTER	
	CREATE_TABLE	
	DESCRIBE	
	DROP	
LF-Tag policy - Table	ALL (Super)	
	ALTER	
	DESCRIBE	
	DELETE	
	DROP	
	INSERT	
	SELECT	

Ressource	Berechtigung	
Resource link - Database or Table	DESCRIBE	
	DROP	
Table with data filters	DESCRIBE	
	DROP	
	SELECT	
Table with column filter	SELECT	

Themen

- [Lake Formation erteilt und widerruft AWS CLI Befehle](#)
- [Lake-Formation-Berechtigungen](#)

Lake Formation erteilt und widerruft AWS CLI Befehle

Jede Berechtigungsbeschreibung in diesem Abschnitt enthält Beispiele für die Erteilung der Berechtigung mithilfe eines AWS CLI Befehls. Im Folgenden finden Sie die Zusammenfassungen der Lake Formation grant-permissions und revoke-permissions AWS CLI der Befehle.

```
grant-permissions
[--catalog-id <value>]
--principal <value>
--resource <value>
--permissions <value>
[--permissions-with-grant-option <value>]
[--cli-input-json <value>]
[--generate-cli-skeleton <value>]
```

```
revoke-permissions
[--catalog-id <value>]
--principal <value>
--resource <value>
```

```
--permissions <value>
[--permissions-with-grant-option <value>]
[--cli-input-json <value>]
[--generate-cli-skeleton <value>]
```

Eine ausführliche Beschreibung dieser Befehle finden Sie unter [grant-permissions und revoke-permissions](#) in der Befehlsreferenz.AWS CLI Dieser Abschnitt enthält zusätzliche Informationen zu dieser Option. `--principal`

Der Wert der `--principal` Option ist einer der folgenden:

- Amazon-Ressourcenname (ARN) für einen AWS Identity and Access Management (IAM) -Benutzer oder eine Rolle
- ARN für einen Benutzer oder eine Gruppe, die sich über einen SAML-Anbieter wie Microsoft Active Directory Federation Service (AD FS) authentifiziert
- ARN für einen Amazon Quick-Benutzer oder eine Gruppe
- Für kontoübergreifende Berechtigungen eine AWS Konto-ID, eine Organisations-ID oder eine Organisationseinheits-ID
- Für IAM Identity Center-Benutzer oder -Gruppe, ARN für IAM Identity Center-Benutzer oder -Gruppe.

Im Folgenden finden Sie Syntax und Beispiele für alle `--principal` Typen.

Principal ist ein IAM-Benutzer

Syntax:

```
--principal DataLakePrincipalIdentifier=arn:aws:iam::<account-id>:user/<user-name>
```

Beispiel:

```
--principal DataLakePrincipalIdentifier=arn:aws:iam::111122223333:user/
datalake_user1
```

Principal ist eine IAM-Rolle

Syntax:

```
--principal DataLakePrincipalIdentifier=arn:aws:iam::<account-id>:role/<role-name>
```

Beispiel:

```
--principal DataLakePrincipalIdentifier=arn:aws:iam::111122223333:role/workflowrole
```

Principal ist ein Benutzer, der sich über einen SAML-Anbieter authentifiziert

Syntax:

```
--principal DataLakePrincipalIdentifier=arn:aws:iam::<account-id>:saml-provider/<SAMLproviderName>:user/<user-name>
```

Beispiele:

```
--principal DataLakePrincipalIdentifier=arn:aws:iam::111122223333:saml-provider/idp1:user/datalake_user1
```

```
--principal DataLakePrincipalIdentifier=arn:aws:iam::111122223333:saml-provider/AthenaLakeFormation0kta:user/athena-user@example.com
```

Principal ist eine Gruppe, die sich über einen SAML-Anbieter authentifiziert

Syntax:

```
--principal DataLakePrincipalIdentifier=arn:aws:iam::<account-id>:saml-provider/<SAMLproviderName>:group/<group-name>
```

Beispiele:

```
--principal DataLakePrincipalIdentifier=arn:aws:iam::111122223333:saml-provider/idp1:group/data-scientists
```

```
--principal DataLakePrincipalIdentifier=arn:aws:iam::111122223333:saml-provider/AthenaLakeFormation0kta:group/my-group
```

Principal ist ein Benutzer der Amazon Quick Enterprise Edition

Syntax:

```
--principal DataLakePrincipalIdentifier=arn:aws:quicksight:<region>:<account-id>:user/<namespace>/<user-name>
```

 Note

Für *<namespace>* müssen Sie default angeben.

Beispiel:

```
--principal DataLakePrincipalIdentifier=arn:aws:quicksight:us-east-1:111122223333:user/default/bi_user1
```

Principal ist eine Amazon Quick Enterprise Edition-Gruppe

Syntax:

```
--principal DataLakePrincipalIdentifier=arn:aws:quicksight:<region>:<account-id>:group/<namespace>/<group-name>
```

 Note

Für *<namespace>* müssen Sie default angeben.

Beispiel:

```
--principal DataLakePrincipalIdentifier=arn:aws:quicksight:us-east-1:111122223333:group/default/data_scientists
```

Principal ist ein AWS Konto

Syntax:

```
--principal DataLakePrincipalIdentifier=<account-id>
```

Beispiel:

```
--principal DataLakePrincipalIdentifier=111122223333
```

Principal ist eine Organisation

Syntax:

```
--principal DataLakePrincipalIdentifier=arn:aws:organizations::<account-id>:organization/<organization-id>
```

Beispiel:

```
--principal  
DataLakePrincipalIdentifier=arn:aws:organizations::111122223333:organization/o-  
abcdefghijkl
```

Principal ist eine Organisationseinheit

Syntax:

```
--principal DataLakePrincipalIdentifier=arn:aws:organizations::<account-id>:ou/<organization-id>/<organizational-unit-id>
```

Beispiel:

```
--principal DataLakePrincipalIdentifier=arn:aws:organizations::111122223333:ou/o-  
abcdefghijkl/ou-ab00-cdefghij
```

Principal ist ein IAM Identity Center-Identitätsbenutzer oder eine Identitätsgruppe

Beispiel: Benutzer

```
--principal DataLakePrincipalIdentifier=arn:aws:identitystore:::user/<UserID>
```

Beispiel: Gruppe:

```
--principal DataLakePrincipalIdentifier=arn:aws:identitystore:::group/<GroupID>
```

Principal ist eine IAM-Gruppe - **IAMAllowedPrincipals**

Lake Formation legt einer Gruppe, die **IAMAllowedPrincipals** standardmäßig aufgerufen wird, Super Berechtigungen für alle Datenbanken und Tabellen im Datenkatalog fest. Wenn

diese Gruppenberechtigung für eine Datenbank oder eine Tabelle existiert, haben alle Prinzipale in Ihrem Konto über die IAM-Prinzipalrichtlinien für Zugriff auf die Ressource. AWS Glue Es bietet Abwärtskompatibilität, wenn Sie beginnen, Lake Formation Formation-Berechtigungen zu verwenden, um die Datenkatalogressourcen zu sichern, für die zuvor durch IAM-Richtlinien geschützt waren. AWS Glue

Wenn Sie Lake Formation verwenden, um Berechtigungen für Ihre Data Catalog-Ressourcen zu verwalten, müssen Sie zuerst die IAMAllowedPrincipals Berechtigungen für die Ressourcen widerrufen oder die Principals und die Ressourcen für den Hybridzugriffsmodus aktivieren, damit die Lake Formation Formation-Berechtigungen funktionieren.

Beispiel:

```
--principal DataLakePrincipalIdentifier=IAM_Allowed_Principals
```

Principal ist eine IAM-Gruppe - **ALLIAMPrincipals**

Wenn Sie ALLIAMPrincipals Gruppenberechtigungen für eine Datenkatalogressource gewähren, erhält jeder Prinzipal im Konto mithilfe von Lake Formation Formation-Berechtigungen und IAM-Berechtigungen Zugriff auf die Datenkatalogressource.

Beispiel:

```
--principal DataLakePrincipalIdentifier=123456789012:IAMPrincipals
```

Lake-Formation-Berechtigungen

Dieser Abschnitt enthält die verfügbaren Lake Formation Formation-Berechtigungen, die Sie Principals gewähren können.

ALTER

Berechtigung	Für diese Ressource gewährt	Der Stipendiat braucht auch
ALTER	DATABASE	glue:UpdateDatabase
ALTER	TABLE	glue:UpdateTable

Berechtigung	Für diese Ressource gewährt	Der Stipendiat braucht auch
ALTER	LF-Tag	lakeformation:UpdateLFTag

Ein Principal mit dieser Berechtigung kann Metadaten für eine Datenbank oder Tabelle im Datenkatalog ändern. Bei Tabellen können Sie das Spaltenschema ändern und Spaltenparameter hinzufügen. Sie können keine Spalten in den zugrunde liegenden Daten ändern, auf die eine Metadatentabelle verweist.

Wenn es sich bei der Eigenschaft, die geändert wird, um einen registrierten Amazon Simple Storage Service (Amazon S3) -Standort handelt, muss der Principal über Datenstandortberechtigungen für den neuen Standort verfügen.

Example

Im folgenden Beispiel wird dem Benutzer die ALTER Berechtigung für die Datenbank `datalake_user1 retail` im AWS Konto 1111-2222-3333 erteilt.

```
aws lakeformation grant-permissions --principal
  DataLakePrincipalIdentifier=arn:aws:iam::111122223333:user/datalake_user1 --
permissions "ALTER" --resource '{ "Database": {"Name":"retail"}}'
```

Example

Das folgende Beispiel erteilt einem Benutzer Zugriff `datalake_user1` auf ALTER die Tabelle in der Datenbank `inventory retail`

```
aws lakeformation grant-permissions --principal
  DataLakePrincipalIdentifier=arn:aws:iam::111122223333:user/datalake_user1
--permissions "ALTER" --resource '{ "Table": {"DatabaseName":"retail",
"Name":"inventory"}}'
```

CREATE_DATABASE

Berechtigung	Für diese Ressource gewährt	Der Stipendiat braucht auch
CREATE_DATABASE	Data Catalog	glue:CreateDatabase

Ein Principal mit dieser Berechtigung kann eine Metadaten Datenbank oder einen Ressourcenlink im Datenkatalog erstellen. Der Principal kann auch Tabellen in der Datenbank erstellen.

Example

Das folgende Beispiel gewährt dem Benutzer `CREATE_DATABASE` das AWS Konto `datalake_user1 1111-2222-3333`.

```
aws lakeformation grant-permissions --principal
DataLakePrincipalIdentifier=arn:aws:iam::111122223333:user/datalake_user1 --
permissions "CREATE_DATABASE" --resource '{ "Catalog": {} }'
```

Wenn ein Principal eine Datenbank im Datenkatalog erstellt, werden keine Berechtigungen für die zugrunde liegenden Daten gewährt. Die folgenden zusätzlichen Metadatenberechtigungen werden gewährt (zusammen mit der Möglichkeit, diese Berechtigungen anderen zu gewähren):

- `CREATE_TABLE` in der Datenbank
- `ALTER` Datenbank
- `DROP` Datenbank

Beim Erstellen einer Datenbank kann der Principal optional einen Amazon S3 S3-Standort angeben. Je nachdem, ob der Prinzipal über Datenspeicherberechtigungen verfügt, reicht die `CREATE_DATABASE` Berechtigung möglicherweise nicht in allen Fällen aus, um Datenbanken zu erstellen. Es ist wichtig, die folgenden drei Fälle zu berücksichtigen.

Erstellen Sie einen Datenbank-Anwendungsfall	Berechtigungen erforderlich
Die Standorteigenschaft ist nicht spezifiziert.	<code>CREATE_DATABASE</code> ist ausreichend.
Die Standorteigenschaft ist angegeben, und der Standort wird nicht von Lake Formation verwaltet (ist nicht registriert).	<code>CREATE_DATABASE</code> ist ausreichend.
Die Standorteigenschaft ist angegeben, und der Standort wird von Lake Formation verwaltet (ist registriert).	<code>CREATE_DATABASE</code> ist erforderlich, zuzüglich der Berechtigungen für den Datenspeicherort für den angegebenen Standort.

CREATE_TABLE

Berechtigung	Für diese Ressource gewährt	Der Stipendiat braucht auch
CREATE_TABLE	DATABASE	glue:CreateTable

Ein Principal mit dieser Berechtigung kann eine Metadatentabelle oder einen Ressourcenlink im Datenkatalog innerhalb der angegebenen Datenbank erstellen.

Example

Im folgenden Beispiel wird dem Benutzer die `datalake_user1` Berechtigung erteilt, Tabellen in der `retail` Datenbank im AWS Konto 1111-2222-3333 zu erstellen.

```
aws lakeformation grant-permissions --principal
DataLakePrincipalIdentifier=arn:aws:iam::111122223333:user/datalake_user1
--permissions "CREATE_TABLE" --resource '{ "Database": {"Name":"retail"} }'
```

Wenn ein Principal eine Tabelle im Datenkatalog erstellt, werden dem Prinzipal alle Lake Formation Formation-Berechtigungen für die Tabelle gewährt, mit der Möglichkeit, diese Berechtigungen anderen zu gewähren.

Kontoübergreifende Zuschüsse

Wenn ein Datenbankeigentümerkonto einem Empfängerkonto Zuschüsse gewährt `CREATE_TABLE` und ein Benutzer des Empfängerkontos erfolgreich eine Tabelle in der Datenbank des Besitzerkontos erstellt, gelten die folgenden Regeln:

- Der Benutzer und die Data Lake-Administratoren im Empfängerkonto verfügen über alle Lake Formation Formation-Berechtigungen für die Tabelle. Sie können anderen Principals in ihrem Konto Berechtigungen für die Tabelle gewähren. Sie können Prinzipalen im Besitzerkonto oder in anderen Konten keine Berechtigungen erteilen.
- Data Lake-Administratoren im Besitzerkonto können anderen Prinzipalen in ihrem Konto Berechtigungen für die Tabelle gewähren.

Berechtigungen zum Speicherort von Daten

Wenn Sie versuchen, eine Tabelle zu erstellen, die auf einen Amazon S3 S3-Standort verweist, reicht die `CREATE_TABLE` Berechtigung möglicherweise nicht aus, um eine Tabelle zu erstellen, je nachdem, ob Sie über Datenstandortberechtigungen verfügen. Es ist wichtig, die folgenden drei Fälle zu berücksichtigen.

Erstellen Sie einen Anwendungsfall für Tabellen	Berechtigungen erforderlich
Der angegebene Standort wird nicht von Lake Formation verwaltet (ist nicht registriert).	<code>CREATE_TABLE</code> ist ausreichend.
Der angegebene Standort wird von Lake Formation verwaltet (ist registriert), und die enthaltene Datenbank hat keine Standorteigenschaft oder eine Standorteigenschaft, die kein Amazon S3 S3-Präfix des Tabellenstandorts ist.	<code>CREATE_TABLE</code> ist erforderlich plus Datenspeicherberechtigungen für den angegebenen Standort.
Der angegebene Standort wird von Lake Formation verwaltet (ist registriert), und die enthaltene Datenbank hat eine Standorteigenschaft, die auf einen registrierten Standort verweist und ein Amazon S3 S3-Präfix des Tabellenstandorts ist.	<code>CREATE_TABLE</code> ist ausreichend.

DATA_LOCATION_ACCESS

Berechtigung	Auf dieser Ressource gewährt	Der Stipendiat braucht auch
<code>DATA_LOCATION_ACCESS</code>	Amazon-S3-Speicherort	(Amazon S3 S3-Berechtigungen für den Standort, die durch die Rolle angegeben werden müssen, die für die Registrierung des Standorts verwendet wurde.)

Dies ist die einzige Berechtigung zum Speicherort von Daten. Ein Principal mit dieser Berechtigung kann eine Metadaten-Datenbank oder -Tabelle erstellen, die auf den angegebenen Amazon S3 S3-Speicherort verweist. Der Standort muss registriert sein. Ein Principal, der über Datenspeicherberechtigungen für einen Standort verfügt, verfügt auch über Standortberechtigungen für untergeordnete Standorte.

Example

Im folgenden Beispiel werden dem Benutzer `datalake_user1` im AWS Konto `1111-2222-3333` Berechtigungen `s3://products/retail` zum Speicherort von Daten erteilt.

```
aws lakeformation grant-permissions --principal
DataLakePrincipalIdentifier=arn:aws:iam::111122223333:user/datalake_user1
--permissions "DATA_LOCATION_ACCESS" --resource '{ "DataLocation":
{"ResourceArn":"arn:aws:s3:::products/retail"} }'
```

`DATA_LOCATION_ACCESS` ist nicht erforderlich, um die zugrunde liegenden Daten abzufragen oder zu aktualisieren. Diese Berechtigung gilt nur für das Erstellen von Datenkatalogressourcen.

Weitere Informationen zu Berechtigungen zum Speicherort von Daten finden Sie unter [Underlying data access control](#).

DELETE

Berechtigung	Für diese Ressource gewährt	Der Stipendiat braucht auch
DELETE	TABLE	(Wenn der Standort registriert ist, sind keine zusätzlichen IAM-Berechtigungen erforderlich.)

Ein Principal mit dieser Berechtigung kann die zugrunde liegenden Daten an dem in der Tabelle angegebenen Amazon S3 S3-Standort einfügen, aktualisieren und lesen. Der Principal kann die Tabelle auch in der Lake Formation Formation-Konsole anzeigen und Informationen über die Tabelle mit der AWS Glue API abrufen.

Example

Im folgenden Beispiel wird dem Benutzer die DELETE Berechtigung für die Tabelle inventory in datalake_user1 der Datenbank retail im AWS Konto 1111-2222-3333 erteilt.

```
aws lakeformation grant-permissions --principal
DataLakePrincipalIdentifier=arn:aws:iam::111122223333:user/datalake_user1
--permissions "DELETE" --resource '{ "Table": {"DatabaseName":"retail",
"Name":"inventory"}}'
```

Diese Berechtigung gilt nur für Daten in Amazon S3 und nicht für Daten in anderen Datenspeichern wie Amazon Relational Database Service (Amazon RDS).

DESCRIBE

Berechtigung	Für diese Ressource gewährt	Der Stipendiat braucht auch
DESCRIBE	Link zur Tabellenressource	glue:GetTable
	Link zur Datenbankressource	glue:GetDatabase
DESCRIBE	DATABASE	glue:GetDatabase
DESCRIBE	TABLE	glue:GetTable
DESCRIBE	LF-Tag	glue:GetTable
		glue:GetDatabase
		lakeformation:GetResourceLFTags
		lakeformation:ListLFTags
		lakeformation:GetLFTag
		lakeformation:SearchTablesByLFTags

Berechtigung	Für diese Ressource gewährt	Der Stipendiat braucht auch
		lakeformation:SearchDatabasesByLFTags

Ein Principal mit dieser Berechtigung kann die angegebene Datenbank, Tabelle oder den angegebenen Ressourcenlink anzeigen. Es werden keine anderen Datenkatalogberechtigungen implizit gewährt, und es werden keine Datenzugriffsberechtigungen implizit gewährt. Datenbanken und Tabellen werden in den Abfrage-Editoren integrierter Services angezeigt, aber es können keine Abfragen an sie gestellt werden, sofern nicht andere Lake Formation Formation-Berechtigungen (z. B. SELECT) erteilt wurden.

Beispielsweise kann ein Benutzer, der DESCRIBE über eine Datenbank verfügt, die Datenbank und alle Datenbankmetadaten (Beschreibung, Speicherort usw.) sehen. Der Benutzer kann jedoch nicht herausfinden, welche Tabellen die Datenbank enthält, und er kann keine Tabellen in der Datenbank löschen, ändern oder erstellen. Ebenso kann ein Benutzer, der DESCRIBE über eine Tabelle verfügt, die Tabelle und die Tabellenmetadaten (Beschreibung, Schema, Speicherort usw.) sehen, aber keine Abfragen für die Tabelle löschen, ändern oder ausführen.

Im Folgenden finden Sie einige zusätzliche Regeln für DESCRIBE:

- Wenn ein Benutzer andere Lake Formation Formation-Berechtigungen für eine Datenbank, Tabelle oder einen Ressourcenlink hat, DESCRIBE wird dies implizit gewährt.
- Wenn ein Benutzer nur SELECT über eine Teilmenge von Spalten für eine Tabelle verfügt (teilweise SELECT), kann der Benutzer nur diese Spalten sehen.
- Einem Benutzer DESCRIBE, der in einer Tabelle nur teilweise eine Auswahl getroffen hat, können Sie keine Zugriffsrechte gewähren. Umgekehrt können Sie für Tabellen, für die eine Erteilung gewährt wurde, keine Liste mit Aufnahme- oder Ausschlusslisten für Spalten angeben. DESCRIBE

Example

Im folgenden Beispiel wird dem Benutzer `datalake_user1` die DESCRIBE Berechtigung für den Link zur Tabellenressource `inventory-link` in der Datenbank `retail` im AWS Konto `1111-2222-3333` erteilt.

```
aws lakeformation grant-permissions --principal
DataLakePrincipalIdentifier=arn:aws:iam::111122223333:user/datalake_user1
```

```
--permissions "DESCRIBE" --resource '{ "Table": {"DatabaseName":"retail",
"Name":"inventory-link"}}'
```

DROP

Berechtigung	Für diese Ressource erteilt	Der Stipendiat braucht auch
DROP	DATABASE	glue:DeleteDatabase
DROP	TABLE	glue:DeleteTable
DROP	LF-Tag	lakeformation:DeleteLFTag
DROP	Link zur Datenbankressource	glue:DeleteDatabase
	Link zur Tabellenressource	glue:DeleteTable

Ein Principal mit dieser Berechtigung kann einen Datenbank-, Tabellen- oder Ressourcenlink im Datenkatalog löschen. Sie können DROP für eine Datenbank nicht einem externen Konto oder einer externen Organisation gewähren.

Warning

Beim Löschen einer Datenbank werden alle Tabellen in der Datenbank gelöscht.

Example

Im folgenden Beispiel wird dem Benutzer die DROP Berechtigung für die Datenbank `datalake_user1 retail` im AWS Konto `1111-2222-3333` erteilt.

```
aws lakeformation grant-permissions --principal
DataLakePrincipalIdentifier=arn:aws:iam::111122223333:user/datalake_user1 --
permissions "DROP" --resource '{ "Database": {"Name":"retail"}}'
```


Example

Das folgende Beispiel erteilt dem Benutzer DROP Zugriff datalake_user1 auf die Tabelle in der Datenbank. inventory retail

```
aws lakeformation grant-permissions --principal
DataLakePrincipalIdentifier=arn:aws:iam::111122223333:user/datalake_user1
--permissions "DROP" --resource '{ "Table": {"DatabaseName":"retail",
"Name":"inventory"}}'
```

Example

Im folgenden Beispiel wird DROP dem Benutzer für datalake_user1 die Tabelle ein Ressourcenlink inventory-link in der Datenbank gewährtretail.

```
aws lakeformation grant-permissions --principal
DataLakePrincipalIdentifier=arn:aws:iam::111122223333:user/datalake_user1 --
permissions "DROP" --resource '{ "Table": {"DatabaseName":"retail", "Name":"inventory-
link"}}'
```

INSERT

Berechtigung	Für diese Ressource gewährt	Der Stipendiat braucht auch
INSERT	TABLE	(Wenn der Standort registrie rt ist, sind keine zusätzlichen IAM-Berechtigungen erforderl ich.)

Ein Principal mit dieser Berechtigung kann die zugrunde liegenden Daten an dem in der Tabelle angegebenen Amazon S3 S3-Standort einfügen, aktualisieren und lesen. Der Principal kann die Tabelle auch in der Lake Formation Formation-Konsole anzeigen und Informationen über die Tabelle mit der AWS Glue API abrufen.

Example

Im folgenden Beispiel wird dem Benutzer die INSERT Berechtigung für die Tabelle inventory in datalake_user1 der Datenbank retail im AWS Konto 1111-2222-3333 erteilt.

```
aws lakeformation grant-permissions --principal
DataLakePrincipalIdentifier=arn:aws:iam::111122223333:user/datalake_user1
--permissions "INSERT" --resource '{ "Table": {"DatabaseName":"retail",
"Name":"inventory"}}'
```

Diese Berechtigung gilt nur für Daten in Amazon S3 und nicht für Daten in anderen Datenspeichern wie Amazon RDS.

SELECT

Berechtigung	Für diese Ressource gewährt	Der Stipendiat braucht auch
SELECT	• TABLE	(Wenn der Standort registriert ist, sind keine zusätzlichen IAM-Berechtigungen erforderlich.)

Ein Principal mit dieser Berechtigung kann eine Tabelle im Datenkatalog anzeigen und die zugrunde liegenden Daten in Amazon S3 an dem in der Tabelle angegebenen Speicherort abfragen. Der Principal kann die Tabelle in der Lake Formation Konsole anzeigen und Informationen über die Tabelle mit der AWS Glue API abrufen. Wenn bei der Erteilung dieser Berechtigung eine Spaltenfilterung angewendet wurde, kann der Principal die Metadaten nur für die enthaltenen Spalten anzeigen und nur Daten aus den enthaltenen Spalten abfragen.

Note

Es liegt in der Verantwortung des integrierten Analysedienstes, die Spaltenfilterung bei der Verarbeitung einer Abfrage anzuwenden.

Example

Im folgenden Beispiel wird dem Benutzer die SELECT Berechtigung für die Tabelle `inventory` in `datalake_user1` der Datenbank `retail` im AWS Konto `1111-2222-3333` erteilt.

```
aws lakeformation grant-permissions --principal
DataLakePrincipalIdentifier=arn:aws:iam::111122223333:user/datalake_user1
```

```
--permissions "SELECT" --resource '{ "Table": {"DatabaseName":"retail",  
"Name":"inventory"}}'
```

Diese Berechtigung gilt nur für Daten in Amazon S3 und nicht für Daten in anderen Datenspeichern wie Amazon RDS.

Sie können bestimmte Spalten mit einer optionalen Aufnahme- oder Ausschlussliste filtern (den Zugriff darauf einschränken). Eine Aufnahmeliste gibt die Spalten an, auf die zugegriffen werden kann. Eine Ausschlussliste gibt die Spalten an, auf die nicht zugegriffen werden kann. In Ermangelung einer Aufnahme- oder Ausschlussliste sind alle Tabellenspalten zugänglich.

Die Ergebnisse von `glue:GetTable` geben nur die Spalten zurück, zu deren Anzeige der Aufrufer berechtigt ist. Integrierte Dienste wie Amazon Athena und Amazon Redshift berücksichtigen Spalten mit Ein- und Ausschlusslisten.

Example

Das folgende Beispiel gewährt `SELECT` dem Benutzer `datalake_user1` in der Tabelle `inventory` mithilfe einer Aufnahmeliste Zuteilungen.

```
aws lakeformation grant-permissions --principal  
DataLakePrincipalIdentifier=arn:aws:iam::111122223333:user/datalake_user1 --  
permissions "SELECT" --resource '{ "TableWithColumns": {"DatabaseName":"retail",  
"Name":"inventory", "ColumnNames": ["prodcode","location","period","withdrawals"]}}'
```

Example

Im nächsten Beispiel wird mithilfe einer Ausschlussliste für die `inventory` Tabelle gewährt `SELECT`.

```
aws lakeformation grant-permissions --principal  
DataLakePrincipalIdentifier=arn:aws:iam::111122223333:user/datalake_user1 --  
permissions "SELECT" --resource '{ "TableWithColumns": {"DatabaseName":"retail",  
"Name":"inventory", "ColumnWildcard": {"ExcludedColumnNames": ["intkey",  
"prodcode"]}}}'
```

Für die `SELECT` Genehmigung gelten die folgenden Einschränkungen:

- Bei der Erteilung `SELECT` können Sie die Option „Gewährung“ nicht angeben, wenn die Spaltenfilterung angewendet wird.
- Sie können die Zugriffskontrolle nicht auf Spalten einschränken, bei denen es sich um Partitionsschlüssel handelt.

- Einem Prinzipal mit der SELECT Berechtigung für eine Teilmenge von Spalten in einer Tabelle kann dieALTER, DROPDELETE, oder INSERT -Berechtigung für diese Tabelle nicht erteilt werden. Ebenso kann einem Prinzipal mit der INSERT Berechtigung ALTER DROPDELETE,, oder für eine Tabelle die SELECT Berechtigung zur Spaltenfilterung nicht erteilt werden.

Die SELECT Berechtigung wird auf der Seite Datenberechtigungen der Lake Formation Formation-Konsole immer als separate Zeile angezeigt. Die folgende Abbildung zeigt, SELECT dass sie den Benutzern dataLake_user2 und in dataLake_user3 allen Spalten der inventory Tabelle gewährt wird.

Data permissions (8) Choose a database or table for which to review, grant or revoke user permissions.						
Find by properties						
Database: retail X Table: inventory X Clear filter						
	Principal ▾	Principal type ▾	Resource type ▾	Resource ▾	Owner account ID ▾	Permissions ▾
☐	dataLake_user3	IAM user	Table	inventory	111122223333	Insert
☐	dataLake_user3	IAM user	Column	retail.inventory.*	111122223333	Select
☐	dataLake_user2	AD user	Table	inventory	111122223333	Delete, Insert
☐	dataLake_user2	AD user	Column	retail.inventory.*	111122223333	Select

Super

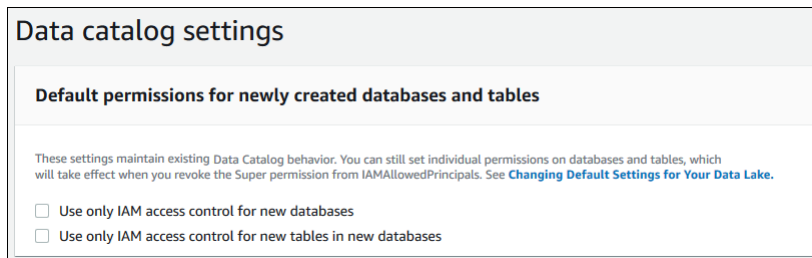
Berechtigung	Für diese Ressource gewährt	Der Stipendiat braucht auch
Super	DATABASE	glue:*Database*
Super	TABLE	glue:*Table*, glue:*Partition*

Diese Berechtigung ermöglicht es einem Principal, jeden unterstützten Lake Formation Formation-Vorgang in der Datenbank oder Tabelle auszuführen. Sie können einem externen Konto keinen Zugriff Super auf eine Datenbank gewähren.

Diese Genehmigung kann mit den anderen Lake Formation Formation-Berechtigungen koexistieren. Sie können beispielsweise die INSERT Berechtigungen SuperINSERT, und für eine Metadaten-tabelle gewähren. Der Principal kann dann alle unterstützten Operationen an der Tabelle ausführen. Beim Widerrufen Super bleiben die INSERT Berechtigungen SELECT und erhalten, und der Prinzipal kann nur Auswahl- und Einfügevorgänge ausführen.

Anstatt es einem einzelnen Prinzipal Super zu gewähren, können Sie es der Gruppe `IAMAllowedPrincipals` gewähren. Die `IAMAllowedPrincipals` Gruppe wird automatisch erstellt und umfasst alle IAM-Benutzer und -Rollen, denen gemäß Ihren IAM-Richtlinien Zugriff auf Ihre Datenkatalogressourcen gewährt wird. Wenn `IAMAllowedPrincipals` für eine Datenkatalogressource ein Zugriff gewährt Super wird, wird der Zugriff auf die Ressource effektiv ausschließlich durch IAM-Richtlinien gesteuert.

Sie können die automatische Super Genehmigung `IAMAllowedPrincipals` für neue Katalogressourcen erhalten, indem Sie die Optionen auf der Einstellungsseite der Lake Formation Formation-Konsole nutzen.



- Um allen neuen Datenbanken Zugriff Super `IAMAllowedPrincipals` zu gewähren, wählen Sie Nur IAM-Zugriffskontrolle für neue Datenbanken verwenden aus.
- Um allen neuen Tabellen in neuen Datenbanken Zugriff Super zu `IAMAllowedPrincipals` gewähren, wählen Sie Nur IAM-Zugriffskontrolle für neue Tabellen in neuen Datenbanken verwenden aus.

Note

Diese Option bewirkt, dass das Kontrollkästchen Nur IAM-Zugriffskontrolle für neue Tabellen in dieser Datenbank verwenden im Dialogfeld Datenbank erstellen standardmäßig aktiviert ist. Mehr tut es nicht. Es ist das Kontrollkästchen im Dialogfeld Datenbank erstellen, das die Erteilung von Super an aktiviert `IAMAllowedPrincipals`.

Diese Optionen auf der Einstellungsseite sind standardmäßig aktiviert. Weitere Informationen finden Sie hier:

- [the section called “Ändern der Standardeinstellungen für Ihren Data Lake”](#)
- [the section called “Aktualisierung der AWS Glue Datenberechtigungen auf das Lake Formation Formation-Modell”](#)

SUPER_USER

Berechtigung	Für diese Ressource gewährt	Der Stipendiat braucht auch
Super user	Catalog	glue:GetCatalog

Sie können die Super user Berechtigung nur bestimmten Hauptbenutzern für Kataloge innerhalb des Standarddatenkatalogs gewähren. Sie können keine Super user Berechtigungen für den Standardkatalog oder für andere Ressourcentypen wie Datenbanken und Tabellen oder für Prinzipale in externen Konten gewähren. Die Super user Berechtigungs-berechtigung ermöglicht es einem Prinzipal, jeden unterstützten Lake Formation Formation-Vorgang für die Datenbanken und Tabellen innerhalb des erteilten Katalogs auszuführen.

Mit der Super user Berechtigung kann der Hauptbenutzer (Empfänger) die folgenden Aktionen mit den Ressourcen (Kataloge, Datenbanken und Tabellen) innerhalb des Katalogs ausführen:

- CREATE_DATABASE, DESCRIBE Berechtigungen für den Katalog.
- DROP, ALTERCREATE_TABLE, DESCRIBE (effektivSUPER) Berechtigungen für alle Datenbanken innerhalb des Katalogs.
- DROP,ALTER,DESCRIBE, SELECTINSERT, DELETE (effektivSUPER) Berechtigungen für alle Tabellen in allen Datenbanken innerhalb des Katalogs.
- All(effektiv SUPER-) Berechtigungen für Kataloge innerhalb des Katalogs.
- Erteilbare Berechtigungen (die Möglichkeit, diese Berechtigungen anderen Hauptbenutzern zu gewähren) für alle Kataloge, Datenbanken und Tabellen innerhalb des Katalogs.

Mit der Super user Berechtigung für eine Katalogressource darf der Empfänger keine Aktionen im Katalog ausführen oder ALTER delegierenDROP.

ASSOCIATE

Berechtigung	Für diese Ressource gewährt	Der Stipendiat braucht auch
ASSOCIATE	LF-Tag	glue:GetDatabase glue:GetTable

Berechtigung	Für diese Ressource gewährt	Der Stipendiat braucht auch
		lakeformation:AddLFTagsToResource"
		lakeformation:RemoveLFTagsFromResource"
		lakeformation:GetResourceLFTags
		lakeformation:ListLFTags
		lakeformation:GetLFTag
		lakeformation:SearchTablesByLFTags
		lakeformation:SearchDatabasesByLFTags

Ein Principal mit dieser Berechtigung für ein LF-Tag kann das LF-Tag einer Datenkatalogressource zuweisen. Implizite Gewährung von Zuschüssen. ASSOCIATE DESCRIBE

Example

In diesem Beispiel wird dem Benutzer `datalake_user1` die ASSOCIATE Erlaubnis für das LF-Tag mit dem Schlüssel erteilt. `module` Es gewährt Berechtigungen zum Anzeigen und Zuweisen aller Werte für diesen Schlüssel, wie durch das Sternchen (*) gekennzeichnet.

```
aws lakeformation grant-permissions --principal
  DataLakePrincipalIdentifier=arn:aws:iam::111122223333:user/
  datalake_user1 --permissions "ASSOCIATE" --resource '{ "LFTag":
    {"CatalogId":"111122223333","TagKey":"module","TagValues":["*"]}}'
```

Integration von IAM Identity Center

Mit AWS IAM Identity Center können Sie eine Verbindung zu Identitätsanbietern (IdPs) herstellen und den Zugriff für Benutzer und Gruppen über AWS Analysedienste hinweg zentral verwalten. Sie können Identitätsanbieter wie Okta, Ping und Microsoft Entra ID (früher Azure Active Directory) in IAM Identity Center integrieren, damit Benutzer in Ihrer Organisation über eine Single-Sign-On-Erfahrung auf Daten zugreifen können. IAM Identity Center unterstützt auch die Verbindung weiterer externer Identitätsanbieter.

Weitere Informationen finden Sie unter [Unterstützte Identitätsanbieter](#) im AWS IAM Identity Center Benutzerhandbuch.

Sie können die Anwendung in IAM Identity Center AWS Lake Formation als aktivierte Anwendung konfigurieren, und Data Lake-Administratoren können autorisierten Benutzern und Gruppen detaillierte Berechtigungen für Ressourcen gewähren. AWS Glue Data Catalog

Benutzer aus Ihrer Organisation können sich mit dem Identitätsanbieter Ihrer Organisation bei jeder Identity Center-fähigen Anwendung anmelden und Datensätze mit Lake Formation Formations-Berechtigungen abfragen. Mit dieser Integration können Sie den Zugriff auf AWS Dienste verwalten, ohne mehrere IAM-Rollen erstellen zu müssen.

[Die Weitergabe vertrauenswürdiger Identitäten](#) ist eine AWS IAM Identity Center Funktion, mit der Administratoren von Connected den Zugriff auf Servicedaten gewähren und prüfen AWS-Services können. Der Zugriff auf diese Daten basiert auf Benutzerattributen wie Gruppenzuordnungen. Die Einrichtung der Verbreitung vertrauenswürdiger Identitäten erfordert die Zusammenarbeit zwischen den Administratoren von Connected AWS-Services und den IAM Identity Center-Administratoren. Weitere Informationen finden Sie unter [Voraussetzungen und Überlegungen](#).

Einschränkungen finden Sie unter [Einschränkungen bei der IAM Identity Center-Integration](#).

Themen

- [Voraussetzungen für die Integration von IAM Identity Center mit Lake Formation](#)
- [Lake Formation mit dem IAM Identity Center verbinden](#)
- [Aktualisierung der IAM Identity Center-Integration](#)
- [Löschen einer Lake Formation Formations-Verbindung mit IAM Identity Center](#)
- [Benutzern und Gruppen Berechtigungen gewähren](#)
- [Einbeziehen des IAM Identity Center-Benutzerkontextes in die Protokolle CloudTrail](#)

Voraussetzungen für die Integration von IAM Identity Center mit Lake Formation

Im Folgenden sind die Voraussetzungen für die Integration von IAM Identity Center in Lake Formation aufgeführt.

1. IAM Identity Center aktivieren — Die Aktivierung von IAM Identity Center ist eine Voraussetzung für die Unterstützung von Authentifizierung und Identitätsweitergabe.
2. Wählen Sie Ihre Identitätsquelle — Nachdem Sie IAM Identity Center aktiviert haben, benötigen Sie einen Identitätsanbieter für die Verwaltung von Benutzern und Gruppen. Sie können entweder das integrierte Identity Center-Verzeichnis als Identitätsquelle verwenden oder einen externen IdP wie Microsoft Entra ID oder Okta verwenden.

Weitere Informationen finden Sie unter [Ihre Identitätsquelle verwalten](#) und [Connect zu einem externen Identitätsanbieter](#) herstellen im AWS IAM Identity Center Benutzerhandbuch.

3. Eine IAM-Rolle erstellen — Für die Rolle, die eine IAM Identity Center-Verbindung herstellt, sind Berechtigungen zum Erstellen und Ändern der Anwendungskonfiguration in Lake Formation und IAM Identity Center erforderlich, wie in der folgenden Inline-Richtlinie beschrieben.

Sie müssen Berechtigungen gemäß den Best Practices für IAM hinzufügen. Die spezifischen Berechtigungen werden in den folgenden Verfahren beschrieben. Weitere Informationen finden Sie unter [Erste Schritte mit IAM Identity Center](#).

JSON

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Action": [
        "lakeformation:CreateLakeFormationIdentityCenterConfiguration",
        "sso:CreateApplication",
        "sso:PutApplicationAssignmentConfiguration",
        "sso:PutApplicationAuthenticationMethod",
        "sso:PutApplicationGrant",
        "sso:PutApplicationAccessScope"
      ],
      "Resource": [
        "*"
      ]
    }
  ]
}
```

```

    ]
  }
}

```

Wenn Sie Datenkatalogressourcen für externe Benutzer AWS-Konten oder Organisationen gemeinsam nutzen, benötigen Sie die AWS Resource Access Manager (AWS RAM) - Berechtigungen zum Erstellen von gemeinsamen Ressourcen. Weitere Informationen zu den für die gemeinsame Nutzung von Ressourcen erforderlichen Berechtigungen finden Sie unter [Voraussetzungen für die kontoübergreifende gemeinsame Nutzung von Daten](#).

Die folgenden Inline-Richtlinien enthalten spezifische Berechtigungen, die zum Anzeigen, Aktualisieren und Löschen von Eigenschaften der Lake Formation Formation-Integration mit IAM Identity Center erforderlich sind.

- Verwenden Sie die folgende Inline-Richtlinie, damit eine IAM-Rolle eine Lake Formation Formation-Integration mit IAM Identity Center anzeigen kann.

JSON

```

{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Action": [
        "lakeformation:DescribeLakeFormationIdentityCenterConfiguration",
        "sso:DescribeApplication"
      ],
      "Resource": [
        "*"
      ]
    }
  ]
}

```

- Verwenden Sie die folgende Inline-Richtlinie, damit eine IAM-Rolle eine Lake Formation Formation-Integration mit IAM Identity Center aktualisieren kann. Die Richtlinie umfasst auch optionale Berechtigungen, die für die gemeinsame Nutzung von Ressourcen mit externen Konten erforderlich sind.

JSON

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Action": [
        "lakeformation:UpdateLakeFormationIdentityCenterConfiguration",
        "lakeformation:DescribeLakeFormationIdentityCenterConfiguration",
        "sso:DescribeApplication",
        "sso:UpdateApplication"
      ],
      "Resource": [
        "*"
      ]
    }
  ]
}
```

- Verwenden Sie die folgende Inline-Richtlinie, um einer IAM-Rolle das Löschen einer Lake Formation Formation-Integration mit IAM Identity Center zu ermöglichen.

JSON

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Action": [
        "lakeformation:DeleteLakeFormationIdentityCenterConfiguration",
        "sso:DeleteApplication"
      ],
      "Resource": [
        "*"
      ]
    }
  ]
}
```

- Informationen zu IAM-Berechtigungen, die erforderlich sind, um Data Lake-Berechtigungen für IAM Identity Center-Benutzer und -Gruppen zu gewähren oder zu widerrufen, finden Sie unter. [IAM-Berechtigungen sind erforderlich, um Lake Formation-Berechtigungen zu gewähren oder zu widerrufen](#)

Beschreibung der Berechtigungen

- `lakeformation:CreateLakeFormationIdentityCenterConfiguration`— Erzeugt die Lake Formation iDC-Konfiguration.
- `lakeformation:DescribeLakeFormationIdentityCenterConfiguration`— Beschreibt eine bestehende iDC-Konfiguration.
- `lakeformation>DeleteLakeFormationIdentityCenterConfiguration`— Ermöglicht das Löschen einer vorhandenen Lake Formation iDC-Konfiguration.
- `lakeformation:UpdateLakeFormationIdentityCenterConfiguration`— Wird verwendet, um eine bestehende Lake Formation iDC-Konfiguration zu ändern.
- `sso:CreateApplication` – Zur Erstellung einer IAM-Identity-Center-Anwendung verwendet.
- `sso>DeleteApplication` – Zum Löschen einer IAM-Identity-Center-Anwendung verwendet.
- `sso:UpdateApplication` – Zur Aktualisierung einer IAM-Identity-Center-Anwendung verwendet.
- `sso:PutApplicationGrant` – Zur Änderung der Informationen zu vertrauenswürdigen Token-Ausstellern verwendet.
- `sso:PutApplicationAuthenticationMethod`— Gewährt Lake Formation iDC-Authentifizierungszugriff.
- `sso:GetApplicationGrant` – Zum Auflisten der Informationen zu vertrauenswürdigen Token-Ausstellern verwendet.
- `sso>DeleteApplicationGrant` – Löscht die Informationen zum vertrauenswürdigen Token-Aussteller.
- `sso:PutApplicationAccessScope`— Fügt die Liste der autorisierten Ziele für einen IAM Identity Center-Zugriffsbereich für eine Anwendung hinzu oder aktualisiert sie.
- `sso:PutApplicationAssignmentConfiguration`— Wird verwendet, um zu konfigurieren, wie Benutzer Zugriff auf eine Anwendung erhalten.

Lake Formation mit dem IAM Identity Center verbinden

Bevor Sie IAM Identity Center zur Verwaltung von Identitäten verwenden können, um mithilfe von Lake Formation Zugriff auf Datenkatalogressourcen zu gewähren, müssen Sie die folgenden Schritte ausführen. Sie können die IAM Identity Center-Integration mithilfe der Lake Formation Formation-Konsole oder AWS CLI erstellen.

AWS-Managementkonsole

Um Lake Formation mit IAM Identity Center zu verbinden

1. Melden Sie sich bei an AWS-Managementkonsole und öffnen Sie die Lake Formation Formation-Konsole unter <https://console.aws.amazon.com/lakeformation/>.
2. Wählen Sie im linken Navigationsbereich die Option IAM Identity Center-Integration aus.

Create IAM Identity Center Integration

Enable IAM Identity Center and then create Lake Formation - IAM Identity Center integration to manage identities from IAM Identity Center (external IdPs like Azure AD or Okta Universal Directory). [Learn more](#)

▼ How it works

Enable IAM Identity Center

Enable IAM Identity Center for your account or organization and select an identity provider.

Create Lake Formation integration

Integrate Lake Formation with IAM Identity Center to permit Lake Formation to access users from your selected identity provider.

Grant permissions

Grant permissions to users on Data Catalog databases and tables using fine-grained Lake Formation permissions.

Connect Lake Formation to IAM Identity Center



Connect to organization instance of IAM Identity Center

Manage access to Lake Formation by assigning users and groups from the Identity Center directory for your organization. [Learn more](#)

Recommended



Connect to account instance of IAM Identity Center

Manage access to Lake Formation by assigning existing or creating dedicated users and groups from your Identity Center directory. [Learn more](#)

instance of IAM Identity Center
Manage access to Lake Formation by assigning users and groups from your Identity Center directory.
 `arn:aws:sso::instance/ssoinstances-6987513bf5410c2f`

Add AWS account and organization IDs

Add AWS accounts and organizations whose users need access to Lake Formation managed resources.

AWS Accounts and AWS organizations

Enter one or more AWS account IDs and AWS organization IDs. Press Enter after each ID.

 Choose AWS account, AWS organization ID

► Lake Formation application integration - optional

Lake Formation mit dem IAM Identity Center verbinden, um Datenorte, die mit Lake Formation registriert sind, auf behalf of the user.

 After this step, you can't edit the connection. You can edit AWS accounts, organizations, and applications. If you want to modify the connection, delete it and create a new connection.

3. (Optional) Geben Sie eine oder mehrere gültige AWS-Konto IDs Organisationen oder and/or Organisationseinheiten ein IDs, IDs um externen Konten den Zugriff auf die Datenkatalogressourcen zu ermöglichen. Wenn Benutzer oder Gruppen von IAM Identity Center versuchen, auf von Lake Formation verwaltete Datenkatalogressourcen zuzugreifen, nimmt Lake Formation eine IAM-Rolle an, um den Metadatenzugriff zu autorisieren. Wenn die IAM-Rolle zu einem externen Konto gehört, das keine AWS Glue Ressourcenrichtlinie und keine AWS RAM Ressourcenfreigabe hat, können die Benutzer und Gruppen von IAM Identity Center nicht auf die Ressource zugreifen, selbst wenn sie über Lake Formation Formation-Berechtigungen verfügen.

Lake Formation verwendet den Dienst AWS Resource Access Manager (AWS RAM), um die Ressource mit externen Konten und Organisationen zu teilen. AWS RAM sendet eine Einladung an das Konto des Empfängers, die gemeinsame Nutzung der Ressource anzunehmen oder abzulehnen.

Weitere Informationen finden Sie unter [Annahme einer Einladung zur gemeinsamen Nutzung von Ressourcen AWS RAM](#).

 Note

Lake Formation ermöglicht es IAM-Rollen von externen Konten, im Namen von IAM Identity Center-Benutzern und -Gruppen als Trägerrollen für den Zugriff auf Datenkatalogressourcen zu fungieren. Berechtigungen können jedoch nur für Datenkatalogressourcen innerhalb des Eigentümerkontos erteilt werden. Wenn Sie versuchen, Benutzern und Gruppen von IAM Identity Center Berechtigungen für Datenkatalogressourcen in einem externen Konto zu gewähren, gibt Lake Formation die folgende Fehlermeldung aus: „Kontoübergreifende Zuweisungen werden für den Prinzipal nicht unterstützt“.

4. (Optional) Geben Sie auf dem Integrationsbildschirm Create Lake Formation die Anwendungen ARNs von Drittanbietern an, die auf Daten an Amazon S3 S3-Standorten zugreifen können, die bei Lake Formation registriert sind. Lake Formation verkauft begrenzte temporäre Anmeldeinformationen in Form von AWS STS Token an registrierte Amazon S3 S3-Standorte auf der Grundlage der effektiven Berechtigungen, sodass autorisierte Anwendungen im Namen von Benutzern auf Daten zugreifen können.
5. Wählen Sie Absenden aus.

Nachdem der Lake Formation-Administrator die Schritte abgeschlossen und die Integration erstellt hat, werden die IAM Identity Center-Eigenschaften in der Lake Formation Konsole angezeigt. Durch das Erledigen dieser Aufgaben wird Lake Formation zu einer IAM Identity Center-fähigen Anwendung. Die Eigenschaften in der Konsole umfassen auch den Integrationsstatus. Der Integrationsstatus gibt an, Success wann der Vorgang abgeschlossen ist. Dieser Status gibt an, ob die IAM Identity Center-Konfiguration abgeschlossen ist.

AWS CLI

- Das folgende Beispiel zeigt, wie die Lake Formation Integration mit IAM Identity Center erstellt wird. Sie können auch die Status (ENABLED,DISABLED) der Anwendungen angeben.

```
aws lakeformation create-lake-formation-identity-center-configuration \
  --catalog-id <123456789012> \
  --instance-arn <arn:aws:sso:::instance/ssoins-112111f12ca1122p> \
  --share-recipients '[{"DataLakePrincipalIdentifier": "<123456789012>"},
                      {"DataLakePrincipalIdentifier": "<555555555555>"}]' \
  --external-filtering '{"AuthorizedTargets": [<app arn1>, "<app arn2>"],
                      "Status": "ENABLED"}'
```

- Das folgende Beispiel zeigt, wie eine Lake Formation Integration mit IAM Identity Center angezeigt wird.

```
aws lakeformation describe-lake-formation-identity-center-configuration
  --catalog-id <123456789012>
```

Aktualisierung der IAM Identity Center-Integration

Nachdem Sie die Verbindung hergestellt haben, können Sie Drittanbieteranwendungen für die IAM Identity Center-Integration hinzufügen, um sie in Lake Formation zu integrieren und im Namen der Benutzer Zugriff auf Amazon S3 S3-Daten zu erhalten. Sie können auch vorhandene Anwendungen aus der IAM Identity Center-Integration entfernen. Sie

können Anwendungen mithilfe der Lake Formation Formation-Konsole und mithilfe von [UpdateLakeFormationIdentityCenterConfiguration](#) Operation hinzufügen oder entfernen. AWS CLI

Note

Nachdem Sie die IAM Identity Center-Integration erstellt haben, können Sie die Instanz ARN nicht aktualisieren.

AWS-Managementkonsole

So aktualisieren Sie eine bestehende IAM Identity Center-Verbindung mit Lake Formation

1. Melden Sie sich bei an AWS-Managementkonsole und öffnen Sie die Lake Formation Formation-Konsole unter <https://console.aws.amazon.com/lakeformation/>.
2. Wählen Sie im linken Navigationsbereich die Option IAM Identity Center-Integration aus.
3. Wählen Sie auf der IAM Identity Center-Integrationsseite Hinzufügen aus.
4. Geben Sie eine oder mehrere gültige AWS-Konto IDs Organisationen oder and/or Organisationseinheiten ein IDs, IDs um externen Konten den Zugriff auf die Datenkatalogressourcen zu ermöglichen.
5. Geben Sie auf dem Bildschirm Anwendungen hinzufügen die Anwendung IDs der Drittanbieteranwendungen ein, die Sie in Lake Formation integrieren möchten.
6. Wählen Sie Hinzufügen aus.

AWS CLI

Sie können Drittanbieteranwendungen für die IAM Identity Center-Integration hinzufügen oder entfernen, indem Sie den folgenden AWS CLI Befehl ausführen. Wenn Sie den externen Filterstatus auf festlegenENABLED, ermöglicht dies dem IAM Identity Center, Identitätsmanagement für Drittanbieteranwendungen bereitzustellen, um auf von Lake Formation verwaltete Daten zuzugreifen. Sie können die IAM Identity Center-Integration auch aktivieren oder deaktivieren, indem Sie den Anwendungsstatus festlegen.

```
aws lakeformation update-lake-formation-identity-center-configuration \
  --external-filtering '{"AuthorizedTargets": [<app arn1>, "<app arn2>"], "Status":
  "ENABLED"}' \
  --share-recipients '[{"DataLakePrincipalIdentifier": "<444455556666>"}
  {"DataLakePrincipalIdentifier": "<777788889999>"}]' \
```

```
--application-status ENABLED
```

Löschen einer Lake Formation Formation-Verbindung mit IAM Identity Center

Wenn Sie eine bestehende IAM Identity Center-Integration löschen möchten, können Sie dies mithilfe der Lake Formation Formation-Konsole oder [DeleteLakeFormationIdentityCenterConfiguration](#)-Operation tun. AWS CLI

AWS-Managementkonsole

So löschen Sie eine bestehende IAM Identity Center-Verbindung mit Lake Formation

1. Melden Sie sich bei an AWS-Managementkonsole und öffnen Sie die Lake Formation Formation-Konsole unter <https://console.aws.amazon.com/lakeformation/>.
2. Wählen Sie im linken Navigationsbereich die Option IAM Identity Center-Integration aus.
3. Wählen Sie auf der IAM Identity Center-Integrationsseite Löschen aus.
4. Bestätigen Sie auf dem Bildschirm „Integration bestätigen“ die Aktion und wählen Sie Löschen aus.

AWS CLI

Sie können die IAM Identity Center-Integration löschen, indem Sie den folgenden AWS CLI Befehl ausführen.

```
aws lakeformation delete-lake-formation-identity-center-configuration \  
  --catalog-id <123456789012>
```

Benutzern und Gruppen Berechtigungen gewähren

Ihr Data Lake-Administrator kann Benutzern und Gruppen von IAM Identity Center Berechtigungen für Datenkatalogressourcen (Datenbanken, Tabellen und Ansichten) gewähren, um einen einfachen Datenzugriff zu ermöglichen. Um Data Lake-Berechtigungen zu gewähren oder zu widerrufen, benötigt der Erteilende Berechtigungen für die folgenden IAM Identity Center-Aktionen.

- [DescribeUser](#)

- [DescribeGroup](#)
- [DescribeInstance](#)

Sie können Berechtigungen gewähren, indem Sie die Lake Formation Formation-Konsole, die API oder die verwenden AWS CLI.

Weitere Informationen zur Erteilung von Berechtigungen finden Sie unter [the section called “Erteilen von Datenberechtigungen”](#).

 Note

Sie können nur Berechtigungen für Ressourcen in Ihrem Konto gewähren. Um Benutzern und Gruppen Berechtigungen für Ressourcen, die mit Ihnen gemeinsam genutzt werden, zu kaskadieren, müssen Sie AWS RAM Resource Shares verwenden.

AWS-Managementkonsole

Um Benutzern und Gruppen Berechtigungen zu gewähren

1. Melden Sie sich bei an AWS-Managementkonsole und öffnen Sie die Lake Formation Formation-Konsole unter <https://console.aws.amazon.com/lakeformation/>.
2. Wählen Sie in der Lake Formation-Konsole unter Berechtigungen die Option Data Lake-Berechtigungen aus.
3. Wählen Sie Grant aus.
4. Wählen Sie auf der Seite Data Lake-Berechtigungen gewähren die Option IAM Identity Center-Benutzer und -Gruppen aus.
5. Wählen Sie Hinzufügen aus, um die Benutzer und Gruppen auszuwählen, denen Berechtigungen erteilt werden sollen.

Grant permissions

Principals

Choose the principals to grant permissions.

☒ **IAM users and roles**
Users or roles from this AWS account.

☐ **IAM Identity Center**
- *new*
Users and groups configured in IAM Identity Center.

☐ **SAML users and groups**
SAML users and group or QuickSight ARNs.

☐ **External accounts**
AWS account, AWS organization or IAM principal outside of this account

IAM users and roles

Add one or more IAM users or roles.

Choose IAM principals to add ▼

AWSServiceRoleForRedshift X
Role

- Wählen Sie auf dem Bildschirm „Benutzer und Gruppen zuweisen“ die and/or Benutzergruppen aus, denen Berechtigungen erteilt werden sollen.

Wählen Sie Zuweisen aus.

Assign users and groups ✕

Users

user1 Remove

user2 Remove

Groups

DataStewards Remove

Manage groups [↗](#)

[Learn more about managing groups from IAM Identity Center](#) [↗](#)

Cancel Assign

- Wählen Sie als Nächstes die Methode zum Erteilen von Berechtigungen aus.

Anweisungen zum Erteilen von Berechtigungen mithilfe der Methode „Benannte Ressourcen“ finden Sie unter [Erteilen von Datenberechtigungen mithilfe der benannten Ressourcenmethode](#).

Anweisungen zur Erteilung von Berechtigungen mithilfe von LF-Tags finden Sie unter [Erteilen von Data Lake-Berechtigungen mithilfe der LF-TBAC-Methode](#)

- Wählen Sie die Datenkatalogressourcen aus, für die Sie Berechtigungen erteilen möchten.
- Wählen Sie die Datenkatalogberechtigungen aus, die Sie gewähren möchten.
- Wählen Sie Gewähren aus.

AWS CLI

Das folgende Beispiel zeigt, wie IAM Identity SELECT Center-Benutzerberechtigungen für eine Tabelle erteilt werden.

```
aws lakeformation grant-permissions \  
--principal DataLakePrincipalIdentifier=arn:aws:identitystore:::user/<UserId> \  
--permissions "SELECT" \  
--resource '{ "Table": { "DatabaseName": "retail", "TableWildcard": {} } }'
```

Informationen zum Abrufen `UserId` aus dem IAM Identity Center finden Sie unter [GetUserId](#) Vorgang in der IAM Identity Center API-Referenz.

Einbeziehen des IAM Identity Center-Benutzerkontextes in die Protokolle CloudTrail

Lake Formation verwendet die [Verkaufsfunktion für Anmeldeinformationen](#), um temporären Zugriff auf Amazon S3 S3-Daten zu ermöglichen. Wenn ein IAM Identity Center-Benutzer eine Anfrage an einen integrierten Analysedienst sendet, enthalten die CloudTrail Protokolle standardmäßig nur die IAM-Rolle, die der Service für den kurzfristigen Zugriff annimmt. Wenn Sie eine benutzerdefinierte Rolle verwenden, um den Amazon S3 S3-Datenstandort bei Lake Formation zu registrieren, können Sie sich dafür entscheiden, den Kontext des IAM Identity Center-Benutzers in die CloudTrail Ereignisse einzubeziehen und dann die Benutzer zu verfolgen, die auf Ihre Ressourcen zugreifen.

Important

Um Amazon S3 S3-API-Anfragen auf Objektebene in die aufzunehmen CloudTrail, müssen Sie die CloudTrail Ereignisprotokollierung für den Amazon S3 S3-Bucket und die Objekte aktivieren. Weitere Informationen finden Sie unter [Aktivieren der CloudTrail Ereignisprotokollierung für Amazon S3 S3-Buckets und -Objekte](#) im Amazon S3 S3-Benutzerhandbuch.

So aktivieren Sie die Prüfung von Anmeldedaten an Data Lake-Standorten, die mit benutzerdefinierten Rollen registriert sind

1. Melden Sie sich bei der Lake Formation Konsole unter an <https://console.aws.amazon.com/lakeformation/>.
2. Erweitern Sie in der linken Navigationsleiste die Option Administration und wählen Sie Datenkatalogeinstellungen aus.
3. Wählen Sie unter Erweitertes Auditing die Option Bereitgestellten Kontext weitergeben aus.
4. Wählen Sie Speichern.

Sie können die erweiterte Überwachungsoption auch aktivieren, indem Sie das Parameters Attribut im [PutDataLakeSettings](#) Vorgang festlegen. Standardmäßig ist der SET_CONTEXT Parameterwert auf „true“ gesetzt.

```
{
  "DataLakeSettings": {
    "Parameters": {"SET_CONTEXT": "true"},
  }
}
```

Im Folgenden finden Sie einen Auszug aus einem CloudTrail Ereignis mit der erweiterten Überwachungsoption. Dieses Protokoll enthält sowohl den Sitzungskontext des IAM Identity Center-Benutzers als auch die benutzerdefinierte IAM-Rolle, die Lake Formation für den Zugriff auf den Amazon S3 S3-Datenstandort übernommen hat. Sehen Sie sich den onBehalfOf Parameter im folgenden Auszug an.

```
{
  "eventVersion": "1.09",
  "userIdentity": {
    "type": "AssumedRole",
    "principalId": "AR0AW7F7M0X40YE6FLIFN:access-grants-e653760c-4e8b-44fd-94d9-309e035b75ab",
    "arn": "arn:aws:sts::123456789012:assumed-role/accessGrantsTestRole/access-grants-e653760c-4e8b-44fd-94d9-309e035b75ab",
    "accountId": "123456789012",
    "accessKeyId": "ASIAW7F7M0X4CQLD4JIZN",
    "sessionContext": {
      "sessionIssuer": {
        "type": "Role",
```

```

        "principalId": "AROAW7F7M0X40YE6FLIFN",
        "arn": "arn:aws:iam::123456789012:role/accessGrantsTestRole",
        "accountId": "123456789012",
        "userName": "accessGrantsTestRole"
    },
    "attributes": {
        "creationDate": "2023-08-09T17:24:02Z",
        "mfaAuthenticated": "false"
    }
},
"onBehalfOf": {
    "userId": "<identityStoreUserId>",
    "identityStoreArn": "arn:aws:identitystore::<restOfIdentityStoreArn>"
}
},
"eventTime": "2023-08-09T17:25:43Z",
"eventSource": "s3.amazonaws.com",
"eventName": "GetObject",
....

```

Hinzufügen eines Amazon S3 S3-Standorts zu Ihrem Data Lake

Um einen Datenstandort als Speicher in Ihrem Data Lake hinzuzufügen, registrieren Sie den Standort (Data Lake-Standort) bei AWS Lake Formation. Anschließend können Sie Lake Formation Formation-Berechtigungen für eine detaillierte Zugriffskontrolle auf AWS Glue Data Catalog Objekte verwenden, die auf diese Position und auf die zugrunde liegenden Daten in der Position verweisen.

Lake Formation ermöglicht auch die Registrierung eines Datenstandorts im Hybridzugriffsmodus und bietet Ihnen die Flexibilität, Lake Formation Formation-Berechtigungen für Datenbanken und Tabellen in Ihrem Datenkatalog selektiv zu aktivieren. Im Hybridzugriffsmodus verfügen Sie über einen inkrementellen Pfad, mit dem Sie Lake Formation Formation-Berechtigungen für eine bestimmte Gruppe von Benutzern festlegen können, ohne die Berechtigungsrichtlinien anderer vorhandener Benutzer oder Workloads zu unterbrechen.

Weitere Informationen zur Einrichtung des hybriden Zugriffsmodus finden Sie unter [Hybrider Zugriffsmodus](#)

Wenn Sie einen Standort registrieren, werden dieser Amazon S3 S3-Pfad und alle Ordner unter diesem Pfad registriert.

Nehmen wir zum Beispiel an, Sie haben eine Amazon S3 S3-Pfadorganisation wie die folgende:

/mybucket/accounting/sales/

Wenn Sie sich registrieren S3://mybucket/accounting, ist der sales Ordner ebenfalls registriert und wird von Lake Formation verwaltet.

Weitere Informationen zur Registrierung von Standorten finden Sie unter [Underlying data access control](#).

Note

Lake Formation Formations-Berechtigungen werden für strukturierte Daten (angeordnet in Tabellen mit Zeilen und Spalten) empfohlen. Wenn Ihre Daten objektbasierte unstrukturierte Daten enthalten, sollten Sie erwägen, Amazon S3-Zugriffsberechtigungen zur Verwaltung des Datenzugriffs zu verwenden.

Themen

- [Anforderungen für Rollen, die zur Registrierung von Standorten verwendet werden](#)
- [Registrierung eines Amazon S3 S3-Standorts](#)
- [Registrierung eines verschlüsselten Amazon S3 S3-Standorts](#)
- [Registrierung eines Amazon S3 S3-Standorts in einem anderen AWS Konto](#)
- [AWS Kontoübergreifende Registrierung eines verschlüsselten Amazon S3 S3-Standorts](#)
- [Abmeldung eines Amazon S3 S3-Standorts](#)

Anforderungen für Rollen, die zur Registrierung von Standorten verwendet werden

Sie müssen eine AWS Identity and Access Management (IAM) -Rolle angeben, wenn Sie einen Amazon Simple Storage Service (Amazon S3) -Standort registrieren. AWS Lake Formation nimmt diese Rolle beim Zugriff auf die Daten an diesem Standort an.

Sie können einen der folgenden Rollentypen verwenden, um einen Standort zu registrieren:

- Die dienstleistungsbezogene Rolle von Lake Formation. Diese Rolle gewährt die erforderlichen Berechtigungen für den Standort. Die Verwendung dieser Rolle ist die einfachste Methode,

den Standort zu registrieren. Weitere Informationen erhalten Sie unter [Verwenden von serviceverknüpften Rollen für Lake Formation](#) und [Einschränkungen für dienstbezogene Rollen](#).

- Eine benutzerdefinierte Rolle. Verwenden Sie eine benutzerdefinierte Rolle, wenn Sie mehr Berechtigungen gewähren müssen, als die dienstverknüpfte Rolle bietet.

In den folgenden Fällen müssen Sie eine benutzerdefinierte Rolle verwenden:

- Bei der Registrierung eines Standorts in einem anderen Konto.

Weitere Informationen erhalten Sie unter [the section called “Registrierung eines Amazon S3 S3-Standorts in einem anderen AWS Konto”](#) und [the section called “AWS Kontoübergreifende Registrierung eines verschlüsselten Amazon S3 S3-Standorts”](#).

- Wenn Sie ein AWS verwaltetes CMK (aws/s3) verwendet haben, um den Amazon S3 S3-Standort zu verschlüsseln.

Weitere Informationen finden Sie unter [Registrierung eines verschlüsselten Amazon S3 S3-Standorts](#).

- Wenn Sie mit Amazon EMR auf den Standort zugreifen möchten.

Wenn Sie bereits einen Standort mit der serviceverknüpften Rolle registriert haben und mit Amazon EMR auf den Standort zugreifen möchten, müssen Sie den Standort abmelden und ihn mit einer benutzerdefinierten Rolle erneut registrieren. Weitere Informationen finden Sie unter [the section called “Abmeldung eines Amazon S3 S3-Standorts”](#).

Verwenden von serviceverknüpften Rollen für Lake Formation

AWS Lake Formation verwendet eine dienstbezogene AWS Identity and Access Management (IAM-) Rolle. Eine serviceverknüpfte Rolle ist eine einzigartige Art von IAM-Rolle, die direkt mit Lake Formation verknüpft ist. Die dienstverknüpfte Rolle ist von Lake Formation vordefiniert und umfasst alle Berechtigungen, die der Dienst benötigt, um andere AWS Dienste in Ihrem Namen aufzurufen.

Eine serviceverknüpfte Rolle erleichtert die Einrichtung von Lake Formation, da Sie keine Rolle erstellen und die erforderlichen Berechtigungen manuell hinzufügen müssen. Lake Formation definiert die Berechtigungen seiner dienstbezogenen Rolle, und sofern nicht anders definiert, kann nur Lake Formation seine Rollen übernehmen. Die definierten Berechtigungen umfassen die Vertrauens- und Berechtigungsrichtlinie. Diese Berechtigungsrichtlinie kann keinen anderen IAM-Entitäten zugewiesen werden.

Diese dienstbezogene Rolle vertraut darauf, dass die folgenden Dienste die Rolle übernehmen:

- `lakeformation.amazonaws.com`

Wenn Sie eine serviceverknüpfte Rolle in Konto A verwenden, um einen Amazon S3 S3-Standort zu registrieren, der Konto B gehört, muss die Amazon S3 S3-Bucket-Richtlinie (eine ressourcenbasierte Richtlinie) in Konto B Zugriffsberechtigungen für die serviceverknüpfte Rolle in Konto A gewähren.

Informationen zur Verwendung einer serviceverknüpften Rolle zur Registrierung eines Datenstandorts finden Sie unter: [Einschränkungen für dienstbezogene Rollen](#)

Note

Richtlinien zur Dienststeuerung (SCPs) wirken sich nicht auf dienstverknüpfte Rollen aus. Weitere Informationen finden Sie im AWS Organizations Benutzerhandbuch unter [Richtlinien zur Servicesteuerung \(SCPs\)](#).

Dienstbezogene Rollenberechtigungen für Lake Formation

Lake Formation verwendet die angegebene dienstbezogene Rolle.

`AWSServiceRoleForLakeFormationDataAccess` Diese Rolle bietet eine Reihe von Amazon Simple Storage Service (Amazon S3) -Berechtigungen, die es dem integrierten Service von Lake Formation (z. B. Amazon Athena) ermöglichen, auf registrierte Standorte zuzugreifen. Wenn Sie einen Data Lake-Standort registrieren, müssen Sie eine Rolle angeben, die über die erforderlichen Amazon S3 read/write S3-Berechtigungen für diesen Standort verfügt. Anstatt eine Rolle mit den erforderlichen Amazon S3 S3-Berechtigungen zu erstellen, können Sie diese serviceverknüpfte Rolle verwenden.

Wenn Sie die serviceverknüpfte Rolle zum ersten Mal als Rolle angeben, mit der ein Pfad registriert werden soll, werden die serviceverknüpfte Rolle und eine neue IAM-Richtlinie in Ihrem Namen erstellt. Lake Formation fügt den Pfad zur Inline-Richtlinie hinzu und fügt ihn der dienstbezogenen Rolle hinzu. Wenn Sie nachfolgende Pfade mit der serviceverknüpften Rolle registrieren, fügt Lake Formation den Pfad der vorhandenen Richtlinie hinzu.

Registrieren Sie einen Data Lake-Standort, während Sie als Data Lake-Administrator angemeldet sind. Suchen Sie dann in der IAM-Konsole nach der Rolle `AWSServiceRoleForLakeFormationDataAccess` und sehen Sie sich die zugehörigen Richtlinien an.

Nachdem Sie den Standort registriert haben `s3://my-kinesis-test/logs`, erstellt Lake Formation beispielsweise die folgende Inline-Richtlinie und hängt sie an `AWSServiceRoleForLakeFormationDataAccess`.

JSON

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Sid": "LakeFormationDataAccessPermissionsForS3",
      "Effect": "Allow",
      "Action": [
        "s3:PutObject",
        "s3:GetObject",
        "s3:DeleteObject",
        "s3:AbortMultipartUpload",
        "s3:ListMultipartUploadParts"
      ],
      "Resource": [
        "arn:aws:s3:::my-kinesis-test/logs/*"
      ]
    },
    {
      "Sid": "LakeFormationDataAccessPermissionsForS3ListBucket",
      "Effect": "Allow",
      "Action": [
        "s3:ListBucket",
        "s3:ListBucketMultipartUploads"
      ],
      "Resource": [
        "arn:aws:s3:::my-kinesis-test"
      ]
    }
  ]
}
```

Schaffung einer dienstbezogenen Rolle für Lake Formation

Sie müssen eine serviceverknüpfte Rolle nicht manuell erstellen. Wenn Sie einen Amazon S3 S3-Standort bei Lake Formation in der AWS-Managementkonsole, der AWS CLI oder der AWS API registrieren, erstellt Lake Formation die serviceverknüpfte Rolle für Sie.

Important

Diese serviceverknüpfte Rolle kann in Ihrem Konto erscheinen, wenn Sie eine Aktion in einem anderen Service abgeschlossen haben, der die von dieser Rolle unterstützten Features verwendet. Weitere Informationen finden Sie unter [In meinem IAM-Konto wird eine neue Rolle angezeigt](#).

Wenn Sie diese serviceverknüpfte Rolle löschen und sie dann erneut erstellen müssen, können Sie dasselbe Verfahren anwenden, um die Rolle in Ihrem Konto neu anzulegen. Wenn Sie einen Amazon S3 S3-Standort bei Lake Formation registrieren, erstellt Lake Formation die serviceverknüpfte Rolle erneut für Sie.

Sie können die IAM-Konsole auch verwenden, um eine serviceverknüpfte Rolle mit dem Lake Formation Formation-Anwendungsfall zu erstellen. Erstellen Sie in der AWS CLI oder der AWS API eine dienstverknüpfte Rolle mit dem `lakeformation.amazonaws.com` Dienstenamen. Weitere Informationen finden Sie unter [Erstellen einer serviceverknüpften Rolle](#) im IAM-Benutzerhandbuch. Wenn Sie diese serviceverknüpfte Rolle löschen, können Sie mit demselben Verfahren die Rolle erneut erstellen.

Bearbeiten einer serviceverknüpften Rolle für Lake Formation

In Lake Formation können Sie die `AWSServiceRoleForLakeFormationDataAccess` serviceverknüpfte Rolle nicht bearbeiten. Da möglicherweise verschiedene Entitäten auf die Rolle verweisen, kann der Rollename nach dem Erstellen einer serviceverknüpften Rolle nicht mehr geändert werden. Sie können jedoch die Beschreibung der Rolle mit IAM bearbeiten. Weitere Informationen finden Sie unter [Bearbeiten einer serviceverknüpften Rolle](#) im IAM-Benutzerhandbuch.

Löschen einer serviceverknüpften Rolle für Lake Formation

Wenn Sie ein Feature oder einen Dienst, die bzw. der eine serviceverknüpften Rolle erfordert, nicht mehr benötigen, sollten Sie diese Rolle löschen. Auf diese Weise haben Sie keine ungenutzte juristische Stelle, die nicht aktiv überwacht oder verwaltet wird. Sie müssen jedoch die Ressourcen für Ihre serviceverknüpften Rolle zunächst bereinigen, bevor Sie sie manuell löschen können.

 Note

Wenn der Lake Formation Formation-Dienst die Rolle verwendet, wenn Sie versuchen, die Ressourcen zu löschen, schlägt das Löschen möglicherweise fehl. Wenn dies passiert, warten Sie einige Minuten und versuchen Sie es erneut.

Um Lake Formation-Ressourcen zu löschen, die von der Lake Formation verwendet werden

- Wenn Sie die serviceverknüpfte Rolle verwendet haben, um Amazon S3 S3-Standorte bei Lake Formation zu registrieren, müssen Sie vor dem Löschen der serviceverknüpften Rolle den Standort abmelden und ihn mit einer benutzerdefinierten Rolle erneut registrieren.

So löschen Sie die serviceverknüpfte Rolle mit IAM

Verwenden Sie die IAM-Konsole, die oder die API, um die serviceverknüpfte AWS CLI Rolle zu löschen. `AWS AWSServiceRoleForLakeFormationDataAccess` Weitere Informationen finden Sie unter [Löschen einer serviceverknüpften Rolle](#) im IAM-Leitfaden.

Im Folgenden sind die Anforderungen für eine benutzerdefinierte Rolle aufgeführt:

- Wählen Sie beim Erstellen der neuen Rolle auf der Seite Rolle erstellen der IAM-Konsole AWS Service und dann unter Anwendungsfall auswählen die Option Lake Formation aus.

Wenn Sie die Rolle unter Verwendung eines anderen Pfads erstellen, stellen Sie sicher, dass für die Rolle eine Vertrauensstellung besteht. `lakeformation.amazonaws.com` Weitere Informationen finden Sie unter [Ändern einer Vertrauensrichtlinie für Rollen \(Konsole\)](#).

- Die Rolle muss über eine Inline-Richtlinie verfügen, die Amazon S3 read/write S3-Berechtigungen für den Standort gewährt. Im Folgenden finden Sie eine typische Richtlinie.

JSON

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

```

        "s3:DeleteObject"
    ],
    "Resource": [
        "arn:aws:s3:::awsexamplebucket/*"
    ]
},
{
    "Effect": "Allow",
    "Action": [
        "s3:ListBucket"
    ],
    "Resource": [
        "arn:aws:s3:::awsexamplebucket"
    ]
}
]
}

```

- Fügen Sie der IAM-Rolle die folgende Vertrauensrichtlinie hinzu, damit der Lake Formation Formation-Dienst die Rolle übernehmen und temporäre Anmeldeinformationen an die integrierten Analyse-Engines weitergeben kann.

Um den IAM Identity Center-Benutzerkontext in die CloudTrail Protokolle aufzunehmen, muss die Vertrauensrichtlinie über die entsprechende Berechtigung für die Aktion verfügen.

`sts:SetContext`

JSON

```

{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Sid": "DataCatalogViewDefinerAssumeRole1",
      "Effect": "Allow",
      "Principal": {
        "Service": [
          "lakeformation.amazonaws.com"
        ]
      },
      "Action": [
        "sts:AssumeRole",
        "sts:SetContext"
      ]
    }
  ]
}

```

```
    }
  ]
}
```

- Der Data Lake-Administrator, der den Standort registriert, muss über die entsprechenden `iam:PassRole` Berechtigungen für die Rolle verfügen.

Im Folgenden finden Sie eine Inline-Richtlinie, die diese Berechtigung gewährt. `<account-id>` Ersetzen Sie es durch eine gültige AWS Kontonummer und `<role-name>` ersetzen Sie es durch den Namen der Rolle.

JSON

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Sid": "PassRolePermissions",
      "Effect": "Allow",
      "Action": [
        "iam:PassRole"
      ],
      "Resource": [
        "arn:aws:iam::111122223333:role/<role-name>"
      ]
    }
  ]
}
```

- Damit Lake Formation Logs zu Logs hinzufügen und Metriken veröffentlichen kann, fügen Sie die folgende Inline-Richtlinie hinzu. CloudWatch

Note

Das Schreiben in CloudWatch Logs ist kostenpflichtig.

JSON

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



```
"Statement": [
  {
    "Sid": "Sid1",
    "Effect": "Allow",
    "Action": [
      "logs:CreateLogStream",
      "logs:CreateLogGroup",
      "logs:PutLogEvents"
    ],
    "Resource": [
      "arn:aws:logs:us-east-1:111122223333:log-group:/aws-lakeformation-acceleration/*",
      "arn:aws:logs:us-east-1:111122223333:log-group:/aws-lakeformation-acceleration/*:log-stream:*"
    ]
  }
]
```

Registrierung eines Amazon S3 S3-Standorts

Sie müssen eine AWS Identity and Access Management (IAM) -Rolle angeben, wenn Sie einen Amazon Simple Storage Service (Amazon S3) -Standort registrieren. Lake Formation übernimmt diese Rolle, wenn es integrierten AWS Diensten, die auf die Daten an diesem Standort zugreifen, temporäre Anmeldeinformationen gewährt.

Important

Vermeiden Sie es, einen Amazon S3 S3-Bucket zu registrieren, für den Zahlungen durch den Antragsteller aktiviert ist. Bei Buckets, die bei Lake Formation registriert sind, wird die Rolle, mit der der Bucket registriert wurde, immer als der Anforderer angesehen. Wenn ein anderes AWS Konto auf den Bucket zugreift, wird dem Bucket-Besitzer der Datenzugriff in Rechnung gestellt, sofern die Rolle zu demselben Konto gehört wie der Bucket-Besitzer.

Sie können die AWS Lake Formation Konsole, die Lake Formation API oder AWS Command Line Interface (AWS CLI) verwenden, um einen Amazon S3 S3-Standort zu registrieren.

Bevor Sie beginnen

Überprüfen Sie die [Anforderungen für die Rolle, die zur Registrierung des Standorts verwendet wurde](#).

Um einen Standort zu registrieren (Konsole)

 Important

Bei den folgenden Verfahren wird davon ausgegangen, dass sich der Amazon S3 S3-Standort in demselben AWS Konto wie der Datenkatalog befindet und dass die Daten am Standort nicht verschlüsselt sind. Andere Abschnitte in diesem Kapitel behandeln die kontoübergreifende Registrierung und die Registrierung verschlüsselter Standorte.

1. Öffnen Sie die AWS Lake Formation Konsole unter <https://console.aws.amazon.com/lakeformation/>. Melden Sie sich als Data Lake-Administrator oder als Benutzer mit der `lakeformation:RegisterResource` IAM-Berechtigung an.
2. Wählen Sie im Navigationsbereich unter Verwaltung die Option Data Lake-Standorte aus.
3. Wählen Sie Speicherort registrieren und anschließend Durchsuchen, um einen Amazon Simple Storage Service (Amazon S3) -Pfad auszuwählen.
4. (Optional, aber dringend empfohlen) Wählen Sie Standortberechtigungen überprüfen aus, um eine Liste aller vorhandenen Ressourcen am ausgewählten Amazon S3 S3-Standort und deren Berechtigungen anzuzeigen.

Die Registrierung des ausgewählten Standorts kann dazu führen, dass Ihre Lake Formation Benutzer Zugriff auf Daten erhalten, die sich bereits an diesem Standort befinden. Durch das Anzeigen dieser Liste können Sie sicherstellen, dass die vorhandenen Daten sicher bleiben.

5. Wählen Sie für die IAM-Rolle entweder die `AWSServiceRoleForLakeFormationDataAccess` serviceverknüpfte Rolle (Standard) oder eine benutzerdefinierte IAM-Rolle, die die Anforderungen in erfüllt. [the section called "Anforderungen für Rollen, die zur Registrierung von Standorten verwendet werden"](#)

Sie können einen registrierten Standort oder andere Details nur aktualisieren, wenn Sie ihn mit einer benutzerdefinierten IAM-Rolle registrieren. Um einen Standort zu bearbeiten, der mit einer serviceverknüpften Rolle registriert wurde, sollten Sie den Standort abmelden und ihn erneut registrieren.

6. Wählen Sie die Option Datenkatalogverbund aktivieren, damit Lake Formation eine Rolle übernehmen und temporäre Anmeldeinformationen an integrierte AWS Dienste weitergeben kann, um auf Tabellen in Verbunddatenbanken zuzugreifen. Wenn ein Standort bei Lake Formation registriert ist und Sie denselben Speicherort für eine Tabelle in einer Verbunddatenbank verwenden möchten, müssen Sie denselben Standort mit der Option Datenkatalogverbund aktivieren registrieren.
7. Wählen Sie den Hybrid-Zugriffsmodus, um Lake Formation Formation-Berechtigungen standardmäßig nicht zu aktivieren. Wenn Sie den Amazon S3 S3-Standort im Hybridzugriffsmodus registrieren, können Sie Lake Formation Formation-Berechtigungen aktivieren, indem Sie Prinzipale für Datenbanken und Tabellen unter diesem Standort auswählen.

Weitere Informationen zur Einrichtung des hybriden Zugriffsmodus finden Sie unter. [Hybrider Zugriffsmodus](#)

8. Wählen Sie Standort registrieren aus.

Um einen Standort zu registrieren (AWS CLI)

1. Registrieren Sie einen neuen Standort bei Lake Formation

In diesem Beispiel wird eine dienstbezogene Rolle verwendet, um den Standort zu registrieren. Sie können das `--role-arn` Argument stattdessen verwenden, um Ihre eigene Rolle anzugeben.

<s3-path> Ersetzen Sie es durch einen gültigen Amazon S3 S3-Pfad, die Kontonummer durch ein gültiges AWS Konto und **<s3-access-role>** durch eine IAM-Rolle, die über Berechtigungen zur Registrierung eines Datenstandorts verfügt.

 Note

Sie können die Eigenschaften eines registrierten Standorts nicht bearbeiten, wenn er mit einer serviceverknüpften Rolle registriert ist.

```
aws lakeformation register-resource \  
  --resource-arn arn:aws:s3:::<s3-path> \  
  --use-service-linked-role
```

Im folgenden Beispiel wird eine benutzerdefinierte Rolle verwendet, um den Standort zu registrieren.

```
aws lakeformation register-resource \  
  --resource-arn arn:aws:s3:::<s3-path> \  
  --role-arn arn:aws:iam::<123456789012>:role/<s3-access-role>
```

2. Um einen bei Lake Formation registrierten Standort zu aktualisieren

Sie können einen registrierten Standort nur bearbeiten, wenn er mit einer benutzerdefinierten IAM-Rolle registriert ist. Bei einem Standort, der mit einer serviceverknüpften Rolle registriert ist, sollten Sie die Registrierung des Standorts aufheben und ihn erneut registrieren. Weitere Informationen finden Sie unter [the section called “Abmeldung eines Amazon S3 S3-Standorts”](#).

```
aws lakeformation update-resource \  
  --role-arn arn:aws:iam::<123456789012>:role/<s3-access-role>\  
  --resource-arn arn:aws:s3:::<s3-path>
```

```
aws lakeformation update-resource \  
  --resource-arn arn:aws:s3:::<s3-path> \  
  --use-service-linked-role
```

3. Registrieren Sie einen Datenstandort im Hybridzugriffsmodus mit Verbund

```
aws lakeformation register-resource \  
  --resource-arn arn:aws:s3:::<s3-path> \  
  --role-arn arn:aws:iam::<123456789012>:role/<s3-access-role> \  
  --hybrid-access-enabled
```

```
aws lakeformation register-resource \  
  --resource-arn arn:aws:s3:::<s3-path> \  
  --role-arn arn:aws:iam::<123456789012>:role/<s3-access-role> \  
  --with-federation
```

```
aws lakeformation update-resource \  
  --resource-arn arn:aws:s3:::<s3-path> \  
  --role-arn arn:aws:iam::<123456789012>:role/<s3-access-role> \  
  --with-federation
```

```
--hybrid-access-enabled
```

Weitere Informationen finden Sie unter [RegisterResource](#)API-Betrieb.

Note

Sobald Sie einen Amazon S3 S3-Standort registriert haben, gibt jede AWS Glue Tabelle, die auf den Standort (oder einen seiner untergeordneten Standorte) verweist, den Wert für den `IsRegisteredWithLakeFormation` Parameter wie `true` im `GetTable` Aufruf zurück. Es gibt eine bekannte Einschränkung, dass Datenkatalog-API-Operationen, wie z. B. `GetTables` und `SearchTables` nicht, den Wert für den `IsRegisteredWithLakeFormation` Parameter aktualisieren und den Standardwert zurückgeben, der falsch ist. Es wird empfohlen, die `GetTable` API zu verwenden, um den richtigen Wert für den `IsRegisteredWithLakeFormation` Parameter anzuzeigen.

Registrierung eines verschlüsselten Amazon S3 S3-Standorts

Lake Formation ist in [AWS Key Management Service](#)(AWS KMS) integriert, sodass Sie andere integrierte Dienste zum Verschlüsseln und Entschlüsseln von Daten an Amazon Simple Storage Service (Amazon S3) -Standorten einfacher einrichten können.

Beide werden vom Kunden verwaltet AWS KMS keys und Von AWS verwaltete Schlüssel werden unterstützt. Derzeit encryption/decryption wird die Client-Seite nur mit Athena unterstützt.

Sie müssen eine AWS Identity and Access Management (IAM-) Rolle angeben, wenn Sie einen Amazon S3 S3-Standort registrieren. Für verschlüsselte Amazon S3 S3-Standorte muss entweder die Rolle über die Berechtigung zum Verschlüsseln und Entschlüsseln von Daten mit dem verfügen AWS KMS key, oder die KMS-Schlüsselrichtlinie muss Berechtigungen für den Schlüssel der Rolle gewähren.

Important

Vermeiden Sie es, einen Amazon S3 S3-Bucket zu registrieren, für den Zahlungen durch den Antragsteller aktiviert ist. Bei Buckets, die bei Lake Formation registriert sind, wird die Rolle, mit der der Bucket registriert wurde, immer als der Anforderer angesehen. Wenn ein anderes

AWS Konto auf den Bucket zugreift, wird dem Bucket-Besitzer der Datenzugriff in Rechnung gestellt, sofern die Rolle zu demselben Konto gehört wie der Bucket-Besitzer.

Lake Formation verwendet eine serviceverknüpfte Rolle, um Ihre Datenstandorte zu registrieren. Diese Rolle hat jedoch mehrere [Einschränkungen](#). Aufgrund dieser Einschränkungen empfehlen wir, stattdessen eine benutzerdefinierte IAM-Rolle zu erstellen und zu verwenden, um mehr Flexibilität und Kontrolle zu gewährleisten. Die benutzerdefinierte Rolle, die Sie für die Registrierung des Standorts erstellen, muss die unter angegebenen Anforderungen erfüllen. [the section called “Anforderungen für Rollen, die zur Registrierung von Standorten verwendet werden”](#)

 Important

Wenn Sie eine verwendet haben Von AWS verwalteter Schlüssel , um den Amazon S3 S3-Standort zu verschlüsseln, können Sie die serviceverknüpfte Rolle Lake Formation nicht verwenden. Sie müssen eine benutzerdefinierte Rolle verwenden und der Rolle IAM-Berechtigungen für den Schlüssel hinzufügen. Einzelheiten finden Sie weiter unten in diesem Abschnitt.

In den folgenden Verfahren wird erklärt, wie Sie einen Amazon S3 S3-Standort registrieren, der entweder mit einem vom Kunden verwalteten Schlüssel oder einem verschlüsselt ist Von AWS verwalteter Schlüssel.

- [Registrierung eines mit einem vom Kunden verwalteten Schlüssel verschlüsselten Standorts](#)
- [Registrierung eines mit einem verschlüsselten Standort Von AWS verwalteter Schlüssel](#)

Bevor Sie beginnen

Prüfen Sie die [Anforderungen für die Rolle, die zur Registrierung des Standorts verwendet](#) wurde.

Um einen Amazon S3 S3-Standort zu registrieren, der mit einem vom Kunden verwalteten Schlüssel verschlüsselt ist

 Note

Wenn sich der KMS-Schlüssel oder der Amazon S3 S3-Standort nicht in demselben AWS Konto wie der Datenkatalog befinden, folgen Sie [the section called “AWS Kontoübergreifende](#)

Registrierung eines verschlüsselten Amazon S3 S3-Standorts“ stattdessen den Anweisungen unter.

1. Öffnen Sie die AWS KMS Konsole unter <https://console.aws.amazon.com/kms> und melden Sie sich als AWS Identity and Access Management (IAM-) Administratorbenutzer oder als Benutzer an, der die Schlüsselrichtlinie des KMS-Schlüssels ändern kann, der zur Verschlüsselung des Standorts verwendet wird.
2. Wählen Sie im Navigationsbereich die Option Vom Kunden verwaltete Schlüssel und dann den Namen des gewünschten KMS-Schlüssels aus.
3. Wählen Sie auf der Seite mit den KMS-Schlüsseldetails die Registerkarte Schlüsselrichtlinie aus, und führen Sie dann einen der folgenden Schritte aus, um Ihre benutzerdefinierte Rolle oder die mit dem Lake Formation Service verknüpfte Rolle als KMS-Schlüsselbenutzer hinzuzufügen:
 - Wenn die Standardansicht angezeigt wird (mit den Abschnitten Schlüsseladministratoren, Schlüssellöschung, Schlüsselbenutzer und Andere AWS Konten), fügen Sie im Abschnitt Schlüsselbenutzer Ihre benutzerdefinierte Rolle oder die mit dem Lake Formation Service verknüpfte Rolle `AWSServiceRoleForLakeFormationDataAccess` hinzu.
 - Wenn die Schlüsselrichtlinie (JSON) angezeigt wird — Bearbeiten Sie die Richtlinie, um Ihre benutzerdefinierte Rolle oder die mit dem Lake Formation Service verknüpfte Rolle `AWSServiceRoleForLakeFormationDataAccess` zum Objekt „Verwendung des Schlüssels zulassen“ hinzuzufügen, wie im folgenden Beispiel gezeigt.

 Note

Wenn das Objekt fehlt, fügen Sie es mit den im Beispiel gezeigten Berechtigungen hinzu. In dem Beispiel wird die serviceverknüpfte Rolle verwendet.

```
...
{
  "Sid": "Allow use of the key",
  "Effect": "Allow",
  "Principal": {
    "AWS": [
      "arn:aws:iam::111122223333:role/aws-service-role/
lakeformation.amazonaws.com/AWSServiceRoleForLakeFormationDataAccess",
      "arn:aws:iam::111122223333:user/keyuser"
```

```

        ]
      },
      "Action": [
        "kms:Encrypt",
        "kms:Decrypt",
        "kms:ReEncrypt*",
        "kms:GenerateDataKey*",
        "kms:DescribeKey"
      ],
      "Resource": "*"
    },
    ...

```

4. Öffnen Sie die AWS Lake Formation Konsole unter. <https://console.aws.amazon.com/lakeformation/> Melden Sie sich als Data Lake-Administrator oder als Benutzer mit der `lakeformation:RegisterResource` IAM-Berechtigung an.
5. Wählen Sie im Navigationsbereich unter Verwaltung die Option Data Lake-Standorte aus.
6. Wählen Sie Speicherort registrieren und anschließend Durchsuchen, um einen Amazon Simple Storage Service (Amazon S3) -Pfad auszuwählen.
7. (Optional, aber dringend empfohlen) Wählen Sie Standortberechtigungen überprüfen, um eine Liste aller vorhandenen Ressourcen am ausgewählten Amazon S3 S3-Standort und deren Berechtigungen anzuzeigen.

Die Registrierung des ausgewählten Standorts kann dazu führen, dass Ihre Lake Formation Formation-Benutzer Zugriff auf Daten erhalten, die sich bereits an diesem Standort befinden. Durch das Anzeigen dieser Liste können Sie sicherstellen, dass die vorhandenen Daten sicher bleiben.

8. Wählen Sie für die IAM-Rolle entweder die `AWSServiceRoleForLakeFormationDataAccess` serviceverknüpfte Rolle (Standard) oder Ihre benutzerdefinierte Rolle, die dem entspricht. [the section called “Anforderungen für Rollen, die zur Registrierung von Standorten verwendet werden”](#)
9. Wählen Sie „Standort registrieren“.

Weitere Informationen zur serviceverknüpften Rolle finden Sie unter [Dienstbezogene Rollenberechtigungen für Lake Formation](#).

Um einen Amazon S3 S3-Standort zu registrieren, der verschlüsselt ist mit einem Von AWS verwalteter Schlüssel

⚠ Important

Wenn sich der Amazon S3 S3-Standort nicht in demselben AWS Konto wie der Datenkatalog befindet, folgen Sie [the section called “AWS Kontoübergreifende Registrierung eines verschlüsselten Amazon S3 S3-Standorts”](#) stattdessen den Anweisungen unter.

1. Erstellen Sie eine IAM-Rolle, die zur Registrierung des Standorts verwendet werden soll. Stellen Sie sicher, dass es die unter aufgeführten Anforderungen erfüllt. [the section called “Anforderungen für Rollen, die zur Registrierung von Standorten verwendet werden”](#)
2. Fügen Sie der Rolle die folgende Inline-Richtlinie hinzu. Sie gewährt Berechtigungen für den Schlüssel zur Rolle. In der Resource Spezifikation muss der Amazon-Ressourcenname (ARN) des Von AWS verwalteter Schlüssel angegeben werden. Sie können den ARN von der AWS KMS Konsole abrufen. Um den richtigen ARN zu erhalten, stellen Sie sicher, dass Sie sich bei der AWS KMS Konsole mit demselben AWS Konto und derselben Region anmelden Von AWS verwalteter Schlüssel , mit der der Standort verschlüsselt wurde.

JSON

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Action": [
        "kms:Encrypt",
        "kms:Decrypt",
        "kms:ReEncrypt*",
        "kms:GenerateDataKey*",
        "kms:DescribeKey"
      ],
      "Resource": "arn:aws:kms:us-east-1:111122223333:key/1234abcd-12ab-34cd-56ef-1234567890ab"
    }
  ]
}
```

Sie können KMS-Schlüsselalias anstelle der Schlüssel-ID verwenden -
`arn:aws:kms:region:account-id:key/alias/your-key-alias`

Weitere Informationen finden Sie [im AWS KMS Abschnitt Aliase im](#) AWS Key Management Service Entwicklerhandbuch.

3. Öffnen Sie die AWS Lake Formation Konsole unter. <https://console.aws.amazon.com/lakeformation/> Melden Sie sich als Data Lake-Administrator oder als Benutzer mit der `lakeformation:RegisterResource` IAM-Berechtigung an.
4. Wählen Sie im Navigationsbereich unter Verwaltung die Option Data Lake-Standorte aus.
5. Wählen Sie Standort registrieren und anschließend Durchsuchen, um einen Amazon S3 S3-Pfad auszuwählen.
6. (Optional, aber dringend empfohlen) Wählen Sie Standortberechtigungen überprüfen, um eine Liste aller vorhandenen Ressourcen am ausgewählten Amazon S3 S3-Standort und deren Berechtigungen anzuzeigen.

Die Registrierung des ausgewählten Standorts kann dazu führen, dass Ihre Lake Formation Formation-Benutzer Zugriff auf Daten erhalten, die sich bereits an diesem Standort befinden. Durch das Anzeigen dieser Liste können Sie sicherstellen, dass die vorhandenen Daten sicher bleiben.

7. Wählen Sie für die IAM-Rolle die Rolle aus, die Sie in Schritt 1 erstellt haben.
8. Wählen Sie Standort registrieren.

Registrierung eines Amazon S3 S3-Standorts in einem anderen AWS Konto

AWS Lake Formation ermöglicht es Ihnen, Amazon Simple Storage Service (Amazon S3) -Standorte AWS kontenübergreifend zu registrieren. Wenn sich der beispielsweise in Konto A AWS Glue Data Catalog befindet, kann ein Benutzer in Konto A einen Amazon S3 S3-Bucket in Konto B registrieren.

Die Registrierung eines Amazon S3 S3-Buckets in AWS Konto B mithilfe einer AWS Identity and Access Management (IAM-) Rolle in AWS Konto A erfordert die folgenden Berechtigungen:

- Die Rolle in Konto A muss Berechtigungen für den Bucket in Konto B gewähren.
- Die Bucket-Richtlinie in Konto B muss der Rolle in Konto A Zugriffsberechtigungen gewähren.

⚠ Important

Vermeiden Sie es, einen Amazon S3 S3-Bucket zu registrieren, für den Zahlungen durch den Antragsteller aktiviert ist. Bei Buckets, die bei Lake Formation registriert sind, wird die Rolle, mit der der Bucket registriert wurde, immer als der Anforderer angesehen. Wenn ein anderes AWS Konto auf den Bucket zugreift, wird dem Bucket-Besitzer der Datenzugriff in Rechnung gestellt, sofern die Rolle zu demselben Konto gehört wie der Bucket-Besitzer.

Sie können die dienstverknüpfte Rolle Lake Formation nicht verwenden, um einen Standort in einem anderen Konto zu registrieren. Sie müssen stattdessen eine benutzerdefinierte Rolle verwenden. Die Rolle muss die Anforderungen von erfüllen. [the section called “Anforderungen für Rollen, die zur Registrierung von Standorten verwendet werden”](#) Weitere Informationen zur serviceverknüpften Rolle finden Sie unter [Dienstbezogene Rollenberechtigungen für Lake Formation](#).

Bevor Sie beginnen

Überprüfen Sie die [Anforderungen für die Rolle, mit der der Standort registriert](#) wurde.

Um einen Standort in einem anderen AWS Konto zu registrieren

ℹ Note

Wenn der Standort verschlüsselt ist, folgen Sie [the section called “AWS Kontoübergreifende Registrierung eines verschlüsselten Amazon S3 S3-Standorts”](#) stattdessen den Anweisungen unter.

Das folgende Verfahren geht davon aus, dass ein Principal im Konto 1111-2222-3333, das den Datenkatalog enthält, den Amazon S3 S3-Bucket registrieren möchte, der sich im Konto awsexamplebucket1 1234-5678-9012 befindet.

1. Melden Sie sich im Konto 1111-2222-3333 bei der an und öffnen Sie die IAM-Konsole unter. AWS-Managementkonsole <https://console.aws.amazon.com/iam/>
2. Erstellen Sie eine neue Rolle oder zeigen Sie eine vorhandene Rolle an, die die Anforderungen in erfüllt. [the section called “Anforderungen für Rollen, die zur Registrierung von Standorten verwendet werden”](#) Stellen Sie sicher, dass die Rolle Amazon S3 S3-Berechtigungen gewährtawsexamplebucket1.

3. Öffnen Sie die Amazon S3 S3-Konsole unter <https://console.aws.amazon.com/s3/>. Melden Sie sich mit dem Konto 1234-5678-9012 an.
4. Wählen Sie in der Liste mit den Bucket-Namen den Bucket-Namen aus. awsexamplebucket1
5. Wählen Sie Berechtigungen.
6. Wählen Sie auf der Seite „Berechtigungen“ die Option Bucket Policy aus.
7. Fügen Sie im Bucket-Policy-Editor die folgende Richtlinie ein. Ersetzen Sie *<role-name>* durch den Namen Ihrer Rolle.

JSON

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Principal": {
        "AWS": "arn:aws:iam::111122223333:role/<role-name>"
      },
      "Action": "s3:ListBucket",
      "Resource": "arn:aws:s3:::awsexamplebucket1"
    },
    {
      "Effect": "Allow",
      "Principal": {
        "AWS": "arn:aws:iam::111122223333:role/<role-name>"
      },
      "Action": [
        "s3:DeleteObject",
        "s3:GetObject",
        "s3:PutObject"
      ],
      "Resource": "arn:aws:s3:::awsexamplebucket1/*"
    }
  ]
}
```

8. Wählen Sie Speichern.
9. Öffnen Sie die AWS Lake Formation Konsole unter <https://console.aws.amazon.com/lakeformation/>. Melden Sie sich als Data Lake-Administrator oder als Benutzer mit

ausreichenden Berechtigungen zum Registrieren von Standorten beim Konto 1111-2222-3333 an.

10. Wählen Sie im Navigationsbereich unter Verwaltung die Option Data Lake-Standorte aus.
11. Wählen Sie auf der Seite Data Lake-Standorte die Option Standort registrieren aus.
12. Geben Sie auf der Seite Speicherort registrieren für den Amazon S3 S3-Pfad den Bucket-Namen eins3://awsexamplebucket1.

 Note

Sie müssen den Bucket-Namen eingeben, da kontoübergreifende Buckets nicht in der Liste erscheinen, wenn Sie Durchsuchen wählen.

13. Wählen Sie für die IAM-Rolle Ihre Rolle aus.
14. Wählen Sie Standort registrieren.

AWS Kontoübergreifende Registrierung eines verschlüsselten Amazon S3 S3-Standorts

AWS Lake Formation integriert in [AWS Key Management Service](#)(AWS KMS), damit Sie andere integrierte Dienste zum Verschlüsseln und Entschlüsseln von Daten an Amazon Simple Storage Service (Amazon S3) -Standorten einfacher einrichten können.

Beide vom Kunden verwalteten Schlüssel und Von AWS verwaltete Schlüssel werden unterstützt. Clientseitig encryption/decryption wird nicht unterstützt.

 Important

Vermeiden Sie es, einen Amazon S3 S3-Bucket zu registrieren, für den Zahlungen durch den Antragsteller aktiviert ist. Bei Buckets, die bei Lake Formation registriert sind, wird die Rolle, mit der der Bucket registriert wurde, immer als der Anforderer angesehen. Wenn ein anderes AWS Konto auf den Bucket zugreift, wird dem Bucket-Besitzer der Datenzugriff in Rechnung gestellt, sofern die Rolle zu demselben Konto gehört wie der Bucket-Besitzer.

In diesem Abschnitt wird erklärt, wie Sie einen Amazon S3 S3-Standort unter den folgenden Umständen registrieren:

- Die Daten am Amazon S3 S3-Standort werden mit einem KMS-Schlüssel verschlüsselt, der in erstellt wurde AWS KMS.
- Der Amazon S3 S3-Standort befindet sich nicht in demselben AWS Konto wie der AWS Glue Data Catalog.
- Der KMS-Schlüssel befindet sich entweder in demselben AWS Konto wie der Datenkatalog oder nicht.

Die Registrierung eines AWS KMS—verschlüsselten Amazon S3 S3-Buckets in AWS Konto B mithilfe einer AWS Identity and Access Management (IAM-) Rolle in AWS Konto A erfordert die folgenden Berechtigungen:

- Die Rolle in Konto A muss Berechtigungen für den Bucket in Konto B gewähren.
- Die Bucket-Richtlinie in Konto B muss der Rolle in Konto A Zugriffsberechtigungen gewähren.
- Wenn sich der KMS-Schlüssel in Konto B befindet, muss die Schlüsselrichtlinie Zugriff auf die Rolle in Konto A gewähren, und die Rolle in Konto A muss Berechtigungen für den KMS-Schlüssel gewähren.

Im folgenden Verfahren erstellen Sie eine Rolle in dem AWS Konto, das den Datenkatalog enthält (Konto A in der vorherigen Diskussion). Anschließend verwenden Sie diese Rolle, um den Standort zu registrieren. Lake Formation übernimmt diese Rolle beim Zugriff auf zugrunde liegende Daten in Amazon S3. Die übernommene Rolle verfügt über die erforderlichen Berechtigungen für den KMS-Schlüssel. Daher müssen Sie Prinzipalen, die mit ETL-Aufträgen oder integrierten Diensten wie z. B. auf die zugrunde liegenden Daten zugreifen, keine Berechtigungen für den KMS-Schlüssel gewähren. Amazon Athena

Important

Sie können die dienstverknüpfte Rolle Lake Formation nicht verwenden, um einen Standort in einem anderen Konto zu registrieren. Sie müssen stattdessen eine benutzerdefinierte Rolle verwenden. Die Rolle muss die Anforderungen von erfüllen. [the section called “Anforderungen für Rollen, die zur Registrierung von Standorten verwendet werden”](#) Weitere Informationen zur serviceverknüpften Rolle finden Sie unter [Dienstbezogene Rollenberechtigungen für Lake Formation](#).

Bevor Sie beginnen

Überprüfen Sie die [Anforderungen für die Rolle, mit der der Standort registriert](#) wurde.

Um einen verschlüsselten Amazon S3 S3-Standort AWS kontenübergreifend zu registrieren

1. Melden Sie sich mit demselben AWS Konto wie der Datenkatalog an AWS-Managementkonsole und öffnen Sie die IAM-Konsole unter <https://console.aws.amazon.com/iam/>.
2. Erstellen Sie eine neue Rolle oder zeigen Sie eine vorhandene Rolle an, die die Anforderungen in [the section called "Anforderungen für Rollen, die zur Registrierung von Standorten verwendet werden"](#) erfüllt. Stellen Sie sicher, dass die Rolle eine Richtlinie enthält, die Amazon S3 S3-Berechtigungen für den Standort gewährt.
3. Wenn sich der KMS-Schlüssel nicht in demselben Konto wie der Datenkatalog befindet, fügen Sie der Rolle eine Inline-Richtlinie hinzu, die die erforderlichen Berechtigungen für den KMS-Schlüssel gewährt. Es folgt eine Beispiellrichtlinie. Ersetzen Sie Region und Konto-ID durch die Region und Kontonummer des KMS-Schlüssels. `<key-id>` Ersetzen Sie durch die Schlüssel-ID.

JSON

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Action": [
        "kms:Encrypt",
        "kms:Decrypt",
        "kms:ReEncrypt*",
        "kms:GenerateDataKey*",
        "kms:DescribeKey"
      ],
      "Resource": "arn:aws:kms:us-east-1:111122223333:key/<key-id>"
    }
  ]
}
```

4. Fügen Sie in der Amazon S3 S3-Konsole eine Bucket-Richtlinie hinzu, die der Rolle die erforderlichen Amazon S3 S3-Berechtigungen gewährt. Hier finden Sie ein Beispiel für eine Bucket-Richtlinie. Ersetzen Sie die Konto-ID durch die AWS Kontonummer des Datenkatalogs, `<role-name>` durch den Namen Ihrer Rolle und `<bucket-name>` durch den Namen des Buckets.

JSON

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Principal": {
        "AWS": "arn:aws:iam::111122223333:role/<role-name>"
      },
      "Action": "s3:ListBucket",
      "Resource": "arn:aws:s3:::<bucket-name>"
    },
    {
      "Effect": "Allow",
      "Principal": {
        "AWS": "arn:aws:iam::111122223333:role/<role-name>"
      },
      "Action": [
        "s3:DeleteObject",
        "s3:GetObject",
        "s3:PutObject"
      ],
      "Resource": "arn:aws:s3:::<bucket-name>/*"
    }
  ]
}
```

5. Fügen Sie AWS KMS unter die Rolle als Benutzer des KMS-Schlüssels hinzu.
 - a. Öffnen Sie die AWS KMS Konsole unter <https://console.aws.amazon.com/kms>. Melden Sie sich dann als Administratorbenutzer oder als Benutzer an, der die Schlüsselrichtlinie des KMS-Schlüssels ändern kann, der zur Verschlüsselung des Speicherorts verwendet wird.
 - b. Wählen Sie im Navigationsbereich die Option Vom Kunden verwaltete Schlüssel und dann den Namen des KMS-Schlüssels aus.
 - c. Wenn auf der Seite mit den KMS-Schlüsseldetails auf der Registerkarte Schlüsselrichtlinie die JSON-Ansicht der Schlüsselrichtlinie nicht angezeigt wird, wählen Sie Zur Richtlinienansicht wechseln aus.

- d. Wählen Sie im Abschnitt Schlüsselrichtlinie die Option Bearbeiten und fügen Sie dem Allow use of the key Objekt den Amazon-Ressourcennamen (ARN) der Rolle hinzu, wie im folgenden Beispiel gezeigt.

 Note

Wenn das Objekt fehlt, fügen Sie es mit den im Beispiel gezeigten Berechtigungen hinzu.

```
...
{
  "Sid": "Allow use of the key",
  "Effect": "Allow",
  "Principal": {
    "AWS": [
      "arn:aws:iam::<catalog-account-id>:role/<role-name>"
    ]
  },
  "Action": [
    "kms:Encrypt",
    "kms:Decrypt",
    "kms:ReEncrypt*",
    "kms:GenerateDataKey*",
    "kms:DescribeKey"
  ],
  "Resource": "*"
},
...
```

Weitere Informationen finden Sie unter [Zulassen, dass Benutzer mit anderen Konten einen KMS-Schlüssel verwenden](#) können im AWS Key Management Service Entwicklerhandbuch.

6. Öffnen Sie die AWS Lake Formation Konsole unter <https://console.aws.amazon.com/lakeformation/>. Melden Sie sich als Data Lake-Administrator beim Data AWS Catalog-Konto an.
7. Wählen Sie im Navigationsbereich unter Verwaltung die Option Data Lake-Standorte aus.
8. Wählen Sie Standort registrieren aus.

9. Geben Sie auf der Seite Standort registrieren für Amazon S3 S3-Pfad den Standortpfad als `s3://<bucket>/<prefix>`. `<bucket>` Ersetzen Sie ihn durch den Namen des Buckets und `<prefix>` durch den Rest des Pfads für den Standort.

 Note

Sie müssen den Pfad eingeben, da kontoübergreifende Buckets nicht in der Liste angezeigt werden, wenn Sie Durchsuchen wählen.

10. Wählen Sie für die IAM-Rolle die Rolle aus Schritt 2 aus.
11. Wählen Sie Standort registrieren aus.

Abmeldung eines Amazon S3 S3-Standorts

Sie können einen Amazon Simple Storage Service (Amazon S3) -Standort abmelden, wenn Sie nicht mehr möchten, dass er von Lake Formation verwaltet wird. Die Abmeldung eines Standorts hat keine Auswirkungen auf die Datenstandortberechtigungen von Lake Formation, die für diesen Standort erteilt wurden. Sie können einen Standort, für den Sie die Registrierung aufgehoben haben, erneut registrieren, und die Berechtigungen für den Datenspeicherort bleiben in Kraft. Sie können eine andere Rolle verwenden, um den Standort erneut zu registrieren.

Um einen Standort abzumelden (Konsole)

1. Öffnen Sie die AWS Lake Formation Konsole unter <https://console.aws.amazon.com/lakeformation/> Melden Sie sich als Data Lake-Administrator oder als Benutzer mit der `lakeformation:RegisterResource` IAM-Berechtigung an.
2. Wählen Sie im Navigationsbereich unter Verwaltung die Option Data Lake-Standorte aus.
3. Wählen Sie einen Speicherort aus, und klicken Sie im Menü Aktionen auf Entfernen.
4. Wenn Sie zur Bestätigung aufgefordert werden, wählen Sie Entfernen.

Hybrider Zugriffsmodus

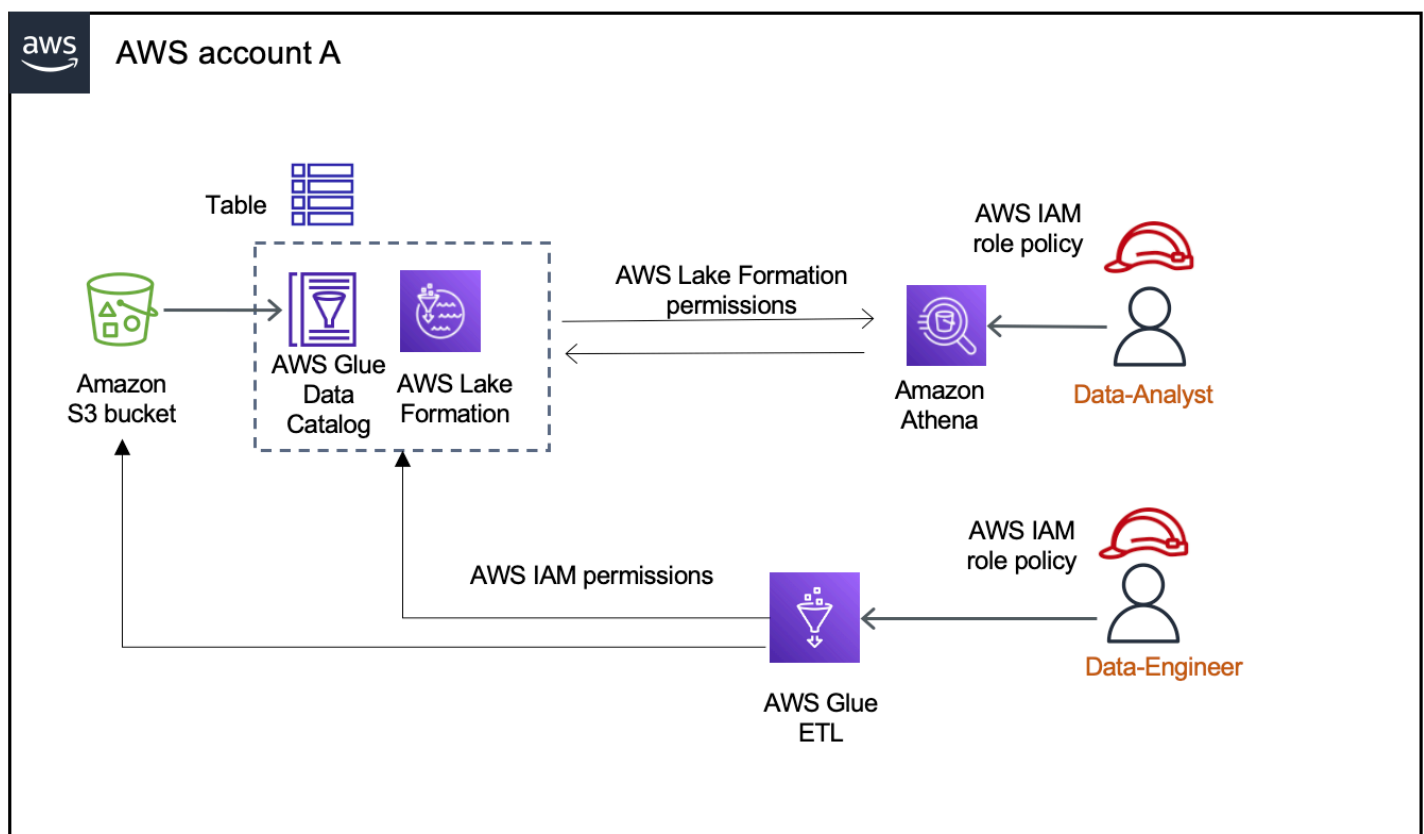
AWS Lake Formation Der hybride Zugriffsmodus unterstützt zwei Berechtigungspfade für dieselben Objekte. AWS Glue Data Catalog

Im ersten Schritt können Sie mit Lake Formation bestimmte Principals auswählen und ihnen Lake Formation Formations-Berechtigungen für den Zugriff auf Kataloge, Datenbanken, Tabellen und

Ansichten gewähren, indem Sie sich dafür anmelden. Der zweite Weg ermöglicht allen anderen Prinzipalen den Zugriff auf diese Ressourcen über die standardmäßigen IAM-Prinzipalrichtlinien für Amazon S3 und AWS Glue Aktionen.

Wenn Sie einen Amazon S3 S3-Standort bei Lake Formation registrieren, haben Sie die Möglichkeit, entweder Lake Formation Formations-Berechtigungen für alle Ressourcen an diesem Standort durchzusetzen oder den hybriden Zugriffsmodus zu verwenden. Der hybride Zugriffsmodus erzwingt standardmäßig nur `CREATE_TABLE` `UPDATE_TABLE` Berechtigungen. `CREATE_PARTITION` Wenn sich ein Amazon S3 S3-Standort im Hybridmodus befindet, können Sie Lake Formation Formations-Berechtigungen aktivieren, indem Sie Prinzipale für die Datenkatalogobjekte unter diesem Standort auswählen. Das bedeutet, dass sowohl Lake Formation Formations-Berechtigungen als auch IAM-Berechtigungen den Zugriff auf diese Daten kontrollieren können. Das bedeutet, dass für registrierte Principals sowohl Lake Formation Formations-Berechtigungen als auch IAM-Berechtigungen für den Zugriff auf die Daten erforderlich sind, während non-opted-in Principals weiterhin ausschließlich mit IAM-Berechtigungen auf Daten zugreifen.

Somit bietet der hybride Zugriffsmodus die Flexibilität, Lake Formation selektiv für Kataloge, Datenbanken und Tabellen in Ihrem Datenkatalog für eine bestimmte Gruppe von Benutzern zu aktivieren, ohne den Zugriff für andere bestehende Benutzer oder Workloads zu unterbrechen.



Überlegungen und Einschränkungen finden Sie unter [Überlegungen und Einschränkungen des hybriden Zugriffsmodus](#).

Begriffe und Definitionen

Im Folgenden finden Sie die Definitionen von Datenkatalogressourcen, die darauf basieren, wie Sie Zugriffsberechtigungen einrichten:

Ressource Lake Formation

Eine Ressource, die bei Lake Formation registriert ist. Benutzer benötigen Lake Formation Formation-Berechtigungen, um auf die Ressource zugreifen zu können.

AWS Glue Ressource

Eine Ressource, die nicht bei Lake Formation registriert ist. Benutzer benötigen nur IAM-Berechtigungen, um auf die Ressource zuzugreifen, da sie über `IAMAllowedPrincipals` Gruppenberechtigungen verfügt. Die Genehmigungen für Lake Formation werden nicht durchgesetzt.

Weitere Informationen zu `IAMAllowedPrincipals` Gruppenberechtigungen finden Sie unter [Berechtigungen für Metadaten](#).

Hybride Ressource

Eine Ressource, die im Hybridzugriffsmodus registriert ist. Je nachdem, welche Benutzer auf die Ressource zugreifen, wechselt die Ressource dynamisch zwischen einer Lake Formation Formation-Ressource und einer AWS Glue Ressource.

Allgemeine Anwendungsfälle im hybriden Zugriffsmodus

Sie können den hybriden Zugriffsmodus verwenden, um den Zugriff in Szenarien für die gemeinsame Nutzung von Daten mit einem Konto und zwischen Konten bereitzustellen:

Szenarien mit einem einzigen Konto

- Eine AWS Glue Ressource in eine Hybridressource konvertieren — In diesem Szenario verwenden Sie Lake Formation derzeit nicht, möchten aber Lake Formation Formation-Berechtigungen für Datenkatalogobjekte übernehmen. Wenn Sie den Amazon S3 S3-Standort im Hybridzugriffsmodus registrieren, können Sie Benutzern, die sich für bestimmte Datenbanken und Tabellen entscheiden, die auf diesen Standort verweisen, Lake Formation Formation-Berechtigungen gewähren.

- Eine Lake Formation Formation-Ressource in eine Hybridressource konvertieren — Derzeit verwenden Sie Lake Formation Formation-Berechtigungen, um den Zugriff auf eine Data Catalog-Datenbank zu steuern, möchten aber neuen Principals mithilfe von IAM-Berechtigungen für Amazon S3 Zugriff gewähren, AWS Glue ohne die bestehenden Lake Formation Formation-Berechtigungen zu unterbrechen.

Wenn Sie eine Datenstandortregistrierung auf den Hybridzugriffsmodus aktualisieren, können neue Principals mithilfe von IAM-Berechtigungsrichtlinien auf die Data Catalog-Datenbank zugreifen, die auf den Amazon S3 S3-Standort verweist, ohne die Lake Formation Formation-Berechtigungen der bestehenden Benutzer zu unterbrechen.

Bevor Sie die Datenstandortregistrierung aktualisieren, um den Hybridzugriffsmodus zu aktivieren, müssen Sie zunächst Prinzipale aktivieren, die derzeit mit Lake Formation Formation-Berechtigungen auf die Ressource zugreifen.

Dadurch soll eine mögliche Unterbrechung des aktuellen Workflows verhindert werden.

Sie müssen der IAMAllowedPrincipal Gruppe auch Super Berechtigungen für die Tabellen in der Datenbank erteilen.

Szenarien für den kontenübergreifenden Datenaustausch

- AWS Glue Ressourcen im hybriden Zugriffsmodus gemeinsam nutzen — In diesem Szenario verfügt das Produzentenkonto über Tabellen in einer Datenbank, die derzeit mit einem Verbraucherkonto gemeinsam genutzt werden, das IAM-Berechtigungsrichtlinien für Amazon S3 und AWS Glue Aktionen verwendet. Der Datenstandort der Datenbank ist nicht bei Lake Formation registriert.

Bevor Sie den Datenstandort im Hybridzugriffsmodus registrieren, müssen Sie die Einstellungen der kontoübergreifenden Version auf Version 4 aktualisieren. Version 4 enthält die neuen AWS RAM Berechtigungsrichtlinien, die für die kontoübergreifende gemeinsame Nutzung erforderlich sind, wenn die IAMAllowedPrincipal Gruppe über die erforderlichen Super Berechtigungen für die Ressource verfügt. Für Ressourcen mit IAMAllowedPrincipal Gruppenberechtigungen können Sie externen Konten Lake Formation Formation-Berechtigungen gewähren und sie für die Verwendung von Lake Formation Formation-Berechtigungen aktivieren. Der Data Lake-Administrator im Empfängerkonto kann den Prinzipalen im Konto Lake Formation Formation-Berechtigungen gewähren und sie aktivieren, um die Lake Formation Formation-Berechtigungen durchzusetzen.

- Lake Formation Formation-Ressourcen im hybriden Zugriffsmodus gemeinsam nutzen — Derzeit enthält das Produzentenkonto Tabellen in einer Datenbank, die mit einem Verbraucherkonto gemeinsam genutzt werden, wodurch Lake Formation Formation-Berechtigungen durchgesetzt werden. Der Datenstandort der Datenbank ist bei Lake Formation registriert.

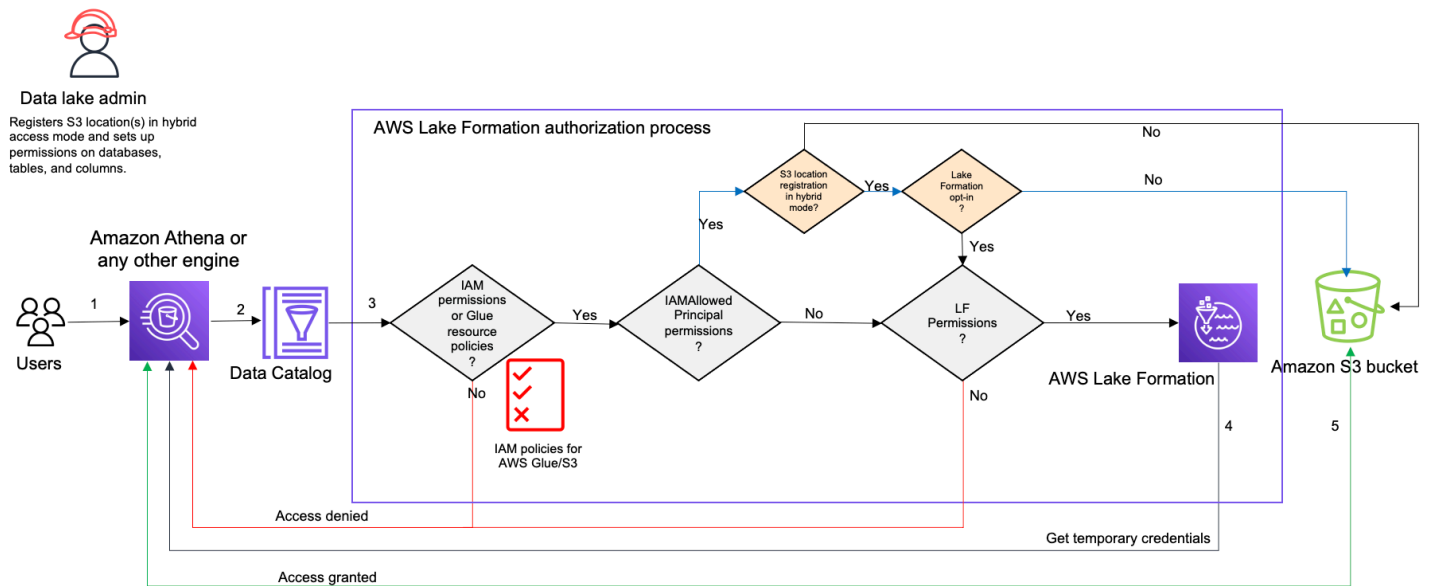
In diesem Fall können Sie die Amazon S3-Standortregistrierung auf den Hybridzugriffsmodus aktualisieren und die Daten aus Amazon S3 und Metadaten aus dem Datenkatalog mithilfe von Amazon S3 S3-Bucket-Richtlinien und Datenkatalog-Ressourcenrichtlinien an Prinzipale im Kundenkonto weitergeben. Sie müssen die bestehenden Lake Formation Formation-Berechtigungen erneut gewähren und die Principals aktivieren, bevor Sie die Amazon S3 S3-Standortregistrierung aktualisieren. Außerdem müssen Sie der Gruppe Super Berechtigungen für die Tabellen in der Datenbank erteilen. `IAMAllowedPrincipals`

Themen

- [So funktioniert der hybride Zugriffsmodus](#)
- [Einrichtung des hybriden Zugriffsmodus — häufig vorkommende Szenarien](#)
- [Prinzipale und Ressourcen aus dem Hybridzugriffsmodus entfernen](#)
- [Prinzipale und Ressourcen im Hybridzugriffsmodus anzeigen](#)
- [Weitere Ressourcen](#)

So funktioniert der hybride Zugriffsmodus

Das folgende Diagramm zeigt, wie die Lake Formation Formation-Autorisierung im Hybridzugriffsmodus funktioniert, wenn Sie die Datenkatalogressourcen abfragen.



Vor dem Zugriff auf Daten in Ihrem Data Lake richtet ein Data Lake-Administrator oder ein Benutzer mit Administratorberechtigungen individuelle Benutzerrichtlinien für Datenkatalogtabellen ein, um den Zugriff auf Tabellen in Ihrem Datenkatalog zuzulassen oder zu verweigern. Anschließend registriert ein Principal, der über die erforderlichen Berechtigungen zur Ausführung des RegisterResource Vorgangs verfügt, den Amazon S3 S3-Standort der Tabelle bei Lake Formation im Hybridzugriffsmodus. Wenn ein Datenstandort nicht bei Lake Formation registriert ist, erteilt der Administrator bestimmten Benutzern Lake Formation Formation-Berechtigungen für die Data Catalog-Datenbanken und -Tabellen und stimmt ihnen zu, Lake Formation Formation-Berechtigungen für diese Datenbanken und Tabellen im Hybridzugriffsmodus zu verwenden.

1. Sendet eine Abfrage — Ein Principal übermittelt eine Abfrage oder ein ETL-Skript mithilfe eines integrierten Services wie Amazon Athena AWS Glue, Amazon EMR oder Amazon Redshift Spectrum.
2. Fordert Daten an — Die integrierte Analyse-Engine identifiziert die angeforderte Tabelle und sendet die Metadatenanforderung an den Datenkatalog (,). GetTable GetDatabase
3. Prüft die Berechtigungen — Der Datenkatalog überprüft die Zugriffsberechtigungen des abfragenden Prinzips mit Lake Formation.
 - a. Wenn der Tabelle keine IAMAllowedPrincipals Gruppenberechtigungen zugewiesen sind, werden Lake Formation Formation-Berechtigungen erzwungen.
 - b. Wenn sich der Principal für die Verwendung Lake Formation Formation-Berechtigungen im Hybridzugriffsmodus entschieden hat und der Tabelle IAMAllowedPrincipals Gruppenberechtigungen zugewiesen sind, werden Lake Formation Formation-Berechtigungen

durchgesetzt. Die Abfrage-Engine wendet die Filter an, die sie von Lake Formation erhalten hat, und gibt die Daten an den Benutzer zurück.

- c. Wenn der Tabellenstandort nicht bei Lake Formation registriert ist und der Principal sich nicht für die Verwendung von Lake Formation Formation-Berechtigungen im Hybridzugriffsmodus entschieden hat, prüft der Datenkatalog, ob der Tabelle `IAMAllowedPrincipals` Gruppenberechtigungen zugewiesen sind. Wenn diese Berechtigung für die Tabelle vorhanden ist, erhalten alle Prinzipale im Konto Super oder All Berechtigungen für die Tabelle.

Der Verkauf von Anmeldeinformationen für Lake Formation ist nicht verfügbar, auch wenn diese Option aktiviert ist, es sei denn, der Datenstandort ist bei Lake Formation registriert.

4. Anmeldeinformationen abrufen — Der Datenkatalog überprüft und teilt der Engine mit, ob der Tabellenstandort bei Lake Formation registriert ist oder nicht. Wenn die zugrunde liegenden Daten bei Lake Formation registriert sind, fordert die Analyse-Engine Lake Formation nach temporären Anmeldeinformationen für den Zugriff auf Daten im Amazon S3 S3-Bucket an.
5. Daten abrufen — Wenn der Principal berechtigt ist, auf die Tabellendaten zuzugreifen, bietet Lake Formation temporären Zugriff auf die integrierte Analyse-Engine. Mithilfe des temporären Zugriffs ruft die Analyse-Engine die Daten von Amazon S3 ab und führt die erforderlichen Filter wie Spalten-, Zeilen- oder Zellenfilterung durch. Wenn die Engine die Ausführung des Jobs beendet hat, gibt sie die Ergebnisse an den Benutzer zurück. Dieser Prozess wird als Anmeldeinformationsvergabe bezeichnet. Für weitere Informationen siehe [Integration mit Lake Formation](#).
6. Wenn der Datenstandort der Tabelle nicht bei Lake Formation registriert ist, erfolgt der zweite Aufruf von der Analyse-Engine direkt an Amazon S3. Die betreffende Amazon S3 S3-Bucket-Richtlinie und die IAM-Benutzerrichtlinie werden im Hinblick auf den Datenzugriff bewertet. Wenn Sie IAM-Richtlinien verwenden, stellen Sie sicher, dass Sie die bewährten IAM-Methoden befolgen. Weitere Informationen finden Sie unter [Bewährte Sicherheitsmethoden in IAM im IAM-Benutzerhandbuch](#).

Einrichtung des hybriden Zugriffsmodus — häufig vorkommende Szenarien

Wie bei Lake Formation Formation-Berechtigungen gibt es im Allgemeinen zwei Arten von Szenarien, in denen Sie den Hybridzugriffsmodus verwenden können, um den Datenzugriff zu verwalten: Gewähren Sie Zugriff auf Prinzipale innerhalb eines Systems AWS-Konto und gewähren Sie Zugriff auf einen externen AWS-Konto oder Prinzipal.

Dieser Abschnitt enthält Anweisungen zur Einrichtung des hybriden Zugriffsmodus in den folgenden Szenarien:

Verwalten Sie Berechtigungen im hybriden Zugriffsmodus innerhalb eines AWS-Konto

- [Eine AWS Glue Ressource in eine Hybridressource konvertieren](#)— Sie gewähren derzeit Zugriff auf Tabellen in einer Datenbank für alle Principals in Ihrem Konto mithilfe von IAM-Berechtigungen für Amazon S3 und AWS Glue möchten Lake Formation verwenden, um Berechtigungen schrittweise zu verwalten.
- [Umwandlung einer Lake Formation Formation-Ressource in eine Hybridressource](#)— Sie verwenden derzeit Lake Formation, um den Zugriff auf Tabellen in einer Datenbank für alle Prinzipale in Ihrem Konto zu verwalten, möchten Lake Formation jedoch nur für bestimmte Prinzipale verwenden. Sie möchten Zugriff auf neue Principals gewähren, indem Sie IAM-Berechtigungen für AWS Glue und Amazon S3 für dieselbe Datenbank und dieselben Tabellen verwenden.

Verwalten Sie Berechtigungen im hybriden Zugriffsmodus für mehrere AWS-Konto

- [Gemeinsame Nutzung einer AWS Glue Ressource im hybriden Zugriffsmodus](#)— Sie verwenden Lake Formation derzeit nicht, um Berechtigungen für eine Tabelle zu verwalten, möchten aber Lake Formation-Berechtigungen anwenden, um Prinzipalen in einem anderen Konto Zugriff zu gewähren.
- [Gemeinsame Nutzung einer Lake Formation Formation-Ressource im hybriden Zugriffsmodus](#)— Sie verwenden Lake Formation, um den Zugriff auf eine Tabelle zu verwalten, möchten aber Zugriff für Principals in einem anderen Konto gewähren, indem Sie IAM-Berechtigungen für AWS Glue und Amazon S3 für dieselbe Datenbank und dieselben Tabellen verwenden.

Einrichtung des hybriden Zugriffsmodus — Allgemeine Schritte

1. Registrieren Sie den Amazon S3 S3-Datenstandort bei Lake Formation, indem Sie den Hybrid-Zugriffsmodus auswählen.
2. Principals müssen über die DATA_LOCATION Berechtigung für einen Data Lake-Standort verfügen, um Datenkatalogtabellen oder Datenbanken zu erstellen, die auf diesen Speicherort verweisen.
3. Stellen Sie die Einstellung für kontoübergreifende Version auf Version 4 ein.

4. Gewähren Sie bestimmten IAM-Benutzern oder -Rollen detaillierte Berechtigungen für Datenbanken und Tabellen. Stellen Sie gleichzeitig sicher, dass Sie der IAMAllowedPrincipals Gruppe in der Datenbank und allen oder ausgewählten Tabellen in der Datenbank All Berechtigungen zuweisen. Super
5. Wählen Sie die Prinzipale und Ressourcen aus. Andere Principals im Konto können weiterhin auf die Datenbanken und Tabellen zugreifen, indem sie IAM-Berechtigungsrichtlinien für AWS Glue und Amazon S3 S3-Aktionen verwenden.
6. Bereinigen Sie optional die IAM-Berechtigungsrichtlinien für Amazon S3 für die Principals, die sich für die Verwendung von Lake Formation Formation-Berechtigungen angemeldet haben.

Voraussetzungen für die Einrichtung des hybriden Zugriffsmodus

Im Folgenden sind die Voraussetzungen für die Einrichtung des hybriden Zugriffsmodus aufgeführt:

Note

Wir empfehlen, dass ein Lake Formation-Administrator den Amazon S3 S3-Standort im Hybridzugriffsmodus registriert und Prinzipale und Ressourcen aktiviert.

1. Erteilen Sie die Datenstandortberechtigung (DATA_LOCATION_ACCESS), um Datenkatalogressourcen zu erstellen, die auf die Amazon S3 S3-Standorte verweisen. Datenstandortberechtigungen steuern die Fähigkeit, Datenkatalogkataloge, Datenbanken und Tabellen zu erstellen, die auf bestimmte Amazon S3 S3-Standorte verweisen.
2. Um Data Catalog-Ressourcen mit einem anderen Konto im Hybridzugriffsmodus gemeinsam zu nutzen (ohne die IAMAllowedPrincipals Gruppenberechtigungen für die Ressource zu entfernen), müssen Sie die Einstellungen der kontoübergreifenden Version auf Version 4 oder höher aktualisieren. Um die Version mit der Lake Formation Console zu aktualisieren, wählen Sie Version 4 oder Version 5 unter Einstellungen für kontoübergreifende Versionen auf der Seite mit den Datenkatalogeinstellungen aus.

Sie können den `put-data-lake-settings` AWS CLI Befehl auch verwenden, um den `CROSS_ACCOUNT_VERSION` Parameter auf Version 4 oder 5 zu setzen:

```
aws lakeformation put-data-lake-settings --region us-east-1 --data-lake-settings
  file://settings
{
```

```

    "DataLakeAdmins": [
      {
        "DataLakePrincipalIdentifier": "arn:aws:iam::<111122223333>:user/<user-name>"
      }
    ],
    "CreateDatabaseDefaultPermissions": [],
    "CreateTableDefaultPermissions": [],
    "Parameters": {
      "CROSS_ACCOUNT_VERSION": "5"
    }
  }
}

```

3.

Um kontenübergreifende Berechtigungen im Hybridzugriffsmodus zu gewähren, muss der Gewährer über die erforderlichen IAM-Berechtigungen für AWS Glue Dienste und Dienste verfügen. AWS RAM Die AWS verwaltete Richtlinie `AWSLakeFormationCrossAccountManager` gewährt die erforderlichen Berechtigungen. Um die kontoübergreifende gemeinsame Nutzung von Daten im Hybridzugriffsmodus zu ermöglichen, haben wir die `AWSLakeFormationCrossAccountManager` verwaltete Richtlinie aktualisiert und zwei neue IAM-Berechtigungen hinzugefügt:

- RAM: `ListResourceSharePermissions`
- RAM: `AssociateResourceSharePermission`

Note

Wenn Sie die AWS verwaltete Richtlinie nicht für die Rolle des Antragstellers verwenden, fügen Sie die oben genannten Richtlinien zu Ihren benutzerdefinierten Richtlinien hinzu.

Amazon S3 S3-Bucket-Standort und Benutzerzugriff

Wenn Sie einen Katalog, eine Datenbank oder eine Tabelle in der erstellen AWS Glue Data Catalog, können Sie den Amazon S3 S3-Bucket-Speicherort der zugrunde liegenden Daten angeben und ihn bei Lake Formation registrieren. In den folgenden Tabellen wird beschrieben, wie Berechtigungen für AWS Glue und Lake Formation Formation-Benutzer (Principals) funktionieren, basierend auf dem Amazon S3 S3-Datenspeicherort der Tabelle oder Datenbank.

Amazon S3 S3-Standort ist bei Lake Formation registriert

Amazon S3 S3-Speicherort einer Datenbank	AWS Glue Benutzer	Lake Formation Formation-Benutzer
Registriert bei Lake Formation (im Hybrid-Zugriffsmodus oder im Lake Formation Formation-Modus)	Haben Sie read/write Zugriff auf den Amazon S3 S3-Datenstandort, indem Sie die Berechtigungen der IAMAllowed Principals-Gruppe (Superzugriff) erben.	Erben Sie die Berechtigungen zum Erstellen von Tabellen von der ihnen erteilten CREATE TABLE-Berechtigung.
Kein zugeordneter Amazon S3 S3-Standort	Für die Ausführung der Anweisungen CREATE TABLE und INSERT TABLE ist die ausdrückliche DATA LOCATION-Berechtigung erforderlich.	Für die Ausführung der Anweisungen CREATE TABLE und INSERT TABLE ist die ausdrückliche DATA LOCATION-Berechtigung erforderlich.

IsRegisteredWithLakeFormationTabelleneigenschaft

Die `IsRegisteredWithLakeFormation` Eigenschaft einer Tabelle gibt an, ob die Datenposition der Tabelle bei Lake Formation für den Anforderer registriert ist. Wenn der Berechtigungsmodus des Standorts als Lake Formation registriert ist, gilt die `IsRegisteredWithLakeFormation` Eigenschaft `true` für alle Benutzer, die auf den Datenstandort zugreifen, da alle Benutzer als für diese Tabelle angemeldet gelten. Wenn der Standort im Hybridzugriffsmodus registriert ist, wird der Wert `true` nur für Benutzer festgelegt, die sich für diese Tabelle angemeldet haben.

Funktionsweise von **IsRegisteredWithLakeFormation**

Berechtigungsmodus	Benutzer/Rollen	IsRegisteredWithLakeFormation	Description
Lake Formation	Alle	Wahr	Wenn ein Standort bei Lake Formation registriert ist, wird die <code>IsRegistered</code>

Berechtigungsmodus	Benutzer/Rollen	IsRegisteredWithLakeFormation	Description
			redWithLakeFormation Eigenschaft für alle Benutzer auf true gesetzt. Das bedeutet, dass die in Lake Formation definierten Berechtigungen für den registrierten Standort gelten. Der Verkauf von Anmeldeinformationen wird von Lake Formation durchgeführt.

Berechtigungsmodus	Benutzer/Rollen	IsRegisteredWithLakeFormation	Description
Hybrider Zugriffsmodus	Hat sich angemeldet	Wahr	Für Benutzer, die sich für die Verwendung von Lake Formation für den Datenzugriff und die Verwaltung einer Tabelle entschieden haben, wird die <code>IsRegisteredWithLakeFormation</code> Eigenschaft <code>true</code> für diese Tabelle auf gesetzt. Sie unterliegen den in Lake Formation für den registrierten Standort definierten Genehmigungsrichtlinien.

Berechtigungsmodus	Benutzer/Rollen	IsRegisteredWithLakeFormation	Description
Hybrider Zugriffsmodus	Nicht angemeldet	Falsch	Für Benutzer, die sich nicht für die Verwendung von Lake Formation-Berechtigungen entschieden haben, ist die IsRegisteredWithLakeFormation-Eigenschaft auf gesetztfalse. Sie unterliegen nicht den in Lake Formation für den registrierten Standort definierten Genehmigungsrichtlinien. Stattdessen befolgen die Benutzer die Amazon S3-Berechtigungsrichtlinien.

Eine AWS Glue Ressource in eine Hybridressource konvertieren

Gehen Sie wie folgt vor, um einen Amazon S3-Standort im Hybridzugriffsmodus zu registrieren und neue Lake Formation-Benutzer einzubinden, ohne den Datenzugriff der bestehenden Data Catalog-Benutzer zu unterbrechen.

Beschreibung des Szenarios — Der Datenstandort ist nicht bei Lake Formation registriert, und der Benutzerzugriff auf die Data Catalog-Datenbank und die Tabellen wird durch IAM-Berechtigungsrichtlinien für Amazon S3 und AWS Glue Aktionen bestimmt.

Die IAMAllowedPrincipals Gruppe hat standardmäßig Super Berechtigungen für alle Tabellen in der Datenbank.

Um den Hybridzugriffsmodus für einen Datenstandort zu aktivieren, der nicht bei Lake Formation registriert ist

1. Registrieren Sie einen Amazon S3 S3-Standort, um den Hybrid-Zugriffsmodus zu aktivieren.

Console

1. Melden Sie sich als Data Lake-Administrator bei der [Lake Formation Formation-Konsole](#) an.
2. Wählen Sie im Navigationsbereich unter Administration die Option Data Lake-Standorte aus.
3. Wählen Sie Standort registrieren aus.

Register location

Amazon S3 location

Register an Amazon S3 path as the storage location for your data lake.

Amazon S3 path

Choose an Amazon S3 path for your data lake.

e.g.: s3://bucket/prefix/

Browse

Review location permissions - strongly recommended

Registering the selected location may result in your users gaining access to data already at that location. Before registering a location, we recommend that you review existing location permissions on resources in that location.

Review location permissions

IAM role

To add or update data, Lake Formation needs read/write access to the chosen Amazon S3 path. Choose a role that you know has permission to do this, or choose the **AWSServiceRoleForLakeFormationDataAccess** service-linked role. When you register the first Amazon S3 path, the service-linked role and a new inline policy are created on your behalf. Lake Formation adds the first path to the inline policy and attaches it to the service-linked role. When you register subsequent paths, Lake Formation adds the path to the existing policy.

AWSServiceRoleForLakeFormationDataAccess ▼

 Do not select the service linked role if you plan to use EMR.

☐ **Enable Data Catalog Federation**

Checking this box will allow Lake Formation to assume a role to access tables in a federated database.

Permission mode

Select the permission mode you want to use to manage access.

☒ **Hybrid access mode - new**

Lake Formation permissions can co-exist with IAM permission policies for AWS Glue and S3 actions to manage access. [Learn more](#) 

☐ **Lake Formation**

Only Lake Formation permissions are enforced.

Cancel

Register location

- Wählen Sie im Fenster Standort registrieren den Amazon S3-Pfad aus, den Sie bei Lake Formation registrieren möchten.
- Wählen Sie für die IAM-Rolle entweder die **AWSServiceRoleForLakeFormationDataAccess** serviceverknüpfte Rolle (Standard)

oder eine benutzerdefinierte IAM-Rolle, die die Anforderungen von erfüllt.

[Anforderungen für Rollen, die zur Registrierung von Standorten verwendet werden](#)

6. Wählen Sie den Hybrid-Zugriffsmodus, um detaillierte Lake Formation Zugriffskontrollrichtlinien auf Opt-in-Prinzipale und Data Catalog-Datenbanken und -Tabellen anzuwenden, die auf den registrierten Standort verweisen.

Wählen Sie Lake Formation, damit Lake Formation Zugriffsanfragen für den registrierten Standort autorisieren kann.

7. Wählen Sie Standort registrieren.

AWS CLI

Im Folgenden finden Sie ein Beispiel für die Registrierung eines Datenstandorts bei Lake Formation HybridAccessEnabled mit:true/false. Der Standardwert für den Parameter ist falsch. HybridAccessEnabled Ersetzen Sie den Amazon S3 S3-Pfad, den Rollennamen und die AWS Konto-ID durch gültige Werte.

```
aws lakeformation register-resource --cli-input-json file:file path
json:
{
  "ResourceArn": "arn:aws:s3:::s3-path",
  "UseServiceLinkedRole": false,
  "RoleArn": "arn:aws:iam::<123456789012>:role/<role-name>",
  "HybridAccessEnabled": true
}
```

2. Gewähren Sie Berechtigungen und stimmen Sie Principals zu, um Lake Formation Formations-Berechtigungen für Ressourcen im Hybridzugriffsmodus zu verwenden

Bevor Sie sich für Prinzipale und Ressourcen im Hybridzugriffsmodus entscheiden, stellen Sie sicher, dass für die Datenbanken und Tabellen, deren Standort bei Lake Formation im Hybridzugriffsmodus registriert ist, Super oder All Berechtigungen zum IAMAllowedPrincipals Gruppieren vorhanden sind.

Note

Sie können der IAMAllowedPrincipals Gruppe All tables innerhalb einer Datenbank keine Zugriffsrechte gewähren. Sie müssen jede Tabelle separat aus dem Drop-down-Menü auswählen und Berechtigungen erteilen. Wenn Sie neue Tabellen

in der Datenbank erstellen, können Sie auch die `Use only IAM access control for new tables in new databases` in den Datenkatalogeinstellungen verwenden. Diese Option erteilt der `IAMAllowedPrincipals` Gruppe automatisch die `Super` Berechtigung, wenn Sie neue Tabellen in der Datenbank erstellen.

Console

1. Wählen Sie in der Lake Formation Formation-Konsole unter Datenkatalog die Option Kataloge, Datenbanken oder Tabellen aus.
2. Wählen Sie einen Katalog, eine Datenbank oder eine Tabelle aus der Liste aus und wählen Sie im Menü Aktionen die Option Grant aus.
3. Wählen Sie Principals aus, um mithilfe von benannten Ressourcenmethoden oder LF-Tags Berechtigungen für die Datenbank, Tabellen und Spalten zu gewähren.

Wählen Sie alternativ Datenberechtigungen aus, wählen Sie aus der Liste die Prinzipale aus, denen Berechtigungen erteilt werden sollen, und wählen Sie dann Grant aus.

Weitere Informationen zum Erteilen von Datenberechtigungen finden Sie unter [Erteilen von Berechtigungen für Datenkatalogressourcen](#).

Note

Wenn Sie einem Prinzipal die Berechtigung „Tabelle erstellen“ erteilen, müssen Sie dem Prinzipal auch Datenspeicherberechtigungen (`DATA_LOCATION_ACCESS`) erteilen. Diese Berechtigung ist nicht erforderlich, um Tabellen zu aktualisieren. Weitere Informationen finden Sie unter [Erteilung von Berechtigungen zum Speicherort von Daten](#).

4. Wenn Sie die Methode „Benannte Ressource“ verwenden, um Berechtigungen zu erteilen, ist die Option, Prinzipale und Ressourcen zu aktivieren, im unteren Bereich der Seite Datenberechtigungen gewähren verfügbar.

Wählen Sie Lake Formation Formation-Berechtigungen sofort wirksam machen, um Lake Formation Formation-Berechtigungen für die Prinzipale und Ressourcen zu aktivieren.

Hybrid access mode

In hybrid access mode, Lake Formation and IAM policies for AWS Glue and S3 work together.

☒ **Make Lake Formation permissions effective immediately**

Lake Formation permissions are enforced for databases, tables, and principals.

ⓘ You might get access denied.

If the checkbox is selected, your Lake Formation permissions are enforced. Make sure that you've completed the required setup for Lake Formation for the permissions to work. If the checkbox is clear, you can go to [hybrid access mode](#) to add resources and principals. [Learn more](#)

Cancel

Grant

5. Wählen Sie Grant (Erteilen).

Wenn Sie Principal A für Tabelle A auswählen, die auf einen Datenstandort verweist, ermöglicht es Principal A, mithilfe von Lake Formation Formations-Berechtigungen auf den Speicherort dieser Tabelle zuzugreifen, wenn der Datenstandort im Hybridmodus registriert ist.

AWS CLI

Im Folgenden finden Sie ein Beispiel für die Auswahl eines Prinzipals und einer Tabelle im Hybridzugriffsmodus. Ersetzen Sie den Rollennamen, die AWS Konto-ID, den Datenbanknamen und den Tabellennamen durch gültige Werte.

```
aws lakeformation create-lake-formation-opt-in --cli-input-json file://file path
json:
{
  "Principal": {
    "DataLakePrincipalIdentifier":
"arn:aws:iam::<123456789012>:role/<hybrid-access-role>"
  },
  "Resource": {
    "Table": {
      "CatalogId": "<123456789012>",
      "DatabaseName": "<hybrid_test>",
      "Name": "<hybrid_test_table>"
    }
  }
}
```

}

- a. (Optional) Wenn Sie LF-Tags zur Erteilung von Berechtigungen wählen, können Sie in einem separaten Schritt festlegen, dass Prinzipale Lake Formation Formation-Berechtigungen verwenden. Sie können dies tun, indem Sie in der linken Navigationsleiste unter Berechtigungen den Hybrid-Zugriffsmodus auswählen.
- b. Wählen Sie im unteren Bereich der Seite Hybrid-Zugriffsmodus die Option Hinzufügen aus, um Ressourcen und Prinzipale zum Hybridzugriffsmodus hinzuzufügen.
- c. Wählen Sie auf der Seite Ressourcen und Prinzipale hinzufügen die Kataloge, Datenbanken und Tabellen aus, die im Hybridzugriffsmodus registriert sind.

Sie können `All tables` unter einer Datenbank auswählen, ob Sie Zugriff gewähren möchten.

Add resources and principals

Choose databases, tables, and principals to add in hybrid access mode. Lake Formation permissions will be enforced.

[Learn more](#)

Resources

Catalogs

Databases

Select one or more databases.

Choose databases

testdb

Tables - optional

Select one or more tables.

Choose tables

testtable

- d. Wählen Sie Principals aus, um Lake Formation Formation-Berechtigungen im hybriden Zugriffsmodus zu verwenden.
 - Principals — Sie können IAM-Benutzer und -Rollen für dasselbe Konto oder für ein anderes Konto auswählen. Sie können auch SAML-Benutzer und -Gruppen auswählen.

- **Attribute** — Wählen Sie Attribute aus, um Berechtigungen auf der Grundlage von Attributen zu gewähren.

Principals

☐ **IAM users and roles**
Users or roles from this AWS account.

☐ **External accounts**
AWS account, AWS organization or IAM principal outside of this account.

☐ **SAML users and groups**
SAML users and group or QuickSight ARNs.

☒ **Attributes - new**
Define permissions using attributes (IAM session tags) with a Cedar policy expression.

Attribute expression

Add tag key-value pairs from IAM roles or [IAM session tags](#). Separate values with commas. **AND** logic applies between pairs, **OR** logic within keys. Verify tag entries for accuracy.

Key	Value
Department	Sales

[Add key-value pair](#)

Expression review

The attribute expression above will be written in the following Cedar policy. Use CLI/SDK to edit or write custom Cedar policy.

```

permit (principal, action, resource)
when {
  context.iam.principalTags.hasTag("Department")
  && context.iam.principalTags.getTag("Department") == "Sales"
};
        
```

Permission scope

☒ This account
 ☐ External account

- Geben Sie das Schlüssel-Wert-Paar ein, um einen Grant auf der Grundlage von Attributen zu erstellen. Überprüfen Sie den Cedar-Richtlinienausdruck auf der Konsole. Weitere Informationen zu Cedar finden Sie unter [Was ist Cedar? | Sprachreferenz für Cedar Policy GuideLink](#).
- Wählen Sie Hinzufügen aus.

Allen IAMs roles/users mit passenden Attributen wird Zugriff gewährt.

- e. Wählen Sie Hinzufügen aus.

Umwandlung einer Lake Formation Formation-Ressource in eine Hybridressource

In Fällen, in denen Sie derzeit Lake Formation Formation-Berechtigungen für Ihre Datenkatalog-Datenbanken und -Tabellen verwenden, können Sie die Eigenschaften der Standortregistrierung bearbeiten, um den Hybridzugriffsmodus zu aktivieren. Auf diese Weise können Sie neuen Principals mithilfe von IAM-Berechtigungsrichtlinien für Amazon S3 und AWS Glue Aktionen Zugriff auf dieselben Ressourcen gewähren, ohne bestehende Lake Formation Formation-Berechtigungen zu unterbrechen.

Beschreibung des Szenarios — Bei den folgenden Schritten wird davon ausgegangen, dass Sie einen Datenstandort bei Lake Formation registriert haben und dass Sie Berechtigungen für Prinzipale für Datenbanken, Tabellen oder Spalten eingerichtet haben, die auf diesen Speicherort verweisen. Wenn der Standort mit einer dienstverknüpften Rolle registriert wurde, können Sie die Standortparameter nicht aktualisieren und den Hybridzugriffsmodus nicht aktivieren. Die `IAMAllowedPrincipals` Gruppe verfügt standardmäßig über Superberechtigungen für die Datenbank und all ihre Tabellen.

Important

Aktualisieren Sie eine Standortregistrierung nicht auf den Hybridzugriffsmodus, ohne die Prinzipale zu aktivieren, die auf Daten an diesem Standort zugreifen.

Aktivierung des hybriden Zugriffsmodus für einen bei Lake Formation registrierten Datenstandort

1.

Warning

Wir empfehlen nicht, einen von Lake Formation verwalteten Datenstandort in den hybriden Zugriffsmodus zu konvertieren, um zu vermeiden, dass die Berechtigungsrichtlinien anderer vorhandener Benutzer oder Workloads unterbrochen werden.

Entscheiden Sie sich für die bestehenden Principals, die über Lake Formation Formation-Berechtigungen verfügen.

1. Führen Sie die Berechtigungen auf, die Sie Principals für Kataloge, Datenbanken und Tabellen erteilt haben, und überprüfen Sie sie. Weitere Informationen finden Sie unter [Datenbank- und Tabellenberechtigungen in Lake Formation anzeigen](#).
 2. Wählen Sie in der linken Navigationsleiste unter Berechtigungen den Hybrid-Zugriffsmodus und dann Hinzufügen aus.
 3. Wählen Sie auf der Seite Prinzipale und Ressourcen hinzufügen die Kataloge, Datenbanken und Tabellen aus dem Amazon S3 S3-Datenspeicherort aus, die Sie im Hybridzugriffsmodus verwenden möchten. Wählen Sie die Principals aus, die bereits über Lake Formation Formation-Berechtigungen verfügen.
 4. Wählen Sie Hinzufügen, um die Prinzipale für die Verwendung von Lake Formation Formation-Berechtigungen im Hybridzugriffsmodus zu aktivieren.
2. Aktualisieren Sie die Amazon S3 bucket/prefix S3-Registrierung, indem Sie die Option Hybrid-Zugriffsmodus wählen.

Console

1. Melden Sie sich als Data Lake-Administrator bei der Lake Formation Formation-Konsole an.
2. Wählen Sie im Navigationsbereich unter Registrieren und Ingest die Option Data Lake-Standorte aus.
3. Wählen Sie einen Standort aus, und klicken Sie im Menü Aktionen auf Bearbeiten.
4. Wählen Sie den Hybrid-Zugriffsmodus.
5. Wählen Sie Speichern.
6. Wählen Sie unter Datenkatalog die Datenbank oder Tabelle aus und gewähren Sie der aufgerufenen virtuellen Gruppe Super oder All Berechtigungen `IAMAllowedPrincipals`.
7. Stellen Sie sicher, dass der Zugriff Ihrer bestehenden Lake Formation Formation-Benutzer nicht unterbrochen wird, wenn Sie die Eigenschaften der Standortregistrierung aktualisiert haben. Melden Sie sich als Lake Formation-Principal bei der Athena-Konsole an und führen Sie eine Beispielabfrage für eine Tabelle aus, die auf den aktualisierten Speicherort verweist.

Überprüfen Sie auf ähnliche Weise den Zugriff von AWS Glue Benutzern, die IAM-Berechtigungsrichtlinien für den Zugriff auf die Datenbank und die Tabellen verwenden.

AWS CLI

Im Folgenden finden Sie ein Beispiel für die Registrierung eines Datenstandorts bei Lake Formation HybridAccessEnabled mit:true/false. Der Standardwert für den Parameter ist falsch. HybridAccessEnabled Ersetzen Sie den Amazon S3 S3-Pfad, den Rollennamen und die AWS Konto-ID durch gültige Werte.

```
aws lakeformation update-resource --cli-input-json file://file path
json:
{
  "ResourceArn": "arn:aws:s3:::<s3-path>",
  "RoleArn": "arn:aws:iam::<123456789012>:role/<test>",
  "HybridAccessEnabled": true
}
```

Gemeinsame Nutzung einer AWS Glue Ressource im hybriden Zugriffsmodus

Teilen Sie Daten mit einem anderen AWS-Konto oder einem Principal in einem anderen, indem Sie Lake Formation AWS-Konto Formation-Berechtigungen durchsetzen, ohne den IAM-basierten Zugriff vorhandener Data Catalog-Benutzer zu unterbrechen.

Beschreibung des Szenarios — Das Produzentenkonto verfügt über eine Datenkatalog-Datenbank, deren Zugriff mithilfe von IAM-Prinzipalrichtlinien für Amazon S3 und AWS Glue Aktionen gesteuert wird. Der Datenstandort der Datenbank ist nicht bei Lake Formation registriert. Die IAMAllowedPrincipals Gruppe hat standardmäßig Super Berechtigungen für die Datenbank und all ihre Tabellen.

Erteilung kontenübergreifender Lake Formation Formation-Berechtigungen im Hybridzugriffsmodus

1. Produzentenkonto eingerichtet

1. Melden Sie sich mit einer Rolle, die über lakeformation:PutDataLakeSettings IAM-Berechtigungen verfügt, bei der Lake Formation Formation-Konsole an.
2. Gehen Sie zu den Datenkatalogeinstellungen und wählen Sie die Einstellungen **Version 4** für die kontoübergreifende Version aus.

Wenn Sie derzeit Version 1 oder 2 verwenden, lesen Sie die [Aktualisierung der Versionseinstellungen für die kontenübergreifende gemeinsame Nutzung von Daten](#) Anweisungen zur Aktualisierung auf Version 3.

Beim Upgrade von Version 3 auf 4 sind keine Änderungen der Berechtigungsrichtlinien erforderlich.

3. Registrieren Sie den Amazon S3 S3-Speicherort der Datenbank oder Tabelle, die Sie im Hybridzugriffsmodus teilen möchten.
4. Vergewissern Sie sich, dass für die Datenbanken und Tabellen, deren Datenspeicherort Sie im obigen Schritt im Hybridzugriffsmodus registriert haben, Super Berechtigungen für die IAMAllowedPrincipals Gruppe vorhanden sind.
5. Erteilen Sie Lake Formation Formation-Berechtigungen für AWS Organisationen, Organisationseinheiten (OUs) oder direkt mit einem IAM-Prinzipal in einem anderen Konto.
6. Wenn Sie einem IAM-Prinzipal direkt Berechtigungen gewähren, wählen Sie den Prinzipal aus dem Verbraucherkonto aus, um Lake Formation Formation-Berechtigungen im Hybridzugriffsmodus durchzusetzen, indem Sie die Option Lake Formation Formation-Berechtigungen sofort wirksam machen aktivieren aktivieren.

Wenn Sie einem anderen AWS Konto kontoübergreifende Berechtigungen gewähren, werden die Lake Formation Formation-Berechtigungen bei der Aktivierung des Kontos nur für die Administratoren dieses Kontos durchgesetzt. Der Data Lake-Administrator des Empfängerkontos muss die Berechtigungen kaskadieren und die Principals im Konto aktivieren, um Lake Formation Formation-Berechtigungen für die gemeinsam genutzten Ressourcen durchzusetzen, die sich im Hybridzugriffsmodus befinden.

Wenn Sie die Option Mit LF-Tags abgeglichene Ressourcen auswählen, um kontoübergreifende Berechtigungen zu gewähren, müssen Sie zuerst den Schritt „Berechtigungen erteilen“ abschließen. Sie können Principals und Ressourcen in einem separaten Schritt für den Hybridzugriffsmodus aktivieren, indem Sie in der linken Navigationsleiste der Lake Formation Formation-Konsole unter Berechtigungen den Hybridzugriffsmodus auswählen. Wählen Sie dann Hinzufügen, um die Ressourcen und Principals hinzuzufügen, für die Sie Lake Formation Formation-Berechtigungen erzwingen möchten.

2. Kundenkonto eingerichtet

1. Melden Sie sich <https://console.aws.amazon.com/lakeformation/> als Data Lake-Administrator bei der Lake Formation Konsole an.
2. Gehen Sie zur <https://console.aws.amazon.com/ram/Startseite> und nehmen Sie die Einladung zur gemeinsamen Nutzung von Ressourcen an. Auf der Registerkarte Für mich freigegeben in der AWS RAM Konsole werden die Datenbank und die Tabellen angezeigt, die für Ihr Konto freigegeben sind.
3. Erstellen Sie einen Ressourcenlink zur gemeinsam genutzten and/or Datenbanktabelle in Lake Formation.
4. Erteilen Sie den IAM-Prinzipalen in Ihrem (Verbraucher-) Konto Grant on target Berechtigungen für den Ressourcenlink und Berechtigungen (für die ursprünglich gemeinsam genutzte Ressource).
5. Erteilen Sie den Prinzipalen in Ihrem Konto Lake Formation-Berechtigungen für die Datenbank oder Tabelle, die mit Ihnen geteilt wurde. Entscheiden Sie sich für die Prinzipale und Ressourcen, um Lake Formation-Berechtigungen im hybriden Zugriffsmodus durchzusetzen, indem Sie die Option Lake Formation-Berechtigungen sofort wirksam machen aktivieren.
6. Testen Sie die Lake Formation-Berechtigungen des Prinzipals, indem Sie Athena-Beispielabfragen ausführen. Testen Sie den bestehenden Zugriff Ihrer AWS Glue Benutzer mit IAM-Prinzipalrichtlinien für Amazon S3 und AWS Glue Aktionen.

(Optional) Entfernen Sie die Amazon S3 S3-Bucket-Richtlinie für den Datenzugriff und die IAM-Prinzipalrichtlinien für AWS Glue und den Amazon S3 S3-Datenzugriff für die Prinzipale, die Sie für die Verwendung von Lake Formation-Berechtigungen konfiguriert haben.

Gemeinsame Nutzung einer Lake Formation-Ressource im hybriden Zugriffsmodus

Erlauben Sie neuen Data Catalog-Benutzern in einem externen Konto den Zugriff auf Data Catalog-Datenbanken und -Tabellen mithilfe von IAM-basierten Richtlinien, ohne die bestehenden Kontofreigabeberechtigungen von Lake Formation zu unterbrechen.

Beschreibung des Szenarios: Das Produzentenkonto verfügt über eine von Lake Formation verwaltete Datenbank und Tabellen, die mit einem externen (Verbraucher-) Konto auf Konto- oder IAM-Prinzipalebene gemeinsam genutzt werden. Der Datenstandort der Datenbank ist bei Lake

Formation registriert. Die IAMAllowedPrincipals Gruppe hat keine Super Berechtigungen für die Datenbank und ihre Tabellen.

Neuen Data Catalog-Benutzern kontenübergreifenden Zugriff über IAM-basierte Richtlinien gewähren, ohne bestehende Lake Formation Formation-Berechtigungen zu unterbrechen

1. Produzentenkonto eingerichtet

1. Melden Sie sich mit einer Rolle bei der Lake Formation Formation-Konsole anlakeformation:PutDataLakeSettings.
2. Wählen Sie unter Einstellungen für den Datenkatalog die Einstellungen **Version 4** für die kontenübergreifende Version aus.

Wenn Sie derzeit Version 1 oder 2 verwenden, lesen Sie die [Aktualisierung der Versionseinstellungen für die kontenübergreifende gemeinsame Nutzung von Daten](#) Anweisungen zur Aktualisierung auf Version 3.

Für ein Upgrade von Version 3 auf 4 sind keine Änderungen der Berechtigungsrichtlinien erforderlich.

3. Führen Sie die Berechtigungen auf, die Sie Prinzipalen für Datenbanken und Tabellen erteilt haben. Weitere Informationen finden Sie unter [Datenbank- und Tabellenberechtigungen in Lake Formation anzeigen](#).
4. Gewähren Sie bestehende kontenübergreifende Berechtigungen von Lake Formation erneut, indem Sie sich für Prinzipale und Ressourcen entscheiden.

Note

Bevor Sie eine Datenstandortregistrierung auf den Hybridzugriffsmodus aktualisieren, um kontenübergreifende Berechtigungen zu gewähren, müssen Sie mindestens eine kontenübergreifende Datenfreigabe pro Konto erneut gewähren. Dieser Schritt ist erforderlich, um die AWS RAM verwalteten Berechtigungen zu aktualisieren, die der Ressourcenfreigabe zugeordnet sind. AWS RAM

Im Juli 2023 hat Lake Formation die AWS RAM verwalteten Berechtigungen aktualisiert, die für die gemeinsame Nutzung von Datenbanken und Tabellen verwendet werden:

- `arn:aws:ram::aws:permission/AWSRAMLFEnabledGlueAllTablesReadWriteForDatabase`(Richtlinie zur gemeinsamen Nutzung auf Datenbankebene)

- `arn:aws:ram::aws:permission/AWSRAMLFEnabledGlueTableReadWrite`(Freigaberichtlinie auf Tabellenebene)
Für kontoübergreifende Genehmigungen, die vor Juli 2023 erteilt wurden, gelten diese aktualisierten Berechtigungen nicht. AWS RAM
Wenn Sie Prinzipalen direkt kontoübergreifende Berechtigungen erteilt haben, müssen Sie diese Berechtigungen den Prinzipalen einzeln erneut gewähren. Wenn Sie diesen Schritt überspringen, wird bei den Prinzipalen, die auf die gemeinsam genutzte Ressource zugreifen, möglicherweise ein unzulässiger Kombinationsfehler angezeigt.

5. Geh nach <https://console.aws.amazon.com/ram/Hause>.
6. Auf der Registerkarte Von mir gemeinsam genutzt in der AWS RAM Konsole werden die Datenbank- und Tabellennamen angezeigt, die Sie mit einem externen Konto oder Prinzipal geteilt haben.

Stellen Sie sicher, dass die mit der gemeinsam genutzten Ressource verknüpften Berechtigungen den richtigen ARN haben.
7. Stellen Sie sicher, dass die Ressourcen in der AWS RAM Freigabe Associated den Status haben. Wenn der Status als angezeigt wird `Associating`, warten Sie, bis sie in den `Associated` Status wechseln. Wenn der Status lautet `Failed`, halten Sie an und wenden Sie sich an das Lake Formation-Serviceteam.
8. Wählen Sie in der linken Navigationsleiste unter Berechtigungen den Hybrid-Zugriffsmodus und dann Hinzufügen aus.
9. Auf der Seite „Prinzipale und Ressourcen hinzufügen“ werden die Datenbanken, and/ or Tabellen und Prinzipale angezeigt, die Zugriff haben. Sie können die erforderlichen Aktualisierungen vornehmen, indem Sie Prinzipale und Ressourcen hinzufügen oder entfernen.
10. Wählen Sie die Principals mit Lake Formation Formation-Berechtigungen für die Datenbank und die Tabellen aus, die Sie in den Hybridzugriffsmodus ändern möchten. Wählen Sie die Datenbanken und Tabellen aus.
11. Wählen Sie Hinzufügen, um die Principals zu aktivieren, um Lake Formation Formation-Berechtigungen im Hybridzugriffsmodus durchzusetzen.
12. Erteilen Sie der virtuellen Gruppe `Super IAMAllowedPrincipals` Berechtigungen für Ihre Datenbank und ausgewählte Tabellen.
13. Bearbeiten Sie die Registrierung des Amazon S3 S3-Standorts Lake Formation in den Hybridzugriffsmodus.

14. Erteilen Sie den AWS Glue Benutzern im externen (Verbraucher-) Konto mithilfe von IAM-Berechtigungsrichtlinien für Amazon S3 AWS Glue S3-Aktionen Berechtigungen.

2. Kundenkonto eingerichtet

1. Melden Sie sich <https://console.aws.amazon.com/lakeformation/> als Data Lake-Administrator bei der Lake Formation Konsole an.
2. Gehen Sie zur <https://console.aws.amazon.com/ram/Startseite> und nehmen Sie die Einladung zur gemeinsamen Nutzung von Ressourcen an. Auf der Registerkarte Mit mir geteilte Ressourcen auf der AWS RAM Seite werden die Datenbank- und Tabellennamen angezeigt, die mit Ihrem Konto geteilt wurden.

Stellen Sie für das AWS RAM Teilen sicher, dass die angehängte Berechtigung den richtigen ARN der geteilten AWS RAM Einladung enthält. Prüfen Sie, ob sich die Ressourcen in der AWS RAM Freigabe im Associated Status befinden. Wenn der Status als angezeigt wird `Associating`, warten Sie, bis sie in den Associated Status wechseln. Wenn der Status lautet `Failed`, halten Sie an und wenden Sie sich an das Lake Formation-Serviceteam.

3. Erstellen Sie einen Ressourcenlink zur gemeinsam genutzten and/or Datenbanktabelle in Lake Formation.
4. `Describe` Erteilen Sie den IAM-Prinzipalen in Ihrem (Verbraucher-) Konto `Grant on target` Berechtigungen für den Ressourcenlink und Berechtigungen (für die ursprünglich gemeinsam genutzte Ressource).
5. Als Nächstes richten Sie Lake Formation Berechtigungen für Principals in Ihrem Konto in der gemeinsam genutzten Datenbank oder Tabelle ein.

Wählen Sie in der linken Navigationsleiste unter Berechtigungen den Hybridzugriffsmodus aus.

6. Wählen Sie im unteren Bereich der Seite für den hybriden Zugriffsmodus die Option Hinzufügen aus, um die Prinzipale und die Datenbank oder Tabelle zu aktivieren, die über das Produzentenkonto für Sie freigegeben wurde.
7. Erteilen Sie den AWS Glue Benutzern in Ihrem Konto mithilfe von IAM-Berechtigungsrichtlinien für Amazon S3 AWS Glue S3-Aktionen Berechtigungen.
8. Testen Sie die Lake Formation Berechtigungen und AWS Glue -Berechtigungen der Benutzer, indem Sie mit Athena separate Beispielabfragen für die Tabelle ausführen

(Optional) Bereinigen Sie die IAM-Berechtigungsrichtlinien für Amazon S3 für die Principals, die sich im Hybridzugriffsmodus befinden.

Prinzipale und Ressourcen aus dem Hybridzugriffsmodus entfernen

Gehen Sie wie folgt vor, um Datenbanken, Tabellen und Prinzipale aus dem Hybridzugriffsmodus zu entfernen.

Console

1. Melden Sie sich bei der Lake Formation Formation-Konsole unter an <https://console.aws.amazon.com/lakeformation/>.
2. Wählen Sie unter Berechtigungen die Option Hybrid-Zugriffsmodus aus.
3. Aktivieren Sie auf der Seite Hybrid-Zugriffsmodus das Kontrollkästchen neben dem Datenbank- oder Tabellennamen und wählen Sie Remove.
4. In einer Warnmeldung werden Sie aufgefordert, die Aktion zu bestätigen. Wählen Sie Remove (Entfernen) aus.

Lake Formation erzwingt keine Berechtigungen mehr für diese Ressourcen, und der Zugriff auf diese Ressource wird mithilfe von IAM und AWS Glue Berechtigungen gesteuert. Dies kann dazu führen, dass der Benutzer keinen Zugriff mehr auf diese Ressource hat, wenn er nicht über die entsprechenden IAM-Berechtigungen verfügt.

AWS CLI

Das folgende Beispiel zeigt, wie Ressourcen aus dem Hybridzugriffsmodus entfernt werden.

```
aws lakeformation delete-lake-formation-opt-in --cli-input-json file://file path

json:
{
  "Principal": {
    "DataLakePrincipalIdentifier": "arn:aws:iam::<123456789012>:role/role name"
  },
  "Resource": {
    "Table": {
      "CatalogId": "<123456789012>",
      "DatabaseName": "<database name>",
      "Name": "<table name>"
    }
  }
}
```

Prinzipale und Ressourcen im Hybridzugriffsmodus anzeigen

Gehen Sie wie folgt vor, um Datenbanken, Tabellen und Prinzipale im Hybridzugriffsmodus anzuzeigen.

Console

1. Melden Sie sich bei der Lake Formation Konsole unter an <https://console.aws.amazon.com/lakeformation/>.
2. Wählen Sie unter Berechtigungen die Option Hybrid-Zugriffsmodus aus.
3. Auf der Seite Hybridzugriffsmodus werden die Ressourcen und Prinzipale angezeigt, die sich derzeit im Hybridzugriffsmodus befinden.

AWS CLI

Das folgende Beispiel zeigt, wie alle Opt-in-Prinzipale und Ressourcen aufgelistet werden, die sich im Hybridzugriffsmodus befinden.

```
aws lakeformation list-lake-formation-opt-ins
```

Das folgende Beispiel zeigt, wie Opt-In für ein bestimmtes Principal-Resource-Paar aufgelistet wird.

```
aws lakeformation list-lake-formation-opt-ins --cli-input-json file://file path

json:
{
  "Principal": {
    "DataLakePrincipalIdentifier": "arn:aws:iam::<account-id>:role/<role name>"
  },
  "Resource": {
    "Table": {
      "CatalogId": "<account-id>",
```



```
        "DatabaseName": "<database name>",
        "Name": "<table name>"
    }
}
```

Weitere Ressourcen

Im folgenden Blogbeitrag führen wir Sie durch die Anweisungen zur Integration von Lake Formation Formation-Berechtigungen im Hybrid-Zugriffsmodus für ausgewählte Benutzer, während die Datenbank bereits für andere Benutzer über IAM- und Amazon S3 S3-Berechtigungen zugänglich ist. Wir werden uns die Anweisungen zur Einrichtung des hybriden Zugriffsmodus innerhalb eines AWS Kontos und zwischen zwei Konten ansehen.

- [Einführung des hybriden Zugriffsmodus für AWS Glue Data Catalog den sicheren Zugriff mithilfe von Lake Formation und IAM- und Amazon S3 S3-Richtlinien.](#)

Objekte erstellen in AWS Glue Data Catalog

AWS Lake Formation verwendet den AWS Glue Data Catalog (Datenkatalog), um Metadaten zu Data Lakes, Datenquellen, Transformationen und Zielen zu speichern. Metadaten sind Daten zu den Daten im Datensatz. Jedes AWS Konto hat einen Datenkatalog pro AWS Region.

Die Metadaten im Datenkatalog sind in einer dreistufigen Datenhierarchie organisiert, die Kataloge, Datenbanken und Tabellen umfasst. Es organisiert Daten aus verschiedenen Quellen in logischen Containern, den sogenannten Katalogen. Jeder Katalog stellt Daten aus Quellen wie Amazon Redshift Data Warehouses, Amazon DynamoDB Datenbanken und Datenquellen von Drittanbietern wie Snowflake, MySQL und über 30 externen Datenquellen dar, die über föderierte Konnektoren integriert sind. Sie können auch neue Kataloge im Datenkatalog erstellen, um Daten in S3 Table Buckets oder Redshift Managed Storage (RMS) zu speichern.

In Tabellen werden Informationen über die zugrunde liegenden Daten gespeichert, einschließlich Schemainformationen, Partitionsinformationen und Datenspeicherort. Datenbanken sind Sammlungen von Tabellen. Der Datenkatalog enthält auch Ressourcenlinks, d. h. Links zu gemeinsam genutzten Katalogen, Datenbanken und Tabellen in externen Konten, die für den kontenübergreifenden Zugriff auf Daten im Data Lake verwendet werden.

Der Datenkatalog ist ein verschachteltes Katalogobjekt, das Kataloge, Datenbanken und Tabellen enthält. Er wird durch die AWS-Konto ID referenziert und ist der Standardkatalog in einem Konto und einer AWS-Region. Der Datenkatalog verwendet eine dreistufige Hierarchie (catalog.database.table), um Tabellen zu organisieren.

- **Katalog** — Die oberste Ebene der dreistufigen Metadatenhierarchie des Datenkatalogs. Sie können einem Datenkatalog über einen Verbund mehrere Kataloge hinzufügen.
- **Datenbank** — Die zweite Ebene der Metadatenhierarchie, die aus Tabellen und Ansichten besteht. Eine Datenbank wird in vielen Datensystemen wie Amazon Redshift und Trino auch als Schema bezeichnet.
- **Tabelle und Ansicht** — Die dritte Ebene der dreistufigen Datenhierarchie des Datenkatalogs.

Alle Iceberg-Tabellen in Amazon S3 werden im Standard-Datenkatalog mit der Katalog-ID = AWS-Konto ID gespeichert. Sie können Verbundkataloge erstellen AWS Glue Data Catalog, in denen Definitionen von Tabellen in Amazon Redshift, Amazon S3 Table Storage oder anderen Datenquellen von Drittanbietern über den Verbund gespeichert werden.

Themen

- [Einen Katalog erstellen](#)
- [Erstellen einer Datenbank](#)
- [Erstellen von Tabellen](#)
- [AWS Glue Data Catalog Ansichten von Gebäuden](#)

Einen Katalog erstellen

Kataloge stellen die höchste oder oberste Ebene in der dreistufigen Metadatenhierarchie von dar. AWS Glue Data Catalog Sie können mehrere Methoden verwenden, um Daten in den Datenkatalog aufzunehmen und Kataloge mit mehreren Ebenen zu erstellen.

Weitere Informationen zum Erstellen von Katalogen aus externen Datenquellen finden Sie unter [Bringen Sie Ihre Daten in die AWS Glue Data Catalog](#)

Um einen Katalog mit der Lake Formation Formation-Konsole zu erstellen, müssen Sie als Data Lake-Administrator oder Katalogersteller angemeldet sein. Ein Katalogersteller ist ein Principal, dem die CREATE_CATALOG Genehmigung für Lake Formation erteilt wurde. Eine Liste der Katalogersteller finden Sie auf der Seite Administrative Rollen und Aufgaben der Lake Formation Formation-Konsole.

Um diese Liste anzeigen zu können, müssen Sie über die `lakeformation:ListPermissions` IAM-Berechtigung verfügen und als Data Lake-Administrator oder als Katalogersteller mit der Option „Gewähren“ für die `CREATE_CATALOG` Berechtigung angemeldet sein.

Erstellen einer Datenbank

Metadatentabellen im Datenkatalog werden in Datenbanken gespeichert. Sie können so viele Datenbanken erstellen, wie Sie benötigen, und Sie können für jede Datenbank unterschiedliche Lake Formation Formations-Berechtigungen gewähren.

Datenbanken können über eine optionale Standorteigenschaft verfügen. Dieser Standort befindet sich normalerweise innerhalb eines Amazon Simple Storage Service (Amazon S3) -Standorts, der bei Lake Formation registriert ist. Wenn Sie einen Speicherort angeben, benötigen Principals keine Datenspeicherortberechtigungen, um Datenkatalogtabellen zu erstellen, die auf Speicherorte innerhalb des Datenbankspeicherorts verweisen. Weitere Informationen finden Sie unter [Underlying data access control](#).

Um eine Datenbank mit der Lake Formation Formations-Konsole zu erstellen, müssen Sie als Data Lake-Administrator oder Datenbankersteller angemeldet sein. Ein Datenbankersteller ist ein Principal, dem die Lake Formation `CREATE_DATABASE` Formations-Genehmigung erteilt wurde. Eine Liste der Datenbankersteller finden Sie auf der Seite Administrative Rollen und Aufgaben der Lake Formation Formations-Konsole. Um diese Liste anzeigen zu können, müssen Sie über die `lakeformation:ListPermissions` IAM-Berechtigung verfügen und als Data Lake-Administrator oder als Datenbankersteller mit der Grant-Option für die `CREATE_DATABASE` Berechtigung angemeldet sein.

So erstellen Sie eine Datenbank

1. Öffnen Sie die AWS Lake Formation Konsole unter <https://console.aws.amazon.com/lakeformation/> und melden Sie sich als Data Lake-Administrator oder Datenbankersteller an.
2. Wählen Sie im Navigationsbereich unter Datenkatalog die Option Datenbanken aus.
3. Wählen Sie Datenbank erstellen aus.
4. Geben Sie im Dialogfeld Datenbank erstellen einen Datenbanknamen, einen optionalen Speicherort und eine optionale Beschreibung ein.
5. Wählen Sie optional Nur IAM-Zugriffskontrolle für neue Tabellen in dieser Datenbank verwenden aus.

Weitere Informationen zu dieser Option finden Sie unter [the section called “Ändern der Standardeinstellungen für Ihren Data Lake”](#).

6. Wählen Sie Datenbank erstellen aus.

Erstellen von Tabellen

AWS Lake Formation Metadatentabellen enthalten Informationen über Daten im Data Lake, einschließlich Schemainformationen, Partitionsinformationen und Datenspeicherort. Diese Tabellen werden im AWS Glue Datenkatalog gespeichert. Sie verwenden sie, um auf die zugrunde liegenden Daten im Data Lake zuzugreifen und diese Daten mit Lake Formation Formation-Berechtigungen zu verwalten. Tabellen werden in Datenbanken im Datenkatalog gespeichert.

Es gibt mehrere Möglichkeiten, Datenkatalogtabellen zu erstellen:

- Führen Sie einen Crawler in AWS Glue aus. Weitere Informationen finden Sie unter [Definieren von Crawlern](#) im AWS Glue Entwicklerhandbuch.
- Erstellen Sie einen Workflow und führen Sie ihn aus. Siehe [the section called “Daten mithilfe von Workflows importieren”](#).
- Erstellen Sie manuell eine Tabelle mit der Lake Formation Formation-Konsole, der AWS Glue API oder AWS Command Line Interface (AWS CLI).
- Erstellen Sie eine Tabelle mit Amazon Athena.
- Erstellen Sie einen Ressourcenlink zu einer Tabelle in einem externen Konto. Siehe [the section called “Ressourcenlinks erstellen”](#).

Erstellen von Apache-Iceberg-Tabellen

AWS Lake Formation unterstützt die Erstellung von Apache Iceberg-Tabellen, die das Apache Parquet-Datenformat verwenden, AWS Glue Data Catalog wobei sich die Daten in Amazon S3 befinden. Eine Tabelle im Data Catalog ist die Metadatendefinition, die die Daten in einem Datenspeicher repräsentiert. Standardmäßig erstellt Lake Formation Iceberg v2-Tabellen. Den Unterschied zwischen v1- und v2-Tabellen finden Sie unter [Formatversionsänderungen](#) in der Apache-Iceberg-Dokumentation.

[Apache Iceberg](#) ist ein offenes Tabellenformat für sehr große analytische Datensätze. Iceberg ermöglicht einfache Änderungen an Ihrem Schema, auch bekannt als Schemaentwicklung. Das

bedeutet, dass Benutzer Spalten zu einer Datentabelle hinzufügen, umbenennen oder daraus entfernen können, ohne die zugrunde liegenden Daten zu stören. Iceberg unterstützt auch die Datenversionierung, sodass Benutzer Änderungen an Daten im Laufe der Zeit nachverfolgen können. Dadurch wird die Zeitreisefeature aktiviert, mit der Benutzer auf die bisherigen Versionen von Daten zugreifen und diese abfragen und Datenänderungen zwischen Aktualisierungen und Löschungen analysieren können.

Sie können die Lake Formation Formation-Konsole oder den `CreateTable` Vorgang in der AWS Glue API verwenden, um eine Iceberg-Tabelle im Datenkatalog zu erstellen. Weitere Informationen finden Sie unter [CreateTable action \(Python: `create\_table`\)](#).

Wenn Sie eine Iceberg-Tabelle im Data Catalog erstellen, müssen Sie das Tabellenformat und den Metadaten-Dateipfad in Amazon S3 angeben, um Lese- und Schreibvorgänge durchführen zu können.

Sie können Lake Formation verwenden, um Ihre Iceberg-Tabelle mithilfe detaillierter Zugriffskontrollberechtigungen zu sichern, wenn Sie den Amazon S3 S3-Datenstandort bei registrieren. AWS Lake Formation Für Quelldaten in Amazon S3 und Metadaten, die nicht bei Lake Formation registriert sind, wird der Zugriff durch IAM-Berechtigungsrichtlinien für Amazon S3 und AWS Glue Aktionen bestimmt. Weitere Informationen finden Sie unter [Verwaltung von Lake Formation Formation-Berechtigungen](#).

Note

Data Catalog unterstützt nicht das Erstellen von Partitionen und das Hinzufügen von Iceberg-Tabelleneigenschaften.

Themen

- [Voraussetzungen](#)
- [Erstellen einer Iceberg-Tabelle](#)

Voraussetzungen

Um Iceberg-Tabellen im Data Catalog zu erstellen und Lake-Formation-Datenzugriffsberechtigungen einzurichten, müssen Sie die folgenden Anforderungen erfüllen:

1. Berechtigungen, die zum Erstellen von Iceberg-Tabellen ohne die bei Lake Formation registrierten Daten erforderlich sind.

Zusätzlich zu den Berechtigungen, die zum Erstellen der Tabelle im Data Catalog erforderlich sind, benötigt der Tabellenersteller folgende Berechtigungen:

- `s3:PutObject` in Ressource `arn:aws:s3:::{bucketName}`
 - `s3:GetObject` in Ressource `arn:aws:s3:::{bucketName}`
 - `s3:DeleteObject` in Ressource `arn:aws:s3:::{bucketName}`
2. Berechtigungen, die zum Erstellen von Iceberg-Tabellen mit den bei Lake Formation registrierten Daten erforderlich sind.

Um Lake Formation zur Verwaltung und Sicherung der Daten in Ihrem Data Lake zu verwenden, registrieren Sie Ihren Amazon-S3-Speicherort, der die Daten für Tabellen enthält, bei Lake Formation. Auf diese Weise kann Lake Formation Anmeldeinformationen an AWS Analysedienste wie Athena, Redshift Spectrum und Amazon EMR weitergeben, um auf Daten zuzugreifen. Weitere Informationen zur Registrierung eines Amazon S3 S3-Standorts finden Sie unter [Hinzufügen eines Amazon S3 S3-Standorts zu Ihrem Data Lake](#).

Ein Principal, der die zugrunde liegenden Daten liest und schreibt, die bei Lake Formation registriert sind, benötigt folgende Berechtigungen:

- `lakeformation:GetDataAccess`
- `DATA_LOCATION_ACCESS`

Ein Principal, der über Berechtigungen zum Speichern von Daten für einen Standort verfügt, hat auch Standortberechtigungen für alle untergeordneten Standorte.

Weitere Informationen zu Berechtigungen für den Datenspeicherort finden Sie unter [Zugrundeliegende Datenzugriffskontrolle](#).

Um die Komprimierung zu aktivieren, muss der Service eine IAM-Rolle übernehmen, die über Berechtigungen zum Aktualisieren von Tabellen im Data Catalog verfügt. Einzelheiten finden Sie unter [Voraussetzungen für die Tabellenoptimierung](#).

Erstellen einer Iceberg-Tabelle

Sie können Iceberg v1- und v2-Tabellen mit der Lake Formation Formation-Konsole oder AWS Command Line Interface wie auf dieser Seite dokumentiert erstellen. Sie können Iceberg-Tabellen

auch mit der AWS Glue Konsole oder erstellen. AWS-Glue-Crawler Weitere Informationen finden Sie unter [Data Catalog und Crawler](#) im AWS Glue -Entwicklerhandbuch.

So erstellen Sie eine Iceberg-Tabelle

Console

1. Melden Sie sich bei an AWS-Managementkonsole und öffnen Sie die Lake Formation Formation-Konsole unter <https://console.aws.amazon.com/lakeformation/>.
2. Wählen Sie unter „Data Catalog“ die Option Tabellen aus, und verwenden Sie die Schaltfläche Tabelle erstellen, um die folgenden Attribute anzugeben:
 - Tabellenname: Geben Sie einen Namen für die Tabelle ein. Wenn Sie Athena verwenden, um auf Tabellen zuzugreifen, verwenden Sie diese [Benennungstipps](#) im Amazon-Athena-Benutzerhandbuch.
 - Datenbank: Wählen Sie eine bestehende Datenbank oder erstellen Sie eine neue.
 - Beschreibung: Die Beschreibung der Tabelle. Sie können eine Beschreibung zum besseren Verständnis der Inhalte der Tabelle schreiben.
 - Tabellenformat: Wählen Sie als Tabellenformat Apache Iceberg.

The screenshot shows the AWS Lake Formation console interface. At the top, there's a 'Table format' section with an 'Info' link. Below it, a message states: 'Data Catalog managed tables support data compaction for Apache Iceberg table type. [Learn more](#)'. There are two radio button options: 'Standard AWS Glue table (default)' with the subtext 'Create a standard AWS Glue table.', and 'Apache Iceberg table' which is selected, with the subtext 'Create a table in Apache Iceberg table format.'. Below this is the 'Table optimization' section, which says 'Enable optimization capabilities for Apache Iceberg tables enhance query performance.' and lists three checked options: 'Compaction' (Combine small data files into larger, more efficient files to optimize table performance.), 'Snapshot retention - new' (Optimize table storage by removing old snapshots from metadata overhead and expiring files that are no longer needed.), and 'Orphan file deletion - new' (Automatically clean up orphan files periodically.).

- Tabellenoptimierung
 - Compaction – Datendateien werden zusammengeführt und neu geschrieben, um veraltete Daten zu entfernen und fragmentierte Daten in größeren, effizienteren Dateien zu konsolidieren.

- **Aufbewahrung von Snapshots:** Snapshots sind Versionen einer Iceberg-Tabelle mit Zeitstempel. Mit Konfigurationen zur Beibehaltung von Snapshots können Kunden festlegen, wie lange und wie viele Snapshots beibehalten werden sollen. Die Konfiguration eines Optimierers zur Aufbewahrung von Snapshots kann helfen, den Speicheraufwand zu minimieren, indem ältere, unnötige Snapshots und die zugehörigen zugrunde liegenden Dateien entfernt werden.
- **Löschen verwaister Dateien:** Verwaiste Dateien sind Dateien, auf die in den Metadaten der Iceberg-Tabelle nicht mehr verwiesen wird. Diese Dateien können sich im Laufe der Zeit ansammeln, insbesondere nach Vorgängen wie dem Löschen von Tabellen oder fehlgeschlagenen ETL-Aufträgen. Wenn Sie das Löschen verwaister Dateien aktivieren AWS Glue , können Sie diese unnötigen Dateien regelmäßig identifizieren und entfernen, wodurch Speicherplatz frei wird.

Weitere Informationen finden Sie unter [Optimieren von Iceberg-Tabellen](#).

- **IAM-Rolle:** Um die Komprimierung auszuführen, übernimmt der Dienst in Ihrem Namen eine IAM-Rolle. Sie können über das Dropdown-Menü eine IAM-Rolle auswählen. Die Rolle sollte die erforderlichen Berechtigungen für die Verdichtung haben.

Weitere Informationen zu den erforderlichen Berechtigungen finden Sie unter Voraussetzungen für die [Tabellenoptimierung](#).

- **Speicherort:** Geben Sie den Pfad zu dem Ordner in Amazon S3 an, in dem die Metadatentabelle gespeichert ist. Iceberg benötigt eine Metadatendatei und einen Speicherort im Data Catalog, um Lese- und Schreibvorgänge durchführen zu können.
- **Schema:** Wählen Sie Spalten hinzufügen, um Spalten und Datentypen der Spalten hinzuzufügen. Sie haben die Möglichkeit, eine leere Tabelle zu erstellen und das Schema später zu aktualisieren. Data Catalog unterstützt Hive-Datentypen. Weitere Informationen finden Sie unter [Datentypen](#).

Mit Iceberg können Sie Schema und Partition weiterentwickeln, nachdem Sie die Tabelle erstellt haben. Sie können [Athena-Abfragen](#) verwenden, um das Tabellenschema zu aktualisieren, und [Spark-Abfragen](#), um Partitionen zu aktualisieren.

AWS CLI

```
aws glue create-table \  
  --database-name iceberg-db \  
  --region us-west-2 \  
  --table-name <table-name>
```



```
--open-table-format-input '{
  "IcebergInput": {
    "MetadataOperation": "CREATE",
    "Version": "2"
  }
}' \
--table-input '{"Name":"test-iceberg-input-demo",
  "TableType": "EXTERNAL_TABLE",
  "StorageDescriptor":{
    "Columns":[
      {"Name":"col1", "Type":"int"},
      {"Name":"col2", "Type":"int"},
      {"Name":"col3", "Type":"string"}
    ],
    "Location":"s3://DOC_EXAMPLE_BUCKET_ICEBERG/"
  }
}'
```

Optimieren von Iceberg-Tabellen

Lake Formation unterstützt mehrere Optionen zur Tabellenoptimierung, um die Verwaltung und Leistung von Apache Iceberg-Tabellen zu verbessern, die von den AWS Analyse-Engines und ETL-Jobs verwendet werden. Diese Optimierer sorgen für eine effiziente Speichernutzung, eine verbesserte Abfrageleistung und ein effektives Datenmanagement. In Lake Formation sind drei Arten von Tabellenoptimierern verfügbar:

- **Komprimierung:** Bei der Datenkomprimierung werden kleine Datendateien komprimiert, um den Speicherverbrauch zu reduzieren und die Leseleistung zu verbessern. Datendateien werden zusammengeführt und neu geschrieben, um veraltete Daten zu entfernen und fragmentierte Daten in größeren, effizienteren Dateien zu konsolidieren. Die Komprimierung kann so konfiguriert werden, dass sie bei Bedarf automatisch oder manuell ausgelöst wird.
- **Aufbewahrung von Snapshots:** Snapshots sind Versionen einer Iceberg-Tabelle mit Zeitstempel. Mit Konfigurationen zur Beibehaltung von Snapshots können Kunden festlegen, wie lange und wie viele Snapshots beibehalten werden sollen. Die Konfiguration eines Optimierers zur Aufbewahrung von Snapshots kann helfen, den Speicheraufwand zu minimieren, indem ältere, unnötige Snapshots und die zugehörigen zugrunde liegenden Dateien entfernt werden.
- **Löschen verwaister Dateien:** Verwaiste Dateien sind Dateien, auf die in den Metadaten der Iceberg-Tabelle nicht mehr verwiesen wird. Diese Dateien können sich im Laufe der Zeit

ansammeln, insbesondere nach Vorgängen wie dem Löschen von Tabellen oder fehlgeschlagenen ETL-Aufträgen. Wenn Sie das Löschen verwaister Dateien aktivieren AWS Glue , können Sie diese überflüssigen Dateien regelmäßig identifizieren und entfernen, wodurch Speicherplatz frei wird.

Sie können die Optimierer für die Komprimierung, die Aufbewahrung von Snapshots und das Löschen verwaister Dateien für einzelne Iceberg-Tabellen im Datenkatalog mithilfe der AWS Glue Konsole oder API-Operationen aktivieren oder deaktivieren. AWS CLI AWS Glue

Weitere Informationen finden Sie unter [Optimieren von Iceberg-Tabellen](#) im Entwicklerhandbuch. AWS Glue

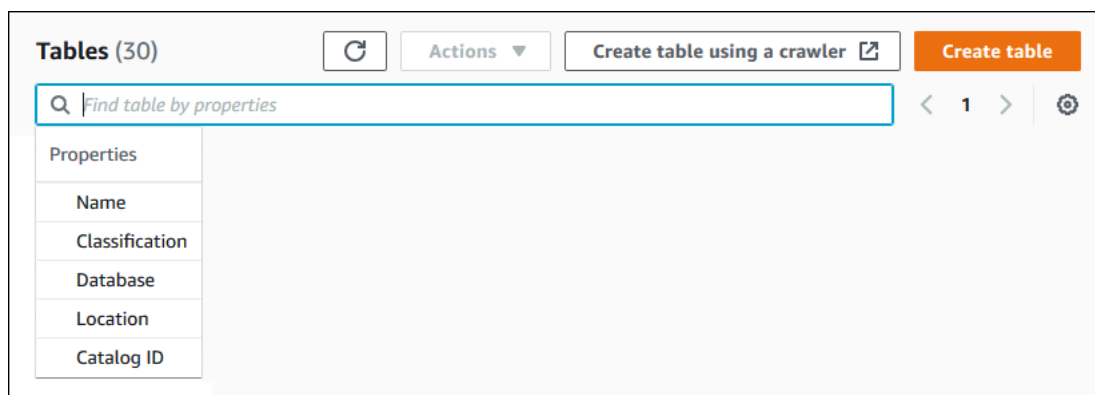
Nach Tabellen suchen

Sie können die AWS Lake Formation Konsole verwenden, um nach Datenkatalogtabellen nach Namen, Speicherort, enthaltender Datenbank und mehr zu suchen. In den Suchergebnissen werden nur die Tabellen angezeigt, für die Sie Lake Formation Formation-Berechtigungen haben.

Um nach Tabellen zu suchen (Konsole)

1. Melden Sie sich bei der an AWS-Managementkonsole und öffnen Sie die Lake Formation Formation-Konsole unter <https://console.aws.amazon.com/lakeformation/>.
2. Wählen Sie im Navigationsbereich Tables (Tabellen) aus.
3. Positionieren Sie den Cursor im Suchfeld oben auf der Seite. Das Feld hat den Platzhaltertext Tabelle anhand von Eigenschaften suchen.

Das Eigenschaftenmenü mit den verschiedenen Tabelleneigenschaften, nach denen gesucht werden kann, wird angezeigt.



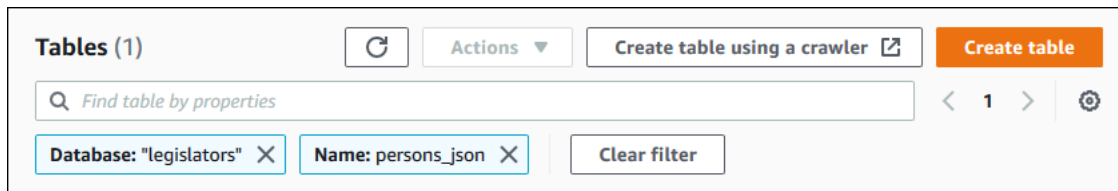
4. Führen Sie eine der folgenden Aktionen aus:

- Suchen Sie nach der enthaltenen Datenbank.
 1. Wählen Sie im Menü Eigenschaften die Option Datenbank und wählen Sie dann entweder eine Datenbank aus dem angezeigten Menü Datenbanken aus, oder geben Sie einen Datenbanknamen ein und drücken Sie die Eingabetaste.

Die Tabellen, für die Sie in der Datenbank berechtigt sind, werden aufgelistet.

2. (Optional) Um die Liste auf eine einzige Tabelle in der Datenbank einzuschränken, positionieren Sie den Cursor erneut im Suchfeld, wählen Sie Name aus dem Eigenschaftenmenü und wählen entweder einen Tabellennamen aus dem angezeigten Menü Tabellen aus, oder geben Sie einen Tabellennamen ein und drücken Sie die Eingabetaste.

Die einzelne Tabelle wird aufgelistet, und sowohl der Datenbankname als auch der Tabellename werden als Kacheln unter dem Suchfeld angezeigt.



Um den Filter anzupassen, schließen Sie eine der Kacheln oder wählen Sie Filter löschen.

- Suchen Sie nach anderen Eigenschaften.
 1. Wählen Sie im Eigenschaften-Menü eine Sucheigenschaft aus.

Um nach der AWS Konto-ID zu suchen, wählen Sie im Menü „Eigenschaften“ die Option „Katalog-ID“, geben Sie eine gültige AWS Konto-ID ein (z. B. 111122223333) und drücken Sie die Eingabetaste.

Um nach Standort zu suchen, wählen Sie im Menü „Eigenschaften“ die Option „Standort“ und anschließend im daraufhin angezeigten Menü „Standorte“ einen Standort aus. Alle Tabellen im Stammverzeichnis des ausgewählten Speicherorts (z. B. Amazon S3) werden zurückgegeben.

Suchen nach Tabellen mit AWS CLI

- Das folgende Beispiel zeigt, wie eine Teilsuche ausgeführt wird. Mit dem `--search-text` Parameter können Sie nach Tabellen suchen, die den angegebenen Text in ihren Metadaten

enthalten. In diesem Fall werden alle Tabellen zurückgegeben, deren Name, Beschreibung oder andere Metadatenfelder das Wort „Kunde“ enthalten.

```
aws glue search-tables
  --search-text "customer"
  --region AWS-Region
  --max-results 10
  --sort-criteria "FieldName=Name,Sort=ASC"
```

Gemeinsame Nutzung von Datenkatalogtabellen und Datenbanken für mehrere AWS Konten

Sie können Datenkatalogressourcen (Datenbanken und Tabellen) mit externen AWS Konten gemeinsam nutzen, indem Sie den externen Konten Lake Formation Berechtigungen für die Ressourcen gewähren. Benutzer können dann Abfragen und Jobs ausführen, die Tabellen mehrerer Konten verknüpfen und abfragen. Wenn Sie eine Datenkatalogressource mit einem anderen Konto gemeinsam nutzen, können Prinzipale in diesem Konto mit dieser Ressource arbeiten, als ob sich die Ressource in ihrem Datenkatalog befände.

Sie teilen Ressourcen nicht mit bestimmten Prinzipalen in externen AWS Konten — Sie teilen die Ressourcen mit einem Konto oder einer Organisation. Wenn Sie eine Ressource mit einer AWS Organisation teilen, teilen Sie die Ressource mit allen Konten auf allen Ebenen in dieser Organisation. Der Data Lake-Administrator in jedem externen Konto muss dann den Prinzipalen in ihrem Konto Berechtigungen für die gemeinsam genutzten Ressourcen gewähren.

Weitere Informationen erhalten Sie unter [Kontoübergreifender Datenaustausch in Lake Formation](#) und [Erteilen von Berechtigungen für Datenkatalogressourcen](#).

 Weitere Informationen finden Sie auch unter:

- [Zugreifen auf und Anzeigen von gemeinsam genutzten Datenkatalogtabellen und Datenbanken](#)
- [Voraussetzungen](#)

AWS Glue Data Catalog Ansichten von Gebäuden

In der ist eine Ansicht eine virtuelle Tabelle AWS Glue Data Catalog, deren Inhalt durch eine SQL-Abfrage definiert wird, die auf eine oder mehrere Tabellen verweist. Sie können mithilfe von SQL-Editoren für Amazon Athena, Amazon Redshift oder Apache Spark mit EMR Serverless oder Version 5.0 eine Datenkatalogansicht erstellen, die auf bis zu 10 Tabellen verweist. AWS Glue Die einer Ansicht zugrunde liegenden Referenztabellen können zu derselben Datenbank oder zu verschiedenen Datenbanken innerhalb desselben AWS-Konto Datenkatalogs gehören.

Sie können auf AWS Glue Standardtabellen und Tabellen in offenen Tabellenformaten (OTF) wie [Apache Hudi](#), Linux Foundation [Delta Lake](#) und [Apache Iceberg](#) verweisen, wobei die zugrunde liegenden Daten an Amazon S3 S3-Speicherorten gespeichert sind, bei denen Sie registriert sind. AWS Lake Formation Darüber hinaus können Sie Ansichten aus Verbundtabellen aus Amazon Redshift-Datenfreigaben erstellen, die mit Lake Formation gemeinsam genutzt werden.

Differenzierung von Datenkatalogansichten von anderen Ansichtstypen

Datenkatalogansichten unterscheiden sich von Apache Hive-, Apache Spark- und Amazon Athena Athena-Ansichten. Die Datenkatalogansicht ist eine systemeigene Funktion von und ist eine vom AWS Glue Data Catalog Definierer erstellte Ansicht mit mehreren Dialekten. Sie können eine Datenkatalogansicht mit einem der unterstützten Analysedienste wie Athena oder Amazon Redshift Spectrum erstellen und mit anderen unterstützten Analysediensten auf dieselbe Ansicht zugreifen. Andererseits werden die Ansichten Apache Hive, Apache Spark und Athena unabhängig voneinander in jedem Analytics-Service wie Athena und Amazon Redshift erstellt und sind nur innerhalb dieses Dienstes sichtbar und zugänglich.

Was ist eine definere Ansicht?

Eine Definer-Ansicht ist eine SQL-Ansicht, die auf den Berechtigungen des Prinzipals basiert, der sie erstellt hat. Die Definiererrolle verfügt über die erforderlichen Berechtigungen für den Zugriff auf die referenzierten Tabellen und führt die SQL-Anweisung aus, die die Ansicht definiert. Der Definierer erstellt die Ansicht und gibt sie mithilfe AWS Lake Formation seiner detaillierten Zugriffskontrolle für andere Benutzer frei.

Wenn ein Benutzer die Definer-Ansicht abfragt, verwendet die Abfrage-Engine die Berechtigungen der Definer-Rolle, um auf die zugrunde liegenden Referenztabellen zuzugreifen. Dieser Ansatz ermöglicht es Benutzern, mit der Ansicht zu interagieren, ohne direkten Zugriff auf die Quelltabellen zu benötigen, wodurch die Sicherheit erhöht und die Datenzugriffsverwaltung vereinfacht wird.

Um eine Definer-Ansicht einzurichten, kann sich die Definer-IAM-Rolle innerhalb desselben AWS Kontos wie die Basistabellen oder in einem anderen Konto befinden, wobei kontoübergreifende Definerrollen verwendet werden. Weitere Informationen zu den für die Definerrolle erforderlichen Berechtigungen finden Sie unter [Voraussetzungen für das Erstellen von Ansichten](#)

Ein Framework für Ansichten mit mehreren Dialekten

Der Datenkatalog unterstützt die Erstellung von Ansichten mit mehreren SQL-Dialekten (Structured Query Language). SQL ist eine Sprache, die zum Speichern und Verarbeiten von Informationen in einer relationalen Datenbank verwendet wird, und jede AWS Analyse-Engine verwendet ihre eigene Variante von SQL oder ihren eigenen SQL-Dialekt.

Sie erstellen eine Datenkatalogsicht in einem SQL-Dialekt mit einer der unterstützten Analytics-Abfrage-Engines. Anschließend können Sie die Ansicht aktualisieren, indem Sie die `ALTER VIEW` Anweisung in einem anderen SQL-Dialekt in jeder anderen unterstützten Analyse-Engine verwenden. Jeder Dialekt muss jedoch auf denselben Satz von Tabellen, Spalten und Datentypen verweisen.

Sie können über die `GetTable` API und die Konsole auf die verschiedenen Dialekte zugreifen, AWS CLI die für die Ansicht verfügbar sind. AWS Somit ist die Datenkatalogansicht sichtbar und kann über verschiedene unterstützte Analyse-Engines abgefragt werden.

Durch die Definition eines gemeinsamen Ansichtsschemas und eines Metadatenobjekts, das Sie von mehreren Engines abfragen können, ermöglichen Ihnen Datenkatalogansichten die Verwendung einheitlicher Ansichten für Ihren gesamten Data Lake.

Weitere Informationen darüber, wie das Schema für jeden Dialekt aufgelöst wird, finden Sie unter [dem Link zur API-Referenz](#). Weitere Informationen zu den Abgleichsregeln für verschiedene Typen finden Sie unter [dem Link zum entsprechenden Abschnitt im API-Dokument](#).

Integration mit Lake Formation Formation-Berechtigungen

Sie können AWS Lake Formation verwenden, um die Berechtigungsverwaltung für AWS Glue Data Catalog Benutzeransichten zu zentralisieren. Sie können mithilfe der Methode für benannte Ressourcen oder mithilfe von LF-Tags detaillierte Berechtigungen für die Datenkatalogansichten gewähren und diese für AWS Organisationen und Organisationseinheiten AWS-Konten gemeinsam nutzen. Sie können die AWS-Regionen Datenkatalogansichten auch mithilfe von Ressourcenlinks gemeinsam nutzen und darauf zugreifen. Auf diese Weise können Benutzer auf Daten zugreifen, ohne die Datenquelle duplizieren und die zugrunde liegenden Tabellen gemeinsam nutzen zu müssen.

Die CREATE VIEW DDL-Anweisung einer Datenkatalogsicht kann auf die AWS Glue Standardtabellen und Tabellen in offenen Tabellenformaten (OTF) wie Hudi, Delta Lake und Iceberg verweisen, wobei die zugrunde liegenden Daten in Amazon S3 S3-Standorten gespeichert sind, die bei Lake Formation registriert sind, sowie auf die Verbundtabellen aus Amazon Redshift Datashare, die mit Lake Formation gemeinsam genutzt werden, gespeichert sind. Die Tabellen können ein beliebiges Dateiformat haben, sofern die Engine, mit der die Ansicht abgefragt wurde, dieses Format unterstützt. Sie können auch auf integrierte Funktionen der Engine verweisen, auf der sie ausgeführt wird. Andere modulspezifische Ressourcen sind jedoch möglicherweise nicht zulässig. Weitere Details finden Sie unter [Überlegungen und Einschränkungen im Datenkatalog](#).

Anwendungsfälle

Im Folgenden sind die wichtigen Anwendungsfälle für Datenkatalog-Ansichten aufgeführt:

- Erstellen und verwalten Sie Berechtigungen für ein einzelnes Ansichtsschema. Auf diese Weise können Sie das Risiko inkonsistenter Berechtigungen für doppelte Ansichten vermeiden, die in mehreren Engines erstellt wurden.
- Erteilen Sie Benutzern Berechtigungen für eine Ansicht, die auf mehrere Tabellen verweist, ohne Berechtigungen direkt für die zugrunde liegenden Referenztabellen zu gewähren.
- Filtern Sie Tabellen auf Zeilenebene mithilfe von LF-Tags (wobei LF-Tags nur bis zur Spaltenebene kaskadiert werden), indem Sie LF-Tags auf Ansichten anwenden und Benutzern auf LF-Tags basierende Berechtigungen gewähren.

Unterstützte Analysedienste für Ansichten AWS

Die folgenden AWS Analysedienste unterstützen die Erstellung von Datenkatalogansichten:

- Amazon Redshift
- Amazon Athena versie 3
- Apache Spark auf EMR Serverless
- Apache Spark auf Version 5.0 AWS Glue

Weitere Ressourcen

In diesem Handbuch erfahren Sie mehr über den Datenkatalog und nutzen die folgenden Ressourcen:

Das folgende Video zeigt, wie Ansichten von Athena und Amazon Redshift erstellt und abgefragt werden.

Themen

- [Voraussetzungen für das Erstellen von Ansichten](#)
- [Datenkatalogsichten mithilfe von DDL-Anweisungen erstellen](#)
- [Datenkatalogsichten erstellen mit AWS Glue APIs](#)
- [Erteilen von Berechtigungen für Datenkatalog-Ansichten](#)
- [Materialisierte Ansichten](#)

Voraussetzungen für das Erstellen von Ansichten

- Um Ansichten in Data Catalog zu erstellen, müssen Sie die zugrunde liegenden Amazon S3 S3-Datenspeicherorte der Referenztabellen bei Lake Formation registrieren. Einzelheiten zur Registrierung von Daten bei Lake Formation finden Sie unter [Hinzufügen eines Amazon S3 S3-Standorts zu Ihrem Data Lake](#).
- Nur IAM-Rollen können Datenkatalogansichten erstellen. Andere IAM-Identitäten können keine Datenkatalogsichten erstellen.
- Die IAM-Rolle, die die Ansicht definiert, muss über die folgenden Berechtigungen verfügen:
 - Lake Formation SELECT Formation-Genehmigung mit der `Grantable` Option für alle Referenztabellen, einschließlich aller Spalten.
 - Lake Formation `CREATE_TABLE` Formation-Berechtigung für die Zieldatenbank, in der Ansichten erstellt werden.
 - Eine Vertrauenspolitik, damit die Lake Formation und ihre AWS Glue Dienste die Rolle übernehmen.

JSON

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Sid": "DataCatalogViewDefinerAssumeRole1",
      "Effect": "Allow",
      "Principal": {
        "Service": [
          "glue.amazonaws.com",
```



```

        "lakeformation.amazonaws.com"
    ]
},
    "Action": "sts:AssumeRole"
}
]
}

```

- Das Ziel: PassRole Genehmigung für AWS Glue und Lake Formation.

JSON

```

{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Sid": "DataCatalogViewDefinerPassRole1",
      "Action": [
        "iam:PassRole"
      ],
      "Effect": "Allow",
      "Resource": "*",
      "Condition": {
        "StringEquals": {
          "iam:PassedToService": [
            "glue.amazonaws.com",
            "lakeformation.amazonaws.com"
          ]
        }
      }
    }
  ]
}

```

- AWS Glue und Genehmigungen für Lake Formation.

JSON

```

{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",

```

```

        "Action": [
            "Glue:GetDatabase",
            "Glue:GetDatabases",
            "Glue:CreateTable",
            "Glue:GetTable",
            "Glue:GetTables",
            "Glue:BatchGetPartition",
            "Glue:GetPartitions",
            "Glue:GetPartition",
            "Glue:GetTableVersion",
            "Glue:GetTableVersions",
            "Glue:PassConnection",
            "lakeFormation:GetDataAccess"
        ],
        "Resource": "*"
    }
}

```

- Sie können keine Ansichten in einer Datenbank erstellen, für die der IAMAllowedPrincipals Gruppe ALL Berechtigungen erteilt wurden. Super Sie können entweder der IAMAllowedPrincipals Gruppe die Super Berechtigung für eine Datenbank entziehen, sie einsehen oder eine neue Datenbank erstellen [Schritt 4: Stellen Sie Ihre Datenspeicher auf das Lake Formation Formation-Berechtigungsmodell um](#), wobei das Kontrollkästchen Nur IAM-Zugriffssteuerung für neue Tabellen in dieser Datenbank verwenden unter Standardberechtigungen für neu erstellte Tabellen deaktiviert ist.

Datenkatalogsichten mithilfe von DDL-Anweisungen erstellen

Sie können AWS Glue Data Catalog Ansichten mit SQL-Editoren für Athena, Amazon Redshift und mit dem AWS Glue APIs/erstellen.AWS CLI

Um eine Datenkatalogsicht mit SQL-Editoren zu erstellen, wählen Sie Athena oder Redshift Spectrum und erstellen Sie die Ansicht mit einer DDL-Anweisung (CREATE VIEWData Definition Language). Nachdem Sie eine Ansicht im Dialekt der ersten Engine erstellt haben, können Sie eine ALTER VIEW DDL-Anweisung der zweiten Engine verwenden, um die zusätzlichen Dialekte hinzuzufügen.

Bei der Definition von Ansichten ist es wichtig, Folgendes zu berücksichtigen:

- Definition von Ansichten mit mehreren Dialekten — Wenn Sie eine Ansicht mit mehreren Dialekten definieren, müssen die Schemas der verschiedenen Dialekte übereinstimmen. Jeder SQL-Dialekt

hat eine etwas andere Syntaxspezifikation. Die Abfragesyntax, die die Datenkatalogansicht definiert, sollte in allen Dialekten exakt dieselbe Spaltenliste, einschließlich Typen und Namen, ergeben. Diese Informationen werden in `StorageDescriptor` der Ansicht gespeichert. Die Dialekte müssen auch auf dieselben zugrunde liegenden Tabellenobjekte aus dem Datenkatalog verweisen.

Um einer Ansicht mithilfe von DDL einen weiteren Dialekt hinzuzufügen, können Sie die Anweisung verwenden. `ALTER VIEW` Wenn eine `ALTER VIEW` Anweisung versucht, die Sichtdefinition zu aktualisieren, z. B. den Speicherdeskriptor oder die zugrunde liegenden Tabellen der Ansicht zu ändern, gibt die Anweisung einen Fehler mit der Meldung „Eingabe und vorhandener Speicherdeskriptor stimmen nicht überein“. Sie können SQL-Cast-Operationen verwenden, um sicherzustellen, dass die Typen der View-Spalten übereinstimmen.

- Eine Ansicht aktualisieren — Um die Ansicht zu aktualisieren, können Sie die `UpdateTable` API verwenden. Wenn Sie die Ansicht aktualisieren, ohne dass die Speicherdeskriptoren oder die Referenztabelle übereinstimmen, können Sie das `FORCE` Flag angeben (die Syntax finden Sie in der Engine-SQL-Dokumentation). Nach einer erzwungenen Aktualisierung übernimmt die Ansicht die erzwungenen Tabellen `StorageDescriptor` und die Referenztabelle. Jede weitere `ALTER VIEW` DDL sollte den geänderten Werten entsprechen. Eine Ansicht, die aktualisiert wurde, sodass sie inkompatible Dialekte enthält, erhält den Status „Veraltet“. Der Status der Ansicht ist in der Lake Formation Konsole und bei Verwendung der `GetTable` Operation sichtbar.
- Auf einen Varchar-Spalten Typ als Zeichenfolge verweisen — Es ist nicht möglich, einen Varchar-Spalten Typ von Redshift Spectrum in eine Zeichenfolge umzuwandeln. Wenn in Redshift Spectrum eine Ansicht mit einem Varchar-Spalten Typ erstellt wird und ein nachfolgender Dialekt versucht, auf dieses Feld als Zeichenfolge zu verweisen, behandelt der Datenkatalog es als Zeichenfolge, ohne dass das Flag erforderlich ist. `FORCE`
- Behandlung komplexer Typfelder — Amazon Redshift behandelt alle komplexen Typen als [SUPER-Typen](#), während Athena den komplexen Typ spezifiziert. Wenn eine Ansicht über ein SUPER Typfeld verfügt und eine andere Engine diese Spalte als einen bestimmten komplexen Typ referenziert, z. B. `struct (<street_address:struct<street_number:int, street_name:string, street_type:string>>)`, geht der Datenkatalog davon aus, dass es sich bei dem Feld um einen spezifischen komplexen Typ handelt, und verwendet diesen im Speicherdeskriptor, ohne dass das Flag erforderlich ist. `Force`

Weitere Informationen zur Syntax für die Erstellung und Verwaltung von Datenkatalogsichten finden Sie unter:

- [Verwenden von AWS Glue Data Catalog Ansichten](#) im Amazon Athena Athena-Benutzerhandbuch.
- Die [Abfragesyntax für die Glue-Datenkatalogansicht](#) finden Sie im Amazon Athena Athena-Benutzerhandbuch.
- [Erstellen von Ansichten AWS Glue Data Catalog im](#) Amazon Redshift Database Developer Guide.

Weitere Informationen zu den SQL-Befehlen für Ansichten im Datenkatalog finden Sie unter [CREATE EXTERNAL VIEW](#), [ALTER EXTERNAL VIEW](#) und [DROP EXTERNAL VIEW](#).

Nachdem Sie eine Datenkatalog-Ansicht erstellt haben, sind die Details der Ansicht in der Lake Formation Formation-Konsole verfügbar.

1. Wählen Sie in der Lake Formation Formation-Konsole unter Datenkatalog die Option Ansichten aus.
2. Eine Liste der verfügbaren Ansichten wird auf der Seite „Ansichten“ angezeigt.
3. Wählen Sie eine Ansicht aus der Liste aus und auf der Detailseite werden die Attribute der Ansicht angezeigt.

[AWS Lake Formation](#) > [Views](#) > europe_players

europe_players

Version 1 (Current version) ▾ Actions ▾

Details

Name europe_players	Database views_demo_database	Definer role admin
Last updated November 22, 2023 at 10:41 PM UTC	Status Ready	Description -

Schema

[SQL definitions](#)

LF-Tags

Cross-account access

Underlying tables

SQL definitions (2)

Add SQL definition ▾

List of available SQL definitions in different engines. Choose an engine from the list to add or edit the definition.

Find engine

< 1 >

Engine name ▲	Version ▼	Status ▼	SQL statement	Edit definition
Athena	3	Ready	View	Amazon Athena
Redshift	1.0	Ready	View	Amazon Redshift

Schema

Wählen Sie eine Column Zeile aus und wählen Sie LF-Tags bearbeiten, um Tag-Werte zu aktualisieren oder neue LF-Tags zuzuweisen.

SQL-Definitionen

Sie können eine Liste der verfügbaren SQL-Definitionen sehen. Wählen Sie SQL-Definition hinzufügen und wählen Sie eine Abfrage-Engine aus, um eine SQL-Definition hinzuzufügen. Wählen Sie unter der Edit definition Spalte eine Abfrage-Engine (Athena oder Amazon Redshift) aus, um eine SQL-Definition zu aktualisieren.

LF-Tags

Wählen Sie LF-Tags bearbeiten, um Werte für ein Tag zu bearbeiten oder neue Tags zuzuweisen. Sie können LF-Tags verwenden, um Berechtigungen für Ansichten zu erteilen.

Kontoübergreifender Zugriff

Sie können eine Liste der Organisationen und Organisationseinheiten (OUs) sehen AWS-Konten, für die Sie die Datenkatalogansicht freigegeben haben.

Zugrundeliegende Tabellen

Die zugrunde liegenden Tabellen, auf die in der SQL-Definition verwiesen wird, die zur Erstellung der Ansicht verwendet wurde, werden auf dieser Registerkarte angezeigt.

Datenkatalogsichten erstellen mit AWS Glue APIs

Sie können und verwenden AWS Glue [CreateTable](#), [UpdateTable](#) APIs um Ansichten im Datenkatalog zu erstellen und zu aktualisieren. Die UpdateTable Operationen CreateTable und haben eine neue TableInput Struktur fürViewDefinition,,SearchTables,GetTable, GetTablesGetTableVersion, GetTableVersions Operationen stellen die ViewDefinition Ausgabesyntax für Ansichten bereit. Darüber hinaus gibt es ein neues Status Feld in der GetTable API-Ausgabe.

Zwei neue AWS Glue Verbindungen sind für die Validierung des SQL-Dialekts für jede unterstützte Abfrage-Engine Amazon Athena und Amazon Redshift verfügbar.

Die CreateTable und UpdateTable APIs sind asynchron, wenn sie mit Ansichten verwendet werden. Wenn diese mit mehreren SQL-Dialekten aufgerufen APIs werden, wird der Aufruf mit jeder Engine überprüft, um festzustellen, ob der Dialekt auf dieser Engine ausgeführt werden kann und ob das resultierende Schema der Ansicht aus jedem Dialekt übereinstimmt. Der AWS Glue Dienst verwendet diese Verbindungen, um interne Aufrufe an die Analyse-Engines zu tätigen. Diese Aufrufe simulieren, was die Engine tut, um zu überprüfen, ob eine CREATE VIEW oder eine ALTER VIEW SQL-DDL auf der Engine ausgeführt wurde.

Wenn das bereitgestellte SQL gültig ist und die Schemas in den verschiedenen View-Dialekten übereinstimmen, schreibt die AWS Glue API das Ergebnis atomar fest. Atomicity ermöglicht das Erstellen oder Ändern von Ansichten mit mehreren Dialekten ohne Ausfallzeiten.

Themen

- [AWS Glue Verbindungen werden hergestellt, um den Status zu überprüfen](#)
- [Der Status der View-Generierung wird validiert](#)
- [Asynchrone Zustände und Operationen](#)
- [Sehen Sie sich Szenarien mit Fehlern bei der Erstellung bei asynchronen Vorgängen an](#)

AWS Glue Verbindungen werden hergestellt, um den Status zu überprüfen

Um eine AWS Glue Data Catalog Ansicht mithilfe der UpdateTable Operationen CreateTable oder zu erstellen oder zu aktualisieren, müssen Sie einen neuen AWS Glue Verbindungstyp für die Validierung erstellen und ihn der unterstützten Analytics-Engine zur Verfügung stellen. Diese Verbindungen sind erforderlich, um Datenkatalogansichten mit Athena oder Amazon Redshift zu verwenden. Sie können diese Verbindungen nur mit AWS CLI AWS SDKs, oder erstellen. AWS Glue APIs Sie können das nicht verwenden AWS-Managementkonsole , um die AWS Glue Verbindung herzustellen.

Note

Wenn die View Definer-Rolle und die Rolle, die CreateTable Or aufruft, unterschiedlich UpdateTable sind, benötigen beide in ihrer IAM-Richtlinienerklärung eine `glue:PassConnection` entsprechende Genehmigung.

Weitere Informationen finden Sie in der Dokumentation zum [Erstellen](#) AWS CLI einer Verbindung.

AWS CLI Befehl zum Erstellen einer Verbindung

Im Folgenden finden AWS CLI Sie einen Befehl zum Erstellen einer Verbindung:

```
aws glue create-connection --region us-east-1
--endpoint-url https://glue.us-east-1.amazonaws.com
--cli-input-json file:///root/path/to/create-connection.json
```

AWS CLI Eingabe JSON

Für Amazon Redshift:

```
{
  "CatalogId": "123456789012",
  "ConnectionInput": {
    "ConnectionType": "VIEW_VALIDATION_REDSHIFT",
    "Name": "views-preview-cluster-connection-2",
    "Description": "My first Amazon Redshift validation connection",
    "ConnectionProperties": {
      "DATABASE": "dev",
      "CLUSTER_IDENTIFIER": "glue-data-catalog-views-preview-cluster"
    }
  }
}
```

```
    }  
  }  
}
```

Für Amazon Athena:

```
{  
  "CatalogId": "123456789012",  
  "ConnectionInput": {  
    "ConnectionType": "VIEW_VALIDATION_ATHENA",  
    "Name": "views-preview-cluster-connection-3",  
    "Description": "My first Amazon Athena validation connection",  
    "ConnectionProperties": {  
      "WORKGROUP_NAME": "workgroup-name"  
    }  
  }  
}
```

Der Status der View-Generierung wird validiert

Wenn Sie die UpdateTable Operationen CreateTable oder ausführen, zeigt das Status Feld für die GetTable API-Ausgabe die Details zum Status der Ansichtserstellung an. Für create Anfragen, bei denen die Tabelle noch nicht existiert, AWS Glue wird für die Dauer des asynchronen Prozesses eine leere Tabelle erstellt. Beim Aufrufen GetTable können Sie ein optionales boolesches Flag übergeben `IncludeStatusDetails`, das Diagnoseinformationen zur Anfrage anzeigt. Im Falle eines Fehlers zeigt dieses Flag eine Fehlermeldung mit individuellen Status für jeden Dialekt an.

Fehler bei Vorgängen zum Erstellen, Lesen, Aktualisieren und Löschen von Ansichten (CRUD) können entweder während der Verarbeitung im AWS Glue/Lake Formation Service oder während der View-SQL-Validierung in Amazon Redshift oder Athena auftreten. Wenn bei der Validierung in einer Engine ein Fehler auftritt, gibt der AWS Glue Service die Fehlermeldung aus, die die Engine zurückgibt.

Statusfelder

Im Folgenden sind die Statusfelder aufgeführt:

- **Status:** ein allgemeiner Status, der unabhängig von verschiedenen Arten von Jobs ist:
 - IN_WARTESCHLANGE
 - IN_PROGRESS

- **ERFOLG**
- **FEHLGESCHLAGEN**
- **Aktion** — Gibt an, welche Aktion für die Tabelle aufgerufen wurde. Derzeit sind nur CREATE UPDATE Operationen verfügbar.

Bei der Arbeit mit Ansichten ist es wichtig, zwischen CREATE Operationen UPDATE und zu unterscheiden. Der Operationstyp bestimmt, wie Sie beim Abfragen der Tabellen vorgehen sollten.

Eine UPDATE Operation bedeutet, dass die Tabelle bereits im Datenkatalog vorhanden ist. In diesem Fall können Sie die zuvor erstellte Tabelle problemlos weiter abfragen. Andererseits zeigt eine CREATE Operation an, dass die Tabelle noch nie erfolgreich erstellt wurde. Wenn eine Tabelle als markiert ist CREATE, schlägt der Versuch, sie abzufragen, fehl, da die Tabelle noch nicht im System vorhanden ist. Daher ist es wichtig, den Operationstyp (UPDATE oder CREATE) zu identifizieren, bevor Sie versuchen, eine Tabelle abzufragen.

- **RequestedBy** — Der ARN des Benutzers, der die asynchrone Änderung angefordert hat.
- **UpdatedBy** — Der ARN des Benutzers, der den asynchronen Änderungsprozess zuletzt manuell geändert hat, z. B. eine Stornierung oder Änderung beantragt hat.
- **Fehler** — Dieses Feld wird nur angezeigt, wenn der Status FAILED lautet. Dies ist eine Ausnahmemeldung auf übergeordneter Ebene. Für jeden Dialekt können unterschiedliche Fehler auftreten.
 - **ErrorCode** — Die Art der Ausnahme.
 - **ErrorMessage** — eine kurze Beschreibung der Ausnahme.
- **RequestTime** — eine nach ISO 8601 formatierte Datumszeichenfolge, die den Zeitpunkt angibt, zu dem die Änderung initiiert wurde.
- **UpdateTime** — eine nach ISO 8601 formatierte Datumszeichenfolge, die den Zeitpunkt angibt, zu dem der Status zuletzt aktualisiert wurde.

Asynchrone Zustände und Operationen

Wenn Sie eine `glue:CreateTable` Anforderung ausführen, beginnt die asynchrone Erstellung der Datenkatalogansicht. In den folgenden Abschnitten beschreibt dieses Dokument die Status AWS Glue Ansicht, die in einer `glue:GetTable` Antwort verfügbar ist. Der Kürze halber wird in diesem Abschnitt die vollständige Antwort weggelassen.

```
{  
  "Table": {
```

```
    ...
    "Status": {
        ...
        "Action": "CREATE",
        "State": "QUEUED",
    }
}
```

Beide oben genannten Attribute stellen wichtige Diagnoseinformationen dar, die den Status des asynchronen Vorgangs sowie die Aktionen angeben, die in dieser Ansicht ausgeführt werden können. Im Folgenden sind die möglichen Werte aufgeführt, die diese Attribute annehmen können.

1. Status.Action

- a. CREATE
- b. UPDATE

2. Status.State

- a. IN_WARTESCHLANGE
- b. IN_PROGRESS
- c. ERFOLG
- d. FEHLGESCHLAGEN

Es ist auch wichtig zu beachten, dass einige Aktualisierungen in einer Datenkatalogansicht keinen asynchronen Vorgang erfordern. Beispielsweise möchte man vielleicht das `Description` Attribut der Tabelle aktualisieren. Da hierfür keine asynchronen Operationen erforderlich sind, werden die resultierenden Tabellenmetadaten keine `habenStatus`, und das Attribut schon. `NULL`

```
{
  "Table": {
    ...,
    "Description": "I changed this attribute!"
  }
}
```

Als Nächstes wird in diesem Thema untersucht, wie sich die obigen Statusinformationen auf Vorgänge auswirken können, die in einer AWS Glue Ansicht ausgeführt werden können.

Klebstoff: CreateTable

Für diese API gibt es keine Änderungen im Vergleich zu den `glue:CreateTable` Funktionen für jede Glue-Tabelle. `CreateTable` kann für jeden Tabellennamen aufgerufen werden, der noch nicht existiert.

kleben: UpdateTable

Dieser Vorgang kann nicht für eine AWS Glue Ansicht ausgeführt werden, die die folgenden Statusinformationen enthält:

1. Aktion == CREATE und Status == QUEUED
2. Aktion == CREATE und Status == IN_PROGRESS
3. Aktion == CREATE und Status == FAILED
4. Aktion == UPDATE und Status == QUEUED
5. Aktion == UPDATE und Status == IN_PROGRESS

Zusammenfassend lässt sich sagen, dass Sie eine Datenkatalogansicht nur aktualisieren können, wenn sie die folgenden Anforderungen erfüllt.

1. Sie wurde erfolgreich zum ersten Mal erstellt.
 - a. Aktion == CREATE und State == SUCCESS
2. Es hat nach einem asynchronen Aktualisierungsvorgang einen Terminalstatus erreicht.
 - a. Aktion == UPDATE und Status == ERFOLG
 - b. Aktion == UPDATE und Status == FEHLGESCHLAGEN
3. Es hat ein NULL State-Attribut als Ergebnis einer synchronen Aktualisierung.

kleben: DeleteTable

Bei dieser Operation gibt es keine Änderungen im Vergleich zu den `glue:DeleteTable` Funktionen für jede AWS Glue Tabelle. Sie können eine Datenkatalogansicht unabhängig von ihrem Status löschen.

kleben: GetTable

Bei dieser Operation gibt es keine Änderungen im Vergleich zu den `glue:GetTable` Funktionen für jede AWS Glue Tabelle. Sie können eine Datenkatalogansicht jedoch erst dann von den Analytical Engines abfragen, wenn sie erfolgreich zum ersten Mal erstellt wurde. `Action == CREATE` and

State == SUCCESS. Nachdem Sie eine Datenkatalogsicht zum ersten Mal erfolgreich erstellt haben, können Sie die Ansicht unabhängig von ihrem Status abfragen.

 Note

Alle Informationen in diesem Abschnitt gelten für alle gelesenen Tabellen APIs wie `GetTableGetTables`, und `SearchTables`.

Sehen Sie sich Szenarien mit Fehlern bei der Erstellung bei asynchronen Vorgängen an

Die folgenden Beispiele sind repräsentativ für die Arten von Fehlern, die aus API-Aufrufen `CreateTable` oder `UpdateTable` Anzeigen von API-Aufrufen resultieren können. Sie erheben keinen Anspruch auf Vollständigkeit, da die Fehleroberfläche von SQL-Abfragefehlern ziemlich groß ist.

Szenario 1: Fehler bei der Amazon Redshift Redshift-Abfrage

Die für Amazon Redshift bereitgestellte Abfrage enthält einen falsch geschriebenen Tabellennamen, der während der Überprüfung nicht im Datenkatalog gefunden wurde. Der daraus resultierende Fehler wird in dem Status Feld in der `GetTable` Antwort für die Ansicht angezeigt.

`GetTableAnfrage`:

```
{
  "CatalogId": "123456789012",
  "DatabaseName": "async-view-test-db",
  "TableInput": {
    "Name": "view-athena-redshift-72",
    "Description": "This is an atomic operation",
    "StorageDescriptor": {
      "Columns": [
        { "Name": "col1", "Type": "int" },
        { "Name": "col2", "Type": "string" },
        { "Name": "col3", "Type": "double" }
      ]
    },
    "ViewDefinition": {
      "Definer": "arn:aws:iam::123456789012:role/GDCViewDefiner",
      "SubObjects": [ "arn:aws:glue:us-east-1:123456789012:table/gdc-view-playground-db/table_1" ],

```

```

    "Representations": [
      {
        "Dialect": "ATHENA",
        "DialectVersion": "3",
        "ViewOriginalText": "SELECT * FROM \"gdc-view-playground-db\".
\"table_1\";",
        "ValidationConnection": "athena-connection"
      },
      {
        "Dialect": "REDSHIFT",
        "DialectVersion": "1.0",
        "ViewOriginalText": "SELECT * FROM \"gdc-view-playground-external-
schema\".\"table__1\";",
        "ValidationConnection": "redshift-connection"
      }
    ]
  }
}

```

GetTableAntwort:

```

IncludeStatusDetails = FALSE
{
  "Table": {
    "Name": "view-athena-redshift-72",
    "DatabaseName": "async-view-test-db",
    "Description": "",
    "CreateTime": "2024-07-11T11:39:19-07:00",
    "UpdateTime": "2024-07-11T11:39:19-07:00",
    "Retention": 0,
    "ViewOriginalText": "",
    "ViewExpandedText": "",
    "TableType": "",
    "CreatedBy": "arn:aws:iam::123456789012:user/zcaisse",
    "IsRegisteredWithLakeFormation": false,
    "CatalogId": "123456789012",
    "IsRowFilteringEnabled": false,
    "VersionId": "-1",
    "DatabaseId": "<databaseID>",
    "IsMultiDialectView": false,
    "Status": {
      "RequestedBy": "arn:aws:iam::123456789012:user/zcaisse",

```

```

        "UpdatedBy": "arn:aws:iam::123456789012:user/zcaisse",
        "RequestTime": "2024-07-11T11:39:19-07:00",
        "UpdateTime": "2024-07-11T11:40:06-07:00",
        "Action": "CREATE",
        "State": "FAILED"
    }
}

IncludeStatusDetails = TRUE
{
    "Table": {
        "Name": "view-athena-redshift-72",
        "DatabaseName": "async-view-test-db",
        "Description": "",
        "CreateTime": "2024-07-11T11:39:19-07:00",
        "UpdateTime": "2024-07-11T11:39:19-07:00",
        "Retention": 0,
        "ViewOriginalText": "",
        "ViewExpandedText": "",
        "TableType": "",
        "CreatedBy": "arn:aws:iam::123456789012:user/zcaisse",
        "IsRegisteredWithLakeFormation": false,
        "CatalogId": "123456789012",
        "IsRowFilteringEnabled": false,
        "VersionId": "-1",
        "DatabaseId": "<databaseID>",
        "IsMultiDialectView": false,
        "Status": {
            "RequestedBy": "arn:aws:iam::123456789012:user/zcaisse",
            "UpdatedBy": "arn:aws:iam::123456789012:user/zcaisse",
            "RequestTime": "2024-07-11T11:39:19-07:00",
            "UpdateTime": "2024-07-11T11:40:06-07:00",
            "Action": "CREATE",
            "State": "FAILED",
            "Error": {
                "ErrorCode": "QueryExecutionException",
                "ErrorMessage": "Error received during view SQL validation
using a connection: [Connection Name: redshift-connection | Query Execution
Id: ddb711d3-2415-4aa9-b251-6a76ab4f41b1 | Timestamp: Thu Jul 11 18:39:37 UTC
2024]: Redshift returned error for the statement: ERROR: AwsClientException:
EntityNotFoundException from glue - Entity Not Found"
            },
            "Details": {

```

```

    "RequestedChange": {
      "Name": "view-athena-redshift-72",
      "DatabaseName": "async-view-test-db",
      "Description": "This is an atomic operation",
      "Retention": 0,
      "StorageDescriptor": {
        "Columns": [
          {
            "Name": "col1",
            "Type": "int"
          },
          {
            "Name": "col2",
            "Type": "string"
          },
          {
            "Name": "col3",
            "Type": "double"
          }
        ],
        "Compressed": false,
        "NumberOfBuckets": 0,
        "SortColumns": [],
        "StoredAsSubDirectories": false
      },
      "TableType": "VIRTUAL_VIEW",
      "IsRegisteredWithLakeFormation": false,
      "CatalogId": "123456789012",
      "IsRowFilteringEnabled": false,
      "VersionId": "-1",
      "DatabaseId": "<databaseID>",
      "ViewDefinition": {
        "IsProtected": true,
        "Definer": "arn:aws:iam::123456789012:role/GDCViewDefiner",
        "SubObjects": [
          "arn:aws:glue:us-east-1:123456789012:table/gdc-view-
playground-db/table_1"
        ],
        "Representations": [
          {
            "Dialect": "ATHENA",
            "DialectVersion": "3",
            "ViewOriginalText": "SELECT * FROM \"gdc-view-
playground-db\".\"table_1\"",

```

```

        "IsStale": false
      },
      {
        "Dialect": "REDSHIFT",
        "DialectVersion": "1.0",
        "ViewOriginalText": "SELECT * FROM \"gdc-view-playground-external-schema\".\"table__1\";",
        "IsStale": false
      }
    ]
  },
  "IsMultiDialectView": true
},
"ViewValidations": [
  {
    "Dialect": "ATHENA",
    "DialectVersion": "3",
    "ViewValidationText": "SELECT * FROM \"gdc-view-playground-db\".\"table_1\"",
    "UpdateTime": "2024-07-11T11:40:06-07:00",
    "State": "SUCCESS"
  },
  {
    "Dialect": "REDSHIFT",
    "DialectVersion": "1.0",
    "ViewValidationText": "SELECT * FROM \"gdc-view-playground-external-schema\".\"table__1\";",
    "UpdateTime": "2024-07-11T11:39:37-07:00",
    "State": "FAILED",
    "Error": {
      "ErrorCode": "QueryExecutionException",
      "ErrorMessage": "Error received during view SQL validation using a connection: [Connection Name: redshift-connection | Query Execution Id: ddb711d3-2415-4aa9-b251-6a76ab4f41b1 | Timestamp: Thu Jul 11 18:39:37 UTC 2024]: Redshift returned error for the statement: ERROR: AwsClientException: EntityNotFoundException from glue - Entity Not Found"
    }
  }
]
}
}
}

```


Szenario 2: Ungültige Amazon Redshift Redshift-Verbindung

Die Amazon Redshift Redshift-Verbindung im folgenden Beispiel ist fehlerhaft, da sie auf eine Amazon Redshift Redshift-Datenbank verweist, die auf dem angegebenen Endpunkt nicht vorhanden ist. cluster/serverless Amazon Redshift kann die Ansicht nicht validieren und das Status Feld in der GetTable Antwort zeigt den Fehler an ("State": "FAILED" von Amazon Redshift).

GetTableAnfrage:

```
{
  "CatalogId": "123456789012",
  "DatabaseName": "async-view-test-db",
  "TableInput": {
    "Name": "view-athena-redshift-73",
    "Description": "This is an atomic operation",
    "StorageDescriptor": {
      "Columns": [
        { "Name": "col1", "Type": "int" },
        { "Name": "col2", "Type": "string" },
        { "Name": "col3", "Type": "double" }
      ]
    },
    "ViewDefinition": {
      "Definer": "arn:aws:iam::123456789012:role/GDCViewDefiner",
      "SubObjects": [ "arn:aws:glue:us-east-1:123456789012:table/gdc-view-playground-db/table_1" ],
      "Representations": [
        {
          "Dialect": "ATHENA",
          "DialectVersion": "3",
          "ViewOriginalText": "SELECT * FROM \"gdc-view-playground-db\".\"table_1\"",
          "ValidationConnection": "athena-connection"
        },
        {
          "Dialect": "REDSHIFT",
          "DialectVersion": "1.0",
          "ViewOriginalText": "SELECT * FROM \"gdc-view-playground-external-schema\".\"table_1\";",
          "ValidationConnection": "redshift-connection-malformed"
        }
      ]
    }
  }
}
```

```

    }
  }
}

```

GetTableAntwort:

```

IncludeStatusDetails = FALSE
{
  "Table": {
    "Name": "view-athena-redshift-73",
    "DatabaseName": "async-view-test-db",
    "Description": "",
    "CreateTime": "2024-07-11T11:43:27-07:00",
    "UpdateTime": "2024-07-11T11:43:27-07:00",
    "Retention": 0,
    "ViewOriginalText": "",
    "ViewExpandedText": "",
    "TableType": "",
    "CreatedBy": "arn:aws:iam::123456789012:user/zcaisse",
    "IsRegisteredWithLakeFormation": false,
    "CatalogId": "123456789012",
    "IsRowFilteringEnabled": false,
    "VersionId": "-1",
    "DatabaseId": "<databaseID>",
    "IsMultiDialectView": false,
    "Status": {
      "RequestedBy": "arn:aws:iam::123456789012:user/zcaisse",
      "UpdatedBy": "arn:aws:iam::123456789012:user/zcaisse",
      "RequestTime": "2024-07-11T11:43:27-07:00",
      "UpdateTime": "2024-07-11T11:43:40-07:00",
      "Action": "CREATE",
      "State": "FAILED"
    }
  }
}

IncludeStatusDetails = TRUE
{
  "Table": {
    "Name": "view-athena-redshift-73",
    "DatabaseName": "async-view-test-db",
    "Description": "",
    "CreateTime": "2024-07-11T11:43:27-07:00",
    "UpdateTime": "2024-07-11T11:43:27-07:00",

```

```

"Retention": 0,
"ViewOriginalText": "",
"ViewExpandedText": "",
"TableType": "",
"CreatedBy": "arn:aws:iam::123456789012:user/zcaisse",
"IsRegisteredWithLakeFormation": false,
"CatalogId": "123456789012",
"IsRowFilteringEnabled": false,
"VersionId": "-1",
"DatabaseId": "<databaseID>",
"IsMultiDialectView": false,
"Status": {
  "RequestedBy": "arn:aws:iam::123456789012:user/zcaisse",
  "UpdatedBy": "arn:aws:iam::123456789012:user/zcaisse",
  "RequestTime": "2024-07-11T11:43:27-07:00",
  "UpdateTime": "2024-07-11T11:43:40-07:00",
  "Action": "CREATE",
  "State": "FAILED",
  "Error": {
    "ErrorCode": "QueryExecutionException",
    "ErrorMessage": "Error received during view SQL validation using a
connection: [Connection Name: redshift-connection-malformed | Query Execution Id:
69bfafd4-3d51-4cb0-9320-7ce5404b1809 | Timestamp: Thu Jul 11 18:43:38 UTC 2024]:
Redshift returned error for the statement: FATAL: database \"devooo\" does not exist"
  },
  "Details": {
    "RequestedChange": {
      "Name": "view-athena-redshift-73",
      "DatabaseName": "async-view-test-db",
      "Description": "This is an atomic operation",
      "Retention": 0,
      "StorageDescriptor": {
        "Columns": [
          {
            "Name": "col1",
            "Type": "int"
          },
          {
            "Name": "col2",
            "Type": "string"
          },
          {
            "Name": "col3",
            "Type": "double"
          }
        ]
      }
    }
  }
}

```

```

        }
    ],
    "Compressed": false,
    "NumberOfBuckets": 0,
    "SortColumns": [],
    "StoredAsSubDirectories": false
},
"TableType": "VIRTUAL_VIEW",
"IsRegisteredWithLakeFormation": false,
"CatalogId": "123456789012",
"IsRowFilteringEnabled": false,
"VersionId": "-1",
"DatabaseId": "<databaseID>",
"ViewDefinition": {
    "IsProtected": true,
    "Definer": "arn:aws:iam::123456789012:role/GDCViewDefiner",
    "SubObjects": [
        "arn:aws:glue:us-east-1:123456789012:table/gdc-view-
playground-db/table_1"
    ],
    "Representations": [
        {
            "Dialect": "ATHENA",
            "DialectVersion": "3",
            "ViewOriginalText": "SELECT * FROM \"gdc-view-
playground-db\".\"table_1\"",
            "IsStale": false
        },
        {
            "Dialect": "REDSHIFT",
            "DialectVersion": "1.0",
            "ViewOriginalText": "SELECT * FROM \"gdc-view-
playground-external-schema\".\"table_1\";",
            "IsStale": false
        }
    ]
},
"IsMultiDialectView": true
},
"ViewValidations": [
    {
        "Dialect": "ATHENA",
        "DialectVersion": "3",

```

```

        "ViewValidationText": "SELECT * FROM \"gdc-view-playground-db\n\".\n\"table_1\"",
        "UpdateTime": "2024-07-11T11:43:40-07:00",
        "State": "SUCCESS"
    },
    {
        "Dialect": "REDSHIFT",
        "DialectVersion": "1.0",
        "ViewValidationText": "SELECT * FROM \"gdc-view-playground-\nexternal-schema\"\n\"table_1\";",
        "UpdateTime": "2024-07-11T11:43:38-07:00",
        "State": "FAILED",
        "Error": {
            "ErrorCode": "QueryExecutionException",
            "ErrorMessage": "Error received during view SQL validation\nusing a connection: [Connection Name: redshift-connection-malformed | Query Execution\nId: 69bfafd4-3d51-4cb0-9320-7ce5404b1809 | Time\nstamp: Thu Jul 11 18:43:38 UTC 2024]: Redshift returned error for the statement: FATAL:\ndatabase \"devooo\" does not exist"
        }
    }
]
}
}
}
}

```

Szenario 3: Fehler bei der Athena-Abfrage

Die SQL für Athena hier ist ungültig, weil die Abfrage den Datenbanknamen falsch buchstabiert. Die Athena-Abfragevalidierung fängt dies ab und der daraus resultierende Fehler wird durch das Status Objekt in einem Aufruf angezeigt. GetTable

GetTableAnfrage:

```
{
  "CatalogId": "123456789012",
  "DatabaseName": "async-view-test-db",
  "TableInput": {
    "Name": "view-athena-redshift-70",
    "Description": "This is an atomic operation",

```

```

    "StorageDescriptor": {
      "Columns": [
        { "Name": "col1", "Type": "int" },
        { "Name": "col2", "Type": "string" },
        { "Name": "col3", "Type": "double" }
      ]
    },
    "ViewDefinition": {
      "Definer": "arn:aws:iam::123456789012:role/GDCViewDefiner",
      "SubObjects": [ "arn:aws:glue:us-east-1:123456789012:table/gdc-view-playground-db/table_1" ],
      "Representations": [
        {
          "Dialect": "ATHENA",
          "DialectVersion": "3",
          "ViewOriginalText": "SELECT * FROM \"gdc--view-playground-db\".\"table_1\"",
          "ValidationConnection": "athena-connection"
        },
        {
          "Dialect": "REDSHIFT",
          "DialectVersion": "1.0",
          "ViewOriginalText": "SELECT * FROM \"gdc-view-playground-external-schema\".\"table_1\";",
          "ValidationConnection": "redshift-connection"
        }
      ]
    }
  }
}

```

GetTableAntwort:

```

IncludeStatusDetails = FALSE
{
  "Table": {
    "Name": "view-athena-redshift-70",
    "DatabaseName": "async-view-test-db",
    "Description": "",
    "CreateTime": "2024-07-11T11:09:53-07:00",
    "UpdateTime": "2024-07-11T11:09:53-07:00",
    "Retention": 0,
    "ViewOriginalText": "",

```

```

    "ViewExpandedText": "",
    "TableType": "",
    "CreatedBy": "arn:aws:iam::123456789012:user/",
    "IsRegisteredWithLakeFormation": false,
    "CatalogId": "123456789012",
    "IsRowFilteringEnabled": false,
    "VersionId": "-1",
    "DatabaseId": "<databaseID>",
    "IsMultiDialectView": false,
    "Status": {
      "RequestedBy": "arn:aws:iam::123456789012:user/zcaisse",
      "UpdatedBy": "arn:aws:iam::123456789012:user/zcaisse",
      "RequestTime": "2024-07-11T11:09:54-07:00",
      "UpdateTime": "2024-07-11T11:10:41-07:00",
      "Action": "CREATE",
      "State": "FAILED",
    }
  }
}

```

IncludeStatusDetails = TRUE

```

{
  "Table": {
    "Name": "view-athena-redshift-70",
    "DatabaseName": "async-view-test-db",
    "Description": "",
    "CreateTime": "2024-07-11T11:09:53-07:00",
    "UpdateTime": "2024-07-11T11:09:53-07:00",
    "Retention": 0,
    "ViewOriginalText": "",
    "ViewExpandedText": "",
    "TableType": "",
    "CreatedBy": "arn:aws:iam::123456789012:user/zcaisse",
    "IsRegisteredWithLakeFormation": false,
    "CatalogId": "123456789012",
    "IsRowFilteringEnabled": false,
    "VersionId": "-1",
    "DatabaseId": "<databaseID>",
    "IsMultiDialectView": false,
    "Status": {
      "RequestedBy": "arn:aws:iam::123456789012:user/zcaisse",
      "UpdatedBy": "arn:aws:iam::123456789012:user/zcaisse",
      "RequestTime": "2024-07-11T11:09:54-07:00",
      "UpdateTime": "2024-07-11T11:10:41-07:00",
    }
  }
}

```

```

    "Action": "CREATE",
    "State": "FAILED",
    "Error": {
      "ErrorCode": "QueryExecutionException",
      "ErrorMessage": "Error received during view SQL validation using
a connection: [Connection Name: athena-connection | Query Execution Id: d9bb1e6d-
ce26-4b35-8276-8a199af966aa | Timestamp: Thu Jul 11 18:10:
41 UTC 2024]: Athena validation FAILED: {ErrorCategory: 2,ErrorType: 1301,Retryable:
false,ErrorMessage: line 1:118: Schema 'gdc--view-playground-db' does not exist}"
    },
    "Details": {
      "RequestedChange": {
        "Name": "view-athena-redshift-70",
        "DatabaseName": "async-view-test-db",
        "Description": "This is an atomic operation",
        "Retention": 0,
        "StorageDescriptor": {
          "Columns": [
            {
              "Name": "col1",
              "Type": "int"
            },
            {
              "Name": "col2",
              "Type": "string"
            },
            {
              "Name": "col3",
              "Type": "double"
            }
          ],
          "Compressed": false,
          "NumberOfBuckets": 0,
          "SortColumns": [],
          "StoredAsSubDirectories": false
        },
        "TableType": "VIRTUAL_VIEW",
        "IsRegisteredWithLakeFormation": false,
        "CatalogId": "123456789012",
        "IsRowFilteringEnabled": false,
        "VersionId": "-1",
        "DatabaseId": "<databaseID>",
        "ViewDefinition": {
          "IsProtected": true,

```



```

        "Definer": "arn:aws:iam::123456789012:role/GDCViewDefiner",
        "SubObjects": [
            "arn:aws:glue:us-east-1:123456789012:table/gdc-view-
playground-db/table_1"
        ],
        "Representations": [
            {
                "Dialect": "ATHENA",
                "DialectVersion": "3",
                "ViewOriginalText": "SELECT * FROM \"gdc--view-
playground-db\".\"table_1\"",
                "IsStale": false
            },
            {
                "Dialect": "REDSHIFT",
                "DialectVersion": "1.0",
                "ViewOriginalText": "SELECT * FROM \"gdc-view-
playground-external-schema\".\"table_1\";",
                "IsStale": false
            }
        ]
    },
    "IsMultiDialectView": true
},
"ViewValidations": [
    {
        "Dialect": "ATHENA",
        "DialectVersion": "3",
        "ViewValidationText": "SELECT * FROM \"gdc--view-playground-db
\".\"table_1\"",
        "UpdateTime": "2024-07-11T11:10:41-07:00",
        "State": "FAILED",
        "Error": {
            "ErrorCode": "QueryExecutionException",
            "ErrorMessage": "Error received during view SQL validation
using a connection: [Connection Name: athena-connection | Query Execution Id:
d9bb1e6d-ce26-4b35-8276-8a199af966aa | Timestamp: Thu J
ul 11 18:10:41 UTC 2024]: Athena validation FAILED: {ErrorCategory: 2,ErrorType:
1301,Retryable: false,ErrorMessage: line 1:118: Schema 'gdc--view-playground-db' does
not exist}"
        }
    },
    {
        "Dialect": "REDSHIFT",

```

```

        "DialectVersion": "1.0",
        "ViewValidationText": "SELECT * FROM \"gdc-view-playground-external-schema\".\"table_1\";",
        "UpdateTime": "2024-07-11T11:10:41-07:00",
        "State": "SUCCESS"
    }
}
}
}
}
}

```

Szenario 4: Die Speicherdeskriptoren stimmen nicht überein

Das für den Athena-Dialekt bereitgestellte SQL wählt col1 und, col2 während das SQL für Redshift nur selektiert. col1 Dies führt zu einem Fehler bei der Nichtübereinstimmung des Speicherdeskriptors.

GetTableAnfrage:

```

{
  "CatalogId": "123456789012",
  "DatabaseName": "async-view-test-db",
  "TableInput": {
    "Name": "view-athena-redshift-71",
    "Description": "This is an atomic operation",
    "StorageDescriptor": {
      "Columns": [
        { "Name": "col1", "Type": "int" },
        { "Name": "col2", "Type": "string" },
        { "Name": "col3", "Type": "double" }
      ]
    },
    "ViewDefinition": {
      "Definer": "arn:aws:iam::123456789012:role/GDCViewDefiner",
      "SubObjects": [ "arn:aws:glue:us-east-1:123456789012:table/gdc-view-playground-db/table_1" ],
      "Representations": [
        {
          "Dialect": "ATHENA",
          "DialectVersion": "3",
          "ViewOriginalText": "SELECT col1, col2 FROM \"gdc-view-playground-db\".\"table_1\"",

```

```

        "ValidationConnection": "athena-connection"
    },
    {
        "Dialect": "REDSHIFT",
        "DialectVersion": "1.0",
        "ViewOriginalText": "SELECT col1 FROM \"gdc-view-playground-external-schema\".\"table_1\";",
        "ValidationConnection": "redshift-connection"
    }
]
}
}
}
}

```

GetTableAntwort:

```
IncludeStatusDetails = FALSE
```

```

{
  "Table": {
    "Name": "view-athena-redshift-71",
    "DatabaseName": "async-view-test-db",
    "Description": "",
    "CreateTime": "2024-07-11T11:22:02-07:00",
    "UpdateTime": "2024-07-11T11:22:02-07:00",
    "Retention": 0,
    "ViewOriginalText": "",
    "ViewExpandedText": "",
    "TableType": "",
    "CreatedBy": "arn:aws:iam::123456789012:user/zcaisse",
    "IsRegisteredWithLakeFormation": false,
    "CatalogId": "123456789012",
    "IsRowFilteringEnabled": false,
    "VersionId": "-1",
    "DatabaseId": "<databaseID>",
    "IsMultiDialectView": false,
    "Status": {
      "RequestedBy": "arn:aws:iam::123456789012:user/zcaisse",
      "UpdatedBy": "arn:aws:iam::123456789012:user/zcaisse",
      "RequestTime": "2024-07-11T11:22:02-07:00",
      "UpdateTime": "2024-07-11T11:23:19-07:00",
      "Action": "CREATE",
      "State": "FAILED"
    }
  }
}

```

```

    }
  }
}

IncludeStatusDetails = TRUE

{
  "Table": {
    "Name": "view-athena-redshift-71",
    "DatabaseName": "async-view-test-db",
    "Description": "",
    "CreateTime": "2024-07-11T11:22:02-07:00",
    "UpdateTime": "2024-07-11T11:22:02-07:00",
    "Retention": 0,
    "ViewOriginalText": "",
    "ViewExpandedText": "",
    "TableType": "",
    "CreatedBy": "arn:aws:iam::123456789012:user/zcaisse",
    "IsRegisteredWithLakeFormation": false,
    "CatalogId": "123456789012",
    "IsRowFilteringEnabled": false,
    "VersionId": "-1",
    "DatabaseId": "<databaseID>",
    "IsMultiDialectView": false,
    "Status": {
      "RequestedBy": "arn:aws:iam::123456789012:user/zcaisse",
      "UpdatedBy": "arn:aws:iam::123456789012:user/zcaisse",
      "RequestTime": "2024-07-11T11:22:02-07:00",
      "UpdateTime": "2024-07-11T11:23:19-07:00",
      "Action": "CREATE",
      "State": "FAILED",
      "Error": {
        "ErrorCode": "InvalidInputException",
        "ErrorMessage": "Engine and existing storage descriptor mismatch"
      },
    },
    "Details": {
      "RequestedChange": {
        "Name": "view-athena-redshift-71",
        "DatabaseName": "async-view-test-db",
        "Description": "This is an atomic operation",
        "Retention": 0,
        "StorageDescriptor": {
          "Columns": [
            {

```

```

        "Name": "col1",
        "Type": "int"
    },
    {
        "Name": "col2",
        "Type": "string"
    },
    {
        "Name": "col3",
        "Type": "double"
    }
],
"Compressed": false,
"NumberOfBuckets": 0,
"SortColumns": [],
"StoredAsSubDirectories": false
},
"TableType": "VIRTUAL_VIEW",
"IsRegisteredWithLakeFormation": false,
"CatalogId": "123456789012",
"IsRowFilteringEnabled": false,
"VersionId": "-1",
"DatabaseId": "<databaseID>",
"ViewDefinition": {
    "IsProtected": true,
    "Definer": "arn:aws:iam::123456789012:role/GDCViewDefiner",
    "SubObjects": [
        "arn:aws:glue:us-east-1:123456789012:table/gdc-view-
playground-db/table_1"
    ],
    "Representations": [
        {
            "Dialect": "ATHENA",
            "DialectVersion": "3",
            "ViewOriginalText": "SELECT col1, col2 FROM \"gdc-view-
playground-db\".\"table_1\"",
            "IsStale": false
        },
        {
            "Dialect": "REDSHIFT",
            "DialectVersion": "1.0",
            "ViewOriginalText": "SELECT col1 FROM \"gdc-view-
playground-external-schema\".\"table_1\";",
            "IsStale": false
        }
    ]
}

```

```
    },
    "IsMultiDialectView": true
},
"ViewValidations": [
  {
    "Dialect": "ATHENA",
    "DialectVersion": "3",
    "ViewValidationText": "SELECT col1, col2 FROM \"gdc-view-playground-db\".\"table_1\"",
    "UpdateTime": "2024-07-11T11:23:19-07:00",
    "State": "FAILED",
    "Error": {
      "ErrorCode": "InvalidInputException",
      "ErrorMessage": "Engine and existing storage descriptor mismatch"
    }
  },
  {
    "Dialect": "REDSHIFT",
    "DialectVersion": "1.0",
    "ViewValidationText": "SELECT col1 FROM \"gdc-view-playground-external-schema\".\"table_1\";",
    "UpdateTime": "2024-07-11T11:22:49-07:00",
    "State": "FAILED",
    "Error": {
      "ErrorCode": "InvalidInputException",
      "ErrorMessage": "Engine and existing storage descriptor mismatch"
    }
  }
]
}
}
```

Erteilen von Berechtigungen für Datenkatalog-Ansichten

Nachdem Sie Ansichten in der erstellt haben AWS Glue Data Catalog, können Sie Prinzipalen in allen AWS-Konten Organisationen und Organisationseinheiten Data Lake-Berechtigungen für Ansichten gewähren. Sie können Berechtigungen mithilfe von LF-Tags oder der Methode mit der benannten

Ressource erteilen. Weitere Informationen zum Markieren von Ressourcen finden Sie unter [Tag-basierte Zugangskontrolle von Lake Formation](#). Weitere Informationen zum direkten Erteilen von Berechtigungen für Ansichten finden Sie unter [Erteilen von Berechtigungen für Ansichten mithilfe der benannten Ressourcenmethode](#).

Materialisierte Ansichten

Themen

- [Differenzierung materialisierter Ansichten von anderen Ansichtstypen](#)
- [Anwendungsfälle](#)
- [Die wichtigsten Konzepte](#)
- [Berechtigungen für materialisierte Ansichten](#)
- [Materialisierte Ansichten erstellen und verwalten](#)
- [Speicher und Datenzugriff](#)
- [AWS Lake Formation Integration mit Berechtigungen](#)
- [Überwachung und Debugging](#)
- [Verwaltung von Aktualisierungsaufträgen](#)
- [Überwachung und Problembehebung](#)
- [Überlegungen und Einschränkungen](#)

Im AWS Glue Datenkatalog ist eine materialisierte Ansicht eine verwaltete Tabelle, in der das vorberechnete Ergebnis einer SQL-Abfrage im Apache Iceberg-Format gespeichert wird. Im Gegensatz zu Standard-Datenkatalogsichten, die die Abfrage bei jedem Zugriff ausführen, speichern materialisierte Ansichten die Abfrageergebnisse physisch und aktualisieren sie, wenn sich die zugrunde liegenden Quelltabellen ändern. Sie können materialisierte Ansichten mit Apache Spark Version 3.5.6+ in Amazon Athena, Amazon EMR oder erstellen. AWS Glue

Materialisierte Ansichten verweisen auf Apache Iceberg-Tabellen, die im AWS Glue Datenkatalog registriert sind, wobei vorberechnete Daten als Apache Iceberg-Tabellen in Amazon S3 S3-Tabellen oder Amazon S3 S3-Allzweck-Buckets gespeichert sind, sodass sie von mehreren Abfrage-Engines wie Amazon Athena, Amazon Redshift und Iceberg-kompatiblen Engines von Drittanbietern aus zugänglich sind.

Differenzierung materialisierter Ansichten von anderen Ansichtstypen

Materialisierte Ansichten unterscheiden sich grundlegend von AWS Glue Datenkatalogansichten, Apache Spark-Ansichten und Amazon Athena Athena-Ansichten. Während es sich bei Datenkatalogansichten um virtuelle Tabellen handelt, die die SQL-Abfragedefinition bei jedem Zugriff ausführen, speichern materialisierte Ansichten die vorberechneten Abfrageergebnisse physisch. Dadurch werden redundante Berechnungen vermieden und die Abfrageleistung für komplexe Transformationen, auf die häufig zugegriffen wird, erheblich verbessert.

Materialisierte Ansichten unterscheiden sich auch von herkömmlichen Datentransformationspipelines, die mit AWS Glue ETL- oder benutzerdefinierten Spark-Jobs erstellt wurden. Anstatt benutzerdefinierten Code für die Änderungserkennung, inkrementelle Aktualisierungen und Workflow-Orchestrierung zu schreiben, definieren Sie materialisierte Ansichten mithilfe der Standard-SQL-Syntax. Der AWS Glue Datenkatalog überwacht automatisch Quelltabellen, erkennt Änderungen und aktualisiert materialisierte Ansichten mithilfe einer vollständig verwalteten Recheninfrastruktur.

Anwendungsfälle

Im Folgenden sind wichtige Anwendungsfälle für materialisierte Ansichten aufgeführt:

- Beschleunigen Sie komplexe analytische Abfragen — Erstellen Sie materialisierte Ansichten, die teure Verknüpfungen, Aggregationen und Fensterfunktionen vorab berechnen. Spark-Engines schreiben nachfolgende Abfragen automatisch neu, um die im Voraus berechneten Ergebnisse zu verwenden, wodurch die Latenz von Abfragen und die Rechenkosten reduziert werden.
- Vereinfachen Sie Datenumwandlungs-Pipelines — Ersetzen Sie komplexe ETL-Jobs, die sich um die Änderungserkennung, inkrementelle Updates und Workflow-Orchestrierung kümmern, durch einfache SQL-basierte Definitionen für materialisierte Ansichten. Der AWS Glue Datenkatalog verwaltet die gesamte betriebliche Komplexität automatisch.
- Ermöglichen Sie Self-Service-Analysen mit geregelter Datenzugriff — Erstellen Sie kuratierte materialisierte Ansichten, die Rohdaten in einsatzbereite Datensätze umwandeln. Gewähren Sie Benutzern Zugriff auf materialisierte Ansichten, ohne die zugrunde liegenden Quelltabellen offenzulegen. Dies vereinfacht das Sicherheitsmanagement und ermöglicht gleichzeitig Self-Service-Analysen.
- Optimieren Sie das Feature-Engineering für maschinelles Lernen — Definieren Sie materialisierte Ansichten, die Feature-Transformationen für ML-Modelle implementieren. Die automatische Aktualisierungsfunktion stellt sicher, dass die Feature-Speicher bei der Weiterentwicklung der Quelldaten aktuell bleiben, während die inkrementelle Aktualisierung die Rechenkosten minimiert.

- Implementieren Sie eine effiziente gemeinsame Nutzung von Daten — Erstellen Sie materialisierte Ansichten, die Daten für bestimmte Nutzer filtern und transformieren. Teilen Sie materialisierte Ansichten über Konten und Regionen hinweg AWS Lake Formation, indem Sie die Notwendigkeit von Datenduplikationen vermeiden und gleichzeitig eine zentralisierte Verwaltung aufrechterhalten.

Die wichtigsten Konzepte

Automatische Aktualisierung

Die automatische Aktualisierung ist eine Funktion, die Ihre Quelltabellen kontinuierlich überwacht und materialisierte Ansichten gemäß einem von Ihnen definierten Zeitplan aktualisiert. Wenn Sie eine materialisierte Ansicht erstellen, können Sie mithilfe einer zeitbasierten Planung mit Intervallen von bis zu einer Stunde eine Aktualisierungshäufigkeit angeben. Der AWS Glue Datenkatalog verwendet eine verwaltete Spark-Recheninfrastruktur, um Aktualisierungsvorgänge im Hintergrund auszuführen und alle Aspekte der Änderungserkennung und der inkrementellen Aktualisierungen transparent zu handhaben.

Wenn sich die Quelldaten zwischen den Aktualisierungsintervallen ändern, ist die materialisierte Ansicht vorübergehend veraltet. Abfragen, die direkt auf die materialisierte Ansicht zugreifen, geben möglicherweise veraltete Ergebnisse zurück, bis die nächste geplante Aktualisierung abgeschlossen ist. In Szenarien, die sofortigen Zugriff auf die aktuellsten Daten erfordern, können Sie mit dem `REFRESH MATERIALIZED VIEW SQL`-Befehl eine manuelle Aktualisierung ausführen.

Inkrementelle Aktualisierung

Die inkrementelle Aktualisierung ist eine Optimierungstechnik, bei der nur die Daten verarbeitet werden, die sich in den Quelltabellen seit der letzten Aktualisierung geändert haben, anstatt die gesamte materialisierte Ansicht neu zu berechnen. Der AWS Glue Datenkatalog nutzt die Metadatenebene von Apache Iceberg, um Änderungen in Quelltabellen effizient nachzuverfolgen und festzustellen, welche Teile der materialisierten Ansicht aktualisiert werden müssen.

Dieser Ansatz reduziert die Rechenkosten und die Aktualisierungsdauer im Vergleich zu vollständigen Aktualisierungsvorgängen erheblich, insbesondere bei großen Datensätzen, bei denen sich nur ein kleiner Prozentsatz der Daten zwischen den Aktualisierungszyklen ändert. Der inkrementelle Aktualisierungsmechanismus funktioniert automatisch. Sie müssen keine benutzerdefinierte Logik schreiben, um geänderte Daten zu erkennen oder zu verarbeiten.

Automatisches Umschreiben von Abfragen

Automatisches Umschreiben von Abfragen ist eine Funktion zur Abfrageoptimierung, die in Spark-Engines von Amazon Athena, Amazon EMR und verfügbar ist. AWS Glue Wenn Sie eine Abfrage anhand von Basistabellen ausführen, analysiert der Spark-Optimierer Ihren Abfrageplan und ermittelt automatisch, ob verfügbare materialisierte Ansichten die Abfrage effizienter erfüllen können. Wenn eine geeignete materialisierte Ansicht vorhanden ist, schreibt der Optimierer die Abfrage transparent neu, sodass die vorberechneten Ergebnisse verwendet werden, anstatt die Basistabellen zu verarbeiten.

Diese Optimierung erfolgt, ohne dass Änderungen am Anwendungscode oder an den Abfrageanweisungen erforderlich sind. Der Spark-Optimierer stellt sicher, dass das automatische Umschreiben von Abfragen nur angewendet wird, wenn die materialisierte Ansicht aktuell ist und zu genauen Ergebnissen führen kann. Wenn eine materialisierte Ansicht veraltet ist oder die Abfrageanforderungen nicht vollständig erfüllt, führt der Optimierer den ursprünglichen Abfrageplan anhand der Basistabellen aus, wobei der Korrektheit Vorrang vor der Leistung eingeräumt wird.

Rolle des View-Definers

Eine materialisierte Ansicht funktioniert auf der Grundlage der Berechtigungen der IAM-Rolle, mit der sie erstellt wurde. Sie wird als View Definer-Rolle bezeichnet. Die Definerrolle muss Lesezugriff auf alle Basistabellen haben, auf die in der Definition der materialisierten Ansicht verwiesen wird, und muss über Berechtigungen zum Erstellen von Tabellen in der Zieldatenbank verfügen. Wenn der AWS Glue Datenkatalog eine materialisierte Ansicht aktualisiert, übernimmt er die Rolle des Definierers, um auf Quelltabellen zuzugreifen und aktualisierte Ergebnisse zu schreiben.

Dieses Sicherheitsmodell ermöglicht es Ihnen, Benutzern Zugriff auf materialisierte Ansichten zu gewähren, ohne ihnen direkte Berechtigungen für die zugrunde liegenden Quelltabellen zu gewähren. Wenn die Rolle des View Definers den Zugriff auf eine Basistabelle verliert, schlagen nachfolgende Aktualisierungsvorgänge fehl, bis die Berechtigungen wiederhergestellt sind.

Berechtigungen für materialisierte Ansichten

Um materialisierte Ansichten zu erstellen und zu verwalten, müssen Sie Berechtigungen konfigurieren AWS Lake Formation . Die IAM-Rolle, die die materialisierte Ansicht erstellt (die Definer-Rolle), erfordert spezielle Berechtigungen für Quelltabellen und Zieldatenbanken.

Erforderliche Berechtigungen für die Definer-Rolle

Die Definierrolle muss über die folgenden Lake Formation Formation-Berechtigungen verfügen:

- Für Quelltabellen — SELECT- oder ALL-Berechtigungen ohne Zeilen-, Spalten- oder Zellenfilter
- In der Zieldatenbank — CREATE_TABLE-Berechtigung
- Über den AWS Glue Datenkatalog — GetTable und API-Berechtigungen CreateTable

Wenn Sie eine materialisierte Ansicht erstellen, wird der ARN der Definiererrolle in der Ansichtsdefinition gespeichert. Der AWS Glue Datenkatalog übernimmt diese Rolle, wenn automatische Aktualisierungsvorgänge ausgeführt werden. Wenn die Definiererrolle den Zugriff auf Quelltabellen verliert, schlagen Aktualisierungsvorgänge fehl, bis die Berechtigungen wiederhergestellt sind.

IAM-Berechtigungen für Jobs AWS Glue

Für die IAM-Rolle Ihres AWS Glue Jobs sind die folgenden Berechtigungen erforderlich:

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Action": [
        "glue:GetCatalog",
        "glue:GetCatalogs",
        "glue:GetTable",
        "glue:GetTables",
        "glue:CreateTable",
        "glue:UpdateTable",
        "glue>DeleteTable",
        "glue:GetDatabase",
        "glue:GetDatabases",
        "cloudwatch:PutMetricData"
      ],
      "Resource": "*"
    },
    {
      "Effect": "Allow",
      "Action": [
        "s3:GetObject",
        "s3:PutObject",
        "s3>DeleteObject"
      ],
      "Resource": [
```

```

        "arn:aws:s3:::amzn-s3-demo-bucket/*"
    ],
    },
    {
        "Effect": "Allow",
        "Action": [
            "s3:ListBucket"
        ],
        "Resource": [
            "arn:aws:s3:::amzn-s3-demo-bucket"
        ]
    },
    {
        "Effect": "Allow",
        "Action": [
            "logs:CreateLogGroup",
            "logs:CreateLogStream",
            "logs:PutLogEvents"
        ],
        "Resource": [
            "arn:aws:logs:*:*:*:/aws-glue/*"
        ]
    },
    {
        "Effect": "Allow",
        "Action": [
            "lakeformation:GetDataAccess"
        ],
        "Resource": "*"
    }
]
}

```

Die Rolle, die Sie für die automatische Aktualisierung von Materialized View verwenden, muss über die iam: PassRole -Berechtigung für die Rolle verfügen.

```

{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Action": [

```

```

        "iam:PassRole"
    ],
    "Resource": [
        "arn:aws:iam::111122223333:role/materialized-view-role-name"
    ]
}
]
}

```

Damit Glue die materialisierte Ansicht automatisch für Sie aktualisiert, muss die Rolle außerdem über die folgende Vertrauensrichtlinie verfügen, die es dem Dienst ermöglicht, die Rolle zu übernehmen.

```

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

```

Wenn die Materialized View in S3 Tables Buckets gespeichert ist, müssen Sie der Rolle außerdem die folgende Berechtigung hinzufügen.

```

{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Action": [
        "s3tables:PutTableMaintenanceConfiguration"
      ],
      "Resource": "arn:aws:s3tables:*:123456789012:*"
    }
  ]
}

```

```
]
}
```

Zugriff auf materialisierte Ansichten gewähren

Um anderen Benutzern Zugriff auf die Abfrage einer materialisierten Ansicht zu gewähren, verwenden Sie, AWS Lake Formation um die SELECT-Berechtigung für die Materialized View-Tabelle zu gewähren. Benutzer können die Materialized View abfragen, ohne direkten Zugriff auf die zugrunde liegenden Quelltabellen zu benötigen.

Ausführliche Informationen zur Konfiguration von Lake Formation Formation-Berechtigungen finden Sie unter Erteilen und Widerrufen von Berechtigungen für Datenkatalogressourcen im AWS Lake Formation Entwicklerhandbuch.

Materialisierte Ansichten erstellen und verwalten

Sie erstellen materialisierte Ansichten mithilfe der `CREATE MATERIALIZED VIEW` SQL-Anweisung in Spark-Engines. Die View-Definition spezifiziert die SQL-Abfrage, die die Transformationslogik, den Zieldatenbank- und Tabellennamen sowie die optionale Aktualisierungskonfiguration definiert. Sie können komplexe Transformationen definieren, einschließlich Aggregationen, Verknüpfungen über mehrere Tabellen hinweg, Filter und Fensterfunktionen.

```
CREATE MATERIALIZED VIEW sales_summary
AS
SELECT
    region,
    product_category,
    SUM(sales_amount) as total_sales,
    COUNT(DISTINCT customer_id) as unique_customers
FROM sales_transactions
WHERE transaction_date >= current_date - interval '90' day
GROUP BY region, product_category;
```

Um die automatische Aktualisierung zu konfigurieren, nehmen Sie den Aktualisierungszeitplan in Ihre View-Definition auf:

```
CREATE MATERIALIZED VIEW sales_summary
SCHEDULE REFRESH EVERY 1 HOUR
AS
```

```
SELECT region, product_category, SUM(sales_amount) as total_sales
FROM sales_transactions
GROUP BY region, product_category;
```

Sie können eine materialisierte Ansicht jederzeit manuell aktualisieren, indem Sie den `REFRESH MATERIALIZED VIEW` folgenden Befehl verwenden:

```
REFRESH MATERIALIZED VIEW sales_summary;
```

Um den Aktualisierungszeitplan einer vorhandenen materialisierten Ansicht zu ändern, verwenden Sie die `ALTER MATERIALIZED VIEW` folgende Anweisung:

```
ALTER MATERIALIZED VIEW sales_summary
ADD SCHEDULE REFRESH EVERY 2 HOURS;
```

Verschachtelte materialisierte Ansichten

Sie können materialisierte Ansichten erstellen, die auf andere materialisierte Ansichten als Basistabellen verweisen, wodurch mehrstufige Datentransformationen ermöglicht werden. Wenn Sie verschachtelte Materialized Views erstellen, verfolgt der AWS Glue Datenkatalog Abhängigkeiten und verteilt Aktualisierungen automatisch über die Materialized View-Hierarchie. Wenn eine materialisierte Basisansicht aktualisiert wird, werden alle von ihr abhängigen Downstream-Materialized Views entsprechend aktualisiert.

Diese Funktion ermöglicht es Ihnen, komplexe Transformationen in logische Phasen zu zerlegen, was die Wartbarkeit verbessert und eine selektive Aktualisierung der Transformationsebenen auf der Grundlage Ihrer Datenaktualisierungsanforderungen ermöglicht.

Speicher und Datenzugriff

Materialisierte Ansichten speichern vorberechnete Ergebnisse als Apache Iceberg-Tabellen in S3-Tabellen-Buckets oder S3-Buckets für allgemeine Zwecke in Ihrem Konto. AWS Der AWS Glue Datenkatalog verwaltet alle Aspekte der Wartung von Iceberg-Tabellen, einschließlich der Komprimierung und Aufbewahrung von Snapshots, mithilfe der automatisierten Optimierungsfunktionen von S3 Tables.

Da materialisierte Ansichten als Iceberg-Tabellen gespeichert werden, können Sie sie direkt von jeder Iceberg-kompatiblen Engine lesen, einschließlich Amazon Athena, Amazon Redshift und Analyseplattformen von Drittanbietern. Dieser Zugriff auf mehrere Engines stellt sicher, dass Ihre

vorberechneten Daten in Ihrem gesamten Analytics-Ökosystem ohne Datenduplizierung oder Formatkonvertierung zugänglich bleiben.

AWS Lake Formation Integration mit Berechtigungen

Sie können es verwenden AWS Lake Formation , um detaillierte Berechtigungen für materialisierte Ansichten zu verwalten. Der Ersteller der Ansicht wird automatisch Eigentümer der materialisierten Ansicht und kann anderen Benutzern oder Rollen mithilfe der benannten Ressourcenmethode oder AWS Lake Formation LF-Tags Berechtigungen gewähren.

Wenn Sie einem Benutzer die SELECT Berechtigung für eine materialisierte Ansicht gewähren, kann er die vorberechneten Ergebnisse abfragen, ohne Zugriff auf die zugrunde liegenden Quelltabellen zu benötigen. Dieses Sicherheitsmodell vereinfacht die Datenzugriffsverwaltung und ermöglicht es Ihnen, das Prinzip der geringsten Rechte zu implementieren, sodass Benutzer nur auf die spezifischen Datentransformationen zugreifen können, die sie benötigen.

Mithilfe der Funktionen zur AWS kontenübergreifenden gemeinsamen Nutzung können Sie materialisierte Ansichten für Konten, AWS Organisationen und Organisationseinheiten gemeinsam nutzen AWS Lake Formation. Mithilfe von Ressourcenlinks können Sie auch AWS regionsübergreifend auf materialisierte Ansichten zugreifen und so eine zentrale Datenverwaltung mit verteiltem Datenzugriff ermöglichen.

Überwachung und Debugging

Der AWS Glue Datenkatalog veröffentlicht alle Aktualisierungsvorgänge von materialisierten Ansichten und die zugehörigen Metriken auf Amazon CloudWatch. Sie können die Startzeit, die Endzeit, die Dauer, das verarbeitete Datenvolumen und den Aktualisierungsstatus von Aktualisierungen anhand von CloudWatch Metriken überwachen. Wenn Aktualisierungsvorgänge fehlschlagen, werden Fehlermeldungen und Diagnoseinformationen in CloudWatch Protokollen erfasst.

Sie können CloudWatch Alarmer einrichten, um Benachrichtigungen zu erhalten, wenn Aktualisierungsaufträge die erwartete Dauer überschreiten oder wiederholt fehlschlagen. Der AWS Glue Datenkatalog veröffentlicht auch Änderungsereignisse sowohl für erfolgreiche als auch für fehlgeschlagene Aktualisierungsläufe, sodass Sie Materialized View-Operationen in eine umfassendere Workflow-Automatisierung integrieren können.

Um den aktuellen Status einer materialisierten Ansicht zu überprüfen, verwenden Sie den DESCRIBE MATERIALIZED VIEW SQL-Befehl, der Metadaten zurückgibt, darunter den Verfallsstatus, den Zeitstempel der letzten Aktualisierung und die Konfiguration des Aktualisierungszeitplans.

Verwaltung von Aktualisierungsaufträgen

Starten einer manuellen Aktualisierung

Löst eine sofortige Aktualisierung außerhalb des geplanten Intervalls aus.

Erforderliche Berechtigung: Die für den API-Aufruf verwendeten AWS Anmeldeinformationen müssen über eine `glue:GetTable` Berechtigung für die materialisierte Ansicht verfügen.

Für den S3-Tabellenkatalog:

```
aws glue start-materialized-view-refresh-task-run \  
  --catalog-id <ACCOUNT_ID>:s3tablescatalog/<CATALOG_NAME> \  
  --database-name <DATABASE_NAME> \  
  --table-name <MV_TABLE_NAME>
```

Für Root Catalog:

```
aws glue start-materialized-view-refresh-task-run \  
  --catalog-id <ACCOUNT_ID> \  
  --database-name <DATABASE_NAME> \  
  --table-name <MV_TABLE_NAME>
```

Aktualisierungsstatus wird überprüft

Rufen Sie den Status eines bestimmten Aktualisierungsauftrags ab:

```
aws glue get-materialized-view-refresh-task-run \  
  --catalog-id <CATALOG_ID> \  
  --materialized-view-refresh-task-run-id <TASK_RUN_ID>
```

Aktualisierungsverlauf auflisten

Alle Aktualisierungsaufträge für eine materialisierte Ansicht anzeigen:

```
aws glue list-materialized-view-refresh-task-runs \  
  --catalog-id <CATALOG_ID> \  
  --database-name <DATABASE_NAME> \  
  --table-name <MV_TABLE_NAME>
```

 Note

Wird <ACCOUNT_ID>:s3tablescatalog/<CATALOG_NAME> für S3-Tabellen oder <ACCOUNT_ID> für den Stammkatalog verwendet.

Eine laufende Aktualisierung wird gestoppt

Brechen Sie einen laufenden Aktualisierungsauftrag ab:

```
aws glue stop-materialized-view-refresh-task-run \  
  --catalog-id <CATALOG_ID> \  
  --database-name <DATABASE_NAME> \  
  --table-name <MV_TABLE_NAME>
```

Überwachung und Problembehebung

Es gibt drei Möglichkeiten, Aktualisierungsaufträge für Materialized Views zu überwachen:

CloudWatch Metriken

Sehen Sie sich aggregierte Metriken für all Ihre Materialized View Refresh-Jobs an unter: CloudWatch

Verfügbare Metriken:

- AWS/Glue-Namespace mit Abmessungen:
 - CatalogId: Ihre Katalog-ID
 - DatabaseName: Datenbank, die die materialisierte Ansicht enthält
 - TableName: Name der materialisierten Ansicht
 - TaskType: Auf "" MaterializedViewRefresh gesetzt

In der Konsole anzeigen:

1. Navigieren Sie zu CloudWatch Konsole → Metriken
2. Wählen Sie den AWS/Glue-Namespace
3. Nach Dimensionen filtern: CatalogId,, DatabaseName TableName TaskType
4. Sehen Sie sich Kennzahlen für Erfolg, Misserfolg und Dauer von Aufträgen an

Beispiel für eine CloudWatch Metrik-Abfrage:

```
{AWS/Glue,CatalogId,DatabaseName,TableName,TaskType} MaterializedViewRefresh
```

Verwenden von AWS CLI:

```
aws cloudwatch get-metric-statistics \  
  --namespace AWS/Glue \  
  --metric-name <MetricName> \  
  --dimensions Name=CatalogId,Value=<CATALOG_ID> \  
               Name=DatabaseName,Value=<DATABASE_NAME> \  
               Name=TableName,Value=<TABLE_NAME> \  
               Name=TaskType,Value=MaterializedViewRefresh \  
  --start-time <START_TIME> \  
  --end-time <END_TIME> \  
  --period 3600 \  
  --statistics Sum \  
  --region <REGION>
```

CloudWatch Logs

Detaillierte Ausführungsprotokolle für einzelne Ausführungen von Aktualisierungsaufgaben anzeigen:

Protokollgruppe: /aws-glue/materialized-views/<task_run_id>

Wo <task_run_id> ist eine UUID (z. B. abc12345-def6-7890-ghij-klmnopqrstuv).

Protokolle anzeigen:

```
# List log streams for a task run  
aws logs describe-log-streams \  
  --log-group-name /aws-glue/materialized-views/<TASK_RUN_ID> \  
  --region <REGION>  
  
# Get log events  
aws logs get-log-events \  
  --log-group-name /aws-glue/materialized-views/<TASK_RUN_ID> \  
  --log-stream-name <LOG_STREAM_NAME> \  
  --region <REGION>
```

In der CloudWatch Konsole:

1. Navigieren Sie zu CloudWatch → Protokollgruppen
2. Suchen Sie nach /aws-glue/materialized-views/
3. Wählen Sie die Protokollgruppe mit Ihrer Aufgabenausführungs-ID aus
4. Sehen Sie sich detaillierte Ausführungsprotokolle, Fehler und die Spark-Jobausgabe an

Benachrichtigungen

Abonnieren Sie Ereignisse für Benachrichtigungen in Echtzeit über Statusänderungen bei der Aktualisierung von Jobs:

Verfügbare Ereignistypen:

- Die Aufgabe zur Aktualisierung von Glue Materialized View wurde gestartet
- Die Aktualisierungsaufgabe von Glue Materialized View war erfolgreich
- Die Aktualisierungsaufgabe für Glue Materialized View ist fehlgeschlagen
- Fehler beim Aufrufen der automatischen Aktualisierung von Glue Materialized View

Eine Regel erstellen:

```
aws events put-rule \  
  --name materialized-view-refresh-notifications \  
  --event-pattern '{  
    "source": ["aws.glue"],  
    "detail-type": [  
      "Glue Materialized View Refresh Task Started",  
      "Glue Materialized View Refresh Task Succeeded",  
      "Glue Materialized View Refresh Task Failed",  
      "Glue Materialized View Auto-Refresh Invocation Failure"  
    ]  
  }' \  
  --region <REGION>
```

Ein Ziel hinzufügen (z. B. ein SNS-Thema):

```
aws events put-targets \  
  --rule materialized-view-refresh-notifications \  
  --targets "Id"="1", "Arn"="arn:aws:sns:<REGION>:<ACCOUNT_ID>:<TOPIC_NAME>" \  
  --region <REGION>
```

Aktualisierungsstatus anzeigen

Überprüfen Sie den Status Ihrer Materialized View-Aktualisierungsaufträge mithilfe der AWS Glue API:

```
aws glue get-materialized-view-refresh-task-run \  
  --catalog-id <CATALOG_ID> \  
  --materialized-view-refresh-task-run-id <TASK_RUN_ID> \  
  --region <REGION>
```

Oder listen Sie alle letzten Aktualisierungsläufe auf:

```
aws glue list-materialized-view-refresh-task-runs \  
  --catalog-id <CATALOG_ID> \  
  --database-name <DATABASE_NAME> \  
  --table-name <MV_TABLE_NAME> \  
  --region <REGION>
```

Das zeigt:

- Uhrzeit der letzten Aktualisierung
- Aktualisierungsstatus (ERFOLGREICH, FEHLGESCHLAGEN, LÄUFT, GESTOPPT)
- ID der Aufgabenausführung
- Fehlermeldungen (falls fehlgeschlagen)

Allgemeine Aktualisierungsstatus:

- WIRD AUSGEFÜHRT: Der Aktualisierungsjob wird gerade ausgeführt
- ERFOLGREICH: Die Aktualisierung wurde erfolgreich abgeschlossen
- FEHLGESCHLAGEN: Bei der Aktualisierung ist ein Fehler aufgetreten
- GESTOPPT: Die Aktualisierung wurde manuell abgebrochen

Fehlerbehebung bei fehlgeschlagenen Aktualisierungen:

Wenn eine Aktualisierung fehlschlägt, überprüfen Sie:

1. IAM-Berechtigungen: Stellen Sie sicher, dass die Definiererrolle Zugriff auf alle Basistabellen und den Speicherort der materialisierten Ansicht hat

2. Verfügbarkeit von Basistabellen: Stellen Sie sicher, dass alle referenzierten Tabellen existieren und zugänglich sind
3. Gültigkeit der Abfrage: Stellen Sie sicher, dass die SQL-Abfrage für den Spark-SQL-Dialekt gültig ist
4. Ressourcenlimits: Prüfen Sie, ob Sie die Limits für gleichzeitige Aktualisierungen für Ihr Konto erreicht haben

Verwenden Sie die `GetMaterializedViewRefreshTaskRun` API, um detaillierte Fehlermeldungen abzurufen.

Überlegungen und Einschränkungen

- Materialisierte Ansichten können nur auf Apache Iceberg-Tabellen verweisen, die im AWS Glue Datenkatalog als Basistabellen registriert sind.
- Die Erstellung von Ansichten und das automatische Umschreiben von Abfragen sind nur über Spark-Engines in Apache Spark Version 3.5.6 und höher in Amazon Athena, Amazon EMR und AWS Glue (Version 5.1) verfügbar.
- Materialisierte Ansichten stimmen letztendlich mit Basistabellen überein. Während des Aktualisierungsfensters können Abfragen, die direkt auf die materialisierte Ansicht zugreifen, veraltete Daten zurückgeben. Führen Sie eine manuelle Aktualisierung durch, um sofort auf aktuelle Daten zugreifen zu können.
- Das minimale automatische Aktualisierungsintervall beträgt eine Stunde. In Anwendungsfällen, die häufigere Updates erfordern, führen Sie manuelle Aktualisierungen programmgesteuert mit dem Befehl aus. `REFRESH MATERIALIZED VIEW`
- Beim Umschreiben von Abfragen wird der Korrektheit Vorrang vor der Leistung eingeräumt. Wenn eine materialisierte Ansicht veraltet ist oder die Abfrageanforderungen nicht genau erfüllen kann, führen Spark-Engines die ursprüngliche Abfrage anhand der Basistabellen aus.

Daten mithilfe von Workflows in Lake Formation importieren

Mit AWS Lake Formation können Sie Ihre Daten mithilfe von Workflows importieren. Ein Workflow definiert die Datenquelle und den Zeitplan für den Import von Daten in Ihren Data Lake. Es ist ein Container für AWS Glue Crawler, Jobs und Trigger, die verwendet werden, um die Prozesse zum Laden und Aktualisieren des Data Lakes zu orchestrieren.

Themen

- [Baupläne und Arbeitsabläufe in Lake Formation](#)
- [Einen Workflow erstellen](#)
- [Einen Workflow ausführen](#)

Baupläne und Arbeitsabläufe in Lake Formation

Ein Workflow umfasst eine komplexe ETL-Aktivität (Extrahieren, Transformieren und Laden) mit mehreren Aufträgen. Workflows generieren AWS Glue Crawler, Jobs und Trigger, um das Laden und Aktualisieren von Daten zu orchestrieren. Lake Formation führt einen Workflow als eine Einheit aus und verfolgt ihn. Sie können einen Workflow so konfigurieren, dass er bei Bedarf oder nach einem Zeitplan ausgeführt wird.

Note

Spark Parquet Writer unterstützt keine Sonderzeichen in Spaltennamen. Dies ist eine technische Einschränkung des Writers selbst, kein Konfigurationsproblem.

Workflows, die Sie in Lake Formation erstellen, sind in der AWS Glue Konsole als gerichteter azyklischer Graph (DAG) sichtbar. Jeder DAG-Knoten ist ein Job, Crawler oder Trigger. Um den Fortschritt zu überwachen und Fehler zu beheben, können Sie den Status jedes Knotens im Workflow verfolgen.

Wenn ein Lake Formation Workflow abgeschlossen ist, erhält der Benutzer, der den Workflow ausgeführt hat, die Lake Formation SELECT Formation-Berechtigung für die Datenkatalogtabellen, die der Workflow erstellt.

Sie können Workflows auch in erstellenAWS Glue. Da Sie mit Lake Formation jedoch einen Workflow anhand eines Blueprints erstellen können, ist die Erstellung von Workflows in Lake Formation viel einfacher und automatisierter. Lake Formation bietet die folgenden Arten von Bauplänen:

- **Datenbank-Snapshot** — Lädt Daten aus allen Tabellen aus einer JDBC-Quelle in den Data Lake oder lädt sie neu. Sie können einige Daten anhand eines Ausschlussmusters aus der Quelle ausschließen.
- **Inkrementelle Datenbank** — Lädt nur neue Daten aus einer JDBC-Quelle in den Data Lake, die auf zuvor gesetzten Lesezeichen basieren. Sie geben die einzelnen Tabellen in der JDBC-Quelldatenbank an, die eingeschlossen werden sollen. Für jede Tabelle wählen Sie die

Lesezeichenspalten und die Lesezeichen-Sortierreihenfolge aus, um den Überblick über die Daten zu behalten, die zuvor geladen wurden. Wenn Sie zum ersten Mal einen inkrementellen Datenbank-Blueprint für eine Gruppe von Tabellen ausführen, lädt der Workflow alle Daten aus den Tabellen und legt Lesezeichen für den nächsten inkrementellen Datenbank-Blueprint-Lauf fest. Sie können daher einen inkrementellen Datenbank-Blueprint anstelle des Datenbanksnapshot-Blueprints verwenden, um alle Daten zu laden, vorausgesetzt, Sie geben jede Tabelle in der Datenquelle als Parameter an.

- Protokolldatei — Daten werden massenweise aus Protokolldateiquellen geladen AWS CloudTrail, darunter Elastic Load Balancing-Logs und Application Load Balancer Balancer-Logs.

Anhand der folgenden Tabelle können Sie entscheiden, ob Sie einen Datenbank-Snapshot oder einen inkrementellen Datenbank-Blueprint verwenden möchten.

Verwenden Sie einen Datenbank-Snapshot, wenn...	Verwenden Sie eine inkrementelle Datenbank, wenn...
• Die Schemaentwicklung ist flexibel. (Spalten werden umbenannt, vorherige Spalten werden gelöscht und an ihrer Stelle werden neue Spalten hinzugefügt.) • Vollständige Konsistenz zwischen der Quelle und dem Ziel ist erforderlich.	• Die Entwicklung des Schemas erfolgt inkrementell. (Es werden nur nacheinander Spalten hinzugefügt.) • Es werden nur neue Zeilen hinzugefügt; vorherige Zeilen werden nicht aktualisiert.

Note

Benutzer können von Lake Formation erstellte Blueprints und Workflows nicht bearbeiten.

Einen Workflow erstellen

Bevor Sie beginnen, stellen Sie sicher, dass Sie der Rolle die erforderlichen Datenberechtigungen und Datenspeicherberechtigungen erteilt haben `LakeFormationWorkflowRole`. Auf diese Weise kann der Workflow Metadatentabellen im Datenkatalog erstellen und Daten an Zielorte in Amazon S3 schreiben. Weitere Informationen erhalten Sie unter [\(Optional\) Erstellen Sie eine IAM-Rolle für Workflows](#) und [Überblick über die Genehmigungen für Lake Formation](#).

 Note

Lake Formation verwendet `GetTemplateInstance`, `GetTemplateInstances`, und `InstantiateTemplate` Operationen, um Workflows aus Blueprints zu erstellen. Diese Operationen sind nicht öffentlich verfügbar und werden nur intern zur Erstellung von Ressourcen in Ihrem Namen verwendet. Sie erhalten CloudTrail Ereignisse für die Erstellung von Workflows.

Um einen Workflow aus einem Blueprint zu erstellen

1. Öffnen Sie die AWS Lake Formation Konsole unter <https://console.aws.amazon.com/lakeformation/>. Melden Sie sich als Data Lake-Administrator oder als Benutzer mit Data Engineer-Rechten an. Weitere Informationen finden Sie unter [Referenz zu Personas und IAM-Berechtigungen in Lake Formation](#).
2. Wählen Sie im Navigationsbereich Blueprints und dann Blueprint verwenden aus.
3. Wählen Sie auf der Seite Blueprint verwenden eine Kachel aus, um den Blueprint-Typ auszuwählen.
4. Geben Sie unter Importquelle die Datenquelle an.

Wenn Sie aus einer JDBC-Quelle importieren, geben Sie Folgendes an:

- Datenbankverbindung — Wählen Sie eine Verbindung aus der Liste aus. Erstellen Sie zusätzliche Verbindungen mithilfe der AWS Glue Konsole. Der JDBC-Benutzername und das JDBC-Kennwort in der Verbindung bestimmen, auf welche Datenbankobjekte der Workflow Zugriff hat.
- Quelldatenpfad — Geben Sie `<database>` je nach `<schema>` `<table>` Datenbankprodukt `<database>`//oder/`<table>` ein. Oracle Database und MySQL unterstützen kein Schema im Pfad. Sie können das Prozentzeichen (%) durch `<schema>` oder `<table>` ersetzen. Geben Sie beispielsweise für eine Oracle-Datenbank mit einem Systembezeichner (SID) von `einorcl`, `orcl/%` um alle Tabellen zu importieren, auf die der in der Verbindung angegebene Benutzer Zugriff hat.

 Important

In diesem Feld wird zwischen Groß- und Kleinschreibung unterschieden. Der Workflow schlägt fehl, wenn die Groß- und Kleinschreibung für eine der Komponenten nicht übereinstimmt.

Wenn Sie eine MySQL-Datenbank angeben, verwendet AWS Glue ETL standardmäßig den `Mysql5-JDBC-Treiber`, sodass My nicht nativ unterstützt SQL8 wird. Sie können das ETL-Jobskript bearbeiten, um einen `customJdbcDriverS3Path` Parameter zu verwenden, wie in [JDBC connectionType Values](#) im AWS Glue Developer Guide beschrieben, um einen anderen JDBC-Treiber zu verwenden, der My unterstützt. SQL8

Wenn Sie aus einer Protokolldatei importieren, stellen Sie sicher, dass die Rolle, die Sie für den Workflow angeben (die „Workflow-Rolle“), über die erforderlichen IAM-Berechtigungen für den Zugriff auf die Datenquelle verfügt. Um beispielsweise AWS CloudTrail Protokolle zu importieren, muss der Benutzer über die `cloudtrail:LookupEvents` Berechtigungen `cloudtrail:DescribeTrails` und verfügen, um die Liste der CloudTrail Protokolle bei der Erstellung des Workflows zu sehen, und die Workflow-Rolle muss über Berechtigungen für den CloudTrail Standort in Amazon S3 verfügen.

5. Führen Sie eine der folgenden Aktionen aus:

- Identifizieren Sie für den Blueprint-Typ Datenbank-Snapshot optional eine Teilmenge der zu importierenden Daten, indem Sie ein oder mehrere Ausschlussmuster angeben. Bei diesen Ausschlussmustern handelt es sich um Muster im UNIX-Stilglob. Sie werden als Eigenschaft der Tabellen gespeichert, die durch den Workflow erstellt werden.

Einzelheiten zu den verfügbaren Ausschlussmustern finden Sie unter [Einschluss- und Ausschlussmuster](#) im AWS Glue Entwicklerhandbuch.

- Geben Sie für den Blueprint-Typ Inkrementelle Datenbank die folgenden Felder an. Fügen Sie für jede zu importierende Tabelle eine Zeile hinzu.

Tabellenname

Zu importierende Tabelle. Muss ausschließlich in Kleinbuchstaben geschrieben werden.

Schlüssel als Lesezeichen speichern

Durch Kommas getrennte Liste von Spaltennamen, die die Lesezeichenschlüssel definieren. Wenn das Feld leer ist, wird der Primärschlüssel verwendet, um neue Daten zu ermitteln. Die Groß- und Kleinschreibung für jede Spalte muss mit der in der Datenquelle definierten Groß- und Kleinschreibung übereinstimmen.

Note

Der Primärschlüssel gilt nur dann als Standardlesezeichenschlüssel, wenn er sequenziell erhöht oder verringert wird (ohne Lücken). Wenn Sie den Primärschlüssel als Lesezeichenschlüssel verwenden möchten und dieser Lücken aufweist, müssen Sie die Primärschlüsselspalte als Lesezeichenschlüssel benennen.

Reihenfolge der Lesezeichen

Wenn Sie Aufsteigend wählen, werden Zeilen mit Werten, die größer sind als die mit den Lesezeichen markierten Werte, als neue Zeilen identifiziert. Wenn Sie Absteigend wählen, werden Zeilen, deren Werte kleiner als die mit der Textmarke markierten Werte sind, als neue Zeilen identifiziert.

Partitionierungsschema

(Optional) Liste der Partitionierungsschlüsselspalten, getrennt durch Schrägstriche (/).
year/month/dayBeispiel:.

Incremental data
Enter tables in the data source to import along with bookmark columns to determine previously imported data.

Table name	Bookmark keys	Bookmark order	Partitioning scheme - optional	
Enter a table name	Enter a bookmark	Choose a sort. ▼	Type partitioning	Remove
Comma-delimited list of bookmark columns.				
Add				

Weitere Informationen finden Sie unter [Verfolgen verarbeiteter Daten mithilfe von Job-Lesezeichen](#) im AWS Glue Entwicklerhandbuch.

6. Geben Sie unter Importziel die Zieldatenbank, den Amazon S3 S3-Zielort und das Datenformat an.

Stellen Sie sicher, dass die Workflow-Rolle über die erforderlichen Lake Formation Formation-Berechtigungen für die Datenbank und den Amazon S3 S3-Zielstandort verfügt.

 Note

Derzeit unterstützen Blueprints die Verschlüsselung von Daten am Ziel nicht.

7. Wählen Sie eine Importhäufigkeit.

Sie können einen cron Ausdruck mit der Option Benutzerdefiniert angeben.

8. Unter Importoptionen:
 - a. Geben Sie einen Workflow-Namen ein.
 - b. Wählen Sie unter Rolle die Rolle ausLakeFormationWorkflowRole, in der Sie sie erstellt haben([Optional](#)) [Erstellen Sie eine IAM-Rolle für Workflows](#).
 - c. Geben Sie optional ein Tabellenpräfix an. Das Präfix wird den Namen der Datenkatalogtabellen vorangestellt, die der Workflow erstellt.
9. Wählen Sie Erstellen und warten Sie, bis die Konsole meldet, dass der Workflow erfolgreich erstellt wurde.

 Tip

Haben Sie die folgende Fehlermeldung erhalten?

User: arn:aws:iam::<account-id>:user/<username> is not authorized to perform: iam:PassRole on resource:arn:aws:iam::<account-id>:role/<rolename>...

Falls ja, überprüfen Sie, ob Sie in allen Policen die AWS Kontonummer durch eine gültige ersetzt <account-id> haben.

 Weitere Informationen finden Sie auch unter:

- [Baupläne und Arbeitsabläufe in Lake Formation](#)

Einen Workflow ausführen

Sie können einen Workflow mit der Lake Formation Formation-Konsole, der AWS Glue Konsole, der AWS Glue Befehlszeilenschnittstelle (AWS CLI) oder der API ausführen.

So führen Sie einen Workflow aus (Lake Formation Formation-Konsole)

1. Öffnen Sie die AWS Lake Formation Konsole unter <https://console.aws.amazon.com/lakeformation/>. Melden Sie sich als Data Lake-Administrator oder als Benutzer mit Data Engineer-Rechten an. Weitere Informationen finden Sie unter [Referenz zu Personas und IAM-Berechtigungen in Lake Formation](#).
2. Wählen Sie im Navigationsbereich die Option Blueprints aus.
3. Wählen Sie auf der Seite Blueprints den Workflow aus. Wählen Sie dann im Menü Aktionen die Option Start aus.
4. Während der Ausführung des Workflows können Sie seinen Fortschritt in der Spalte Status der letzten Ausführung anzeigen. Wählen Sie gelegentlich die Schaltfläche „Aktualisieren“.

Der Status wechselt von LÄUFT zu Wird erkannt, importiert und ist ABGESCHLOSSEN.

Wenn der Workflow abgeschlossen ist:

- Der Datenkatalog enthält neue Metadatentabellen.
- Ihre Daten werden in den Data Lake aufgenommen.

Wenn der Workflow fehlschlägt, gehen Sie wie folgt vor:

- a. Wählen Sie den Workflow aus. Wählen Sie Aktionen und dann Diagramm anzeigen aus.

Der Workflow wird in der AWS Glue Konsole geöffnet.

- b. Wählen Sie den Workflow aus und gehen Sie auf die Registerkarte History (Verlauf).
- c. Wählen Sie unter Verlauf den letzten Lauf aus und klicken Sie auf Laufdetails anzeigen.
- d. Wählen Sie im dynamischen (Laufzeit-) Diagramm einen fehlgeschlagenen Job oder Crawler aus und überprüfen Sie die Fehlermeldung. Fehlgeschlagene Knoten sind entweder rot oder gelb.

 Weitere Informationen finden Sie auch unter:

- [Baupläne und Arbeitsabläufe in Lake Formation](#)

Bringen Sie Ihre Daten in die AWS Glue Data Catalog

Sie können Verbundkataloge im AWS Glue Data Catalog (Datenkatalog) erstellen und Daten über Amazon S3-Data Lakes und Amazon Redshift Redshift-Data Warehouses hinweg vereinheitlichen. Sie können auch Daten aus Ihren Betriebsdatenbanken und Datenquellen von Drittanbietern wie PostgreSQL, Google BigQuery, MySQL und anderen integrieren. Amazon DynamoDB Der Datenkatalog bietet ein zentrales Metadaten-Repository, das die Verwaltung und Erkennung von Daten in unterschiedlichen Systemen erleichtert.

Der Datenkatalog lässt sich über föderierte Konnektoren in über 30 externe Datenquellen integrieren. Mit dieser Integration können Sie Daten aus diesen externen Quellen abfragen, ohne Daten-Pipelines erstellen zu müssen, in die die Daten zuerst aufgenommen werden. AWS

Nachdem Sie die externen Daten katalogisiert haben, können Sie sie verwenden, AWS Lake Formation um die Datenzugriffsberechtigungen im Datenkatalog zentral zu verwalten. Data Lake-Administratoren können anderen IAM-Prinzipalen (Benutzern oder Rollen) innerhalb desselben Kontos oder kontenübergreifend mithilfe von Methoden zur tagbasierten Zugriffskontrolle (LF-Tags) und benannten Ressourcen detaillierte Zugriffsberechtigungen gewähren.

Durch die Verwendung von LF-Tags können Datenadministratoren Ressourcen auf der Grundlage von Attributen wie Domain und Vertraulichkeitsstufe logisch organisieren, wodurch das Berechtigungsmanagement vereinfacht und gleichzeitig konsistente Zugriffskontrollen für Analyse- und Machine-Learning-Dienste wie Athena, Amazon EMR oder Redshift Spectrum gewährleistet werden. AWS Glue

Der Datenkatalog bietet die folgenden Methoden zur Verwaltung von Daten und Berechtigungen für externe Datensätze und externe Metastores:

- Integrieren Sie Amazon S3 S3-Tabellen-Buckets in Data Catalog — Sie können Amazon S3 S3-Tabellen als Datenkatalogobjekte veröffentlichen und katalogisieren und den Katalog über die Lake Formation Konsole oder mithilfe von AWS Glue API-Operationen als Lake Formation Datenspeicherort registrieren.
- Bringen Sie Daten aus Amazon Redshift Redshift-Data Warehouses in den AWS Glue Data Catalog — Registrieren Sie einen vorhandenen [Amazon Redshift Redshift-Namespaces](#) oder einen Cluster mit dem Datenkatalog und erstellen Sie einen mehrstufigen Verbundkatalog im Datenkatalog.

Sie können mit jeder beliebigen Abfrage-Engine, die mit der OpenAPI-Spezifikation des Apache Iceberg REST-Katalogs kompatibel ist, wie Amazon EMR Serverless und Amazon Athena, auf Ihre Daten zugreifen.

- Iceberg RESTRemote-Kataloge mit dem Datenkatalog verbinden — Verbinden Sie Iceberg REST Remote-Kataloge mit dem Datenkatalog und greifen Sie mithilfe von Analyse-Engines sicher auf in Amazon S3 gespeicherte Iceberg Remote-Tabellen zu. AWS
- Aus externen Datenquellen mit dem Datenkatalog verbinden — Verbinden Sie den Datenkatalog mithilfe von AWS Glue Verbindungen mit externen Datenquellen und erstellen Sie Verbundkataloge, um Zugriffsberechtigungen für Datensätze mithilfe von Lake Formation zentral zu verwalten. Eine Migration von Metadaten in den Datenkatalog ist nicht erforderlich.
- Kataloge erstellen, um Amazon Redshift Redshift-Tabellen im Datenkatalog zu verwalten — Möglicherweise haben Sie derzeit weder einen Amazon Redshift Redshift-Producer-Cluster noch einen Amazon Redshift Redshift-Datashare verfügbar, möchten aber Amazon Redshift Redshift-Tabellen mithilfe von Data Catalog erstellen und verwalten. Sie können damit beginnen, einen AWS Glue verwalteten Katalog mithilfe der `glue:CreateCatalog` API-Operation oder der AWS Lake Formation Konsole zu erstellen, indem Sie den Katalogtyp auf `Managed` und `Catalog source` als `Redshift` festlegen.
- Veröffentlichen von Amazon Redshift Redshift-Datenfreigaben mit Data Catalog — Veröffentlichen Sie [Amazon Redshift Redshift-Datenfreigaben](#) in Data Catalog und verwenden Sie Lake Formation, um den Datenzugriff auf Datashares zentral zu verwalten und den Benutzerzugriff einzuschränken.

Sie können Ihre Daten mit Amazon Redshift Spectrum abfragen.

- Datenkatalog Connect externen Hive-Metastores verbinden — Verbinden Sie den Datenkatalog mit externen Metastores, um Zugriffsberechtigungen für Datensätze in Amazon S3 mithilfe von Lake Formation zu verwalten. Eine Migration von Metadaten in den Datenkatalog ist nicht erforderlich.
- Integrieren Sie Lake Formation mit AWS Data Exchange — Lake Formation unterstützt die Lizenzierung des Zugriffs auf Ihre Daten über AWS Data Exchange. Informationen zur Lizenzierung Ihrer Lake Formation Formation-Daten finden Sie unter [Was ist AWS Data Exchange](#) im AWS Data Exchange Benutzerhandbuch enthalten.

Topics

- [Katalogverbund für entfernte Iceberg-Kataloge](#)
- [Überführung Amazon Redshift Redshift-Daten in die AWS Glue Data Catalog](#)
- [Zusammenführung mit externen Datenquellen in der AWS Glue Data Catalog](#)

- [Erstellen eines Amazon S3 Tables-Katalogs in AWS Glue Data Catalog](#)
- [Erstellen eines verwalteten Amazon Redshift Redshift-Katalogs in der AWS Glue Data Catalog](#)
- [Verwaltung von Berechtigungen für Daten in einem Amazon Redshift Redshift-Datashare](#)
- [Verwaltung von Berechtigungen für Datensätze, die externe Metastores verwenden](#)

Katalogverbund für entfernte Iceberg-Kataloge

Catalog Federation in AWS Glue bietet mithilfe AWS von Analyse-Engines direkten und sicheren Zugriff auf Iceberg-Tabellen, die in Amazon S3 gespeichert und in Remote-Katalogen katalogisiert sind. Der Katalogverbund synchronisiert Metadaten zwischen Data Catalog- und Remote-Katalogen, wenn Sie auf Remote-Tabellen zugreifen. Es wird von einer Vielzahl von Analyse-Engines unterstützt, darunter Amazon Redshift, Amazon EMR, Amazon Athena AWS Glue, Engines von Drittanbietern wie Apache Spark und mehr.

Der Katalogverbund kommuniziert mit Remote-Katalogsystemen, um Tabellen zu erkennen, und Lake Formation, um den Zugriff auf Tabellendaten in Amazon S3 zu autorisieren. AWS Glue Data Catalog Wenn Sie eine Verbundtabelle abfragen, ermittelt Data Catalog zum Zeitpunkt der Abfrage die neuesten Tabelleninformationen im Remote-Katalog und ruft den Amazon S3 S3-Speicherort, das aktuelle Schema und die Partitionsinformationen der Tabelle ab. Ihre Analyse-Engine (Amazon Athena, Amazon Redshift, Amazon EMR) verwendet diese Informationen dann, um direkt von Amazon S3 aus auf Iceberg-Datendateien zuzugreifen. Lake Formation verwaltet den Zugriff auf Tabelle (n), indem es bereichsbezogene Anmeldeinformationen für die in Amazon S3 gespeicherten Tabellendaten verkauft, sodass die Engines detaillierte Berechtigungen auf verbundene Tabellen anwenden können.

Funktionen von Catalog Federation

Regiert mit Lake Formation

Bei föderierten Iceberg-Katalogen in Data Catalog handelt es sich um in Lake Formation registrierte Ressourcen, mit denen Sie mithilfe von Lake Formation Formation-Zuschüssen detaillierte Berechtigungen auf Zeilen-, Spalten- und Zellenebene für Iceberg-Tabellen in föderierten Iceberg-Katalogen gewähren können. Föderierte Iceberg-Kataloge und zugehörige Objekte können sicher zwischen Konten gemeinsam genutzt werden. AWS Federated Iceberg-Kataloge funktionieren auch mit der auf Lake Formation Tags basierenden Zugriffskontrolle, sodass Sie die Steuerung mithilfe von Tags skalieren können.

Netzwerkkonfigurationen

Der Katalogverbund unterstützt direkte Verbindungen zu Remote-Katalogquellen mithilfe von Standard-HTTPS-Konnektivität. Es unterstützt auch Konnektivität über Amazon VPC, wenn Sie die Netzwerkisolierung aufrechterhalten möchten, und Konnektivität mithilfe von Proxyunterstützung, wenn Sie eine sichere Kommunikation über Organisations-Firewalls wünschen.

Topics

- [Mit dem Snowflake Iceberg-Katalog verbinden](#)
- [Föderiere zu Databricks Unity Catalog](#)

Mit dem Snowflake Iceberg-Katalog verbinden

AWS Glue Data Catalog verbindet sich mit der Snowflake Verwendung der OAuth2 Anmeldeinformationen eines Dienstprinzipals. Snowflake Sie können diesen Verbund verwenden, um eine Verbindung zu Snowflake Horizon Snowflake Polaris Katalogen herzustellen. Dieser Authentifizierungsmechanismus ermöglicht Data Catalog den Zugriff auf die Metadaten verschiedener Objekte (wie Kataloge, Datenbanken und Tabellen) in Ihrem Katalog, basierend auf den mit dem Dienstprinzipal verknüpften Rechten. Um den Zugriff auf die richtigen Objekte sicherzustellen, ist es wichtig, dem Snowflake Dienstprinzipal die erforderlichen Berechtigungen zum Lesen der Metadaten dieser Objekte zu erteilen.

Voraussetzungen

Bevor Sie in Data Catalog einen Verbundkatalog erstellen, der von Lake Formation verwaltet wird, stellen Sie sicher, dass Sie über die folgenden Berechtigungen verfügen:

Ihr IAM-Prinzipal (Benutzer oder Rolle) muss über die folgenden Berechtigungen verfügen:

- Genehmigungen für Lake Formation —`lakeformation:RegisterResource`,
`lakeformation:DescribeResource`
- AWS Glue Berechtigungen
—`glue:CreateConnection`,`glue:CreateCatalog`,`glue:GetConnection`,
`glue:PassConnection`
- Secrets Manager Manager-Berechtigungen —`secretsmanager:CreateSecret`,
`secretsmanager:GetSecretValue`
- IAM-Berechtigungen —`iam:CreateRole`, `iam:AttachRolePolicy` `iam:PassRole`

Sie müssen ein Lake Formation Data Lake-Administrator sein oder über CREATE_CATALOG Berechtigungen für den Datenkatalog verfügen

Verbundkatalog erstellen

Konsole verwenden

1. Melden Sie sich bei der Konsole an und öffnen Sie die Lake Formation Formation-Konsole unter <https://console.aws.amazon.com/lakeformation/>.
2. Wählen Sie im AWS Seitenbereich oben rechts die bevorzugte Region aus.
3. Wählen Sie im linken Navigationsbereich Kataloge aus.
4. Wählen Sie „Katalog erstellen“, um den Workflow „Katalog erstellen“ zu öffnen.
5. Wählen Sie im Schritt Datenquelle auswählen eine der verfügbaren Optionen Snowflake aus.
6. Im Schritt „Katalogdetails festlegen“ geben Sie drei Informationen an: Katalogdetails, Verbindungsdetails und Registrierungsdetails.
7. Geben Sie im Container mit den Katalogdetails einen eindeutigen Namen für Ihren AWS Glue Verbundkatalog ein und geben Sie den Namen des vorhandenen Snowflake Katalogs ein.
8. Im Container mit den Verbindungsdetails können Sie entweder eine bestehende Verbindung auswählen, auf die Sie Zugriff haben, oder die Konfiguration angeben, um einen neuen Connector zu erstellen.
9. Zu den neuen Verbindungskonfigurationen gehören:
 - Verbindungsname — Ein eindeutiger Name des AWS Glue Verbindungsobjekts.
 - Instanz-URL — Die Endpunkt-URL Ihres bestehenden Snowflake Kontos.
 - Authentifizierung — Geben Sie die Authentifizierungskonfiguration an, die für die Verbindung zum Remote-Katalogserver AWS Glue verwendet wird. AWS Glue unterstützt beides OAuth2 und die benutzerdefinierte Authentifizierung.
 - Token-URL — Geben Sie die URL des Identitätsanbieters des Remote-Katalogs an.
 - OAuth2 Client-ID — Geben Sie die Client-ID der OAuth2 Anmeldeinformationen an, die Ihrem Remote-Katalog zugeordnet sind.
 - Geheim — Speichern und verwenden Sie den geheimen OAuth2 Client-Schlüssel, indem AWS Secrets Manager Sie den geheimen Wert in das Textfeld eingeben. Wenn Sie das Geheimnis manuell in der Konsole eingeben, AWS Glue erstellt es das Geheimnis in Ihrem Namen.
 - Gültigkeitsbereich der Token-URL — Geben Sie den OAuth Bereich für die Authentifizierung an.

- Filter für die Kataloghülle — Wählen Sie aus, ob Objekte in Klein- oder Großbuchstaben aus Ihrem Remote-Katalog in den Datenkatalog übernommen werden sollen.
10. Erstellen Sie eine IAM-Rolle, mit der die AWS Glue Dienstprinzipale von Lake Formation auf geheime Standorte bzw. Amazon S3 S3-Standorte von entfernten Iceberg-Tabellen zugreifen können. AWS Secrets Manager Wählen Sie die IAM-Rolle in der Dropdownliste für die Registrierung aus. Einzelheiten zu den IAM-Richtlinien finden Sie in den Schritten 2 und 3 im folgenden CLI-Abschnitt.
 11. Wählen Sie Verbindung testen aus, um zu testen, ob Ihre Verbindungseigenschaften und der IAM-Rollenzugriff korrekt konfiguriert sind.
 12. Wählen Sie Weiter aus, um Ihre Einstellungen zu überprüfen.
 13. Wählen Sie auf der Überprüfungsseite die Option Katalog erstellen aus.

Verwenden von -CLI

1. Erstellen Sie ein AWS Secrets Manager Geheimnis

Der AWS Glue Connector unterstützt zwei Authentifizierungstypen — OAuth2 und Benutzerdefiniert. Wenn Sie OAuth2 die Option verwenden, verwenden Sie diese Option, AWS Secrets Manager um das Client-Geheimnis des Snowflake Dienstprinzipals zu speichern. Sie werden dieses Geheimnis später beim Erstellen der AWS Glue Verbindung verwenden. Verwenden Sie für die benutzerdefinierte Authentifizierung, AWS Secrets Manager um das Zugriffstoken zu speichern und abzurufen.

Ersetzen Sie im folgenden Beispiel *your-snowflake-secret*, *client_secret*, *region* durch Ihre eigenen Informationen.

```
aws secretsmanager create-secret \
--name your-snowflake-secret \
--description "Snowflake secret" \
--secret-string '{
"USER_MANAGED_CLIENT_APPLICATION_CLIENT_SECRET": "client_secret"
}' \
--region region
```

 Note

USER_MANAGED_CLIENT_APPLICATION_CLIENT_SECRET ist ein reserviertes Schlüsselwort, das AWS Glue verwendet wird, um auf einen geheimen Client-Wert im Secret zu verweisen. Verwenden Sie dasselbe Schlüsselwort, wenn Sie das Geheimnis auch in der Lake Formation Formation-Konsole erstellen.

2. Erstellen Sie eine IAM-Rolle, die dem AWS Glue Verbindungsobjekt Zugriff auf das im vorherigen Schritt erstellte Geheimnis gewährt

Das AWS Glue Verbindungsobjekt benötigt Zugriff auf das AWS Secrets Manager Geheimnis, wenn Sie es AWS Secrets Manager zum Speichern, Abrufen und Aktualisieren Ihres OAuth geheimen Tokens verwenden. Das AWS Glue Verbindungsobjekt benötigt außerdem Zugriff, um die Amazon VPC-Netzwerkschnittstellen zu erstellen, zu beschreiben und zu verwenden, wenn Sie einen Amazon VPC-Endpunkt verwenden, um die Konnektivität zu Ihrem Snowflake Konto einzuschränken.

Erstellen Sie eine IAM-Richtlinie und fügen Sie sie einer IAM-Rolle hinzu. Fügen Sie der Vertrauensrichtlinie AWS Glue einen Dienstprinzipal hinzu.

Ersetzen Sie im folgenden Beispiel *your-secrets-manager-ARN* durch *your-vpc-id*, und *your-subnet-id1* durch Ihre eigenen Informationen.

Example IAM-Richtlinie

```
{
  "Version": "2012-10-17",
  "Statement": [{
    "Effect": "Allow",
    "Action": [
      "secretsmanager:GetSecretValue",
      "secretsmanager:DescribeSecret",
      "secretsmanager:PutSecretValue"
    ],
    "Resource": [
      "your-secrets-manager-ARN"
    ]
  },
  {
    "Effect": "Allow",
```

```

        "Action": [
            "ec2:CreateNetworkInterface",
            "ec2>DeleteNetworkInterface",
            "ec2:DescribeNetworkInterfaces"
        ],
        "Resource": "*",
        "Condition": {
            "ArnEquals": {
                "ec2:Vpc": "arn:aws:ec2:region:account-id:vpc/your-vpc-id",
                "ec2:Subnet": ["arn:aws:ec2:region:account-id:subnet/your-  
subnet-id1"]
            }
        }
    }
}

```

Example Vertrauensrichtlinie

```

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

```

3. Erstellen Sie eine IAM-Richtlinie, die Lake Formation Lesezugriff auf den Amazon S3 S3-Speicherort des Katalogs gewährt

Als Katalogbesitzer eines Verbundkatalogs in Data Catalog verwenden Sie Lake Formation, um Ihren Datenteams einen groben Tabellenzugriff, feinkörnigen Zugriff auf Spalten-, Zeilen- und Zellenebene sowie tagbasierten Zugriff zu gewähren. Lake Formation verwendet eine IAM-Rolle, die ihm Zugriff auf die zugrunde liegenden Amazon S3 S3-Standorte Ihrer entfernten Iceberg-Tabellen gewährt. Dieser Zugriff ermöglicht es Lake Formation, bereichsbezogene Zugangsdaten an Analyse-Engines zu verkaufen, die Remote-Tabellen abfragen.

Erstellen Sie eine IAM-Richtlinie und fügen Sie sie einer IAM-Rolle hinzu. Fügen Sie Lake Formation Service Principal zur Rollenvertrauensrichtlinie hinzu.

Ersetzen Sie im folgenden Beispiel *amzn-s3-demo-bucketN* und *your-kms-key* durch Ihre eigenen Informationen.

Example IAM-Richtlinie

```
{
  "Version": "2012-10-17",
  "Statement": [{
    "Effect": "Allow",
    "Action": [
      "s3:GetObject"
    ],
    "Resource": [
      "arn:aws:s3:::amzn-s3-demo-bucket1/*",
      "arn:aws:s3:::amzn-s3-demo-bucket2/*"
    ]
  },
  {
    "Effect": "Allow",
    "Action": [
      "s3:ListBucket"
    ],
    "Resource": [
      "arn:aws:s3:::amzn-s3-demo-bucket1",
      "arn:aws:s3:::amzn-s3-demo-bucket2"
    ]
  },
  {
    "Effect": "Allow",
    "Action": [
      "kms:Decrypt",
      "kms:Encrypt"
    ],
    "Resource": [
      "your-kms-key"
    ]
  }
]
```

Example Vertrauensrichtlinie

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

Note

Wenn Sie die Lake Formation Formation-Konsole verwenden, um einen Verbundkatalog zu erstellen, verwendet die Konsole eine einzige IAM-Rolle, an die beide Richtlinien angehängt sind, um die Einrichtung abzuschließen.

4. Erstellen Sie ein Verbindungsobjekt AWS Glue

AWS Glue Connector unterstützt OAuth2 und benutzerdefinierte Authentifizierungsmethoden. Das Datenkatalog-Verbindungsobjekt unterstützt eine CATALOG_CASING_FILTER Konfiguration, mit der Sie Objekte in Klein- oder Großbuchstaben in Ihrem Remote-Katalog in Data Catalog übernehmen können.

Das folgende Beispiel verwendet die OAuth2 Authentifizierungskonfiguration, um eine AWS Glue Verbindung herzustellen. *highlighted sections* Ersetzen Sie es durch Ihre Informationen.

```
aws glue create-connection \
  --connection-input '{
    "Name": "your-glue-connection-to-snowflake-account",
    "ConnectionType": "SNOWFLAKEICEBERGRESTCATALOG",
    "ConnectionProperties": {
      "INSTANCE_URL": "your-snowflake-account-URL",
      "ROLE_ARN": "your-IAM-role-for-secrets-and-VPC-access",
      "CATALOG_CASING_FILTER": "LOWERCASE_ONLY"
    },
    "AuthenticationConfiguration": {
```



```

    "AuthenticationType": "OAUTH2",
    "OAuth2Properties": {
      "OAuth2GrantType": "CLIENT_CREDENTIALS",
      "TokenUrl": "your-internal-or-external-token-server-url",
      "OAuth2ClientApplication": {
        "UserManagedClientApplicationClientId": "our-client-id"
      },
      "TokenUrlParametersMap": {
        "scope": "all-apis"
      }
    },
    "SecretArn": "arn:aws:secretsmanager:your-aws-region:your-aws-account-id:secret:snowflake-secret"
  }
}'

```

5. AWS Glue Verbindung als Lake Formation Formation-Ressource registrieren

Mithilfe des AWS Glue Verbindungsobjekts (erstellt in Schritt 4) und der IAM-Rolle (erstellt in Schritt 3) können Sie das AWS Glue Verbindungsobjekt jetzt als von Lake Formation verwaltete Ressource registrieren.

Ersetzen Sie *your-glue-connector-arn* und *your-IAM-role-ARN-having-LF-access* durch Ihre Informationen.

```

aws lakeformation register-resource \
  --resource-arn your-glue-connector-arn \
  --role-arn your-IAM-role-ARN-having-LF-access \
  --with-federation \
  --with-privileged-access

```

6. Erstellen Sie einen Verbundkatalog im Datenkatalog

Nachdem Sie ein AWS Glue Verbindungsobjekt erstellt und bei Lake Formation registriert haben, können Sie im Datenkatalog einen Verbundkatalog erstellen:

Geben Sie dem Verbundkatalog einen eindeutigen Namen unter *your-federated-catalog-name*, verweisen Sie unter *at* auf den Katalog und geben Sie den Verbindungsnamen ein *catalog-name-in-Snowflake*, der zuvor Snowflake unter erstellt wurde. *your-glue-connection-name*

```

aws glue create-catalog \

```

```
--name your-federated-catalog-name \
--catalog-input '{
  "FederatedCatalog": {
    "Identifier": catalog-name-in-Snowflake,
    "ConnectionName": your-glue-connection-name"
  },
  "CreateTableDefaultPermissions": [],
  "CreateDatabaseDefaultPermissions": []
}'
```

Überlegungen bei der Integration mit Snowflake

- Wenn Sie Ressourcen (wie Datenbanken und Tabellen) ablegen Snowflake, widerruft Lake Formation nicht automatisch die für diese Verbundressource erteilten Berechtigungen. Um die Zugriffsberechtigungen zu entfernen, müssen Sie die Berechtigungen, die zuvor mithilfe von Lake Formation für die Verbundressource gewährt wurden, explizit widerrufen.
- Wenn Sie den Remote-Katalog mit `CATALOG_CASING_FILTER='UPPERCASE_ONLY'` Konfiguration bereitstellen, werden Datenbanken und Tabellen mit Bezeichnern in Großbuchstaben zusammengefasst, Objekte mit Kleinbuchstaben jedoch nicht.
- Sie können dieselbe AWS Glue Verbindung wiederverwenden, um mehrere Verbundkataloge zu erstellen. Durch das Löschen eines Katalogs wird die zugehörige Verbindung nicht gelöscht. Um eine Verbindung zu löschen, verwenden Sie bitte den AWS `aws glue delete-connection` CLI-Befehl und stellen Sie sicher, dass zuerst alle zugehörigen Kataloge gelöscht werden.
- Verschachtelte Namespaces im Polaris Katalog werden nicht unterstützt. Das heißt, der Katalogverbund kann auf entfernte Iceberg Tabellen zugreifen, die einer dreiteiligen Notation folgen. `catalog.database.table`

Föderiere zu Databricks Unity Catalog

AWS Glue Data Catalog verbindet sich Databricks mit der Verwendung der OAuth2 Anmeldeinformationen eines Dienstprinzipals. Databricks Dieser Authentifizierungsmechanismus ermöglicht den AWS Glue Data Catalog Zugriff auf die Metadaten verschiedener Objekte (wie Kataloge, Datenbanken und Tabellen) auf der Grundlage der Databricks Unity Catalog dem Dienstprinzipal zugewiesenen Berechtigungen. Um den Zugriff auf die richtigen Objekte sicherzustellen, ist es wichtig, dem Dienstprinzipal die erforderlichen Berechtigungen Databricks zum Lesen der Metadaten dieser Objekte zu gewähren.

Als Nächstes ermöglicht der Katalogverbund die Erkennung und Abfrage von Iceberg Tabellen in Ihrem Databricks Unity-Katalog. Um Delta-Tabellen lesen zu können, stellen Sie bitte sicher, dass Iceberg Metadaten für diese Tabellen mit verfügbar sind. Uniform Folgen Sie dem Databricks Tutorial und der Dokumentation, um den Service Principal und die zugehörigen Rechte in Ihrem Databricks Workspace zu erstellen.

Voraussetzungen

Bevor Sie in Data Catalog einen Verbundkatalog erstellen, der von Lake Formation verwaltet wird, stellen Sie sicher, dass Sie über die folgenden Berechtigungen verfügen:

Ihr IAM-Prinzipal (Benutzer oder Rolle) muss über die folgenden Berechtigungen verfügen:

- Genehmigungen für Lake Formation —`lakeformation:RegisterResource`,
`lakeformation:DescribeResource`
- AWS Glue Berechtigungen
—`glue:CreateConnection`,`glue:CreateCatalog`,`glue:GetConnection`,
`glue:PassConnection`
- Secrets Manager Manager-Berechtigungen —`secretsmanager:CreateSecret`,
`secretsmanager:GetSecretValue`
- IAM-Berechtigungen —`iam:CreateRole`, `iam:AttachRolePolicy` `iam:PassRole`

Sie müssen ein Lake Formation Data Lake-Administrator sein oder über `CREATE_CATALOG` Berechtigungen für den Datenkatalog verfügen

Verbundkatalog erstellen

Konsole verwenden

1. Melden Sie sich bei der Konsole an und öffnen Sie die Lake Formation Konsole unter <https://console.aws.amazon.com/lakeformation/>.
2. Wählen Sie im AWS Seitenbereich oben rechts die bevorzugte Region aus.
3. Wählen Sie im linken Navigationsbereich Kataloge aus.
4. Wählen Sie „Katalog erstellen“, um den Workflow „Katalog erstellen“ zu öffnen.
5. Wählen Sie im Schritt Datenquelle auswählen eine der verfügbaren Optionen Databricks aus.
6. Im Schritt „Katalogdetails festlegen“ geben Sie drei Informationen an: Katalogdetails, Verbindungsdetails und Registrierungsdetails.

7. Geben Sie im Container mit den Katalogdetails einen eindeutigen Namen für Ihren AWS Glue Verbundkatalog ein und geben Sie den Namen des vorhandenen Databricks Katalogs ein.
8. Im Container mit den Verbindungsdetails können Sie entweder eine bestehende Verbindung auswählen, auf die Sie Zugriff haben, oder die Konfiguration angeben, um einen neuen Connector zu erstellen.
9. Zu den neuen Verbindungskonfigurationen gehören:
 - Verbindungsname — Ein eindeutiger Name des AWS Glue Verbindungsobjekts.
 - Workspace-URL — Die Endpunkt-URL Ihres vorhandenen Databricks Workspace.
 - Authentifizierung — Geben Sie die Authentifizierungskonfiguration an, die für die Verbindung zum Remote-Katalogserver AWS Glue verwendet wird. AWS Glue unterstützt beides OAuth2 und die benutzerdefinierte Authentifizierung.
 - Token-URL — Geben Sie die URL des Identitätsanbieters des Remote-Katalogs an.
 - OAuth2 Client-ID — Geben Sie die Client-ID der OAuth2 Anmeldeinformationen an, die Ihrem Remote-Katalog zugeordnet sind.
 - Geheim — Speichern und verwenden Sie den geheimen OAuth2 Client-Schlüssel, indem AWS Secrets Manager Sie den geheimen Wert in das Textfeld eingeben. Wenn Sie das Geheimnis manuell in der Konsole eingeben, AWS Glue erstellt es das Geheimnis in Ihrem Namen.
 - Gültigkeitsbereich der Token-URL — Geben Sie den OAuth Bereich für die Authentifizierung an.
10. Erstellen Sie eine IAM-Rolle, mit der die AWS Glue Dienstprinzipale von Lake Formation auf geheime Standorte bzw. Amazon S3 S3-Standorte von Iceberg Remote-Tabellen zugreifen können. Wählen Sie die IAM-Rolle in der Dropdownliste für die Registrierung aus. Einzelheiten zu den IAM-Richtlinien finden Sie in den Schritten 2 und 3 im folgenden CLI-Abschnitt.
11. Wählen Sie Verbindung testen aus, um zu testen, ob Ihre Verbindungseigenschaften und der IAM-Rollenzugriff korrekt konfiguriert sind. Die Testverbindungsfunktion ist nicht verfügbar, wenn Databricks Sie eine Verbindung mit Amazon VPC herstellen.
12. Wählen Sie Weiter, um Ihre Einstellungen zu überprüfen.
13. Wählen Sie auf der Überprüfungsseite die Option Katalog erstellen aus.

Verwenden von -CLI

1. Erstellen Sie ein AWS Secrets Manager Geheimnis

Der AWS Glue Connector unterstützt zwei Authentifizierungstypen — OAuth2 und Benutzerdefiniert. Wenn Sie OAuth2 die Option verwenden, verwenden Sie diese Option, AWS Secrets Manager um das Client-Geheimnis des Databricks Dienstprinzipals zu speichern. Sie werden dieses Geheimnis später verwenden, wenn Sie die AWS Glue Verbindung erstellen. Verwenden Sie für die benutzerdefinierte Authentifizierung, AWS Secrets Manager um das Zugriffstoken zu speichern und abzurufen.

Ersetzen Sie im folgenden Beispiel `<databricks-secret>`, `<client_secret>`, `<region>` durch Ihre eigenen Informationen.

```
aws secretsmanager create-secret \
--name <databricks-secret> \
--description "Databricks secret" \
--secret-string '{
"USER_MANAGED_CLIENT_APPLICATION_CLIENT_SECRET": "<client_secret>"
}' \
--region <region>
```

Note

USER_MANAGED_CLIENT_APPLICATION_CLIENT_SECRET ist ein reserviertes Schlüsselwort, das AWS Glue verwendet wird, um auf einen geheimen Client-Wert im Secret zu verweisen. Verwenden Sie dasselbe Schlüsselwort, wenn Sie das Geheimnis auch in der Lake Formation Formation-Konsole erstellen.

2. Erstellen Sie eine IAM-Rolle, die dem AWS Glue Verbindungsobjekt Zugriff auf das im vorherigen Schritt erstellte Geheimnis gewährt

Das AWS Glue Verbindungsobjekt benötigt Zugriff auf das AWS Secrets Manager Geheimnis, wenn Sie es AWS Secrets Manager zum Speichern, Abrufen und Aktualisieren Ihres OAuth geheimen Tokens verwenden. Das AWS Glue Verbindungsobjekt benötigt außerdem Zugriff, um die Amazon VPC-Netzwerkschnittstellen zu erstellen, zu beschreiben und zu verwenden, wenn Sie einen Amazon VPC-Endpunkt verwenden, um die Konnektivität zu Ihrem Databricks Workspace einzuschränken.

Erstellen Sie eine IAM-Richtlinie und fügen Sie sie einer IAM-Rolle hinzu. Fügen Sie der Vertrauensrichtlinie AWS Glue einen Dienstprinzipal hinzu.

Ersetzen Sie im folgenden Beispiel *<your-secrets-manager-ARN>*, und *<your-subnet-id1>* durch Ihre eigenen Informationen.

Example IAM-Richtlinie

```
{
  "Version": "2012-10-17",
  "Statement": [{
    "Effect": "Allow",
    "Action": [
      "secretsmanager:GetSecretValue",
      "secretsmanager:DescribeSecret",
      "secretsmanager:PutSecretValue"
    ],
    "Resource": [
      "<your-secrets-manager-ARN>"
    ]
  },
  {
    "Effect": "Allow",
    "Action": [
      "ec2:CreateNetworkInterface",
      "ec2:DeleteNetworkInterface",
      "ec2:DescribeNetworkInterfaces"
    ],
    "Resource": "*",
    "Condition": {
      "ArnEquals": {
        "ec2:Vpc": "arn:aws:ec2:region:account-id:vpc/<your-vpc-id>",
        "ec2:Subnet": ["arn:aws:ec2:region:account-id:subnet/<your-
subnet-id1>"]
      }
    }
  }
]
```

Example Vertrauensrichtlinie

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

```

    "Effect": "Allow",
    "Principal": {
        "Service": "glue.amazonaws.com"
    },
    "Action": "sts:AssumeRole"
  ]
}

```

3. Erstellen Sie eine IAM-Richtlinie, die Lake Formation Lesezugriff auf den Amazon S3 S3-Speicherort des Katalogs gewährt

Als Katalogbesitzer eines Verbundkatalogs in Data Catalog verwenden Sie Lake Formation, um Ihren Datenteams einen groben Tabellenzugriff, feinkörnigen Zugriff auf Spalten-, Zeilen- und Zellenebene sowie tagbasierten Zugriff zu gewähren. Lake Formation verwendet eine IAM-Rolle, die ihm Zugriff auf die zugrunde liegenden Amazon S3 S3-Standorte Ihrer entfernten Iceberg-Tabellen gewährt. Dieser Zugriff ermöglicht es Lake Formation, bereichsbezogene Zugangsdaten an Analyse-Engines zu verkaufen, die Remote-Tabellen abfragen.

Erstellen Sie eine IAM-Richtlinie und fügen Sie sie einer IAM-Rolle hinzu. Fügen Sie Lake Formation Service Principal zur Vertrauensrichtlinie für IAM-Rollen hinzu.

Ersetzen Sie im folgenden Beispiel *<your-s3-bucket-N>* und *<your-kms-key>* durch Ihre eigenen Informationen.

Example IAM-Richtlinie

```

{
  "Version": "2012-10-17",
  "Statement": [{
    "Effect": "Allow",
    "Action": [
      "s3:GetObject"
    ],
    "Resource": [
      "arn:aws:s3:::<your-s3-bucket-1>/*",
      "arn:aws:s3:::<your-s3-bucket-2>/*"
    ]
  },
  {
    "Effect": "Allow",
    "Action": [
      "s3:ListBucket"
    ]
  }
]
}

```

```

    ],
    "Resource": [
        "arn:aws:s3:::<your-s3-bucket-1>",
        "arn:aws:s3:::<your-s3-bucket-2>"
    ]
  },
  {
    "Effect": "Allow",
    "Action": [
        "kms:Decrypt",
        "kms:Encrypt"
    ],
    "Resource": [
        "<your-kms-key>"
    ]
  }
]
}

```

Example Vertrauensrichtlinie

```

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

```

Note

Wenn Sie die Lake Formation Formation-Konsole verwenden, um einen Verbundkatalog zu erstellen, verwendet die Konsole eine einzige IAM-Rolle, an die beide Richtlinien angehängt sind, um die Einrichtung abzuschließen.

4. Erstellen Sie ein Verbindungsobjekt AWS Glue

Data Catalog unterstützt connectionType: DATABRICKSICEBERGRESTCATALOG für die Verbindung von Data Catalog mit. Databricks Dieser AWS Glue Connector unterstützt OAuth2 benutzerdefinierte Authentifizierungsmethoden.

Das folgende Beispiel verwendet die OAuth2 Authentifizierungskonfiguration, um eine AWS Glue Verbindung herzustellen. *highlighted sections* Ersetzen Sie es durch Ihre Informationen.

```
aws glue create-connection \
  --connection-input '{
    "Name": "<your-glue-connection-to-databricks-unity-account>",
    "ConnectionType": "DATABRICKSICEBERGRESTCATALOG",
    "ConnectionProperties": {
      "INSTANCE_URL": "<your-databricks-workspace-catalog-URL>",
      "ROLE_ARN": "<your-IAM-role-for-secrets-and-VPC-access>"
    },
    "AuthenticationConfiguration": {
      "AuthenticationType": "OAUTH2",
      "OAuth2Properties": {
        "OAuth2GrantType": "CLIENT_CREDENTIALS",
        "TokenUrl": "<your-internal-or-external-token-server-url>",
        "OAuth2ClientApplication": {
          "UserManagedClientApplicationClientId": "<your-client-id>"
        },
        "TokenUrlParametersMap": {
          "scope": "all-apis"
        }
      },
      "SecretArn": "arn:aws:secretsmanager:<aws-region>:<your-aws-account-id>:secret:<databricks-secret>"
    }
  }'
```

5. AWS Glue Verbindung als Lake Formation Formation-Ressource registrieren

Mithilfe des AWS Glue Verbindungsobjekts (erstellt in Schritt 4) und der IAM-Rolle (erstellt in Schritt 3) können Sie das AWS Glue Verbindungsobjekt jetzt als von Lake Formation verwaltete Ressource registrieren.

Ersetzen Sie *<your-glue-connector-arn>* und *<your-IAM-role-ARN-having-LF-access>* durch Ihre Informationen.

```
aws lakeformation register-resource \
  --resource-arn <your-glue-connector-arn> \
  --role-arn <your-IAM-role-ARN-having-LF-access> \
  --with-federation \
  --with-privileged-access
```

6. Erstellen Sie einen Verbundkatalog im Datenkatalog

Nachdem Sie ein AWS Glue Verbindungsobjekt erstellt und bei Lake Formation registriert haben, können Sie im Datenkatalog einen Verbundkatalog erstellen:

Geben Sie dem Verbundkatalog einen eindeutigen Namen unter *<your-federated-catalog-name>*, verweisen Sie unter *at* auf den Katalog und geben Sie den Verbindungsnamen ein "*<catalog-name-in-Databricks>*", der zuvor Databricks unter erstellt wurde. "*<your-glue-connection-name>*"

```
aws glue create-catalog \
  --name <your-federated-catalog-name> \
  --catalog-input '{
    "FederatedCatalog": {
      "Identifier": "<catalog-name-in-Databricks>",
      "ConnectionName": "<your-glue-connection-name>"
    },
    "CreateTableDefaultPermissions": [],
    "CreateDatabaseDefaultPermissions": []
  }'
```

Überlegungen bei der Integration mit Databricks

- Wenn Sie Ressourcen (wie Datenbanken und Tabellen) in der löschen Databricks, widerruft Lake Formation nicht automatisch die für diese Verbundressource erteilten Berechtigungen. Um die Zugriffsberechtigungen zu entfernen, müssen Sie die Berechtigungen, die zuvor mithilfe von Lake Formation für die Verbundressource gewährt wurden, explizit widerrufen.
- Mit dieser Integration können Sie in Amazon S3 gespeicherte Iceberg-Tabellen abfragen. Wenn Sie ein anderes Tabellenformat oder Objektspeicher verwenden, können Sie Metadaten in Remote-Katalogen mit den zugehörigen Datenbanken und Tabellen verbinden AWS Glue und diese auflisten, aber Abfrageoperationen wie schlagen bei Abfragen mit dem Fehler „Tabelle

konnte nicht gelesen `SELECT ColumnFoo from TableBar` werden“ fehl. Apache Iceberg Der Objektspeicherort wird nicht unterstützt. '

- Sie können dieselbe AWS Glue Verbindung wiederverwenden, um mehrere Verbundkataloge zu erstellen. Durch das Löschen eines Katalogs wird das zugehörige Verbindungsobjekt nicht gelöscht. Um ein Verbindungsobjekt zu löschen, verwenden Sie bitte den AWS `aws glue delete-connection` CLI-Befehl und stellen Sie sicher, dass zuerst alle zugehörigen Kataloge gelöscht werden.

Überführung Amazon Redshift Redshift-Daten in die AWS Glue Data Catalog

Sie können Analysedaten in Amazon Redshift Redshift-Data Warehouses im AWS Glue Data Catalog (Datenkatalog) verwalten und Amazon S3-Data Lakes und Amazon Redshift Redshift-Data Warehouses vereinheitlichen. Amazon Redshift ist ein vollständig verwalteter Data-Warehouse-Service im Petabyte-Bereich in der Cloud. AWS Ein Amazon-Redshift-Data-Warehouse ist eine Sammlung von Datenverarbeitungsressourcen, den so genannten Knoten, die zu Gruppen, den so genannten Clustern, zusammengefasst werden. In jedem Cluster wird eine Amazon-Redshift-Engine ausgeführt, und er enthält mindestens eine Datenbank.

In Amazon Redshift können Sie von Amazon Redshift bereitgestellte Cluster und serverlose Namespaces erstellen und diese im Datenkatalog registrieren. Auf diese Weise können Sie Daten in Amazon Redshift Managed Storage (RMS) und Amazon S3 S3-Buckets vereinheitlichen und auf Daten von Apache Iceberg-kompatiblen Analyse-Engines zugreifen.

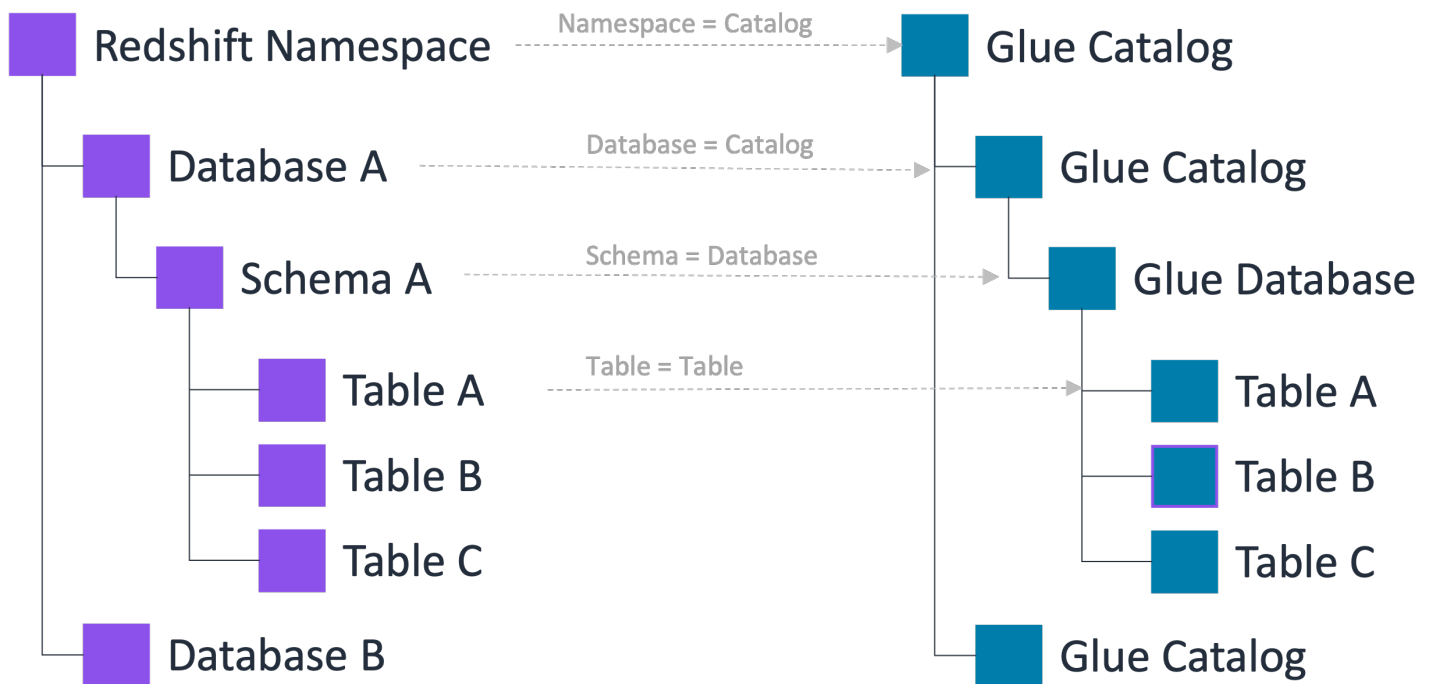
Durch die Registrierung von Namespaces und Clustern können Sie Zugriff auf Daten gewähren, ohne sie kopieren oder verschieben zu müssen. Weitere Informationen zur Registrierung von Clustern und Namespaces in Amazon Redshift finden Sie unter [Registrierung von Amazon Redshift Redshift-Clustern](#) und Namespaces in der. AWS Glue Data Catalog

In Amazon Redshift können Sie Daten über Datashares oder durch die Registrierung von Namespaces und Clustern bei Data Catalog gemeinsam nutzen. Bei Datashares, die auf der Ebene einzelner Datenbankobjekte betrieben werden, müssen Sie die gemeinsame Nutzung für jede Tabelle oder Ansicht aktivieren. Im Gegensatz dazu funktioniert die Veröffentlichung von Namespaces auf Cluster- oder Namespace-Ebene. Wenn Sie einen Cluster oder Namespace im Datenkatalog registrieren, werden alle darin enthaltenen Datenbanken und Tabellen automatisch gemeinsam genutzt, ohne dass Sie die gemeinsame Nutzung für einzelne Objekte konfigurieren müssen.

Im Datenkatalog können Sie für jeden Namespace oder Cluster einen Verbundkatalog erstellen. Ein Katalog wird als Verbundkatalog bezeichnet, wenn er auf eine Entität außerhalb des Datenkatalogs verweist. Tabellen und Ansichten im Amazon Redshift Redshift-Namespace werden als einzelne Tabellen im Datenkatalog aufgeführt. Sie können Datenbanken und Tabellen im Verbundkatalog mit ausgewählten IAM-Prinzipalen und SAML-Benutzern innerhalb desselben Kontos oder in einem anderen Konto mit Lake Formation teilen. Sie können auch Zeilen- und Spaltenfilterausdrücke verwenden, um den Zugriff auf bestimmte Daten einzuschränken. Weitere Informationen finden Sie unter [Datenfilterung und Sicherheit auf Zellebene in Lake Formation](#).

Der Datenkatalog unterstützt eine dreistufige Metadatenhierarchie, die Kataloge, Datenbanken und Tabellen (und Ansichten) umfasst. Wenn Sie einen Namespace beim Datenkatalog registrieren, wird die Amazon Redshift Redshift-Datenhierarchie der dreistufigen Hierarchie des Datenkatalogs wie folgt zugeordnet:

- Der Amazon Redshift Redshift-Namespace wird zu einem mehrstufigen Katalog im Datenkatalog.
- Die zugehörige Amazon Redshift Redshift-Datenbank ist als Katalog im Datenkatalog registriert.
- Das Amazon Redshift Redshift-Schema wird zu einer Datenbank im Datenkatalog.
- Die Amazon Redshift Redshift-Tabelle wird zu einer Tabelle im Datenkatalog.



Mit dieser dreistufigen Metadatenhierarchie können Sie auf Amazon Redshift Redshift-Tabellen zugreifen, indem Sie die dreiteilige Notation „catalog1/catalog2.database.table“ im Datenkatalog verwenden. Außerdem können Datenteams dieselbe Organisation beibehalten, die Amazon Redshift für die Organisation von Tabellen innerhalb des Data Catalog-Kontos verwendet.

In Lake Formation können Sie die Daten von Amazon Redshift mithilfe einer detaillierten Zugriffskontrolle für die Datenkatalogressourcen sicher verwalten. Mit dieser Integration können Sie analytische Daten aus einem einzigen Katalog mit einem gemeinsamen Zugriffskontrollmechanismus verwalten, sichern und abfragen.

Einschränkungen finden Sie unter [Einschränkungen beim Einbringen von Amazon Redshift Data Warehouse-Daten in die AWS Glue Data Catalog](#).

Themen

- [Wichtigste Vorteile](#)
- [Rollen und Zuständigkeiten](#)
- [Voraussetzungen für die Verwaltung von Amazon Redshift Redshift-Namespaces in AWS Glue Data Catalog](#)
- [Erstellen von Amazon Redshift Redshift-Verbundkatalogen](#)
- [Katalogobjekte anzeigen](#)
- [Aktualisierung eines Verbundkatalogs](#)
- [Zugreifen auf einen gemeinsam genutzten Verbundkatalog](#)
- [Löschen eines Verbundkatalogs](#)
- [Verbundkataloge abfragen](#)
- [Weitere Ressourcen](#)

Wichtigste Vorteile

Die Registrierung von Amazon Redshift Redshift-Clustern und -Namespaces mit den AWS Glue Data Catalog und die Vereinheitlichung von Daten in Amazon S3 S3-Data Lakes und Amazon Redshift Redshift-Data Warehouses bietet die folgenden Vorteile:

- Einheitliches Abfrageerlebnis — Fragen Sie Ihre von Amazon Redshift verwalteten Daten und Daten in den Amazon S3 S3-Buckets mit einer beliebigen mit Apache Iceberg kompatiblen Abfrage-Engine ab, z. B. Amazon EMR Serverless und Amazon Athena, ohne Daten verschieben oder kopieren zu müssen.

- **Konsistenter Datenzugriff für alle Services** — Sie müssen Datenbank- und Tabellennamen in Ihren Daten-Pipelines nicht aktualisieren, wenn Sie von verschiedenen AWS Analysediensten aus auf dieselben föderierten Datenquellen zugreifen, da die Datenquellen im Datenkatalog registriert sind.
- **Präzise Zugriffskontrolle** — Sie können Lake Formation Berechtigungen anwenden, um den Zugriff auf die Verbunddatenquellen mithilfe detaillierter Zugriffssteuerungsberechtigungen zu verwalten.

Rollen und Zuständigkeiten

Rolle	Verantwortung
Clusteradministrator für Amazon Redshift Producer	Registriert den Cluster oder Namespace im Datenkatalog.
Administrator von Lake Formation für den Data Lake	Nimmt die Cluster- oder Namespace-Einladung an, erstellt Verbundkataloge und gewährt anderen Prinzipalen Zugriff auf die Verbundkataloge.
Lake Formation Administrator (nur lesbar)	Erkennt den Verbundkatalog und fragt Amazon Redshift Redshift-Tabellen im Verbundkatalog ab.
Rolle bei der Datenübertragung	Amazon Redshift übernimmt in Ihrem Namen die Übertragung von Daten zum und vom Amazon S3 S3-Bucket.

Im Folgenden sind die wichtigsten Schritte aufgeführt, um Benutzern Zugriff auf einen Amazon Redshift Redshift-Namespace zu gewähren:

1. In Amazon Redshift registriert der Producer-Cluster-Administrator einen Cluster oder Namespace im Datenkatalog.
2. Der Data Lake-Administrator akzeptiert die Namespace-Einladung vom Amazon Redshift Producer-Cluster-Administrator und erstellt einen Verbundkatalog im Datenkatalog.

Nach Abschluss dieses Schritts können Sie den Amazon Redshift Redshift-Namespaces-Katalog im Datenkatalog verwalten.

3. Erteilen Sie Benutzern Berechtigungen für Kataloge, Datenbanken und Tabellen. Sie können den gesamten Namespace-Katalog oder eine Teilmenge von Tabellen für Benutzer desselben Kontos oder eines anderen Kontos gemeinsam nutzen.

Voraussetzungen für die Verwaltung von Amazon Redshift Redshift-Namespaces in AWS Glue Data Catalog

1. Einen Data Lake-Administrator erstellen — Erstellen Sie eine IAM-Rolle, die autorisiert ist, die Namespace-Einladung anzunehmen, die AWS Glue Data Catalog Objekte (Kataloge, Datenbanken, Tabellen/Ansichten) zu erstellen und anderen Benutzern Lake Formation Formation-Berechtigungen zu gewähren.

step-by-stepAnweisungen zum Erstellen eines Data Lake-Administrators finden Sie unter. [Erstellen Sie einen Data Lake-Administrator](#)

2. Aktualisieren Sie die Data Lake-Administratorberechtigungen.

Zusätzlich zu den Data Lake-Administratorberechtigungen benötigt der Data Lake-Administrator die folgenden Berechtigungen, um eine Amazon Redshift Redshift-Namespaces-Einladung in Lake Formation anzunehmen, die Data Catalog-Ressourcen zu erstellen oder zu aktualisieren und den Data Lake-Zugriff zu aktivieren:

JSON

```
{
  "Version": "2012-10-17",
  "Id": "glue-enable-datalake-access",
  "Statement": [{
    "Effect": "Allow",
    "Action": [
      "redshift:AssociateDataShareConsumer",
      "redshift:DescribeDataSharesForConsumer",
      "redshift:DescribeDataShares",
      "redshift-serverless:CreateNamespace",
      "redshift-serverless:CreateWorkgroup",
      "redshift-serverless>DeleteNamespace",
```

```

        "redshift-serverless:DeleteWorkgroup",
        "ec2:DescribeAccountAttributes",
        "ec2:DescribeSubnets",
        "ec2:DescribeSecurityGroups",
        "ec2:DescribeAvailabilityZones",
        "s3:createBucket",
        "s3:deleteBucket",
        "s3:putBucketPolicy",
        "s3:putEncryptionConfiguration",
        "s3:putLifecycleConfiguration",
        "s3:putBucketVersioning",
        "iam:CreateRole"
    ],
    "Resource": "*"
},
{
    "Action": [
        "iam:PassRole"
    ],
    "Effect": "Allow",
    "Resource": "arn:aws:iam::*:role/data transfer role name",
    "Condition": {
        "StringLike": {
            "iam:PassedToService": [
                "glue.amazonaws.com"
            ]
        }
    }
}
]
}

```

3. Wenn es sich bei der IAM-Rolle, die für die Erstellung von Verbundkatalogen verwendet wird, nicht um einen Data Lake-Administrator handelt, müssen Sie der Rolle die entsprechende Berechtigung erteilen. Create catalog

Um Ersteller von Katalogen zu erstellen

- a. Öffnen Sie die Lake Formation Formation-Konsole unter <https://console.aws.amazon.com/lakeformation/>.
- b. Wählen Sie unter Administration die Option Administrative Rollen und Aufgaben aus.
- c. Wählen Sie Grant (Erteilen).

- d. Wählen Sie auf dem Bildschirm Berechtigungen gewähren einen IAM-Benutzer oder eine IAM-Rolle aus.
- e. Wählen Sie „Katalogberechtigung erstellen“ aus.
- f. Optional können Sie auch die erteilbare Berechtigung „Katalog erstellen“ erteilen. Die erteilbare Berechtigung ermöglicht es dem Ersteller des Katalogs, die `Create catalog` Berechtigung anderen Hauptbenutzern zu erteilen.
- g. Wählen Sie Grant (Erteilen).

AWS CLI Beispiel für die Erteilung von Berechtigungen zur Erstellung eines Verbundkatalogs.

```
aws lakeformation grant-permissions \
--cli-input-json \
'{
  "Principal": {
    "DataLakePrincipalIdentifier": "arn:aws:iam::123456789012:role/Admin"
  },
  "Resource": {
    "Catalog": {
    }
  },
  "Permissions": [
    "CREATE_CATALOG",
    "DESCRIBE"
  ]
}'
```

4. Erstellen Sie eine Administratorrolle mit Schreibschutz, um die Amazon Redshift-Verbundkataloge im Datenkatalog von Amazon Redshift Query Editor v2 zu finden.

Um die Amazon Redshift-Tabellen im Verbundkatalog von Amazon Redshift Query Editor v2 aus abzufragen, stellen Sie sicher, dass die Administrator-Rollenrichtlinie Schreibgeschützt den ARN für die mit dem Amazon Redshift Service verknüpfte Rolle- enthält. `AWSServiceRoleForRedshift`

```
aws lakeformation put-data-lake-settings
  --region us-east-1 \
  --data-lake-settings \
  '{
```

```
"DataLakeAdmins": [{"DataLakePrincipalIdentifier":"arn:aws:iam::123456789012:role/Admin"}],
  "ReadOnlyAdmins":[{"DataLakePrincipalIdentifier":"arn:aws:iam::123456789012:role/aws-service-role/redshift.amazonaws.com/AWSServiceRoleForRedshift"}],
  "CreateDatabaseDefaultPermissions":[],
  "CreateTableDefaultPermissions":[],
  "Parameters":{"CROSS_ACCOUNT_VERSION":"4","SET_CONTEXT":"TRUE"}
}'
```

- Erstellen Sie eine Datenübertragungsrolle, die Amazon Redshift in Ihrem Namen übernehmen kann, um Daten zum und vom Amazon S3 S3-Bucket zu übertragen.

Wenn Sie den Data Lake-Zugriff für Apache Iceberg-kompatible Abfrage-Engines wie Athena, Amazon EMR auf Amazon EC2 aktivieren, um auf die Amazon Redshift Redshift-Ressourcen im Datenkatalog zuzugreifen, müssen Sie eine IAM-Rolle mit den erforderlichen Berechtigungen für die Datenübertragung zum und vom Amazon S3 S3-Bucket erstellen.

JSON

```
{
  "Version":"2012-10-17",
  "Id": "glue-enable-datalake-access",
  "Statement": [{
    "Sid": "DataTransferRolePolicy",
    "Effect": "Allow",
    "Action": [ "glue:GetCatalog",
                "glue:GetDatabase",
                "kms:GenerateDataKey",
                "kms:Decrypt"],
    "Resource": "*"
  }]
}
```

- Fügen Sie der Datenübertragungsrolle für AWS Glue und Amazon Redshift Redshift-Services die folgende Vertrauensrichtlinie hinzu, um die Rolle für die Übertragung von Daten zum und vom Amazon S3 S3-Bucket zu übernehmen.

JSON

```

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

```

7. Fügen Sie dem Schlüssel die folgende Schlüsselrichtlinie hinzu, wenn Sie einen vom AWS KMS Kunden verwalteten Schlüssel verwenden, um die Daten im Amazon Redshift Redshift-Cluster/ Namespace zu verschlüsseln. Ersetzen Sie die Kontonummer durch eine gültige Kontonummer und geben Sie den AWS Namen der Datenübertragungsrolle an. Standardmäßig werden die Daten im Amazon Redshift Redshift-Cluster mit einem KMS-Schlüssel verschlüsselt. Lake Formation bietet die Möglichkeit, Ihren benutzerdefinierten KMS-Schlüssel für die Verschlüsselung zu erstellen. Wenn Sie einen vom Kunden verwalteten Schlüssel verwenden, müssen Sie dem Schlüssel bestimmte Schlüsselrichtlinien hinzufügen.

Weitere Informationen zum Verwalten von Berechtigungen eines kundenseitig verwalteten Schlüssels finden Sie unter [Kundenseitig verwaltete Schlüssel](#).

JSON

```

{
  "Version": "2012-10-17",
  "Id": "auto-redshift-3",
  "Statement": [{
    "Sid": "RedshiftAllowAccessPolicy",
    "Effect": "Allow",
    "Principal": {
      "AWS": "*"
    },
    "Action": [
      "kms:Encrypt",
      "kms:Decrypt",
      "kms:ReEncrypt*",

```

```

        "kms:GenerateDataKey*",
        "kms:CreateGrant",
        "kms:DescribeKey"
    ],
    "Resource": "*",
    "Condition": {
        "StringEquals": {
            "kms:CallerAccount": "111122223333",
            "kms:ViaService": "redshift.us-east-1.amazonaws.com"
        }
    }
},
{
    "Sid": "RedshiftServerlessAllowAccessPolicy",
    "Effect": "Allow",
    "Principal": {
        "AWS": "*"
    },
    "Action": [
        "kms:Encrypt",
        "kms:Decrypt",
        "kms:ReEncrypt*",
        "kms:GenerateDataKey*",
        "kms:CreateGrant",
        "kms:DescribeKey"
    ],
    "Resource": "*",
    "Condition": {
        "StringEquals": {
            "kms:CallerAccount": "111122223333",
            "kms:ViaService": "redshift-serverless.us-
east-1.amazonaws.com"
        }
    }
},
{
    "Sid": "DirectMetadataAccess",
    "Effect": "Allow",
    "Principal": {
        "AWS": "arn:aws:iam::111122223333:root"
    },
    "Action": [
        "kms:Describe*",
        "kms:Get*",

```

```

        "kms:List*",
        "kms:RevokeGrant"
    ],
    "Resource": "*"
  },
  {
    "Sid": "GenerateDataKeyDecryptDataTransferRole",
    "Effect": "Allow",
    "Principal": {
      "AWS": "arn:aws:iam::111122223333:role/data-transfer-role-name"
    },
    "Action": [
      "kms:GenerateDataKey",
      "kms:Decrypt"
    ],
    "Resource": "*",
    "Condition": {
      "StringEquals": {
        "kms:ViaService": "s3.us-east-1.amazonaws.com"
      }
    }
  }
]
}

```

Erstellen von Amazon Redshift Redshift-Verbundkatalogen

In diesem Thema werden die Schritte beschrieben, die Sie ausführen müssen, um eine Cluster- oder Namespace-Einladung anzunehmen, einen Verbundkatalog mit mehreren Ebenen zu erstellen und anderen Prinzipalen Berechtigungen zu erteilen. Sie können diese Aufgaben mit der Lake Formation Formation-Konsole, dem AWS Command Line Interface (AWS CLI) oder APIs/ausführenSDKs. Die Beispiele in diesem Thema zeigen den Producer-Cluster/-Namespace, den Datenkatalog und den Datenverbraucher in demselben Konto.

Weitere Informationen zu den kontoübergreifenden Funktionen von Lake Formation finden Sie unter [Kontoübergreifender Datenaustausch in Lake Formation](#).

So verwalten Sie einen Amazon Redshift Redshift-Namespace im Datenkatalog

1. Überprüfen Sie eine Namespace-Einladung und akzeptieren Sie sie.

Console

1. Melden Sie sich bei der Lake Formation Formation-Konsole als Data Lake-Administrator unter an <https://console.aws.amazon.com/lakeformation/>. Navigieren Sie unter Datenkatalog zur Seite Kataloge.
2. Überprüfen Sie die Namespace-Einladung, auf die Sie zugreifen dürfen. In der Spalte Status wird Ihr aktueller Teilnahmestatus für den Namespace angezeigt. Der Status Nicht akzeptiert gibt an, dass Sie dem Namespace hinzugefügt wurden, ihn aber noch nicht akzeptiert oder die Einladung abgelehnt haben.

The screenshot displays the AWS Lake Formation console interface. At the top, there's a 'Catalogs' section with links for 'How it works', 'Create a catalog', 'Manage catalog permissions', and 'Access from query editors'. Below this is a banner for 'Create a federated catalog for your S3 Table Buckets' with an 'Enable S3 Table integration' button. The main content area is divided into two sections: 'Pending catalog invitations (4)' and 'Catalogs (1)'. The 'Pending catalog invitations' section shows a table with four entries, each representing a namespace invitation with details like Name, Source account ID, Received date, and Status (all marked as 'Accepted, catalog not created'). The 'Catalogs' section shows a single entry for the 'Default' catalog.

Name	Source account ID	Received	Status
arn:aws:redshift-serverless:us-east-2:451785580005:namespace:c0381d75-3f21-49f2-b2c3-44d000803a71		November 20, 2024 at 10:16 PM UTC	Accepted, catalog not created
arn:aws:redshift-serverless:us-east-2:451785580005:namespace/4a798b4c-71d8-4df4-b77f-52cff8ac80a1		November 20, 2024 at 5:38 PM UTC	Accepted, catalog not created
arn:aws:redshift:us-east-2:451785580005:namespace:48a491a6-d5d8-415b-b5b2-3832a4affb08		November 26, 2024 at 3:45 PM UTC	Accepted, catalog not created
arn:aws:redshift:us-east-2:451785580005:namespace:a77f139c-5a19-4b53-a662-c2f50db2fc28		December 3, 2024 at 2:21 PM UTC	Accepted, catalog not created

Name	Type	Source	Owner account...	Shared resource	Shared resour...	Shared resource owner region
Default	Default	Default catalog	-	-	-	-

3. Um auf eine Namespace- oder Cluster-Einladung zu antworten, wählen Sie den Namen der Einladung aus und klicken Sie auf Einladung überprüfen. Überprüfen Sie unter Einladung annehmen oder ablehnen die Einladungsdetails. Wählen Sie Annehmen, um die Einladung anzunehmen, oder Ablehnen, um die Einladung abzulehnen. Sie erhalten keinen Zugriff auf den Namespace, wenn Sie die Einladung ablehnen.

AWS CLI

Die folgenden Beispiele zeigen, wie Sie die Einladung anzeigen, annehmen und registrieren können. Ersetzen Sie die AWS-Konto ID durch eine gültige AWS-Konto ID. Ersetzen Sie das `data-share-arn` durch den tatsächlichen Amazon-Ressourcennamen (ARN), der auf den Namespace verweist.

1. Eine ausstehende Einladung anzeigen.

```
aws redshift describe-data-shares \
  --data-share-arn 'arn:aws:redshift:us-
east-1:123456789012:datashare:abcd1234-1234-ab12-cd34-1a2b3c4d5e6f/
ds_internal_namespace' \
```

2. Nehmen Sie eine Einladung an.

```
aws redshift associate-data-share-consumer \
  --data-share-arn 'arn:aws:redshift:us-
east-1:123456789012:datashare:abcd1234-1234-ab12-cd34-1a2b3c4d5e6f/
ds_internal_namespace' \
  --consumer-arn 'arn:aws:glue:us-east-1:123456789012:catalog'
```

3. Registrieren Sie den Cluster oder Namespace im Lake Formation Konto.

Verwenden Sie den [RegisterResource](#) API-Vorgang, um den Datashare in Lake Formation zu registrieren. `DataShareArn` ist der Eingabeparameter für `ResourceArn`

Note

Dies ist ein obligatorischer Schritt.

```
aws lakeformation register-resource \
  --resource-arn 'arn:aws:redshift:us-
east-1:123456789012:datashare:abcd1234-1234-ab12-cd34-1a2b3c4d5e6f/
ds_internal_namespace'
```

2. Erstellen Sie einen Verbundkatalog.

Nachdem Sie eine Einladung angenommen haben, müssen Sie im Datenkatalog einen Verbundkatalog erstellen, der die Objekte im Amazon Redshift Redshift-Namespaces dem Datenkatalog zuordnet. Sie müssen ein Data Lake-Administrator oder ein Benutzer oder eine Rolle sein, der über die erforderlichen Berechtigungen zum Erstellen eines Katalogs verfügt.

Console

1. Nachdem Sie die Namespace-Einladung akzeptiert haben, wird die Seite Katalogdetails festlegen angezeigt.
2. Geben Sie auf der Seite „Katalogdetails festlegen“ einen eindeutigen Namen für den Katalog ein. Verwenden Sie Kleinbuchstaben für Katalognamen. Katalognamen müssen weniger als oder gleich 255 Zeichen lang sein. Sie verwenden diesen Bezeichner für die interne Zuordnung des Namespaces in der Metadatenhierarchie (CatalogID.DBName.Schema.Table).
3. Geben Sie eine Beschreibung für den Katalog ein. Die Beschreibung muss weniger als oder gleich 2048 Zeichen lang sein.
4. Aktivieren Sie als Nächstes das Kontrollkästchen Zugriff auf diesen Katalog von Iceberg-kompatiblen Engines, um den Zugriff auf die Amazon Redshift Redshift-Ressourcen mithilfe von Apache Iceberg-kompatiblen Analyse-Engines wie Athena und Apache Spark auf Amazon EMR zu ermöglichen.

Sie müssen den Data-Lake-Zugriff nicht aktivieren, um mit Amazon Redshift auf die Verbundkataloge zuzugreifen.

Catalog details

A catalog is the top level in the Data Catalog's three-level data hierarchy and contains Data Catalog objects.

Name

Catalog name is required, in lowercase characters, and no longer than 255 characters.

Type

Federated

Source

Redshift

Description - optional

Descriptions can be up to 2048 characters long.

Access from engines

You can access this catalog from open source engines as well as Amazon Redshift.

☒ Access this catalog from Iceberg compatible engines.

Choose this option to access the data catalog using with Apache Spark running on an EMR cluster.

IAM role

Role used by Redshift for loading data to and from S3 bucket that is created for the managed workgroup.



[View](#)

[Create an IAM role](#)

Encryption options

Your data is encrypted by default with a key that AWS owns and manages for you. To choose a different key, customize your encryption settings.

☐ Customize encryption settings

To use the default key, clear this option.

[Cancel](#)

[Skip to Review and create](#)

[Next](#)

5. Damit diese Abfrage-Engines in Amazon Redshift-Namespaces lesen und schreiben können, AWS Glue wird ein verwalteter Amazon Redshift Redshift-Cluster mit den Rechen- und Speicherressourcen erstellt, die für Lese- und Schreibvorgänge erforderlich sind, ohne die Amazon Redshift Data Warehouse-Workloads zu beeinträchtigen.

Sie müssen auch eine IAM-Rolle mit den Berechtigungen bereitstellen, die für die Übertragung von Daten zum und vom Amazon S3 S3-Bucket erforderlich sind.

6. Standardmäßig werden die Daten im Amazon Redshift Redshift-Cluster mit einem AWS verwalteten Schlüssel verschlüsselt. Lake Formation bietet die Möglichkeit, Ihren benutzerdefinierten KMS-Schlüssel für die Verschlüsselung zu erstellen. Wenn Sie einen vom Kunden verwalteten Schlüssel verwenden, müssen Sie dem Schlüssel bestimmte Schlüsselrichtlinien hinzufügen.

Wählen Sie die Verschlüsselungseinstellungen anpassen, wenn Sie einen vom Kunden verwalteten Schlüssel verwenden, um die Daten im Amazon Redshift Redshift-Cluster/ Namespace zu verschlüsseln. Um einen benutzerdefinierten Schlüssel zu verwenden, müssen Sie Ihrem KMS-Schlüssel eine zusätzliche benutzerdefinierte Richtlinie für verwaltete Schlüssel hinzufügen. Weitere Informationen finden Sie unter [Voraussetzungen für die Verwaltung von Amazon Redshift Redshift-Namespace in AWS Glue Data Catalog](#).

AWS CLI

Verwenden Sie den folgenden Beispielcode, um einen Katalog mit den Amazon Redshift Redshift-Daten zu erstellen, die mithilfe von im AWS CLI Datenkatalog veröffentlicht wurden.

```
aws glue create-catalog
--cli-input-json \
'{
  "Name": "nscatalog",
  "CatalogInput": {
    "Description": "Redshift federated catalog",
    "CreateDatabaseDefaultPermissions" : [],
    "CreateTableDefaultPermissions": [],
    "FederatedCatalog": {
      "Identifier": "arn:aws:redshift:us-
east-1:123456789012:datashare:11524d7f-f56d-45fe-83f7-d7bb0a4d6d71/
ds_internal_namespace",
      "ConnectionName": "aws:redshift"
    },
    "CatalogProperties": {
      "DataLakeAccessProperties" : {
        "DataLakeAccess" : true,
        "DataTransferRole" :
"arn:aws:iam::123456789012:role/DataTransferRole"
      }
    }
  }
}'
```

3. Erteilen Sie Benutzern in Ihrem Konto oder in externen Konten Berechtigungen.

AWS-Managementkonsole

1. Wählen Sie Weiter, um anderen Benutzern Berechtigungen für die gemeinsam genutzten Kataloge, Datenbanken und Tabellen zu gewähren.
2. Wählen Sie auf dem Bildschirm „Berechtigungen hinzufügen“ die Hauptbenutzer und die Berechtigungstypen aus, die Sie gewähren möchten.

Add permissions

Principals

Choose the principals to grant permissions.

☒ **IAM users and roles**
Users or roles from this AWS account.

☐ **SAML users and groups**
SAML users and group or QuickSight ARNs.

☐ **External accounts**
AWS account, AWS organization or IAM principal outside of this account

IAM users and roles

Add one or more IAM users or roles.

Choose IAM principals to add

UserRole X
Role

Catalog permissions

Choose the permissions to grant on the catalog. Choosing Super user overwrites individual permissions, granting unrestricted administrative access.

☐ **Super user**
A super user has unrestricted administrative privileges to perform any operation on all resources within the catalog (databases, tables, and views).

Catalog permissions

Choose specific access permissions to grant.

☒ **Create database**
☐ **Describe**
☐ **Alter**

☐ **Drop**

☐ **Super**
This permission is the union of all the individual permissions to the left, and supersedes them.

Grantable permissions

Choose the permission that can be granted to others.

☒ **Create database**
☐ **Describe**
☐ **Alter**

☐ **Drop**

☐ **Super**
This permission allows the principal to grant any of the permissions to the left, and supersedes those grantable permissions.

Cancel

Add

a. Wählen Sie im Abschnitt Prinzipale einen Prinzipaltyp aus und geben Sie dann Prinzipale an, denen Berechtigungen erteilt werden sollen.

- IAM-Benutzer und -Rollen – wählen Sie mindestens einen Benutzer oder eine Rolle aus der Liste der IAM-Benutzer und -Rollen aus.

Erstellen von Amazon Redshift Redshift-Verbundkatalogen

410

- SAML-Benutzer und -Gruppen — Geben Sie für SAML und Amazon Quick Benutzer und Gruppen einen oder mehrere Amazon-Ressourcennamen (ARNs) für Benutzer oder Gruppen ein, die über SAML verbunden sind, oder ARNs für Amazon Quick-Benutzer oder -Gruppen. Drücken Sie nach jedem ARN die Eingabetaste.

Informationen zur Erstellung der Befehle finden Sie unter Befehle AWS CLI gewähren ARNs und widerrufen. AWS CLI

- Externe Konten — Geben Sie für AWS, AWS Organisation oder IAM-Principal ein oder mehrere gültige AWS Konten IDs, Organisationen IDs, Organisationseinheiten IDs oder ARN für den IAM-Benutzer oder die IAM-Rolle ein. Drücken Sie nach jeder ID die Eingabetaste. Eine Organisations-ID besteht aus „o-“, gefolgt von 10—32 Kleinbuchstaben oder Ziffern. Eine Organisationseinheits-ID beginnt mit „ou-“, gefolgt von 4—32 Kleinbuchstaben oder Ziffern (der ID des Stammes, der die Organisationseinheit enthält). Auf diese Zeichenfolge folgen ein zweiter Gedankenstrich „-“ und 8 bis 32 zusätzliche Kleinbuchstaben oder Ziffern.
- b. Wählen Sie im Abschnitt Berechtigungen die Berechtigungen und erteilbare Berechtigungen aus.

Wählen Sie unter Katalogberechtigungen mindestens eine Berechtigung aus, die Sie gewähren möchten. Wählen Sie unter Erteilbare Berechtigungen die Berechtigungen aus, die der Zuschussempfänger anderen Hauptbenutzern in seinem Konto gewähren kann. AWS Diese Option wird nicht unterstützt, wenn Sie einem IAM-Prinzipal von einem externen Konto aus Berechtigungen gewähren.

Wählen Sie Superuser aus, um dem Benutzer uneingeschränkte Berechtigungen für die Ressourcen (Datenbanken, Tabellen, Ansichten) innerhalb des Katalogs zu gewähren.

3. Wählen Sie Hinzufügen aus.

AWS CLI

Verwenden Sie die folgenden Beispiele, um Katalog-, Datenbank- und Tabellenberechtigungen zu gewähren, indem Sie: AWS CLI

- Das folgende Beispiel zeigt, wie Berechtigungen für den Verbundkatalog erteilt werden.

```
aws lakeformation grant-permissions
--cli-input-cli-json \
```

```
{
  "Principal": {
    "DataLakePrincipalIdentifier": "arn:aws:iam::123456789012:role/
non-admin"
  },
  "Resource": {
    "Catalog": {
      "Id": "123456789012:nscatalog"
    }
  },
  "Permissions": [
    "DESCRIBE", "CREATE_CATALOG"
  ],
  "PermissionsWithGrantOption": [
  ]
}
```

- Verwenden Sie das folgende Beispiel, um Berechtigungen für eine Datenbank zu erteilen.

```
aws lakeformation grant-permissions \
  --cli-input-json \
  '{
    "Principal": {

      "DataLakePrincipalIdentifier": "arn:aws:iam::123456789012:role/non-admin"
    },
    "Resource": {
      "Database": {
        "CatalogId": "123456789012:nscatalog/dev",
        "Name": "public"
      }
    },
    "Permissions": [
      "ALL"
    ]
  }'
```

- Das folgende Beispiel zeigt, wie Berechtigungen für eine Tabelle in der Amazon Redshift Redshift-Datenbank erteilt werden.

```
aws lakeformation grant-permissions \
  --cli-input-json \
  '{
```

```

    "Principal": {
      "DataLakePrincipalIdentifier": "arn:aws:iam::123456789012:role/non-admin",
      "Resource": {
        "Table": {
          "CatalogId": "123456789012:nscatalog2/dev",
          "DatabaseName": "public",
          "TableWildcard" : {}
        }
      },
      "Permissions": [
        "ALL"
      ]
    }
  }

```

4. Wählen Sie Weiter, um die Katalogdetails zu überprüfen und einen Verbundkatalog zu erstellen. Der neu erstellte Verbundkatalog und die Katalogobjekte werden auf der Seite Kataloge angezeigt.

Mit wird auf einen Amazon Redshift Redshift-Verbundkatalog verwiesen. catalogID = 123456789012:Redshift-federated catalog id

Katalogobjekte anzeigen

Nachdem Sie den Verbundkatalog erstellt haben, können Sie die Objekte im Katalog mit der Lake Formation Formation-Konsole oder AWS CLI anzeigen.

AWS-Managementkonsole

1. Öffnen Sie die Lake Formation Formation-Konsole unter <https://console.aws.amazon.com/lakeformation/>.
2. Wählen Sie unter Datenkatalog die Option Kataloge aus.
3. Wählen Sie einen Verbundkatalog aus der Liste auf der Seite Kataloge aus.
4. Auf der Seite mit der Katalogübersicht werden die Katalogobjekte (Datenbanken und Tabellen) angezeigt, für die Sie Berechtigungen haben. Auf der Registerkarte „Berechtigungen“ werden die IAM-Prinzipale angezeigt, denen Berechtigungen für diese Objekte erteilt wurden.

AWS CLI

- Das folgende AWS CLI Beispiel zeigt, wie der Katalog der obersten Ebene angefordert wird.

```
aws glue get-catalog \  
--catalog-id 123456789012:nscatalog
```

Antwort

```
{  
  "Catalog": {  
    "CatalogId": "123456789012:nscatalog",  
    "Name": "nscatalog",  
    "ResourceArn": "arn:aws:glue:us-east-1:123456789012:catalog/nscatalog",  
    "Description": "Redshift published Catalog",  
    "CreateTime": "2024-09-05T14:49:16-07:00",  
    "FederatedCatalog": {  
      "Identifier": "arn:aws:redshift:us-east-1:123456789012:datashare:b1234589-e823-4a14-ad8e-077085540a50/ds_internal_namespace",  
      "ConnectionName": "aws:redshift"  
    },  
    "CatalogProperties": {  
      "DataLakeAccessProperties": {  
        "DataLakeAccess": true,  
        "DataTransferRole": "arn:aws:iam::123456789012:role/DataTransferRole",  
        "KmsKey": "AWS_OWNED_KMS_KEY",  
        "ManagedWorkgroupName": "123456789012:nscatalog",  
        "ManagedWorkgroupStatus": "AVAILABLE",  
        "RedshiftDatabaseName": "dev"  
      },  
      "CatalogIdentifier": "e2309c2c2fb048f1a3069dfdc1c7883e",  
      "CreateTableDefaultPermissions": [],  
      "CreateDatabaseDefaultPermissions": []  
    }  
  }  
}
```

- Das folgende Beispiel zeigt, wie alle Kataloge im Konto angefordert werden.

```
aws glue get-catalogs \  

```



```
--recursive
```

- Die folgende Beispielanforderung zeigt, wie Sie einen Amazon Redshift Redshift-Katalog auf Datenbankebene abrufen.

```
aws glue get-catalog \  
--catalog-id 123456789012:namespace catalog name/redshift database name
```

- Die folgende Beispielanforderung zeigt, wie die Datenbanken im Amazon Redshift Redshift-Katalog auf Datenbankebene abgerufen werden.

```
aws glue get-databases \  
--catalog-id 123456789012:namespace catalog name/redshift database name
```

- Die folgende Beispielanforderung zeigt, wie Sie eine Amazon Redshift Redshift-Tabelle in den Katalog aufnehmen können.

```
aws glue get-table \  
--catalog-id 123456789012:parent catalog name/redshift database \  
--database-name redshift schema name \  
--name table name
```

- Das folgende Beispiel zeigt, wie Sie alle Tabellen aus der Amazon Redshift Redshift-Datenbank abrufen.

```
aws glue get-tables \  
--catalog-id 123456789012:namespace catalog name/redshift database name \  
--database-name RS schema name
```

Aktualisierung eines Verbundkatalogs

Sie können einen Amazon Redshift Redshift-Verbundkatalog im Datenkatalog mithilfe der Lake Formation Formation-Konsole, der AWS CLI oder der [UpdateCatalog](#) API-Operation aktualisieren.

AWS-Managementkonsole

Gehen Sie wie folgt vor, um Ihren Verbundkatalog mit der Lake Formation Console zu aktualisieren.

1. Melden Sie sich bei an AWS-Managementkonsole und öffnen Sie die Lake Formation Formation-Konsole unter <https://console.aws.amazon.com/lakeformation/>.
2. Wählen Sie im linken Navigationsbereich unter Datenkatalog die Option Kataloge aus.
3. Wählen Sie auf der Seite Kataloge den Amazon Redshift Redshift-Verbundkatalog aus, den Sie aktualisieren möchten.
4. Wählen Sie unter Aktionen die Option Bearbeiten aus.
5. Wählen Sie auf dem Bildschirm „Katalogdetails festlegen“ im Abschnitt „Zugriff über Engines“ die Option Auf diesen Katalog von Iceberg-kompatiblen Engines zugreifen aus. Wenn Sie diese Option aktivieren, wird der Zugriff auf den Data Lake für Apache Iceberg-kompatible Abfrage-Engines aktiviert.
6. Erstellen Sie als Nächstes eine neue IAM-Rolle oder wählen Sie eine bestehende IAM-Rolle aus, die über die Richtlinie verfügt, die Berechtigungen zur Durchführung von Datenübertragungen zum und vom Amazon S3 S3-Bucket gewährt.

Weitere Informationen zu Berechtigungen finden Sie unter. [Voraussetzungen für die Verwaltung von Amazon Redshift Redshift-Namespaces in AWS Glue Data Catalog](#)

7. Standardmäßig werden Ihre Daten im Amazon Redshift Redshift-Cluster mit einem Von AWS verwalteter Schlüssel verschlüsselt. Wenn Sie Daten mit einem vom Kunden verwalteten Schlüssel verschlüsseln möchten, erstellen Sie entweder einen KMS-Schlüssel oder wählen Sie einen vorhandenen Schlüssel mit den [Voraussetzungen für die Verwaltung von Amazon Redshift Redshift-Namespaces in AWS Glue Data Catalog](#) im Abschnitt definierten Berechtigungen aus.
8. Wählen Sie Speichern.

Nach erfolgreichem Abschluss wird auf der Seite mit den Katalogdetails der Name der verwalteten Arbeitsgruppe mit dem Status „Erfolgreich“ angezeigt.

AWS CLI

Im Folgenden finden Sie ein Beispiel für die `update-catalog` CLI-Eingabe mit deaktiviertem Data Lake-Zugriff, indem Sie den `DataLakeAaccess` Parameterwert auf `festlegenfalse` festlegen.

```
aws glue update-catalog --cli-input-json \  
'{  
  "Name": "nscatalog",  
  "CatalogInput": {  
    "Description": "Redshift published catalog",
```

```

    "CreateDatabaseDefaultPermissions" : [],
    "CreateTableDefaultPermissions": [],
    "FederatedCatalog": {
        "Identifier": "arn:aws:redshift:us-
east-1:123456789012:datashare:11524d7f-f56d-45fe-83f7-d7bb0a4d6d71/
ds_internal_namespace",
        "ConnectionName": "aws:redshift"
    },
    "CatalogProperties": {
        "DataLakeAccessProperties" : {
            "DataLakeAccess" : false
        }
    }
}
}'

```

Zugreifen auf einen gemeinsam genutzten Verbundkatalog

AWS Lake Formation Kontoübergreifende Funktionen ermöglichen Benutzern die sichere gemeinsame Nutzung verteilter Data Lakes über mehrere AWS-Konto AWS Unternehmen, Organisationen oder direkt mit IAM-Prinzipalen in einem anderen Konto, wodurch ein detaillierter Zugriff auf die Metadaten und die zugrunde liegenden Daten ermöglicht wird.

Lake Formation verwendet den Dienst AWS Resource Access Manager (AWS RAM), um die gemeinsame Nutzung von Ressourcen zu erleichtern. Wenn Sie eine Katalogressource mit einem anderen Konto teilen, AWS RAM sendet es eine Einladung an das Konto des Empfängers, den Ressourcenzuschuss anzunehmen oder abzulehnen.

Integrierte Analysedienste wie Amazon Athena und Redshift Spectrum benötigen Ressourcenlinks, um gemeinsam genutzte Ressourcen in Abfragen einbeziehen zu können. Principals müssen einen Ressourcenlink zu AWS Glue Data Catalog einer gemeinsam genutzten Ressource von einer anderen erstellen. AWS-Konto Weitere Informationen zu Ressourcenlinks finden Sie unter [Funktionsweise von Ressourcenlinks in Lake Formation](#).

Ein Katalog-Link-Container ist ein Datenkatalog-Objekt, das auf einen lokalen oder kontoübergreifenden Verbundkatalog auf Datenbankebene von anderen Konten aus verweist. AWS Sie können auch Datenbank-Links und Tabellenlinks innerhalb eines Katalog-Link-Containers erstellen. Wenn Sie einen Datenbank-Link oder einen Tabellen-Link erstellen, müssen Sie eine Zielressource angeben, die sich unter demselben Amazon Redshift Redshift-Zielkatalog auf Datenbankebene (Amazon Redshift Redshift-Datenbank) befindet.

Um einen Katalog-Link-Container zu erstellen, benötigen Sie die Lake Formation `CREATE_CATALOG` oder die `glue:CreateCatalog` Genehmigung.

Für die gemeinsame Nutzung von Datenbanken oder Tabellen im Verbundkatalog zwischen AWS-Konto s müssen Sie über die kontoübergreifende Version der Einstellungen Version 4 oder höher verfügen.

Erstellen eines Katalog-Link-Containers zu einem kontoübergreifenden Verbundkatalog

Sie können einen Katalog-Link-Container erstellen, der auf einen Verbundkatalog auf Redshift-Datenbankebene in einer beliebigen AWS Region verweist, indem Sie die AWS Lake Formation Konsole, die AWS Glue `CreateCatalog` API oder () verwenden. AWS Command Line Interface
AWS CLI

So erstellen Sie einen Katalog-Link-Container zu einem gemeinsam genutzten Katalog (Konsole)

1. Öffnen Sie die AWS Lake Formation Konsole unter <https://console.aws.amazon.com/lakeformation/>. Melden Sie sich als Schulleiter an, der über die `CREATE_CATALOG` Genehmigung für Lake Formation verfügt.
2. Wählen Sie im Navigationsbereich Kataloge und dann Katalog erstellen aus.
3. Geben Sie auf der Seite „Katalogdetails festlegen“ die folgenden Informationen ein:

Name

Geben Sie einen Namen ein, der denselben Regeln entspricht wie ein Katalogname. Der Name kann mit dem Namen des gemeinsam genutzten Zielkatalogs identisch sein.

Typ

Wählen Sie Katalog-Link-Container als Katalogtyp aus.

Quelle

Wählen Sie Redshift.

Redshift-Katalog von Target

Wählen Sie einen Verbundkatalog auf Redshift-Datenbankebene oder wählen Sie einen lokalen (eigenen) Katalog aus der Liste aus.

Die Liste enthält alle Kataloge, die mit Ihrem Konto geteilt wurden. Beachten Sie, dass die Konto-ID des Katalogbesitzers in jedem Katalog aufgeführt ist. Wenn Sie keinen Katalog sehen, von dem Sie wissen, dass er mit Ihrem Konto geteilt wurde, überprüfen Sie Folgendes:

- Wenn Sie kein Data Lake-Administrator sind, überprüfen Sie, ob der Data Lake-Administrator Ihnen Lake Formation-Berechtigungen für den Katalog erteilt hat.
- Wenn Sie ein Data Lake-Administrator sind und sich Ihr Konto nicht in derselben AWS Organisation wie das gewährende Konto befindet, stellen Sie sicher, dass Sie die Einladung AWS Resource Access Manager (AWS RAM) zur gemeinsamen Nutzung von Ressourcen für den Katalog akzeptiert haben. Weitere Informationen finden Sie unter [Annahme einer Einladung zur gemeinsamen Nutzung von Ressourcen AWS RAM](#).

 Note

Beim Erstellen eines Katalog-Link-Containers über die Konsole wird möglicherweise das Drop-down-Menü Target Redshift Catalog angezeigt, No matches wenn Sie versuchen, einen kontoübergreifenden Redshift-Katalog auszuwählen. Trotz dieser Anzeige können Sie den Ziel-ARN des Amazon Redshift Redshift-Katalogs auf Datenbankebene (Amazon Redshift Redshift-Datenbank) manuell in das Eingabefeld eingeben, und das Formular funktioniert trotzdem korrekt. Beispiel: `arn:aws:glue:us-east-1:123456789012:catalog/federated-catalog-redshift/dev`.

Dieses Verhalten tritt auf, weil die Konsole nur innerhalb des aktuell angemeldeten Kontos nach potenziellen Kandidaten suchen kann. Das Drop-down-Menü ist als automatische Vervollständigungsfunktion vorgesehen, aber Sie können es ARNs für den kontoübergreifenden Zugriff immer noch manuell eingeben.

4. Damit Apache Iceberg-Abfrage-Engines Lese- und Schreibvorgänge in Amazon Redshift-Namespaces durchführen können, AWS Glue wird ein verwalteter Amazon Redshift Redshift-Cluster mit den Rechen- und Speicherressourcen erstellt, die für Lese- und Schreibvorgänge erforderlich sind, ohne die Amazon Redshift Data Warehouse-Workloads zu beeinträchtigen. Sie müssen eine IAM-Rolle mit den Berechtigungen bereitstellen, die für die Übertragung von Daten zum und vom Amazon-S3-Bucket erforderlich sind.
5. Wählen Sie Weiter aus.

6. (Optional) Wählen Sie Berechtigungen hinzufügen, um anderen Prinzipalen Berechtigungen zu gewähren.

Durch das Erteilen von Berechtigungen für einen Katalog-Link-Container werden jedoch keine Berechtigungen für den (verknüpften) Zielkatalog gewährt. Sie müssen die Berechtigungen für den Zielkatalog separat erteilen, damit der Katalog-Link in Athena sichtbar ist.

7. Überprüfen Sie als Nächstes die Details des Katalog-Link-Containers und wählen Sie Katalog erstellen aus.

Anschließend können Sie den Namen des Link-Containers auf der Seite Kataloge einsehen.

Jetzt können Sie Datenbank-Links und Tabellen-Links im Katalog-Link-Container erstellen, um den Zugriff von Abfrage-Engines aus zu ermöglichen.

CLI-Beispiel für einen Katalog-Link-Container erstellen

- Im folgenden Beispiel spezifiziert das `TargetRedshiftCatalog` Objekt den ARN des Amazon Redshift Redshift-Katalogs auf Datenbankebene (Amazon Redshift Redshift-Datenbank). Der `DataLakeAccess` muss aktiviert sein, wenn Sie den Katalog-Link-Container erstellen.

```
aws glue create-catalog \  
  --cli-input-json  
  '{  
    "Name": "linkcontainer",  
    "CatalogInput": {  
      "TargetRedshiftCatalog": {  
        "CatalogArn": "arn:aws:us-east-1:123456789012:catalog/nscatalog/dev"  
      },  
      "CatalogProperties": {  
        "DataLakeAccessProperties" : {  
          "DataLakeAccess" : true,  
          "DataTransferRole" : "arn:aws:iam::111122223333:role/  
DataTransferRole"  
        }  
      }  
    }  
  }'
```

Erstellen von Ressourcenlinks unter dem Katalog-Link-Container

Sie können Ressourcenlinks zu Datenbanken und Tabellenlinks unter einem Katalog-Link-Container erstellen. Wenn Sie Datenbankressourcen-Links oder Tabellenressourcen-Links erstellen, müssen Sie eine Zielressource angeben, die sich unter demselben Amazon Redshift Redshift-Zielkatalog auf Datenbankebene (Amazon Redshift Redshift-Datenbank) befindet, auf den der Link-Container verweist.

Sie können mithilfe der AWS Lake Formation Konsole, der API oder AWS Command Line Interface (AWS CLI) einen Ressourcenlink zu einer gemeinsam genutzten Amazon Redshift Redshift-Datenbank oder einer Tabelle erstellen.

- Detaillierte Anweisungen finden Sie unter [Einen Ressourcenlink zu einer gemeinsam genutzten Datenkatalog-Datenbank erstellen](#).

Im Folgenden finden Sie ein AWS CLI Beispiel für die Erstellung eines Datenbankressourcen-Links unter einem Katalog-Link-Container.

```
aws glue create-database \  
  --cli-input-json \  
  '{  
    "CatalogId": "111122223333:linkcontainer",  
    "DatabaseInput": {  
      "Name": "dblink",  
      "TargetDatabase": {  
        "CatalogId": "123456789012:nscatalog/dev",  
        "DatabaseName": "schema1"  
      }  
    }  
  }'
```

- Um einen Tabellenressourcen-Link unter einem Katalog-Link-Container zu erstellen, müssen Sie zunächst eine lokale AWS Glue Datenbank erstellen AWS Glue Data Catalog , die den Tabellenressourcen-Link enthält.

Weitere Informationen zum Erstellen von Ressourcenlinks zu gemeinsam genutzten Tabellen finden Sie unter [Einen Ressourcenlink zu einer gemeinsam genutzten Datenkatalogtabelle erstellen](#).

- Erstellen Sie eine Datenbank, die die Tabelle enthält (Beispiel für einen Ressourcenlink)

```
aws glue create-database \  
  --cli-input-json \  
    '{  
      "CatalogId": "111122223333:linkcontainer",  
      "DatabaseInput": {  
        "Name": "db1",  
        "Description": "creating parent database for table link"  
      }  
    }'
```

- Beispiel für einen Tabellenressourcenlink erstellen

```
aws glue create-table \  
  --cli-input-json \  
    '{  
      "CatalogId": "111122223333:linkcontainer",  
      "DatabaseName": "db1",  
      "TableInput": {  
        "Name": "tablelink",  
        "TargetTable": {  
          "CatalogId": "123456789012:nscatalog/dev",  
          "DatabaseName": "schema1",  
          "Name": "table1"  
        }  
      }  
    }'
```

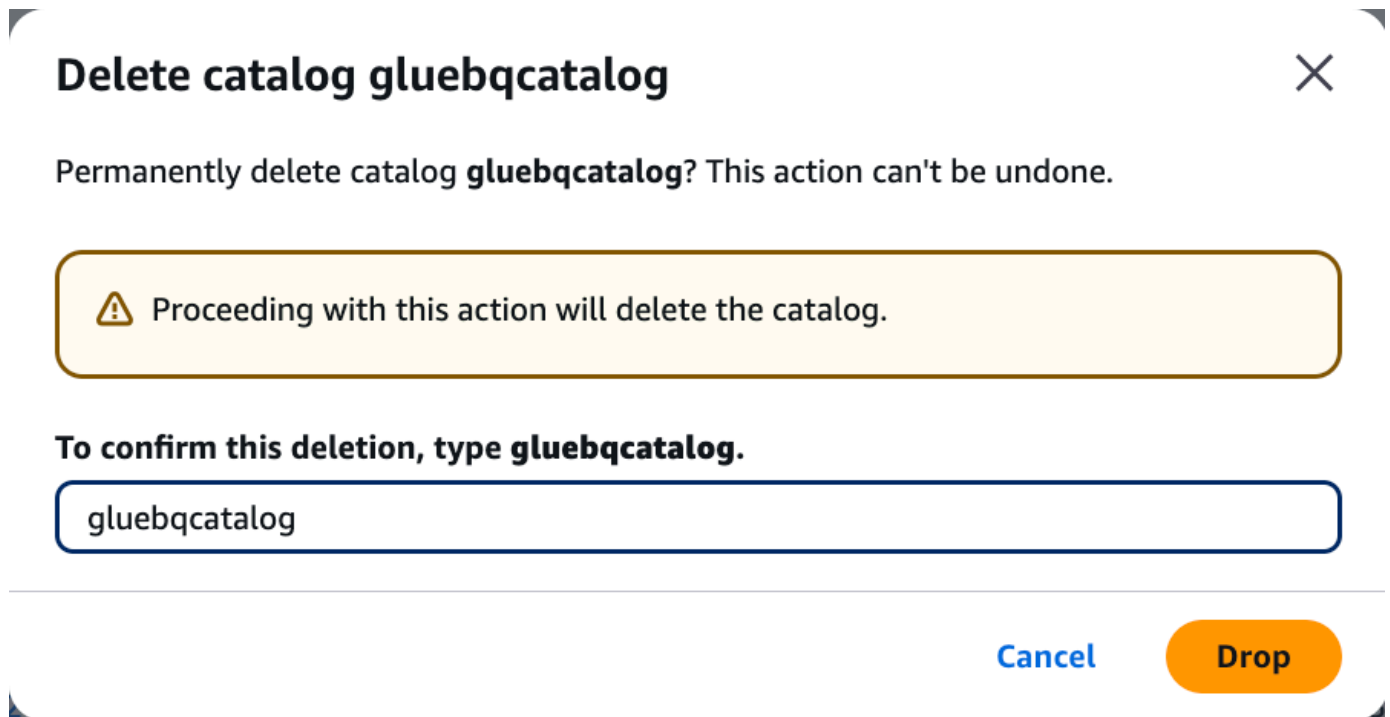
Löschen eines Verbundkatalogs

Sie können die Verbundkataloge löschen, die Sie AWS Glue Data Catalog mithilfe des `glue:DeleteCatalog` Vorgangs oder der Konsole erstellt haben. AWS Lake Formation

So löschen Sie einen Verbundkatalog (Konsole)

1. Öffnen Sie die Lake Formation Konsole unter <https://console.aws.amazon.com/lakeformation/>.
2. Wählen Sie im Navigationsbereich unter Datenkatalog die Option Kataloge aus.
3. Wählen Sie den Katalog, den Sie löschen möchten, aus der Katalogliste aus.

4. Wählen Sie „Aus Aktionen löschen“.
5. Wählen Sie zur Bestätigung Löschen und der Verbundkatalog wird aus dem Datenkatalog gelöscht.



So löschen Sie einen Verbundkatalog (CLI)

- ```
aws glue delete-catalog
--catalog-id 123456789012:catalog name
```

## Verbundkataloge abfragen

Nachdem Sie anderen Principals Berechtigungen erteilt haben, können sie sich anmelden und mit der Abfrage der Tabellen in den Verbundkatalogen beginnen, indem sie sich mit Amazon Redshift, Amazon EMR und ETL bei den SQL-Tools anmelden. Amazon Athena AWS Glue

Weitere Informationen zum Herstellen einer Verbindung AWS Glue Data Catalog mit dem Endpunkt der Apache Iceberg REST-Erweiterung oder der eigenständigen Spark-Anwendung finden Sie unter [Zugriff auf den](#) Abschnitt im Entwicklerhandbuch. AWS Glue Data Catalog AWS Glue

Sie können DDL-Abfragen (Data Definition Language) verwenden, um Tabellen in der Datenbank mit Apache Spark auf Amazon EMR zu erstellen und zu verwalten. Um Tabellen in der Amazon Redshift

Redshift-Datenbank zu erstellen und zu löschen, muss der Principal über Lake Formation Create table Drop Formation-Berechtigungen verfügen.

Weitere Informationen zur Gewährung von Datenkatalogberechtigungen finden Sie unter [Erteilen von Berechtigungen für Datenkatalogressourcen](#).

Weitere Informationen zum Abfragen der Katalogressourcen von finden Sie unter [Abfragen AWS Glue Data Catalog von Amazon Athena](#) im Amazon Athena Athena-Benutzerhandbuch.

## Weitere Ressourcen

Sie können [Amazon SageMaker Lakehouse](#) verwenden, um einen einheitlichen Zugriff auf Daten sowohl in Data Warehouses als auch in Data Lakes zu erreichen. Über SageMaker Lakehouse können Sie bevorzugte Analytics-, Machine Learning- und Business Intelligence-Engines über eine offene Apache Iceberg REST-API verwenden, um den sicheren Zugriff auf Daten mit konsistenten, detaillierten Zugriffskontrollen zu gewährleisten.

- [SageMaker Amazon-Werkstatt](#)
- [Vereinfachen Sie den Datenzugriff für Ihr Unternehmen mit Amazon SageMaker Lakehouse](#)

## Zusammenführung mit externen Datenquellen in der AWS Glue Data Catalog

Sie können den AWS Glue Data Catalog (Datenkatalog) über Verbindungen mit Data Warehouses wie Amazon Redshift, Snowflake, Cloud-Datenbanken wie Amazon RDS Amazon DynamoDB, Oracle und Streaming-Diensten wie Amazon MSK und lokalen Systemen wie Teradata verbinden. AWS Glue Diese Verbindungen werden im gespeichert AWS Glue Data Catalog und bei registriert AWS Lake Formation, sodass Sie für jede verfügbare Datenquelle einen Verbundkatalog erstellen können.

Ein Verbundkatalog ist ein Container der obersten Ebene, der auf eine Datenbank in einem externen Datensystem verweist. Damit können Sie die Daten direkt aus dem externen Datensystem abfragen, ohne dass ein ETL-Prozess (Extrahieren, Transformieren und Laden) erforderlich ist.

Weitere Informationen zu AWS Glue Verbindungen finden Sie unter [Verbindung zu Daten](#) herstellen im AWS Glue Entwicklerhandbuch.

Data Lake-Administratoren können Verbundkataloge mit [Amazon SageMaker Lakehouse](#) oder erstellen. [Amazon Athena](#)

Data Lake-Administratoren können dann mithilfe von Lake Formation detaillierte Berechtigungen für die Objekte innerhalb des Katalogs gewähren und so den Zugriff auf verschiedenen Ebenen wie Katalog, Datenbank, Tabelle, Spalte, Zeile oder Zelle steuern. Datenanalysten können die katalogisierten Datenquellen mithilfe von Athena entdecken und abfragen, wobei Lake Formation die definierten Zugriffsrichtlinien durchsetzt. Analysten können Daten aus mehreren Quellen in einer einzigen Abfrage zusammenführen, ohne sich mit jeder Quelle einzeln verbinden zu müssen.

## Themen

- [Workflow](#)
- [Voraussetzungen für die Verbindung des Datenkatalogs mit externen Datenquellen](#)
- [Erstellen eines Verbundkatalogs mithilfe einer Verbindung AWS Glue](#)
- [Katalogobjekte anzeigen](#)
- [Löschen eines Verbundkatalogs](#)
- [Verbundkataloge abfragen](#)
- [Weitere Ressourcen](#)

## Workflow

Ein Data Lake-Administrator oder ein Benutzer mit den erforderlichen Berechtigungen führt die folgenden Schritte aus, um eine Verbindung AWS Glue Data Catalog zu einer externen Datenquelle herzustellen.

1. Stellt eine AWS Glue Verbindung zur Datenquelle her. Wenn Sie die Verbindung registrieren, muss die bei der Registrierung der Verbindung verwendete IAM-Rolle Zugriff auf die Lambda-Funktion und den Amazon S3 S3-Spill-Bucket-Speicherort haben.
2. Registriert die Verbindung mit Lake Formation.
3. Erstellt einen Verbundkatalog im Datenkatalog mithilfe einer AWS Glue Verbindung, um eine Verbindung zu den verfügbaren Datenquellen herzustellen. Die Datenbanken, Tabellen und Ansichten werden automatisch im Datenkatalog katalogisiert und bei Lake Formation registriert.
4. Gewährt Datenanalysten mit Lake Formation Formation-Berechtigungen Zugriff auf bestimmte Kataloge, Datenbanken und Tabellen. Mithilfe von Lake Formation können differenzierte Zugriffskontrollrichtlinien für Data Lakes, Warehouses und OLTP-Quellen definiert werden, wodurch Sicherheitsfilter auf Zeilen- und Spaltenebene aktiviert werden.

Datenanalysten können dann über den Datenkatalog mithilfe von SQL-Abfragen in Athena auf alle Daten zugreifen, ohne separate Verbindungen oder Datenquellenanmeldedaten zu benötigen. Analysten können föderierte SQL-Abfragen ausführen, bei denen Daten aus mehreren Quellen gescannt werden, sodass Daten ohne komplexe Datenpipeline direkt zusammengeführt werden.

## Voraussetzungen für die Verbindung des Datenkatalogs mit externen Datenquellen

Um eine Verbindung AWS Glue Data Catalog zu externen Datenquellen herzustellen, die Verbindung mit Lake Formation zu registrieren und Verbundkataloge einzurichten, müssen Sie die folgenden Anforderungen erfüllen:

### Note

Es wird empfohlen, dass ein Lake Formation Data Lake-Administrator die AWS Glue Verbindungen für die Verbindung mit externen Datenquellen erstellt und die Verbundkataloge erstellt.

#### 1. Erstellen Sie IAM-Rollen.

- Erstellen Sie eine Rolle, die über die erforderlichen Berechtigungen für die Bereitstellung von Ressourcen (Lambda-Funktion, Amazon S3 S3-Spill-Bucket, IAM-Rolle und die AWS Glue Verbindung) verfügt, die für die Herstellung einer Verbindung zur externen Datenquelle erforderlich sind.
- Erstellen Sie eine Rolle, die über die erforderlichen Mindestberechtigungen für den Zugriff auf die AWS Glue Verbindungseigenschaften (die Lambda-Funktion und den Amazon S3 S3-Spill-Bucket) verfügt. Dies ist die Rolle, die Sie angeben, wenn Sie die Verbindung bei Lake Formation registrieren.

Um Lake Formation zur Verwaltung und Sicherung der Daten in Ihrem Data Lake zu verwenden, müssen Sie die AWS Glue Verbindung bei Lake Formation registrieren. Auf diese Weise kann Lake Formation Anmeldeinformationen an Amazon Athena weitergeben, um die föderierten Datenquellen abzufragen.

Die Rolle muss über `Select Describe` Berechtigungen für den Amazon S3 S3-Bucket und die Lambda-Funktion verfügen.

- s3: ListBucket
- s3: GetObject
- Lambda: InvokeFunction

JSON

```
{
 "Version": "2012-10-17",
 "Statement": [
 {
 "Effect": "Allow",
 "Action": [
 "s3:*"
],
 "Resource": [
 "arn:aws:s3:::amzn-s3-demo-bucket1/object/*",
 "arn:aws:s3:::amzn-s3-demo-bucket1/object"
]
 },
 {
 "Sid": "lambdainvoke",
 "Effect": "Allow",
 "Action": "lambda:InvokeFunction",
 "Resource": "arn:aws:lambda:us-east-1:123456789012:function:example-lambda-function"
 },
 {
 "Sid": "gluepolicy",
 "Effect": "Allow",
 "Action": "glue:*",
 "Resource": "*"
 }
]
}
```

- Fügen Sie der IAM-Rolle, die bei der Registrierung der Verbindung verwendet wird, die folgende Vertrauensrichtlinie hinzu:

JSON

```
{
```

```

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

```

- Der Data Lake-Administrator, der die Verbindung registriert, muss über die entsprechenden `iam:PassRole` Berechtigungen für die Rolle verfügen.

Im Folgenden finden Sie eine Inline-Richtlinie, die diese Berechtigung gewährt. `<account-id>` Ersetzen Sie es durch eine gültige AWS Kontonummer und `<role-name>` ersetzen Sie es durch den Namen der Rolle.

JSON

```

{
 "Version": "2012-10-17",
 "Statement": [
 {
 "Sid": "PassRolePermissions",
 "Effect": "Allow",
 "Action": [
 "iam:PassRole"
],
 "Resource": [
 "arn:aws:iam::111122223333:role/example-role-name"
]
 }
]
}

```

- Um Verbundkataloge in Data Catalog zu erstellen, stellen Sie sicher, dass es sich bei der verwendeten IAM-Rolle um einen Lake Formation Data Lake-Administrator handelt, indem

Sie die Data Lake-Einstellungen überprüfen (). `aws lakeformation get-data-lake-settings`

Wenn Sie kein Data Lake-Administrator sind, benötigen Sie die Lake Formation `CREATE_CATALOG` Formation-Berechtigung, um einen Katalog zu erstellen. Das folgende Beispiel zeigt, wie Sie die erforderlichen Berechtigungen zum Erstellen von Katalogen gewähren.

```
aws lakeformation grant-permissions \
--cli-input-json \
 '{
 "Principal": {
 "DataLakePrincipalIdentifier": "arn:aws:iam::123456789012:role/non-
admin"
 },
 "Resource": {
 "Catalog": {
 }
 },
 "Permissions": [
 "CREATE_CATALOG",
 "DESCRIBE"
]
 }'
```

2. Fügen Sie dem Schlüssel die folgende Schlüsselrichtlinie hinzu, wenn Sie einen vom AWS KMS Kunden verwalteten Schlüssel zum Verschlüsseln der Daten in der Datenquelle verwenden. Ersetzen Sie die Kontonummer durch eine gültige AWS Kontonummer und geben Sie den Rollennamen an. Standardmäßig werden die Daten mit einem KMS-Schlüssel verschlüsselt. Lake Formation bietet die Möglichkeit, Ihren benutzerdefinierten KMS-Schlüssel für die Verschlüsselung zu erstellen. Wenn Sie einen vom Kunden verwalteten Schlüssel verwenden, müssen Sie dem Schlüssel bestimmte Schlüsselrichtlinien hinzufügen.

Weitere Informationen zum Verwalten von Berechtigungen eines kundenseitig verwalteten Schlüssels finden Sie unter [Kundenseitig verwaltete Schlüssel](#).

JSON

```
{
```

```
"Version": "2012-10-17",
"Statement": [
 {
 "Effect": "Allow",
 "Action": [
 "kms:Encrypt",
 "kms:Decrypt",
 "kms:ReEncrypt*",
 "kms:GenerateDataKey*",
 "kms:DescribeKey"
],
 "Resource": "arn:aws:kms:us-east-1:123456789012:key/key-1"
 }
]
```

## Erstellen eines Verbundkatalogs mithilfe einer Verbindung AWS Glue

Um eine Verbindung AWS Glue Data Catalog zu externen Datenquellen herzustellen, müssen Sie AWS Glue Verbindungen verwenden, die die Kommunikation mit den externen Datenquellen ermöglichen. Sie können AWS Glue Verbindungen mithilfe der AWS Glue Konsole, der [Create Connection](#) API und der Amazon SageMaker Lakehouse-Konsole herstellen.

Eine schrittweise Anleitung zum Herstellen einer AWS Glue Verbindung finden Sie unter [Verbindung zu Daten](#) herstellen im AWS Glue Entwicklerhandbuch oder unter [Verbindungen in Amazon SageMaker Lakehouse erstellen](#).

Wenn ein Benutzer eine Abfrage für Verbundtabellen ausführt, vergibt Lake Formation Anmeldeinformationen, die eine in der AWS Glue Verbindung angegebene AWS Lambda Funktion aufrufen, um Metadatenobjekte aus der Datenquelle abzurufen.

### AWS-Managementkonsole

Um einen Verbundkatalog aus einer externen Datenquelle zu erstellen und Berechtigungen einzurichten (Konsole)

1. Öffnen Sie die Lake Formation Konsole unter <https://console.aws.amazon.com/lakeformation/>.
2. Wählen Sie im Navigationsbereich unter Datenkatalog die Option Kataloge aus.
3. Wählen Sie die Option Katalog erstellen aus.



#### 4. Geben Sie auf der Seite „Katalogdetails festlegen“ die folgenden Informationen ein:

- Step 1  
**Set catalog details**  
 Step 2 - optional  
 Grant permissions  
 Step 3  
 Review and create

##### Set catalog details

Create a catalog in the Data Catalog.

###### Catalog details

A catalog is the top level in the Data Catalog's three-level data hierarchy and contains Data Catalog objects.

###### Name

Catalog name is required, in lowercase characters, and no longer than 255 characters.

###### Type

###### Source

###### Connection

###### Description - optional

Descriptions can be up to 2048 characters long.

##### Register Glue connection with Lake Formation

You can access this catalog from AWS Glue data connections.

###### IAM role

Choose a role that has permissions to invoke an AWS Glue connector.


[View](#)
[Create an IAM role](#)

☒ Activate the connector and connect to the data source.

A connector is a piece of code that runs on AWS Lambda that translates between the target data source and query engine (Athena).

###### Encryption options

Your data is encrypted by default with a key that AWS owns and manages for you. To choose a different key, customize your encryption settings.

☐ Customize encryption settings

To use the default key, clear this option.

[Cancel](#)
[Skip to Review and create](#)
[Next](#)

- **Name** — Ein eindeutiger Name für Ihren Verbundkatalog. Der Name kann nicht geändert werden und muss in Kleinbuchstaben geschrieben werden. Der Name darf aus maximal 255 Zeichen bestehen. Konto.
- **Typ** — Wählen Sie den Verbundkatalog als Katalogtyp aus.
- **Quelle** — Wählen Sie eine Datenquelle aus der Dropdownliste aus. Die Datenquellen, für die Sie Verbindungen erstellt haben, werden angezeigt. Weitere Informationen zum Herstellen einer AWS Glue Verbindung zu einer externen Datenquelle finden Sie unter [Creating connections for connectors](#) im AWS Glue Developer Guide oder [Creating connections in Amazon SageMaker Lakehouse](#).
- **Verbindung** — Wählen Sie eine bestehende AWS Glue Verbindung zur Datenquelle aus.
- **Beschreibung** — Geben Sie eine Beschreibung für den aus der Datenquelle erstellten Katalog ein.

5. Wählen Sie eine IAM-Rolle aus, damit Lake Formation davon ausgeht, dass sie Anmeldeinformationen für die Abfrage-Engine für den Zugriff auf Daten aus der Datenquelle weitergibt. Diese Rolle muss über die erforderlichen Berechtigungen verfügen, um auf die AWS Glue Verbindung zuzugreifen und die Lambda-Funktion aufzurufen, um auf Daten aus der externen Datenquelle zuzugreifen.

Sie können auch eine neue Rolle in der IAM-Konsole erstellen.

Die erforderlichen Berechtigungen finden Sie im [Voraussetzungen für die Verbindung des Datenkatalogs mit externen Datenquellen](#) Abschnitt.

6. Wählen Sie die Option Connector aktivieren, um eine Verbindung zur Datenquelle herzustellen, damit Athena Verbundabfragen ausführen kann.

Eine Liste der unterstützten Konnektoren finden Sie unter [Registrieren Sie Ihre Verbindung](#) im Amazon Athena Athena-Benutzerhandbuch.

7. Verschlüsselungsoptionen — Wählen Sie die Option Verschlüsselungseinstellungen anpassen, wenn Sie einen benutzerdefinierten Schlüssel zum Verschlüsseln des Katalogs verwenden möchten. Um einen benutzerdefinierten Schlüssel zu verwenden, müssen Sie Ihrem KMS-Schlüssel eine zusätzliche benutzerdefinierte Richtlinie für verwaltete Schlüssel hinzufügen.
8. Wählen Sie Weiter, um anderen Prinzipalen Berechtigungen zu gewähren.
9. Wählen Sie auf der Seite Berechtigungen gewähren die Option Berechtigungen hinzufügen aus.
10. Wählen Sie auf dem Bildschirm „Berechtigungen hinzufügen“ die Hauptbenutzer und die Arten der zu erteilenden Berechtigungen aus.

## Add permissions

### Principals

Choose the principals to grant permissions.

☒ **IAM users and roles**  
Users or roles from this AWS account.

☐ **SAML users and groups**  
SAML users and group or QuickSight ARNs.

☐ **External accounts**  
AWS account, AWS organization or IAM principal outside of this account

#### IAM users and roles

Add one or more IAM users or roles.

Choose IAM principals to add

UserRole X  
Role

### Catalog permissions

Choose the permissions to grant on the catalog. Choosing Super user overwrites individual permissions, granting unrestricted administrative access.

☐ **Super user**  
A super user has unrestricted administrative privileges to perform any operation on all resources within the catalog (databases, tables, and views).

#### Catalog permissions

Choose specific access permissions to grant.

☒ **Create database**

☐ Describe

☐ Alter

☐ Drop

☐ **Super**  
This permission is the union of all the individual permissions to the left, and supersedes them.

#### Grantable permissions

Choose the permission that can be granted to others.

☒ **Create database**

☐ Describe

☐ Alter

☐ Drop

☐ **Super**  
This permission allows the principal to grant any of the permissions to the left, and supersedes those grantable permissions.

Cancel

Add

- Wählen Sie im Abschnitt Prinzipale einen Prinzipaltyp aus und geben Sie dann Prinzipale an, denen Berechtigungen erteilt werden sollen.

- IAM-Benutzer und -Rollen – wählen Sie mindestens einen Benutzer oder eine Rolle aus der Liste der IAM-Benutzer und -Rollen aus.
- SAML-Benutzer und -Gruppen — Geben Sie für SAML und Amazon Quick Benutzer und Gruppen einen oder mehrere Amazon-Ressourcennamen (ARNs) für Benutzer oder Gruppen ein, die über SAML verbunden sind, oder ARNs für Amazon Quick-Benutzer oder -Gruppen. Drücken Sie nach jedem ARN die Eingabetaste.
- Wählen Sie im Abschnitt Berechtigungen die Berechtigungen und erteilbare Berechtigungen aus.

Wählen Sie unter Katalogberechtigungen mindestens eine Berechtigung aus, die Sie gewähren möchten.

Wählen Sie Superuser aus, um uneingeschränkte Administratorberechtigungen für alle Ressourcen im Katalog zu gewähren.

Wählen Sie unter Erteilbare Berechtigungen die Berechtigungen aus, die der Zuwendungsempfänger anderen Hauptbenutzern in seinem Konto gewähren kann. AWS Diese Option wird nicht unterstützt, wenn Sie einem IAM-Prinzipal von einem externen Konto aus Berechtigungen gewähren.

11. Wählen Sie Weiter, um die Informationen zu überprüfen und den Katalog zu erstellen. In der Katalogliste wird der neue Verbundkatalog angezeigt.

Die Liste der Datenspeicherorte zeigt die neu registrierte Verbundverbindung.

Data lake locations (7)

Find data lake storage

Actions

Register location

< 1 >

|                       | Data lake location                               | IAM role                                          | Location Type        | Permission mode    | Last modified                     |
|-----------------------|--------------------------------------------------|---------------------------------------------------|----------------------|--------------------|-----------------------------------|
| <input type="radio"/> | <a href="#">ddb_ds_3</a>                         | <a href="#">SageMakerStudioQueryExecutionR...</a> | Federated connection | Lake Formation     | November 26, 2024 at 10:34 PM UTC |
| <input type="radio"/> | <a href="#">postgre_db2</a>                      | <a href="#">SageMakerStudioQueryExecutionR...</a> | Federated connection | Lake Formation     | November 24, 2024 at 11:12 AM UTC |
| <input type="radio"/> | <a href="#">sf_ds2</a>                           | <a href="#">SageMakerStudioQueryExecutionR...</a> | Federated connection | Lake Formation     | November 24, 2024 at 3:27 AM UTC  |
| <input type="radio"/> | <a href="#">s3://amazon-sagemaker-5390106...</a> | <a href="#">datazone_usr_role_50wwm8ts855...</a>  | Amazon S3            | Lake Formation     | November 24, 2024 at 3:10 AM UTC  |
| <input type="radio"/> | <a href="#">ddb_ds_2</a>                         | <a href="#">SageMakerStudioQueryExecutionR...</a> | Federated connection | Lake Formation     | November 24, 2024 at 3:05 AM UTC  |
| <input type="radio"/> | <a href="#">s3://amazon-sagemaker-5390106...</a> | <a href="#">datazone_usr_role_adtmv7d4lm98...</a> | Amazon S3            | Lake Formation     | November 23, 2024 at 9:15 PM UTC  |
| <input type="radio"/> | <a href="#">s3://data-lake-pk-us-east-2</a>      | <a href="#">AWSServiceRoleForLakeFormation...</a> | Amazon S3            | Hybrid access mode | November 21, 2024 at 7:40 PM UTC  |

## AWS CLI

Um einen Verbundkatalog aus einer externen Datenquelle zu erstellen und Berechtigungen einzurichten

1. Das folgende Beispiel zeigt, wie eine AWS Glue Verbindung hergestellt wird.

```
aws glue create-connection
--connection-input \
 '{
 "Name": "DynamoDB connection",
 "ConnectionType": "DYNAMODB",
 "Description": "A connection created for DynamoDB",
 "ConnectionProperties": {},
 "AthenaProperties": {"spill_prefix": "your_spill_prefix",
 "lambda_function_arn": "Lambda_function_arn",
 "spill_bucket": "Your_Bucket_name",
 "AuthenticationConfiguration": {}
 }'
```

2. Das folgende Beispiel zeigt, wie eine AWS Glue Verbindung mit Lake Formation registriert wird.

```
aws lakeformation register-resource
--cli-input-json \
 '{"ResourceArn': "arn:aws:glue:us-east-1:123456789012:connection/
dynamo", "RoleArn": "arn:aws:iam::123456789012:role/
AdminTelemetry", "WithFederation": true}'
```

3. Das folgende Beispiel zeigt, wie ein Verbundkatalog erstellt wird.

```
aws glue create-catalog
--cli-input-json \
 '{
 "Name": "ddbcatalog",
 "CatalogInput": {"CatalogProperties": {"DataLakeAccessProperties":
{"DataTransferRole": "arn:aws:iam::123456789012:role/role name"}},
 "CreateDatabaseDefaultPermissions": [],
 "CreateTableDefaultPermissions": [],
 "FederatedCatalog": {"ConnectionName": "dynamo", "Identifier": "dynamo"}
 }'
```

}'

## Katalogobjekte anzeigen

AWS Glue Erstellt für jede verfügbare Datenquelle einen entsprechenden Katalog im AWS Glue Data Catalog. Nachdem Sie einen Katalog erstellt haben, können Sie die Datenbanken und Tabellen im Katalog mit der Lake Formation Formation-Konsole oder anzeigen AWS CLI. Wählen Sie in der &Snowconsole; Ihren Auftrag aus der Tabelle.

1. Öffnen Sie die Lake Formation Formation-Konsole unter <https://console.aws.amazon.com/lakeformation/>.
2. Wählen Sie unter Datenkatalog die Option Kataloge aus. Auf der Seite „Kataloge“ werden die Kataloge angezeigt, für die Sie Berechtigungen haben.

**Catalogs (11)** Actions View Create catalog

A catalog is the top level in the Data Catalog's three-level data hierarchy and contains Data Catalog objects.

Find catalogs by name

|                       | Name                | Type      | Source                 | Owner account... | Shared resource | Shared resourc... | Shared resource owner region |
|-----------------------|---------------------|-----------|------------------------|------------------|-----------------|-------------------|------------------------------|
| <input type="radio"/> | 30005               | Default   | Default catalog        | 0005             | -               | -                 | -                            |
| <input type="radio"/> | bkaiyuan_nscatal... | Federated | Redshift               | 0005             | -               | -                 | -                            |
| <input type="radio"/> | bkaiyuan_test_ca... | Federated | -                      | 0005             | -               | -                 | -                            |
| <input type="radio"/> | linkcontainer-leon  | Managed   | Catalog Link container | 0005             | -               | -                 | -                            |
| <input type="radio"/> | mymulticatalog      | Federated | TPCDS                  | 0005             | -               | -                 | -                            |
| <input type="radio"/> | test-bug-share      | Federated | Redshift               | 0005             | -               | -                 | -                            |
| <input type="radio"/> | test-zetl           | Managed   | Redshift               | 0005             | -               | -                 | -                            |
| <input type="radio"/> | test-zetl-mwg       | Managed   | Redshift               | 0005             | -               | -                 | -                            |
| <input type="radio"/> | tpcdscatalog        | Federated | TPCDS                  | 0005             | -               | -                 | -                            |
| <input type="radio"/> | yansoncatalog2      | Federated | Redshift               | 0005             | -               | -                 | -                            |
| <input type="radio"/> | zetltest123         | Managed   | Redshift               | 0005             | -               | -                 | -                            |

3. Wählen Sie einen Katalog aus der Liste aus, um die im Katalog enthaltenen Datenbanken und Tabellen anzuzeigen. Die Liste enthält die Datenbanken in Ihrem Konto und Ressourcenlinks. Dabei handelt es sich um Links zu gemeinsam genutzten Datenbanken und Tabellen in externen Konten, die für den kontenübergreifenden Zugriff auf Daten im Data Lake verwendet werden.

**Catalog summary**

Name

451785580005

Catalog ARN

arn:aws:glue:us-west-2:451785580005:catalog

Data encryption

-

IAM role

-

KMS key for optimization

-

Objects

Permissions

Table optimizations

Databases (1/14)

Find databases

Actions

View

Tables

Views

Descript...

| Name                                  | Owner account ID | Lake Fo... | Default ...  | Shared ...    | Shared ...  | Shared ... | Amazo...                          | Descript...  |
|---------------------------------------|------------------|------------|--------------|---------------|-------------|------------|-----------------------------------|--------------|
| arfarajpostgresldb                    |                  | -          | Lake Form... | -             | -           | -          | -                                 | -            |
| aws:cloudtrail                        |                  | -          | Lake Form... | -             | -           | -          | -                                 | -            |
| default                               |                  | -          | Lake Form... | -             | -           | -          | -                                 | -            |
| gluedynamodb                          |                  | -          | Lake Form... | -             | -           | -          | -                                 | -            |
| mysnowflakedb                         |                  | -          | Lake Form... | -             | -           | -          | -                                 | -            |
| snowflakedb                           |                  | -          | Lake Form... | -             | -           | -          | -                                 | -            |
| test-db-0737fa687d584b2d9ab72fbd...   |                  | -          | Lake Form... | test-db-0...  | 45178558... | -          | -                                 | -            |
| test-db-1927b03560764a4b81a216e9...   |                  | -          | Lake Form... | test-db-1...  | 45178558... | -          | -                                 | -            |
| test-db-32ee54b6949b4fdd85b8ff066...  |                  | -          | Lake Form... | test-db-3...  | 45178558... | -          | -                                 | -            |
| test-db-5978c2e076aa4583a28df124f...  |                  | -          | Lake Form... | test-db-5...  | 45178558... | -          | -                                 | -            |
| test-db-5cebe417bf734eafbbeaf7d3d6... |                  | -          | Lake Form... | test-db-5c... | 45178558... | -          | -                                 | -            |
| test-db-7fa7ca8de2b84232ae3e8dcf...   |                  | -          | Lake Form... | -             | -           | -          | <a href="http://db">http://db</a> | database ... |
| test-db-bb19fb486dc14ad68813612...    |                  | -          | Lake Form... | -             | -           | -          | <a href="http://db">http://db</a> | database ... |
| test-db-cdec6ecaa0f143b7b4d6f24a8...  |                  | -          | Lake Form... | test-db-cd... | 45178558... | -          | -                                 | -            |

4. Wählen Sie unter Ansicht die Option Tabellen, um die Tabellen in der Datenbank anzuzeigen und zu verwalten.

## AWS CLI Beispiele für die Anzeige von Katalogen und Datenbanken

Das folgende Beispiel zeigt, wie Sie einen Katalog mithilfe von AWS CLI

```
aws glue get-catalog \
--catalog-id 123456789012:dynamodbcatalog
```

Das folgende Beispiel zeigt, wie alle Kataloge im Konto angefordert werden.

```
aws glue get-catalogs \
--recursive
```

Die folgende Beispielanforderung zeigt, wie die Datenbanken im Katalog abgerufen werden.

```
aws glue get-database \
```

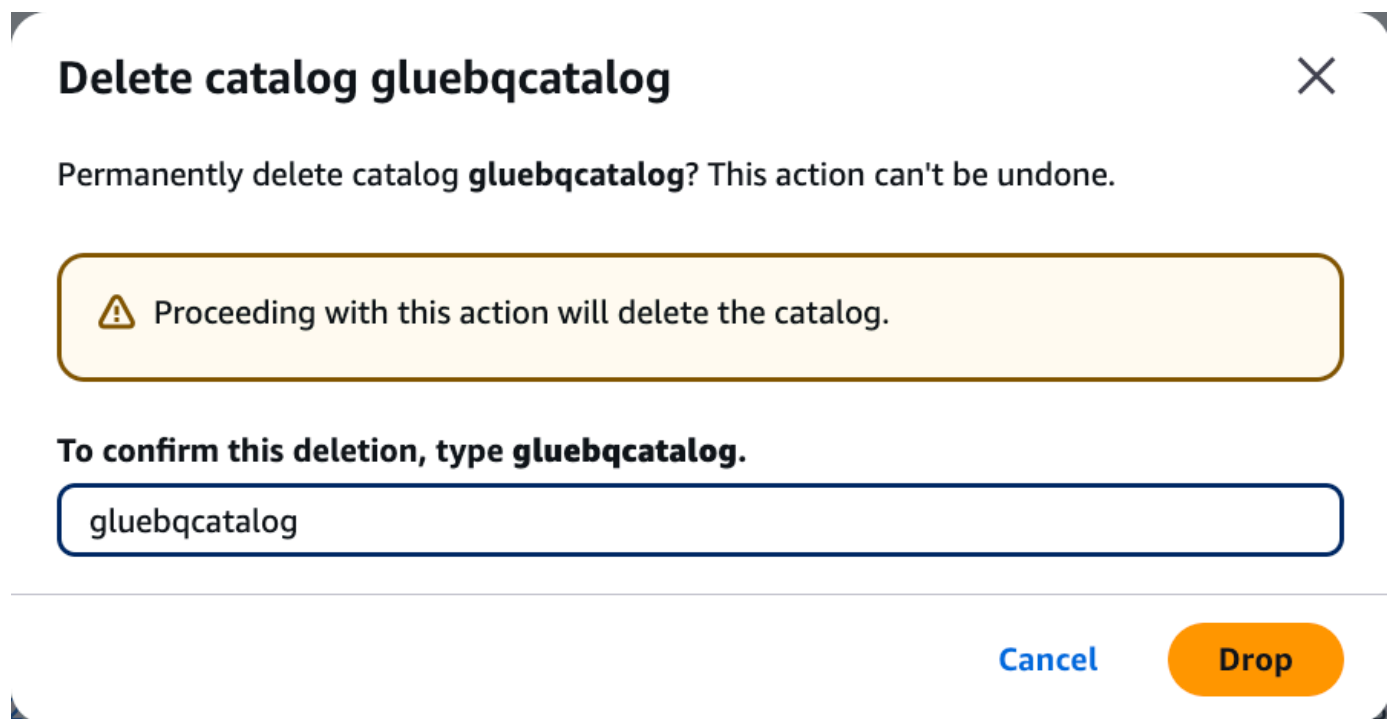
```
--catalog-id 123456789012:dynamodbcatalog
--database-name database name
```

## Löschen eines Verbundkatalogs

Sie können die Verbundkataloge löschen, die Sie AWS Glue Data Catalog mithilfe des `glue:DeleteCatalog` Vorgangs oder der Konsole erstellt haben. AWS Lake Formation

So löschen Sie einen Verbundkatalog (Konsole)

1. Öffnen Sie die Lake Formation Konsole unter <https://console.aws.amazon.com/lakeformation/>.
2. Wählen Sie im Navigationsbereich unter Datenkatalog die Option Kataloge aus.
3. Wählen Sie den Katalog, den Sie löschen möchten, aus der Katalogliste aus.
4. Wählen Sie „Aus Aktionen löschen“.
5. Wählen Sie zur Bestätigung Löschen und der Verbundkatalog wird aus dem Datenkatalog gelöscht.



So löschen Sie einen Verbundkatalog (CLI)

```
• aws glue delete-catalog
```



```
--catalog-id 123456789012:catalog name
```

## Verbundkataloge abfragen

Nachdem Sie anderen Prinzipalen Berechtigungen erteilt haben, können sie sich anmelden und mit der Abfrage der Tabellen in den Verbundkatalogen mit Athena beginnen.

Um Tabellen in der Verbunddatenbank zu erstellen und zu löschen, muss der Principal über Lake Formation Create table Drop Formation-Berechtigungen verfügen.

Weitere Informationen zum Erteilen von Datenkatalogberechtigungen finden Sie unter [Erteilen von Berechtigungen für Datenkatalogressourcen](#).

Weitere Informationen zum Abfragen des Datenkatalogs von finden Sie unter [Abfragen AWS Glue Data Catalog von Amazon Athena](#) im Amazon Athena Benutzerhandbuch.

## Weitere Ressourcen

In diesem Blogbeitrag zeigen wir, wie Datenanalysten jetzt sicher auf Daten zugreifen und diese abfragen können, die außerhalb von S3-Data Lakes gespeichert sind, einschließlich Amazon Redshift Redshift-Data Warehouses und Amazon DynamoDB Datenbanken, und das alles über eine einzige, einheitliche Oberfläche. Administratoren können nun Zugriffskontrollen auf unterschiedlichen Granularitätsebenen anwenden, um sicherzustellen, dass sensible Daten geschützt bleiben und gleichzeitig der Datenzugriff erweitert wird. Dies ermöglicht es Unternehmen, Dateninitiativen zu beschleunigen und gleichzeitig Sicherheit und Compliance aufrechtzuerhalten, was zu einer schnelleren, datengestützten Entscheidungsfindung führt.

- [Katalogisieren und verwalten Sie föderierte Amazon Athena Athena-Abfragen mit Amazon Lakehouse SageMaker](#)

## Erstellen eines Amazon S3 Tables-Katalogs in AWS Glue Data Catalog

[Amazon S3 S3-Tabellen](#) bieten S3-Speicher, der speziell für Analyse-Workloads optimiert ist, wodurch die Abfrageleistung verbessert und gleichzeitig die Kosten gesenkt werden. Die Daten in S3 Tables werden in einem neuen Bucket-Typ gespeichert: einem Tabellen-Bucket, der Tabellen als Unterressourcen speichert. S3-Tabellen verfügen über eine integrierte Unterstützung für den Apache

Iceberg-Standard, mit dem Sie mithilfe gängiger Abfrage-Engines wie Apache Spark problemlos Tabellendaten in Amazon S3 S3-Tabellen-Buckets abfragen können.

Sie können Amazon S3 S3-Tabellen-Buckets und -Tabellen in AWS Glue Data Catalog (Data Catalog) integrieren und den Katalog über die Lake Formation Formation-Konsole oder mithilfe des Service APIs als Lake Formation Formation-Datenspeicherort registrieren. Wenn Ihre Organisation Daten im Datenkatalog verwaltet und den Datenstandort bei Lake Formation registriert, können Sie Lake Formation verwenden, um den Zugriff auf Ihre Datensätze zu kontrollieren.

Sie können Lake Formation Formation-Berechtigungen mithilfe der tagbasierten Zugriffskontrolle und der Methode für benannte Ressourcen auf die Verbunddatenbanken anwenden und sie für mehrere AWS-Konten AWS Organizations und Organisationseinheiten gemeinsam nutzen (OUs). Sie können die Verbunddatenbanken auch direkt für IAM-Prinzipale von einem anderen Konto aus freigeben.

Weitere Informationen finden Sie unter [Verwenden von Amazon S3 S3-Tabellen mit AWS Analysediensten](#) im Amazon Simple Storage Service-Benutzerhandbuch.

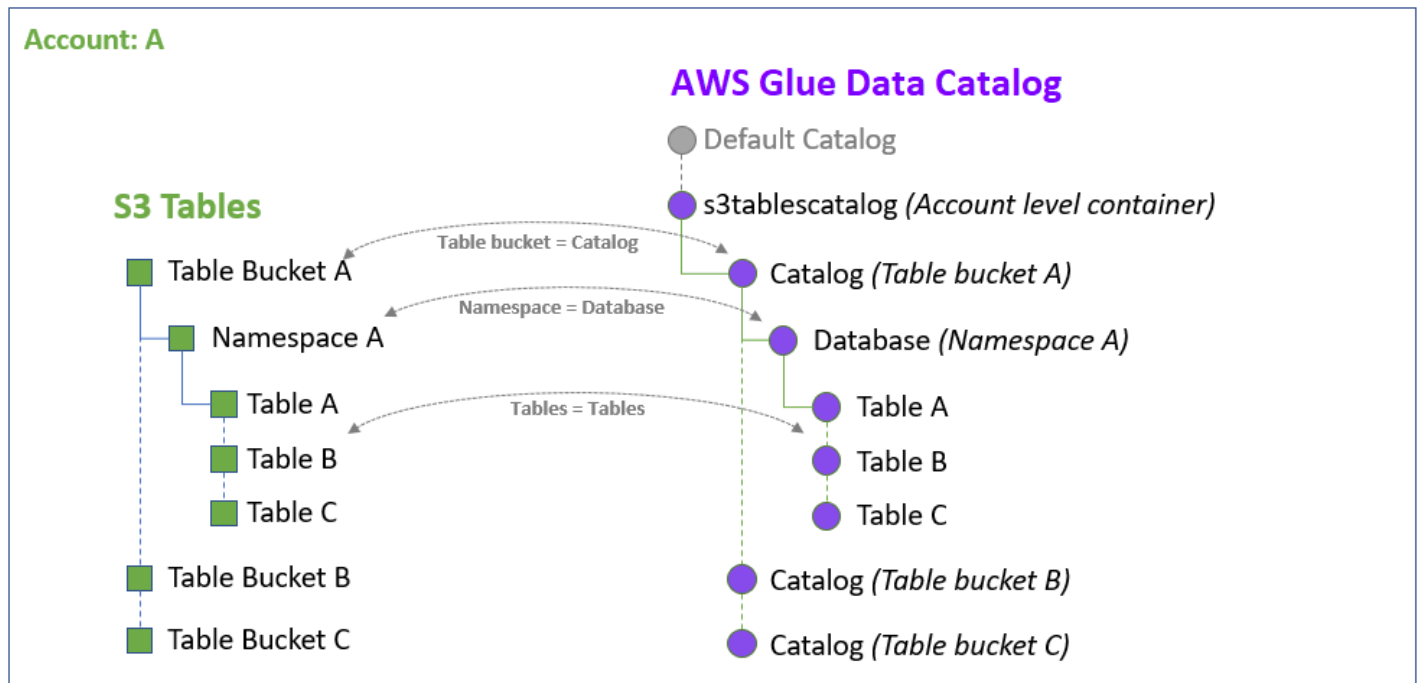
## Themen

- [So funktioniert die Integration von Data Catalog und Lake Formation](#)
- [Voraussetzungen für die Integration des Amazon S3 S3-Tabellenkatalogs mit Data Catalog und Lake Formation](#)
- [Aktivierung der Amazon S3 S3-Tabellenintegration](#)
- [Datenbanken und Tabellen im S3-Tabellenkatalog erstellen](#)
- [Registrierung eines Amazon S3 S3-Tabellen-Buckets in einem anderen AWS Konto](#)
- [Gewähren von Berechtigungen](#)

## So funktioniert die Integration von Data Catalog und Lake Formation

Wenn Sie den S3-Tabellenkatalog in den Data Catalog und Lake Formation integrieren, erstellt der AWS Glue Service einen einzelnen Verbundkatalog, der `s3tablescatalog` im für Sie spezifischen Standarddatenkatalog Ihres AWS-Region Kontos aufgerufen wird. Die Integration ordnet alle Amazon S3 S3-Tabellen-Bucket-Ressourcen in Ihrem Konto und AWS-Region im Verbundkatalog auf folgende Weise zu:

- Amazon S3 S3-Tabellen-Buckets werden im Datenkatalog zu einem mehrstufigen Katalog.
- Der zugehörige Amazon S3 S3-Namespace ist als Datenbank im Datenkatalog registriert.
- Die Amazon S3 S3-Tabellen im Tabellen-Bucket werden zu Tabellen im Datenkatalog.



Nach der Integration mit Lake Formation können Sie Apache Iceberg-Tabellen im Tabellen-Buckets-Katalog erstellen und über integrierte AWS Analyse-Engines wie Amazon EMR sowie Analyse-Engines von Drittanbietern darauf zugreifen. Amazon Athena

## Voraussetzungen für die Integration des Amazon S3 S3-Tabellenkatalogs mit Data Catalog und Lake Formation

Im Folgenden sind die Voraussetzungen für die Aktivierung der Amazon S3 S3-Tabellenintegration mit AWS Glue Data Catalog und aufgeführt AWS Lake Formation.

1. Der Integrationsprozess für AWS Analysedienste wurde aktualisiert. Wenn Sie die Integration mit der Vorschauversion eingerichtet haben, können Sie Ihre aktuelle Integration weiterhin verwenden. Der aktualisierte Integrationsprozess bietet jedoch Leistungsverbesserungen. Um die Integration zu aktualisieren:
  1. Löschen Sie zunächst Ihren vorhandenen S3-Tabellenkatalog in Lake Formation. Um den Katalog zu löschen, wählen Sie den `s3tablescatalog` Katalog aus der Katalogliste aus und klicken Sie dann auf **Aus Aktionen löschen**.
  2. Als Nächstes deregistrieren Sie den Datenspeicherort für `s3tablescatalog`
    - a. Wählen Sie in der Lake Formation Formation-Konsole im Abschnitt **Administrations** die Option **Data Locations** aus.

- b. Wählen Sie einen Standort aus und klicken Sie im Menü Aktionen auf Entfernen.
- c. Wenn Sie zur Bestätigung aufgefordert werden, wählen Sie „Entfernen“.

Ausführliche Anweisungen zum Abmelden einer Datenposition finden Sie im [Abmeldung eines Amazon S3 S3-Standorts](#) Abschnitt.

- d. Folgen Sie dann den aktualisierten Integrationsschritten im [Aktivierung der Amazon S3 S3-Tabellenintegration](#) Abschnitt.

2. Wenn Sie die Amazon S3-Tabellenintegration aktivieren, registriert Lake Formation automatisch den Standort der S3-Tabellen. Um den Tabellen-Bucket-Standort bei Lake Formation zu registrieren, benötigen Sie ein IAM role/user mit `lakeformation:RegisterResource` und `lakeformation:RegisterResourceWithPrivilegedAccess` und `lakeformation>CreateCatalog` -Berechtigungen. Wenn ein Benutzer ohne Administratorrechte mit diesen Berechtigungen einen Katalogspeicherort registriert, erteilt Lake Formation ihm automatisch die `DATA_LOCATION_ACCESS` Berechtigung für diesen Standort, sodass der aufrufende Prinzipal alle unterstützten Lake Formation Operationen an dem registrierten Datenstandort ausführen kann.

3. Wenn Sie die Integration von S3-Tabellen aktivieren, müssen Sie eine IAM-Rolle für Lake Formation auswählen, um Anmeldeinformationen für den Datenzugriff weiterzugeben. Erstellen Sie eine IAM-Rolle für den Lake Formation Datenzugriff auf Ihre S3-Tabellen-Buckets. Die IAM-Rolle, die bei der Registrierung des Tabellen-Buckets bei Lake Formation verwendet wird, erfordert die folgenden Berechtigungen:

JSON

```
{
 "Version": "2012-10-17",
 "Statement": [
 {
 "Sid": "LakeFormationPermissionsForS3ListTableBucket",
 "Effect": "Allow",
 "Action": [
 "s3tables:ListTableBuckets"
],
 "Resource": [
 "*"
]
 }
],
}
```

```

 {
 "Sid": "LakeFormationDataAccessPermissionsForS3TableBucket",
 "Effect": "Allow",
 "Action": [
 "s3tables:CreateTableBucket",
 "s3tables:GetTableBucket",
 "s3tables:CreateNamespace",
 "s3tables:GetNamespace",
 "s3tables:ListNamespaces",
 "s3tables>DeleteNamespace",
 "s3tables>DeleteTableBucket",
 "s3tables:CreateTable",
 "s3tables>DeleteTable",
 "s3tables:GetTable",
 "s3tables:ListTables",
 "s3tables:RenameTable",
 "s3tables:UpdateTableMetadataLocation",
 "s3tables:GetTableMetadataLocation",
 "s3tables:GetTableData",
 "s3tables:PutTableData"
],
 "Resource": [
 "arn:aws:s3tables:us-east-1:123456789012:bucket/*"
]
 }
]
}

```

Weitere Informationen finden Sie unter [Anforderungen für Rollen, die zur Registrierung von Standorten verwendet werden](#).

4. Fügen Sie der IAM-Rolle die folgende Vertrauensrichtlinie hinzu, damit der Lake Formation-Dienst die Rolle übernehmen und temporäre Anmeldeinformationen an die integrierten Analyse-Engines weitergeben kann.

```

{
 "Effect": "Allow",
 "Principal": {
 "Service": "lakeformation.amazonaws.com"
 },
 "Action": [
 "sts:AssumeRole",

```

```

 "sts:SetSourceIdentity",
 "sts:SetContext" # add action to trust relationship when using IAM Identity
 center principals with Lake Formation
]
}

```

## Aktivierung der Amazon S3 S3-Tabellenintegration

Sie können Amazon S3 S3-Tabellen-Buckets mit der Amazon S3 S3-Konsole erstellen und sie in AWS Analysedienste integrieren. Weitere Informationen finden Sie unter [Verwenden von Amazon S3 S3-Tabellen mit AWS Analysediensten](#).

In AWS Lake Formation können Sie die Integration von Amazon S3 Tables mit AWS Glue Data Catalog und AWS Lake Formation mithilfe der Lake Formation Formation-Konsole aktivieren oder verwenden AWS CLI.

So integrieren Sie Amazon S3 S3-Tabellen mit Data Catalog und Lake Formation (Konsole)

1. Öffnen Sie die Lake Formation Formation-Konsole unter <https://console.aws.amazon.com/lakeformation/>.
2. Wählen Sie im Navigationsbereich unter Datenkatalog die Option Kataloge aus.
3. Wählen Sie auf der Seite „Kataloge“ die Option S3-Tabellenintegration aktivieren aus.

**Catalogs**

▼ **How it works**

- Create a catalog**  
Register Redshift databases as catalogs in the Data Catalog.  
[Learn more](#)
- Manage catalog permissions**  
Manage permissions for specific catalogs, databases, tables and fine-grained data access. [Learn more](#)
- Access from query editors**  
Access catalog objects from [Redshift Query Editor v2](#) and [Athena Console](#).

ⓘ Automatically create a catalog from an S3 table bucket. Allows external engines to access data in Amazon S3 locations with full table access. Enable S3 Table integration ✕

**Catalogs (2)** [Info](#)

A catalog is the top level in the Data Catalog's three-level data hierarchy and contains Data Catalog objects.

🔍 Find catalogs by name

| Name | Type | Source | Owner account ID | Shared resource | Shared resource... | Shared resource ... |
|------|------|--------|------------------|-----------------|--------------------|---------------------|
|------|------|--------|------------------|-----------------|--------------------|---------------------|

🔄 Actions ▼ View ▼ Create catalog

4. Wählen Sie eine IAM-Rolle mit den erforderlichen Berechtigungen, damit Lake Formation davon ausgehen kann, Anmeldeinformationen an die analytischen Abfrage-Engines weiterzugeben. Informationen zu den Berechtigungen, die für die Rolle für den Datenzugriff erforderlich sind, finden Sie [step3-permissions](#) im Abschnitt Voraussetzungen.

### Enable S3 Table integration ✕

Once integration is enabled, every table bucket in this account and region will automatically be available under the s3tablescatalog catalog in AWS Data Catalog.

**Select a principal to register**  
AWS LakeFormation needs to be able to call S3 Tables APIs on your behalf to retrieve S3 Table buckets, namespace, and tables. S3 tables must be registered with AWS LakeFormation with an IAM role that can be assumed.

Select a role to register ▼

☐ Allow external engines to access data in Amazon S3 locations with full table access

**Cancel** **Enable**

**i** When you register an S3 tables catalog in Lake Formation, the registering principal automatically receives permissions to perform all supported Lake Formation operations on the registered data location.

- Wählen Sie die Option Externen Engines den Zugriff auf Daten an Amazon S3 S3-Standorten mit vollständigem Tabellenzugriff erlauben aus. Wenn Sie den vollständigen Tabellenzugriff für Engines von Drittanbietern aktivieren, gibt Lake Formation Anmeldeinformationen direkt an die Drittanbieter-Engine zurück, ohne eine IAM-Sitzungs-Tag-Validierung durchzuführen. Das bedeutet, dass Sie keine detaillierten Zugriffskontrollen für Lake Formation auf die Tabellen anwenden können, auf die zugegriffen wird.
- Wählen Sie Enable (Aktivieren) aus. Der neue Katalog für S3-Tabellen wird der Katalogliste hinzugefügt. Wenn Sie die Integration des S3-Tabellenkatalogs aktivieren, registriert der Dienst den Datenstandort des S3-Tabellen-Buckets bei Lake Formation.
- Wählen Sie den Katalog aus, um Katalogobjekte anzuzeigen und anderen Prinzipalen Berechtigungen zu erteilen.

Success Successfully created catalog s3tablescatalog.

### s3tablescatalog Actions

#### Catalog summary

| Name            | Permissions for newly created tables | Description |
|-----------------|--------------------------------------|-------------|
| s3tablescatalog | -                                    | -           |

#### Catalog connection details

Connect to data stored in lakes, warehouses, and other external data sources and publish to unified Iceberg data catalog.

|                                |          |
|--------------------------------|----------|
| Access for Open Source Engine  | IAM role |
| -                              | -        |
| Namespace register status      | KMS key  |
| Registered to AWS Data Catalog | -        |

Objects Permissions

#### Data permissions for catalog s3tablescatalog (1)

View all permissions
Revoke
Grant

| <input type="checkbox"/> | Principal | Princip... | Princip...    | Resour... | Database | Table | Resource | Catalog     | LF-Tag ex... | Permissions     | Grantable       | RAM F |
|--------------------------|-----------|------------|---------------|-----------|----------|-------|----------|-------------|--------------|-----------------|-----------------|-------|
| <input type="checkbox"/> | Admin     | IAM role   | arn:aws:ia... | Catalog   | -        | -     | -        | 45178558... | -            | All, Alter, ... | All, Alter, ... | -     |

Informationen zum Erstellen von Katalogen mit mehreren Ebenen finden Sie im Abschnitt [Erstellen eines Tabellen-Buckets](#) im Amazon Simple Storage Service-Benutzerhandbuch.

Um Amazon S3-Tabellen mit Data Catalog und Lake Formation (CLI) zu integrieren

1. Registrieren Sie den S3 Tables-Katalog als Lake Formation Formation-Datenspeicherort.

```
aws lakeformation register-resource \
 --resource-arn 'arn:aws:s3tables:us-east-1:123456789012:bucket/*' \
 --role-arn 'arn:aws:iam::123456789012:role/LakeFormationDataAccessRole' \
 --with-federation
 --with-privileged-access
```

2. Erstellen Sie einen Katalog.

```
aws glue create-catalog --cli-input-json file://input.json

'{
 "Name": "s3tablescatalog",
 "CatalogInput" : {
 "FederatedCatalog": {
 "Identifier": "arn:aws:s3tables:us-east-1:123456789012:bucket/*",
 "ConnectionName": "aws:s3tables"
 },
 },
}
```



```
"CreateDatabaseDefaultPermissions": [],
"CreateTableDefaultPermissions": []
}
'
```

## Datenbanken und Tabellen im S3-Tabellenkatalog erstellen

Sie können Datenbanken erstellen, um Ihre Apache Iceberg-Tabellen zu organisieren, und Tabellen, um das Schema und den Speicherort Ihrer Daten im S3-Tabellenkatalog zu definieren.

Erstellen Sie eine Datenbank (Konsole)

1. Öffnen Sie die Lake Formation Formation-Konsole unter <https://console.aws.amazon.com/lakeformation/> und melden Sie sich als Data Lake-Administrator oder Datenbankersteller an.
2. Wählen Sie im Navigationsbereich unter Datenkatalog die Option Datenbanken aus.
3. Wählen Sie Datenbank erstellen aus.
4. Wählen Sie auf der Seite Datenbank erstellen die Option Datenbank aus und geben Sie die folgenden Details ein:
  - Name — Ein eindeutiger Name für die Datenbank
  - Datenkatalog — Wählen Sie den S3-Tabellenkatalog aus. Die Datenbank wird sich in diesem Katalog befinden.
  - Beschreibung — (Optional) Fügen Sie eine Beschreibung und einen Speicherort hinzu.
  - IAM-Zugriffskontrolle für neue Tabellen — Wählen Sie optional die Option Nur IAM-Zugriffskontrolle für neue Tabellen in dieser Datenbank verwenden aus. Informationen zu dieser Option finden Sie im Abschnitt [Ändern der Standardeinstellungen für Ihren Data Lake](#).
  - Wählen Sie Datenbank erstellen. Die erstellte Datenbank wird im S3-Tabellenkatalog angezeigt.

Erstellen Sie eine Datenbank mit AWS CLI

Der folgende CLI-Befehl zeigt, wie eine Datenbank im S3-Tabellenkatalog erstellt wird.

```
aws glue create-database
--region us-east-1 \
--catalog-id "123456789012:s3tablescatalog/test" \

```

```
--database-input \
'{ "Name": "testglueclidbcreation" }'
```

## Erstellen Sie eine Tabelle (AWS-Managementkonsole)

Sie können Apache Iceberg-Metadatentabellen im S3-Tabellenkatalog mithilfe der Lake Formation Formation-Konsole oder der AWS Glue CreateTable API erstellen.

1. Öffnen Sie die Lake Formation Formation-Konsole unter <https://console.aws.amazon.com/lakeformation/> und melden Sie sich als Data Lake-Administrator oder als Benutzer mit entsprechender CreateTable Berechtigung an.
2. Wählen Sie im Navigationsbereich unter Datenkatalog die Option Tabellen aus.
3. Wählen Sie Create table (Tabelle erstellen) aus.
4. Geben Sie auf der Seite Tabelle erstellen die Tabellendetails ein:

## Create table [Info](#)

### Table details

Create a table in the Data Catalog.

#### Name

If you plan to access the table from Amazon Athena, then the name should be under 256 characters and contain only lowercase letters (a-z), numbers (0-9), and underscore (\_). For more information, see [Athena names](#).

#### Catalog

Table is contained within this catalog.



[Create a catalog](#)

#### Database

Table is contained within this database.



[Create database](#)

### Table format

#### ☒ Apache Iceberg Table

Create a table in the Apache Iceberg table format

### Schema [Info](#)

View and manage table schema.

[Upload schema](#)[Delete](#)[Edit](#)[Add column](#)

< 1 >

No available schema

[Cancel](#)[Submit](#)

- Name — Geben Sie einen eindeutigen Namen für die Tabelle ein.
- Katalog — Wählen Sie den Katalog der S3-Tabellen als Katalog aus.
- Datenbank — Wählen Sie die Datenbank im S3-Tabellenkatalog aus.

- **Beschreibung** — Geben Sie eine Beschreibung für die Tabelle ein.
- **Schema** — Wählen Sie Spalten hinzufügen, um Spalten und Datentypen der Spalten hinzuzufügen. Sie haben die Möglichkeit, eine leere Tabelle zu erstellen und das Schema später zu aktualisieren. Mit Iceberg können Sie Schema und Partition weiterentwickeln, nachdem Sie die Tabelle erstellt haben. Sie können Athena-Abfragen verwenden, um das Tabellenschema zu aktualisieren, und Spark-Abfragen, um Partitionen zu aktualisieren.

5. Wählen Sie Absenden aus.

Erstellen Sie eine Tabelle (AWS CLI)

```
aws glue create-table \
--database-name "testglueclidbcreation" \
--catalog-id "123456789012:s3tablescatalog/test" \
--region us-east-1 \
--table-input \
'{ "Name": "testtablegluecli", "Parameters": { "format": "ICEBERG" },
 "StorageDescriptor": { "Columns": [{"Name": "x", "Type": "int", "Parameters":
 {"required": "true"}}] } }'
```

## Registrierung eines Amazon S3 S3-Tabellen-Buckets in einem anderen AWS Konto

Sie können einzelne Amazon S3 S3-Tabellen-Buckets (ARN-Format:arn:aws:s3tables:us-east-1:*account-id*:bucket/*bucket-name*) von einem AWS Konto bei Lake Formation in einem anderen Konto registrieren. Sie können beispielsweise einen Tabellen-Bucket von Konto A in Lake Formation von Konto B registrieren.

### Voraussetzungen

Bevor Sie mit der kontoübergreifenden Bucket-Registrierung beginnen:

- Erstellen Sie einen Tabellen-Bucket in Konto A.
- Erstellen Sie eine IAM-Rolle in Konto B mit den entsprechenden Berechtigungen für die Bucket-Registrierung.

Weitere Informationen zu den Berechtigungen, die für die Registrierung eines Tabellen-Buckets bei Lake Formation erforderlich sind, finden Sie unter [Voraussetzungen für die Integration des Amazon S3 S3-Tabellenkatalogs mit Data Catalog und Lake Formation](#).

- Registrieren Sie den Tabellen-Bucket in dem Konto, in dem Sie den S3-Tabellenkatalog erstellen werden.
- Für den kontoübergreifenden Zugriff muss es sich bei der Rolle, die bei der Registrierung des Tabellen-Buckets angegeben wurde, um eine In-Account-Rolle mit entsprechenden Berechtigungen für den kontoübergreifenden Bucket handeln. Die Rolle benötigt die erforderlichen IAM-Aktionen von S3 Tables, um auf Bucket-Ressourcen zugreifen zu können.

## Kontoübergreifende Tabellen-Bucket-Registrierung

In den folgenden Verfahren ist Konto A das Konto, dem die Ressource gehört, und Konto B ist der Ort, an dem der Tabellen-Bucket für die Verwaltung von Zugriffsberechtigungen registriert wird.

1. Melden Sie sich bei Konto A AWS-Managementkonsole an.

Öffnen Sie die Amazon S3 S3-Konsole unter <https://console.aws.amazon.com/s3/>.

2. Erstellen Sie einen Tabellen-Bucket. Weitere Informationen finden Sie unter [Erstellen eines Tabellen-Buckets](#) im Amazon S3 S3-Benutzerhandbuch.
3. Registrieren Sie den Tabellen-Bucket in Konto B.

Verwenden Sie den AWS CLI , um den Tabellen-Bucket von Konto A bei Lake Formation in Konto B zu registrieren.

```
aws lakeformation register-resource \
--resource-arn 'arn:aws:s3tables:us-east-1:account-A-id:bucket/single-bucket-name' \
\
--role-arn arn:aws:iam::account-B-id:role/role-name \
--region us-east-1
```

Ersetzen Sie account-A-id single-bucket-name, account-B-id, und Rollenname durch Ihre spezifischen Werte.

4. Erstellen Sie als Nächstes einen Katalog für den Tabellen-Bucket in Konto B.

Erstellen Sie einen Katalog mit dem AWS CLI.

```
aws glue create-catalog --region us-east-1 \
--cli-input-json \
'{
 "Name": "catalog-name",
 "CatalogInput" : {
 "FederatedCatalog": {
 "Identifier": "arn:aws:s3tables:us-east-1:account A:bucket/single-bucket-name",
 "ConnectionName": "aws:s3tables"
 },
 "CreateDatabaseDefaultPermissions": [],
 "CreateTableDefaultPermissions": []
 }
}'
```

Ersetzen Sie *catalog-name*, *account-A-id*, und *bucket-name* durch Ihre spezifischen Werte.

Das folgende CLI-Beispiel zeigt, wie die Details des Katalogs angezeigt werden.

```
aws glue get-catalog \
--catalog-id account-id:catalog-name \
--region us-east-1
```

5. Erstellen Sie als Nächstes Datenbanken und Tabellen im neu erstellten Katalog in Konto B.

Erstellen Sie eine Datenbank.

```
aws glue create-database \
--region us-east-1 \
--catalog-id "account-B-id:catalog-name" \
--database-input \
'{
 "Name": "database-name"
}'
```

Erstellen Sie eine -Tabelle.

```
aws glue create-table \
--database-name database-name \
--catalog-id account-B-id:catalog-name\
```

```
--region us-east-1 \
--table-input \
{
 "Name": "table-name",
 "Parameters": {
 "format": "ICEBERG"
 },
 "StorageDescriptor": {
 "Columns": [
 {"Name": "x", "Type": "int", "Parameters": {"required": "true"}}
]
 }
}
```

Ersetzen Sie Datenbankname `account-B-id`, Katalogname und Tabellennamen durch Ihre spezifischen Werte.

- Die folgenden Beispiele zeigen, wie die Objekte im Katalog angezeigt werden.

Datenbankdetails anzeigen.

```
aws glue get-database \
 --name database-name \
 --catalog-id account-B-id:catalog-name \
 --region us-east-1
```

Tabellendetails anzeigen.

```
aws glue get-table \
 --name table-name \
 --database-name database-name \
 --catalog-id account-B-id:catalog-name \
 --region us-east-1
```

Ersetzen Sie Datenbanknamen `account-B-id`, Katalognamen und Tabellennamen durch Ihre spezifischen Werte.

## Gewähren von Berechtigungen

Nachdem Sie Ihre S3-Tabellen integriert haben, können Sie anderen IAM-Rollen und Benutzern in Ihrem Konto Berechtigungen für den S3-Tabellenkatalog und

die Katalogobjekte (Tabellen-Buckets, Datenbanken, Tabellen) gewähren. Mit Lake Formation Formation-Berechtigungen können Sie Zugriffskontrollen auf Tabellen-, Spalten- und Zeilenebene für Benutzer integrierter Analyse-Engines wie Amazon Redshift Spectrum und Athena definieren.

Sie können Berechtigungen entweder mithilfe der benannten Ressourcenmethode oder der Tag-Based Access Control (LF-TBAC) -Methode (Lake Formation, Tag-Based Access Control) gewähren. Bevor Sie Berechtigungen mithilfe von LF-Tags und LF-Tag-Ausdrücken gewähren, müssen Sie diese definieren und sie Datenkatalogobjekten zuweisen.

Weitere Informationen finden Sie unter [Verwaltung von LF-Tags für die Zugriffskontrolle auf Metadaten](#).

Sie können Datenbanken und Tabellen mit externen AWS Konten teilen, indem Sie den externen Konten Lake Formation Formation-Berechtigungen gewähren. Benutzer können dann Abfragen und Jobs ausführen, die Tabellen mehrerer Konten verknüpfen und abfragen. Wenn Sie eine Katalogressource mit einem anderen Konto gemeinsam nutzen, können die Principals in diesem Konto mit dieser Ressource arbeiten, als ob sich die Ressource in ihrem Datenkatalog befände.

Wenn Sie Datenbanken und Tabellen mit externen Konten gemeinsam nutzen, ist die Superuser-Berechtigung nicht verfügbar.

Ausführliche Anweisungen zur Erteilung von Berechtigungen finden Sie im [Verwaltung von Lake Formation Formation-Berechtigungen](#) Abschnitt.

AWS CLI Beispiel für die Erteilung von Berechtigungen für eine Amazon S3 S3-Tabelle

```
aws lakeformation grant-permissions \
--cli-input-json \
'{
 "Principal": {
 "DataLakePrincipalIdentifier":"arn:aws:iam::111122223333:role/DataAnalystRole"
 },
 "Resource": {
 "Table": {
 "CatalogId":"111122223333:s3tablescatalog/amzn-s3-demo-bucket1",
 "DatabaseName":"S3 table bucket namespace <example_namespace>",
 "Name":"S3 table bucket table name <example_table>"
 }
 },
 "Permissions": [
 "SELECT"
]
}
```



```
}'
```

Im Folgenden sind die Parameter aufgeführt, die in den Befehl aufgenommen werden müssen:

- **DataLakePrincipalIdentifier** — IAM-Benutzer-, Rollen- oder Gruppen-ARN zur Erteilung von Berechtigungen
- **CatalogId** — 12-stellige AWS Konto-ID, der der Datenkatalog gehört
- **DatabaseName** — Name des Namespaces für den Amazon S3 S3-Tabellen-Bucket
- **Name** — Name der Amazon S3 S3-Tabelle, Bucket-Tabellenname
- **Berechtigungen** — Zu erteilende Berechtigungen. Zu den Optionen gehören: SELECT, INSERT, DELETE, DESCRIBE, ALTER, DROP, ALLL und SUPER

## Zugreifen auf gemeinsam genutzte Amazon S3 S3-Tabellen

Nachdem Sie kontoübergreifende Berechtigungen für eine Datenbank oder Tabelle im S3-Tabellenkatalog erteilt haben, müssen Sie für den Zugriff auf die Ressourcen Ressourcenlinks zu den gemeinsam genutzten Datenbanken und Tabellen erstellen.

1. Erstellen Sie im Zielkonto (dem Konto, das die gemeinsam genutzten Ressourcen empfängt) einen Datenbankressourcen-Link. Detaillierte Anweisungen finden Sie unter [Einen Ressourcenlink zu einer gemeinsam genutzten Datenkatalog-Datenbank erstellen](#).

### CLI-Beispiel zum Erstellen eines Datenbankressourcenlinks

```
aws glue create-database
--region us-east-1
--catalog-id "111122223333"
--database-input \
'{
 "Name": "s3table_resourcelink",
 "TargetDatabase": {
 "CatalogId": "011426214932:s3tablescatalog/chmni-s3-table-bucket-011426214932",
 "DatabaseName": "s3_table_ns"
 },
 "CreateTableDefaultPermissions": []
}'
```

2. Erteilen Sie kontoübergreifende Berechtigungen für die Tabelle.

## CLI-Beispiel für die kontoübergreifende Erteilung von Berechtigungen

```
aws lakeformation grant-permissions \
--region us-east-1 \
--cli-input-json \
'{
 "Principal": {
 "DataLakePrincipalIdentifier": "arn:aws:iam::111122223333:role/
S3TablesTestExecRole"
 },
 "Resource": {
 "Table": {
 "CatalogId": "011426214932:s3tablescatalog/chmni-s3-table-
bucket-011426214932",
 "DatabaseName": "s3_table_ns",
 "Name": "test_s3_iceberg_table"
 }
 },
 "Permissions": [
 "ALL"
]
}'
```

3. Erteilen Sie die DESCRIBE Genehmigung für die Lake Formation für den Ressourcenlink.

CLI-Beispiel für die Erteilung der Beschreibungsberechtigung für den Ressourcenlink.

```
aws lakeformation grant-permissions \
--principal DataLakePrincipalIdentifier=arn:aws:iam::111122223333:role/
S3TablesTestExecRole
--resource Database='{CatalogId=111122223333;, Name=s3table_resourcelink}' \
--permissions DESCRIBE
```

## Erstellen eines verwalteten Amazon Redshift Redshift-Katalogs in der AWS Glue Data Catalog

Möglicherweise verfügen Sie heute nicht über einen Amazon Redshift Redshift-Producer-Cluster oder einen Amazon Redshift Redshift-Datashare, möchten aber Amazon Redshift Redshift-Tabellen mit dem erstellen und verwalten. AWS Glue Data Catalog Sie können damit beginnen, einen AWS Glue

verwalteten Katalog mithilfe der `glue:CreateCatalog` API oder der AWS Lake Formation Konsole zu erstellen, indem Sie den Katalogtyp auf `Managed` und `Catalog source` als `Redshift` festlegen. In diesem Schritt wird Folgendes ausgeführt:

- Erstellt einen Katalog im Datenkatalog
- Registriert den Katalog als Datenspeicherort für Lake Formation
- erstellt eine von Amazon Redshift verwaltete serverlose Arbeitsgruppe
- Verknüpft Amazon Redshift Serverless Workgroup und Data Catalog mithilfe eines Datashare-Objekts

Um einen verwalteten Katalog zu erstellen und Berechtigungen einzurichten (Konsole)

1. Öffnen Sie die Lake Formation Konsole unter <https://console.aws.amazon.com/lakeformation/>.
2. Wählen Sie im Navigationsbereich unter Datenkatalog die Option Kataloge aus.
3. Wählen Sie die Option Katalog erstellen aus.
4. Geben Sie auf der Seite „Katalogdetails festlegen“ die folgenden Informationen ein:
  - Name — Ein eindeutiger Name für Ihren verwalteten Katalog. Der Name kann nicht geändert werden und muss in Kleinbuchstaben geschrieben werden. Der Name darf aus maximal 255 Zeichen bestehen.
  - Typ — Wählen Sie `Managed catalog` den Katalogtyp aus.
  - Speicher — Wählen Sie `Redshift Speicher` aus.
  - Beschreibung — Geben Sie eine Beschreibung für den aus der Datenquelle erstellten Katalog ein.
5. Sie können Apache Spark-Anwendungen verwenden, die auf Amazon EMR auf Amazon EC2 ausgeführt werden, um auf die Amazon Redshift Redshift-Datenbanken in der zuzugreifen. AWS Glue Data Catalog

Damit Apache Spark Lese- und Schreibvorgänge in verwaltetem Amazon Redshift-Speicher ausführen kann, AWS Glue wird ein verwalteter Amazon Redshift Redshift-Cluster mit den Rechen- und Speicherressourcen erstellt, die für Lese- und Schreibvorgänge erforderlich sind, ohne die Amazon Redshift Data Warehouse-Workloads zu beeinträchtigen. Sie müssen auch eine IAM-Rolle mit den Berechtigungen bereitstellen, die für die Übertragung von Daten zum und vom Amazon S3 S3-Bucket erforderlich sind. Informationen zu den

für die Datenübertragungsrolle erforderlichen Berechtigungen finden Sie in Schritt 5 im [Voraussetzungen für die Verwaltung von Amazon Redshift Redshift-Namespaces in AWS Glue Data Catalog](#) Abschnitt.

6. Standardmäßig werden die Daten im Amazon Redshift Redshift-Cluster mit einem AWS verwalteten Schlüssel verschlüsselt. Lake Formation bietet die Möglichkeit, Ihren benutzerdefinierten KMS-Schlüssel für die Verschlüsselung zu erstellen. Wenn Sie einen vom Kunden verwalteten Schlüssel verwenden, müssen Sie dem Schlüssel bestimmte Schlüsselrichtlinien hinzufügen.
7. Wählen Sie die Verschlüsselungseinstellungen anpassen, wenn Sie einen vom Kunden verwalteten Schlüssel verwenden, um die Daten im verwalteten Amazon Redshift Redshift-Speicher zu verschlüsseln. Um einen benutzerdefinierten Schlüssel zu verwenden, müssen Sie Ihrem KMS-Schlüssel eine zusätzliche benutzerdefinierte Richtlinie für verwaltete Schlüssel hinzufügen. Weitere Informationen finden Sie unter [Voraussetzungen für die Verwaltung von Amazon Redshift Redshift-Namespaces in AWS Glue Data Catalog](#).
8. Verschlüsselungsoptionen — Wählen Sie die Option Verschlüsselungseinstellungen anpassen, wenn Sie einen benutzerdefinierten Schlüssel zum Verschlüsseln des Katalogs verwenden möchten. Um einen benutzerdefinierten Schlüssel zu verwenden, müssen Sie Ihrem KMS-Schlüssel eine zusätzliche benutzerdefinierte Richtlinie für verwaltete Schlüssel hinzufügen.
9. Wählen Sie Weiter, um anderen Prinzipalen Berechtigungen zu gewähren.
10. Wählen Sie auf der Seite Berechtigungen gewähren die Option Berechtigungen hinzufügen aus.
11. Wählen Sie auf dem Bildschirm „Berechtigungen hinzufügen“ die Hauptbenutzer und die Arten der zu erteilenden Berechtigungen aus.

## Add permissions



### Principals

Choose the principals to grant permissions.



#### IAM users and roles

Users or roles from this AWS account.



#### SAML users and groups

SAML users and group or QuickSight ARNs.



#### External accounts

AWS account, AWS organization or IAM principal outside of this account

### IAM users and roles

Add one or more IAM users or roles.

Choose IAM principals to add



UserRole X  
Role

### Catalog permissions

Choose the permissions to grant on the catalog. Choosing Super user overwrites individual permissions, granting unrestricted administrative access.

☐ Super user

A super user has unrestricted administrative privileges to perform any operation on all resources within the catalog (databases, tables, and views).

### Catalog permissions

Choose specific access permissions to grant.

☒ Create database ☐ Describe ☐ Alter

☐ Drop

☐ Super

This permission is the union of all the individual permissions to the left, and supersedes them.

### Grantable permissions

Choose the permission that can be granted to others.

☒ Create database ☐ Describe ☐ Alter

☐ Drop

☐ Super

This permission allows the principal to grant any of the permissions to the left, and supersedes those grantable permissions.

Cancel

Add

- Wählen Sie im Abschnitt Prinzipale einen Prinzipaltyp aus und geben Sie dann Prinzipale an, denen Berechtigungen erteilt werden sollen.

- IAM-Benutzer und -Rollen – wählen Sie mindestens einen Benutzer oder eine Rolle aus der Liste der IAM-Benutzer und -Rollen aus.
- SAML-Benutzer und -Gruppen — Geben Sie für SAML und Amazon Quick Benutzer und Gruppen einen oder mehrere Amazon-Ressourcennamen (ARNs) für Benutzer oder Gruppen ein, die über SAML verbunden sind, oder ARNs für Amazon Quick-Benutzer oder -Gruppen. Drücken Sie nach jedem ARN die Eingabetaste.

Informationen zur Erstellung der Befehle finden Sie unter Befehle AWS CLI gewähren ARNs und widerrufen. AWS CLI

- Wählen Sie im Abschnitt Berechtigungen die Berechtigungen und erteilbare Berechtigungen aus.

Wählen Sie unter Katalogberechtigungen mindestens eine Berechtigung aus, die Sie gewähren möchten.

Wählen Sie Superuser aus, um uneingeschränkte Administratorberechtigungen für alle Ressourcen im Katalog zu gewähren.

Wählen Sie unter Erteilbare Berechtigungen die Berechtigungen aus, die der Empfänger der Gewährung anderen Hauptbenutzern in seinem AWS Konto gewähren kann. Diese Option wird nicht unterstützt, wenn Sie einem IAM-Prinzipal von einem externen Konto aus Berechtigungen gewähren.

12. Wählen Sie Weiter, um die Informationen zu überprüfen und den Katalog zu erstellen. In der Katalogliste wird der neue verwaltete Katalog angezeigt.

So erstellen Sie einen Verbundkatalog (CLI)

- Das folgende Beispiel zeigt, wie ein Verbundkatalog erstellt wird.

```
aws glue create-catalog --cli-input-json file://input.json

{
 "Name": "CatalogName",
 "CatalogInput": {
 "Description": "Redshift published Catalog",
 "CreateDatabaseDefaultPermissions" : [],
 "CreateTableDefaultPermissions": [],
 "CatalogProperties": {
 "DataLakeAccessProperties" : {
```

```

 "DataLakeAccess" : "true",
 "DataTransferRole" : "DTR arn",
 "KMSKey": "kms key arn", // Optional
 "CatalogType": "aws:redshift"
 }
}
}
}

```

## Get-Catalog-Antwort von Glue

```

aws glue get-catalog \
 --catalog-id account-id:catalog-name \
 --region us-east-1

Response:
{
 "Catalog": {
 "Name": "CatalogName",
 "Description": "Glue Catalog for Redshift z-etl use case",
 "CreateDatabaseDefaultPermissions" : [],
 "CreateTableDefaultPermissions": [],
 "CatalogProperties": {
 "DataLakeAccessProperties" : {
 "DataLakeAccess": "true",
 "DataTransferRole": "DTR arn",
 "KMSKey": "kms key arn",
 "ManagedWorkgroupName": "MWG name",
 "ManagedWorkgroupStatus": "MWG status",
 "RedshiftDatabaseName": "RS db name",
 "NamespaceArn": "namespace key arn",
 "CatalogType": "aws:redshift"
 }
 }
 }
}

```

# Verwaltung von Berechtigungen für Daten in einem Amazon Redshift Redshift-Datashare

Mit AWS Lake Formation können Sie Daten in einem Datashare von Amazon Redshift sicher verwalten. Amazon Redshift ist ein vollständig verwalteter Data-Warehouse-Service im Petabyte-Bereich in der Cloud. AWS Mithilfe der Funktion zur gemeinsamen Nutzung von Daten hilft Ihnen Amazon Redshift dabei, Daten gemeinsam zu nutzen. AWS-Konten Weitere Informationen zur gemeinsamen Nutzung von Amazon Redshift-Daten finden Sie unter [Überblick über die gemeinsame Nutzung von Daten in Amazon Redshift](#).

In Amazon Redshift erstellt der Producer-Cluster-Administrator eine Datenfreigabe und teilt sie mit dem Data Lake-Administrator. step-by-stepAnweisungen zum Erstellen eines Data Lake-Administrators finden Sie unter. [Erstellen Sie einen Data Lake-Administrator](#)

Nachdem Sie (Data Lake-Administrator) die Datenfreigabe akzeptiert haben, müssen Sie eine AWS Glue Data Catalog Datenbank für die spezifische Datenfreigabe erstellen. Auf diese Weise können Sie den Zugriff darauf mithilfe der Lake Formation Formation-Berechtigungen steuern. Lake Formation ordnet jeden Datashare einer entsprechenden Datenkatalogdatenbank zu. Diese werden im Datenkatalog als Verbunddatenbanken angezeigt.

Eine Datenbank wird als föderierte Datenbank bezeichnet, wenn sie auf eine Entität außerhalb des Datenkatalogs verweist. Tabellen und Ansichten im Amazon Redshift Redshift-Datashare werden als einzelne Tabellen im Datenkatalog aufgeführt. Sie können die Verbunddatenbank mit ausgewählten IAM-Prinzipalen und SAML-Benutzern innerhalb desselben Kontos oder in einem anderen Konto mit Lake Formation teilen. Sie können auch Zeilen- und Spaltenfilterausdrücke verwenden, um den Zugriff auf bestimmte Daten einzuschränken. Weitere Informationen finden Sie unter [Datenfilterung und Sicherheit auf Zellebene in Lake Formation](#).

Um Benutzern Zugriff auf eine Amazon Redshift Redshift-Datenfreigabe zu gewähren, müssen Sie wie folgt vorgehen:

1. Aktualisieren Sie die Datenkatalogeinstellungen, um Lake Formation Formation-Berechtigungen zu aktivieren.
2. Nehmen Sie die Datashare-Einladung des Amazon Redshift Producer-Cluster-Administrators an und registrieren Sie das Datashare in Lake Formation.

Nach Abschluss dieses Schritts können Sie den Datenaustausch im Lake Formation Data Catalog verwalten.



3. Erstellen Sie eine Verbunddatenbank und definieren Sie Berechtigungen für diese Datenbank.
4. Erteilen Sie Benutzern Berechtigungen für Datenbanken und Tabellen. Sie können die gesamte Datenbank oder eine Teilmenge von Tabellen für Benutzer desselben Kontos oder eines anderen Kontos gemeinsam nutzen.

Einschränkungen finden Sie unter [Einschränkungen beim Datenaustausch mit Amazon Redshift](#).

## Themen

- [Voraussetzungen für die Einrichtung von Berechtigungen für Amazon Redshift Redshift-Datenfreigaben](#)
- [Berechtigungen für Amazon Redshift Redshift-Datenfreigaben einrichten](#)
- [Abfragen verbundener Datenbanken](#)

## Voraussetzungen für die Einrichtung von Berechtigungen für Amazon Redshift Redshift-Datenfreigaben

Aktualisieren Sie die Standardeinstellungen für den Datenkatalog

Um Lake Formation-Berechtigungen für die Datenkatalogressourcen zu aktivieren, empfehlen wir, die Standardeinstellungen für den Datenkatalog in Lake Formation zu deaktivieren. Weitere Informationen finden Sie unter [Ändern Sie das Standardberechtigungsmodell oder verwenden Sie den hybriden Zugriffsmodus](#).

### Berechtigungen aktualisieren

Zusätzlich zu den Data Lake-Administratorberechtigungen (AWSLakeFormationDataAdmin) sind auch die folgenden Berechtigungen erforderlich, um eine Amazon Redshift-Datenfreigabe in Lake Formation zu akzeptieren:

- `glue:PassConnection on aws:redshift`
- `redshift:AssociateDataShareConsumer`
- `redshift:DescribeDataSharesForConsumer`
- `redshift:DescribeDataShares`

Der IAM-Benutzer des Data Lake-Administrators verfügt implizit über die folgenden Berechtigungen.

- `data_location_access`
- Datenbank erstellen
- Lakeformation: Ressource registrieren

## Berechtigungen für Amazon Redshift Redshift-Datenfreigaben einrichten

In diesem Thema werden die Schritte beschrieben, die Sie ausführen müssen, um eine Einladung zur gemeinsamen Nutzung anzunehmen, eine Verbunddatenbank zu erstellen und Berechtigungen zu erteilen. Sie können die Lake Formation Formation-Konsole oder die AWS Command Line Interface (AWS CLI) verwenden. Die Beispiele in diesem Thema zeigen den Producer-Cluster, den Datenkatalog und den Datenverbraucher in demselben Konto.

Weitere Informationen zu den kontoübergreifenden Funktionen von Lake Formation finden Sie unter [Kontoübergreifender Datenaustausch in Lake Formation](#).

So richten Sie Berechtigungen für eine Datenfreigabe ein

1. Überprüfen Sie eine Datashare-Einladung und akzeptieren Sie sie.

### Console

1. Melden Sie sich bei der Lake Formation Formation-Konsole als Data Lake-Administrator unter an <https://console.aws.amazon.com/lakeformation/>. Navigieren Sie zur Seite „Datenfreigabe“.
2. Überprüfen Sie die Datashares, auf die Sie zugreifen dürfen. In der Spalte Status wird Ihr aktueller Teilnahmestatus für den Datenaustausch angezeigt. Der Status Ausstehend gibt an, dass Sie zu einem Datashare hinzugefügt wurden, ihn aber noch nicht akzeptiert oder die Einladung abgelehnt haben.
3. Um auf eine DataShare-Einladung zu antworten, wählen Sie den Namen des Datenaustauschs aus und klicken Sie auf Einladung überprüfen. Überprüfen Sie unter Datashare annehmen oder ablehnen die Details der Einladung. Wählen Sie Annehmen, um die Einladung anzunehmen, oder Ablehnen, um die Einladung abzulehnen. Sie erhalten keinen Zugriff auf den Datashare, wenn Sie die Einladung ablehnen.

## AWS CLI

Die folgenden Beispiele zeigen, wie Sie die Einladung ansehen, annehmen und registrieren können. Ersetzen Sie die AWS-Konto ID durch eine gültige AWS-Konto ID. Ersetzen Sie das `data-share-arn` durch den tatsächlichen Amazon-Ressourcennamen (ARN), der auf den Datashare verweist.

### 1. Eine ausstehende Einladung anzeigen.

```
aws redshift describe-data-shares \
 --data-share-arn 'arn:aws:redshift:us-
east-1:111122223333:datashare:abcd1234-1234-ab12-cd34-1a2b3c4d5e6f/
federatedds' \
```

### 2. Akzeptieren Sie eine Datenfreigabe.

```
aws redshift associate-data-share-consumer \
 --data-share-arn 'arn:aws:redshift:us-
east-1:111122223333:datashare:abcd1234-1234-ab12-cd34-1a2b3c4d5e6f/
federatedds' \
 --consumer-arn 'arn:aws:glue:us-east-1:111122223333:catalog
```

### 3. Registrieren Sie den Datashare im Lake Formation Formation-Konto. Verwenden Sie den [RegisterResource](#) API-Vorgang, um den Datashare in Lake Formation zu registrieren. `DataShareArn` ist der Eingabeparameter für `ResourceArn`

#### Note

Dies ist ein obligatorischer Schritt.

```
aws lakeformation register-resource \
 --resource-arn 'arn:aws:redshift:us-
east-1:111122223333:datashare:abcd1234-1234-ab12-cd34-1a2b3c4d5e6f/
federatedds'
```

### 2. Erstellen Sie eine Datenbank.

Nachdem Sie eine Datashare-Einladung angenommen haben, müssen Sie eine Datenbank erstellen, die auf die Amazon Redshift Redshift-Datenbank verweist, die dem Datashare zugeordnet ist. Sie müssen ein Data Lake-Administrator sein, um eine Datenbank erstellen zu können.

## Console

1. Wählen Sie im Bereich Einladungen den Datashare aus und klicken Sie auf Datenbankdetails festlegen.
2. Geben Sie im Feld Datenbankdetails festlegen einen eindeutigen Namen und eine eindeutige Kennung für die Datenfreigabe ein. Sie verwenden diesen Bezeichner, um den Datashare intern in der Metadatenhierarchie (DBName.Schema.Table) zuzuordnen.
3. Wählen Sie Weiter, um anderen Benutzern Berechtigungen für die gemeinsam genutzte Datenbank und die Tabellen zu gewähren.

## AWS CLI

Verwenden Sie den folgenden Beispielcode, um eine Datenbank zu erstellen, die mithilfe von auf die Amazon Redshift Redshift-Datenbank verweist, die mit Lake Formation gemeinsam genutzt wird AWS CLI.

```
aws glue create-database --cli-input-json \

'{
 "CatalogId": "111122223333",
 "DatabaseInput": {
 "Name": "tahoedb",
 "FederatedDatabase": {
 "Identifier": "arn:aws:redshift:us-
east-1:111122223333:datashare:abcd1234-1234-ab12-cd34-1a2b3c4d5e6f/federatedds",
 "ConnectionName": "aws:redshift"
 }
 }
}'
```

3. Erteilen Sie Berechtigungen.

Nachdem Sie die Datenbank erstellt haben, können Sie Benutzern in Ihrem Konto oder externen AWS-Konten Organisationen Berechtigungen gewähren. Sie können keine

Schreibberechtigungen für Daten (Einfügen, Löschen) und Metadatenberechtigungen (Ändern, Löschen, Erstellen) für die Verbunddatenbank gewähren, die einem Amazon Redshift Redshift-Datenshare zugeordnet ist. Weitere Informationen zum Erteilen von Berechtigungen finden Sie unter: [Verwaltung von Lake Formation Formation-Berechtigungen](#)

#### Note

Als Data Lake-Administrator können Sie nur Tabellen in den Verbunddatenbanken anzeigen. Um andere Aktionen ausführen zu können, müssen Sie sich selbst mehr Berechtigungen für diese Tabellen gewähren.

## Console

1. Wählen Sie auf dem Bildschirm Berechtigungen gewähren die Benutzer aus, denen Sie Berechtigungen erteilen möchten.
2. Wählen Sie Grant (Erteilen).

## AWS CLI

Verwenden Sie die folgenden Beispiele, um Datenbank- und Tabellenberechtigungen zu gewähren, indem Sie AWS CLI:

```
aws lakeformation grant-permissions --input-cli-json file://input.json

{
 "Principal": {
 "DataLakePrincipalIdentifier": "arn:aws:iam::111122223333:user/non-admin"
 },
 "Resource": {
 "Database": {
 "CatalogId": "111122223333",
 "Name": "tahoedb"
 }
 },
 "Permissions": [
 "DESCRIBE"
],
 "PermissionsWithGrantOption": [
```

```
]
 }
}
```

```
aws lakeformation grant-permissions --input-cli-json file://input.json
```

```
{
 "Principal": {
 "DataLakePrincipalIdentifier":
"arn:aws:iam::111122223333:user/non-admin"
 },
 "Resource": {
 "Table": {
 "CatalogId": "111122223333",
 "DatabaseName": "tahoedb",
 "Name": "public.customer"
 }
 },
 "Permissions": [
 "SELECT"
],
 "PermissionsWithGrantOption": [
 "SELECT"
]
}
```

## Abfragen verbundener Datenbanken

Nachdem Sie die Berechtigungen erteilt haben, können sich Benutzer anmelden und mit der Abfrage der Verbunddatenbank mithilfe von Amazon Redshift beginnen. Benutzer können jetzt den lokalen Datenbanknamen verwenden, um in SQL-Abfragen auf den Amazon Redshift Redshift-Datashare zu verweisen. In Amazon Redshift wird für die Kundentabelle im öffentlichen Schema, die über den Datashare gemeinsam genutzt wird, eine entsprechende Tabelle wie `public.customer` im Datenkatalog erstellt.

1. Vor der Abfrage der Verbunddatenbank mit Amazon Redshift erstellt der Clusteradministrator mithilfe des folgenden Befehls eine Datenbank aus der Data Catalog-Datenbank:

```
CREATE DATABASE sharedcustomerdb FROM ARN
'arn:aws:glue:<region>:111122223333:database/tahoedb' WITH DATA CATALOG SCHEMA
tahoedb
```

2. Der Clusteradministrator erteilt Nutzungsberechtigungen für die Datenbank.

```
GRANT USAGE ON DATABASE sharedcustomerdb TO IAM:user;
```

3. Sie (der Verbundbenutzer) können sich jetzt bei den SQL-Tools anmelden, um die Tabelle abzufragen.

```
Select * from sharedcustomerdb.public.customer limit 10;
```

Weitere Informationen finden Sie unter [Abfragen AWS Glue Data Catalog](#) im Amazon Redshift Management Guide.

## Verwaltung von Berechtigungen für Datensätze, die externe Metastores verwenden

Mit dem AWS Glue Data Catalog Metadatenverbund (Data Catalog Federation) können Sie den Datenkatalog mit externen Metastores verbinden, die Metadaten für Ihre Amazon S3 S3-Daten speichern, und Datenzugriffsberechtigungen mithilfe von AWS Lake Formation sicher verwalten. Sie müssen die Metadaten nicht aus dem externen Metastore in den Datenkatalog migrieren.

Der Datenkatalog bietet ein zentrales Metadaten-Repository, das die Verwaltung und Erkennung von Daten in unterschiedlichen Systemen erleichtert. Wenn Ihre Organisation Daten im Datenkatalog verwaltet, können Sie AWS Lake Formation damit den Zugriff auf Ihre Datensätze in Amazon S3 kontrollieren.

### Note

Derzeit unterstützen wir nur den Apache Hive-Metastore-Verbund (Version 3 und höher).

Um den Datenkatalogverbund einzurichten, stellen wir eine AWS Serverless Application Model (AWS SAM) -Anwendung namens [GlueDataCatalogFederation- HiveMetastore](#) in der bereit. AWS Serverless Application Repository

Die Referenzimplementierung wird GitHub als Open-Source-Projekt bei [AWS Glue Data Catalog Federation — Hive Metastore](#) bereitgestellt.

Die AWS SAM Anwendung erstellt und stellt die folgenden Ressourcen bereit, die für die Verbindung des Datenkatalogs mit dem Hive-Metastore erforderlich sind:

- Eine AWS Lambda Funktion — Hostet die Implementierung des Verbunddienstes, der zwischen dem Datenkatalog und dem Hive-Metastore kommuniziert. AWS Glue ruft diese Lambda-Funktion auf, um Metadatenobjekte aus dem Hive-Metastore abzurufen.
- Amazon API Gateway— Der Verbindungsendpunkt für Ihren Hive-Metastore, der als Proxy fungiert, um alle Aufrufe an die Lambda-Funktion weiterzuleiten.
- Eine IAM-Rolle — Eine Rolle mit den erforderlichen Berechtigungen, um die Verbindung zwischen dem Datenkatalog und dem Hive-Metastore herzustellen.
- AWS Glue Verbindung — Ein Amazon API Gateway AWS Glue Verbindungstyp, der den Amazon API Gateway Endpunkt und eine IAM-Rolle zum Aufrufen des Endpunkts speichert.

Wenn Sie Tabellen abfragen, ruft der AWS Glue Dienst zur Laufzeit den Hive-Metastore auf und ruft die Metadaten ab. Die Lambda-Funktion fungiert als Übersetzer zwischen dem Hive-Metastore und dem Datenkatalog.

Nachdem Sie die Verbindung hergestellt haben, müssen Sie, um die Metadaten im Hive-Metastore mit dem Datenkatalog zu synchronisieren, eine föderierte Datenbank im Datenkatalog mithilfe der Hive-Metastore-Verbindungsdetails erstellen und diese Datenbank der Hive-Datenbank zuordnen. Eine Datenbank wird als föderierte Datenbank bezeichnet, wenn sie auf eine Entität außerhalb des Datenkatalogs verweist.

Sie können Lake Formation Formations-Berechtigungen mithilfe der tagbasierten Zugriffskontrolle und der Methode der benannten Ressource auf die Verbunddatenbank anwenden und sie für mehrere AWS-Konten AWS Organizations, und Organisationseinheiten (OU) gemeinsam nutzen. Sie können die Verbunddatenbank auch direkt für IAM-Prinzipale von einem anderen Konto aus freigeben.

Mithilfe von Lake Formation Formations-Datenfiltern für die externen Hive-Tabellen können Sie detaillierte Berechtigungen auf Spalten-, Zeilen- und Zellenebene definieren. Sie können Amazon Athena, Amazon Redshift oder Amazon EMR verwenden, um die von Lake Formation verwalteten externen Hive-Tabellen abzufragen.

Weitere Informationen zum kontoübergreifenden Datenaustausch und zur Datenfilterung finden Sie unter:



- [Kontoübergreifender Datenaustausch in Lake Formation](#)
- [Datenfilterung und Sicherheit auf Zellebene in Lake Formation](#)

## Allgemeine Schritte zum Zusammenführen von Metadaten im Datenkatalog

1. Sie erstellen IAM-Benutzer und -Rollen, die über die entsprechenden Berechtigungen verfügen, um die AWS SAM Anwendung bereitzustellen und Verbunddatenbanken zu erstellen.
2. Sie registrieren den Amazon S3 S3-Datenstandort bei Lake Formation, indem Sie die `Enable Data Catalog federation` Option für Datensätze auswählen, die einen externen Hive-Metastore verwenden.
3. Sie konfigurieren die AWS SAM Anwendungseinstellungen (AWS Glue Verbindungsname, URL zum Hive-Metastore und Lambda-Funktionsparameter) und stellen die Anwendung bereit. AWS SAM
4. Die AWS SAM Anwendung stellt die Ressourcen bereit, die erforderlich sind, um den externen Hive-Metastore mit dem Datenkatalog zu verbinden.
5. Um Lake Formation Formation-Berechtigungen auf die Hive-Datenbank und -Tabellen anzuwenden, erstellen Sie mithilfe der Hive-Metastore-Verbindungsdetails eine Datenbank im Datenkatalog und ordnen diese Datenbank der Hive-Datenbank zu.
6. Gewähren Sie Principals in Ihrem Konto oder in einem anderen Konto Berechtigungen für die Verbunddatenbanken.

### Note

Sie können den Datenkatalog mit einem externen Hive-Metastore verbinden, Verbunddatenbanken erstellen und Abfragen und ETL-Skripts für Hive-Datenbanken und -Tabellen ausführen, ohne Lake Formation Formation-Berechtigungen anzuwenden. Für Quelldaten in Amazon S3, die nicht bei Lake Formation registriert sind, wird der Zugriff durch IAM-Berechtigungsrichtlinien für Amazon S3 und AWS Glue Aktionen bestimmt.

Einschränkungen finden Sie unter [Überlegungen und Einschränkungen beim Datenaustausch im Hive-Metadatenpeicher](#).

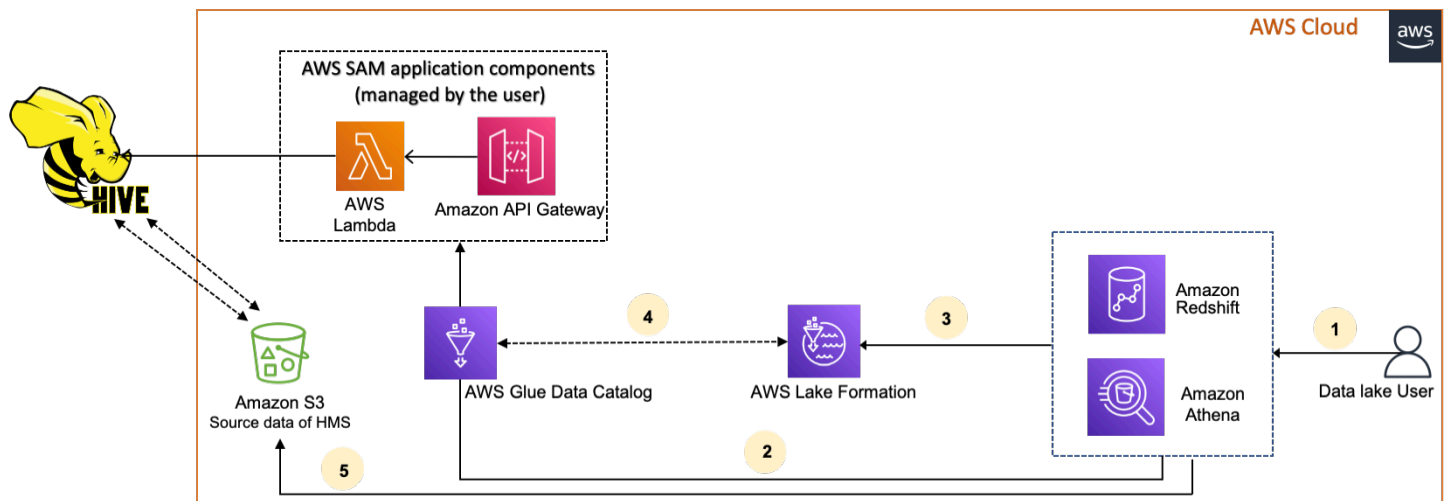
## Themen

- [Workflow](#)

- [Voraussetzungen für die Verbindung des Datenkatalogs mit dem Hive-Metastore](#)
- [Den Datenkatalog mit einem externen Hive-Metastore verbinden](#)
- [Weitere Ressourcen](#)

## Workflow

Das folgende Diagramm zeigt den Arbeitsablauf für die AWS Glue Data Catalog Verbindung mit einem externen Hive-Metastore.



1. Ein Principal sendet eine Anfrage mithilfe eines integrierten Dienstes wie Athena oder Redshift Spectrum.
2. Der integrierte Dienst ruft den Datenkatalog für die Metadaten auf, der wiederum den dahinter verfügbaren Hive-Metastore-Endpoint aufruft und Antworten auf Amazon API Gateway Metadatenanfragen erhält.
3. Der integrierte Dienst sendet die Anfrage an Lake Formation, um die Tabelleninformationen und Anmeldeinformationen für den Zugriff auf die Tabelle zu überprüfen.
4. Lake Formation autorisiert die Anfrage und sendet temporäre Anmeldeinformationen an die integrierte Anwendung, die den Datenzugriff ermöglicht.
5. Unter Verwendung der temporären Anmeldeinformationen, die er von Lake Formation erhalten hat, liest der integrierte Service die Daten aus Amazon S3 und gibt die Ergebnisse an den Principal weiter.

# Voraussetzungen für die Verbindung des Datenkatalogs mit dem Hive-Metastore

Um eine Verbindung mit einem externen Apache Hive-Metastore herzustellen und Datenzugriffsberechtigungen einzurichten, müssen Sie die folgenden Anforderungen erfüllen: AWS Glue Data Catalog

## Note

Wir empfehlen, dass ein Lake Formation-Administrator die AWS SAM Anwendung bereitstellt und nur ein privilegierter Benutzer die Hive-Metastore-Verbindung verwendet, um die entsprechenden Verbunddatenbanken zu erstellen.

## 1. Erstellen Sie IAM-Rollen.

Um die Anwendung bereitzustellen AWS SAM

- Erstellen Sie eine Rolle, die über die erforderlichen Berechtigungen für die Bereitstellung von Ressourcen (Lambda-Funktion Amazon API Gateway, IAM-Rolle und die AWS Glue Verbindung) verfügt, die für die Herstellung einer Verbindung zum Hive-Metastore erforderlich sind.

Um föderierte Datenbanken zu erstellen

Die folgenden Berechtigungen sind für Ressourcen erforderlich:

- `glue:CreateDatabase` on resource `arn:aws:glue:region:account-id:database/gluedatabasename`
- `glue:PassConnection` on resource `arn:aws:glue:region:account-id:connection/hms_connection`

## 2. Registrieren Sie den Amazon S3 S3-Standort bei Lake Formation.

Um Lake Formation zur Verwaltung und Sicherung der Daten in Ihrem Data Lake zu verwenden, müssen Sie den Amazon S3 S3-Standort, der die Daten für Tabellen im Hive-Metastore enthält, bei Lake Formation registrieren. Auf diese Weise kann Lake Formation Anmeldeinformationen an AWS Analysedienste wie Athena, Redshift Spectrum und Amazon EMR weitergeben.

Weitere Informationen zur Registrierung eines Amazon S3 S3-Standorts finden Sie unter [Hinzufügen eines Amazon S3 S3-Standorts zu Ihrem Data Lake](#).

Wenn Sie den Amazon S3 S3-Standort registrieren, aktivieren Sie das Kontrollkästchen Enable Data Catalog Federation, damit Lake Formation eine Rolle für den Zugriff auf Tabellen in einer Verbunddatenbank übernehmen kann.

[AWS Lake Formation](#) > [Data lake locations](#) > Register location

## Register location

### Amazon S3 location

Register an Amazon S3 path as the storage location for your data lake.

#### Amazon S3 path

Choose an Amazon S3 path for your data lake.

*e.g.: s3://bucket/prefix/*

**Browse**

#### Review location permissions - strongly recommended

Registering the selected location may result in your users gaining access to data already at that location. Before registering a location, we recommend that you review existing location permissions on resources in that location.

**Review location permissions**

#### IAM role

To add or update data, Lake Formation needs read/write access to the chosen Amazon S3 path. Choose a role that you know has permission to do this, or choose the **AWSServiceRoleForLakeFormationDataAccess** service-linked role. When you register the first Amazon S3 path, the service-linked role and a new inline policy are created on your behalf. Lake Formation adds the first path to the inline policy and attaches it to the service-linked role. When you register subsequent paths, Lake Formation adds the path to the existing policy.

AWSServiceRoleForLakeFormationDataAccess ▼

 Do not select the service linked role if you plan to use EMR.

☐ **Enable Data Catalog Federation**

Checking this box will allow Lake Formation to assume a role to access tables in a federated database.

Cancel

**Register location**

Weitere Informationen zur Registrierung eines Datenstandorts bei Lake Formation finden Sie unter [Konfigurieren Sie einen Amazon S3 S3-Standort für Ihren Data Lake](#).

### 3. Verwenden Sie die richtige Amazon EMR-Version.

Um Amazon EMR mit den verbundenen Hive-Metastore-Datenbanken verwenden zu können, benötigen Sie Hive Version 3.x oder höher und Amazon EMR Version 6.x oder höher.

## Den Datenkatalog mit einem externen Hive-Metastore verbinden

AWS Glue Data Catalog [Um den mit einem Hive-Metastore zu verbinden, müssen Sie eine AWS SAM Anwendung namens - bereitstellen. GlueDataCatalogFederation HiveMetastore](#) Sie erstellt die Ressourcen, die erforderlich sind, um den externen Hive-Metastore mit dem Datenkatalog zu verbinden. Sie können auf die AWS SAM Anwendung in der zugreifen. AWS Serverless Application Repository

Die AWS SAM Anwendung stellt mithilfe einer Lambda-Funktion die Verbindung für den Hive-Metastore hinter Amazon API Gateway her. Die AWS SAM Anwendung verwendet einen Uniform Resource Identifier (URI) als Benutzereingabe und verbindet den externen Hive-Metastore mit dem Datenkatalog. Wenn ein Benutzer eine Abfrage für Hive-Tabellen ausführt, ruft der Datenkatalog den API-Gateway-Endpunkt auf. Der Endpunkt ruft die Lambda-Funktion auf, um die Metadaten der Hive-Tabellen abzurufen.

Um den Datenkatalog mit dem Hive-Metastore zu verbinden und Berechtigungen einzurichten

#### 1. Stellen Sie die Anwendung bereit. AWS SAM

1. Melden Sie sich bei der an AWS-Managementkonsole und öffnen Sie die AWS Serverless Application Repository.
2. Wählen Sie im Navigationsbereich Available applications (Verfügbare Anwendungen) aus.
3. Wählen Sie Öffentliche Anwendungen.
4. Wählen Sie die Option Apps anzeigen, die benutzerdefinierte IAM-Rollen oder Ressourcenrichtlinien erstellen.
5. Geben Sie im Suchfeld den Namen GlueDataCatalogFederation- einHiveMetastore.
6. Wählen Sie die HiveMetastore Anwendung GlueDataCatalogFederation-.
7. Geben Sie unter Anwendungseinstellungen die folgenden Mindesteinstellungen für Ihre Lambda-Funktion ein:
  - Anwendungsname — Ein Name für Ihre AWS SAM Anwendung.
  - GlueConnectionName- Ein Name für die Verbindung.

- HiveMetastoreURIs- Die URI Ihres Hive-Metastore-Hosts.
  - LambdaMemory- Die Menge des Lambda-Speichers in MB von 128-10240. Der Standardwert ist 1024.
  - LambdaTimeout- Die maximale Laufzeit des Lambda-Aufrufs in Sekunden. Der Standardwert ist 30.
  - VPCSecurityGroupIds und VPCSubnetIDs — Informationen für die VPC, in der der Hive-Metastore existiert.
8. Wählen Sie Ich bestätige, dass diese App benutzerdefinierte IAM-Rollen und Ressourcenrichtlinien erstellt. Um weitere Informationen zu erhalten, wählen Sie den Link Info .
  9. Wählen Sie unten rechts im Abschnitt Anwendungseinstellungen Bereitstellen. Wenn die Bereitstellung abgeschlossen ist, erscheint die Lambda-Funktion im Abschnitt Ressourcen in der Lambda-Konsole.

Die Anwendung wird auf Lambda bereitgestellt. Dem Namen wird serverlessrepo- vorangestellt, um anzuzeigen, dass die Anwendung von bereitgestellt wurde. AWS Serverless Application Repository Wenn Sie die Anwendung auswählen, gelangen Sie zur Seite Ressourcen, auf der alle Ressourcen der Anwendung aufgeführt sind, die bereitgestellt wurden. Zu den Ressourcen gehören die Lambda-Funktion, die die Kommunikation zwischen dem Datenkatalog und dem Hive-Metastore ermöglicht, die AWS Glue Verbindung und andere Ressourcen, die für den Datenbankverbund benötigt werden.

2. Erstellen Sie eine föderierte Datenbank im Datenkatalog.

Nachdem Sie eine Verbindung zum Hive-Metastore hergestellt haben, können Sie im Datenkatalog Verbunddatenbanken erstellen, die auf die externen Hive-Metastore-Datenbanken verweisen. Sie müssen für jede Hive-Metastore-Datenbank, die Sie mit dem Datenkatalog verbinden, eine entsprechende Datenbank im Datenkatalog erstellen.

#### Lake Formation console

1. Wählen Sie auf der Seite Datenfreigabe die Registerkarte Gemeinsam genutzte Datenbanken und dann Datenbank erstellen aus.
2. Wählen Sie unter Verbindungsname den Namen Ihrer Hive-Metastore-Verbindung aus dem Dropdownmenü aus.

3. Geben Sie einen eindeutigen Datenbanknamen und die Federation Source Identifier für die Datenbank ein. Dies ist der Name, den Sie in Ihren SQL-Anweisungen verwenden, wenn Sie Tabellen abfragen. Der Name darf aus maximal 255 Zeichen bestehen und muss innerhalb Ihres Kontos eindeutig sein.
4. Wählen Sie Datenbank erstellen aus.

## AWS CLI

```
aws glue create-database \
'{
 "CatalogId": "<111122223333>",
 "database-input": {
 "Name": "<fed_glue_db>",
 "FederatedDatabase": {
 "Identifier": "<hive_db_on_emr>",
 "ConnectionName": "<hms_connection>"
 }
 }
}'
```

3. Tabellen in der Verbunddatenbank anzeigen.

Nachdem Sie die Verbunddatenbank erstellt haben, können Sie die Liste der Tabellen in Ihrem Hive-Metastore mithilfe der Lake Formation Formation-Konsole oder der anzeigen. AWS CLI

## Lake Formation console

1. Wählen Sie den Datenbanknamen auf der Registerkarte Gemeinsam genutzte Datenbanken aus.
2. Wählen Sie auf der Seite Datenbanken die Option Tabellen anzeigen aus.

## AWS CLI

Die folgenden Beispiele zeigen, wie Sie die Verbindungsdefinition, den Datenbanknamen und einige oder alle Tabellen in der Datenbank abrufen. Ersetzen Sie die ID des Datenkatalogs durch die gültige AWS-Konto ID, mit der Sie die Datenbank erstellt haben. `hms_connection` Ersetzen Sie durch den Verbindungsnamen.

```
aws glue get-connection \
--name <hms_connection> \
--catalog-id 111122223333
```

```
aws glue get-database \
--name <fed_glu_db> \
--catalog-id 111122223333
```

```
aws glue get-tables \
--database-name <fed_glue_db> \
--catalog-id 111122223333
```

```
aws glue get-table \
--database-name <fed_glue_db> \
--name <hive_table_name> \
--catalog-id 111122223333
```

#### 4. Erteilen Sie Berechtigungen.

Nachdem Sie die Datenbank erstellt haben, können Sie anderen IAM-Benutzern und -Rollen in Ihrem Konto oder externen AWS-Konten Organisationen Berechtigungen gewähren. Sie können für die Verbunddatenbanken keine Schreib- (Einfügen, Löschen) und Metadatenberechtigungen (Ändern, Löschen, Erstellen) gewähren. Weitere Informationen zum Erteilen von Berechtigungen finden Sie unter [Verwaltung von Lake Formation Formation-Berechtigungen](#).

#### 5. Fragen Sie die Verbunddatenbanken ab.

Nachdem Sie die Berechtigungen erteilt haben, können sich Benutzer anmelden und mit der Abfrage der Verbunddatenbank mithilfe von Athena und Amazon Redshift beginnen. Benutzer können jetzt den lokalen Datenbanknamen verwenden, um in SQL-Abfragen auf die Hive-Datenbank zu verweisen.

Beispiel einer Amazon Athena Abfragesyntax

fed\_glue\_db Ersetzen Sie es durch den Namen der lokalen Datenbank, den Sie zuvor erstellt haben.

```
Select * from fed_glue_db.customers limit 10;
```



## Weitere Ressourcen

Der folgende Blogbeitrag enthält detaillierte Anweisungen zum Einrichten von Lake Formation Formation-Berechtigungen für eine Hive-Metastore-Datenbank und -Tabellen und deren Abfrage mit Athena. Wir veranschaulichen auch einen Anwendungsfall für kontenübergreifendes Teilen, bei dem ein Lake-Formation-Principal auf Produzentenkonto A eine föderierte Hive-Datenbank und -Tabellen mit LF-Tag für Verbraucherkonto B gemeinsam nutzt.

- [Fragen Sie Ihren Apache Hive-Metastore mit Berechtigungen ab AWS Lake Formation](#)

# Verwaltung von Lake Formation Formation-Berechtigungen

Lake Formation bietet zentrale Zugriffskontrollen für Daten in Ihrem Data Lake. Sie können auf Sicherheitsrichtlinien basierende Regeln für Ihre Benutzer und Anwendungen nach Rollen in Lake Formation definieren, und die Integration mit AWS Identity and Access Management authentifiziert diese Benutzer und Rollen. Sobald die Regeln definiert sind, setzt Lake Formation Ihre Zugriffskontrollen auf Tabellen-, Spalten- und RO-Ebene für Benutzer von Amazon Redshift Spectrum und Amazon Athena durch.

## Topics

- [Erteilung von Berechtigungen zum Speicherort von Daten](#)
- [Erteilen von Berechtigungen für Datenkatalogressourcen](#)
- [Beispielszenario für Berechtigungen](#)
- [Datenfilterung und Sicherheit auf Zellebene in Lake Formation](#)
- [Datenbank- und Tabellenberechtigungen in Lake Formation anzeigen](#)
- [Widerrufen der Genehmigung mithilfe der Lake Formation Formation-Konsole](#)
- [Kontoübergreifender Datenaustausch in Lake Formation](#)
- [Zugreifen auf und Anzeigen von gemeinsam genutzten Datenkatalogtabellen und Datenbanken](#)
- [Ressourcenlinks erstellen](#)
- [Regionsübergreifender Zugriff auf Tabellen](#)

## Erteilung von Berechtigungen zum Speicherort von Daten

Mit Datenstandortberechtigungen AWS Lake Formation in können Prinzipale Datenkatalogressourcen erstellen und ändern, die auf bestimmte registrierte Amazon S3 S3-Standorte verweisen.

Datenstandortberechtigungen funktionieren zusätzlich zu den Datenberechtigungen von Lake Formation, um Informationen in Ihrem Data Lake zu sichern.

Lake Formation verwendet den Dienst AWS Resource Access Manager (AWS RAM) nicht für die Erteilung von Datenstandortberechtigungen, sodass Sie für Datenstandortberechtigungen keine Einladungen zur gemeinsamen Nutzung von Ressourcen annehmen müssen.

Sie können Datenstandortberechtigungen mithilfe der Lake Formation Formation-Konsole, der API oder AWS Command Line Interface (AWS CLI) erteilen.

 Note

Damit ein Grant erfolgreich ist, müssen Sie zuerst den Datenstandort bei Lake Formation registrieren.

 Weitere Informationen finden Sie unter:

- [Underlying data access control](#)

## Themen

- [Erteilen von Datenspeicherberechtigungen \(dasselbe Konto\)](#)
- [Erteilen von Datenstandortberechtigungen \(externes Konto\)](#)
- [Erteilen von Berechtigungen für einen Datenstandort, der mit Ihrem Konto geteilt wird](#)

## Erteilen von Datenspeicherberechtigungen (dasselbe Konto)

Gehen Sie wie folgt vor, um Prinzipalen in Ihrem AWS Konto Datenstandortberechtigungen zu erteilen. Sie können Berechtigungen mithilfe der Lake Formation Formation-Konsole, der API oder der AWS Command Line Interface (AWS CLI) gewähren.

## AWS-Managementkonsole

So gewähren Sie Berechtigungen zum Speicherort von Daten (dasselbe Konto)

1. Öffnen Sie die AWS Lake Formation Konsole unter <https://console.aws.amazon.com/lakeformation/>. Melden Sie sich als Data Lake-Administrator oder als Principal an, dem Berechtigungen für den gewünschten Datenspeicherort erteilt wurden.
2. Wählen Sie im Navigationsbereich unter Berechtigungen die Option Datenspeicherorte aus.
3. Wählen Sie Grant (Erteilen).
4. Stellen Sie sicher, dass im Dialogfeld Berechtigungen gewähren die Kachel Mein Konto ausgewählt ist. Geben Sie dann die folgenden Informationen ein:
  - Wählen Sie für IAM-Benutzer und -Rollen einen oder mehrere Prinzipale aus.

- Geben Sie für SAML- und Amazon Quick-Benutzer und -Gruppen einen oder mehrere Amazon-Ressourcennamen (ARNs) für Benutzer oder Gruppen ein, die über SAML verbunden sind, oder ARNs für Amazon Quick-Benutzer oder -Gruppen.

Geben Sie jeweils einen ARN ein und drücken Sie nach jedem ARN die Eingabetaste. Informationen zur Erstellung von finden Sie ARNs unter [Lake Formation erteilt und widerruft AWS CLI Befehle](#).

- Wählen Sie für Speicherorte die Option Durchsuchen und wählen Sie einen Amazon Simple Storage Service (Amazon S3) -Speicherort aus. Der Standort muss bei Lake Formation registriert sein. Wählen Sie erneut Durchsuchen, um einen weiteren Standort hinzuzufügen. Sie können den Standort auch eingeben, stellen Sie jedoch sicher, dass Sie dem Standort Folgendes `s3://` voranstellen.
- Geben Sie unter Registrierter Kontostandort die AWS Konto-ID ein, bei der der Standort registriert ist. Dies ist standardmäßig Ihre Konto-ID. In einem kontoübergreifenden Szenario können Data Lake-Administratoren in einem Empfängerkonto hier das Besitzerkonto angeben, wenn sie anderen Prinzipalen im Empfängerkonto die Datenspeicherberechtigung erteilen.
- (Optional) Wählen Sie Grantable aus, damit die ausgewählten Principals Datenstandortberechtigungen für den ausgewählten Standort erteilen können.

**Grant permissions** ✕

Add access permissions for specific storage locations.

☒ **My account**  
User or role from this AWS account.

☐ **External account**  
AWS account or AWS organization outside of my account.

**IAM users and roles**  
Add one or more IAM users or roles.

Choose IAM principals to add

**datalake\_user** ✕  
User

**SAML and Amazon QuickSight users and groups**  
Enter a SAML user or group ARN or Amazon QuickSight ARN. Press Enter to add additional ARNs.

Ex: `arn:aws:iam::<AccountId>:saml-provider/<SamlProviderName>`

**Storage locations**  
Choose one or more data lake locations.

**Registered account location**  
The account where this storage location is registered in AWS Lake Formation.

☐ Grantable

## 5. Wählen Sie Grant (Erteilen).

## AWS CLI

Um Berechtigungen für den Datenspeicherort zu gewähren (dasselbe Konto)

- Führen Sie einen `grant-permissions` Befehl aus und gewähren Sie `DATA_LOCATION_ACCESS` dem Principal, wobei Sie den Amazon S3 S3-Pfad als Ressource angeben.

### Example

Im folgenden Beispiel werden dem Benutzer Berechtigungen `s3://retail` zum Speicherort von Daten erteilt `datalake_user1`.

```
aws lakeformation grant-permissions --principal
DataLakePrincipalIdentifier=arn:aws:iam::<account-id>:user/datalake_user1
```

```
--permissions "DATA_LOCATION_ACCESS" --resource '{ "DataLocation":
{"ResourceArn":"arn:aws:s3:::retail"}}'
```

### Example

Im folgenden Beispiel werden einer ALLIAMPrincipals Gruppe s3://retail Datenspeicherberechtigungen erteilt.

```
aws lakeformation grant-permissions --principal
DataLakePrincipalIdentifier=111122223333:IAMPrincipals --
permissions "DATA_LOCATION_ACCESS" --resource '{ "DataLocation":
{"ResourceArn":"arn:aws:s3:::retail", "CatalogId": "111122223333"}}'
```

 Weitere Informationen finden Sie unter:

- [Referenz zu den Genehmigungen von Lake Formation](#)

## Erteilen von Datenstandortberechtigungen (externes Konto)

Gehen Sie wie folgt vor, um einem externen AWS Konto oder einer externen Organisation Datenspeicherberechtigungen zu erteilen.

Sie können Berechtigungen mithilfe der Lake Formation Formation-Konsole, der API oder der AWS Command Line Interface (AWS CLI) gewähren.

Bevor Sie beginnen

Stellen Sie sicher, dass alle Voraussetzungen für den kontoübergreifenden Zugriff erfüllt sind.

Weitere Informationen finden Sie unter [Voraussetzungen](#).

### AWS-Managementkonsole

Um Berechtigungen zum Speicherort von Daten zu gewähren (externes Konto, Konsole)

1. Öffnen Sie die AWS Lake Formation Konsole unter <https://console.aws.amazon.com/lakeformation/>. Melden Sie sich als Data Lake-Administrator an.
2. Wählen Sie im Navigationsbereich unter Berechtigungen die Option Datenspeicherorte und dann Grant aus.

3. Wählen Sie im Dialogfeld „Berechtigungen gewähren“ die Kachel Externes Konto aus.
4. Geben Sie die folgenden Informationen ein:
  - Geben Sie als AWS Konto-ID oder AWS Organisations-ID gültige AWS Kontonummern IDs, Organisation oder Organisationseinheit ein IDs.

Drücken Sie nach jeder ID die Eingabetaste.

Eine Organisations-ID besteht aus „o-“, gefolgt von 10 bis 32 Kleinbuchstaben oder Ziffern.

Eine Organisationseinheit-ID besteht aus „ou-“, gefolgt von 4 bis 32 Kleinbuchstaben oder Ziffern (der ID des Stammes, der die Organisationseinheit enthält). Auf diese Zeichenfolge folgen ein zweites „-“ (Bindestrich) und 8 bis 32 zusätzliche Kleinbuchstaben oder Ziffern.

- Wählen Sie unter Speicherorte die Option Durchsuchen und wählen Sie einen Amazon Simple Storage Service (Amazon S3) -Speicherort aus. Der Standort muss bei Lake Formation registriert sein.

**Grant permissions** ×

Add access permissions for specific storage locations.

☐ My account  
User or role from this AWS account.

☒ External account  
AWS account or AWS organization outside of my account.

AWS account ID or AWS organization ID

111122223333 ×  
Account

Enter one or more AWS account IDs or AWS organization IDs. Press Enter after each ID.

Storage locations  
Choose one or more data lake locations.

☒ Grantable

5. Wählen Sie Grantable aus.
6. Wählen Sie Grant (Erteilen).

## AWS CLI

Um Berechtigungen zum Speicherort von Daten zu gewähren (externes Konto, AWS CLI)

- Um einem externen AWS Konto Berechtigungen zu erteilen, geben Sie einen Befehl ein, der dem folgenden ähnelt.

```
aws lakeformation grant-permissions --principal
DataLakePrincipalIdentifier=111122223333 --permissions
"DATA_LOCATION_ACCESS" --permissions-with-grant-option
"DATA_LOCATION_ACCESS" --resource '{ "DataLocation":
{"CatalogId":"123456789012","ResourceArn":"arn:aws:s3::retail/
transactions/2020q1"}}'
```

Dieser Befehl gewährt DATA\_LOCATION\_ACCESS mit der Grant-Option das Konto 1111-2222-3333 am Amazon S3 S3-Standorts3://retail/transactions/2020q1, das dem Konto 1234-5678-9012 gehört.

Um einer Organisation Berechtigungen zu erteilen, geben Sie einen Befehl ein, der dem folgenden ähnelt.

```
aws lakeformation grant-permissions --principal
DataLakePrincipalIdentifier=arn:aws:organizations::111122223333:organization/
o-abcdefghijkl --permissions "DATA_LOCATION_ACCESS" --permissions-
with-grant-option "DATA_LOCATION_ACCESS" --resource '{"DataLocation":
{"CatalogId":"123456789012","ResourceArn":"arn:aws:s3::retail/
transactions/2020q1"}}'
```

Dieser Befehl gewährt DATA\_LOCATION\_ACCESS der Organisation o-abcdefghijkl am Amazon S3 S3-Standorts3://retail/transactions/2020q1, der dem Konto 1234-5678-9012 gehört, die Option Grant.

Um einem Principal Berechtigungen in einem externen AWS Konto zu erteilen, geben Sie einen Befehl ein, der dem folgenden ähnelt.

```
aws lakeformation grant-permissions --principal
DataLakePrincipalIdentifier=arn:aws:iam::111122223333:user/datalake_user1
--permissions "DATA_LOCATION_ACCESS" --resource '{ "DataLocation":
{"ResourceArn":"arn:aws:s3::retail/transactions/2020q1", "CatalogId":
"123456789012"}}'
```



Dieser Befehl gewährt DATA\_LOCATION\_ACCESS einem Principal das Konto 1111-2222-3333 am Amazon S3 S3-Standort `s3://retail/transactions/2020q1`, das dem Konto 1234-5678-9012 gehört.

### Example

Im folgenden Beispiel werden Datenstandortberechtigungen für Gruppen in einem externen Konto erteilt. `s3://retail ALLIAMPrincipals`

```
aws lakeformation grant-permissions --principal
DataLakePrincipalIdentifier=111122223333:IAMPrincipals --
permissions "DATA_LOCATION_ACCESS" --resource '{ "DataLocation":
{"ResourceArn":"arn:aws:s3:::retail", "CatalogId": "123456789012"} }'
```

 Weitere Informationen finden Sie unter:

- [Referenz zu den Genehmigungen von Lake Formation](#)

## Erteilen von Berechtigungen für einen Datenstandort, der mit Ihrem Konto geteilt wird

Nachdem eine Datenkatalogressource für Ihr AWS Konto freigegeben wurde, können Sie als Data Lake-Administrator anderen Prinzipalen in Ihrem Konto Berechtigungen für die Ressource gewähren. Wenn die ALTER Berechtigung für eine gemeinsam genutzte Tabelle erteilt wurde und die Tabelle auf einen registrierten Amazon S3 S3-Standort verweist, müssen Sie auch Datenstandortberechtigungen für den Standort erteilen. Wenn die ALTER Berechtigung CREATE\_TABLE oder für eine gemeinsam genutzte Datenbank erteilt wird und die Datenbank über eine Standorteigenschaft verfügt, die auf einen registrierten Standort verweist, müssen Sie ebenfalls Datenstandortberechtigungen für den Standort erteilen.

Um einem Hauptbenutzer in Ihrem Konto Datenstandortberechtigungen für einen gemeinsam genutzten Standort zu erteilen, muss Ihrem Konto die DATA\_LOCATION\_ACCESS Berechtigung für den Standort mit der Option „Gewähren“ erteilt worden sein. Wenn Sie dann einem anderen Auftraggeber in Ihrem Konto eine Genehmigung erteilen DATA\_LOCATION\_ACCESS, müssen Sie die

Datenkatalog-ID (AWS Konto-ID) des Eigentümerkontos angeben. Das Besitzerkonto ist das Konto, mit dem der Standort registriert wurde.

Sie können die AWS Lake Formation Konsole, die API oder die AWS Command Line Interface () verwenden, AWS CLI um Datenstandortberechtigungen zu erteilen.

Um Berechtigungen für einen Datenspeicherort zu gewähren, der mit Ihrem Konto geteilt wird (Konsole)

- Führen Sie die Schritte unter [Erteilen von Datenspeicherberechtigungen \(dasselbe Konto\)](#) aus.

Für Speicherorte müssen Sie die Speicherorte eingeben. Geben Sie unter Standort des registrierten AWS Kontos die Konto-ID des Eigentümerkontos ein.

Um Berechtigungen für einen Datenspeicherort zu gewähren, der mit Ihrem Konto geteilt wird (AWS CLI)

- Geben Sie einen der folgenden Befehle ein, um entweder einem Benutzer oder einer Rolle Berechtigungen zu erteilen.

```
aws lakeformation grant-permissions --principal
DataLakePrincipalIdentifier=arn:aws:iam:<account-id>:user/<user-name>
--permissions "DATA_LOCATION_ACCESS" --resource '{ "DataLocation":
{"CatalogId":"<owner-account-ID>","ResourceArn":"arn:aws:s3:::<s3-location>"} }'
aws lakeformation grant-permissions --principal
DataLakePrincipalIdentifier=arn:aws:iam:<account-id>:role/<role-name>
--permissions "DATA_LOCATION_ACCESS" --resource '{ "DataLocation":
{"CatalogId":"<owner-account-ID>","ResourceArn":"arn:aws:s3:::<s3-location>"} }'
```

## Erteilen von Berechtigungen für Datenkatalogressourcen

Sie können Prinzipalen Datenberechtigungen gewähren, AWS Lake Formation sodass die Prinzipale Datenkatalogressourcen erstellen und verwalten und auf die zugrunde liegenden Daten zugreifen können. Sie können Data Lake-Berechtigungen für Kataloge, Datenbanken, Tabellen und Ansichten gewähren. Wenn Sie Berechtigungen für Tabellen gewähren, können Sie den Zugriff auf bestimmte Tabellenspalten oder -zeilen einschränken, um eine noch detailliertere Zugriffskontrolle zu erreichen.

Sie können Berechtigungen für einzelne Kataloge, Datenbanken, Tabellen und Ansichten oder mit einem einzigen Erteilungsvorgang Berechtigungen für alle Datenbanken, Tabellen und Ansichten in

einem Katalog oder einer Datenbank gewähren. Wenn Sie IAM-Prinzipalen Berechtigungen für alle Tabellen in einer Datenbank gewähren, erteilen Sie damit implizit die DESCRIBE Berechtigung für die Datenbank. Die Datenbank wird dann auf der Datenbankseite der Konsole angezeigt und durch den GetDatabases API-Vorgang zurückgegeben. Das gleiche Prinzip gilt auf Katalogebene: Wenn Sie Berechtigungen für Datenbanken innerhalb eines Katalogs erhalten, erhalten Sie auch DESCRIBE Berechtigungen für diesen Katalog.

 **Important**

Die implizite DESCRIBE Berechtigung gilt nur, wenn Sie IAM-Prinzipalen innerhalb desselben Kontos Berechtigungen gewähren. AWS Für kontoübergreifende Ressourcen müssen Sie explizit Berechtigungen erteilen. DESCRIBE Die automatische DESCRIBE Berechtigungsgewährung gilt nicht, wenn die attributebasierte Zugriffskontrolle (ABAC) verwendet wird. Wenn mithilfe von Attributen Berechtigungen für alle Tabellen in einer Datenbank erteilt werden, erteilt Lake Formation der Datenbank nicht implizit DESCRIBE Berechtigungen.

Sie können Berechtigungen entweder mithilfe der benannten Ressourcenmethode oder der Tag-Based Access Control (LF-TBAC) -Methode (Lake Formation, Tag-Based Access Control) gewähren.

Sie können Prinzipalen derselben Person oder externen Konten AWS-Konto oder Organisationen Berechtigungen gewähren. Wenn Sie externen Konten oder Organisationen gewähren, geben Sie Datenkatalogobjekte, deren Eigentümer Sie sind, für diese Konten oder Organisationen frei. Prinzipale in diesen Konten oder Organisationen können dann auf Datenkatalogobjekte, deren Eigentümer Sie sind, und auf die zugrunde liegenden Daten zugreifen.

 **Note**

Derzeit unterstützt die LF-TBAC-Methode die Gewährung kontenübergreifender Berechtigungen für IAM-Prinzipale AWS-Konten, Organisationen und Organisationseinheiten (). OUs

Wenn Sie externen Konten oder Organisationen Berechtigungen gewähren, müssen Sie die Option „Gewähren“ angeben. Nur der Data Lake-Administrator im externen Konto kann auf die gemeinsam genutzten Objekte zugreifen, bis der Administrator anderen Prinzipalen im externen Konto Berechtigungen für die gemeinsam genutzten Objekte erteilt.

Sie können Datenkatalogberechtigungen mithilfe der AWS Lake Formation Konsole, der API oder der AWS Command Line Interface (AWS CLI) gewähren.

 Note

Wenn Sie ein Datenkatalogobjekt löschen, werden alle mit dem Objekt verknüpften Berechtigungen ungültig. Durch das Neuerstellen derselben Ressource mit demselben Namen werden die Lake Formation Formation-Berechtigungen nicht wiederhergestellt. Benutzer müssen erneut neue Berechtigungen einrichten.

 Weitere Informationen finden Sie auch unter:

- [Gemeinsame Nutzung von Datenkatalogtabellen und Datenbanken für mehrere AWS Konten](#)
- [Zugriffskontrolle für Metadaten](#)
- [Referenz zu den Genehmigungen von Lake Formation](#)

## IAM-Berechtigungen sind erforderlich, um Lake Formation Formation-Berechtigungen zu gewähren oder zu widerrufen

Alle Principals, einschließlich des Data Lake-Administrators, benötigen die folgenden AWS Identity and Access Management (IAM-) Berechtigungen, um AWS Lake Formation Datenkatalogberechtigungen oder Datenstandortberechtigungen mit der Lake Formation API oder dem zu erteilen oder zu widerrufen: AWS CLI

- `lakeformation:GrantPermissions`
- `lakeformation:BatchGrantPermissions`
- `lakeformation:RevokePermissions`
- `lakeformation:BatchRevokePermissions`
- `glue:GetTableglue:GetDatabase`, oder `glue:GetCatalog` für eine Tabelle, Datenbank oder einen Katalog, dem Sie mithilfe der benannten Ressourcenmethode Berechtigungen gewähren.

 Note

Data Lake-Administratoren verfügen über implizite Lake Formation Formation-Berechtigungen, um Lake Formation Formation-Berechtigungen zu gewähren und zu widerrufen. Sie benötigen jedoch weiterhin die IAM-Berechtigungen für die Lake Formation Grant- und Revoke-API-Operationen.

IAM-Rollen mit `AWSLakeFormationDataAdmin` AWS verwalteten Richtlinien können keine neuen Data Lake-Administratoren hinzufügen, da diese Richtlinie eine ausdrückliche Ablehnung des Lake Formation Formation-API-Vorgangs enthält, `PutDataLakeSetting`.

Die folgende IAM-Richtlinie wird für Principals empfohlen, die keine Data Lake-Administratoren sind und über die Lake Formation Formation-Konsole Berechtigungen gewähren oder entziehen möchten.

JSON

```
{
 "Version": "2012-10-17",
 "Statement": [
 {
 "Effect": "Allow",
 "Action": [
 "lakeformation:ListPermissions",
 "lakeformation:GrantPermissions",
 "lakeformation:BatchGrantPermissions",
 "lakeformation:RevokePermissions",
 "lakeformation:BatchRevokePermissions",
 "glue:GetCatalogs",
 "glue:GetDatabases",
 "glue:SearchTables",
 "glue:GetTables",
 "glue:GetCatalog",
 "glue:GetDatabase",
 "glue:GetTable",
 "iam:ListUsers",
 "iam:ListRoles",
 "sso-directory:DescribeUser",
 "sso-directory:DescribeGroup",
 "sso:DescribeInstance"
],
 "Resource": "*"
 }
]
}
```

```

 }
]
}
```

Alle in dieser Richtlinie `iam:` enthaltenen Berechtigungen sind in der AWS verwalteten Richtlinie verfügbar. `glue: AWSGlueConsoleFullAccess`

Um Berechtigungen mithilfe der Tag-Based Access Control (LF-TBAC) von Lake Formation zu gewähren, benötigen Principals zusätzliche IAM-Berechtigungen. Weitere Informationen erhalten Sie unter [Bewährte Methoden und Überlegungen zur Tag-basierten Zugriffskontrolle von Lake Formation](#) und [Referenz zu Personas und IAM-Berechtigungen in Lake Formation](#).

### Kontoübergreifende -Berechtigungen

Benutzer, die mithilfe der benannten Ressourcenmethode kontoübergreifende Lake Formation Formation-Berechtigungen gewähren möchten, müssen auch über die Berechtigungen in der `AWSLakeFormationCrossAccountManager` AWS verwalteten Richtlinie verfügen.

Data Lake-Administratoren benötigen dieselben Berechtigungen für die Gewährung kontoübergreifender Berechtigungen sowie die Berechtigung `AWS Resource Access Manager (AWS RAM)`, um Organisationen Berechtigungen gewähren zu können. Weitere Informationen finden Sie unter [Berechtigungen des Data Lake-Administrators](#).

### Der Benutzer mit Administratorrechten

Ein Principal mit Administratorberechtigungen — z. B. mit der `AdministratorAccess` AWS verwalteten Richtlinie — hat die Berechtigung, Lake Formation Formation-Berechtigungen zu erteilen und Data Lake-Administratoren zu erstellen. Um einem Benutzer oder einer Rolle den Zugriff auf Lake Formation-Administratoroperationen zu verweigern, fügen Sie seiner Richtlinie eine Deny Erklärung für Administrator-API-Operationen hinzu oder fügen Sie sie hinzu.

### JSON

```

{
 "Version": "2012-10-17",
 "Statement": [
 {
 "Action": [
 "lakeformation:GetDataLakeSettings",
 "lakeformation:PutDataLakeSettings"
]
 }
]
}
```

```
],
 "Effect": "Deny",
 "Resource": [
 "*"
]
 }
]
}
```

#### Important

Um zu verhindern, dass Benutzer sich mit einem ETL-Skript (Extrahieren, Transformieren und Laden) als Administrator hinzufügen, stellen Sie sicher, dass allen Benutzern und Rollen, die keine Administratoren sind, der Zugriff auf diese API-Operationen verweigert wird. Die AWSLakeFormationDataAdmin AWS verwaltete Richtlinie enthält eine ausdrückliche Ablehnung des Lake Formation Formation-API-Vorgangs, PutDataLakeSetting sodass Benutzer keine neuen Data Lake-Administratoren hinzufügen können.

## Erteilen von Datenberechtigungen mithilfe der benannten Ressourcenmethode

Die Ressourcenmethode Named Data Catalog ist eine Möglichkeit, AWS Glue Data Catalog Objekten wie Katalogen, Datenbanken, Tabellen, Spalten und Ansichten mithilfe eines zentralisierten Ansatzes Berechtigungen zu erteilen. Sie ermöglicht es Ihnen, ressourcenbasierte Richtlinien zu definieren, die den Zugriff auf bestimmte Ressourcen in Ihrem Data Lake steuern.

Wenn Sie die benannte Ressourcenmethode verwenden, um Berechtigungen zu erteilen, können Sie den Ressourcentyp und die Berechtigungen angeben, die Sie für diese Ressource gewähren oder entziehen möchten. Sie können die Berechtigung bei Bedarf auch später widerrufen und so die Berechtigungen von den zugehörigen Ressourcen entfernen.

Sie können Berechtigungen mithilfe der AWS Lake Formation Konsole APIs, oder der AWS Command Line Interface (AWS CLI) erteilen.

### Themen

- [Erteilen von Katalogberechtigungen mithilfe der benannten Ressourcenmethode](#)
- [Erteilen von Datenbankberechtigungen mit der benannten Ressourcenmethode](#)

- [Erteilen von Tabellenberechtigungen mithilfe der benannten Ressourcenmethode](#)
- [Erteilen von Berechtigungen für Ansichten mithilfe der benannten Ressourcenmethode](#)

## Erteilen von Katalogberechtigungen mithilfe der benannten Ressourcenmethode

In den folgenden Schritten wird erklärt, wie Katalogberechtigungen mithilfe der benannten Ressourcenmethode erteilt werden.

### Console

Verwenden Sie die Seite „Berechtigungen gewähren“ in der Lake Formation Konsole. Die Seite ist in die folgenden Abschnitte unterteilt:

- **Prinzipaltyp** — Sie können bestimmten Prinzipalen Berechtigungen gewähren oder Attribut-Tags verwenden.
  - **Principals** — Die IAM-Benutzer, Rollen, IAM Identity Center-Benutzer und -Gruppen, SAML-Benutzer und -Gruppen, AWS Konten, Organisationen oder Organisationseinheiten, denen Berechtigungen erteilt werden sollen.

**Prinzipal nach Attributen** — Fügen Sie Tag-Schlüssel-Wert-Paare aus oder IAM-Sitzungstags hinzu. IAMroles Principals mit übereinstimmenden Attributen erhalten Zugriff auf die angegebene Ressource.

- **LF-Tags oder Katalogressourcen** — Die Kataloge, Datenbanken, Tabellen, Ansichten oder Ressourcenlinks, für die Berechtigungen erteilt werden sollen.
- **Genehmigungen** — Die Lake Formation erteilt Genehmigungen.

#### Note

Informationen zum Erteilen von Berechtigungen für einen Datenbankressourcen-Link finden Sie unter [Erteilen von Ressourcenverknüpfungsberechtigungen](#).

1. Öffnen Sie die Seite „Berechtigungen gewähren“.

Öffnen Sie die AWS Lake Formation Konsole unter <https://console.aws.amazon.com/lakeformation/> und melden Sie sich als Data Lake-Administrator, Ersteller des Katalogs oder als IAM-Benutzer an, der über Grantable-Berechtigungen für den Katalog verfügt.



Führen Sie eine der folgenden Aktionen aus:

- Wählen Sie im Navigationsbereich unter Berechtigungen die Option Datenberechtigungen aus. Wählen Sie dann Grant (Erteilen) aus.
- Wählen Sie im Navigationsbereich unter Datenkatalog die Option Kataloge aus. Wählen Sie dann auf der Seite Kataloge einen Katalog aus und wählen Sie im Menü Aktionen unter Berechtigungen die Option Gewähren aus.

 Note

Sie können über den zugehörigen Ressourcenlink Berechtigungen für einen Katalog gewähren. Wählen Sie dazu auf der Seite Kataloge einen Katalog-Link-Container und wählen Sie im Menü Aktionen die Option Auf Ziel gewähren aus. Weitere Informationen finden Sie unter [Funktionsweise von Ressourcenverbindungen in Lake Formation](#).

2. Wählen Sie anschließend im Abschnitt Principal Type die Option Principals aus, oder geben Sie die Attribute an, die den Principals zugewiesen sind.

## Grant permissions

### Principal type

Grant access by IAM principal or attribute tags.



#### Principals

Grant permissions directly to specific IAM users, roles, or Identity Center principals.



#### Principals by attributes

Grant permissions using attribute tags with Cedar policy expressions.

### Principals

Choose the principals to grant permissions.



#### IAM users and roles

Users or roles from this AWS account.



#### IAM Identity Center - *new*

Users and groups configured in IAM Identity Center.



#### SAML users and groups

SAML users and group or QuickSight ARNs.



#### External accounts

AWS account, AWS organization or IAM principal outside of this account

#### IAM users and roles

Add one or more IAM users or roles.

Choose IAM principals to add



lf-data-analyst X  
User

Geben Sie Principals an

IAM-Benutzer und -Rollen

Wählen Sie einen oder mehrere Benutzer oder Rollen aus der Liste der IAM-Benutzer und -Rollen aus.

IAM Identity Center

Wählen Sie einen oder mehrere Benutzer oder Gruppen aus der Liste Benutzer und Gruppen aus. Wählen Sie Hinzufügen aus, um weitere Benutzer oder Gruppen hinzuzufügen.

SAML-Benutzer und -Gruppen

Geben Sie für SAML- und Quick-Benutzer und -Gruppen einen oder mehrere Amazon-Ressourcennamen (ARNs) für Benutzer oder Gruppen ein, die über SAML verbunden

sind, oder ARNs für Amazon Quick-Benutzer oder -Gruppen. Drücken Sie nach jedem ARN die Eingabetaste.

Informationen zur Erstellung von finden Sie unter ARNs. [Lake Formation erteilt und widerruft AWS CLI Befehle](#)

 Note

Die Integration von Lake Formation mit Quick wird nur für die Quick Enterprise Edition unterstützt.

## Externe Konten

Geben Sie für AWS-Konto, AWS Organisation oder IAM-Principal ein oder mehrere gültige AWS Konten IDs, Organisationen IDs, Organisationseinheiten IDs oder ARN für den IAM-Benutzer oder die IAM-Rolle ein. Drücken Sie nach jeder ID die Eingabetaste.

Eine Organisations-ID besteht aus „o-“, gefolgt von 10—32 Kleinbuchstaben oder Ziffern.

Eine Organisationseinheits-ID beginnt mit „ou-“, gefolgt von 4—32 Kleinbuchstaben oder Ziffern (der ID des Stammes, der die Organisationseinheit enthält). Auf diese Zeichenfolge folgen ein zweiter Gedankenstrich „-“ und 8 bis 32 zusätzliche Kleinbuchstaben oder Ziffern.

## Prinzipale nach Attributen

### Attribute

Fügen Sie die Schlüssel-Wert-Paare des IAM-Tags aus der IAM-Rolle hinzu.

### Umfang der Berechtigungen

Geben Sie an, ob Sie Prinzipalen mit übereinstimmenden Attributen in demselben Konto oder in einem anderen Konto Berechtigungen gewähren.

3. Wählen Sie im Abschnitt LF-Tags oder Katalogressourcen die Option Benannte Datenkatalogressourcen aus.

## LF-Tags or catalog resources

Choose a method to grant permissions.

☐ Resources matched by LF-Tags (recommended)  
Manage permissions indirectly for resources or data matched by a specific set of LF-Tags.

☒ Named Data Catalog resources  
Manage permissions for specific databases or tables, in addition to fine-grained data access.

### Catalogs

Choose catalogs

mycatalogdemo X

### Databases

Select one or more databases.

Choose databases

tpcds1 X  
mycatalogdemo

### Tables - optional

Select one or more tables.

Choose tables

All tables X  
mycatalogdemo

### Views - optional

Select one or more views.

Choose views

### Data filters - optional

Select one or more data filters.

Choose data filters

Load  
more

Create new

[Manage data filters](#)

4. Wählen Sie einen oder mehrere Kataloge aus der Liste Kataloge aus. Sie können auch eine oder mehrere Datenbanken, Tabellen und and/or Datenfilter auswählen.
5. Wählen Sie im Abschnitt Katalogberechtigungen die Optionen Berechtigungen und erteilbare Berechtigungen aus. Wählen Sie unter Katalogberechtigungen mindestens eine Berechtigung aus, die Sie gewähren möchten.

## Catalog permissions

Choose the permissions to grant on the catalog. Choosing Super user overwrites individual permissions, granting unrestricted administrative access.

☐ Super user

A super user has unrestricted administrative privileges to perform any operation on all resources within the catalog (databases, tables, and views).

### Catalog permissions

Choose specific access permissions to grant.

☐ Create database    ☐ Describe    ☐ Alter

☐ Drop

☐ Super

This permission is the union of all the individual permissions to the left, and supersedes them.

### Grantable permissions

Choose the permission that can be granted to others.

☐ Create database    ☐ Describe    ☐ Alter

☐ Drop

☐ Super

This permission allows the principal to grant any of the permissions to the left, and supersedes those grantable permissions.

Cancel

Grant

Wählen Sie Superuser, um uneingeschränkte Administratorrechte zu gewähren, sodass Sie beliebige Operationen mit allen Ressourcen innerhalb des Katalogs (Datenbanken, Tabellen und Ansichten) ausführen können.

### Note

Stellen Sie nach der Erteilung von `Create database` oder für einen Katalog mit einer Standorteigenschaft, die `Alter` auf einen registrierten Standort verweist, sicher, dass Sie auch den Prinzipalen Datenspeicherberechtigungen für den Standort gewähren. Weitere Informationen finden Sie unter [Erteilung von Berechtigungen zum Speicherort von Daten](#).

- (Optional) Wählen Sie unter Erteilbare Berechtigungen die Berechtigungen aus, die der Zuschussempfänger anderen Prinzipalen in seinem Konto gewähren kann. AWS Diese Option wird nicht unterstützt, wenn Sie einem IAM-Prinzipal von einem externen Konto aus Berechtigungen gewähren.
- Wählen Sie Grant (Erteilen).

Auf der Seite „Datenberechtigungen“ werden die Berechtigungsdetails angezeigt. Wenn Sie die Option „Prinzipale nach Attributen“ verwendet haben, um Berechtigungen zu erteilen, können Sie die erteilten Berechtigungen `ALLPrincipals` in der Liste einsehen.

## AWS CLI

Informationen zum Erteilen von Katalogberechtigungen mithilfe von AWS CLI finden Sie unter [Erstellen von Amazon Redshift Redshift-Verbundkatalogen](#).

## Erteilen von Datenbankberechtigungen mit der benannten Ressourcenmethode

In den folgenden Schritten wird erklärt, wie Datenbankberechtigungen mithilfe der benannten Ressourcenmethode erteilt werden.

### Console

Verwenden Sie die Seite „Berechtigungen gewähren“ in der Lake Formation Formation-Konsole. Die Seite ist in die folgenden Abschnitte unterteilt:

- **Prinzipaltyp** — Der Bereich `Principals` umfasst die IAM-Benutzer, -Rollen, IAM Identity Center-Benutzer und -Gruppen, SAML-Benutzer und -Gruppen, AWS Konten, Organisationen oder Organisationseinheiten, für die Berechtigungen erteilt werden sollen. Im Abschnitt `Prinzipale nach Attributen` können Sie die Schlüssel und Werte für die Attribute angeben, die den IAM-Rollen zugeordnet sind.
- **LF-Tags oder Katalogressourcen** — Die Datenbanken, Tabellen, Ansichten oder Ressourcenlinks, für die Berechtigungen erteilt werden sollen.
- **Genehmigungen** — Die Lake Formation erteilt Genehmigungen.

#### Note

Informationen zum Erteilen von Berechtigungen für einen Datenbankressourcen-Link finden Sie unter [Erteilen von Ressourcenverknüpfungsberechtigungen](#).

1. Öffnen Sie die Seite „Berechtigungen gewähren“.

Öffnen Sie die AWS Lake Formation Konsole unter <https://console.aws.amazon.com/lakeformation/> und melden Sie sich als Data Lake-Administrator, Datenbankersteller oder IAM-Benutzer an, der über Grantable-Berechtigungen für die Datenbank verfügt.

Führen Sie eine der folgenden Aktionen aus:

- Wählen Sie im Navigationsbereich unter Berechtigungen die Option Datenberechtigungen aus. Wählen Sie dann Grant (Erteilen) aus.
- Wählen Sie im Navigationsbereich unter Datenkatalog die Option Datenbanken aus. Wählen Sie dann auf der Seite Datenbanken eine Datenbank aus, und wählen Sie im Menü Aktionen unter Berechtigungen die Option Gewähren aus.

#### Note

Sie können Berechtigungen für eine Datenbank über ihren Ressourcenlink gewähren. Wählen Sie dazu auf der Seite Datenbanken einen Ressourcenlink und dann im Menü Aktionen die Option Für Ziel gewähren aus. Weitere Informationen finden Sie unter [Funktionsweise von Ressourcenverbindungen in Lake Formation](#).

2. Geben Sie im Abschnitt Prinzipaltyp die Hauptbenutzer an, oder erteilen Sie den Prinzipalen mithilfe von Attributen Berechtigungen.

## Grant permissions

### Principals

Choose the principals to grant permissions.

☒ **IAM users and roles**  
Users or roles from this AWS account.

☐ **IAM Identity Center**  
- *new*  
Users and groups configured in IAM Identity Center.

☐ **SAML users and groups**  
SAML users and group or QuickSight ARNs.

☐ **External accounts**  
AWS account, AWS organization or IAM principal outside of this account

#### IAM users and roles

Add one or more IAM users or roles.

Choose IAM principals to add

AWSServiceRoleForRedshift   
Role

## IAM-Benutzer und -Rollen

Wählen Sie einen oder mehrere Benutzer oder Rollen aus der Liste der IAM-Benutzer und -Rollen aus.

## IAM Identity Center

Wählen Sie einen oder mehrere Benutzer oder Gruppen aus der Liste Benutzer und Gruppen aus. Wählen Sie Hinzufügen aus, um weitere Benutzer oder Gruppen hinzuzufügen.

## SAML-Benutzer und -Gruppen

Geben Sie für SAML- und Quick-Benutzer und -Gruppen einen oder mehrere Amazon-Ressourcennamen (ARNs) für Benutzer oder Gruppen ein, die über SAML verbunden sind, oder ARNs für Amazon Quick-Benutzer oder -Gruppen. Drücken Sie nach jedem ARN die Eingabetaste.

Informationen zur Erstellung von finden Sie unter ARNs. [Lake Formation erteilt und widerruft AWS CLI Befehle](#)

### Note

Die Integration von Lake Formation mit Quick wird nur für die Quick Enterprise Edition unterstützt.

## Externe Konten

Geben Sie für AWS-Konto, AWS Organisation oder IAM-Principal ein oder mehrere gültige AWS Konten IDs, Organisationen IDs, Organisationseinheiten IDs oder ARN für den IAM-Benutzer oder die IAM-Rolle ein. Drücken Sie nach jeder ID die Eingabetaste.

Eine Organisations-ID besteht aus „o-“, gefolgt von 10—32 Kleinbuchstaben oder Ziffern.

Eine Organisationseinheits-ID beginnt mit „ou-“, gefolgt von 4—32 Kleinbuchstaben oder Ziffern (der ID des Stammes, der die Organisationseinheit enthält). Auf diese Zeichenfolge folgen ein zweiter Gedankenstrich „-“ und 8 bis 32 zusätzliche Kleinbuchstaben oder Ziffern.



## Prinzipale nach Attributen

Geben Sie den Attributschlüssel und den Wert (e) an. Wenn Sie mehr als einen Wert wählen, erstellen Sie einen Attributausdruck mit einem OR-Operator. Das heißt, wenn einer der Attribut-Tag-Werte, die einer IAM-Rolle oder einem IAM-Benutzer zugewiesen sind, übereinstimmt, role/user erhält der Benutzer Zugriffsberechtigungen für die Ressource.

Wählen Sie den Berechtigungsbereich aus, indem Sie angeben, ob Sie Prinzipalen mit entsprechenden Attributen in demselben Konto oder in einem anderen Konto Berechtigungen gewähren.

3. Wählen Sie im Abschnitt LF-Tags oder Katalogressourcen die Option Benannte Datenkatalogressourcen aus.

## LF-Tags or catalog resources

Choose a method to grant permissions.

☐ Resources matched by LF-Tags (recommended)  
Manage permissions indirectly for resources or data matched by a specific set of LF-Tags.

☒ Named Data Catalog resources  
Manage permissions for specific databases or tables, in addition to fine-grained data access.

### Catalogs

Choose catalogs

Default catalog

### Databases

Select one or more databases.

Choose databases

sales

### Tables - optional

Select one or more tables.

Choose tables

### Views - optional

Select one or more views.

Choose views

### Data filters - optional

Select one or more data filters.

Choose data filters

Load more

Create new

[Manage data filters](#)

4. Wählen Sie eine oder mehrere Datenbanken aus der Datenbankliste aus. Sie können auch einen oder mehrere and/or Tabellendatenfilter auswählen.
5. Wählen Sie im Abschnitt Berechtigungen die Berechtigungen und erteilbare Berechtigungen aus. Wählen Sie unter Datenbankberechtigungen eine oder mehrere Berechtigungen aus, die Sie gewähren möchten.

## Database permissions

### Database permissions

Choose specific access permissions to grant.

- ☐ Create table   ☐ Alter   ☐ Drop  
☐ Describe

### ☐ Super

This permission is the union of all the individual permissions to the left, and supersedes them.

### Grantable permissions

Choose the permission that may be granted to others.

- ☐ Create table   ☐ Alter   ☐ Drop  
☐ Describe

### ☐ Super

This permission allows the principal to grant any of the permissions to the left, and supersedes those grantable permissions.

### Note

Nachdem Sie eine Datenbank mit einer `Create Table` Standorteigenschaft, die `Alter` auf einen registrierten Standort verweist, erteilt haben, müssen Sie sicherstellen, dass Sie auch den Prinzipalen Datenspeicherberechtigungen für den Standort gewähren. Weitere Informationen finden Sie unter [Erteilung von Berechtigungen zum Speicherort von Daten](#).

6. (Optional) Wählen Sie unter Erteilbare Berechtigungen die Berechtigungen aus, die der Zuschussempfänger anderen Prinzipalen in seinem Konto gewähren kann. AWS Diese Option wird nicht unterstützt, wenn Sie einem IAM-Prinzipal von einem externen Konto aus Berechtigungen gewähren.
7. Wählen Sie Grant (Erteilen).

## AWS CLI

Sie können Datenbankberechtigungen gewähren, indem Sie die benannte Ressourcenmethode und die AWS Command Line Interface (AWS CLI) verwenden.

Um Datenbankberechtigungen zu gewähren, verwenden Sie AWS CLI

- Führen Sie einen `grant-permissions` Befehl aus und geben Sie je nach erteilter Berechtigung eine Datenbank oder den Datenkatalog als Ressource an.

Ersetzen Sie es in den folgenden Beispielen `<account-id>` durch eine gültige AWS Konto-ID.

Example— Gewähren Sie die Erstellung einer Datenbank

In diesem Beispiel wird `CREATE_DATABASE` dem Benutzer eine Genehmigung erteilt `datalake_user1`. Da es sich bei der Ressource, für die diese Berechtigung erteilt wird, um den Datenkatalog handelt, gibt der Befehl eine leere `CatalogResource` Struktur als `resource` Parameter an.

```
aws lakeformation grant-permissions --principal
DataLakePrincipalIdentifier=arn:aws:iam::<account-id>:user/datalake_user1 --
permissions "CREATE_DATABASE" --resource '{ "Catalog": {} }'
```

Example— Erteilt die Erlaubnis, Tabellen in einer bestimmten Datenbank zu erstellen

Das nächste Beispiel gewährt `CREATE_TABLE` dem Benutzer Zugriff auf die Datenbank `retaildatalake_user1`.

```
aws lakeformation grant-permissions --principal
DataLakePrincipalIdentifier=arn:aws:iam::<account-id>:user/datalake_user1 --
permissions "CREATE_TABLE" --resource '{ "Database": { "Name": "retail" } }'
```

Example— Gewährung an ein externes AWS Konto mit der Option `Grant`

Im nächsten Beispiel wird dem externen Konto `1111-2222-3333` `CREATE_TABLE` mit der `Grant-Option` `retail` in der Datenbank gewährt.

```
aws lakeformation grant-permissions --principal
DataLakePrincipalIdentifier=111122223333 --permissions "CREATE_TABLE"
--permissions-with-grant-option "CREATE_TABLE" --resource '{ "Database":
{ "Name": "retail" } }'
```

Example— Zuschuss für eine Organisation

Im nächsten Beispiel werden der Organisation Zuschüsse `ALTER` mit der `Grant-Option` `issues` in der Datenbank gewährt `to-abcdefghijkl`.

```
aws lakeformation grant-permissions --principal
DataLakePrincipalIdentifier=arn:aws:organizations::111122223333:organization/
o-abcdefghijkl --permissions "ALTER" --permissions-with-grant-option "ALTER" --
resource '{ "Database": {"Name":"issues"}}'
```

Example- Gewähren Sie ALLIAMPrincipals an dasselbe Konto

Im nächsten Beispiel wird allen Principals im selben Konto CREATE\_TABLE Berechtigungen für die Datenbank retail erteilt. Diese Option ermöglicht es jedem Prinzipal im Konto, eine Tabelle in der Datenbank und einen Tabellenressourcenlink zu erstellen, sodass integrierte Abfrage-Engines auf gemeinsam genutzte Datenbanken und Tabellen zugreifen können. Diese Option ist besonders nützlich, wenn ein Schulleiter einen kontoübergreifenden Zuschuss erhält und nicht berechtigt ist, Ressourcenlinks zu erstellen. In diesem Szenario kann der Data Lake-Administrator eine Platzhalterdatenbank erstellen und der ALLIAMPrincipal Gruppe CREATE\_TABLE Berechtigungen erteilen, sodass jeder IAM-Prinzipal im Konto Ressourcenlinks in der Platzhalterdatenbank erstellen kann.

```
aws lakeformation grant-permissions --principal
DataLakePrincipalIdentifier=111122223333:IAMPrincipals
--permissions "CREATE_TABLE" --resource '{ "Database":
{"Name":"temp","CatalogId":"111122223333"}}'
```

Example— ALLIAMPrincipals In einem externen Konto gewähren

Das nächste Beispiel gewährt allen Prinzipalen in einem externen Konto retail Zugriff CREATE\_TABLE auf die Datenbank. Diese Option ermöglicht es jedem Prinzipal im Konto, eine Tabelle in der Datenbank zu erstellen.

```
aws lakeformation grant-permissions --principal
DataLakePrincipalIdentifier=111122223333:IAMPrincipals
--permissions "CREATE_TABLE" --resource '{ "Database":
{"Name":"retail","CatalogId":"123456789012"}}'
```

#### Note

Stellen Sie sicher, dass Sie den Prinzipalen auch Datenspeicherberechtigungen für den Standort gewähren, nachdem Sie CREATE\_TABLE oder ALTER für eine Datenbank erteilt

haben, deren Standorteigenschaft auf einen registrierten Standort verweist. Weitere Informationen finden Sie unter [Erteilung von Berechtigungen zum Speicherort von Daten](#).

 Weitere Informationen finden Sie auch unter

- [Referenz zu den Genehmigungen von Lake Formation](#)
- [Erteilen von Berechtigungen für eine Datenbank oder Tabelle, die mit Ihrem Konto geteilt wird](#)
- [Zugreifen auf und Anzeigen von gemeinsam genutzten Datenkatalogtabellen und Datenbanken](#)

## Erteilen von Tabellenberechtigungen mithilfe der benannten Ressourcenmethode

Sie können die Lake Formation Formation-Konsole verwenden oder AWS CLI Lake Formation Formation-Berechtigungen für Datenkatalogtabellen gewähren. Sie können Berechtigungen für einzelne Tabellen gewähren, oder Sie können mit einem einzigen Erteilungsvorgang Berechtigungen für alle Tabellen in einer Datenbank gewähren.

Wenn Sie Berechtigungen für alle Tabellen in einer Datenbank gewähren, gewähren Sie implizit die DESCRIBE Berechtigung für die Datenbank. Die Datenbank wird dann auf der Datenbankseite der Konsole angezeigt und durch den GetDataBases API-Vorgang zurückgegeben. Diese automatische DESCRIBE Berechtigungsgewährung gilt nicht, wenn die attributbasierte Zugriffskontrolle (ABAC) verwendet wird. Wenn mithilfe von Attributen Berechtigungen für alle Tabellen in einer Datenbank erteilt werden, erteilt Lake Formation der Datenbank nicht implizit DESCRIBE Berechtigungen.

Wenn Sie die zu erteilende Berechtigung auswählen `SELECT`, haben Sie die Möglichkeit, einen Spalten-, Zeilen- oder Zellenfilter anzuwenden.

### Console

In den folgenden Schritten wird erklärt, wie Tabellenberechtigungen mithilfe der benannten Ressourcenmethode und der Seite Data-Lake-Berechtigungen gewähren in der Lake Formation Formation-Konsole erteilt werden. Die Seite ist in folgende Abschnitte unterteilt:

- Prinzipaltypen — Die Benutzer, Rollen, AWS Konten, Organisationen oder Organisationseinheiten, denen Berechtigungen erteilt werden sollen. Sie können auch Prinzipalen mit entsprechenden Attributen Berechtigungen erteilen.
- LF-Tags oder Katalogressourcen — Die Datenbanken, Tabellen oder Ressourcenlinks, für die Berechtigungen erteilt werden sollen.
- Genehmigungen — Die Lake Formation erteilt Genehmigungen.

 Note

Informationen zum Erteilen von Berechtigungen für einen Tabellenressourcenlink finden Sie unter [Erteilen von Ressourcenverknüpfungsberechtigungen](#).

1. Öffnen Sie die Seite „Berechtigungen gewähren“.

Öffnen Sie die AWS Lake Formation Konsole unter <https://console.aws.amazon.com/lakeformation/> und melden Sie sich als Data Lake-Administrator, als Tabellenersteller oder als Benutzer an, dem mit der Option „Gewähren“ Berechtigungen für die Tabelle erteilt wurden.

Führen Sie eine der folgenden Aktionen aus:

- Wählen Sie im Navigationsbereich unter Berechtigungen die Option Datenberechtigungen aus. Wählen Sie dann Grant (Erteilen) aus.
- Wählen Sie im Navigationsbereich Tables (Tabellen) aus. Wählen Sie dann auf der Seite Tabellen eine Tabelle aus, und wählen Sie im Menü Aktionen unter Berechtigungen die Option Gewähren aus.

 Note

Sie können über den zugehörigen Ressourcenlink Berechtigungen für eine Tabelle gewähren. Wählen Sie dazu auf der Seite Tabellen einen Ressourcenlink und dann im Menü Aktionen die Option Auf Ziel gewähren aus. Weitere Informationen finden Sie unter [Funktionsweise von Ressourcenverbindungen in Lake Formation](#).

2. Geben Sie als Nächstes im Abschnitt Prinzipaltypen Principals oder Principals mit entsprechenden Attributen an, um Berechtigungen zu gewähren.

## IAM-Benutzer und -Rollen

Wählen Sie einen oder mehrere Benutzer oder Rollen aus der Liste der IAM-Benutzer und -Rollen aus.

## IAM Identity Center

Wählen Sie einen oder mehrere Benutzer oder Gruppen aus der Liste Benutzer und Gruppen aus.

## SAML-Benutzer und -Gruppen

Geben Sie für SAML- und Quick-Benutzer und -Gruppen einen oder mehrere Amazon-Ressourcennamen (ARNs) für Benutzer oder Gruppen ein, die über SAML verbunden sind, oder ARNs für Quick-Benutzer oder -Gruppen. Drücken Sie nach jedem ARN die Eingabetaste.

Informationen zur Erstellung von finden Sie unter ARNs. [Lake Formation erteilt und widerruft AWS CLI Befehle](#)

### Note

Die Integration von Lake Formation mit Quick wird nur für die Quick Enterprise Edition unterstützt.

## Externe Konten

Geben Sie für AWS-Konto „AWS Organisation“ oder „IAM-Principal“ eine oder mehrere gültige Organisationen AWS-Konto IDs IDs, Organisationseinheiten IDs oder den ARN für den IAM-Benutzer oder die IAM-Rolle ein. Drücken Sie nach jeder ID die Eingabetaste.

Eine Organisations-ID besteht aus „o-“, gefolgt von 10—32 Kleinbuchstaben oder Ziffern.

Eine Organisationseinheits-ID beginnt mit „ou-“, gefolgt von 4—32 Kleinbuchstaben oder Ziffern (der ID des Stammes, der die Organisationseinheit enthält). Auf diese Zeichenfolge folgen ein zweites „-“ -Zeichen und 8 bis 32 zusätzliche Kleinbuchstaben oder Ziffern.



## Prinzipale nach Attributen

Geben Sie den Attributschlüssel und den Wert (e) an. Wenn Sie mehr als einen Wert wählen, erstellen Sie einen Attributausdruck mit einem OR-Operator. Das heißt, wenn einer der Attribut-Tag-Werte, die einer IAM-Rolle oder einem IAM-Benutzer zugewiesen sind, übereinstimmt, role/user erhält der Benutzer Zugriffsberechtigungen für die Ressource

Wählen Sie den Berechtigungsbereich aus, indem Sie angeben, ob Sie Prinzipalen mit übereinstimmenden Attributen in demselben Konto oder in einem anderen Konto Berechtigungen gewähren.

3. Wählen Sie im Bereich LF-Tags oder Katalogressourcen eine Datenbank aus. Wählen Sie dann eine oder mehrere Tabellen oder Alle Tabellen aus.

### LF-Tags or catalog resources

☐ Resources matched by LF-Tags (recommended)  
Manage permissions indirectly for resources or data matched by a specific set of LF-Tags.

☒ Named data catalog resources  
Manager permissions for specific databases or tables, in addition to fine-grained data access.

**Databases**  
Select one or more databases.

Choose databases ▼

Load more

retail ✕

**Tables - optional**  
Select one or more tables.

Choose tables ▼

Load more

inventory ✕  
No description available

4. Geben Sie die Berechtigungen ohne Datenfilterung an.

Wählen Sie im Abschnitt Berechtigungen die Tabellenberechtigungen aus, die Sie gewähren möchten, und wählen Sie optional erteilbare Berechtigungen aus.

### Table and column permissions

#### Table permissions

Choose specific access permissions to grant.

☒ Alter
 ☒ Insert
 ☐ Drop

☐ Delete
 ☒ Select
 ☒ Describe

☐ Super
 

This permission is the union of all the individual permissions to the left, and supersedes them.

#### Grantable permissions

Choose the permission that may be granted to others.

☐ Alter
 ☐ Insert
 ☐ Drop

☐ Delete
 ☐ Select
 ☐ Describe

☐ Super
 

This permission allows the principal to grant any of the permissions to the left, and supersedes those grantable permissions.

Wenn Sie Select gewähren, wird der Abschnitt Datenberechtigungen unter dem Abschnitt Tabellen- und Spaltenberechtigungen angezeigt, wobei die Option Gesamter Datenzugriff standardmäßig ausgewählt ist. Akzeptieren Sie die Standardeinstellung.

### Data permissions

☒ All data access  
Grant access to all data without any restrictions.

☐ Simple column-based access  
Grant data access to specific columns only.

☐ Advanced cell-level filters  
Grant access to specific columns and/or rows with data filters.

5. Wählen Sie Grant (Erteilen).
6. Geben Sie die Auswahlberechtigung mit Datenfilterung an

Wählen Sie die Select-Berechtigung aus. Wählen Sie keine anderen Berechtigungen aus.

Der Abschnitt Datenberechtigungen wird unter dem Abschnitt Tabellen- und Spaltenberechtigungen angezeigt.

7. Führen Sie eine der folgenden Aktionen aus:
  - Wenden Sie nur einfache Spaltenfilterung an.
    1. Wählen Sie Einfacher spaltenbasierter Zugriff.

### Table and column permissions

#### Table permissions

Choose specific access permissions to grant.

☐ Alter
 ☐ Insert
 ☐ Drop

☐ Delete
 ☒ Select
 ☐ Describe

☐ Super
 

This permission is the union of all the individual permissions to the left, and supersedes them.

#### Grantable permissions

Choose the permission that may be granted to others.

☐ Alter
 ☐ Insert
 ☐ Drop

☐ Delete
 ☒ Select
 ☐ Describe

☐ Super
 

This permission allows the principal to grant any of the permissions to the left, and supersedes those grantable permissions.

### Data permissions

☐ All data access
 

Grant access to all data without any restrictions.

☒ Simple column-based access
 

Grant data access to specific columns only.

☐ Advanced cell-level filters
 

Grant access to specific columns and/or rows with data filters.

#### Choose permission filter

Choose whether to include or exclude columns.

☒ Include columns
 

Grant permissions to access specific columns.

☐ Exclude columns
 

Grant permissions to access all but specific columns.

#### Select columns

#### Grantable permissions

Choose the permission that may be granted to others.

☐ Select

- Wählen Sie aus, ob Spalten ein- oder ausgeschlossen werden sollen, und wählen Sie dann die Spalten aus, die ein- oder ausgeschlossen werden sollen.

Bei der Erteilung von Berechtigungen für ein externes AWS Konto oder eine externe Organisation werden nur Einschlusslisten unterstützt.

- (Optional) Aktivieren Sie unter „Erteilbare Berechtigungen“ die Option „Gewähren“ für die Berechtigung „Auswählen“.

Wenn Sie die Option „Gewähren“ angeben, kann der Empfänger des Zuschusses Berechtigungen nur für die Spalten gewähren, die Sie ihm gewähren.

**Note**

Sie können die Spaltenfilterung auch nur anwenden, indem Sie einen Datenfilter erstellen, der einen Spaltenfilter spezifiziert und alle Zeilen als Zeilenfilter angibt. Dies erfordert jedoch weitere Schritte.

- Wenden Sie die Spalten-, Zeilen- oder Zellenfilterung an.

1. Wählen Sie Erweiterte Filter auf Zellenebene aus.

**Data permissions**

☐ All data access  
Grant access to all data without any restrictions.

☐ Simple column-based access  
Grant data access to specific columns only.

☒ Advanced cell-level filters  
Grant access to specific columns and/or rows with data filters.

▶ View existing permissions

**Data filters to grant** ↻ 🔗 Manage filters Create new filter

🔍 Find filter

< 1 > ⚙️

| <input type="checkbox"/> | Filter name ▼   | Table ▼ | Database ▼ | Table catalog ID ▼ |
|--------------------------|-----------------|---------|------------|--------------------|
| <input type="checkbox"/> | restrict-pharma | orders  | sales      | 111122223333       |
| <input type="checkbox"/> | no-pharma       | orders  | sales      | 111122223333       |

2. (Optional) Erweitern Sie „Vorhandene Berechtigungen anzeigen“.
3. (Optional) Wählen Sie Neuen Filter erstellen.
4. (Optional) Um Details zu den aufgelisteten Filtern anzuzeigen oder um neue Filter zu erstellen oder bestehende zu löschen, wählen Sie Filter verwalten.

Die Seite Datenfilter wird in einem neuen Browserfenster geöffnet.

Wenn Sie mit der Seite Datenfilter fertig sind, kehren Sie zur Seite „Berechtigungen gewähren“ zurück und aktualisieren Sie die Seite gegebenenfalls, um alle neuen Datenfilter anzuzeigen, die Sie erstellt haben.

5. Wählen Sie einen oder mehrere Datenfilter aus, die auf den Zuschuss angewendet werden sollen.

 Note

Wenn die Liste keine Datenfilter enthält, bedeutet dies, dass für die ausgewählte Tabelle keine Datenfilter erstellt wurden.

## 8. Wählen Sie Grant (Erteilen).

### AWS CLI

Sie können Tabellenberechtigungen gewähren, indem Sie die benannte Ressourcenmethode und die AWS Command Line Interface (AWS CLI) verwenden.

Um Tabellenberechtigungen zu gewähren, verwenden Sie AWS CLI

- Führen Sie einen `grant-permissions` Befehl aus und geben Sie eine Tabelle als Ressource an.

#### Example— Grant für eine einzelne Tabelle — keine Filterung

Im folgenden Beispiel wird dem Benutzer `datalake_user1` im AWS Konto `1111-2222-3333` in der Tabelle in der Datenbank ein `SELECT` und `ALTER` gewährt. `inventory retail`

```
aws lakeformation grant-permissions --principal
DataLakePrincipalIdentifier=arn:aws:iam::111122223333:user/datalake_user1 --
permissions "SELECT" "ALTER" --resource '{ "Table": {"DatabaseName":"retail",
"Name":"inventory"}}'
```

 Note

Wenn Sie die `ALTER` Berechtigung für eine Tabelle erteilen, deren zugrunde liegende Daten sich an einem registrierten Speicherort befinden, müssen Sie sicherstellen, dass Sie auch den Prinzipalen Datenspeicherberechtigungen für diesen Speicherort gewähren. Weitere Informationen finden Sie unter [Erteilung von Berechtigungen zum Speicherort von Daten](#).

### Example— Mit der Option „Gewähren“ für alle Tabellen gewähren — keine Filterung

Im nächsten Beispiel werden Zuschüsse SELECT mit der Grant-Option für alle Tabellen in der Datenbank gewährt `retail`.

```
aws lakeformation grant-permissions --principal
DataLakePrincipalIdentifier=arn:aws:iam::111122223333:user/datalake_user1 --
permissions "SELECT" --permissions-with-grant-option "SELECT" --resource '{ "Table":
{ "DatabaseName": "retail", "TableWildcard": {} } }'
```

### Example— Grant mit einfacher Spaltenfilterung

Im nächsten Beispiel wird eine Teilmenge von Spalten in der Tabelle `persons` gewährt SELECT. Es verwendet eine einfache Spaltenfilterung.

```
aws lakeformation grant-permissions --principal
DataLakePrincipalIdentifier=arn:aws:iam::111122223333:user/datalake_user1 --
permissions "SELECT" --resource '{ "TableWithColumns": {"DatabaseName": "hr",
"Name": "persons", "ColumnNames": ["family_name", "given_name", "gender"]} }'
```

### Example— Grant mit einem Datenfilter

Dieses Beispiel bezieht sich SELECT auf die `orders` Tabelle und wendet den `restrict-pharma` Datenfilter an.

```
aws lakeformation grant-permissions --cli-input-json file://grant-params.json
```

Im Folgenden ist der Inhalt der Datei aufgeführt `grant-params.json`.

```
{
 "Principal": {"DataLakePrincipalIdentifier": "arn:aws:iam::111122223333:user/
datalake_user1"},
 "Resource": {
 "DataCellsFilter": {
 "TableCatalogId": "111122223333",
 "DatabaseName": "sales",
 "TableName": "orders",
 "Name": "restrict-pharma"
 }
 }
}
```

```
},
 "Permissions": ["SELECT"],
 "PermissionsWithGrantOption": ["SELECT"]
}
```

 Weitere Informationen finden Sie auch unter

- [Überblick über die Genehmigungen für Lake Formation](#)
- [Datenfilterung und Sicherheit auf Zellebene in Lake Formation](#)
- [Referenz zu Personas und IAM-Berechtigungen in Lake Formation](#)
- [Erteilen von Ressourcenverknüpfungsberechtigungen](#)
- [Zugreifen auf und Anzeigen von gemeinsam genutzten Datenkatalogtabellen und Datenbanken](#)

## Erteilen von Berechtigungen für Ansichten mithilfe der benannten Ressourcenmethode

In den folgenden Schritten wird erklärt, wie Sie mithilfe der benannten Ressourcenmethode und der Seite „Berechtigungen gewähren“ Berechtigungen für Ansichten gewähren. Die Seite ist in die folgenden Abschnitte unterteilt:

- Haupttypen — Die IAM-Benutzer, Rollen, IAM Identity Center-Benutzer und -Gruppen AWS-Konten, Organisationen oder Organisationseinheiten, denen Berechtigungen erteilt werden sollen. Sie können auch Prinzipalen mit entsprechenden Attributen Berechtigungen erteilen.
- LF-Tags oder Katalogressourcen — Die Datenbanken, Tabellen, Ansichten oder Ressourcenlinks, für die Berechtigungen erteilt werden sollen.
- Berechtigungen — Die zu erteilenden Data Lake-Berechtigungen.

Öffnen Sie die Seite „Berechtigungen gewähren“

1. Öffnen Sie die AWS Lake Formation Konsole unter <https://console.aws.amazon.com/lakeformation/> und melden Sie sich als Data Lake-Administrator, Datenbankersteller oder IAM-Benutzer an, der über Grantable-Berechtigungen für die Datenbank verfügt.
2. Führen Sie eine der folgenden Aktionen aus:

- Wählen Sie im Navigationsbereich unter Berechtigungen die Option Datenberechtigungen aus. Wählen Sie dann Grant (Erteilen) aus.
- Wählen Sie im Navigationsbereich unter Datenkatalog die Option Ansichten aus. Wählen Sie dann auf der Seite Ansichten eine Ansicht aus, und wählen Sie im Menü Aktionen unter Berechtigungen die Option Gewähren aus.

#### Note

Sie können über den zugehörigen Ressourcenlink Berechtigungen für eine Ansicht gewähren. Wählen Sie dazu auf der Seite Ansichten einen Ressourcenlink und dann im Menü Aktionen die Option Auf Ziel gewähren aus. Weitere Informationen finden Sie unter [Funktionsweise von Ressourcenverbindungen in Lake Formation](#).

Geben Sie die Haupttypen an

Wählen Sie im Abschnitt Principals types entweder Principals oder Principals by attributes aus. Wenn Sie Principals wählen, sind die folgenden Optionen verfügbar:

#### IAM-Benutzer und -Rollen

Wählen Sie einen oder mehrere Benutzer oder Rollen aus der Liste der IAM-Benutzer und -Rollen aus.

#### IAM Identity Center

Wählen Sie einen oder mehrere Benutzer oder Gruppen aus der Liste Benutzer und Gruppen aus.

#### SAML-Benutzer und -Gruppen

Geben Sie für SAML- und Quick-Benutzer und -Gruppen einen oder mehrere Amazon-Ressourcennamen (ARNs) für Benutzer oder Gruppen ein, die über SAML verbunden sind, oder ARNs für Amazon Quick-Benutzer oder -Gruppen. Drücken Sie nach jedem ARN die Eingabetaste.

Informationen zur Erstellung von finden Sie unter ARNs. [Lake Formation erteilt und widerruft AWS CLI Befehle](#)



 Note

Die Integration von Lake Formation mit Quick wird nur für die Quick Enterprise Edition unterstützt.

## Externe Konten

Geben Sie für AWS-Konto, AWS Organisation oder IAM-Principal ein oder mehrere gültige AWS Konten IDs, Organisationen IDs, Organisationseinheiten IDs oder ARN für den IAM-Benutzer oder die IAM-Rolle ein. Drücken Sie nach jeder ID die Eingabetaste.

Eine Organisations-ID besteht aus „o-“, gefolgt von 10—32 Kleinbuchstaben oder Ziffern.

Eine Organisationseinheits-ID beginnt mit „ou-“, gefolgt von 4—32 Kleinbuchstaben oder Ziffern (der ID des Stammes, der die Organisationseinheit enthält). Auf diese Zeichenfolge folgen ein zweiter Gedankenstrich „-“ und 8 bis 32 zusätzliche Kleinbuchstaben oder Ziffern.

 Weitere Informationen finden Sie unter:

- [Zugreifen auf und Anzeigen von gemeinsam genutzten Datenkatalogtabellen und Datenbanken](#)

## Prinzipale nach Attributen

Geben Sie den Attributschlüssel und den Wert (e) an. Wenn Sie mehr als einen Wert wählen, erstellen Sie einen Attributausdruck mit einem OR-Operator. Das heißt, wenn einer der Attribut-Tag-Werte, die einer IAM-Rolle oder einem IAM-Benutzer zugewiesen sind, übereinstimmt, role/user erhält der Benutzer Zugriffsberechtigungen für die Ressource

Wählen Sie den Berechtigungsbereich aus, indem Sie angeben, ob Sie Prinzipalen mit übereinstimmenden Attributen in demselben Konto oder in einem anderen Konto Berechtigungen gewähren.

## Geben Sie die Ansichten an

Wählen Sie im Bereich LF-Tags oder Katalogressourcen eine oder mehrere Ansichten aus, für die Sie Berechtigungen gewähren möchten.

1. Wählen Sie Benannte Datenkatalogressourcen aus.
2. Wählen Sie eine oder mehrere Ansichten aus der Liste Ansichten aus. Sie können auch einen oder mehrere Kataloge, Datenbanken, Tabellen und and/or Datenfilter auswählen.

Die Gewährung von Data Lake-Berechtigungen `All tables` innerhalb einer Datenbank führt dazu, dass der Empfänger über Berechtigungen für alle Tabellen und Ansichten in der Datenbank verfügt.

Geben Sie die Berechtigungen an

Wählen Sie im Abschnitt Berechtigungen die Berechtigungen und erteilbare Berechtigungen aus.

**View permissions**

View permissions  
Choose specific access permissions to grant.

☐ Select    ☐ Describe    ☐ Drop

☐ Super  
This permission is the union of all the individual permissions to the left, and supersedes them.

Grantable permissions  
Choose the permission that may be granted to others.

☐ Select    ☐ Describe    ☐ Drop

☐ Super  
This permission allows the principal to grant any of the permissions to the left, and supersedes those grantable permissions.

Cancel    Grant

1. Wählen Sie unter Berechtigungen anzeigen eine oder mehrere Berechtigungen aus, die Sie gewähren möchten.
2. (Optional) Wählen Sie unter Erteilbare Berechtigungen die Berechtigungen aus, die der Empfänger der Gewährung anderen Hauptbenutzern in seiner Umgebung gewähren kann. AWS-Konto  
Diese Option wird nicht unterstützt, wenn Sie einem IAM-Prinzipal von einem externen Konto aus Berechtigungen gewähren.
3. Wählen Sie Grant (Erteilen).

 Weitere Informationen finden Sie unter:

- [Referenz zu den Genehmigungen von Lake Formation](#)
- [Erteilen von Berechtigungen für eine Datenbank oder Tabelle, die mit Ihrem Konto geteilt wird](#)

## Tag-basierte Zugangskontrolle von Lake Formation

Lake Formation Tag-Based Access Control (LF-TBAC) ist eine Autorisierungsstrategie, die Berechtigungen auf der Grundlage von Attributen definiert. In Lake Formation werden diese Attribute als LF-Tags bezeichnet. Sie können LF-Tags an Datenkatalogressourcen anhängen und Lake Formation-Prinzipalen mithilfe dieser LF-Tags Berechtigungen für diese Ressourcen erteilen. Lake Formation ermöglicht Operationen mit diesen Ressourcen, wenn der Principal Zugriff auf einen Tag-Wert gewährt hat, der dem Ressourcen-Tag-Wert entspricht.

LF-TBAC ist hilfreich in Umgebungen, die schnell wachsen, und hilft in Situationen, in denen die Richtlinienverwaltung umständlich wird.

LF-TBAC ist die empfohlene Methode, um Lake Formation-Berechtigungen zu erteilen, wenn es eine große Anzahl von Datenkatalogobjekten gibt, einschließlich Verbundkatalogen, Datenbanken, Tabellen und Ansichten. Lake Formation unterstützt tagbasierte Zugriffskontrolle für Verbundkataloge von Amazon S3 S3-Tabellen, Amazon Redshift Data Warehouses und föderierten Datenquellen wie SQL Server und Amazon DynamoDB Snowflake.

### Note

IAM-Tags sind nicht dasselbe wie LF-Tags. Diese Tags sind nicht austauschbar. LF-Tags werden verwendet, um Lake Formation-Berechtigungen zu gewähren, und IAM-Tags werden verwendet, um IAM-Richtlinien zu definieren.

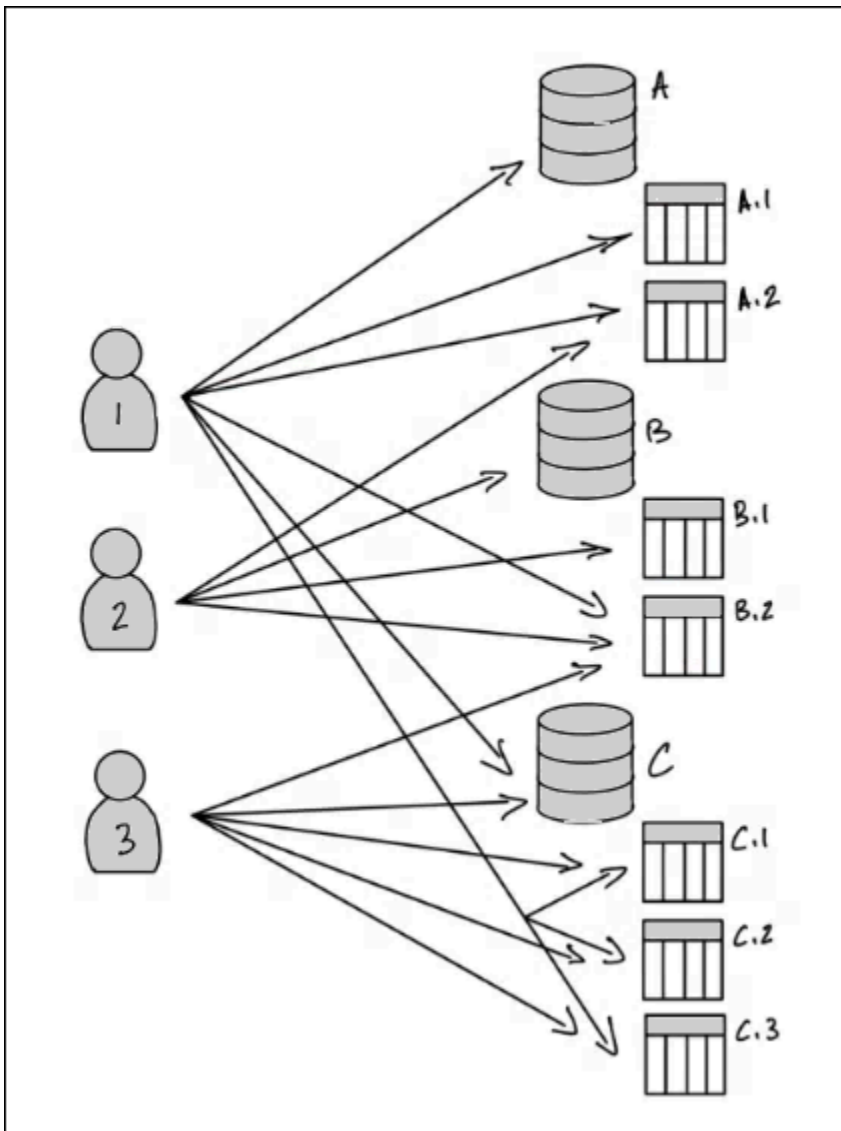
## So funktioniert die Tag-basierte Zugriffskontrolle von Lake Formation

Jedes LF-Tag ist ein Schlüssel-Wert-Paar, z. B. `department=sales` oder `classification=restricted`. Ein Schlüssel kann mehrere definierte Werte haben, wie z. `department=sales,marketing,engineering,finance`.

Um die LF-TBAC-Methode zu verwenden, führen Data Lake-Administratoren und Datentechniker die folgenden Aufgaben aus.

| Aufgabe                                                                                                                                                                                                                            | Einzelheiten zu den Aufgaben                                                       |
|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|------------------------------------------------------------------------------------|
| 1. Definieren Sie die Eigenschaften und Beziehungen von LF-Tags.                                                                                                                                                                   | -                                                                                  |
| 2. Erstelle die LF-Tag-Ersteller in Lake Formation.                                                                                                                                                                                | <a href="#">Hinzufügen von LF-Tag-Erstellern</a>                                   |
| 3. Erstellen Sie das LF-Tag in Lake Formation.                                                                                                                                                                                     | <a href="#">LF-Tags erstellen</a>                                                  |
| 4. Weisen Sie den Datenkatalogressourcen LF-Tags zu.                                                                                                                                                                               | <a href="#">Zuweisen von LF-Tags zu Datenkatalogressourcen</a>                     |
| 5. Erteilen Sie anderen Principals Berechtigungen, um Ressourcen LF-Tags zuzuweisen, optional mit der Option Grant.                                                                                                                | <a href="#">Verwaltung von LF-Tag-Wertberechtigungen</a>                           |
| 6. Erteilen Sie Prinzipalen LF-Tag-Ausdrücke, optional mit der Grant-Option.                                                                                                                                                       | <a href="#">Erteilen von Data Lake-Berechtigungen mithilfe der LF-TBAC-Methode</a> |
| 7. (Empfohlen) Nachdem Sie überprüft haben, ob die Prinzipale über die LF-TBAC-Methode Zugriff auf die richtigen Ressourcen haben, widerrufen Sie die Berechtigungen, die mithilfe der benannten Ressourcenmethode erteilt wurden. | -                                                                                  |

Stellen Sie sich den Fall vor, dass Sie drei Prinzipalen Berechtigungen für drei Datenbanken und sieben Tabellen erteilen müssen.



Um die im obigen Diagramm angegebenen Berechtigungen mithilfe der Methode der benannten Ressource zu erhalten, müssten Sie 17 Zuweisungen vornehmen, und zwar wie folgt (in Pseudocode).

```

GRANT CREATE_TABLE ON Database A TO PRINCIPAL 1
GRANT SELECT, INSERT ON Table A.1 TO PRINCIPAL 1
GRANT SELECT, INSERT ON Table A.2 TO PRINCIPAL 1
GRANT SELECT, INSERT ON Table B.2 TO PRINCIPAL 1
...
GRANT SELECT, INSERT ON Table A.2 TO PRINCIPAL 2
GRANT CREATE_TABLE ON Database B TO PRINCIPAL 2
...
GRANT SELECT, INSERT ON Table C.3 TO PRINCIPAL 3

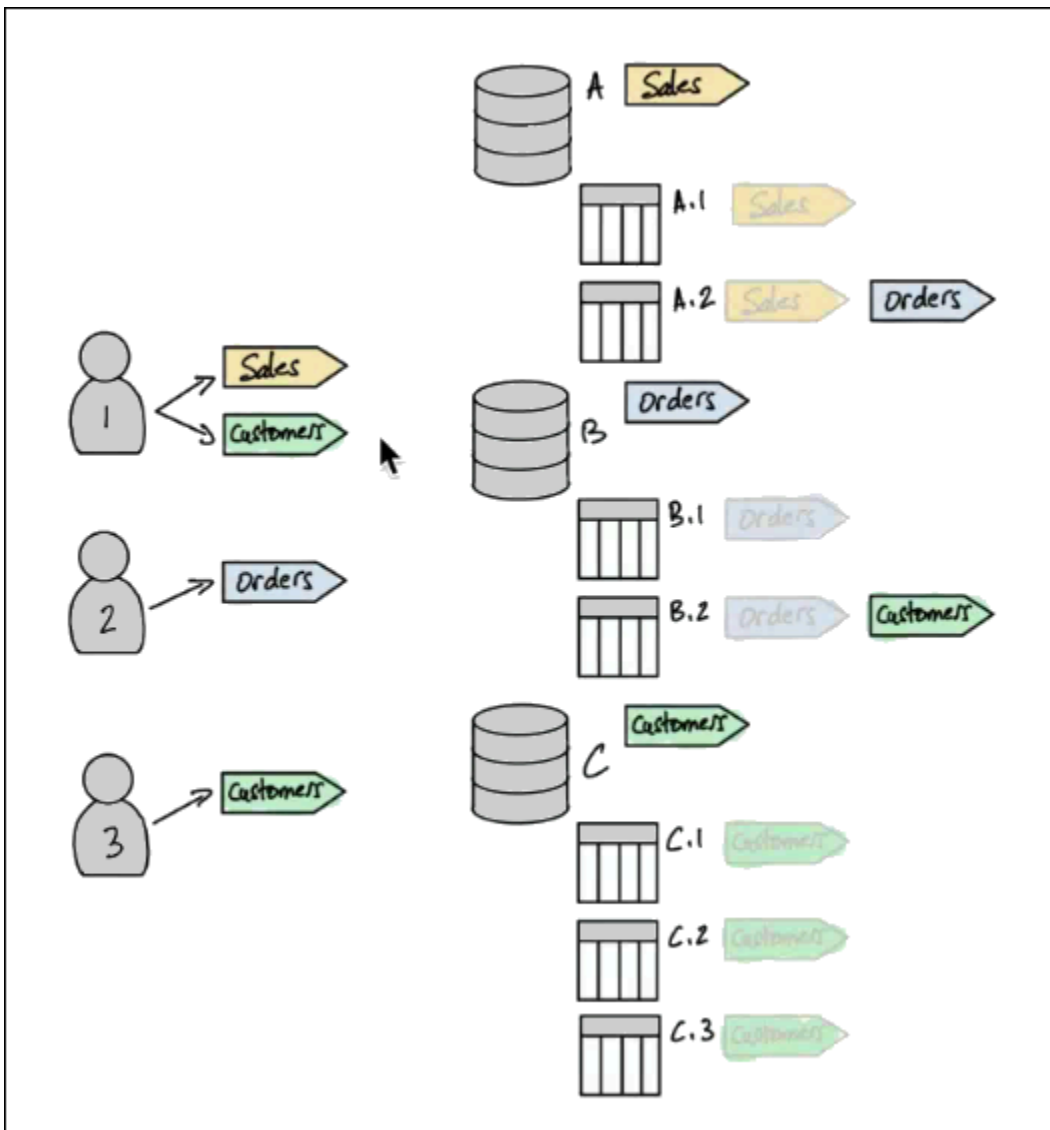
```

Überlegen Sie sich nun, wie Sie mithilfe von LF-TBAC Berechtigungen gewähren würden. Das folgende Diagramm zeigt, dass Sie Datenbanken und Tabellen LF-Tags zugewiesen und Prinzipalen Berechtigungen für LF-Tags erteilt haben.

In diesem Beispiel stellen die LF-Tags Bereiche des Data Lake dar, die Analysen für verschiedene Module einer ERP-Anwendungssuite (Enterprise Resource Planning) enthalten. Sie können sie verwenden, um den Zugriff auf die Analysedaten für die verschiedenen Module zu steuern. Alle LF-Tags haben den Schlüssel `module` und mögliche Werte `SalesOrders`, und. `Customers` Ein Beispiel für ein LF-Tag sieht so aus:

```
module=Sales
```

Das Diagramm zeigt nur die LF-Tag-Werte.



## Tag-Zuweisungen zu Datenkatalogressourcen und Vererbung

Tabellen erben LF-Tags von Datenbanken und Spalten erben LF-Tags von Tabellen. Vererbte Werte können überschrieben werden. Im vorherigen Diagramm werden abgedunkelte LF-Tags vererbt.

Aufgrund der Vererbung muss der Data Lake-Administrator nur die fünf folgenden LF-Tag-Zuweisungen zu Ressourcen vornehmen (in Pseudocode).

```
ASSIGN TAGS module=Sales TO database A
ASSIGN TAGS module=Orders TO table A.2
ASSIGN TAGS module=Orders TO database B
ASSIGN TAGS module=Customers TO table B.2
ASSIGN TAGS module=Customers TO database C
```

## Tag-Zuschüsse für Schulleiter

Nach der Zuweisung von LF-Tags zu den Datenbanken und Tabellen muss der Data Lake-Administrator den Prinzipalen nur vier LF-Tags gewähren, und zwar wie folgt (in Pseudocode).

```
GRANT TAGS module=Sales TO Principal 1
GRANT TAGS module=Customers TO Principal 1
GRANT TAGS module=Orders TO Principal 2
GRANT TAGS module=Customers TO Principal 3
```

Jetzt kann ein Principal mit dem module=Sales LF-Tag auf Datenkatalogressourcen mit dem LF-Tag zugreifen (z. B. Datenbank A), ein Principal mit dem module=Sales LF-Tag kann auf Ressourcen mit dem module=Customers LF-Tag zugreifen usw. module=Customers

Die obigen Grant-Befehle sind unvollständig. Dies liegt daran, dass sie zwar anhand von LF-Tags die Datenkatalogressourcen angeben, für die die Prinzipale Berechtigungen haben, sie geben jedoch nicht genau an, welche Lake Formation Formation-Berechtigungen (z. B. ALTER) die Principals SELECT für diese Ressourcen haben. Daher stellen die folgenden Pseudocode-Befehle genauer dar, wie Lake Formation Formation-Berechtigungen für Datenkatalogressourcen über LF-Tags erteilt werden.

```
GRANT (CREATE_TABLE ON DATABASES) ON TAGS module=Sales TO Principal 1
GRANT (SELECT, INSERT ON TABLES) ON TAGS module=Sales TO Principal 1
GRANT (CREATE_TABLE ON DATABASES) ON TAGS module=Customers TO Principal 1
GRANT (SELECT, INSERT ON TABLES) ON TAGS module=Customers TO Principal 1
GRANT (CREATE_TABLE ON DATABASES) ON TAGS module=Orders TO Principal 2
GRANT (SELECT, INSERT ON TABLES) ON TAGS module=Orders TO Principal 2
```

```
GRANT (CREATE_TABLE ON DATABASES) ON TAGS module=Customers TO Principal 3
GRANT (SELECT, INSERT ON TABLES) ON TAGS module=Customers TO Principal 3
```

## Zusammenstellen — Die daraus resultierenden Berechtigungen für Ressourcen

Angesichts der LF-Tags, die den Datenbanken und Tabellen im vorherigen Diagramm zugewiesen wurden, und der LF-Tags, die den Prinzipalen im Diagramm gewährt wurden, sind in der folgenden Tabelle die Lake Formation Formations-Berechtigungen aufgeführt, die die Prinzipale für die Datenbanken und Tabellen haben.

| Auftraggeber  | Über LF-Tags erteilte Berechtigungen                                                                                                                                                                                                                                                                                                     |
|---------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Schulleiter 1 | <ul style="list-style-type: none"> <li>• CREATE_TABLE auf Datenbank A</li> <li>• SELECT, INSERT in Tabelle A.1</li> <li>• SELECT, INSERT auf Tabelle B.2</li> <li>• CREATE_TABLE auf Datenbank C</li> <li>• SELECT, INSERT in Tabelle C.1</li> <li>• SELECT, INSERT auf Tabelle C.2</li> <li>• SELECT, INSERT auf Tabelle C.3</li> </ul> |
| Schulleiter 2 | <ul style="list-style-type: none"> <li>• SELECT, INSERT auf Tabelle A.2</li> <li>• CREATE_TABLE auf Datenbank B</li> <li>• SELECT, INSERT in Tabelle B.1</li> </ul>                                                                                                                                                                      |
| Schulleiter 3 | <ul style="list-style-type: none"> <li>• SELECT, INSERT auf Tabelle B.2</li> <li>• CREATE_TABLE auf Datenbank C</li> <li>• SELECT, INSERT in Tabelle C.1</li> <li>• SELECT, INSERT auf Tabelle C.2</li> <li>• SELECT, INSERT auf Tabelle C.3</li> </ul>                                                                                  |

## Unterm Strich

In diesem einfachen Beispiel konnte der Data Lake-Administrator mithilfe von fünf Zuweisungsvorgängen und acht Zuweisungsvorgängen 17 Berechtigungen angeben. Bei Dutzenden von Datenbanken und Hunderten von Tabellen wird der Vorteil der LF-TBAC-Methode gegenüber



der benannten Ressourcenmethode deutlich. Im hypothetischen Fall, dass jedem Hauptbenutzer Zugriff auf jede Ressource gewährt werden muss, und wo  $n(P)$  ist die Anzahl der Prinzipale und ist die Anzahl der Ressourcen:  $n(R)$

- Bei der Methode mit der Bezeichnung „Ressourcen“ beträgt die Anzahl der erforderlichen Zuschüsse  $\times n(P) n(R)$
- Bei der LF-TBAC-Methode, bei der ein einziger LF-Tag verwendet wird, ergibt die Gesamtzahl der Zuschüsse an Schulleiter und der Zuweisungen an Ressourcen einen Wert von  $+ n(P) n(R)$

 Weitere Informationen finden Sie auch unter

- [Verwaltung von LF-Tags für die Zugriffskontrolle auf Metadaten](#)
- [Erteilen von Data Lake-Berechtigungen mithilfe der LF-TBAC-Methode](#)

## Themen

- [Verwaltung von LF-Tags für die Zugriffskontrolle auf Metadaten](#)
- [Verwaltung von LF-Tag-Ausdrücken für die Zugriffskontrolle auf Metadaten](#)
- [Verwaltung von LF-Tag-Wertberechtigungen](#)

## Verwaltung von LF-Tags für die Zugriffskontrolle auf Metadaten

Um die Tag-Based Access Control (LF-TBAC) -Methode von Lake Formation zur Sicherung von Datenkatalogobjekten wie Katalogen, Datenbanken, Tabellen, Ansichten und Spalten zu verwenden, erstellen Sie LF-Tags, weisen sie Ressourcen zu und gewähren Prinzipalen LF-Tag-Berechtigungen.

Bevor Sie Datenkatalogobjekten LF-Tags zuweisen oder Prinzipalen Berechtigungen erteilen können, müssen Sie LF-Tags definieren. Nur ein Data Lake-Administrator oder ein Principal mit Berechtigungen zum Erstellen von LF-Tags kann LF-Tags erstellen.

### Ersteller von LF-Tags

LF-Tag Creator ist kein Administrator und hat die Rechte, LF-Tags zu erstellen und zu verwalten. Data Lake-Administratoren können LF-Tag-Ersteller mithilfe der Lake Formation Formation-Konsole oder CLI hinzufügen. LF-Tag-Ersteller verfügen über implizite Lake Formation Formation-Berechtigungen zum Aktualisieren und Löschen von LF-Tags, zum Zuweisen von LF-Tags zu

Ressourcen und zum Erteilen von LF-Tag-Berechtigungen und LF-Tag-Wertberechtigungen an andere Principals.

Mit LF-Tag-Erstellerrollen können Data Lake-Administratoren Tag-Management-Aufgaben wie das Erstellen und Aktualisieren von Tag-Schlüsseln und -Werten an Prinzipale delegieren, die keine Administratoren sind. Data Lake-Administratoren können LF-Tag-Erstellern auch erteilbare Berechtigungen gewähren. `Create LF-Tag` Anschließend kann der LF-Tag-Ersteller anderen Prinzipalen die Erlaubnis zur Erstellung von LF-Tags erteilen.

Sie können zwei Arten von Berechtigungen für LF-Tags gewähren:

- LF-Tag-Berechtigungen `-Create LF-Tag`, und. `Alter Drop` Diese Berechtigungen sind erforderlich, um LF-Tags zu erstellen, zu aktualisieren und zu löschen.

Data Lake-Administratoren und LF-Tag-Ersteller verfügen implizit über diese Berechtigungen für die von ihnen erstellten LF-Tags und können diese Berechtigungen explizit Prinzipalen zur Verwaltung von Tags im Data Lake gewähren.

- Berechtigungen für LF-Tag-Schlüsselwertpaare `-`, und. `Assign Describe Grant with LF-Tag expressions` Diese Berechtigungen sind erforderlich, um Datenkatalogobjekten LF-Tags zuzuweisen und Prinzipalen, die die Tag-basierte Zugriffskontrolle von Lake Formation verwenden, Berechtigungen für die Ressourcen zu gewähren. LF-Tag-Ersteller erhalten diese Berechtigungen implizit, wenn sie LF-Tags erstellen.

Nach Erhalt der `Create LF-Tag` Genehmigung und erfolgreicher Erstellung von LF-Tags kann der LF-Tag-Ersteller Ressourcen LF-Tags zuweisen und anderen Benutzern, die keine Administratorrechte haben, LF-Tag-Berechtigungen (`Create LF-Tag``AlterDrop`, und) zur Verwaltung von Tags im Data Lake gewähren. Sie können LF-Tags mithilfe der Lake Formation Formation-Konsole, der API oder der AWS Command Line Interface (AWS CLI) verwalten.

#### Note

Data Lake-Administratoren verfügen über implizite Lake Formation Berechtigungen, um LF-Tags zu erstellen, zu aktualisieren und zu löschen, Ressourcen LF-Tags zuzuweisen und Prinzipalen LF-Tag-Berechtigungen zu gewähren.

Bewährte Methoden und Überlegungen finden Sie unter [Bewährte Methoden und Überlegungen zur Tag-basierten Zugriffskontrolle von Lake Formation](#)

## Themen

- [Hinzufügen von LF-Tag-Erstellern](#)
- [LF-Tags erstellen](#)
- [LF-Tags werden aktualisiert](#)
- [LF-Tags löschen](#)
- [LF-Tags auflisten](#)
- [Zuweisen von LF-Tags zu Datenkatalogressourcen](#)
- [LF-Tags anzeigen, die einer Ressource zugewiesen sind](#)
- [Die Ressourcen anzeigen, denen ein LF-Tag zugewiesen ist](#)
- [Lebenszyklus eines LF-Tags](#)
- [Vergleich der Tag-basierten Zugriffskontrolle von Lake Formation mit der attributbasierten IAM-Zugriffskontrolle](#)

 Weitere Informationen finden Sie auch unter

- [Verwaltung von LF-Tag-Wertberechtigungen](#)
- [Erteilen von Data Lake-Berechtigungen mithilfe der LF-TBAC-Methode](#)
- [Tag-basierte Zugangskontrolle von Lake Formation](#)

## Hinzufügen von LF-Tag-Erstellern

Standardmäßig können Data Lake-Administratoren LF-Tags erstellen, aktualisieren und löschen, Datenkatalogobjekten Tags zuweisen und Prinzipalen Tag-Berechtigungen gewähren. Wenn Sie die Tag-Erstellung und -Verwaltung an Prinzipale ohne Administratorrechte delegieren möchten, kann der Data Lake-Administrator LF-Tag-Erstellerrollen erstellen und Lake Formation Create LF-Tag Formation-Berechtigungen für die Rollen erteilen. Mit erteilbarer Create LF-Tag Genehmigung können LF-Tag-Ersteller Aufgaben zur Erstellung und Wartung von Tags an andere Personen delegieren, die keine Administratorrechte haben.

Damit Data Lake-Administratoren LF-Tags Datenkatalogressourcen zuweisen können, müssen sie sich selbst assoziierte Rechte für LF-Tags gewähren, die nicht von ihnen erstellt wurden.

**Note**

Kontoübergreifende Zugriffsberechtigungen können nur Berechtigungen beinhalten. `Describe Associate` Sie können Prinzipalen in einem anderen Konto keine `DropAlter`, und `Grant with LFTag expressions` Berechtigungen gewähren `Create LF-Tag`.

## Themen

- [Für die Erstellung von LF-Tags sind IAM-Berechtigungen erforderlich](#)
- [Fügen Sie LF-Tag-Ersteller hinzu](#)

**i** Weitere Informationen finden Sie auch unter

- [Verwaltung von LF-Tag-Wertberechtigungen](#)
- [Erteilen von Data Lake-Berechtigungen mithilfe der LF-TBAC-Methode](#)
- [Tag-basierte Zugangskontrolle von Lake Formation](#)

Für die Erstellung von LF-Tags sind IAM-Berechtigungen erforderlich

Sie müssen Berechtigungen konfigurieren, damit ein Lake Formation-Prinzipal LF-Tags erstellen kann. Fügen Sie der Berechtigungsrichtlinie für den Prinzipal, der ein LF-Tag-Ersteller sein muss, die folgende Anweisung hinzu.

**Note**

Data Lake-Administratoren verfügen zwar über implizite Lake Formation-Berechtigungen, um LF-Tags zu erstellen, zu aktualisieren und zu löschen, Ressourcen LF-Tags zuzuweisen und Prinzipalen LF-Tags zu gewähren, aber Data Lake-Administratoren benötigen auch die folgenden IAM-Berechtigungen.

Weitere Informationen finden Sie unter [Referenz zu Personas und IAM-Berechtigungen in Lake Formation](#).

```
{
```

```
"Sid": "Transformational",
"Effect": "Allow",
 "Action": [
 "lakeformation:AddLFTagsToResource",
 "lakeformation:RemoveLFTagsFromResource",
 "lakeformation:GetResourceLFTags",
 "lakeformation:ListLFTags",
 "lakeformation:CreateLFTag",
 "lakeformation:GetLFTag",
 "lakeformation:UpdateLFTag",
 "lakeformation>DeleteLFTag",
 "lakeformation:SearchTablesByLFTags",
 "lakeformation:SearchDatabasesByLFTags"
]
}
```

Principals, die Ressourcen LF-Tags zuweisen und Prinzipalen LF-Tags gewähren, müssen über dieselben Berechtigungen verfügen, mit Ausnahme der Berechtigungen, und. `CreateLFTag` `UpdateLFTag` `DeleteLFTag`

Fügen Sie LF-Tag-Ersteller hinzu

Ein LF-Tag-Ersteller kann mithilfe der LF-TBAC-Methode ein LF-Tag erstellen, Tag-Schlüssel und -Werte aktualisieren, Tags löschen, Tags mit Datenkatalogressourcen verknüpfen und Prinzipalen Berechtigungen für Datenkatalog-Ressourcen gewähren. Der LF-Tag-Ersteller kann diese Berechtigungen auch Prinzipalen gewähren.

Sie können LF-Tag-Erstellerrollen mithilfe der AWS Lake Formation Konsole, der API oder der () erstellen. AWS Command Line Interface AWS CLI

console

Um einen LF-Tag-Ersteller hinzuzufügen

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

Melden Sie sich als Datalake-Administrator an.

2. Wählen Sie im Navigationsbereich unter Berechtigungen die Option LF-Tags und Berechtigungen aus.

Wählen Sie auf der Seite LF-Tags und Berechtigungen den Abschnitt LF-Tag-Ersteller und dann LF-Tag-Ersteller hinzufügen aus.

## Add LF-Tag creators

LF-Tag creators can create and manage LF-Tags. [Learn more](#) 

### LF-Tag creator details

**IAM users and roles**  
Add IAM users or roles.

Choose IAM principals to add ▼

lf-developer X

User

**Permission**  
Choose the permission to grant.

☒ Create LF-Tag

**Grantable permission**  
Choose the permission that may be granted to others.

☒ Create LF-Tag

Cancel

Add

3. Wählen Sie auf der Seite „LF-Tag-Ersteller hinzufügen“ eine IAM-Rolle oder einen IAM-Benutzer aus, der über die erforderlichen Berechtigungen zum Erstellen von LF-Tags verfügt.
4. Kontrollkästchen „Berechtigung aktivieren“. Create LF-Tag
5. (Optional) Wählen Sie Grantable Permission aus, um den ausgewählten Prinzipalen die Create LF-Tag Erlaubnis zu erteilen. Create LF-Tag
6. Wählen Sie Hinzufügen aus.

## AWS CLI

```
aws lakeformation grant-permissions --cli-input-json file://grantCreate
{
 "Principal": {
 "DataLakePrincipalIdentifier": "arn:aws:iam::123456789012:user/tag-manager"
 },
 "Resource": {
```

```

 "Catalog": {}
 },
 "Permissions": [
 "CreateLFTag"
],
 "PermissionsWithGrantOption": [
 "CreateLFTag"
]
}

```

Die folgenden Berechtigungen sind für eine LF-Tag-Ersteller-Rolle verfügbar:

| Berechtigung                 | Description                                                                                                                                                                                                                                               |
|------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Drop                         | Ein Principal mit dieser Berechtigung für ein LF-Tag kann ein LF-Tag aus dem Data Lake löschen. Der Principal erhält implizite Describe Berechtigungen für alle Tag-Werte einer LF-Tag-Ressource.                                                         |
| Alter                        | Ein Principal mit dieser Berechtigung für ein LF-Tag kann einem LF-Tag Tag-Wert hinzufügen oder daraus entfernen. Der Principal erhält implizite Alter Berechtigungen für alle Tag-Werte eines LF-Tags.                                                   |
| Describe                     | Ein Principal mit dieser Berechtigung für ein LF-Tag kann das LF-Tag und seine Werte einsehen, wenn er Ressourcen LF-Tags zuweist oder Berechtigungen für LF-Tags erteilt. Sie können für alle Schlüsselwerte oder für bestimmte Werte gewähren Describe. |
| Associate                    | Ein Principal mit dieser Berechtigung für ein LF-Tag kann das LF-Tag einer Datenkatalogressource zuweisen. Implizite Gewährung von Zuschüssen. Associate Describe                                                                                         |
| Grant with LF-Tag expression | Ein Principal mit dieser Berechtigung für ein LF-Tag kann mithilfe des LF-Tag-Schlüssels und der LF-Tag-Werte Berechtigungen für Datenkatalogressourcen gewähren. Implizite Gewährung von Zuschüssen. Grant with LF-Tag expression Describe               |

Diese Genehmigungen sind erteilbar. Ein Principal, dem diese Berechtigungen mit der Grant-Option erteilt wurden, kann sie anderen Prinzipalen gewähren.

## LF-Tags erstellen

Alle LF-Tags müssen in Lake Formation definiert werden, bevor sie verwendet werden können. Ein LF-Tag besteht aus einem Schlüssel und einem oder mehreren möglichen Werten für den Schlüssel.

Nachdem der Data Lake-Administrator die erforderlichen IAM-Berechtigungen und Lake Formation Formation-Berechtigungen für die Rolle LF-Tag-Ersteller eingerichtet hat, kann der Principal ein LF-Tag erstellen. Der LF-Tag-Ersteller erhält die implizite Erlaubnis, jeden Tag-Wert aus dem LF-Tag zu aktualisieren oder zu entfernen und das LF-Tag zu löschen.

Sie können LF-Tags mithilfe der AWS Lake Formation Konsole, der API oder der () erstellen. AWS Command Line Interface AWS CLI

## Console

Um ein LF-Tag zu erstellen

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

Melden Sie sich als Principal mit LF-Tag-Erstellerberechtigungen oder als Data Lake-Administrator an.

2. Wählen Sie im Navigationsbereich unter Berechtigungen, LF-Tags und Berechtigungen die Option LF-Tags aus.

Die Seite mit den LF-Tags wird angezeigt.

**LF-Tags (2)** Delete Edit Grant permissions Add LF-Tag

LF-Tags have a key and one or more values that can be associated with Data Catalog resources. [Learn more](#)

|                       | Key        | Values           | Owner account ID | LF-Tag permissions   |
|-----------------------|------------|------------------|------------------|----------------------|
| <input type="radio"/> | test       | 111              |                  | <a href="#">View</a> |
| <input type="radio"/> | Department | Sales, Marketing |                  | <a href="#">View</a> |

3. Wählen Sie „LF-Tag hinzufügen“.



4. Geben Sie im Dialogfeld „LF-Tag hinzufügen“ einen Schlüssel und einen oder mehrere Werte ein.

Jeder Schlüssel muss mindestens einen Wert haben. Um mehrere Werte einzugeben, geben Sie entweder eine durch Kommas getrennte Liste ein und drücken Sie dann die **EINGABETASTE**, oder geben Sie jeweils einen Wert ein und wählen Sie nach jedem Wert die Option Hinzufügen. Die maximal zulässige Anzahl von Werten ist 1000.

5. Wählen Sie Add tag.

## AWS CLI

Um ein LF-Tag zu erstellen

- Geben Sie einen Befehl `create-lf-tag`.

Im folgenden Beispiel wird ein LF-Tag mit Schlüssel `module` und Werten `Customers` und `Orders` erstellt.

```
aws lakeformation create-lf-tag --tag-key module --tag-values Customers Orders
```

Als Tag-Ersteller erhält der Principal die `Alter` Erlaubnis für dieses LF-Tag und kann jeden Tag-Wert aus diesem LF-Tag aktualisieren oder entfernen. Der Principal, der das LF-Tag erstellt, kann auch einem anderen Prinzipal die `Alter` Erlaubnis erteilen, Tag-Werte auf diesem LF-Tag zu aktualisieren und zu entfernen.

LF-Tags werden aktualisiert

Sie aktualisieren ein LF-Tag, für das Sie `Alter` berechtigt sind, indem Sie zulässige Schlüsselwerte hinzufügen oder löschen. Sie können den LF-Tag-Schlüssel nicht ändern. Um den Schlüssel zu ändern, löschen Sie den LF-Tag und fügen Sie einen mit dem erforderlichen Schlüssel hinzu. Zusätzlich zur `Alter` Berechtigung benötigen Sie auch die `lakeformation:UpdateLFTag` IAM-Berechtigung, um Werte zu aktualisieren.

Wenn Sie einen LF-Tag-Wert löschen, wird nicht geprüft, ob dieser LF-Tag-Wert in einer Datenkatalogressource vorhanden ist. Wenn der gelöschte LF-Tag-Wert mit einer Ressource verknüpft ist, ist er für die Ressource nicht mehr sichtbar, und alle Prinzipale, denen Berechtigungen für dieses Schlüssel-Wert-Paar erteilt wurden, verfügen nicht mehr über diese Berechtigungen.

Bevor Sie einen LF-Tag-Wert löschen, können Sie optional den [remove-lf-tags-from-resource](#) Befehlsbefehl verwenden, um das LF-Tag aus den Datenkatalogressourcen zu entfernen, die den Wert haben, den Sie löschen möchten, und dann die Ressource mit den Werten, die Sie behalten möchten, erneut taggen.

Nur Data Lake-Administratoren, der Ersteller des LF-Tags und Principals, die über `Alter` Berechtigungen für das LF-Tag verfügen, können ein LF-Tag aktualisieren.

Sie können ein LF-Tag mithilfe der AWS Lake Formation Konsole, der API oder der () aktualisieren.  
AWS Command Line Interface AWS CLI

## Console

Um ein LF-Tag (Konsole) zu aktualisieren

1. Öffnen Sie die Lake Formation Konsole unter <https://console.aws.amazon.com/lakeformation/>.

Melden Sie sich als Data Lake-Administrator, LF-Tag-Ersteller oder Principal mit entsprechenden `Alter` Berechtigungen für das LF-Tag an.

2. Wählen Sie im Navigationsbereich unter Berechtigungen, LF-Tags und Berechtigungen die Option LF-Tags aus.
3. Wählen Sie auf der Seite LF-Tags ein LF-Tag aus und klicken Sie dann auf Bearbeiten.
4. Fügen Sie im Dialogfeld „LF-Tag bearbeiten“ LF-Tag-Werte hinzu oder entfernen Sie sie.

Um mehrere Werte hinzuzufügen, geben Sie im Feld Werte entweder eine kommasetrennte Liste ein und drücken Sie die Eingabetaste, oder geben Sie jeweils einen Wert ein oder wählen Sie nach jedem Wert die Option Hinzufügen.

5. Wählen Sie Speichern.

## AWS CLI

Um ein LF-Tag () zu aktualisieren AWS CLI

- Geben Sie einen Befehl `update-lf-tag`. Geben Sie eines oder beide der folgenden Argumente an:
  - `--tag-values-to-add`
  - `--tag-values-to-delete`

## Example

Im folgenden Beispiel wird der Wert `vp` durch den Wert `vice-president` für den LF-Tag-Schlüssel ersetzt. `level`

```
aws lakeformation update-lf-tag --tag-key level --tag-values-to-add vice-president
--tag-values-to-delete vp
```

## LF-Tags löschen

Sie können LF-Tags löschen, die nicht mehr verwendet werden. Es wird nicht geprüft, ob das LF-Tag in einer Datenkatalogressource vorhanden ist. Wenn das gelöschte LF-Tag mit einer Ressource verknüpft ist, ist es für die Ressource nicht mehr sichtbar, und alle Prinzipale, denen Berechtigungen für dieses LF-Tag erteilt wurden, verfügen nicht mehr über diese Berechtigungen.

Bevor Sie ein LF-Tag löschen, können Sie optional den [remove-lf-tags-from-resource](#) Befehl verwenden, um das LF-Tag aus allen Ressourcen zu entfernen.

Nur Data Lake-Administratoren, der Ersteller des LF-Tags oder ein Principal, der über Drop Berechtigungen für das LF-Tag verfügt, können ein LF-Tag löschen. Zusätzlich zur Berechtigung benötigt der Principal auch eine `Drop lakeformation:DeleteLFTag` IAM-Berechtigung, um ein LF-Tag zu löschen.

Sie können ein LF-Tag mithilfe der AWS Lake Formation Konsole, der API oder der () löschen. AWS Command Line Interface AWS CLI

## Console

Um ein LF-Tag (Konsole) zu löschen

1. Öffnen Sie die Lake Formation Konsole unter <https://console.aws.amazon.com/lakeformation/>.

Melden Sie sich als Data Lake-Administrator an.

2. Wählen Sie im Navigationsbereich unter Berechtigungen, LF-Tags und Berechtigungen die Option LF-Tags aus.
3. Wählen Sie auf der Seite LF-Tags ein LF-Tag aus und klicken Sie dann auf Löschen.
4. In der Umgebung „Tag löschen“? Um den Löschvorgang zu bestätigen, geben Sie den LF-Tag-Schlüsselwert in das dafür vorgesehene Feld ein und wählen Sie dann Löschen aus.

## AWS CLI

Um ein LF-Tag zu löschen ( )AWS CLI

- Geben Sie einen Befehl `delete-lf-tag`. Geben Sie den Schlüssel des zu löschenden LF-Tags ein.

### Example

Im folgenden Beispiel wird das LF-Tag mit dem Schlüssel gelöscht. `region`

```
aws lakeformation delete-lf-tag --tag-key region
```

## LF-Tags auflisten

Sie können die LF-Tags auflisten, für die Sie die `Describe` oder `Associate` Berechtigungen haben. Die Werte, die mit jedem LF-Tag-Schlüssel aufgeführt sind, sind die Werte, für die Sie berechtigt sind.

Der LF-Tag-Ersteller hat implizite Berechtigungen, um die von ihm erstellten LF-Tags zu sehen.

Data Lake-Administratoren können alle LF-Tags sehen, die im lokalen AWS Konto definiert sind, sowie alle LF-Tags, für die dem lokalen Konto die `Describe` und `Associate` -Berechtigungen von externen Konten erteilt wurden. Der Data Lake-Administrator kann alle Werte für alle LF-Tags sehen.

Sie können LF-Tags mithilfe der AWS Lake Formation Konsole, der API oder der ( ) auflisten. AWS Command Line Interface AWS CLI

### Console

Um LF-Tags aufzulisten (Konsole)

1. Öffnen Sie die Lake Formation Konsole unter <https://console.aws.amazon.com/lakeformation/>.

Melden Sie sich als Ersteller des LF-Tags, als Data Lake-Administrator oder als Principal an, dem Berechtigungen für LF-Tags erteilt wurden und der über die IAM-Berechtigung `lakeformation:ListLFTags` verfügt.

2. Wählen Sie im Navigationsbereich unter Berechtigungen, LF-Tags und Berechtigungen die Option LF-Tags aus.

Die Seite mit den LF-Tags wird angezeigt.

**LF-Tags** | LF-Tag expressions - new | LF-Tag permissions | LF-Tag creators

**LF-Tags (2)** Delete Edit Grant permissions Add LF-Tag

LF-Tags have a key and one or more values that can be associated with Data Catalog resources. [Learn more](#)

< 1 > ⚙

|                       | Key        | Values           | Owner account ID | LF-Tag permissions   |
|-----------------------|------------|------------------|------------------|----------------------|
| <input type="radio"/> | test       | 111              |                  | <a href="#">View</a> |
| <input type="radio"/> | Department | Sales, Marketing |                  | <a href="#">View</a> |

In der Spalte mit der ID des Eigentümerkontos können Sie die LF-Tags ermitteln, die von einem externen Konto aus mit Ihrem Konto geteilt wurden.

## AWS CLI

Um LF-Tags aufzulisten (AWS CLI)

- Führen Sie den folgenden Befehl als Data Lake-Administrator oder als Principal aus, dem Berechtigungen für LF-Tags erteilt wurden und der über die IAM-Berechtigung verfügt.  
`lakeformation:ListLFTags`

```
aws lakeformation list-lf-tags
```

Die Ausgabe sieht folgendermaßen oder ähnlich aus.

```
{
 "LFTags": [
 {
 "CatalogId": "111122223333",
 "TagKey": "level",
 "TagValues": [
 "director",
 "vp",
 "c-level"
]
 },
 {
```

```

 "CatalogId": "111122223333",
 "TagKey": "module",
 "TagValues": [
 "Orders",
 "Sales",
 "Customers"
]
 }
]
}

```

Um auch LF-Tags zu sehen, die von externen Konten gewährt wurden, fügen Sie die Befehlsoption hinzu. `--resource-share-type ALL`

```
aws lakeformation list-lf-tags --resource-share-type ALL
```

Die Ausgabe sieht folgendermaßen oder ähnlich aus. Beachten Sie den `NextToken` Schlüssel, der darauf hinweist, dass es noch mehr aufzulisten gibt.

```

{
 "LFTags": [
 {
 "CatalogId": "111122223333",
 "TagKey": "level",
 "TagValues": [
 "director",
 "vp",
 "c-level"
]
 },
 {
 "CatalogId": "111122223333",
 "TagKey": "module",
 "TagValues": [
 "Orders",
 "Sales",
 "Customers"
]
 }
],
 "NextToken": "eyJleHBpcmF0aW...ZXh0Ijp0cnVlfQ=="
}

```

```
}
```

Wiederholen Sie den Befehl und fügen Sie das `--next-token` Argument hinzu, um alle verbleibenden lokalen LF-Tags und LF-Tags anzuzeigen, die von externen Konten vergeben wurden. LF-Tags von externen Konten befinden sich immer auf einer separaten Seite.

```
aws lakeformation list-lf-tags --resource-share-type ALL
--next-token eyJleHBpcmF0aW...ZXh0Ijp0cnVlfQ==
```

```
{
 "LFTags": [
 {
 "CatalogId": "123456789012",
 "TagKey": "region",
 "TagValues": [
 "central",
 "south"
]
 }
]
}
```

## API

Sie können die für Lake Formation SDKs verfügbaren Tags verwenden, um die Tags aufzulisten, zu deren Anzeige der Anforderer berechtigt ist.

```
import boto3

client = boto3.client('lakeformation')
...

response = client.list_lf_tags(
 CatalogId='string',
 ResourceShareType='ALL',
 MaxResults=50'
)
```

Dieser Befehl gibt ein `dict` Objekt mit der folgenden Struktur zurück:

```
{
 'LFTags': [
 {
 'CatalogId': 'string',
 'TagKey': 'string',
 'TagValues': [
 'string',
]
 },
],
 'NextToken': 'string'
}
```

Weitere Informationen zu den erforderlichen Berechtigungen finden Sie unter [Referenz zu Personas und IAM-Berechtigungen in Lake Formation](#).

### Zuweisen von LF-Tags zu Datenkatalogressourcen

Sie können Datenkatalogressourcen (Datenbanken, Tabellen und Spalten) LF-Tags zuweisen, um den Zugriff auf diese Ressourcen zu kontrollieren. Nur Prinzipale, denen passende LF-Tags gewährt wurden (und Prinzipale, denen Zugriff mit der benannten Ressourcenmethode gewährt wurde), können auf die Ressourcen zugreifen.

Wenn eine Tabelle ein LF-Tag von einer Datenbank erbt oder eine Spalte ein LF-Tag von einer Tabelle erbt, können Sie den geerbten Wert überschreiben, indem Sie dem LF-Tag-Schlüssel einen neuen Wert zuweisen.

Die maximale Anzahl von LF-Tags, die Sie einer Ressource zuweisen können, ist 50.

### Themen

- [Anforderungen für die Verwaltung von Tags, die Ressourcen zugewiesen sind](#)
- [Weisen Sie einer Tabellenspalte LF-Tags zu](#)
- [Weisen Sie einer Datenkatalogressource LF-Tags zu](#)
- [LF-Tags für eine Ressource aktualisieren](#)
- [LF-Tag aus einer Ressource entfernen](#)

Anforderungen für die Verwaltung von Tags, die Ressourcen zugewiesen sind

Um einer Datenkatalogressource ein LF-Tag zuzuweisen, müssen Sie:



- Habe die Lake Formation ASSOCIATE Formation-Genehmigung auf dem LF-Tag.
- Habe die IAM-Erlaubnis `lakeformation:AddLFTagsToResource`.
- Habe die Glue: `GetDatabase` -Erlaubnis für eine Glue-Datenbank.
- Seien Sie der Eigentümer (Ersteller) der Ressource, verfügen Sie über die Super Lake Formation Formation-Berechtigung für die Ressource mit der GRANT Option oder verfügen Sie über die folgenden Berechtigungen mit der GRANT Option:
  - Für Datenbanken im selben AWS Konto: `DESCRIBE`, `CREATE_TABLE`, `ALTER`, und `DROP`
  - Für Datenbanken in einem externen Konto: `DESCRIBE`, `CREATE_TABLE` und `ALTER`
  - Für Tabellen (und Spalten): `DESCRIBE`, `ALTER`, `DROP`, `INSERT`, `SELECT`, und `DELETE`

Außerdem müssen sich das LF-Tag und die Ressource, der es zugewiesen wird, im selben AWS Konto befinden.

Um ein LF-Tag aus einer Datenkatalogressource zu entfernen, müssen Sie diese Anforderungen erfüllen und außerdem über die IAM-Berechtigung verfügen.

`lakeformation:RemoveLFTagsFromResource`

Weisen Sie einer Tabellenspalte LF-Tags zu

Um einer Tabellenspalte LF-Tags zuzuweisen (Konsole)

1. Öffnen Sie die Lake Formation Konsole unter <https://console.aws.amazon.com/lakeformation/>.

Melden Sie sich als Benutzer an, der die oben aufgeführten Anforderungen erfüllt.

2. Wählen Sie im Navigationsbereich Tables (Tabellen) aus.
3. Wählen Sie einen Tabellennamen (nicht das Optionsfeld neben dem Tabellennamen).
4. Wählen Sie auf der Seite mit den Tabellendetails im Abschnitt Schema die Option Schema bearbeiten aus.
5. Wählen Sie auf der Seite Schema bearbeiten eine oder mehrere Spalten aus und wählen Sie dann LF-Tags bearbeiten aus.

 Note

Wenn Sie Spalten hinzufügen oder löschen und eine neue Version speichern möchten, tun Sie dies zuerst. Bearbeiten Sie dann die LF-Tags.

Das Dialogfeld LF-Tags bearbeiten wird angezeigt, in dem alle LF-Tags angezeigt werden, die aus der Tabelle übernommen wurden.

**Edit LF-Tags: product\_id** [Learn More](#)

**LF-Tags**

After they are associated with catalog resources, LF-Tags allow you to create scalable permissions.

| Inherited keys                      | Values                 |
|-------------------------------------|------------------------|
| <input type="text" value="level"/>  | director (inherited) ▼ |
| <input type="text" value="module"/> | Orders (inherited) ▼   |

[Assign new LF-Tag](#)

You can add 50 more tags.

[Cancel](#) [Save](#)

- (Optional) Wählen Sie in der Werteliste neben dem Feld Geerbte Schlüssel einen Wert aus, um den geerbten Wert zu überschreiben.
- (Optional) Wählen Sie „Neues LF-Tag zuweisen“. Wählen Sie dann für Zugewiesene Schlüssel einen Schlüssel und für Werte einen Wert für den Schlüssel aus.

## Edit LF-Tags: product\_id [Learn More](#)

### LF-Tags

After they are associated with catalog resources, LF-Tags allow you to create scalable permissions.

#### Inherited keys

#### Values

#### Assigned keys

You can add 49 more tags.

#### Values

8. (Optional) Wählen Sie erneut Neues LF-Tag zuweisen, um ein weiteres LF-Tag hinzuzufügen.
9. Wählen Sie Speichern.

Weisen Sie einer Datenkatalogressource LF-Tags zu

## Console

Um einer Datenkatalog-Datenbank oder -Tabelle LF-Tags zuzuweisen

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

Melden Sie sich als Benutzer an, der die oben aufgeführten Anforderungen erfüllt.

2. Führen Sie im Navigationsbereich unter Datenkatalog eine der folgenden Aktionen aus:
  - Um Datenbanken LF-Tags zuzuweisen, wählen Sie Datenbanken.
  - Um Tabellen LF-Tags zuzuweisen, wählen Sie Tabellen.

3. Wählen Sie eine Datenbank oder Tabelle aus und klicken Sie im Menü Aktionen auf LF-Tags bearbeiten.

Das Dialogfeld LF-Tags bearbeiten: **resource-name** wird angezeigt.

Wenn eine Tabelle LF-Tags von der Datenbank erbt, die sie enthält, zeigt das Fenster die geerbten LF-Tags an. Andernfalls wird der Text „Der Ressource sind keine geerbten LF-Tags zugeordnet“ angezeigt.

**Edit LF-Tags: inventory**
[Learn More](#)

✕

**LF-Tags**

After they are associated with catalog resources, LF-Tags allow you to create scalable permissions.

**Inherited keys**

Q level

**Values**

director (inherited) ▼

---

**Assigned keys**

Q module ✕

**Assign new LF-Tag**

You can add 49 more tags.

**Values**

Enter LF-Tag value
▲

Orders

Sales

Customers

**Remove**

Cancel

Save

4. (Optional) Wenn eine Tabelle LF-Tags geerbt hat, können Sie für die Werteliste neben dem Feld Geerbte Schlüssel einen Wert auswählen, der den geerbten Wert überschreibt.
5. Gehen Sie wie folgt vor, um neue LF-Tags zuzuweisen:
  - a. Wählen Sie Neues LF-Tag zuweisen.
  - b. Wählen Sie im Feld Zugewiesene Schlüssel einen LF-Tag-Schlüssel und im Feld Werte einen Wert aus.
  - c. (Optional) Wählen Sie erneut Neues LF-Tag zuweisen, um ein zusätzliches LF-Tag zuzuweisen.
6. Wählen Sie Speichern.

## AWS CLI

Um einer Datenkatalogressource LF-Tags zuzuweisen

- Führen Sie den Befehl `add-lf-tags-to-resource` aus.

Im folgenden Beispiel wird der Tabelle in der Datenbank das LF-Tag `module=orders` zugewiesen. `orders` `erp` Es verwendet die Shortcut-Syntax für das Argument. `--lf-tags` Die `CatalogID` Eigenschaft für `--lf-tags` ist optional. Falls nicht angegeben, wird die Katalog-ID der Ressource (in diesem Fall der Tabelle) angenommen.

```
aws lakeformation add-lf-tags-to-resource --resource '{ "Table":
 {"DatabaseName":"erp", "Name":"orders"}}' --lf-tags
CatalogId=111122223333,TagKey=module,TagValues=orders
```

Das Folgende ist die Ausgabe, wenn der Befehl erfolgreich ist.

```
{
 "Failures": []
}
```

Im nächsten Beispiel werden der `sales` Tabelle zwei LF-Tags zugewiesen und die JSON-Syntax für das Argument verwendet. `--lf-tags`

```
aws lakeformation add-lf-tags-to-resource --resource '{ "Table":
 {"DatabaseName":"erp", "Name":"sales"}}' --lf-tags '[{"TagKey":
 "module","TagValues": ["sales"]},{ "TagKey": "environment","TagValues":
 ["development"]}]'
```

Im nächsten Beispiel wird der Spalte der Tabelle das LF-Tag `level=director` zugewiesen. `total sales`

```
aws lakeformation add-lf-tags-to-resource --resource '{ "TableWithColumns":
 {"DatabaseName":"erp", "Name":"sales", "ColumnNames":["total"]}}' --lf-tags
TagKey=level,TagValues=director
```

## LF-Tags für eine Ressource aktualisieren

Um ein LF-Tag für eine Datenkatalogressource zu aktualisieren (AWS CLI)

- Verwenden Sie den `add-lf-tags-to-resource` Befehl, wie im vorherigen Verfahren beschrieben.

Wenn Sie ein LF-Tag mit demselben Schlüssel wie ein vorhandenes LF-Tag hinzufügen, jedoch mit einem anderen Wert, wird der vorhandene Wert aktualisiert.

## LF-Tag aus einer Ressource entfernen

Um ein LF-Tag für eine Datenkatalogressource zu entfernen (AWS CLI)

- Führen Sie den Befehl `remove-lf-tags-from-resource` aus.

Wenn eine Tabelle einen LF-Tag-Wert hat, der den Wert überschreibt, der von der übergeordneten Datenbank übernommen wurde, wird durch das Entfernen dieses LF-Tags aus der Tabelle der geerbte Wert wiederhergestellt. Dieses Verhalten gilt auch für eine Spalte, die aus der Tabelle übernommene Schlüsselwerte überschreibt.

Im folgenden Beispiel wird das LF-Tag `level=director` aus der `total` Spalte der Tabelle entfernt. `sales` Die `CatalogID` Eigenschaft für `--lf-tags` ist optional. Falls nicht angegeben, wird die Katalog-ID der Ressource (in diesem Fall der Tabelle) angenommen.

```
aws lakeformation remove-lf-tags-from-resource
--resource ' { "TableWithColumns":
{ "DatabaseName": "erp", "Name": "sales", "ColumnNames": ["total"] } }'
--lf-tags CatalogId=111122223333,TagKey=level,TagValues=director
```

## LF-Tags anzeigen, die einer Ressource zugewiesen sind

Sie können die LF-Tags anzeigen, die einer Datenkatalogressource zugewiesen sind. Sie müssen über die `ASSOCIATE` Berechtigung `DESCRIBE` oder für ein LF-Tag verfügen, um es anzeigen zu können.

## Console

Um die LF-Tags anzuzeigen, die einer Ressource (Konsole) zugewiesen sind

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

Melden Sie sich als Data Lake-Administrator, Ressourcenbesitzer oder als Benutzer an, dem Lake Formation Formation-Berechtigungen für die Ressource erteilt wurden.

2. Führen Sie im Navigationsbereich unter der Überschrift Datenkatalog einen der folgenden Schritte aus:
  - Um LF-Tags anzuzeigen, die einer Datenbank zugewiesen sind, wählen Sie Datenbanken.
  - Um die einer Tabelle zugewiesenen LF-Tags anzuzeigen, wählen Sie Tabellen.
3. Wählen Sie auf der Seite „Tabellen“ oder „Datenbanken“ den Namen der Datenbank oder Tabelle aus. Scrollen Sie dann auf der Detailseite nach unten zum Abschnitt LF-Tags.

Der folgende Screenshot zeigt die LF-Tags, die einer customers Tabelle zugewiesen sind, die in der Datenbank enthalten ist. retail Das module LF-Tag wird von der Datenbank vererbt. Der credit\_limit Spalte ist das level=vp LF-Tag zugewiesen.

### LF-Tags (3)

Edit tags

LF-Tags are key-value pairs that you can assign to data catalog resources, such as databases, tables, and columns. You can then grant permissions to principals based on these tags to control access to the resources. Table columns inherit all LF-Tags that are assigned to the table. [Learn More](#)

Find tags

< 1 > ⚙

| Resource ▲            | Key ▼       | Value ▼    | Inherited from |
|-----------------------|-------------|------------|----------------|
| customers (table)     | module      | Customers  | retail         |
| customers (table)     | environment | Production | -              |
| credit_limit (column) | level       | vp         | -              |

## AWS CLI

Um die LF-Tags anzuzeigen, die einer Ressource zugewiesen sind ()AWS CLI

- Verwenden Sie einen Befehl ähnlich dem folgenden.

```
aws lakeformation get-resource-lf-tags --show-assigned-lf-tags --
resource '{ "Table": {"CatalogId":"111122223333", "DatabaseName":"erp",
"Name":"sales"}}'
```

Der Befehl gibt die folgende Ausgabe zurück.

```
{
 "TableTags": [
 {
 "CatalogId": "111122223333",
 "TagKey": "module",
 "TagValues": [
 "sales"
]
 },
 {
 "CatalogId": "111122223333",
 "TagKey": "environment",
 "TagValues": [
 "development"
]
 }
],
 "ColumnTags": [
 {
 "Name": "total",
 "Tags": [
 {
 "CatalogId": "111122223333",
 "TagKey": "level",
 "TagValues": [
 "director"
]
 }
]
 }
]
}
```



```
}
```

In dieser Ausgabe werden nur LF-Tags angezeigt, die explizit zugewiesen und nicht vererbt wurden. Wenn Sie alle LF-Tags in allen Spalten sehen möchten, einschließlich geerbter LF-Tags, lassen Sie die Option weg. `--show-assigned-lf-tags`

Die Ressourcen anzeigen, denen ein LF-Tag zugewiesen ist

Sie können alle Datenkatalogressourcen anzeigen, denen ein bestimmter LF-Tag-Schlüssel zugewiesen ist. Dazu benötigen Sie die folgenden Lake Formation Formation-Berechtigungen:

- `Describeoder Associate` auf dem LF-Tag.
- `Describeoder jede andere Genehmigung` von Lake Formation für die Ressource.

Darüber hinaus benötigen Sie die folgenden AWS Identity and Access Management (IAM-) Berechtigungen:

- `lakeformation:SearchDatabasesByLFTags`
- `lakeformation:SearchTablesByLFTags`

## Console

Um die Ressourcen anzusehen, denen ein LF-Tag zugewiesen ist (Konsole)

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

Melden Sie sich als Data Lake-Administrator oder als Benutzer an, der die oben aufgeführten Anforderungen erfüllt.

2. Wählen Sie im Navigationsbereich unter Berechtigungen und LF-Tags und Berechtigungen die Option LF-Tags aus.
3. Wählen Sie einen LF-Tag-Schlüssel (nicht das Optionsfeld neben dem Schlüsselnamen).

Auf der LF-Tag-Detailseite wird eine Liste der Ressourcen angezeigt, denen das LF-Tag zugewiesen wurde.

# module

LF-Tag

Delete

Edit

Key

module

Values

Orders, Sales, Customers

Associated data catalog resources (12)

Q Find resource

| Key    | Values ▾  | Resource type ▾ | Resource ▾                                  |
|--------|-----------|-----------------|---------------------------------------------|
| module | Customers | DATABASE        | <a href="#">retail</a>                      |
| module | Customers | TABLE           | <a href="#">customers</a>                   |
| module | Orders    | TABLE           | <a href="#">inventory</a>                   |
| module | Customers | COLUMN          | <a href="#">customers.cust_first_name</a>   |
| module | Customers | COLUMN          | <a href="#">customers.work_phone_number</a> |
| module | Customers | COLUMN          | <a href="#">customers.company_name</a>      |
| module | Customers | COLUMN          | <a href="#">customers.credit_limit</a>      |

## AWS CLI

Um die Ressourcen anzuzeigen, denen ein LF-Tag zugewiesen ist

- Führen Sie den Befehl `search-tables-by-lf-tags` oder `search-databases-by-lf-tags` aus.

## Example

Das folgende Beispiel listet Tabellen und Spalten auf, denen das `level=vp` LF-Tag zugewiesen wurde. Für jede aufgelistete Tabelle und Spalte werden alle zugewiesenen LF-Tags für die Tabelle oder Spalte ausgegeben, nicht nur der Suchausdruck.

```
aws lakeformation search-tables-by-lf-tags --expression
TagKey=level,TagValues=vp
```

Weitere Informationen zu den erforderlichen Berechtigungen finden Sie unter [Referenz zu Personas und IAM-Berechtigungen in Lake Formation](#).

### Lebenszyklus eines LF-Tags

1. Der LF-Tag-Schöpfer Michael erstellt einen LF-Tag. `module=Customers`
2. Michael vergibt den LF-Tag Associate an den Dateningenieur Eduardo. Implizite Gewährung von `ZuschüssenAssociate.Describe`
3. Michael gewährt Eduardo mit der Grant-Option `Super` auf dem `TischCusts`, sodass Eduardo der Tabelle LF-Tags zuweisen kann. Weitere Informationen finden Sie unter [Zuweisen von LF-Tags zu Datenkatalogressourcen](#).
4. Eduardo weist der Tabelle den LF-Tag zu. `module=customers Custs`
5. Michael gewährt der Dateningenieurin Sandra den folgenden Zuschuss (in Pseudocode).

```
GRANT (SELECT, INSERT ON TABLES) ON TAGS module=customers TO Sandra WITH GRANT OPTION
```

6. Sandra gewährt der Datenanalystin Maria den folgenden Zuschuss.

```
GRANT (SELECT ON TABLES) ON TAGS module=customers TO Maria
```

Maria kann jetzt Abfragen für die `Custs` Tabelle ausführen.

 Weitere Informationen finden Sie auch unter

- [Zugriffskontrolle für Metadaten](#)

## Vergleich der Tag-basierten Zugriffskontrolle von Lake Formation mit der attributbasierten IAM-Zugriffskontrolle

Die attributbasierte Zugriffskontrolle (ABAC) ist eine Autorisierungsstrategie, bei der Berechtigungen basierend auf Attributen definiert werden. In werden diese AWS Attribute als Tags bezeichnet. Sie können Tags an IAM-Ressourcen, einschließlich IAM-Entitäten (Benutzer oder Rollen), und an AWS Ressourcen anhängen. Sie können eine einzelne ABAC-Richtlinie oder einen kleinen Richtlinienatz für Ihre IAM-Prinzipale erstellen. Diese ABAC-Richtlinien können so konzipiert werden, dass Operationen zugelassen werden, wenn das Tag des Prinzipals mit dem Ressourcen-Tag übereinstimmt. ABAC ist in Umgebungen hilfreich, die schnell wachsen, und unterstützt Sie in Situationen, in denen die Richtlinienverwaltung mühsam wird.

Cloud-Sicherheits- und Governance-Teams verwenden IAM, um Zugriffsrichtlinien und Sicherheitsberechtigungen für alle Ressourcen zu definieren, einschließlich Amazon S3 S3-Buckets, Amazon EC2 EC2-Instances und allen Ressourcen, auf die Sie mit einem ARN verweisen können. Die IAM-Richtlinien definieren umfassende (grobe) Berechtigungen für Ihre Data Lake-Ressourcen, um beispielsweise den Zugriff auf Amazon S3 S3-Bucket-, Präfix- oder Datenbankebene zuzulassen oder zu verweigern. [Weitere Informationen zu IAM ABAC finden Sie unter Wozu dient ABAC? AWS](#) im IAM-Benutzerhandbuch.

Sie können beispielsweise drei Rollen mit dem Tag-Schlüssel `project-access` erstellen. Legen Sie den Tag-Wert der ersten Rolle auf `Dev`, den zweiten auf `Marketing` und den dritten auf `Support` fest. Weisen Sie Ressourcen Tags mit dem entsprechenden Wert zu. Sie können dann eine einzelne Richtlinie verwenden, die den Zugriff erlaubt, wenn die Rolle und die Ressource mit demselben Wert für `project-access` markiert sind.

Data Governance-Teams verwenden Lake Formation, um detaillierte Berechtigungen für bestimmte Data Lake-Ressourcen zu definieren. LF-Tags werden Datenkatalogressourcen (Datenbanken, Tabellen und Spalten) zugewiesen und an Principals vergeben. Ein Principal mit LF-Tags, die den LF-Tags einer Ressource entsprechen, kann auf diese Ressource zugreifen. Lake Formation Formation-Berechtigungen sind den IAM-Berechtigungen untergeordnet. Wenn IAM-Berechtigungen einem Benutzer beispielsweise keinen Zugriff auf einen Data Lake gewähren, gewährt Lake Formation diesem Benutzer keinen Zugriff auf Ressourcen innerhalb dieses Data Lakes, selbst wenn der Principal und die Ressource übereinstimmende LF-Tags haben.

Lake Formation Tag-Based Access Control (LF-TBAC) arbeitet mit IAM ABAC zusammen, um zusätzliche Berechtigungsebenen für Ihre Lake Formation Formation-Daten und -Ressourcen bereitzustellen.

- Lake Formation TBAC-Genehmigungen skalieren mit Innovation. Es ist nicht mehr notwendig, dass ein Administrator vorhandene Richtlinien aktualisiert, um den Zugriff auf neue Ressourcen zu erlauben. Nehmen wir beispielsweise an, dass Sie eine IAM-ABAC-Strategie mit dem `project-access` Tag verwenden, um Zugriff auf bestimmte Datenbanken innerhalb von Lake Formation zu gewähren. Mithilfe von LF-TBAC `Project=SuperApp` wird das LF-Tag bestimmten Tabellen oder Spalten zugewiesen, und dasselbe LF-Tag wird einem Entwickler für dieses Projekt gewährt. Über IAM kann der Entwickler auf die Datenbank zugreifen, und LF-TBAC-Berechtigungen gewähren dem Entwickler weiteren Zugriff auf bestimmte Tabellen oder Spalten innerhalb von Tabellen. Wenn dem Projekt eine neue Tabelle hinzugefügt wird, muss der Lake Formation-Administrator der neuen Tabelle nur das Tag zuweisen, damit der Entwickler Zugriff auf die Tabelle erhält.
- Lake Formation TBAC erfordert weniger IAM-Richtlinien. Da Sie IAM-Richtlinien verwenden, um umfassenden Zugriff auf Lake Formation-Ressourcen und Lake Formation TBAC für die Verwaltung eines genaueren Datenzugriffs zu gewähren, erstellen Sie weniger IAM-Richtlinien.
- Mit Lake Formation TBAC können sich Teams schnell verändern und wachsen. Der Grund hierfür ist, dass Berechtigungen für neue Ressourcen automatisch basierend auf Attributen erteilt werden. Wenn beispielsweise ein neuer Entwickler dem Projekt beitrifft, ist es einfach, diesem Entwickler Zugriff zu gewähren, indem Sie dem Benutzer die IAM-Rolle zuordnen und ihm dann die erforderlichen LF-Tags zuweisen. Sie müssen die IAM-Richtlinie nicht ändern, um ein neues Projekt zu unterstützen oder neue LF-Tags zu erstellen.
- Mit Lake Formation TBAC sind detailliertere Genehmigungen möglich. IAM-Richtlinien gewähren Zugriff auf Ressourcen der obersten Ebene, wie z. B. Datenkatalogdatenbanken oder Tabellen. Mit Lake Formation TBAC können Sie Zugriff auf bestimmte Tabellen oder Spalten gewähren, die bestimmte Datenwerte enthalten.

#### Note

IAM-Tags sind nicht dasselbe wie LF-Tags. Diese Tags sind nicht austauschbar. LF-Tags werden verwendet, um Lake Formation-Berechtigungen zu gewähren, und IAM-Tags werden verwendet, um IAM-Richtlinien zu definieren.

## Verwaltung von LF-Tag-Ausdrücken für die Zugriffskontrolle auf Metadaten

LF-Tag-Ausdrücke sind logische Ausdrücke, die aus einem oder mehreren LF-Tags (Schlüssel-Wert-Paaren) bestehen und zur Gewährung von Berechtigungen für Ressourcen verwendet werden. AWS Glue Data Catalog Mit LF-Tag-Ausdrücken können Sie Regeln definieren, die den Zugriff auf

Ihre Datenressourcen auf der Grundlage ihrer Metadaten-Tags regeln. Sie können diese Ausdrücke speichern und sie für mehrere Berechtigungszuweisungen wiederverwenden, wodurch Konsistenz gewährleistet ist und Änderungen an der Tag-Ontologie im Laufe der Zeit problemlos verwaltet werden können.

Innerhalb eines bestimmten LF-Tag-Ausdrucks werden die Tag-Schlüssel mithilfe der AND-Operation kombiniert, während die Werte mithilfe der OR-Operation kombiniert werden. Der Tag-Ausdruck `content_type:Sales AND location:US` steht beispielsweise für Ressourcen, die sich auf Verkaufsdaten in den USA beziehen.

Sie können bis zu 1000 LF-Tag-Ausdrücke in einem erstellen. AWS-Konto Diese Ausdrücke bieten eine flexible und skalierbare Methode zur Verwaltung von Berechtigungen auf der Grundlage von Metadaten-Tags und stellen so sicher, dass nur autorisierte Benutzer oder Anwendungen auf der Grundlage der definierten Tag-Regeln auf bestimmte Datenressourcen zugreifen können.

LF-Tag-Ausdrücke bieten die folgenden Vorteile:

- **Wiederverwendbarkeit** — Durch die Definition und Speicherung von LF-Tag-Ausdrücken müssen Sie dieselben Ausdrücke nicht mehr manuell replizieren, wenn Sie anderen Ressourcen oder Prinzipalen Berechtigungen zuweisen.
- **Konsistenz** — Die Wiederverwendung von LF-Tag-Ausdrücken für mehrere Berechtigungsberechtigungen gewährleistet eine einheitliche Art und Weise, wie Berechtigungen erteilt und verwaltet werden.
- **Verwaltung der Tag-Ontologie** — LF-Tag-Ausdrücke helfen dabei, Änderungen an der Tag-Ontologie im Laufe der Zeit zu verwalten, da Sie die gespeicherten Ausdrücke aktualisieren können, anstatt einzelne Berechtigungsberechtigungen zu ändern.

Weitere Informationen zur tagbasierten Zugriffskontrolle finden Sie im. [Tag-basierte Zugangskontrolle von Lake Formation](#)

### Ersteller von LF-Tag-Ausdrücken

Der LF-Tag Expression Creator ist ein Principal, der über die Rechte zum Erstellen und Verwalten von LF-Tag-Ausdrücken verfügt. Data Lake-Administratoren können LF-Tag-Ausdrucksersteller mithilfe der Lake Formation Formation-Konsole, CLI, API oder SDK hinzufügen. Die Ersteller von LF-Tag-Ausdrücken verfügen über implizite Lake Formation Formation-Berechtigungen, um LF-Tag-Ausdrücke zu erstellen, zu aktualisieren und zu löschen und anderen Prinzipalen LF-Tag-Ausdrucksberechtigungen zu gewähren.

Ersteller von LF-Tag-Ausdrücken, die keine Data Lake-Administratoren sind, erhalten implizite, und Berechtigungen nur für Ausdrücke, die sie erstellt Alter haben. Drop Describe Grant with LF-Tag expression

Data Lake-Administratoren können Erstellern von LF-Tag-Ausdrücken auch erteilbare Berechtigungen gewähren. Create LF-Tag expression Anschließend kann der Ersteller von LF-Tag-Ausdrücken anderen Prinzipalen die Erlaubnis zur Erstellung von LF-Tag-Ausdrücken erteilen.

## Themen

- [Für die Erstellung von LF-Tag-Ausdrücken sind IAM-Berechtigungen erforderlich](#)
- [Fügen Sie Ersteller von LF-Tag-Ausdrücken hinzu](#)
- [LF-Tag-Ausdrücke erstellen](#)
- [LF-Tag-Ausdrücke werden aktualisiert](#)
- [LF-Tag-Ausdrücke löschen](#)
- [LF-Tag-Ausdrücke auflisten](#)

 Weitere Informationen finden Sie auch unter

- [Verwaltung von LF-Tag-Wertberechtigungen](#)
- [Erteilen von Data Lake-Berechtigungen mithilfe der LF-TBAC-Methode](#)
- [Tag-basierte Zugangskontrolle von Lake Formation](#)

Für die Erstellung von LF-Tag-Ausdrücken sind IAM-Berechtigungen erforderlich

Sie müssen Berechtigungen konfigurieren, damit ein Lake Formation-Prinzipal LF-Tag-Ausdrücke erstellen kann. Fügen Sie der Berechtigungsrichtlinie für den Prinzipal, der ein LF-Tag-Ausdrucksersteller sein muss, die folgende Anweisung hinzu.

### Note

Data Lake-Administratoren verfügen zwar über implizite Lake Formation Formation-Berechtigungen, um LF-Tags und LF-Tag-Ausdrücke zu erstellen, zu aktualisieren und zu löschen, Ressourcen LF-Tags zuzuweisen und Prinzipalen LF-Tags- und LF-Tag-

Ausdrucksberechtigungen zu gewähren, aber Data Lake-Administratoren benötigen auch die folgenden IAM-Berechtigungen.

Weitere Informationen finden Sie unter [Referenz zu Personas und IAM-Berechtigungen in Lake Formation](#).

```
{
 "Sid": "Transformational",
 "Effect": "Allow",
 "Action": [
 "lakeformation:AddLFTagsToResource",
 "lakeformation:RemoveLFTagsFromResource",
 "lakeformation:GetResourceLFTags",
 "lakeformation:ListLFTags",
 "lakeformation:CreateLFTag",
 "lakeformation:GetLFTag",
 "lakeformation:UpdateLFTag",
 "lakeformation>DeleteLFTag",
 "lakeformation:SearchTablesByLFTags",
 "lakeformation:SearchDatabasesByLFTags",
 "lakeformation:CreateLFTagExpression",
 "lakeformation>DeleteLFTagExpression",
 "lakeformation:UpdateLFTagExpression",
 "lakeformation:GetLFTagExpression",
 "lakeformation:ListLFTagExpressions",
 "lakeformation:GrantPermissions",
 "lakeformation:RevokePermissions",
 "lakeformation:BatchGrantPermissions",
 "lakeformation:BatchRevokePermissions"
]
}
```

Fügen Sie Ersteller von LF-Tag-Ausdrücken hinzu

Die Ersteller von LF-Tag-Ausdrücken können wiederverwendbare LF-Tag-Ausdrücke erstellen und speichern, Tag-Schlüssel und -Werte aktualisieren, Ausdrücke löschen und Prinzipalen mithilfe der LF-TBAC-Methode Berechtigungen für Datenkatalogressourcen gewähren. Der LF-Tag-Ausdrucksersteller kann diese Berechtigungen auch Prinzipalen gewähren.



Sie können Rollen zum Erstellen von LF-Tag-Ausdrücken mithilfe der AWS Lake Formation Konsole, der API oder der () erstellen. AWS Command Line Interface AWS CLI

console

Um einen LF-Tag Expression Creator hinzuzufügen

1. Öffnen Sie die Lake Formation Konsole unter <https://console.aws.amazon.com/lakeformation/>.

Melden Sie sich als Data Lake-Administrator an.

2. Wählen Sie im Navigationsbereich unter Berechtigungen die Option LF-Tags und Berechtigungen aus.
3. Wählen Sie die Registerkarte LF-Tag-Ausdrücke.
4. Wählen Sie im Abschnitt LF-Tag-Ausdrucksersteller die Option LF-Tag-Ausdrucksersteller hinzufügen aus.

## Add LF-Tag expression creators

LF-Tag expression creators can create and manage LF-Tags expressions.

### LF-Tag expression creator details

**IAM users and roles**  
Add IAM users or roles.

Choose IAM principals to add ▼

datalake\_user X

User

**Permission**  
Choose the permission to grant.

☒ Create LF-Tag expression

**Grantable permission**  
Choose the permission that may be granted to others.

☒ Create LF-Tag expression

[Cancel](#)[Add](#)

5. Wählen Sie auf der Seite „Ersteller von LF-Tag-Ausdrücken hinzufügen“ eine IAM-Rolle oder einen IAM-Benutzer aus, der über die erforderlichen Berechtigungen zum Erstellen von LF-Tag-Ausdrücken verfügt.

6. Aktivieren Sie das Kontrollkästchen „Berechtigung“. Create LF-Tag expression
7. (Optional) Damit die ausgewählten Hauptbenutzer den Hauptbenutzern Create LF-Tag expression Berechtigungen erteilen können, wählen Sie „Berechtigung erteilen“ aus. Create LF-Tag expression
8. Wählen Sie Hinzufügen aus.

## AWS CLI

```
aws lakeformation grant-permissions --cli-input-json file://grantCreate
{
 "Principal": {
 "DataLakePrincipalIdentifier": "arn:aws:iam::123456789012:user/tag-manager"
 },
 "Resource": {
 "Catalog": {}
 },
 "Permissions": [
 "CreateLFTagExpression"
],
 "PermissionsWithGrantOption": [
 "CreateLFTagExpression"
]
}
```

Die Rolle „LF-Tag-Ausdrucksersteller“ kann LF-Tag-Ausdrücke erstellen, aktualisieren oder löschen.

| Berechtigung | Description                                                                                                                  |
|--------------|------------------------------------------------------------------------------------------------------------------------------|
| Create       | Ein Principal mit dieser Berechtigung kann LF-Tag-Ausdrücke zum Data Lake hinzufügen.                                        |
| Drop         | Ein Principal mit dieser Berechtigung für einen LF-Tag-Ausdruck kann einen LF-Tag-Ausdruck aus dem Data Lake löschen.        |
| Alter        | Ein Principal mit dieser Berechtigung für einen LF-Tag-Ausdruck kann den Ausdruckstext eines LF-Tag-Ausdrucks aktualisieren. |

| Berechtigung                 | Description                                                                                                                                                                                                                      |
|------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Describe                     | Ein Principal mit dieser Berechtigung für einen LF-Tag-Ausdruck kann den Inhalt eines LF-Tag-Ausdrucks anzeigen.                                                                                                                 |
| Grant with LF-Tag expression | Diese Berechtigung ermöglicht es dem Empfänger, den Tag-Ausdruck als Ressource zu verwenden, wenn er Zugriffsberechtigungen für Daten oder Metadaten erteilt. Grant with LF-Tag expression Implizite Gewährung gewährt Describe. |
| Super                        | Bei LF-Tag-Ausdrücken gewährt die Super Berechtigung die Möglichkeit itDescribe,, AlterDrop, und anderen Prinzipalen Berechtigungen für den Tag-Ausdruck zu gewähren.                                                            |

Diese Berechtigungen sind erteilbar. Ein Principal, dem diese Berechtigungen mit der Grant-Option erteilt wurden, kann sie anderen Prinzipalen gewähren.

## LF-Tag-Ausdrücke erstellen

Sie müssen alle LF-Tags in Lake Formation definieren und sie den Datenkatalogressourcen zuweisen, bevor sie zum Erstellen von Ausdrücken verwendet werden können. Ein LF-Tag-Ausdruck besteht aus einem weiteren Schlüssel und einem oder mehreren möglichen Werten für jeden Schlüssel.

Nachdem der Data Lake-Administrator die erforderlichen IAM-Berechtigungen und Lake Formation Formation-Berechtigungen für die Rolle LF-Tag-Ausdrucksersteller eingerichtet hat, kann der Principal wiederverwendbare LF-Tag-Ausdrücke erstellen. Der LF-Tag-Ausdrucksersteller erhält implizite Berechtigungen, um den Ausdruckstext zu aktualisieren und den LF-Tag-Ausdruck zu löschen.

Sie können LF-Tag-Ausdrücke mithilfe der AWS Lake Formation Konsole, der API oder der () erstellen. AWS Command Line Interface AWS CLI

## Console

Um einen LF-Tag-Ausdruck zu erstellen

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

- Melden Sie sich als Principal mit LF-Tag Expression Creator-Rechten oder als Data Lake-Administrator an.
- Wählen Sie im Navigationsbereich unter Berechtigungen die Option LF-Tags und Berechtigungen aus.
  - Wählen Sie LF-Tag-Ausdrücke. Die Seite „LF-Tag-Ausdrücke hinzufügen“ wird angezeigt.

## Add LF-Tag Expression

LF-Tag expression creators can create and manage LF-Tag expressions

### Expression details

**Name**  
Enter a name that describes the expression. Expression name cannot be edited after creation.

Name must be less than 1000 characters.

**Description - optional**

Description can be up to 2048 characters.

**Expression**  
Choose the keys and values for this expression. When multiple keys are specified, the keys are joined by an AND operator and when multiple values are specified, the values are joined by an OR operator.

**Key**

**Values**

sales

[Add LF-Tag key-value pair](#)

You can add 49 more LF-Tags.

**Expression review**  
The LF-Tag expression above will be interpreted in the following way.

Department = sales

► **Grant permissions - optional**  
Grant permissions to allow others to manage or grant permissions with the expression.

[Cancel](#)[Add](#)

- Geben Sie die folgenden Informationen ein:

- **Name** — Geben Sie einen eindeutigen Namen für den Ausdruck ein. Sie können den Ausdrucksnamen nicht aktualisieren.
- **Beschreibung** — Geben Sie eine optionale Beschreibung für den Ausdruck mit den Details des Ausdrucks ein.
- **Ausdruck** — Erstellen Sie den Ausdruck, indem Sie Tag-Schlüssel und die zugehörigen Werte angeben. Sie können bis zu 50 Schlüssel pro Ausdruck hinzufügen. Sie benötigen die `Grant with LF-Tags` Lake Formation Formation-Erlaubnis für alle Tags im Ausdruckstext.

Jeder Schlüssel muss mindestens einen Wert haben. Um mehrere Werte einzugeben, geben Sie entweder eine durch Kommas getrennte Liste ein und drücken Sie dann die **EINGABETASTE**, oder geben Sie jeweils einen Wert ein und wählen Sie nach jedem Wert die Option **Hinzufügen**. Die maximal zulässige Anzahl von Werten pro Schlüssel ist 1000.

Lake Formation verwendet die **AND/OR** Logik, um mehrere Schlüssel und Werte in einem Ausdruck zu kombinieren. Innerhalb eines einzigen Paares (Schlüssel: Werteliste) werden die Werte mit dem logischen **OR**-Operator kombiniert. Wenn das Paar beispielsweise (Abteilung: [Vertrieb, Marketing]) lautet, bedeutet dies, dass das Tag übereinstimmt, wenn die Ressource das Abteilungs-Tag mit dem Wert Vertrieb ODER Marketing hat.

Wenn Sie mehrere Schlüssel angeben, werden die Schlüssel durch einen logischen **AND**-Operator verknüpft. Wenn der vollständige Ausdruck also (Department: [Sales, Marketing]) **AND** (Location: [US, Kanada]) lautet, entspricht er Ressourcen, die das Department-Tag mit dem Wert Sales **OR** Marketing und auch das Location-Tag mit dem Wert US **OR** Kanada haben. Im Folgenden finden Sie ein weiteres Beispiel mit mehreren Schlüsseln und Werten:

LF-Tag-AusdruckContentype : (: [Video, Audio]) **UND** (Region: [Europa, Asien]) **UND** (Abteilung: [Technik, ProductManagement]).

Dieser Ausdruck würde Ressourcen entsprechen, die: - das Contentype Tag mit dem Wert Video ODER Audio **UND** - das Region-Tag mit dem Wert Europa ODER Asien **UND** - das Department-Tag mit dem Wert Engineering **OR** haben. ProductManagement

Sie können auch einen Tag-Ausdruck speichern, wenn Sie Data Lake-Berechtigungen mithilfe von LF-Tags gewähren. Wählen Sie die Schlüssel- und Wertepaare aus und

wählen Sie die Option Als neuen Ausdruck speichern. Geben Sie einen Namen ein, der den Ausdruck beschreibt.

### LF-Tags or catalog resources

Choose a method to grant permissions.

☒ **Resources matched by LF-Tags (recommended)**  
Manage permissions indirectly for resources or data matched by a specific set of LF-Tags.

☐ **Named Data Catalog resources**  
Manage permissions for specific databases or tables, in addition to fine-grained data access.

☒ LF-Tag key-value pairs

☐ Saved LF-Tag expressions - *new*

**Key**  

Department ▼

**Values**  

Choose LF-Tag values ▼

marketing ✕ sales ✕

Add LF-Tag key-value pair

You can add 49 more LF-Tags.

**Expression review**

The LF-Tag expression above will be interpreted in the following way.

Department = (marketing OR sales)

☒ **Save as new expression**  
Use saved expressions to grant permissions. Create LF-Tag expression permissions are needed.

**New LF-Tag expression name**

Enter a name that describes the expression. Expression name cannot be edited after creation.

General access

Name must be less than 1000 characters.

- (Optional) Wählen Sie als Nächstes die Benutzer/Rollen und die Berechtigungen für den Ausdruck aus, die Sie ihnen im Konto gewähren möchten. Sie können auch erteilbare Berechtigungen auswählen, die es den Benutzern ermöglichen, diese Berechtigungen anderen Benutzern im Konto zu gewähren. Sie können keine kontoübergreifenden Berechtigungen für die Tagausdrücke gewähren.

### ▼ Grant permissions - optional

Grant permissions to allow others to manage or grant permissions with the expression.

#### IAM users and roles

Users or roles from this AWS account.

Choose IAM principals to add

#### Permissions

Choose the specific LF-Tag permissions to grant.

- ☐ **Describe**  
See keys and values.
- ☐ **Alter**  
Update or delete LF-Tag expressions.
- ☐ **Drop**  
Delete LF-Tag expressions.
- ☐ **Grant with LF-Tag expression**  
Allow principals to grant access permissions using LF-Tag expressions.
- ☐ **Super**  
This permission supersedes the individual permissions set above.

#### Grantable permissions

Choose the permissions that the recipient can grant to other principals.

- ☐ **Describe**  
See keys and values.
- ☐ **Alter**  
Update or delete LF-Tag expressions.
- ☐ **Drop**  
Delete LF-Tag expressions.
- ☐ **Grant with LF-Tag expression**  
Allow principals to grant access permissions using LF-Tag expressions.
- ☐ **Super**  
This permission supersedes the individual permissions set above.

Cancel

Add

6. Wählen Sie Hinzufügen aus.

## AWS CLI

Um einen LF-Tag-Ausdruck zu erstellen

- Geben Sie einen Befehl `create-lf-tag-expression`.

Im folgenden Beispiel wird ein LF-Tag-Ausdruck mit dem Tag `Department` mit den Werten `Sales` und `Marketing` dem Tag `Location` mit dem Wert `US` erstellt.

```
aws lakeformation create-lf-tag-expression \
```

```
-- name "my-tag-expression" \
-- catalog-id "123456789012" \
-- expression '{"Expression":[{"TagKey":"Department","TagValues":
["Sales","Marketing"]},{"TagKey":"Location","TagValues":["US"]}]}'
```

Dieser CLI-Befehl erstellt einen neuen LF-Tag-Ausdruck in der AWS Glue Data Catalog. Der Ausdruck kann verwendet werden, um Datenkatalogressourcen wie Datenbanken, Tabellen, Ansichten oder Spalten auf der Grundlage der zugehörigen Tags Berechtigungen zu gewähren. In diesem Beispiel entspricht der Ausdruck Ressourcen, bei denen der Department Schlüssel Werte Sales oder Marketing und der Location Schlüssel der Wert istUS.

Als Ersteller eines Tag-Ausdrucks erhält der Principal die `Alter` Erlaubnis für diesen LF-Tag-Ausdruck und kann den Ausdruck aktualisieren oder entfernen. Der Prinzipal, der den Ausdruck erstellt, kann auch einem anderen Prinzipal die `Alter` Erlaubnis erteilen, diesen Ausdruck zu aktualisieren und zu entfernen.

### LF-Tag-Ausdrücke werden aktualisiert

Nur Data Lake-Administratoren, der Ersteller des LF-Tag-Ausdrucks und Prinzipale, die über `Alter` oder über `Super` Berechtigungen für den LF-Tag-Ausdruck verfügen, können einen LF-Tag-Ausdruck aktualisieren. Zusätzlich zu den `Alter` Berechtigungen benötigen Sie auch die `lakeformation:UpdateLFTagExpression` IAM-Berechtigung und die Erlaubnis für alle zugrunde liegenden Schlüsselwerte im neuen `Grant with LF-Tag Ausdruckstext`, um Ausdrücke zu aktualisieren.

Sie aktualisieren einen LF-Tag-Ausdruck, indem Sie die Beschreibung, den Ausdruckstext und die für den Ausdruck erteilten Berechtigungen aktualisieren. Sie können den Namen des LF-Tag-Ausdrucks nicht ändern. Um den Namen zu ändern, löschen Sie den LF-Tag-Ausdruck und fügen Sie einen mit den erforderlichen Parametern hinzu.

Sie können einen LF-Tag-Ausdruck mithilfe der AWS Lake Formation Konsole, der API oder der () aktualisieren. AWS Command Line Interface AWS CLI



## Console

Um einen LF-Tag-Ausdruck zu aktualisieren

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

Melden Sie sich als Data Lake-Administrator, als Ersteller des LF-Tags oder als Principal mit `Alter` Berechtigungen für das LF-Tag an.

2. Wählen Sie im Navigationsbereich unter Berechtigungen die Option LF-Tags und Berechtigungen aus.
3. Wählen Sie die Registerkarte LF-Tag-Ausdrücke.
4. Wählen Sie im Abschnitt LF-Tag-Ausdrücke einen LF-Tag-Ausdruck aus und klicken Sie dann auf Bearbeiten.
5. Aktualisieren Sie im Dialogfeld „LF-Tag-Ausdruck bearbeiten“ die Beschreibung und den Ausdruckstext, indem Sie Schlüssel und Werte hinzufügen oder entfernen.

Um mehrere Werte hinzuzufügen, wählen Sie im Feld Werte die Werte aus der Dropdownliste aus.

6. Wählen Sie Speichern.

## AWS CLI

Mit dem `update-lf-tag-expression` Befehl in Lake Formation können Sie einen vorhandenen LF-Tag-Ausdruck aktualisieren.

```
aws lakeformation update-lf-tag-expression \
-- name expression_name \
-- description new_description \
-- catalog-id catalog_id \
-- expression '{"Expression": [{"TagKey": "tag_key", "TagValues": ["tag_value1", "tag_value2", ...]}]}'
```

Die Parameter im bereitgestellten Befehl bedeuten Folgendes:

- `name` — Der Name des vorhandenen benannten Tag-Ausdrucks, den Sie aktualisieren möchten.

- **Beschreibung** — Eine neue Beschreibung für den Ausdruck.  
  
catalog-id — Die ID des Datenkatalogs, in dem sich der Ausdruck des benannten Tags befindet.
- **Ausdruck** — Die neue Tag-Ausdruckszeichenfolge, mit der Sie den Ausdruck aktualisieren möchten.

## LF-Tag-Ausdrücke löschen

Sie können LF-Tag-Ausdrücke löschen, die nicht mehr verwendet werden. Wenn Sie Prinzipalen mithilfe des LF-Tag-Ausdrucks Berechtigungen für Datenkatalogressourcen erteilt haben, haben sie diese Rechte nicht mehr.

Nur Data Lake-Administratoren, der Ersteller des LF-Tag-Ausdrucks oder ein Principal mit Drop Berechtigungen für den LF-Tag-Ausdruck können einen LF-Tag-Ausdruck löschen. Zusätzlich zur Berechtigung benötigt der Principal auch eine `Drop lakeformation:DeleteLFTagExpression` IAM-Berechtigung, um einen LF-Tag-Ausdruck zu löschen.

Sie können einen LF-Tag-Ausdruck mithilfe der AWS Lake Formation Konsole, der API oder der () löschen. AWS Command Line Interface AWS CLI

### Console

Um einen LF-Tag-Ausdruck zu löschen (Konsole)

1. Öffnen Sie die Lake Formation Konsole unter <https://console.aws.amazon.com/lakeformation/>.

Melden Sie sich als Data Lake-Administrator, Ersteller des LF-Tag-Ausdrucks oder als Principal an, der über die Berechtigungen zum Löschen des Ausdrucks verfügt.

2. Wählen Sie im Navigationsbereich unter Berechtigungen die Option LF-Tags und Berechtigungen aus.
3. Wählen Sie die Registerkarte LF-Tag-Ausdruck.
4. Wählen Sie im Abschnitt LF-Tag-Ausdrücke einen LF-Tag-Ausdruck aus und klicken Sie dann auf Löschen.
5. Im Ausdruck „LF-Tag löschen“? Um den Löschvorgang zu bestätigen, geben Sie den Namen des LF-Tag-Ausdrucks in das dafür vorgesehene Feld ein und wählen Sie dann Löschen.

## AWS CLI

Um ein LF-Tag () zu löschen AWS CLI

- Geben Sie einen Befehl `delete-lf-tag-expression`. Geben Sie den Namen des Ausdrucks und die Katalog-ID an, die gelöscht werden sollen.

### Example

Im folgenden Beispiel wird der LF-Tag-Ausdruck mit dem Namen `my-tag-expression` aus dem Datenkatalog mit der ID `123456789012` gelöscht. Der `catalog-id` Parameter ist optional, wenn Sie dasselbe Konto wie Ihre Konfiguration verwenden. AWS CLI Nach dem Löschen eines LF-Tag-Ausdrucks bereinigt Lake Formation die zugehörigen Berechtigungsdatensätze für diesen Ausdruck. Dies umfasst sowohl einzelne Berechtigungsdatensätze als auch aggregierte Berechtigungsdatensätze, die den gelöschten Ausdruck enthalten.

```
aws lakeformation delete-lf-tag-expression \
--name "my-tag-expression" \
--catalog-id "123456789012"
```

## LF-Tag-Ausdrücke auflisten

Sie können die LF-Tag-Ausdrücke auflisten, für die Sie die Beschreibungsberechtigung haben. Data Lake-Administratoren, Ersteller von LF-Tag-Ausdrücken und Administratoren mit Lesezugriff können implizit alle Tag-Ausdrücke in ihrem Konto sehen.

Sie können LF-Tag-Ausdrücke mithilfe der AWS Lake Formation Konsole, der API oder der () auflisten. AWS Command Line Interface AWS CLI

### Console

Um LF-Tag-Ausdrücke aufzulisten (Konsole)

1. Öffnen Sie die Lake Formation Konsole unter <https://console.aws.amazon.com/lakeformation/>.

Melden Sie sich als Ersteller des LF-Tag-Ausdrucks, als Data Lake-Administrator oder als Principal an, dem Berechtigungen für LF-Tag-Ausdrücke erteilt wurden und der über die IAM-Berechtigung verfügt. `lakeformation:ListLFTagExpressions`

2. Im Navigationsbereich unter Berechtigungen, LF-Tags und Berechtigungen.
3. Wählen Sie die Registerkarte LF-Tag-Ausdrücke, um die Ausdrücke zu sehen. Dieser Abschnitt enthält Informationen zu den vorhandenen LF-Tag-Ausdrücken, einschließlich des Ausdrucksnamens, des Ausdrucks selbst mit Links zu den enthaltenen Tags und Optionen zum Erstellen, Bearbeiten oder Löschen von Ausdrücken.

## AWS CLI

Um LF-Tags aufzulisten ()AWS CLI

- Um LF-Tag-Ausdrücke mit dem aufzulisten AWS CLI, können Sie den Befehl verwenden. `list-lf-tag-expressions` Die Anforderungssyntax lautet:

```
aws lakeformation list-lf-tag-expressions \
-- catalog-id "123456789012" \
-- max-items "100" \
-- next-token "next-token"
```

Wobei Folgendes gilt:

- `catalog-id` ist die AWS Konto-ID des Datenkatalogs, für den Sie Tagausdrücke auflisten möchten.
- `max-items` gibt die maximale Anzahl von zurückzugebenden Tag-Ausdrücken an. Wenn dieser Parameter nicht verwendet wird, ist der Standardwert 100.
- `next-token` ist ein Fortsetzungstoken, wenn die Ergebnisse in einer früheren Anfrage gekürzt wurden.

Die Antwort wird eine Liste von LF-Tag-Ausdrücken und gegebenenfalls ein Next-Token enthalten.

## Verwaltung von LF-Tag-Wertberechtigungen

Sie können Prinzipalen die `ALTER` Berechtigungen für LF-Tags gewähren, um LF-Tag-Wertausdrücke zu verwalten. Sie können Prinzipalen auch die `GRANT WITH LF-TAG EXPRESSIONS` Berechtigungen `DESCRIBE ASSOCIATE`, und für LF-Tags gewähren, um die LF-Tags anzuzeigen und sie Datenkatalogressourcen (Datenbanken, Tabellen und Spalten) zuzuweisen. Wenn LF-Tags Datenkatalogressourcen zugewiesen werden, können Sie die Tag-Based Access

Control-Methode (LF-TBAC) von Lake Formation verwenden, um diese Ressourcen zu sichern. Weitere Informationen finden Sie unter [Tag-basierte Zugangskontrolle von Lake Formation](#).

Sie können diese Berechtigungen mit der Grant-Option gewähren, sodass andere Principals sie gewähren können. Die Associate Berechtigungen Grant with LF-Tag expressionsDescribe, und werden unter erklärt. [Fügen Sie LF-Tag-Ersteller hinzu](#)

Sie können die Describe und Associate -Berechtigungen für ein LF-Tag einem externen AWS Konto gewähren. Ein Data Lake-Administrator in diesem Konto kann diese Berechtigungen dann anderen Prinzipalen im Konto gewähren. Principals, denen der Data Lake-Administrator des externen Kontos die Associate Berechtigung erteilt, können dann LF-Tags den Datenkatalogressourcen zuweisen, die Sie mit ihrem Konto geteilt haben.

Bei der Gewährung an ein externes Konto müssen Sie die Option „Gewähren“ angeben.

Sie können Berechtigungen für LF-Tags erteilen, indem Sie die Lake Formation Formation-Konsole, die API oder die AWS Command Line Interface ()AWS CLI verwenden.

## Themen

- [LF-Tag-Berechtigungen mithilfe der Konsole auflisten](#)
- [Erteilen von LF-Tag-Berechtigungen über die Konsole](#)
- [Verwaltung von LF-Tag-Berechtigungen mit dem AWS CLI](#)

Weitere Informationen finden Sie unter [Verwaltung von LF-Tags für die Zugriffskontrolle auf Metadaten](#) und [Tag-basierte Zugangskontrolle von Lake Formation](#).

## LF-Tag-Berechtigungen mithilfe der Konsole auflisten

Sie können die Lake Formation Formation-Konsole verwenden, um die für LF-Tags erteilten Berechtigungen einzusehen. Sie müssen ein LF-Tag-Ersteller oder ein Data Lake-Administrator sein oder über die Associate Berechtigung Describe oder für ein LF-Tag verfügen, um es sehen zu können.

Um die LF-Tag-Berechtigungen aufzulisten (Konsole)

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

Melden Sie sich als Ersteller des LF-Tags, als Data Lake-Administrator oder als Benutzer an, dem die, Drop AlterAssociate, oder Describe -Berechtigungen für LF-Tags erteilt wurden.

- Wählen Sie im Navigationsbereich unter Berechtigungen die Option LF-Tags und Berechtigungen und anschließend den Abschnitt LF-Tag-Berechtigungen aus.

Der Abschnitt LF-Tag-Berechtigungen zeigt eine Tabelle, die Principal-, Tag-Schlüssel, Werte und Berechtigungen enthält.

**LF-Tag permissions (6)**  
View and manage the permissions granted on LF-Tags. [Learn more](#)

Find permissions by LF-Tag key and value

|                       | Principal ▲                        | Principal type ▼ | Keys ▼  | Values ▼   | LF-Tag permissions ▼ | LF-Tag value permissions ▼   | Grantable ▼                  |
|-----------------------|------------------------------------|------------------|---------|------------|----------------------|------------------------------|------------------------------|
| <input type="radio"/> | arn:aws:iam::[redacted]:role/Admin | IAM role         | module  | All values | Alter, Drop          | -                            | Alter, Drop                  |
| <input type="radio"/> | arn:aws:iam::[redacted]:role/Admin | IAM role         | module  | All values | -                    | Describe                     | Describe                     |
| <input type="radio"/> | arn:aws:iam::[redacted]:role/Admin | IAM role         | module  | All values | -                    | Associate                    | Associate                    |
| <input type="radio"/> | arn:aws:iam::[redacted]:role/Admin | IAM role         | module  | All values | -                    | Grant with LF-Tag expression | Grant with LF-Tag expression |
| <input type="radio"/> | arn:aws:iam::[redacted]:role/Admin | IAM role         | LF-Test | All values | -                    | Describe                     | Describe                     |
| <input type="radio"/> | arn:aws:iam::[redacted]:role/Admin | IAM role         | LF-Test | All values | -                    | Associate                    | Associate                    |

## Erteilen von LF-Tag-Berechtigungen über die Konsole

In den folgenden Schritten wird erklärt, wie Sie mithilfe der Seite „LF-Tag-Berechtigungen gewähren“ in der Lake Formation Formation-Konsole Berechtigungen für LF-Tags gewähren. Die Seite ist in folgende Abschnitte unterteilt:

- Berechtigungsarten — Die Art der zu erteilenden Genehmigung.
- Principals — Die IAM-Benutzer oder -Rollen oder SAML-Benutzer oder -Rollen, denen Berechtigungen erteilt werden sollen.
- Berechtigungen für LF-Tag-Schlüssel-Wert-Paare — Die LF-Tag-Schlüssel-Wert-Paare, für die Berechtigungen erteilt werden sollen.
- LF-Tag-Berechtigungen — Die LF-Tags, für die Berechtigungen erteilt werden sollen.
- Berechtigungen für LF-Tag-Ausdrücke — Die LF-Tags, für die Berechtigungen erteilt werden sollen.
- Berechtigungen — Die zu erteilenden Berechtigungen.

Öffnen Sie die Seite „LF-Tag-Berechtigungen gewähren“

1. Öffnen Sie die Lake Formation Konsole unter <https://console.aws.amazon.com/lakeformation/>.

Melden Sie sich als LF-Tag-Ersteller, Data Lake-Administrator oder als Benutzer an. Mit dieser Option wurden LF-Tag-Berechtigungen oder LF-Tag-Schlüssel-Wert-Paar-Berechtigungen für LF-Tags erteilt. Grant

2. Wählen Sie im Navigationsbereich die Option LF-Tags und Berechtigungen und anschließend den Abschnitt LF-Tag-Berechtigungen aus.
3. Klicken Sie auf Gewähren von Berechtigungen aus.

Geben Sie den Berechtigungstyp an

Wählen Sie im Abschnitt Berechtigungstyp einen Berechtigungstyp aus.

#### LF-Tag-Berechtigungen

Wählen Sie die LF-Tag-Berechtigungen, damit Principals LF-Tag-Werte aktualisieren oder LF-Tags löschen können.

#### Berechtigungen für LF-Tag-Schlüsselwertpaare

Wählen Sie die LF-Tag-Berechtigungen für Schlüssel-Wert-Paare, um es Prinzipalen zu ermöglichen, Datenkatalogressourcen LF-Tags zuzuweisen, LF-Tags und -Werte anzuzeigen und Prinzipalen LF-Tag-basierte Berechtigungen für Datenkatalogressourcen zu gewähren.

Die in den folgenden Abschnitten verfügbaren Optionen hängen vom Berechtigungstyp ab.

#### Berechtigungen für LF-Tag-Ausdrücke

Wählen Sie die LF-Tag-Ausdrucksberechtigungen, um es den Prinzipalen zu ermöglichen, Ausdrücke zu aktualisieren oder Ausdrücke zu löschen.

Geben Sie die Prinzipale an

#### Note

Sie können externen Konten oder Prinzipalen in einem anderen Konto keine LF-Tag-Berechtigungen (Alter und Drop) gewähren.

Wählen Sie im Abschnitt **Principals** einen Prinzipaltyp aus und geben Sie die Principals an, denen Berechtigungen erteilt werden sollen.

### Principals

☒ **IAM users and roles**  
Users or roles from this AWS account.

☐ **SAML users and groups**  
SAML users and group or QuickSight ARNs.

☐ **External accounts**  
AWS account, AWS organization or IAM principal outside of this account

**IAM users and roles**  
Add one or more IAM users or roles.  

Choose IAM principals to add ▼

## IAM-Benutzer und -Rollen

Wählen Sie einen oder mehrere Benutzer oder Rollen aus der Liste der IAM-Benutzer und -Rollen aus.

## SAML-Benutzer und -Gruppen

Geben Sie für SAML- und Quick-Benutzer und -Gruppen einen oder mehrere Amazon-Ressourcennamen (ARNs) für Benutzer oder Gruppen ein, die über SAML verbunden sind, oder ARNs für Quick-Benutzer oder -Gruppen. Drücken Sie nach jedem ARN die Eingabetaste.

Informationen zur Erstellung von finden Sie unter ARNs. [Lake Formation erteilt und widerruft AWS CLI Befehle](#)

### Note

Die Integration von Lake Formation mit Quick wird nur für die Quick Enterprise Edition unterstützt.

## Externe Konten

Geben Sie als AWS Konto ein oder mehrere gültige AWS Konten ein IDs. Drücken Sie nach jeder ID die Eingabetaste.

Eine Organisations-ID besteht aus einem „o-“, gefolgt von 10 bis 32 Kleinbuchstaben oder Ziffern.



Eine Organisationseinheits-ID beginnt mit „ou-“, gefolgt von 4 bis 32 Kleinbuchstaben oder Ziffern (der ID des Stammes, der die Organisationseinheit enthält). Auf diese Zeichenfolge folgen ein zweiter Gedankenstrich „-“ und 8 bis 32 zusätzliche Kleinbuchstaben oder Ziffern.

Geben Sie für IAM-Principal den ARN für den IAM-Benutzer oder die IAM-Rolle ein.

Geben Sie die LF-Tags an

Um Berechtigungen für LF-Tags zu gewähren, geben Sie im Abschnitt LF-Tag-Berechtigungen die LF-Tags an, für die Berechtigungen erteilt werden sollen.

### LF-Tag permissions

#### LF-Tags

Choose the LF-Tags you want to grant permissions to.

Choose one or more LF-Tags ▼

Department X

#### Permissions

Choose the specific LF-Tag permissions to grant.

☒ **Alter**  
Update or delete key values.

☒ **Drop**  
Delete tag(s).

#### Grantable permissions

Choose the permissions that the grant recipient(s) can grant to other principals.

☒ **Alter**  
Update or delete key values.

☒ **Drop**  
Delete tag(s).

Cancel

Grant

- Wählen Sie über das Drop-down-Menü ein oder mehrere LF-Tags aus.

Geben Sie die Schlüssel-Wert-Paare für das LF-Tag an

1. Um Berechtigungen für LF-Tag-Schlüssel-Wert-Paare zu gewähren (Sie müssen zuerst LF-Tag-Schlüssel-Wert-Paar-Berechtigungen als Berechtigungstyp auswählen), wählen Sie LF-Tag-Schlüssel-Wert-Paar hinzufügen, um die erste Zeile mit Feldern für die Angabe von LF-Tag-Schlüsseln und Werten anzuzeigen.

### LF-Tag key-value pair permissions

Key

Values

Choose LF-Tag values

▼

Remove

Add LF-Tag key-value pair

You can add 50 more LF-Tags.

Permissions

Choose the specific key-value pair permissions to grant.

☐ Describe

See keys and values.

☐ Associate

Assign LF-Tags to databases, tables, and columns.

☐ Grant with LF-Tag expression

Allow the principal(s) to grant access permissions using the LF-Tag(s).

Grantable permissions

Choose the permissions that the grant recipient(s) can grant to other principals.

☐ Describe

See keys and values.

☐ Associate

Assign LF-Tags to databases, tables, and columns.

☐ Grant with LF-Tag expression

Allow the principal(s) to grant access permissions using the LF-Tag(s).

Cancel

Grant

2. Positionieren Sie den Cursor im Schlüsselfeld, beginnen Sie optional mit der Eingabe, um die Auswahlliste einzugrenzen, und wählen Sie einen LF-Tag-Schlüssel aus.
3. Wählen Sie in der Werteliste einen oder mehrere Werte aus, und drücken Sie dann die Tabulatortaste oder klicken oder tippen Sie auf eine Stelle außerhalb des Felds, um die ausgewählten Werte zu speichern.

 Note

Wenn eine der Zeilen in der Werteliste den Fokus hat, wird durch Drücken der EINGABETASTE das Kontrollkästchen aktiviert oder deaktiviert.

Die ausgewählten Werte werden als Kacheln unter der Werteliste angezeigt. Wählen Sie ✕, um einen Wert zu entfernen. Wählen Sie Entfernen, um das gesamte LF-Tag zu entfernen.

- Um ein weiteres LF-Tag hinzuzufügen, wählen Sie erneut LF-Tag hinzufügen und wiederholen Sie die beiden vorherigen Schritte.

Geben Sie die LF-Tag-Ausdrücke an

- Um Berechtigungen für LF-Tag-Ausdrücke zu gewähren, müssen Sie zunächst LF-Tag-Ausdrucksberechtigungen als Berechtigungstyp auswählen.

### Permission type

Choose the type of permission to grant. [Learn more](#) 

☐ LF-Tag permissions  
Grant permissions on LF-Tags to create, update, and delete LF-Tags.

☐ LF-Tag key-value pair permissions  
Grant permissions on LF-Tag key-value pairs to assign LF-Tags to Data Catalog resources and grant permissions on the resources to principals.

☒ LF-Tag expression permissions - *new*  
Grant permissions on LF-Tag expressions.

### Principals

Choose the principals to grant permissions.

#### IAM users and roles

Add one or more IAM users or roles.

Choose IAM principals to add 

datalake\_user ✕  
User

- Wählen Sie einen LF-Tag-Ausdruck.

3. Die ausgewählten Ausdrücke werden als Kacheln unter der Liste der LF-Tag-Ausdrücke angezeigt. Wählen Sie ✕, um einen Ausdruck zu entfernen.
4. Um einen weiteren LF-Tag-Ausdruck hinzuzufügen, wählen Sie einen anderen Ausdruck.

Geben Sie die Berechtigungen an

In diesem Abschnitt werden entweder die LF-Tag-Berechtigungen oder die LF-Tag-Werteberechtigungen basierend auf dem Berechtigungstyp angezeigt, den Sie im vorherigen Schritt ausgewählt haben.

Wählen Sie je nach Berechtigungstyp, den Sie gewähren möchten, die LF-Tag-Berechtigungen oder die LF-Tag-Schlüsselwertpaar-Berechtigungen und die erteilbaren Berechtigungen aus.

1. Wählen Sie unter LF-Tag-Berechtigungen die zu erteilenden Berechtigungen aus.

Wenn Sie Drop and Alter gewähren, wird implizit Describe gewährt.

Sie müssen für alle Tag-Werte die Berechtigungen Alter und Drop gewähren.

2. Wählen Sie unter LT-Tag-Schlüsselwertberechtigungen die zu erteilenden Berechtigungen aus.

Die Erteilung von Associate gewährt implizit Describe. Wählen Sie den Ausdruck Grant with LF-Tag, um es dem Empfänger zu ermöglichen, mithilfe der LF-TBAC-Methode Zugriffsberechtigungen für Datenkatalogressourcen zu gewähren oder zu widerrufen.

3. Wählen Sie unter LF-Tag-Ausdrucksberechtigungen die zu erteilenden Berechtigungen aus.

Wenn Sie Drop and Alter gewähren, wird implizit Describe gewährt.

Durch die Erteilung der Super-Berechtigung werden alle verfügbaren Berechtigungen gewährt.

4. (Optional) Wählen Sie unter Erteilbare Berechtigungen die Berechtigungen aus, die der Empfänger der Gewährung anderen Hauptbenutzern in seinem AWS Konto gewähren kann.
5. Wählen Sie Grant (Erteilen).

Verwaltung von LF-Tag-Berechtigungen mit dem AWS CLI

Sie können Berechtigungen für LF-Tags gewähren, widerrufen und auflisten, indem Sie die () verwenden. AWS Command Line Interface AWS CLI

## Um LF-Tag-Berechtigungen aufzulisten (AWS CLI)

- Geben Sie einen Befehl ein `list-permissions`. Sie müssen der Ersteller des LF-Tags oder ein Data Lake-Administrator sein oder über die `DropAlter, Grant with LF-Tag permissions` -Berechtigung für ein LF-Tag verfügen `DescribeAssociate`, um es sehen zu können.

Der folgende Befehl fordert alle LF-Tags an, für die Sie Berechtigungen haben.

```
aws lakeformation list-permissions --resource-type LF_TAG
```

Im Folgenden finden Sie eine Beispielausgabe für einen Data Lake-Administrator, der alle LF-Tags sieht, die allen Prinzipalen gewährt wurden. Benutzern ohne Administratorrechte werden nur LF-Tags angezeigt, die ihnen gewährt wurden. LF-Tag-Berechtigungen, die von einem externen Konto aus gewährt wurden, werden auf einer separaten Ergebnisseite angezeigt. Um sie zu sehen, wiederholen Sie den Befehl und geben Sie dem `--next-token` Argument das Token an, das bei der vorherigen Befehlsausführung zurückgegeben wurde.

```
{
 "PrincipalResourcePermissions": [
 {
 "Principal": {
 "DataLakePrincipalIdentifier": "arn:aws:iam::111122223333:user/datalake_admin"
 },
 "Resource": {
 "LFTag": {
 "CatalogId": "111122223333",
 "TagKey": "environment",
 "TagValues": [
 "*"
]
 }
 },
 "Permissions": [
 "ASSOCIATE"
],
 "PermissionsWithGrantOption": [
 "ASSOCIATE"
]
 },
],
}
```

```

 {
 "Principal": {
 "DataLakePrincipalIdentifier": "arn:aws:iam::111122223333:user/
datalake_user1"
 },
 "Resource": {
 "LFTag": {
 "CatalogId": "111122223333",
 "TagKey": "module",
 "TagValues": [
 "Orders",
 "Sales"
]
 }
 },
 "Permissions": [
 "DESCRIBE"
],
 "PermissionsWithGrantOption": []
 },
 ...
],
 "NextToken": "eyJzaG91bGRRdWVy...Wlzc2lvdnMiOnRydWV9"
}

```

Sie können alle Grants für einen bestimmten LF-Tag-Schlüssel auflisten. Der folgende Befehl gibt alle für das LF-Tag gewährten Berechtigungen zurück. `module`

```
aws lakeformation list-permissions --resource-type LF_TAG --resource '{ "LFTag":
{"CatalogId":"111122223333","TagKey":"module","TagValues":["*"]}'
```

Sie können auch LF-Tag-Werte auflisten, die einem bestimmten Prinzipal für ein bestimmtes LF-Tag gewährt wurden. Wenn Sie das `--principal` Argument angeben, müssen Sie das Argument angeben. `--resource` Daher kann der Befehl effektiv nur die Werte anfordern, die einem bestimmten Prinzipal für einen bestimmten LF-Tag-Schlüssel gewährt wurden. Der folgende Befehl zeigt, wie dies für den Principal `datalake_user1` und den LF-Tag-Schlüssel funktioniert. `module`

```
aws lakeformation list-permissions --principal
DataLakePrincipalIdentifier=arn:aws:iam::111122223333:user/
```

```
datalake_user1 --resource-type LF_TAG --resource '{ "LFTag":
{"CatalogId":"111122223333","TagKey":"module","TagValues":["*"]}]'
```

Dies ist eine Beispielausgabe.

```
{
 "PrincipalResourcePermissions": [
 {
 "Principal": {
 "DataLakePrincipalIdentifier": "arn:aws:iam::111122223333:user/
datalake_user1"
 },
 "Resource": {
 "LFTag": {
 "CatalogId": "111122223333",
 "TagKey": "module",
 "TagValues": [
 "Orders",
 "Sales"
]
 }
 },
 "Permissions": [
 "ASSOCIATE"
],
 "PermissionsWithGrantOption": []
 }
]
}
```

Um Berechtigungen für LF-Tags () zu gewähren AWS CLI

1. Verwenden Sie einen Befehl ähnlich dem folgenden. In diesem Beispiel wird `datalake_user1` dem Benutzer die Associate Berechtigung für das LF-Tag mit dem Schlüssel erteilt. `module` Es gewährt Berechtigungen zum Anzeigen und Zuweisen aller Werte für diesen Schlüssel, wie durch das Sternchen (\*) gekennzeichnet.

```
aws lakeformation grant-permissions --principal
DataLakePrincipalIdentifier=arn:aws:iam::111122223333:user/
```

```
datalake_user1 --permissions "ASSOCIATE" --resource '{ "LFTag":
{"CatalogId":"111122223333","TagKey":"module","TagValues":["*"]}}'
```

Durch die Erteilung der Associate Berechtigung wird die Berechtigung implizit erteilt.  
Describe

Das nächste Beispiel gewährt Associate dem externen AWS Konto 1234-5678-9012 auf dem LF-Tag mit dem Schlüssel und der Grant-Option. module Es gewährt Berechtigungen, nur die Werte und anzuzeigen und zuzuweisen. sales orders

```
aws lakeformation grant-permissions --principal
DataLakePrincipalIdentifier=123456789012 --permissions "ASSOCIATE"
--permissions-with-grant-option "ASSOCIATE" --resource '{ "LFTag":
{"CatalogId":"111122223333","TagKey":"module","TagValues":["sales", "orders"]}}'
```

2. Durch die Erteilung der GrantWithLFTagExpression Berechtigung wird die Describe Berechtigung implizit erteilt.

Das nächste Beispiel erteilt GrantWithLFTagExpression einem Benutzer auf dem LF-Tag mit dem Schlüssel die Option module Grant. Es gewährt Berechtigungen zum Anzeigen und Erteilen von Berechtigungen für Datenkatalogressourcen, wobei nur die Werte sales und verwendet werden. orders

```
aws lakeformation grant-permissions --principal
DataLakePrincipalIdentifier=111122223333 --permissions "GrantWithLFTagExpression"
--permissions-with-grant-option "GrantWithLFTagExpression" --resource '{ "LFTag":
{"CatalogId":"111122223333","TagKey":"module","TagValues":["sales", "orders"]}}'
```

3. Im nächsten Beispiel werden einem Benutzer Drop Berechtigungen für das LF-Tag mit dem Schlüssel und der module Option Grant erteilt. Sie gewährt Berechtigungen zum Löschen des LF-Tags. Um ein LF-Tag zu löschen, benötigen Sie Berechtigungen für alle Werte dieses Schlüssels.

```
aws lakeformation grant-permissions --principal
DataLakePrincipalIdentifier=111122223333 --permissions "DROP"
--permissions-with-grant-option "DROP" --resource '{ "LFTag":
{"CatalogId":"111122223333","TagKey":"module","TagValues":["*"]}}'
```

4. Das nächste Beispiel gewährt dem Benutzer mit dem LF-Tag mit dem Schlüssel Alter Berechtigungen mit der module Grant-Option. Es gewährt Berechtigungen zum Löschen des



LF-Tags. Um ein LF-Tag zu aktualisieren, benötigen Sie Berechtigungen für alle Werte dieses Schlüssels.

```
aws lakeformation grant-permissions --principal
DataLakePrincipalIdentifier=111122223333 --permissions "ALTER"
--permissions-with-grant-option "ALTER" --resource '{ "LFTag":
{"CatalogId":"111122223333","TagKey":"module","TagValues":["*"]}]'
```

Um Berechtigungen für LF-Tags () zu widerrufen AWS CLI

- Verwenden Sie einen Befehl ähnlich dem folgenden. In diesem Beispiel wird dem Benutzer die Associate Erlaubnis für das LF-Tag mit dem Schlüssel entzogen. module datalake\_user1

```
aws lakeformation revoke-permissions --principal
DataLakePrincipalIdentifier=arn:aws:iam::111122223333:user/
datalake_user1 --permissions "ASSOCIATE" --resource '{ "LFTag":
{"CatalogId":"111122223333","TagKey":"module","TagValues":["*"]}]'
```

## Erteilen von Data Lake-Berechtigungen mithilfe der LF-TBAC-Methode

Sie können Prinzipalen die DESCRIBE und ASSOCIATE Lake Formation Formation-Berechtigungen für LF-Tags gewähren, sodass sie die LF-Tags anzeigen und sie Datenkatalogressourcen (Datenbanken, Tabellen, Ansichten und Spalten) zuweisen können. Wenn LF-Tags Datenkatalogressourcen zugewiesen werden, können Sie die Tag-Based Access Control-Methode (LF-TBAC) von Lake Formation verwenden, um diese Ressourcen zu sichern. Weitere Informationen finden Sie unter [Tag-basierte Zugangskontrolle von Lake Formation](#).

Zunächst kann nur der Data Lake-Administrator diese Berechtigungen gewähren. Wenn der Data Lake-Administrator diese Berechtigungen mit der Option „Gewähren“ erteilt, können sie von anderen Prinzipalen erteilt werden. Die ASSOCIATE Berechtigungen DESCRIBE und werden unter erklärt. [Bewährte Methoden und Überlegungen zur Tag-basierten Zugriffskontrolle von Lake Formation](#)

Sie können die DESCRIBE und ASSOCIATE -Berechtigungen für ein LF-Tag einem externen AWS Konto gewähren. Ein Data Lake-Administrator in diesem Konto kann diese Berechtigungen dann anderen Prinzipalen im Konto gewähren. Principals, denen der Data Lake-Administrator des externen Kontos die ASSOCIATE Berechtigung erteilt, können dann LF-Tags den Datenkatalogressourcen zuweisen, die Sie mit ihrem Konto geteilt haben.

Wenn Sie die Gewährung an ein externes Konto vornehmen, müssen Sie die Option „Gewähren“ angeben.

Sie können Berechtigungen für LF-Tags mithilfe der AWS Lake Formation Konsole, der API oder der AWS Command Line Interface (AWS CLI) gewähren.

#### Note

Die folgenden Schritte sind für S3-Tables-Kataloge nicht erforderlich. Sie können LF-Tags verwenden, um Berechtigungen für bestehende S3 Tables-Kataloge zu gewähren, ohne sie zu löschen und neu zu erstellen.

Aktivierung der LF-Tags-Unterstützung für bestehende Verbundkataloge, die Lake Formation Formation-Berechtigungen verwenden

Gehen Sie wie folgt vor, wenn Sie bereits Verbundkataloge haben, die Lake Formation Formation-Berechtigungen verwenden, wie Amazon Redshift, oder Amazon DynamoDB Kataloge, die erstellt wurden, bevor die Unterstützung von LF-Tags für Verbundkataloge verfügbar war.

1. Den vorhandenen Katalog löschen — Rufen Sie den `deleteCatalog` API-Vorgang auf, um den vorhandenen Verbundkatalog zu entfernen, der Lake Formation Formation-Berechtigungen verwendet.
2. Neuen Verbundkatalog erstellen — Erstellen Sie einen neuen Katalog und verweisen Sie den neuen Katalog auf Ihren vorhandenen Namespace/Datashare.

Verwenden Sie einen neuen Namen für den Katalog — Bei diesem Vorgang werden Ihre bereits vorhandenen Verbundkataloge aktualisiert, sodass sie die LF-Tag-Funktionalität unterstützen. Wenn Sie denselben Katalognamen verwenden möchten, wenden AWS Sie sich an das Support-Team, um Unterstützung zu erhalten.

## Themen

- [Erteilen von Datenkatalogberechtigungen](#)

#### Weitere Informationen finden Sie auch unter

- [Verwaltung von LF-Tag-Wertberechtigungen](#)

- [Verwaltung von LF-Tags für die Zugriffskontrolle auf Metadaten](#)
- [Tag-basierte Zugangskontrolle von Lake Formation](#)

## Erteilen von Datenkatalogberechtigungen

Verwenden Sie die Lake Formation-Konsole oder AWS CLI, um Sie Lake Formation-Berechtigungen für Datenkatalogdatenbanken, Tabellen, Ansichten und Spalten mithilfe der Tag-Based Access Control (LF-TBAC) -Methode von Lake Formation.

### Console

In den folgenden Schritten wird erklärt, wie Sie mithilfe der Tag-Based Access Control (LF-TBAC) -Methode (Lake Formation, Tag-Based Access Control) und der Seite Data Lake-Berechtigungen gewähren in der Lake Formation-Konsole Berechtigungen gewähren. Die Seite ist in die folgenden Abschnitte unterteilt:

- Principals — Die Benutzer, Rollen und Benutzer, denen Berechtigungen erteilt werden AWS-Konten sollen.
- LF-Tags oder Katalogressourcen — Die Datenbanken, Tabellen oder Ressourcenlinks, für die Berechtigungen erteilt werden sollen.
- Genehmigungen — Die Lake Formation erteilt Genehmigungen.

1. Öffnen Sie die Seite Data Lake-Berechtigungen gewähren.

Öffnen Sie die AWS Lake Formation Konsole unter <https://console.aws.amazon.com/lakeformation/> und melden Sie sich als Data Lake-Administrator oder als Benutzer an, dem Lake Formation-Berechtigungen für Data Catalog-Ressourcen über LF-TBAC mit der Grant-Option erteilt wurden.

Wählen Sie im Navigationsbereich unter Berechtigungen die Option Data Lake-Berechtigungen aus. Wählen Sie dann Grant (Erteilen) aus.

2. Geben Sie die Prinzipale an.

Wählen Sie im Abschnitt Principals einen Prinzipaltyp aus und geben Sie dann die Principals an, denen Berechtigungen erteilt werden sollen.

## Grant permissions

### Principals

Choose the principals to grant permissions.

☒ **IAM users and roles**  
Users or roles from this AWS account.

☐ **IAM Identity Center**  
- *new*  
Users and groups configured in IAM Identity Center.

☐ **SAML users and groups**  
SAML users and group or QuickSight ARNs.

☐ **External accounts**  
AWS account, AWS organization or IAM principal outside of this account

#### IAM users and roles

Add one or more IAM users or roles.

Choose IAM principals to add ▼

AWSServiceRoleForRedshift ✕  
Role

### IAM-Benutzer und -Rollen

Wählen Sie einen oder mehrere Benutzer oder Rollen aus der Liste der IAM-Benutzer und -Rollen aus.

### IAM Identity Center

Wählen Sie einen oder mehrere Benutzer oder aus der Liste Benutzer und Gruppen aus.

### SAML-Benutzer und -Gruppen

Geben Sie für SAML- und Quick-Benutzer und -Gruppen einen oder mehrere Amazon-Ressourcennamen (ARNs) für Benutzer oder Gruppen ein, die über SAML verbunden sind, oder ARNs für Quick-Benutzer oder -Gruppen. Drücken Sie nach jedem ARN die Eingabetaste.

Informationen zur Erstellung von finden Sie unter ARNs. [Lake Formation erteilt und widerruft AWS CLI Befehle](#)

#### Note

Die Integration von Lake Formation mit Quick wird nur für die Quick Enterprise Edition unterstützt.

## Externe Konten

Geben Sie für AWS-Konten AWS Organisation oder IAM-Principal eine oder mehrere gültige Organisationen AWS-Konto IDs IDs, Organisationseinheiten IDs oder ARN für den IAM-Benutzer oder die IAM-Rolle ein. Drücken Sie nach jeder ID die Eingabetaste.

Eine Organisations-ID besteht aus einem „o-“, gefolgt von 10 bis 32 Kleinbuchstaben oder Ziffern.

Eine Organisationseinheits-ID beginnt mit „ou-“, gefolgt von 4 bis 32 Kleinbuchstaben oder Ziffern (der ID des Stammes, der die Organisationseinheit enthält). Auf diese Zeichenfolge folgen ein zweiter Gedankenstrich „-“ und 8 bis 32 zusätzliche Kleinbuchstaben oder Ziffern.

### 3. Geben Sie die LF-Tags an.

Stellen Sie sicher, dass die Option Ressourcen, denen LF-Tags zugeordnet sind, ausgewählt ist. Wählen Sie LF-Tag-Schlüssel-Wert-Paare oder Gespeicherte LF-Tag-Ausdrücke.

#### 1. Wenn Sie die Option LF-Tag-Schlüssel-Wert-Paare wählen, wählen Sie die Schlüssel und Werte aus.

Wenn Sie mehr als einen Wert wählen, erstellen Sie einen LF-Tag-Ausdruck mit einem Operator. OR Das bedeutet, dass Ihnen Berechtigungen für die Ressource erteilt werden, wenn einer der LF-Tag-Werte mit einem LF-Tag übereinstimmt, der einer Datenkatalogressource zugewiesen ist.

## LF-Tags or catalog resources

Choose a method to grant permissions.

☒ **Resources matched by LF-Tags (recommended)**

Manage permissions indirectly for resources or data matched by a specific set of LF-Tags.

☐ **Named Data Catalog resources**

Manage permissions for specific databases or tables, in addition to fine-grained data access.

☒ **LF-Tag key-value pairs**

☐ **Saved LF-Tag expressions - new**

**Key**

Location

**Values**

Choose LF-Tag values

Remove

US

Department

Choose LF-Tag values

Remove

marketing

sales

Add LF-Tag key-value pair

You can add 48 more LF-Tags.

**Expression review**

The LF-Tag expression above will be interpreted in the following way.

Location = US  
AND Department = (marketing OR sales)

☒ **Save as new expression**

Use saved expressions to grant permissions. Create LF-Tag expression permissions are needed.

**New LF-Tag expression name**

Enter a name that describes the expression. Expression name cannot be edited after creation.

new-expression

Name must be less than 1000 characters.

2. (Optional) Wählen Sie erneut „LF-Tag-Schlüssel-Wert-Paar hinzufügen“, um ein anderes LF-Tag anzugeben.

Wenn Sie mehr als ein LF-Tag angeben, erstellen Sie einen LF-Tag-Ausdruck mit einem Operator. AND Dem Prinzipal werden nur dann Berechtigungen für eine Datenkatalogressource gewährt, wenn der Ressource für jedes LF-Tag im LF-Tag-Ausdruck ein passendes LF-Tag zugewiesen wurde.

3. Wählen Sie die Option Als neuen Ausdruck speichern, um den Ausdruck wiederzuverwenden.

Sie Create LF-Tag expression müssen Ausdrücke speichern.

Weitere Hinweise zu LF-Tag-Ausdrücken finden Sie unter. [Verwaltung von LF-Tag-Ausdrücken für die Zugriffskontrolle auf Metadaten](#)

#### 4. Geben Sie die Berechtigungen an.

Geben Sie die Berechtigungen an, die Sie dem Prinzipal für entsprechende Datenkatalogressourcen gewähren möchten. Passende Ressourcen sind Ressourcen, denen LF-Tags zugewiesen wurden, die einem der LF-Tag-Ausdrücke entsprechen, die dem Prinzipal erteilt wurden.

Sie können die Berechtigungen angeben, die für übereinstimmende Datenbanken, übereinstimmende Tabellen und übereinstimmende Ansichten gewährt werden sollen.

▼ Database permissions

Database permissions

Choose specific access permissions to grant.

☐ Create table
☐ Alter
☐ Drop

☐ Describe

☐ Super  
This permission is the union of all the individual permissions to the left, and supersedes them.

Grantable permissions

Choose the permission that may be granted to others.

☐ Create table
☐ Alter
☐ Drop

☐ Describe

☐ Super  
This permission allows the principal to grant any of the permissions to the left, and supersedes those grantable permissions.

▼ Table permissions

Table permissions

Choose specific access permissions to grant.

☐ Alter
☐ Insert
☐ Drop

☐ Delete
☐ Select
☐ Describe

☐ Super  
This permission is the union of all the individual permissions to the left, and supersedes them.

Grantable permissions

Choose the permission that may be granted to others.

☐ Alter
☐ Insert
☐ Drop

☐ Delete
☐ Select
☐ Describe

☐ Super  
This permission allows the principal to grant any of the permissions to the left, and supersedes those grantable permissions.

Wählen Sie unter Datenbankberechtigungen die Datenbankberechtigungen aus, die Sie dem Prinzipal für passende Datenbanken gewähren möchten.

Wählen Sie unter Tabellenberechtigungen die Tabellen- oder Anzeigeberechtigungen aus, die dem Prinzipal für übereinstimmende Tabellen und Ansichten erteilt werden sollen.

Sie können auch `SelectDescribe`, und `Drop` Berechtigungen aus den Tabellenberechtigungen auswählen, die auf Ansichten angewendet werden sollen.

5. Wählen Sie `Grant` (Erteilen).

## AWS CLI

Sie können die Methode AWS Command Line Interface (AWS CLI) und die Tag-Based Access Control (LF-TBAC) -Methode (Lake Formation) verwenden, um Lake Formation Berechtigungen für Data Catalog-Datenbanken, -Tabellen und -Spalten zu gewähren.

Erteilen von Data-Lake-Berechtigungen mithilfe der und der LF-TBAC-Methode AWS CLI

- Verwenden Sie den Befehl `grant-permissions`.

### Example

Im folgenden Beispiel wird dem Benutzer der LF-Tag-Ausdruck `"module=*" (alle Werte des LF-Tag-Schlüssels) gewährt. module datalake_user1` Dieser Benutzer hat Zugriff auf alle passenden Datenbanken `CREATE_TABLE`, d. h. Datenbanken, denen das LF-Tag mit dem Schlüssel mit einem beliebigen Wert zugewiesen wurde. `module`

```
aws lakeformation grant-permissions --principal
DataLakePrincipalIdentifier=arn:aws:iam::111122223333:user/
datalake_user1 --permissions "CREATE_TABLE" --resource '{ "LFTagPolicy":
{"CatalogId":"111122223333","ResourceType":"DATABASE","Expression":
[{"TagKey":"module","TagValues":["*"]}]}'
```

### Example

Im nächsten Beispiel wird dem Benutzer der LF-Tag-Ausdruck `"" (level=director) AND (region=west OR region=south) datalake_user1` Dieser Benutzer verfügt über die `DROP` Berechtigungen `SELECTALTER`, und mit der `Grant-Option` für übereinstimmende Tabellen, denen `level=director` sowohl als auch (oder) zugewiesen wurde. `region=west region=south`

```
aws lakeformation grant-permissions --principal
DataLakePrincipalIdentifier=arn:aws:iam::111122223333:user/
datalake_user1 --permissions "SELECT" "ALTER" "DROP" --permissions-
with-grant-option "SELECT" "ALTER" "DROP" --resource '{ "LFTagPolicy":
```



```
{"CatalogId":"111122223333","ResourceType":"TABLE","Expression": [{"TagKey": "level","TagValues": ["director"]},{ "TagKey": "region","TagValues": ["west", "south"]}]]}]'
```

## Example

Im nächsten Beispiel wird dem Konto 1234-5678-9012 der LF-Tag-Ausdruck "module=orders" zugewiesen. AWS Der Data Lake-Administrator in diesem Konto kann dann den Prinzipalen in seinem Konto den Ausdruck "" module=orders gewähren. Diese Prinzipale sind dann CREATE\_TABLE berechtigt, Datenbanken abzugleichen, die dem Konto 1111-2222-3333 gehören und mit dem Konto 1234-5678-9012 gemeinsam genutzt wurden, indem sie entweder die benannte Ressourcenmethode oder die LF-TBAC-Methode verwenden.

```
aws lakeformation grant-permissions --principal
DataLakePrincipalIdentifier=123456789012 --permissions "CREATE_TABLE" --
permissions-with-grant-option "CREATE_TABLE" --resource '{ "LFTagPolicy":
{"CatalogId":"111122223333","ResourceType":"DATABASE","Expression":
[{"TagKey": "module", "TagValues": ["orders"]}]]}]'
```

## Attributbasierte Zugriffskontrolle

In AWS Lake Formation können Sie Zugriff auf AWS Glue Data Catalog Objekte wie Kataloge, Datenbanken, Tabellen und Datenfilter gewähren, indem Sie Attribute verwenden, bei denen es sich um IAM-Tags und Sitzungs-Tags handelt, die mit IAM-Entitäten wie Rollen und Benutzern verknüpft sind.

Weitere Informationen zur Verwendung von Sitzungs-Tags finden Sie unter [assume-role](#) im Benutzerhandbuch. AWS CLI

Die attributbasierte Zugriffskontrolle (ABAC) ist eine Autorisierungsstrategie, bei der Berechtigungen auf der Grundlage von Attributen definiert werden. AWS nennt diese Attribute Tags. Sie können ABAC verwenden, um Principals innerhalb desselben Kontos oder in einem anderen Konto Zugriff auf die Datenkatalogressourcen zu gewähren. Jeder IAM-Prinzipal mit passenden Schlüsseln und Werten für das IAM-Tag oder das Sitzungs-Tag erhält Zugriff auf die Ressource. Sie müssen über erteilbare Berechtigungen für die Ressourcen verfügen, um diese Berechtigungen gewähren zu können.

Mit ABAC können Sie mehreren Benutzern gleichzeitig Zugriff gewähren. Wenn neue Benutzer der Organisation beitreten, kann ihr Zugriff auf Daten anhand ihrer Attribute, wie z. B. ihrer beruflichen Funktion oder Abteilung, automatisch bestimmt werden, ohne dass Administratoren bestimmte Rollen oder Berechtigungen manuell zuweisen müssen. Durch die Verwendung von Attributen anstelle von Rollen bietet ABAC eine effizientere und wartungsfreundlichere Methode zur Verwaltung des Datenzugriffs über verschiedene Systeme und Umgebungen hinweg und verbessert so letztlich die Datenverwaltung und Compliance.

Weitere Informationen zur Definition von Attributen finden Sie unter [Definieren von Berechtigungen auf der Grundlage von Attributen](#) mit ABAC-Autorisierung.

Informationen zu Einschränkungen, Überlegungen und unterstützten AWS Regionen finden Sie unter [Überlegungen zur attributbasierten Zugriffskontrolle, Einschränkungen und unterstützte Regionen](#).

## Themen

- [Voraussetzungen für die Erteilung von Berechtigungen mithilfe von Attributen](#)
- [Erteilen von Berechtigungen mithilfe der attributbasierten Zugriffskontrolle](#)

## Voraussetzungen für die Erteilung von Berechtigungen mithilfe von Attributen

Um Berechtigungen mithilfe der attributbasierten Zugriffskontrolle (ABAC) zu erteilen, müssen Sie die folgenden Voraussetzungen erfüllen:

- Aktualisieren Sie die Datenkatalogeinstellungen, um Lake Formation-Berechtigungen für Datenkatalogobjekte zu aktivieren. Weitere Informationen finden Sie im Abschnitt [Ändern des Standardberechtigungsmodells oder Verwenden des hybriden Zugriffsmodus](#).
- Stellen Sie die kontoübergreifenden Versionseinstellungen auf zwei oder höher ein.
- [Fügen Sie den IAM-Entitäten, die Zugriff benötigen, Attribute hinzu](#).
- Nur ein Data Lake-Administrator oder ein IAM-Benutzer mit den erforderlichen Berechtigungen kann Zugriff auf Datenkatalogobjekte gewähren. Weitere Informationen zu den erforderlichen Berechtigungen finden Sie unter [IAM-Berechtigungen](#).

## Erteilen von Berechtigungen mithilfe der attributbasierten Zugriffskontrolle

In diesem Thema werden die Schritte beschrieben, die Sie ausführen müssen, um attributbasierte Zugriffsberechtigungen für Datenkatalogressourcen zu gewähren. Sie können die Lake Formation Formation-Konsole oder die AWS Befehlszeilenschnittstelle (AWS CLI) verwenden.

### Erteilen von Berechtigungen mit ABAC (AWS-Managementkonsole)

1. Öffnen Sie die Lake Formation Formation-Konsole unter <https://console.aws.amazon.com/lakeformation/> und melden Sie sich als Data Lake-Administrator, Ressourcenersteller oder als IAM-Benutzer an, der über Grantable-Berechtigungen für die Ressource verfügt.
2. Führen Sie eine der folgenden Aktionen aus:
  - Wählen Sie im Navigationsbereich unter Berechtigungen die Option Data Lake-Berechtigungen aus. Wählen Sie dann Grant (Erteilen) aus.
  - Wählen Sie im Navigationsbereich unter Datenkatalog die Option Kataloge aus. Wählen Sie dann ein Katalogobjekt (Kataloge, Datenbanken, Tabellen und Datenfilter) aus, wählen Sie im Menü Aktionen unter Berechtigungen die Option Gewähren aus.
3. Wählen Sie auf der Seite Berechtigungen gewähren die Option Principals by attribute aus.
4. Geben Sie den Attributschlüssel und den Wert (e) an. Wenn Sie mehr als einen Wert wählen, erstellen Sie einen Attributausdruck mit einem OR Operator. Das heißt, wenn einer der Attribut-Tag-Werte, die einer IAM-Rolle oder einem IAM-Benutzer zugewiesen sind, übereinstimmt, role/user erhält der Benutzer Zugriffsberechtigungen für die Ressource.

Wenn Sie mehr als ein Attribut-Tag angeben, erstellen Sie einen Attributausdruck mit einem AND Operator. Dem Prinzipal werden nur dann Berechtigungen für eine Datenkatalogressource gewährt, wenn dem IAM für jedes Attribut-Tag im Attributausdruck ein passendes Tag zugewiesen role/user wurde.

Überprüfen Sie den resultierenden Cedar-Richtlinienausdruck, der in der Konsole angezeigt wird.

## Grant permissions

### Principal type

Grant access by IAM principal or attribute tags.



#### Principals

Grant permissions directly to specific IAM users, roles, or Identity Center principals.



#### Principals by attributes

Grant permissions using attribute tags with Cedar policy expressions.

### Attributes

Grant permissions using an attribute expression based on user, resource, and contextual attributes.

#### Attribute expression

Add tag key-value pairs from IAM roles or [IAM session tags](#). Separate values with commas. **AND** logic applies between pairs, **OR** logic within keys. Verify tag entries for accuracy.

Key

Value

Add key-value pair

#### Expression review

The attribute expression above will be written in the following Cedar policy. Use CLI/SDK to edit or write custom Cedar policy.

```
permit (principal, action, resource)
when {
 context.iam.principalTags.hasTag("Department")
 && context.iam.principalTags.getTag("Department") == "sales"
};
```

#### Permission scope



This account



External account

- Wählen Sie den Umfang der Berechtigungen aus. Wenn die Empfänger einem externen Konto angehören, wählen Sie Externes Konto und geben Sie die AWS Konto-ID ein.
- Wählen Sie als Nächstes das Datenkatalogkonto oder das Konto für externe Konten aus. Sie müssen über die entsprechenden erteilbaren Berechtigungen für die Ressourcen verfügen, um die Genehmigungen erfolgreich abschließen zu können.

7. Geben Sie an, welche Aktionen Sie für Prinzipale (Benutzer oder Rollen) mit übereinstimmenden Attributen zulassen möchten. Zugriff erhalten IAM-Entitäten, denen Tags und Werte zugewiesen wurden, die mindestens einem Ihrer angegebenen Attributausdrücke entsprechen. Überprüfen Sie den Cedar-Richtlinienausdruck in der Konsole. Weitere Informationen zu Cedar finden Sie unter [Was ist Cedar? | Sprachreferenz für Cedar Policy GuideLink](#).
8. Wählen Sie als Nächstes die Datenkatalogressourcen aus, denen Sie Zugriff gewähren möchten. Sie können diese Berechtigungen für verschiedene Datenkatalogressourcen definieren, darunter Kataloge, Datenbanken, Tabellen und Datenfilter.
9. Wählen Sie Grant (Erteilen).

Mit diesem Ansatz können Sie den Zugriff anhand von Attributen steuern und so sicherstellen, dass nur Benutzer oder Rollen mit den entsprechenden Tags bestimmte Aktionen mit den angegebenen Ressourcen ausführen können.

### Erteilen von Berechtigungen mithilfe von ABAC (AWS CLI)

Das folgende Beispiel zeigt einen Attributausdruck, der erfüllt sein muss, um alle verfügbaren Berechtigungen für die Ressource zu erhalten. Sie können auch individuelle Berechtigungen angeben `Select`, z. B. `Describe`, oder `Drop`. Der Ausdruck verwendet den Cedar-Richtlinienausdruck. Weitere Informationen zu Cedar finden Sie unter [Was ist Cedar? | Sprachreferenz für Cedar Policy GuideLink](#).

Diese Bedingung prüft, ob der IAM-Principal über ein `department` Tag verfügt und der `department` Tag-Wert gleich `sales` ist.

```
aws lakeformation grant-permissions
--principal '{"DataLakePrincipalIdentifier": "111122223333:IAMPrincipals"}' \
--resource '{"Database": {"CatalogId": 111122223333, "Name": "abac-db"}}' \
--permissions ALL \
--condition '{"Expression": "context.iam.principalTags.hasTag(\"department\") \
&& context.iam.principalTags.getTag(\"department\") == \"sales\""}'
```

## Beispielszenario für Berechtigungen

Das folgende Szenario zeigt, wie Sie Berechtigungen einrichten können, um den Zugriff auf Daten in zu sichern AWS Lake Formation.

Shirley ist Datenadministratorin. Sie möchte einen Data Lake für ihr Unternehmen einrichten, AnyCompany. Derzeit werden alle Daten in Amazon S3 gespeichert. John ist Marketingmanager und benötigt Schreibzugriff auf die Einkaufsinformationen von Kunden (enthalten in `s3://customerPurchases`). Diego, ein Marketinganalyst, kommt diesen Sommer zu John. John benötigt die Möglichkeit, Diego Zugriff zu gewähren, damit er Abfragen an den Daten durchführen kann, ohne Shirley einzubeziehen.

Mateo aus der Finanzabteilung benötigt Zugriff, um Buchhaltungsdaten abzufragen (zum Beispiels `s3://transactions`). Er möchte die Transaktionsdaten in Tabellen in einer Datenbank (Finance\_DB) abfragen, die das Finanzteam verwendet. Sein Manager, Arnav, kann ihm Zugriff auf die Finance\_DB gewähren. Er sollte zwar nicht in der Lage sein, Buchhaltungsdaten zu ändern, aber er muss in der Lage sein, Daten in ein Format (Schema) zu konvertieren, das für Prognosen geeignet ist. Diese Daten werden in einem separaten Bucket (`s3://financeForecasts`) gespeichert, den er ändern kann.

Um es zusammenzufassen:

- Shirley ist der Data Lake-Administrator.
- John benötigt eine `CREATE_DATABASE CREATE_TABLE` Genehmigung, um neue Datenbanken und Tabellen im Datenkatalog zu erstellen.
- John benötigt außerdem `SELECT, INSERT`, und `DELETE` Berechtigungen für Tabellen, die er erstellt.
- Diego benötigt `SELECT` Berechtigungen für die Tabelle, um Abfragen ausführen zu können.

Die Mitarbeiter von AnyCompany führen die folgenden Aktionen durch, um Berechtigungen einzurichten. Die in diesem Szenario gezeigten API-Operationen weisen aus Gründen der Übersichtlichkeit eine vereinfachte Syntax auf.

1. Shirley registriert den Amazon S3 S3-Pfad mit Kundenkaufinformationen bei Lake Formation.

```
RegisterResource(ResourcePath("s3://customerPurchases"), false, Role_ARN)
```

2. Shirley gewährt John Zugriff auf den Amazon S3-Pfad, der die Kaufinformationen der Kunden enthält.

```
GrantPermissions(John, S3Location("s3://customerPurchases"),
[DATA_LOCATION_ACCESS]))
```

3. Shirley erteilt John die Erlaubnis, Datenbanken zu erstellen.

```
GrantPermissions(John, catalog, [CREATE_DATABASE])
```

- John erstellt die Datenbank John\_DB. John hat automatisch die CREATE\_TABLE Erlaubnis für diese Datenbank, weil er sie erstellt hat.

```
CreateDatabase(John_DB)
```

- John erstellt die Tabelle, John\_Table auf die verweist s3://customerPurchases. Da er die Tabelle erstellt hat, hat er alle Berechtigungen für sie und kann Berechtigungen für sie erteilen.

```
CreateTable(John_DB, John_Table)
```

- John gewährt seinem Analysten Diego Zugriff auf die Tabelle John\_Table.

```
GrantPermissions(Diego, John_Table, [SELECT])
```

- John gewährt seinem Analysten Diego Zugriff auf dies s3://customerPurchases/London/. Da Shirley sich bereits registriert hat s3://customerPurchases, sind seine Unterordner bei Lake Formation registriert.

```
GrantDataLakePrivileges(123456789012/datalake, Diego, [DATA_LOCATION_ACCESS], [],
S3Location("s3://customerPurchases/London/"))
```

- John erlaubt seinem Analysten Diego, Tabellen in einer Datenbank zu erstellen. John\_DB

```
GrantDataLakePrivileges(123456789012/datalake, Diego, John_DB, [CREATE_TABLE],
[])
```

- Diego erstellt eine Tabelle in John\_DB at s3://customerPurchases/London/ und erhält automatisch ALTER, DROP, SELECT, INSERT, und DELETE Berechtigungen.

```
CreateTable(123456789012/datalake, John_DB, Diego_Table)
```

## Datenfilterung und Sicherheit auf Zellebene in Lake Formation

Wenn Sie Lake Formation-Berechtigungen für eine Datenkatalogtabelle gewähren, können Sie Datenfilterspezifikationen hinzufügen, um den Zugriff auf bestimmte Daten in Abfrageergebnissen und in Lake Formation integrierten Engines einzuschränken. Lake Formation verwendet

Datenfilterung, um Sicherheit auf Spaltenebene, Sicherheit auf Zeilenebene und Sicherheit auf Zellebene zu erreichen. Sie können Datenfilter definieren und auf verschachtelte Spalten anwenden, wenn Ihre Quelldaten verschachtelte Strukturen enthalten.

Mit den Datenfilterfunktionen von Lake Formation können Sie die folgenden Datensicherheitsstufen implementieren.

### Sicherheit auf Spaltenebene

Durch die Gewährung von Berechtigungen für eine Datenkatalogtabelle mit Sicherheit auf Spaltenebene (Spaltenfilterung) können Benutzer nur bestimmte Spalten und verschachtelte Spalten anzeigen, auf die sie in der Tabelle Zugriff haben. Stellen Sie sich eine `persons` Tabelle vor, die in mehreren Anwendungen für ein großes Kommunikationsunternehmen mit mehreren Regionen verwendet wird. Durch die Gewährung von Berechtigungen für Datenkatalogtabellen mit Spaltenfilterung können Benutzer, die nicht in der Personalabteilung arbeiten, daran gehindert werden, personenbezogene Daten (PII) wie Sozialversicherungsnummer oder Geburtsdatum einzusehen. Sie können auch Sicherheitsrichtlinien definieren und nur teilweisen Unterstrukturen von verschachtelten Spalten Zugriff gewähren.

### Sicherheit auf Zeilenebene

Durch die Gewährung von Berechtigungen für eine Datenkatalogtabelle mit Sicherheit auf Zeilenebene (Zeilensfilterung) können Benutzer nur bestimmte Datenzeilen anzeigen, auf die sie in der Tabelle Zugriff haben. Die Filterung basiert auf den Werten einer oder mehrerer Spalten. Sie können bei der Definition von Zeilenfilterausdrücken verschachtelte Spaltenstrukturen einbeziehen. Wenn beispielsweise verschiedene Regionalbüros des Kommunikationsunternehmens über eigene Personalabteilungen verfügen, können Sie die Personendatensätze, die Mitarbeiter der Personalabteilung einsehen können, auf Datensätze beschränken, die nur für Mitarbeiter in ihrer Region verfügbar sind.

### Sicherheit auf Zellebene

Die Sicherheit auf Zellebene kombiniert Zeilen- und Spaltenfilterung für ein hochflexibles Berechtigungsmodell. Wenn Sie die Zeilen und Spalten einer Tabelle als Raster betrachten, können Sie mithilfe der Sicherheit auf Zellebene den Zugriff auf einzelne Elemente (Zellen) des Rasters an beliebiger Stelle in den beiden Dimensionen einschränken. Das heißt, Sie können den Zugriff auf verschiedene Spalten je nach Zeile einschränken. Dies wird durch das folgende Diagramm veranschaulicht, in dem eingeschränkte Spalten schattiert sind.



|      | Col1 | Col2 | Col3 | Col4 | Col5 | Col6 |
|------|------|------|------|------|------|------|
| Row1 |      |      |      |      |      |      |
| Row2 |      |      |      |      |      |      |
| Row3 |      |      |      |      |      |      |
| Row4 |      |      |      |      |      |      |
| Row5 |      |      |      |      |      |      |

Wenn Sie das Beispiel der Personentabelle fortsetzen, können Sie auf Zellenebene einen Datenfilter erstellen, der den Zugriff auf die Spalte mit der Straßenadresse einschränkt, wenn die Spalte mit dem Land in der Zeile auf „Großbritannien“ gesetzt ist, aber den Zugriff auf die Spalte mit der Straßenadresse ermöglicht, wenn die Spalte mit dem Land in der Zeile auf „US“ gesetzt ist.

Filter gelten nur für Lesevorgänge. Daher können Sie nur die SELECT Lake Formation Formation-Genehmigung mit Filtern erteilen.

### Sicherheit auf Zellenebene für verschachtelte Spalten

Lake Formation ermöglicht es Ihnen, Datenfilter mit Sicherheit auf Zellebene für verschachtelte Spalten zu definieren und anzuwenden. Die integrierten Analyse-Engines wie Amazon Athena, Amazon EMR und Amazon Redshift Spectrum unterstützen jedoch die Ausführung von Abfragen für von Lake Formation verwaltete verschachtelte Tabellen mit Sicherheit auf Zeilen- und Spaltenebene.

Einschränkungen finden Sie unter [Einschränkungen bei der Datenfilterung](#).

### Themen

- [Datenfilter in Lake Formation](#)
- [PartiQL-Unterstützung in Zeilenfilterausdrücken](#)
- [Erforderliche Berechtigungen für das Abfragen von Tabellen mit Filterung auf Zellenebene](#)
- [Datenfilter verwalten](#)

## Datenfilter in Lake Formation

Sie können die Sicherheit auf Spalten-, Zeilen- und Zellenebene implementieren, indem Sie Datenfilter erstellen. Sie wählen einen Datenfilter aus, wenn Sie der SELECT Lake Formation die Berechtigung für Tabellen erteilen. Wenn Ihre Tabelle verschachtelte Spaltenstrukturen enthält, können Sie einen Datenfilter definieren, indem Sie die untergeordneten Spalten ein- oder ausschließen und Filterausdrücke auf Zeilenebene für verschachtelte Attribute definieren.

Jeder Datenfilter gehört zu einer bestimmten Tabelle in Ihrem Datenkatalog. Ein Datenfilter enthält die folgenden Informationen:

- Name des Filters
- Der Katalog IDs der Tabelle, die dem Filter zugeordnet ist
- Name der Tabelle
- Name der Datenbank, die die Tabelle enthält
- Spaltenspezifikation — eine Liste von Spalten und verschachtelten Spalten (mit `struct` Datentypen), die in Abfrageergebnissen ein- oder ausgeschlossen werden sollen.
- Zeilenfilterausdruck — ein Ausdruck, der die Zeilen angibt, die in die Abfrageergebnisse aufgenommen werden sollen. Mit einigen Einschränkungen hat der Ausdruck die Syntax einer WHERE Klausel in der PartiQL-Sprache. Um alle Zeilen anzugeben, wählen Sie in der Konsole unter Zugriff auf Zeilenebene die Option Zugriff auf alle Zeilen oder in API-Aufrufen verwenden `AllRowsWildcard` aus.

Weitere Informationen darüber, was in Zeilenfilterausdrücken unterstützt wird, finden Sie unter [PartiQL-Unterstützung in Zeilenfilterausdrücken](#)

Die Stufe der Filterung, die Sie erhalten, hängt davon ab, wie Sie den Datenfilter auffüllen.

- Wenn Sie den Platzhalter „Alle Spalten“ angeben und einen Zeilen-Filter-Ausdruck angeben, richten Sie nur Sicherheit auf Zeilen-Ebene (Zeilenfilterung) ein.
- Wenn Sie bestimmte Spalten und verschachtelte Spalten ein- oder ausschließen und „Alle Zeilen“ mit dem Platzhalter „Alle Zeilen“ angeben, richten Sie nur Sicherheit auf Spaltenebene ein (Spaltenfilterung).
- Wenn Sie bestimmte Spalten ein- oder ausschließen und auch einen Zeilen-Filter-Ausdruck bereitstellen, stellen Sie Sicherheit auf Zellen-Ebene her (Zell-Filterung).

Der folgende Screenshot aus der Lake Formation Formation-Konsole zeigt einen Datenfilter, der eine Filterung auf Zellebene durchführt. Bei Abfragen in der `orders` Tabelle wird der Zugriff auf die `customer_name` Spalte eingeschränkt, und die Abfrageergebnisse geben nur Zeilen zurück, in denen die `product_type` Spalte „Pharma“ enthält.

## Create data filter



### Data filter name

Enter a name that describes this data access filter.

restrict-pharma

Name may contain letters (A-Z), numbers (0-9), hyphens (-), or under-scores (\_), and be less than 256 characters.

### Target database

Select the database that contains the target table.

Choose databases



Load more

sales



054881201579

### Target table

Select the table for which the data filter will be created.

Choose tables



Load more

orders



054881201579

### Column-level access

Choose whether this filter should have column-level restrictions.

- ☐ Access to all columns  
Filter won't have any column restrictions.
- ☐ Include columns  
Filter will only allow access to specific columns.
- ☒ Exclude columns  
Filter will allow access to all but specific columns.

### Select columns

Choose one or more columns



customer\_name



string

Beachten Sie die Verwendung von einfachen Anführungszeichen, um das Zeichenkettenliteral, einzuschließen. 'pharma'

Sie können die Lake Formation Formation-Konsole verwenden, um diesen Datenfilter zu erstellen, oder Sie können das folgende Anforderungsobjekt für den CreateDataCellsFilter API-Vorgang bereitstellen.

```
{
 "Name": "restrict-pharma",
 "DatabaseName": "sales",
 "TableName": "orders",
 "TableCatalogId": "111122223333",
 "RowFilter": {"FilterExpression": "product_type='pharma'"},
 "ColumnWildcard": {
 "ExcludedColumnNames": ["customer_name"]
 }
}
```

Sie können so viele Datenfilter erstellen, wie Sie für eine Tabelle benötigen. Dazu benötigen Sie eine SELECT Genehmigung mit der Grant-Option für eine Tabelle. Data Lake-Administratoren sind standardmäßig berechtigt, Datenfilter für alle Tabellen in diesem Konto zu erstellen. Normalerweise verwenden Sie nur eine Teilmenge der möglichen Datenfilter, wenn Sie einem Prinzipal Berechtigungen für die Tabelle erteilen. Sie könnten beispielsweise einen zweiten Datenfilter für die orders Tabelle erstellen, bei dem es sich um einen row-security-only Datenfilter handelt. Unter Bezugnahme auf den vorherigen Screenshot könnten Sie die Option Zugriff auf alle Spalten wählen und einen Zeilenfilterausdruck von hinzufügenproduct\_type<>pharma. Der Name dieses Datenfilters könnte lautenno-pharma. Er schränkt den Zugriff auf alle Zeilen ein, deren product\_type Spalte auf „Pharma“ gesetzt ist.

Das Anforderungsobjekt für den CreateDataCellsFilter API-Vorgang für diesen Datenfilter ist das Folgende.

```
{
 "Name": "no-pharma",
 "DatabaseName": "sales",
 "TableName": "orders",
 "TableCatalogId": "111122223333",
 "RowFilter": {"FilterExpression": "product_type<>'pharma'"},
 "ColumnNames": ["customer_id", "customer_name", "order_num",
 "product_id", "purchase_date", "product_type",
```

```
}
 "product_manufacturer", "quantity", "price"]
}
```

Sie könnten dann für die `orders` Tabelle mit dem `restrict-pharma` Datenfilter einem Administratorbenutzer und für die `orders` Tabelle mit `SELECT` dem `no-pharma` Datenfilter für Benutzer ohne Administratorrechte gewähren `SELECT`. Benutzern im Gesundheitswesen würden Sie für die `orders` Tabelle vollen Zugriff `SELECT` auf alle Zeilen und Spalten gewähren (kein Datenfilter) oder vielleicht mit einem weiteren Datenfilter, der den Zugriff auf Preisinformationen einschränkt.

Sie können verschachtelte Spalten ein- oder ausschließen, wenn Sie innerhalb eines Datenfilters die Sicherheit auf Spalten- und Zeilenebene angeben. Im folgenden Beispiel wird der Zugriff auf das `product.offer` Feld mithilfe qualifizierter Spaltennamen (in doppelte Anführungszeichen) angegeben. Dies ist wichtig für verschachtelte Felder, um Fehler zu vermeiden, die auftreten, wenn Spaltennamen Sonderzeichen enthalten, und um die Abwärtskompatibilität mit den Sicherheitsdefinitionen der obersten Ebene auf Spaltenebene aufrechtzuerhalten.

```
{
 "Name": "example_dcf",
 "DatabaseName": "example_db",
 "TableName": "example_table",
 "TableCatalogId": "111122223333",
 "RowFilter": { "FilterExpression": "customer.customerName <> 'John'" },
 "ColumnNames": ["customer", "\"product\".\"offer\""]
}
```

 Weitere Informationen finden Sie auch unter

- [Datenfilter verwalten](#)

## PartiQL-Unterstützung in Zeilenfilterausdrücken

Sie können Zeilenfilterausdrücke mithilfe einer Teilmenge von PartiQL-Datentypen, Operatoren und Aggregationen erstellen. Lake Formation erlaubt keine benutzerdefinierten oder standardmäßigen PartiQL-Funktionen im Filterausdruck. Sie können Vergleichsoperatoren verwenden, um Spalten mit Konstanten zu vergleichen (z. B. `views >= 10000`), aber Sie können Spalten nicht mit anderen Spalten vergleichen.

Ein Zeilenfilterausdruck kann ein einfacher Ausdruck oder ein zusammengesetzter Ausdruck sein. Die Gesamtlänge des Ausdrucks muss weniger als 2048 Zeichen betragen.

### Einfacher Ausdruck

Ein einfacher Ausdruck wird das folgende Format haben: `<column name > <comparison operator ><value >`

- Name der Spalte

Dabei kann es sich entweder um eine Datenspalte der obersten Ebene, eine Partitionsspalte oder eine verschachtelte Spalte handeln, die im Tabellenschema vorhanden ist und zu den unten [Unterstützte Datentypen](#) aufgeführten gehören muss.

- Vergleichsoperator

Die folgenden Operatoren werden unterstützt: `=`, `>`, `<`, `>=`, `<=`, `<>`, `!=`, `BETWEEN`, `IN`, `LIKE`, `NOT`, `IS [NOT] NULL`

- Bei allen Zeichenkettenvergleichen und `LIKE` Mustervergleichen wird zwischen Groß- und Kleinschreibung unterschieden. Sie können den `IS [NOT] NULL`-Operator nicht für Partitionsspalten verwenden.
- Spaltenwert

Der Spaltenwert muss dem Datentyp des Spaltennamens entsprechen.

### Zusammengesetzter Ausdruck

Ein zusammengesetzter Ausdruck hat das Format: `( <simple expression >) <AND/OR >(<simple expression >)`. Zusammengesetzte Ausdrücke können mit logischen Operatoren weiter kombiniert werden `AND/OR`.

### Unterstützte Datentypen

Zeilenfilter, die auf eine AWS Glue Data Catalog Tabelle verweisen, die Datentypen enthält, die nicht unterstützt werden, führen zu einem Fehler. Im Folgenden sind die unterstützten Datentypen für Tabellenspalten und Konstanten aufgeführt, die Datentypen zugeordnet Amazon Redshift sind:

- `STRING`, `CHAR`, `VARCHAR`
- `INT`, `LONG`, `BIGINT`, `FLOAT`, `DECIMAL`, `DOUBLE`
- `BOOLEAN`

- STRUCT

Weitere Informationen zu Datentypen in Amazon Redshift finden Sie unter [Datentypen](#) im Amazon Redshift Database Developer Guide.

## Ausdrücke zum Filtern von Zeilen

### Example

Im Folgenden finden Sie Beispiele für gültige Zeilenfilterausdrücke für eine Tabelle mit Spalten: `country` (String), `id` (Long), `year` (partition column of type Integer), `month` (partition column of type Integer)

- `year > 2010 and country != 'US'`
- `(year > 2010 and country = 'US') or (month < 8 and id > 23)`
- `(country between 'Z' and 'U') and (year = 2018)`
- `(country like '%ited%') and (year > 2000)`

### Example

Im Folgenden finden Sie gültige Beispiele für Zeilenfilterausdrücke für eine Tabelle mit verschachtelten Spalten: `year > 2010 and customer.customerId <> 1`

Verschachtelte Felder unter Partitionsspalten sollten bei der Definition von verschachtelten Ausdrücken auf Zeilenebene nicht referenziert werden.

Zeichenkettenkonstanten müssen in einfache Anführungszeichen eingeschlossen werden.

## Reservierte Schlüsselwörter

Wenn Ihr Zeilenfilterausdruck PartiQL-Schlüsselwörter enthält, erhalten Sie einen Analysefehler, da Spaltennamen mit den Schlüsselwörtern in Konflikt geraten können. In diesem Fall maskieren Sie die Spaltennamen, indem Sie doppelte Anführungszeichen verwenden. Einige Beispiele für reservierte Schlüsselwörter sind „first“, „last“, „asc“, „missing“. Eine Liste der reservierten Schlüsselwörter finden Sie in der PartiQL-Spezifikation.

## PartiQL-Referenz

Weitere Hinweise zu PartiQL finden Sie unter <https://partiql.org/>.

## Erforderliche Berechtigungen für das Abfragen von Tabellen mit Filterung auf Zellenebene

Die folgenden AWS Identity and Access Management (IAM-) Berechtigungen sind erforderlich, um Abfragen für Tabellen mit Filterung auf Zellenebene auszuführen.

JSON

```
{
 "Version": "2012-10-17",
 "Statement": [
 {
 "Effect": "Allow",
 "Action": [
 "lakeformation:StartQueryPlanning",
 "lakeformation:GetQueryState",
 "lakeformation:GetWorkUnits",
 "lakeformation:GetWorkUnitResults"
],
 "Resource": "*"
 }
]
}
```

Weitere Informationen zu Lake Formation Formation-Berechtigungen finden Sie unter [Referenz zu Personas und IAM-Berechtigungen in Lake Formation](#).

## Datenfilter verwalten

Um Sicherheit auf Spalten-, Zeilen- und Zellenebene zu implementieren, können Sie Datenfilter erstellen und verwalten. Jeder Datenfilter gehört zu einer Datenkatalogtabelle. Sie können mehrere Datenfilter für eine Tabelle erstellen und dann einen oder mehrere davon verwenden, wenn Sie Berechtigungen für die Tabelle gewähren. Sie können auch Datenfilter für verschachtelte Spalten mit `struct` Datentypen definieren und anwenden, sodass Benutzer nur auf Unterstrukturen verschachtelter Spalten zugreifen können.

Um einen Datenfilter zu erstellen oder anzuzeigen, benötigen Sie eine SELECT entsprechende Genehmigung mit der Option „Gewähren“. Um den Hauptbenutzern in Ihrem Konto das Anzeigen



und Verwenden eines Datenfilters zu ermöglichen, können Sie ihm die DESCRIBE entsprechende Berechtigung erteilen.

 Note

Lake Formation unterstützt nicht die Erteilung von Describe Berechtigungen für einen Datenfilter, der von einem anderen Konto aus geteilt wird.

Sie können Datenfilter mithilfe der AWS Lake Formation Konsole, der API oder der AWS Command Line Interface (AWS CLI) verwalten.

Hinweise zu Datenfiltern finden Sie unter [Datenfilter in Lake Formation](#)

## Einen Datenfilter erstellen

Sie können einen oder mehrere Datenfilter für jede Datenkatalogtabelle erstellen.

Um einen Datenfilter für eine Datenkatalogtabelle (Konsole) zu erstellen

1. Öffnen Sie die Lake Formation Konsole unter <https://console.aws.amazon.com/lakeformation/>.

Melden Sie sich als Data Lake-Administrator, Besitzer der Zieltabelle oder als Principal an, der über eine Lake Formation-Berechtigung für die Zieltabelle verfügt.

2. Wählen Sie im Navigationsbereich unter Datenkatalog die Option Datenfilter aus.
3. Wählen Sie auf der Seite Datenfilter die Option Neuen Filter erstellen aus.
4. Geben Sie im Dialogfeld Datenfilter erstellen die folgenden Informationen ein:
  - Name des Datenfilters
  - Zieldatenbank — Geben Sie die Datenbank an, die die Tabelle enthält.
  - Zieltabelle
  - Zugriff auf Spaltenebene — Belassen Sie diese Einstellung auf Zugriff auf alle Spalten, um nur die Zeilenfilterung festzulegen. Wählen Sie Spalten einschließen oder Spalten ausschließen, um die Spalten- oder Zellenfilterung festzulegen, und geben Sie dann die Spalten an, die ein- oder ausgeschlossen werden sollen.

**Verschachtelte Spalten** — Wenn Sie den Filter auf eine Tabelle anwenden, die verschachtelte Spalten enthält, können Sie explizit Unterstrukturen der verschachtelten Strukturspalten innerhalb eines Datenfilters angeben.

Wenn Sie einem Prinzipal die SELECT-Berechtigung für diesen Filer gewähren, sieht der Principal, der die folgende Abfrage ausführt, nur die Daten für und nicht.

```
customer.customerName customer.customerId
```

```
SELECT "customer" FROM "example_db"."example_table";
```

### Column-level access

Choose whether this filter should have column-level restrictions.

#### Column-level access

Choose whether this filter should have column-level restrictions.

- ☐ Access to all columns
- Filter won't have any column restrictions.
- ☒ Include columns
- Filter will only allow access to specific columns.
- ☐ Exclude columns
- Filter will allow access to all but specific columns.

### Included columns (4/11)

Choose the columns for column-level access

Find column

< 1 >

| <div><div></div></div>              | Name                           | Type   |
|-------------------------------------|--------------------------------|--------|
| <input type="checkbox"/>            | <div>customer</div>            | struct |
| <input type="checkbox"/>            | customerId                     | string |
| <input checked="" type="checkbox"/> | customerName                   | string |
| <input checked="" type="checkbox"/> | <div>customerapplication</div> | struct |
| <input type="checkbox"/>            | appId                          | string |
| <input checked="" type="checkbox"/> | <div>product</div>             | struct |
| <input type="checkbox"/>            | <div>offer</div>               | struct |
| <input type="checkbox"/>            | listingId                      | string |
| <input type="checkbox"/>            | prodId                         | string |
| <input type="checkbox"/>            | type                           | string |
| <input checked="" type="checkbox"/> | purchaseId                     | string |

### Row-level access

Choose whether this filter should have row-level restrictions.

- ☐ Access to all rows
- ☒ Filter rows

#### Row filter expression

Enter the rest of the following query statement `SELECT * FROM nested-table WHERE...`  
Please see the documentation for examples of filter expressions.

customer.customerName <> 'John'

Wenn Sie Berechtigungen für die `customer` Spalte erteilen, erhält der Principal Zugriff auf die Spalte und die verschachtelten Felder unter der Spalte (`customerName` und `customerID`).

- **Zeilenfilterausdruck** — Geben Sie einen Filterausdruck ein, um die Zeilen- oder Zellenfilterung festzulegen. Informationen zu unterstützten Datentypen und Operatoren finden Sie unter [PartiQL-Unterstützung in Zeilenfilterausdrücken](#). Wählen Sie Zugriff auf alle Zeilen, um Zugriff auf alle zu gewähren.

Sie können teilweise Spaltenstrukturen aus verschachtelten Spalten in einen Zeilenfilterausdruck einbeziehen, um Zeilen zu filtern, die einen bestimmten Wert enthalten.

Wenn einem Prinzipal Berechtigungen für eine Tabelle mit einem Zeilenfilterausdruck gewährt werden und der Zugriff auf Spaltenebene auf Zugriff auf alle Spalten festgelegt ist `Select *` from `example_nestedtable` where `customer.customerName <> 'John'`, werden in den Abfrageergebnissen nur Zeilen angezeigt, deren `customerName <> 'John'` Auswertung den Wert `True` ergibt.

Der folgende Screenshot zeigt einen Datenfilter, der die Zellfilterung implementiert. Bei Abfragen der `orders` Tabelle wird der Zugriff auf die `customer_name` Spalte verweigert und es werden nur Zeilen angezeigt, die „Pharma“ in der `product_type` Spalte enthalten.

## Create data filter



### Data filter name

Enter a name that describes this data access filter.

restrict-pharma

Name may contain letters (A-Z), numbers (0-9), hyphens (-), or under-scores (\_), and be less than 256 characters.

### Target database

Select the database that contains the target table.

Choose databases



Load more

sales



054881201579

### Target table

Select the table for which the data filter will be created.

Choose tables



Load more

orders



054881201579

### Column-level access

Choose whether this filter should have column-level restrictions.

- ☐ Access to all columns  
Filter won't have any column restrictions.
- ☐ Include columns  
Filter will only allow access to specific columns.
- ☒ Exclude columns  
Filter will allow access to all but specific columns.

### Select columns

Choose one or more columns



customer\_name  
string



## 5. Wählen Sie Create Filter) (Filter erstellen.

Um einen Datenfilter mit Zellfilterrichtlinien für ein verschachteltes Feld zu erstellen

In diesem Abschnitt wird anhand des folgenden Beispielschemas veranschaulicht, wie ein Datenzellenfilter erstellt wird:

```
[
 { name: "customer", type: "struct<customerId:string,customerName:string>" },
 { name: "customerApplication", type: "struct<appId:string>" },
 { name: "product", type:
"struct<offer:struct<prodId:string,listingId:string>,type:string>" },
 { name: "purchaseId", type: "string" },
]
```

1. Geben Sie auf der Seite Datenfilter erstellen einen Namen für den Datenfilter ein.
2. Verwenden Sie als Nächstes die Dropdownliste, um einen Datenbanknamen und einen Tabellennamen auszuwählen.
3. Wählen Sie im Abschnitt Zugriff auf Spaltenebene die Option Eingeschlossene Spalten und wählen Sie eine verschachtelte Spalte () aus. `customer.customerName`
4. Wählen Sie im Abschnitt Zugriff auf Zeilenebene die Option Zugriff auf alle Zeilen aus.
5. Wählen Sie Create Filter) (Filter erstellen.

Wenn Sie die SELECT Berechtigung für diesen Filter erteilen, erhält der Principal Zugriff auf alle Zeilen in der `customerName` Spalte.

6. Definieren Sie als Nächstes einen weiteren Datenfilter für dieselbe Datenbank/Tabelle.
7. Wählen Sie im Abschnitt Zugriff auf Spaltenebene die Option Eingeschlossene Spalten und wählen Sie eine weitere verschachtelte Spalte aus (). `customer.customerid`
8. Wählen Sie im Abschnitt Zugriff auf Zeilenebene die Option Zeilen filtern aus und geben Sie einen Zeilenfilterausdruck () ein. `customer.customerid <> 5`
9. Wählen Sie Create Filter) (Filter erstellen.

Wenn Sie die SELECT Berechtigung für diesen Filter erteilen, erhält der Principal Zugriff auf alle Zeilen in den `customerId` Feldern und mit Ausnahme der Zeile `customerName`, in der der Wert 5 in der `customerId` Spalte ist.

## Erteilen von Datenfilterberechtigungen

Sie können Prinzipalen die Berechtigungen `SELECT`, `DESCRIBE` und `DROP` Lake Formation für Datenfilter gewähren.

Zunächst können nur Sie die Datenfilter anzeigen, die Sie für eine Tabelle erstellen. Damit ein anderer Principal einen Datenfilter anzeigen und Datenkatalogberechtigungen für den Datenfilter gewähren kann, müssen Sie entweder:

- Gewähren Sie `SELECT` dem Prinzipal mit der `Grant`-Option in einer Tabelle und wenden Sie den Datenfilter auf den Zuschuss an.
- Erteilen Sie dem Prinzipal die `DROP` Berechtigung `DESCRIBE` oder für den Datenfilter.

Sie können die `SELECT` Erlaubnis einem externen AWS Konto erteilen. Ein Data Lake-Administrator in diesem Konto kann diese Berechtigung dann anderen Prinzipalen im Konto gewähren. Wenn Sie die Erteilung an ein externes Konto vornehmen, müssen Sie die Option „Erteilen“ angeben, damit der Administrator des externen Kontos die Berechtigung weiter an andere Benutzer im his/her Konto weitergeben kann. Wenn Sie die Gewährung an einen Hauptbenutzer in Ihrem Konto vornehmen, ist die Gewährung mit der `Grant`-Option optional.

Sie können Berechtigungen für Datenfilter mithilfe der AWS Lake Formation Konsole, der API oder der AWS Command Line Interface (AWS CLI) gewähren und widerrufen.

### Console

1. Melden Sie sich bei der an AWS-Managementkonsole und öffnen Sie die Lake Formation Formation-Konsole unter <https://console.aws.amazon.com/lakeformation/>.
2. Wählen Sie im Navigationsbereich unter Berechtigungen die Option Data Lake-Berechtigungen aus.
3. Wählen Sie auf der Seite Berechtigungen im Abschnitt Datenberechtigungen die Option `Grant` aus.
4. Wählen Sie auf der Seite Datenberechtigungen gewähren die Principals aus, denen die Berechtigungen erteilt werden sollen.
5. Wählen Sie im Abschnitt LF-Tags oder Katalogressourcen die Option Benannte Datenkatalogressourcen aus. Wählen Sie dann die Datenbank, Tabelle und den Datenfilter aus, für die Sie Berechtigungen erteilen möchten.

### LF-Tags or catalog resources

☐ Resources matched by LF-Tags (recommended)  
Manage permissions indirectly for resources or data matched by a specific set of LF-Tags.

☒ Named data catalog resources  
Manager permissions for specific databases or tables, in addition to fine-grained data access.

#### Databases

Select one or more databases.

Choose databases ▼

cloudtrail 106567286946 ✕

Load more

#### Tables - optional

Select one or more tables.

Choose tables ▼

cloudtrail\_logs\_awslogs 106567286946 ✕

Load more

#### Data filters - optional

Select one or more data filters.

Choose data filters ▼

cloudtrail\_lakeformation\_filter 106567286946 ✕

Load more

Create new

[Manage data filters](#) ↗

6. Wählen Sie im Abschnitt Datenfilterberechtigungen die Berechtigungen aus, die Sie den ausgewählten Prinzipalen gewähren möchten.

### Data filter permissions

#### Data filter permissions

Choose specific access permissions to grant.

☐ Select ☒ Describe ☒ Drop

#### Grantable permissions

Choose the permission that may be granted to others.

☐ Select ☐ Describe ☐ Drop



## AWS CLI

- Geben Sie einen `grant-permissions` Befehl ein. Geben Sie `DataCellsFilter` für das `resource` Argument an und geben Sie `DESCRIBE` oder `DROP` für das `Permissions` Argument und optional für das `PermissionsWithGrantOption` Argument an.

Im folgenden Beispiel wird dem Benutzer `datalake_user1` auf `DESCRIBE` dem Datenfilter `restrict-pharma`, der zur `orders` Tabelle in der `sales` Datenbank im AWS Konto 1111-2222-3333 gehört, Genehmigungen mit der Grant-Option gewährt.

```
aws lakeformation grant-permissions --cli-input-json file://grant-params.json
```

Im Folgenden ist der Inhalt der Datei aufgeführt. `grant-params.json`

```
{
 "Principal": {"DataLakePrincipalIdentifier":
 "arn:aws:iam::111122223333:user/datalake_user1"},
 "Resource": {
 "DataCellsFilter": {
 "TableCatalogId": "111122223333",
 "DatabaseName": "sales",
 "TableName": "orders",
 "Name": "restrict-pharma"
 }
 },
 "Permissions": ["DESCRIBE"],
 "PermissionsWithGrantOption": ["DESCRIBE"]
}
```

## Erteilen von Datenberechtigungen, die durch Datenfilter bereitgestellt werden

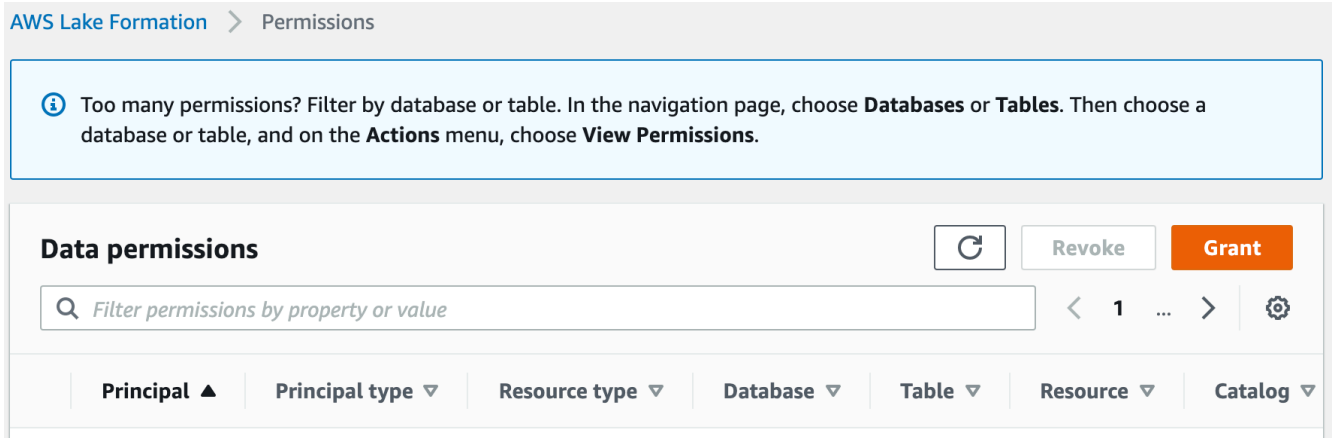
Datenfilter stellen eine Teilmenge von Daten innerhalb einer Tabelle dar. Um Prinzipalen Datenzugriff zu gewähren, müssen diesen Prinzipalen `SELECT` Berechtigungen erteilt werden. Mit dieser Genehmigung können die Principals:

- Den tatsächlichen Tabellennamen in der Liste der Tabellen anzeigen, die mit ihrem Konto geteilt wurden.
- Erstellen Sie Datenfilter für die gemeinsam genutzte Tabelle und gewähren Sie ihren Benutzern Berechtigungen für diese Datenfilter.

## Console

### Um SELECT-Berechtigungen zu gewähren

1. Rufen Sie in der Lake Formation Formation-Konsole die Seite „Berechtigungen“ auf und wählen Sie dann Grant aus.



2. Wählen Sie die Prinzipale aus, auf die Sie Zugriff gewähren möchten, und wählen Sie Benannte Datenkatalogressourcen aus.

### LF-Tags or catalog resources

☐ Resources matched by LF-Tags (recommended)  
Manage permissions indirectly for resources or data matched by a specific set of LF-Tags.

☒ Named data catalog resources  
Manager permissions for specific databases or tables, in addition to fine-grained data access.

#### Databases

Select one or more databases.

Choose databases ▼

cloudtrail  
106567286946 ✕

Load more

#### Tables - optional

Select one or more tables.

Choose tables ▼

cloudtrail\_logs\_awslogs ✕  
106567286946

Load more

#### Data filters - optional

Select one or more data filters.

Choose data filters ▼

cloudtrail\_lakeformation\_filter ✕  
106567286946

Load more

Create new

[Manage data filters](#) 

- Um Zugriff auf die Daten zu gewähren, die der Filter darstellt, wählen Sie unter Datenfilterberechtigungen die Option Auswählen aus.

### Data filter permissions

#### Data filter permissions

Choose specific access permissions to grant.

☒ Select
 ☐ Describe
 ☐ Drop

#### Grantable permissions

Choose the permission that may be granted to others.

☐ Select
 ☐ Describe
 ☐ Drop

Select permissions on data filters will grant access to the table 'cloudtrail\_logs\_awslogs'.

## CLI

Geben Sie einen Befehl ein. `grant-permissions` Geben Sie `DataCellsFilter` für das Argument `Ressource` und `SELECT` für das Argument `Berechtigungen` an.

Das folgende Beispiel gewährt `SELECT` dem Benutzer `datalake_user1` mit der `Grant-Option` `Berechtigungen` für den `Datenfilterrestrict-pharma`, der zu der `orders` Tabelle in der `sales` Datenbank gehört AWS-Konto `1111-2222-3333`.

```
aws lakeformation grant-permissions --cli-input-json file://grant-params.json
```

Im Folgenden finden Sie den Inhalt der Datei `grant-params.json`.

```
{
 "Principal": {
 "DataLakePrincipalIdentifier": "arn:aws:iam::111122223333:user/datalake_user1"
 },
 "Resource": {
 "DataCellsFilter": {
 "TableCatalogId": "111122223333",
 "DatabaseName": "sales",
 "TableName": "orders",
 "Name": "restrict-pharma"
 }
 },
}
```

```
"Permissions": ["SELECT"]
}
```

## Datenfilter anzeigen

Sie können die Lake Formation Formation-Konsole oder die Lake Formation Formation-API verwenden, um Datenfilter anzuzeigen. AWS CLI

Um Datenfilter anzeigen zu können, müssen Sie ein Data Lake-Administrator sein oder über die erforderlichen Berechtigungen für die Datenfilter verfügen.

### Console

1. Melden Sie sich bei der an AWS-Managementkonsole und öffnen Sie die Lake Formation Formation-Konsole unter <https://console.aws.amazon.com/lakeformation/>.
2. Wählen Sie im Navigationsbereich unter Datenkatalog die Option Datenfilter aus.

Auf der Seite werden die Datenfilter angezeigt, auf die Sie Zugriff haben.

Data filters (1)

View

Delete

Create new filter

Find filter

<

1

>

Filter name

Table

Database

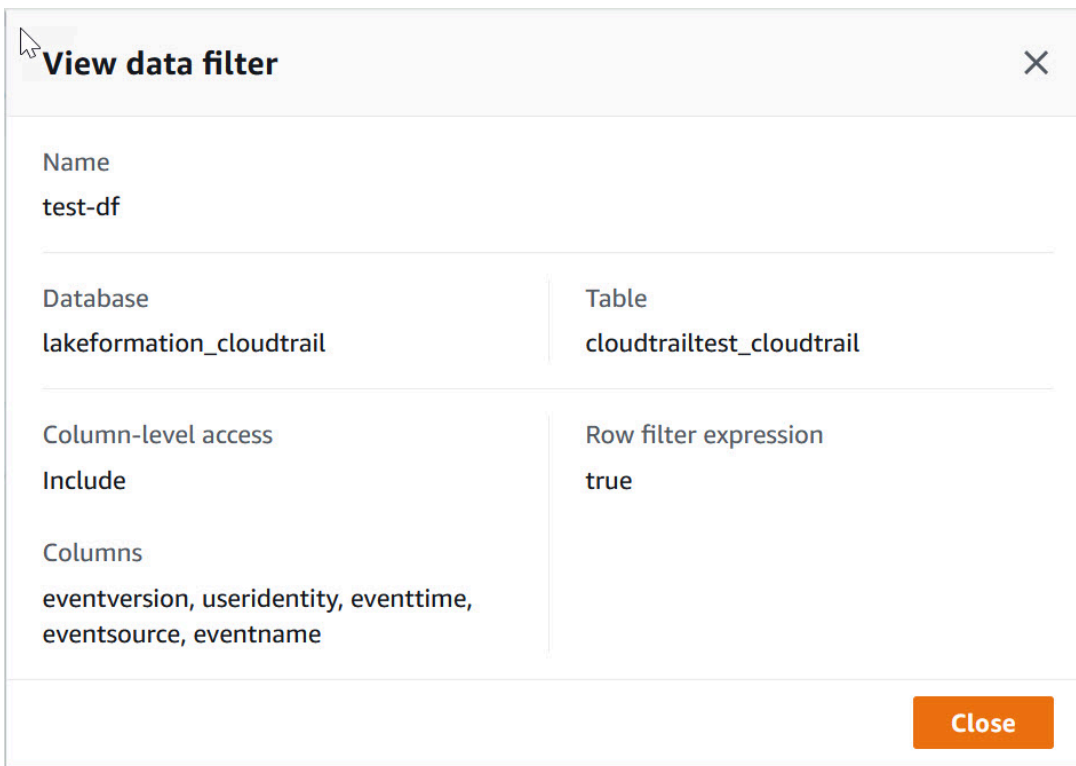
Table catalog ID

test-df

cloudtrailtest\_cloudtrail

lakeformation\_cloudtrail

3. Um die Datenfilterdetails anzuzeigen, wählen Sie den Datenfilter und dann Ansicht aus. Ein neues Fenster mit detaillierten Informationen zum Datenfilter wird angezeigt.



The image shows a 'View data filter' dialog box. It has a title bar with a close button (X). The dialog is divided into several sections: 'Name' with the value 'test-df'; 'Database' with 'lakeformation\_cloudtrail' and 'Table' with 'cloudtrailtest\_cloudtrail'; 'Column-level access' with 'Include' and 'Row filter expression' with 'true'; and 'Columns' with a list of column names: 'eventversion, useridentity, eventtime, eventsource, eventname'. A 'Close' button is at the bottom right.

## AWS CLI

Geben Sie einen `list-data-cells-filter` Befehl ein und geben Sie eine Tabellenressource an.

Das folgende Beispiel listet die Datenfilter für die `cloudtrailtest_cloudtrail` Tabelle auf.

```
aws lakeformation list-data-cells-filter --table '{ "CatalogId":"123456789012",
"DatabaseName":"lakeformation_cloudtrail", "Name":"cloudtrailtest_cloudtrail"}
```

## API/SDK

Verwenden Sie die `ListDataCellsFilter` API und geben Sie eine Tabellenressource an.

Das folgende Beispiel verwendet Python, um die ersten 20 Datenfilter für die `myTable` Tabelle aufzulisten.

```
response = client.list_data_cells_filter(
 Table = {
 'CatalogId': '111122223333',
 'DatabaseName': 'mydb',
 'Name': 'myTable'
```

```
},
MaxResults=20
)
```

## Datenfilterberechtigungen auflisten

Sie können die Lake Formation Formation-Konsole verwenden, um die für Datenfilter erteilten Berechtigungen anzuzeigen.

Um die Berechtigungen für einen Datenfilter anzeigen zu können, müssen Sie ein Data Lake-Administrator sein oder über die erforderlichen Berechtigungen für den Datenfilter verfügen.

### Console

1. Melden Sie sich bei der an AWS-Managementkonsole und öffnen Sie die Lake Formation Formation-Konsole unter <https://console.aws.amazon.com/lakeformation/>.
2. Wählen Sie im Navigationsbereich unter Berechtigungen die Option Datenberechtigungen aus.
3. Klicken oder tippen Sie auf der Seite Datenberechtigungen in das Suchfeld und wählen Sie im Menü Eigenschaften die Option Ressourcentyp aus.
4. Wählen Sie im Menü Ressourcentyp die Option Ressourcentyp: Datenzellenfilter aus.

Die Datenfilter, für die Sie Berechtigungen haben, werden aufgelistet. Möglicherweise müssen Sie horizontal scrollen, um die Spalten Permissions und Granttable zu sehen.

| Data Permissions (58)                |                  |          |        |                 |              |                        |  |
|--------------------------------------|------------------|----------|--------|-----------------|--------------|------------------------|--|
| Principal                            | Resource type    | Database | Table  | Resource        | Catalog      | Permissions            |  |
| <input type="radio"/> datalake_admin | Data cell filter | sales    | orders | no-pharma       | 111122223333 | Describe, Drop, Select |  |
| <input type="radio"/> datalake_admin | Data cell filter | sales    | orders | restrict-pharma | 111122223333 | Describe, Drop, Select |  |
| <input type="radio"/> datalake_user1 | Data cell filter | sales    | orders | restrict-pharma | 111122223333 | Describe               |  |
| <input type="radio"/> datalake_user2 | Data cell filter | sales    | orders | restrict-pharma | 111122223333 | Select                 |  |

### AWS CLI

- Geben Sie einen `list-permissions` Befehl ein. Geben Sie `DataCellsFilter` für das `resource` Argument an und geben Sie `DESCRIBE` oder `DROP` für das `Permissions` Argument und optional für das `PermissionsWithGrantOption` Argument an.

Das folgende Beispiel listet DESCRIBE Berechtigungen mit der Grant-Option für den Datenfilter aufrestrict-pharma. Die Ergebnisse beschränken sich auf Berechtigungen, die für den Prinzipal datalake\_user1 und die orders Tabelle in der sales Datenbank im AWS Konto 1111-2222-3333 erteilt wurden.

```
aws lakeformation list-permissions --cli-input-json file://list-params.json
```

Im Folgenden finden Sie den Inhalt der Datei. grant-params.json

```
{
 "Principal": {"DataLakePrincipalIdentifier":
 "arn:aws:iam::111122223333:user/datalake_user1"},
 "Resource": {
 "DataCellsFilter": {
 "TableCatalogId": "111122223333",
 "DatabaseName": "sales",
 "TableName": "orders",
 "Name": "restrict-pharma"
 }
 },
 "Permissions": ["DESCRIBE"],
 "PermissionsWithGrantOption": ["DESCRIBE"]
}
```

## Datenbank- und Tabellenberechtigungen in Lake Formation anzeigen

Sie können die Lake Formation Berechtigungen anzeigen, die für eine Datenkatalogdatenbank oder -Tabelle erteilt wurden. Sie können dies tun, indem Sie die Lake Formation Konsole, die API oder die AWS Command Line Interface (AWS CLI) verwenden.

Mithilfe der Konsole können Sie Berechtigungen auf den Seiten Datenbanken oder Tabellen oder auf der Seite Datenberechtigungen anzeigen.



 Note

Wenn Sie kein Datenbankadministrator oder Ressourcenbesitzer sind, können Sie die Berechtigungen anderer Principals für die Ressource nur anzeigen, wenn Sie über eine Lake Formation Formation-Berechtigung für die Ressource mit der Grant-Option verfügen. Zusätzlich zu den erforderlichen Lake Formation Formation-Berechtigungen benötigen Sie die AWS Identity and Access Management (IAM-) Berechtigungen `glue:GetDatabases`, `glue:GetDatabase`, `glue:GetTables`, `glue:GetTable`, und `lakeformation:ListPermissions`.

Um die Berechtigungen für eine Datenbank anzuzeigen (Konsole, ab der Datenbankseite)

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

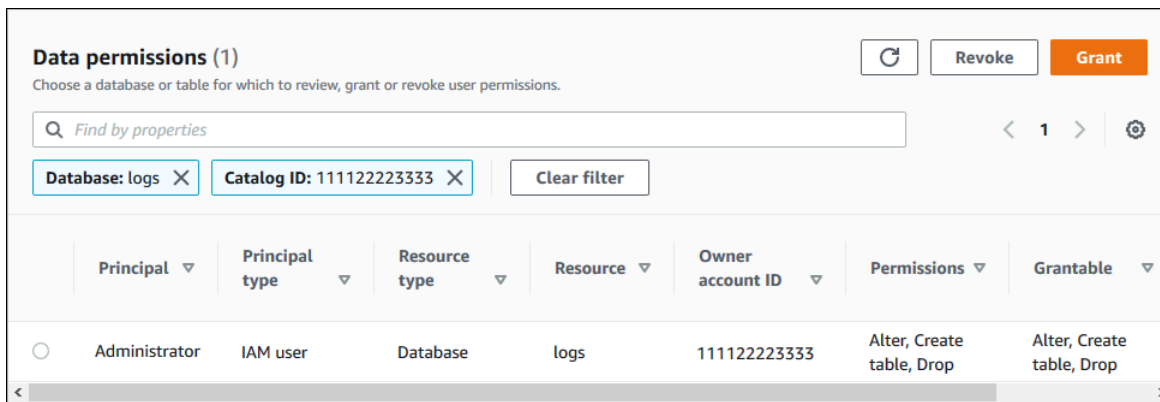
Melden Sie sich mit der Grant-Option als Data Lake-Administrator, Datenbankersteller oder als Benutzer an, der über eine Lake Formation Formation-Berechtigung für die Datenbank verfügt.

2. Wählen Sie im Navigationsbereich Datenbanken aus.
3. Wählen Sie eine Datenbank aus und klicken Sie im Menü Aktionen auf Berechtigungen anzeigen.

 Note

Wenn Sie einen Datenbankressourcenlink wählen, zeigt Lake Formation die Berechtigungen für den Ressourcenlink an, nicht für die Zieldatenbank des Ressourcenlinks.

Auf der Seite Datenberechtigungen werden alle Lake Formation Formation-Berechtigungen für die Datenbank aufgeführt. Der Datenbankname und die Katalog-ID (AWS Konto-ID) des Datenbankbesitzers werden als Bezeichnungen unter dem Suchfeld angezeigt. Die Kacheln weisen darauf hin, dass ein Filter angewendet wurde, um nur die Berechtigungen für diese Datenbank aufzulisten. Sie können den Filter anpassen, indem Sie eine Kachel schließen oder Filter löschen wählen.



So zeigen Sie die Berechtigungen für eine Datenbank an (Konsole, ausgehend von der Seite mit den Datenberechtigungen)

1. Öffnen Sie die Lake Formation Konsole unter <https://console.aws.amazon.com/lakeformation/>.

Melden Sie sich mit der Grant-Option als Data Lake-Administrator, Datenbankersteller oder als Benutzer an, der über eine Lake Formation Berechtigung für die Datenbank verfügt.

2. Wählen Sie im Navigationsbereich die Option Datenberechtigungen aus.
3. Platzieren Sie den Cursor im Suchfeld oben auf der Seite, und wählen Sie im daraufhin angezeigten Eigenschaftenmenü die Option Datenbank aus.
4. Wählen Sie im daraufhin angezeigten Menü Datenbanken eine Datenbank aus.

#### Note

Wenn Sie einen Datenbankressourcenlink wählen, zeigt Lake Formation die Berechtigungen für den Ressourcenlink an, nicht für die Zieldatenbank des Ressourcenlinks.

Auf der Seite Datenberechtigungen werden alle Lake Formation Berechtigungen für die Datenbank aufgeführt. Der Datenbankname wird als Kachel unter dem Suchfeld angezeigt. Die Kachel gibt an, dass ein Filter angewendet wurde, um Berechtigungen nur für diese Datenbank aufzulisten. Sie können den Filter entfernen, indem Sie die Kachel schließen oder Filter löschen wählen.

So zeigen Sie die Berechtigungen für eine Tabelle an (Konsole, ausgehend von der Tabellenseite)

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

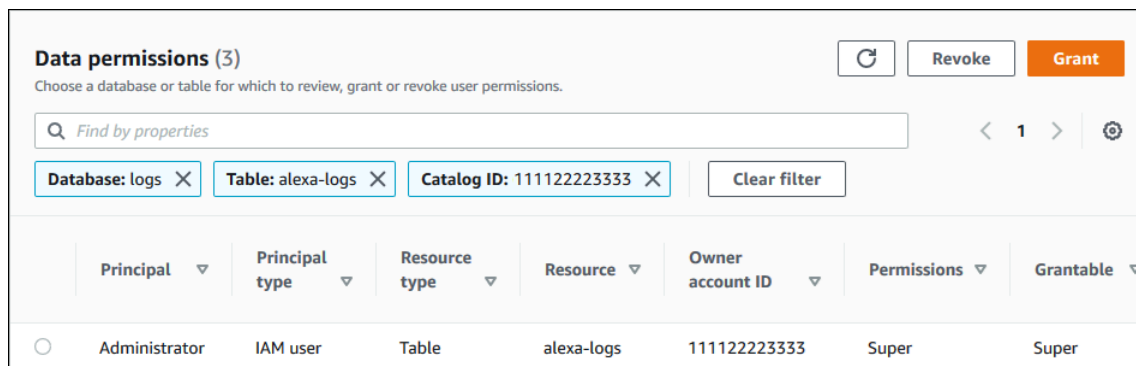
Melden Sie sich mit der Grant-Option als Data Lake-Administrator, Tabellenersteller oder als Benutzer an, der über eine Lake Formation Formation-Berechtigung für die Tabelle verfügt.

2. Wählen Sie im Navigationsbereich Tables (Tabellen) aus.
3. Wählen Sie eine Tabelle aus und klicken Sie im Menü Aktionen auf Berechtigungen anzeigen.

#### Note

Wenn Sie einen Tabellenressourcen-Link wählen, zeigt Lake Formation die Berechtigungen für den Ressourcenlink an, nicht für die Zieltabelle des Ressourcenlinks.

Auf der Seite Datenberechtigungen werden alle Lake Formation Formation-Berechtigungen für die Tabelle aufgeführt. Der Tabellename, der Datenbankname der Datenbank, die die Tabelle enthält, und die Katalog-ID (AWS Konto-ID) des Tabellenbesitzers werden als Beschriftungen unter dem Suchfeld angezeigt. Die Beschriftungen weisen darauf hin, dass ein Filter angewendet wurde, um nur die Berechtigungen für diese Tabelle aufzulisten. Sie können den Filter anpassen, indem Sie ein Label schließen oder Filter löschen wählen.



| Principal                           | Principal type | Resource type | Resource   | Owner account ID | Permissions | Grantable |
|-------------------------------------|----------------|---------------|------------|------------------|-------------|-----------|
| <input type="radio"/> Administrator | IAM user       | Table         | alexa-logs | 111122223333     | Super       | Super     |

So zeigen Sie Berechtigungen für eine Tabelle an (Konsole, ausgehend von der Seite mit den Datenberechtigungen)

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

Melden Sie sich mit der Grant-Option als Data Lake-Administrator, Tabellenersteller oder als Benutzer an, der über eine Lake Formation Formation-Berechtigung für die Tabelle verfügt.

2. Wählen Sie im Navigationsbereich die Option Datenberechtigungen aus.
3. Platzieren Sie den Cursor im Suchfeld oben auf der Seite, und wählen Sie im daraufhin angezeigten Eigenschaftenmenü die Option Datenbank aus.
4. Wählen Sie im daraufhin angezeigten Menü Datenbanken eine Datenbank aus.

 Important

Wenn Sie die Berechtigungen für eine Tabelle anzeigen möchten, die von einem externen AWS Konto aus für Ihr Konto freigegeben wurde, müssen Sie die Datenbank in dem externen Konto auswählen, das die Tabelle enthält, und keinen Ressourcenlink zur Datenbank.

Auf der Seite Datenberechtigungen werden alle Lake Formation Formation-Berechtigungen für die Datenbank aufgeführt.

5. Positionieren Sie den Cursor erneut im Suchfeld, und wählen Sie im daraufhin angezeigten Eigenschaftenmenü die Option Tabelle aus.
6. Wählen Sie im daraufhin angezeigten Menü Tabellen eine Tabelle aus.

Auf der Seite Datenberechtigungen werden alle Lake Formation Formation-Berechtigungen für die Tabelle aufgeführt. Der Tabellename und der Datenbankname der Datenbank, die die Tabelle enthält, werden als Kacheln unter dem Suchfeld angezeigt. Die Kacheln weisen darauf hin, dass ein Filter angewendet wurde, um nur die Berechtigungen für diese Tabelle aufzulisten. Sie können den Filter anpassen, indem Sie eine Kachel schließen oder Filter löschen wählen.

Um die Berechtigungen für eine Tabelle anzuzeigen (AWS CLI)

- Geben Sie einen `list-permissions` Befehl ein.

Das folgende Beispiel listet die Berechtigungen für eine Tabelle auf, die von einem externen Konto gemeinsam genutzt wird. Die `CatalogId` Eigenschaft ist die AWS Konto-ID des externen Kontos, und der Datenbankname bezieht sich auf die Datenbank im externen Konto, die die Tabelle enthält.

```
aws lakeformation list-permissions --resource-type TABLE --resource '{ "Table":
{"DatabaseName":"logs", "Name":"alex-log", "CatalogId":"123456789012"} }'
```

## Widerrufen der Genehmigung mithilfe der Lake Formation Formation-Konsole

Sie können die Konsole verwenden, um alle Arten von Lake Formation Formation-Berechtigungen zu widerrufen — Datenkatalogberechtigungen, Policy-Tag-Berechtigungen, Datenfilterberechtigungen und Standortberechtigungen.

So entziehen Sie Lake Formation Formation-Berechtigungen für eine Ressource (Konsole)

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

Melden Sie sich als Data Lake-Administrator oder als Benutzer an, dem Berechtigungen mit der Grant-Option für die Ressource erteilt wurden.

2. Wählen Sie im Navigationsbereich unter Berechtigungen die Option Data Lake-Berechtigungen, LF-Tags und Berechtigungen oder Datenspeicherorte aus.
3. Wählen Sie die Berechtigung oder den Speicherort aus und wählen Sie dann Widerrufen aus.
4. Wählen Sie in dem sich öffnenden Dialogfeld die Option Widerrufen aus.

## Kontoübergreifender Datenaustausch in Lake Formation

Die kontoübergreifenden Funktionen von Lake Formation ermöglichen es Benutzern AWS-Konten, verteilte Data Lakes sicher über mehrere AWS Organisationen hinweg oder direkt mit IAM-Prinzipalen in einem anderen Konto gemeinsam zu nutzen, wodurch ein detaillierter Zugriff auf die Data Catalog-Metadaten und die zugrunde liegenden Daten ermöglicht wird. Große Unternehmen verwenden in der Regel mehrere AWS-Konten, und viele dieser Konten benötigen möglicherweise Zugriff auf einen Data Lake, der von einem einzigen verwaltet wird. AWS-Konto Benutzer und ETL-Jobs ( AWS Glue Extrahieren, Transformieren und Laden) können Tabellen über mehrere Konten hinweg abfragen und verknüpfen und dabei trotzdem die Vorteile des Datenschutzes auf Tabellen- und Spaltenebene von Lake Formation nutzen.

Wenn Sie Lake Formation-Berechtigungen für eine Datenkatalogressource einem externen Konto oder direkt einem IAM-Prinzipal in einem anderen Konto gewähren, verwendet Lake Formation den Dienst AWS Resource Access Manager (AWS RAM), um die Ressource gemeinsam zu nutzen. Befindet sich das Konto des Empfängers in derselben Organisation wie das Konto des Zuweisungsempfängers, steht die gemeinsam genutzte Ressource dem Empfänger sofort zur Verfügung. Wenn sich das Empfängerkonto nicht in derselben Organisation befindet, AWS RAM sendet es eine Einladung an das Empfängerkonto, die Ressourcenzuweisung anzunehmen oder abzulehnen. Um die gemeinsam genutzte Ressource verfügbar zu machen, muss der Data Lake-Administrator des Empfängerkontos dann die AWS RAM Konsole verwenden oder die AWS CLI Einladung annehmen.

Lake Formation unterstützt die gemeinsame Nutzung von Datenkatalogressourcen mit externen Konten im Hybridzugriffsmodus. Der Hybridzugriffsmodus bietet die Flexibilität, selektiv Lake Formation-Berechtigungen für Datenbanken und Tabellen in Ihrem AWS Glue Data Catalog zu aktivieren.

Mit dem Hybridzugriffsmodus verfügen Sie jetzt über einen inkrementellen Pfad, mit dem Sie Lake Formation-Berechtigungen für eine bestimmte Gruppe von Benutzern festlegen können, ohne die Berechtigungsrichtlinien anderer vorhandener Benutzer oder Workloads zu unterbrechen.

Weitere Informationen finden Sie unter [Hybrider Zugriffsmodus](#).

## Direkter kontenübergreifender Austausch

Autorisierte Principals können Ressourcen explizit mit einem IAM-Prinzipal in einem externen Konto teilen. Diese Funktion ist nützlich, wenn ein Kontoinhaber die Kontrolle darüber haben möchte, wer im externen Konto auf die Ressourcen zugreifen kann. Bei den Berechtigungen, die der IAM-Principal erhält, handelt es sich um eine Kombination aus direkten Zuschüssen und Zuschüssen auf Kontoebene, die an die Hauptbenutzer weitergegeben werden. Nur der Empfänger der Genehmigung kann die direkten kontenübergreifenden Zuschüsse einsehen. Der Hauptbenutzer, der den Ressourcenanteil erhält, kann die Ressource nicht mit anderen Prinzipalen teilen.

## Methoden für die gemeinsame Nutzung von Datenkatalogressourcen

Mit einem einzigen Lake Formation Grant-Vorgang können Sie kontenübergreifende Berechtigungen für die folgenden Datenkatalogressourcen gewähren.

- Eine Datenbank
- Eine einzelne Tabelle (mit optionaler Spaltenfilterung)
- Ein paar ausgewählte Tabellen

- Alle Tabellen in einer Datenbank (mithilfe des Platzhalters „Alle Tabellen“)

Es gibt zwei Möglichkeiten, Ihre Datenbanken und Tabellen für andere Benutzer AWS-Konto oder für IAM-Prinzipale in einem anderen Konto gemeinsam zu nutzen.

- Tag-basierte Zugriffskontrolle von Lake Formation (LF-TBAC) (empfohlen)

Die tagbasierte Zugriffskontrolle von Lake Formation ist eine Autorisierungsstrategie, die Berechtigungen auf der Grundlage von Attributen definiert. Sie können die tagbasierte Zugriffskontrolle verwenden, um Datenkatalogressourcen (Datenbanken, Tabellen und Spalten) mit externen IAM-Prinzipalen AWS-Konten, Organizations und Organisationseinheiten () gemeinsam zu nutzen. OUs In Lake Formation werden diese Attribute LF-Tags genannt. Weitere Informationen finden Sie unter [Verwaltung eines Data Lakes mithilfe der tagbasierten Zugriffskontrolle von Lake Formation](#).

#### Note

Die LF-TBAC-Methode zur Erteilung von Datenkatalogberechtigungen wird für kontoübergreifende Zuschüsse verwendet. AWS Resource Access Manager Lake Formation unterstützt jetzt die Gewährung kontenübergreifender Berechtigungen für Organizations und Organisationseinheiten mithilfe der LF-TBAC-Methode. Um diese Funktion zu aktivieren, müssen Sie die Einstellungen für die kontoübergreifende Version auf Version 3 oder höher aktualisieren. Weitere Informationen finden Sie unter [Aktualisierung der Versionseinstellungen für die kontenübergreifende gemeinsame Nutzung von Daten](#).

- Lake Formation benannte Ressourcen

Die Methode zur kontenübergreifenden Datenfreigabe von Lake Formation mithilfe benannter Ressourcen ermöglicht es Ihnen, Lake Formation Formation-Berechtigungen mit einer Erteilungsoption für Datenkatalogtabellen und Datenbanken an externe AWS-Konten IAM-Prinzipale, Organisationen oder Organisationseinheiten zu gewähren. Bei der Gewährung werden diese Ressourcen automatisch gemeinsam genutzt.

 Note

Sie können dem AWS Glue Crawler auch gestatten, mithilfe von Lake Formation Anmeldeinformationen auf einen Datenspeicher in einem anderen Konto zuzugreifen. Weitere Informationen finden Sie unter [Kontoübergreifendes Crawling](#) im AWS Glue Entwicklerhandbuch.

Integrierte Dienste wie Athena und Amazon Redshift Spectrum benötigen Ressourcenlinks, um gemeinsam genutzte Ressourcen in Abfragen einbeziehen zu können. Weitere Informationen zu Ressourcenlinks finden Sie unter [Funktionsweise von Ressourcenverbindungen in Lake Formation](#)

Hinweise und Einschränkungen finden Sie unter [Bewährte Methoden und Überlegungen für den kontenübergreifenden Datenaustausch](#).

## Themen

- [Voraussetzungen](#)
- [Aktualisierung der Versionseinstellungen für die kontenübergreifende gemeinsame Nutzung von Daten](#)
- [Gemeinsame Nutzung von Datenkatalogtabellen und Datenbanken für mehrere AWS-Konten IAM-Prinzipale von externen Konten aus](#)
- [Erteilen von Berechtigungen für eine Datenbank oder Tabelle, die mit Ihrem Konto geteilt wird](#)
- [Erteilen von Ressourcenverknüpfungsberechtigungen](#)
- [Zugreifen auf die zugrunde liegenden Daten einer gemeinsam genutzten Tabelle](#)
- [Kontoübergreifende Protokollierung CloudTrail](#)
- [Verwaltung kontenübergreifender Berechtigungen sowohl AWS Glue mit Lake Formation als auch mit Lake Formation](#)
- [Alle kontenübergreifenden Zuschüsse mithilfe des GetResourceShares API-Vorgangs anzeigen](#)

 Verwandte Themen

- [Überblick über die Genehmigungen für Lake Formation](#)
- [Zugreifen auf und Anzeigen von gemeinsam genutzten Datenkatalogtabellen und Datenbanken](#)



- [Ressourcenlinks erstellen](#)
- [Problembehandlung beim kontoübergreifenden Zugriff](#)

## Voraussetzungen

Bevor Ihr AWS Konto Datenkatalogressourcen (Kataloge, Datenbanken und Tabellen) mit einem anderen Konto oder Principals in einem anderen Konto gemeinsam nutzen kann und bevor Sie auf die mit Ihrem Konto geteilten Ressourcen zugreifen können, müssen die folgenden Voraussetzungen erfüllt sein.

Allgemeine Anforderungen an die kontenübergreifende gemeinsame Nutzung von Daten

- Um Datenkatalogdatenbanken und -Tabellen im Hybridzugriffsmodus gemeinsam zu nutzen und Objekte in den Verbundkatalogen gemeinsam zu nutzen, müssen Sie die Einstellungen für die kontoübergreifende Version auf Version 4 aktualisieren.
- Bevor Sie kontenübergreifende Berechtigungen für eine Datenkatalogressource gewähren, müssen Sie der IAMAllowedPrincipals Gruppe alle Lake Formation Formation-Berechtigungen für die Ressource entziehen. Wenn der aufrufende Principal kontoübergreifende Berechtigungen für den Zugriff auf eine Ressource hat und die IAMAllowedPrincipals Berechtigung für die Ressource vorhanden ist, wird Lake Formation ausgelöst. AccessDeniedException

Diese Anforderung gilt nur, wenn Sie den zugrunde liegenden Datenstandort im Lake Formation Formation-Modus registrieren. Wenn Sie den Datenstandort im Hybridmodus registrieren, können die IAMAllowedPrincipals Gruppenberechtigungen für die gemeinsam genutzte Datenbank oder Tabelle vorhanden sein.

- Bei Datenbanken, die Tabellen enthalten, die Sie gemeinsam nutzen möchten, müssen Sie verhindern, dass für neue Tabellen die Standardzuteilung Super bis festgelegt wirdIAMAllowedPrincipals. Bearbeiten Sie in der Lake Formation Formation-Konsole die Datenbank und deaktivieren Sie Nur IAM-Zugriffskontrolle für neue Tabellen in dieser Datenbank verwenden, oder geben Sie den folgenden AWS CLI Befehl ein und database ersetzen Sie ihn durch den Namen der Datenbank. Wenn der zugrunde liegende Datenspeicherort im Hybridzugriffsmodus registriert ist, müssen Sie diese Standardeinstellung nicht ändern. Im Hybridzugriffsmodus ermöglicht Ihnen Lake Formation die selektive Durchsetzung Lake Formation Formation-Berechtigungen und IAM-Berechtigungsrichtlinien für Amazon S3 und AWS Glue für dieselbe Ressource.

```
aws glue update-database --name database --database-input
'{"Name": "database", "CreateTableDefaultPermissions": []}'
```

- Um kontoübergreifende Berechtigungen zu gewähren, muss der Gewährer über die erforderlichen AWS Identity and Access Management (IAM-) Berechtigungen für den Dienst verfügen. AWS Glue AWS RAM Die AWS verwaltete Richtlinie AWSLakeFormationCrossAccountManager gewährt die erforderlichen Berechtigungen.

Für Data Lake-Administratoren mit Konten, die gemeinsam genutzte Ressourcen nutzen, AWS RAM muss die folgende zusätzliche Richtlinie gelten. Sie ermöglicht es dem Administrator, Einladungen zur gemeinsamen AWS RAM Nutzung von Ressourcen anzunehmen. Es ermöglicht dem Administrator auch, die gemeinsame Nutzung von Ressourcen mit Organisationen zu aktivieren.

JSON

```
{
 "Version": "2012-10-17",
 "Statement": [
 {
 "Effect": "Allow",
 "Action": [
 "ram:AcceptResourceShareInvitation",
 "ram:RejectResourceShareInvitation",
 "ec2:DescribeAvailabilityZones",
 "ram:EnableSharingWithAwsOrganization"
],
 "Resource": "*"
 }
]
}
```

- Wenn Sie Datenkatalogressourcen für unsere Organisationseinheiten gemeinsam nutzen möchten, muss die gemeinsame Nutzung für Organisationen in aktiviert sein AWS RAM. AWS Organizations

Informationen zum Aktivieren der gemeinsamen Nutzung mit Organisationen finden Sie unter [Aktivieren der gemeinsamen Nutzung mit AWS Organisationen](#) im AWS RAM Benutzerhandbuch.

Sie müssen über die `ram:EnableSharingWithAwsOrganization` entsprechende Berechtigung verfügen, um das Teilen mit Organisationen zu aktivieren.

- Um Ressourcen direkt mit einem IAM-Prinzipal in einem anderen Konto gemeinsam zu nutzen, müssen Sie die Einstellungen für die kontoübergreifende Version auf Version 3 aktualisieren. Diese Einstellung ist auf der Seite mit den Datenkatalogeinstellungen verfügbar. Wenn Sie Version 1 verwenden, lesen Sie die Anweisungen zum Aktualisieren der Einstellung [Aktualisierung der Versionseinstellungen für die kontoübergreifende gemeinsame Nutzung von Daten](#).
- Sie können Datenkatalogressourcen, die mit einem vom AWS Glue Service verwalteten Schlüssel verschlüsselt wurden, nicht mit einem anderen Konto teilen. Sie können nur Datenkatalogressourcen gemeinsam nutzen, die mit dem Verschlüsselungsschlüssel des Kunden verschlüsselt wurden, und das Konto, das die gemeinsame Nutzung der Ressource erhält, muss über Berechtigungen für den Datenkatalog-Verschlüsselungsschlüssel verfügen, um die Objekte zu entschlüsseln.

#### Kontoübergreifender Datenaustausch unter Verwendung der LF-TBAC-Anforderungen

- Um Datenkatalogressourcen mit AWS Organizations Organisationseinheiten (OUs) gemeinsam zu nutzen, müssen Sie die Einstellungen für die kontoübergreifende Version auf Version 3 oder höher aktualisieren.
- Um Datenkatalogressourcen mit Version 3 der Einstellungen der kontoübergreifenden Version gemeinsam nutzen zu können, benötigt der Gewährer die IAM-Berechtigungen, die in der AWS verwalteten Richtlinie `AWSLakeFormationCrossAccountManager` in Ihrem Konto definiert sind.
- Wenn Sie Version 1 oder Version 2 der Einstellungen für die kontoübergreifende Version verwenden, benötigen Sie eine Datenkatalog-Ressourcenrichtlinie (`glue:PutResourcePolicy`), die LF-TBAC aktiviert. Weitere Informationen finden Sie unter [Verwaltung kontoübergreifender Berechtigungen sowohl AWS Glue mit Lake Formation als auch mit Lake Formation](#).
- Wenn Sie derzeit eine AWS Glue Datenkatalog-Ressourcenrichtlinie für die gemeinsame Nutzung von Ressourcen verwenden und mithilfe von Version 3 der Einstellungen für die kontoübergreifende Version kontoübergreifende Berechtigungen gewähren möchten, müssen Sie die `glue:ShareResource` Berechtigung in den Datenkatalogeinstellungen mithilfe der `glue:PutResourcePolicy` API-Operation hinzufügen, wie im Abschnitt gezeigt. [Verwaltung kontoübergreifender Berechtigungen sowohl AWS Glue mit Lake Formation als auch mit Lake Formation](#) Diese Richtlinie ist nicht erforderlich, wenn Ihr Konto mithilfe der AWS Glue Datenkatalog-Ressourcenrichtlinie (`glue:PutResourcePolicy`) Nutzungsberechtigung Version 1

und Version 2) keine kontoübergreifenden Berechtigungen gewährt hat, um kontenübergreifenden Zugriff zu gewähren.

```
{
 "Effect": "Allow",
 "Action": [
 "glue:ShareResource"
],
 "Principal": {"Service": [
 "ram.amazonaws.com"
]},
 "Resource": [
 "arn:aws:glue:<region>:<account-id>:table/*/*",
 "arn:aws:glue:<region>:<account-id>:database/*",
 "arn:aws:glue:<region>:<account-id>:catalog"
]
}
```

- Wenn Ihr Konto mithilfe der AWS Glue Datenkatalog-Ressourcenrichtlinie kontenübergreifende Freigaben vorgenommen hat und Sie derzeit die Methode Named Resource oder LF-TBAC mit kontenübergreifenden Einstellungen Version 3 für die gemeinsame Nutzung von Ressourcen verwenden, müssen Sie das EnableHybrid Argument AWS RAM auf setzen, wenn Sie den API-Vorgang aufrufen. 'true' glue:PutResourcePolicy Weitere Informationen finden Sie unter [Verwaltung kontenübergreifender Berechtigungen sowohl AWS Glue mit Lake Formation als auch mit Lake Formation](#).

Für jedes Konto, das auf die gemeinsam genutzte Ressource zugreift, ist eine Einrichtung erforderlich

- Wenn Sie Ressourcen gemeinsam nutzen AWS-Konten, muss mindestens ein Benutzer im Kundenkonto ein Data Lake-Administrator sein, um gemeinsam genutzte Ressourcen anzeigen zu können. Informationen zum Erstellen eines Data Lake-Administrators finden Sie unter [Erstellen Sie einen Data Lake-Administrator](#).

Der Data Lake-Administrator kann anderen Prinzipalen im Konto Lake Formation Berechtigungen für die gemeinsam genutzten Ressourcen gewähren. Andere Principals können erst dann auf gemeinsam genutzte Ressourcen zugreifen, wenn der Data Lake-Administrator ihnen Berechtigungen für die Ressourcen erteilt.

- Integrierte Dienste wie Athena und Redshift Spectrum benötigen Ressourcenlinks, um gemeinsam genutzte Ressourcen in Abfragen einbeziehen zu können. Prinzipale müssen in ihrem Datenkatalog einen Ressourcenlink zu einer gemeinsam genutzten Ressource von einer anderen erstellen. AWS-Konto Weitere Informationen zu Ressourcenlinks finden Sie unter [Funktionsweise von Ressourcenverbindungen in Lake Formation](#).
- Wenn eine Ressource direkt mit einem IAM-Prinzipal gemeinsam genutzt wird, muss der Principal einen Ressourcenlink erstellen, um die Tabelle mit Athena abzufragen. Um einen Ressourcenlink zu erstellen, benötigt der Principal die Lake Formation CREATE\_TABLE oder CREATE\_DATABASE - Genehmigung und die glue:CreateTable oder glue:CreateDatabase IAM-Berechtigung.

Wenn das Producer-Konto eine andere Tabelle in derselben Datenbank mit demselben oder einem anderen Principal gemeinsam nutzt, kann dieser Principal die Tabelle sofort abfragen.

#### Note

Für den Data Lake-Administrator und für Principals, denen der Data Lake-Administrator Berechtigungen erteilt hat, werden gemeinsam genutzte Ressourcen im Datenkatalog so angezeigt, als ob es sich um lokale (eigene) Ressourcen handeln würde. Aufträge zum Extrahieren, Transformieren und Laden (ETL) können auf die zugrunde liegenden Daten gemeinsam genutzter Ressourcen zugreifen.

Bei gemeinsam genutzten Ressourcen wird auf den Seiten „Tabellen“ und „Datenbanken“ der Lake Formation Formation-Konsole die Konto-ID des Besitzers angezeigt.

Wenn auf die zugrunde liegenden Daten einer gemeinsam genutzten Ressource zugegriffen wird, werden CloudTrail Protokollereignisse sowohl im Konto des Empfängers der gemeinsam genutzten Ressource als auch im Konto des Ressourcenbesitzers generiert. Die CloudTrail Ereignisse können den ARN des Prinzipals enthalten, der auf die Daten zugegriffen hat, aber nur, wenn das Empfängerkonto sich dafür entscheidet, den Prinzipal-ARN in die Protokolle aufzunehmen. Weitere Informationen finden Sie unter [Kontoübergreifende Protokollierung CloudTrail](#).

## Aktualisierung der Versionseinstellungen für die kontenübergreifende gemeinsame Nutzung von Daten

AWS Lake Formation Aktualisiert von Zeit zu Zeit die Einstellungen für den kontenübergreifenden Datenaustausch, um die an der AWS RAM Nutzung vorgenommenen Änderungen zu erkennen und

Aktualisierungen der Funktion für den kontenübergreifenden Datenaustausch zu unterstützen. Wenn Lake Formation dies tut, erstellt es eine neue Version der Einstellungen für die kontoübergreifende Version.

## Hauptunterschiede zwischen den Einstellungen der kontoübergreifenden Version

In den folgenden Abschnitten finden Sie weitere Informationen dazu, wie die kontoübergreifende Datenfreigabe unter verschiedenen kontoübergreifenden Versionseinstellungen funktioniert.

### Note

Um Daten mit einem anderen Konto gemeinsam zu nutzen, muss der Lizenzgeber über `AWSLakeFormationCrossAccountManager` verwaltete IAM-Richtlinienberechtigungen verfügen. Dies ist eine Voraussetzung für alle Versionen.

Die Aktualisierung der Einstellungen für die kontoübergreifende Version hat keine Auswirkungen auf die Berechtigungen, über die der Empfänger für gemeinsam genutzte Ressourcen verfügt. Dies gilt für die Aktualisierung von Version 1 auf Version 2, Version 2 auf Version 3 und Version 1 auf Version 3. Beachten Sie beim Aktualisieren von Versionen die unten aufgeführten Überlegungen.

## Version 1

Methode mit benannter Ressource: Ordnet jede kontoübergreifende Lake Formation Formation-Genehmigungserteilung einer AWS RAM Ressourcenfreigabe zu. Der Benutzer (Rolle des Erteilers oder Principal) benötigt keine zusätzlichen Berechtigungen.

LF-TBAC-Methode: Kontoübergreifende Lake Formation Formation-Genehmigungen werden nicht für die gemeinsame Nutzung von Daten verwendet. AWS RAM Der Benutzer muss über eine entsprechende Genehmigung verfügen. `glue:PutResourcePolicy`

Vorteile der Aktualisierung von Versionen: Erste Version — nicht zutreffend.

Überlegungen bei der Aktualisierung von Versionen: Erste Version — nicht zutreffend

## Version 2

Methode mit benannter Ressource: Optimiert die Anzahl der gemeinsam genutzten AWS RAM Ressourcen, indem mehrere kontoübergreifende Zugriffsberechtigungen einer AWS

RAM Ressourcenfreigabe zugeordnet werden. Der Benutzer benötigt keine zusätzlichen Berechtigungen.

LF-TBAC-Methode: Kontoübergreifende Lake Formation Formation-Genehmigungen werden nicht für die gemeinsame Nutzung von Daten verwendet. AWS RAM Der Benutzer muss über eine entsprechende Genehmigung verfügen. `glue:PutResourcePolicy`

Vorteile der Aktualisierung von Versionen: Skalierbares, kontenübergreifendes Setup durch optimale AWS RAM Kapazitätsauslastung.

Überlegungen beim Aktualisieren von Versionen: Benutzer, die kontoübergreifende Lake Formation Formation-Berechtigungen gewähren möchten, müssen über die Berechtigungen in der `AWSLakeFormationCrossAccountManager` AWS verwalteten Richtlinie verfügen. Andernfalls benötigen Sie die `ram:DisassociateResourceShare` erforderlichen Berechtigungen, um Ressourcen erfolgreich mit einem anderen Konto gemeinsam nutzen zu können.

`ram:AssociateResourceShare`

### Version 3

Methode mit benannter Ressource: Optimiert die Anzahl der gemeinsam genutzten AWS RAM Ressourcen, indem mehrere kontoübergreifende Zugriffsberechtigungen einer AWS RAM Ressourcenfreigabe zugeordnet werden. Der Benutzer benötigt keine zusätzlichen Berechtigungen.

LF-TBAC-Methode: Lake Formation verwendet AWS RAM für kontenübergreifende Zuschüsse. Der Benutzer muss der Erlaubnis die Anweisung `glue:ShareResource` hinzufügen. `glue:PutResourcePolicy` Der Empfänger muss Resource Share-Einladungen von annehmen AWS RAM.

Vorteile der Aktualisierung von Versionen: Unterstützt die folgenden Funktionen:

- Ermöglicht die explizite gemeinsame Nutzung von Ressourcen mit einem IAM-Prinzipal in einem externen Konto.

Weitere Informationen finden Sie unter [Erteilen von Berechtigungen für Datenkatalogressourcen](#).

- Ermöglicht kontenübergreifende Freigaben mithilfe der LF-TBAC-Methode für Organizations oder Organisationseinheiten (). OUs
- Macht die Verwaltung zusätzlicher AWS Glue Richtlinien für kontenübergreifende Zuschüsse überflüssig.

Überlegungen bei der Aktualisierung von Versionen: Wenn Sie die LF-TBAC-Methode zur gemeinsamen Nutzung von Ressourcen verwenden und der Empfänger eine ältere Version als Version 3 verwendet und der Empfänger Version 3 oder höher verwendet, erhält der Zuwendungsgeber die folgende Fehlermeldung: „Ungültiger kontenübergreifender Zuschussantrag. Für das Kundenkonto gibt es die Opt-In für die kontenübergreifende Version: v3. Bitte aktualisieren Sie CrossAccountVersion DataLakeSetting auf die Minimalversion v3 (Service: AmazonDataCatalog; Statuscode: 400; Fehlercode: InvalidInputException)“. Wenn der Fördergeber jedoch Version 3 verwendet und der Empfänger Version 1 oder Version 2 verwendet, werden die kontenübergreifenden Zuschüsse mit LF-Tags erfolgreich durchgeführt.

Kontoübergreifende Zuschüsse, die mit der Methode der benannten Ressource gewährt wurden, sind zwischen verschiedenen Versionen kompatibel. Selbst wenn das Zuschusskonto eine ältere Version (Version 1 oder 2) und das Empfängerkonto eine neuere Version (Version 3 oder höher) verwendet, funktioniert die Funktion für den kontenübergreifenden Zugriff problemlos und ohne Kompatibilitätsprobleme oder -fehler.

Um Ressourcen direkt mit IAM-Prinzipalen in einem anderen Konto gemeinsam zu nutzen, muss nur der Grantor Version 3 verwenden.

Kontoübergreifende Zuschüsse, die mit der LF-TBAC-Methode gewährt werden, setzen voraus, dass Benutzer über eine Ressourcenrichtlinie im Konto verfügen. AWS Glue Data Catalog Wenn Sie auf Version 3 aktualisieren, gewährt LF-TBAC Nutzungen. AWS RAM Damit AWS RAM kontenübergreifende Zuschüsse erfolgreich sein können, müssen Sie die `glue:ShareResource` Erklärung zu Ihren bestehenden Datenkatalog-Ressourcenrichtlinien hinzufügen, wie im Abschnitt beschrieben. [Verwaltung kontenübergreifender Berechtigungen sowohl AWS Glue mit Lake Formation als auch mit Lake Formation](#)

## Version 4

Der Zuwendungsgeber benötigt Version 4 oder höher, um Datenkatalogressourcen im hybriden Zugriffsmodus oder Objekte in einem Verbundkatalog gemeinsam nutzen zu können.

## Version 5

Cross Account Version 5 verbessert die kontenübergreifende gemeinsame Nutzung von Ressourcen, sodass Sie eine unbegrenzte Anzahl von Tabellen für ein anderes Konto freigeben können, wodurch die bisherigen Beschränkungen für die Ressourcenzuweisung pro Ressourcentyp entfallen. Führen Sie zunächst über die Lake Formation Formation-Konsole oder API ein Upgrade auf kontenübergreifende Version 5 durch. Bei allen neuen kontenübergreifenden Zugriffsberechtigungen werden automatisch Platzhaltermuster in der Ressourcenfreigabe anstelle



von individuellen Ressourcenzuordnungen verwendet. Alle bestehenden kontenübergreifenden Aktien funktionieren weiterhin, und alle bestehenden Lake Formation APIs bleiben kompatibel.

Vorteile der Aktualisierung von Versionen: Cross-account v5 verbessert die kontenübergreifende gemeinsame Nutzung, sodass Sie Hunderttausende von Tabellen kontenübergreifend gemeinsam nutzen können.

Überlegungen bei der Aktualisierung von Versionen: Neue Zuschüsse nach dem Upgrade auf Version 5 fügen vorhandenen Resource AWS Manager-Ressourcenfreigaben Platzhaltermuster hinzu oder erstellen neue Freigaben mit Platzhaltermustern. Nach dem Upgrade auf Version 5 wird ein Downgrade nicht unterstützt.

## Optimieren Sie die gemeinsam AWS RAM genutzten Ressourcen

Neue Versionen (Version 2 und höher) von kontenübergreifenden Zuschüssen nutzen die AWS RAM Kapazität optimal, um die kontenübergreifende Nutzung zu maximieren. Wenn Sie eine Ressource mit einem externen AWS-Konto oder einem IAM-Prinzipal gemeinsam nutzen, erstellt Lake Formation möglicherweise eine neue Ressourcenfreigabe oder ordnet die Ressource einer vorhandenen Freigabe zu. Durch die Verknüpfung mit bestehenden Aktien reduziert Lake Formation die Anzahl der Einladungen zur gemeinsamen Nutzung von Ressourcen, die ein Verbraucher annehmen muss. Version 5 optimiert die RAM-Nutzung weiter, indem auf Platzhaltern basierende Ressourcenmuster anstelle von einzelnen Ressourcenzuordnungen verwendet werden, wodurch die Ressourcenzuordnungen pro gemeinsam genutzter Ressource erheblich reduziert werden.

## Aktivieren Sie AWS RAM Freigaben über TBAC oder geben Sie Ressourcen direkt für Prinzipale frei

Um Ressourcen direkt mit IAM-Prinzipalen in einem anderen Konto zu teilen oder um kontenübergreifende TBAC-Freigaben für Organizations oder Organisationseinheiten zu aktivieren, müssen Sie die Einstellungen für die kontenübergreifende Version auf Version 3 aktualisieren.

Weitere Informationen AWS RAM zu Ressourcenlimits finden Sie unter. [Bewährte Methoden und Überlegungen für den kontenübergreifenden Datenaustausch](#)

## Erforderliche Berechtigungen für die Aktualisierung der kontenübergreifenden Versionseinstellungen

Wenn ein kontenübergreifender Berechtigungsgeber IAM-Richtlinienberechtigungen `AWSLakeFormationCrossAccountManager` verwaltet hat, ist für die Rolle oder den Prinzipal des kontenübergreifenden Berechtigungsgewährers keine zusätzliche Berechtigungseinrichtung erforderlich. Wenn der kontenübergreifende Erteilende jedoch die verwaltete Richtlinie nicht

verwendet, sollten der Rolle oder dem Prinzipal, der die Rechte erteilt hat, die folgenden IAM-Berechtigungen erteilt werden, damit die neue Version der kontoübergreifenden Erteilung erfolgreich ist.

## JSON

```
{
 "Version": "2012-10-17",
 "Statement": [
 {
 "Sid": "VisualEditor1",
 "Effect": "Allow",
 "Action": [
 "ram:AssociateResourceShare",
 "ram:DisassociateResourceShare",
 "ram:GetResourceShares"
],
 "Resource": "*",
 "Condition": {
 "StringLike": {
 "ram:ResourceShareName": "LakeFormation*"
 }
 }
 }
]
}
```

## Um die neue Version zu aktivieren

Gehen Sie wie folgt vor, um die Einstellungen der kontoübergreifenden Version über die AWS Lake Formation Konsole oder die zu aktualisieren AWS CLI.

### Console

1. Wählen Sie auf der Seite mit den Einstellungen für den Datenkatalog unter Einstellungen für kontoübergreifende Versionen die Option Version 2, Version 3, Version 4 oder Version 5. Wenn Sie Version 1 auswählen, verwendet Lake Formation den Standardmodus für die gemeinsame Nutzung von Ressourcen.

AWS Lake Formation &gt; Data catalog settings

## Data catalog settings

### Default permissions for newly created databases and tables

These settings maintain existing AWS Glue Data Catalog behavior. You can still set individual permissions on databases and tables, which will take effect when you revoke the Super permission from IAMAllowedPrincipals. See [Changing Default Settings for Your Data Lake](#).

- ☐ Use only IAM access control for new databases
- ☐ Use only IAM access control for new tables in new databases

### Default permissions for AWS CloudTrail

These settings specify the information being shown in AWS CloudTrail.

#### Resource owners

Enter resource owners you wish to share your CloudTrail access details with.

Enter one or more AWS account IDs. Press Enter after each ID.

### Cross account version settings

Version 1

Version 2

Version 3

Version 3

cross account permissions. See

Cancel

Save

2. Wählen Sie Speichern.

## AWS Command Line Interface (AWS CLI)

Verwenden Sie den `put-data-lake-settings` AWS CLI Befehl, um den `CROSS_ACCOUNT_VERSION` Parameter einzustellen. Zulässige Werte sind 1, 2, 3, 4 und 5.

```
aws lakeformation put-data-lake-settings --region us-east-1 --data-lake-settings
 file://settings
{
```

```
"DataLakeAdmins": [
 {
 "DataLakePrincipalIdentifier": "arn:aws:iam::111122223333:user/test"
 }
],
"CreateDatabaseDefaultPermissions": [],
"CreateTableDefaultPermissions": [],
"Parameters": {
 "CROSS_ACCOUNT_VERSION": "3"
}
}
```

#### Important

Sobald Sie Version 2 oder Version 3 ausgewählt haben, durchlaufen alle neuen Zuschüsse für benannte Ressourcen den neuen kontenübergreifenden Zuweisungsmodus. Um die AWS RAM Kapazität Ihrer vorhandenen kontoübergreifenden Anteile optimal zu nutzen, empfehlen wir Ihnen, die mit der älteren Version gewährten Zuschüsse zu widerrufen und im neuen Modus erneut zu gewähren.

## Gemeinsame Nutzung von Datenkatalogtabellen und Datenbanken für mehrere AWS-Konten IAM-Prinzipale von externen Konten aus

Dieser Abschnitt enthält Anweisungen dazu, wie Sie einem externen Konto, einem IAM-Prinzipal, einer AWS Organisation oder einer Organisationseinheit AWS kontenübergreifende Berechtigungen für Datenkatalogressourcen gewähren können. Bei der Gewährung werden diese Ressourcen automatisch gemeinsam genutzt.

### Themen

- [Datenaustausch mit tagbasierter Zugriffskontrolle](#)
- [Kontoübergreifender Datenaustausch mithilfe der benannten Ressourcenmethode](#)

## Datenaustausch mit tagbasierter Zugriffskontrolle

AWS Lake Formation Tag-basierte Zugriffskontrolle (LF-TBAC) ist eine Autorisierungsstrategie, die Berechtigungen auf der Grundlage von Attributen definiert. In den folgenden Schritten wird erklärt, wie kontoübergreifende Berechtigungen mithilfe von LF-Tags erteilt werden.

Einrichtung für das Konto erforderlich producer/grantor

### 1. LF-Tags hinzufügen.

1. Melden Sie sich bei der Lake Formation Console als Data Lake-Administrator oder LF-Tag-Ersteller an.
2. Wählen Sie in der linken Navigationsleiste Berechtigungen und LF-Tags und Berechtigungen aus.
3. Wählen Sie LF-Tag hinzufügen.

Eine ausführliche Anleitung zum Erstellen von LF-Tags finden Sie unter [LF-Tags erstellen](#)

### 2. Erteilen Sie IAM-Prinzipalen in Ihrem Konto oder externen Konten die Berechtigungen Describe and/or Associate mit LF-Tag-Schlüssel-Wert-Paaren.

Die Erteilung von Berechtigungen für LF-Tag-Schlüssel-Wert-Paare ermöglicht es den Prinzipalen, die LF-Tags einzusehen und sie den Datenkatalogressourcen (Datenbanken, Tabellen und Spalten) zuzuweisen.

3. Als Nächstes kann der Data Lake-Administrator oder ein IAM-Prinzipal mit Associate-Berechtigung das LF-Tag Datenbanken, Tabellen oder Spalten zuweisen. Weitere Informationen finden Sie unter [Zuweisen von LF-Tags zu Datenkatalogressourcen](#).
4. Als Nächstes erteilen Sie externen Konten mithilfe von LF-Tag-Ausdrücken Datenberechtigungen. Dadurch kann der Empfänger oder Empfänger der Berechtigungen auf die Datenkatalogressource (n) zugreifen, die mit denselben Schlüsseln und Werten gekennzeichnet sind.
  1. Wählen Sie im Navigationsbereich die Optionen Berechtigungen und Datenberechtigungen aus.
  2. Wählen Sie Grant (Erteilen).
  3. Wählen Sie auf der Seite Berechtigungen gewähren für Principals die Option Externe Konten aus und geben Sie die AWS-Konto Empfänger-ID oder die IAM-Rolle des Prinzipals oder den Amazon-Ressourcennamen (ARN) für den Prinzipal (Principal-ARN) ein, wenn Sie einem

externen Prinzipal eine direkte kontoübergreifende Gewährung gewähren. Nachdem Sie die Konto-ID eingegeben haben, müssen Sie die Eingabetaste drücken.

### Principals

Choose the principals to grant permissions.

☐ **IAM users and roles**  
Users or roles from this AWS account.

☐ **IAM Identity Center - new**  
Users and groups configured in IAM Identity Center.

☐ **SAML users and groups**  
SAML users and group or QuickSight ARNs.

☒ **External accounts**  
AWS account, AWS organization or IAM principal outside of this account

**AWS account, AWS organization, or IAM principal outside of this account**  
Enter one or more AWS account IDs, AWS organization IDs, or IAM principal ARNs. Press Enter after each ID or ARN.

Granting data permissions to organizations is not supported when granting permissions by using LF-Tags.

### LF-Tags or catalog resources

Choose a method to grant permissions.

☒ **Resources matched by LF-Tags (recommended)**  
Manage permissions indirectly for resources or data matched by a specific set of LF-Tags.

☐ **Named Data Catalog resources**  
Manage permissions for specific databases or tables, in addition to fine-grained data access.

☒ **LF-Tag key-value pairs**

☐ **Saved LF-Tag expressions - new**

**Key**

**Values**

4. Wählen Sie für LF-Tags oder Katalogressourcen die Option Ressourcen, denen LF-Tags zugeordnet sind (empfohlen).
  - a. Wählen Sie die Option LF-Tag-Schlüssel-Wert-Paare oder Gespeicherte LF-Tag-Ausdrücke.

- b. Wenn Sie LF-Tag-Schlüssel-Wert-Paare wählen, geben Sie den Schlüssel und die Werte des LF-Tags ein, das der Datenkatalogressource zugeordnet ist, die mit dem Konto des Empfängers gemeinsam genutzt wird.

Dem Empfänger werden Berechtigungen für die Datenkatalogressourcen gewährt, denen im LF-Tag-Ausdruck ein passendes LF-Tag zugewiesen wurde. Wenn der LF-Tag-Ausdruck mehrere Werte pro Tag-Schlüssel angibt, kann jeder der Tag-Werte übereinstimmen.

5. Wählen Sie die Berechtigungen auf Datenbank- oder Tabellenebene aus, die für Ressourcen gewährt werden sollen, die dem LF-Tag-Ausdruck entsprechen.

 **Important**

Da der Data Lake-Administrator den Prinzipalen im Empfängerkonto Berechtigungen für gemeinsam genutzte Ressourcen gewähren muss, müssen Sie mit der Option Grant immer kontoübergreifende Berechtigungen gewähren.

Weitere Informationen finden Sie unter [Erteilen von LF-Tag-Berechtigungen über die Konsole](#).

 **Note**

Prinzipalen, die direkte kontoübergreifende Zuschüsse erhalten, steht die Option „Gewährbare Berechtigungen“ nicht zur Verfügung.

Einrichtung für das Konto erforderlich receiving/grantee

1. Melden Sie sich bei der Lake Formation Console als Data Lake-Administrator des Verbraucherkontos an.
2. Als Nächstes erhalten Sie den Ressourcenanteil im Kundenkonto.
  1. Öffnen Sie die AWS RAM Konsole.
  2. Wählen Sie im Navigationsbereich unter Für mich freigegeben die Option Resource Shares aus.
  3. Wählen Sie die Ressourcenfreigaben aus und klicken Sie auf Ressourcenfreigabe akzeptieren.

3. Wenn Sie eine Ressource mit einem anderen Konto teilen, gehört die Ressource immer noch zum Produzentenkonto und ist in der Athena-Konsole nicht sichtbar. Um die Ressource in der Athena-Konsole sichtbar zu machen, müssen Sie einen Ressourcenlink erstellen, der auf die gemeinsam genutzte Ressource verweist. Anweisungen zum Erstellen eines Ressourcenlinks finden Sie unter [Einen Ressourcenlink zu einer gemeinsam genutzten Datenkatalogtabelle erstellen](#) und [Einen Ressourcenlink zu einer gemeinsam genutzten Datenkatalog-Datenbank erstellen](#)
  1. Wählen Sie im Datenkatalog die Option Datenbanken oder Tabellen aus.
  2. Wählen Sie auf der Databases/Tables Seite den Link Erstellen, Ressource aus.
  3. Geben Sie die folgenden Informationen für einen Datenbankressourcen-Link ein:
    - Name des Ressourcenlinks — Ein eindeutiger Name für den Ressourcenlink.
    - Zielkatalog — Der Katalog, in dem Sie den Ressourcenlink erstellen.
    - Gemeinsam genutzte Datenbankregion — Die Region der Datenbank, die für Sie freigegeben wurde, wenn Sie den Ressourcenlink in einer anderen Region erstellen.
    - Gemeinsam genutzte Datenbank — Wählen Sie die gemeinsam genutzte Datenbank aus.
    - Katalog-ID der gemeinsam genutzten Datenbank — Geben Sie die Katalog-ID für die gemeinsam genutzte Datenbank ein.
  4. Wählen Sie Erstellen aus. Sie können den neu erstellten Ressourcenlink in der Datenbankliste sehen.

In ähnlicher Weise können Sie einen Ressourcenlink zu einer gemeinsam genutzten Tabelle erstellen.

4. Erteilen Sie nun den IAM-Prinzipalen, die Sie die Ressource gemeinsam nutzen, die Beschreibungsberechtigung für den Ressourcenlink.
  1. Wählen Sie auf der Seite Datenbanken/Tabellen den Ressourcenlink aus, und wählen Sie im Menü Aktionen die Option Gewähren aus.
  2. Wählen Sie im Abschnitt Berechtigungen gewähren die Option IAM-Benutzer und -Rollen aus.
  3. Wählen Sie die IAM-Rolle aus, der Sie Zugriff auf den Ressourcenlink gewähren möchten.
  4. Wählen Sie im Abschnitt Berechtigungen für Ressourcenlinks die Option Beschreiben aus.
  5. Wählen Sie Grant (Erteilen).
5. Erteilen Sie als Nächstes den Prinzipalen im Verbraucherkonto LF-Tag-[Schlüsselwertberechtigungen](#).



Sie sollten die LF-Tags, die mit Ihnen geteilt wurden, im Verbraucherkonto auf der Lake Formation Formation-Konsole unter Berechtigungen, LF-Tags und Berechtigungen finden können. Sie können von Grantor geteilte Tags mit Ressourcen verknüpfen, die über das Grantor-Konto gemeinsam genutzt wurden. Dazu gehören: Datenbanken, Tabellen und Spalten. Sie können anderen Prinzipalen weitere Berechtigungen für die Ressourcen gewähren.

LF-Tags | LF-Tag expressions - new | **LF-Tag permissions** | LF-Tag creators

**LF-Tag permissions (8)** View Revoke Grant permissions

View and manage the permissions granted on LF-Tags. [Learn more](#)

Find permissions by LF-Tag key and value

|                       | Principal               | Principal type | Resource name               | Resource type         | LF-Tag permissions | LF-Tag value permissions     |
|-----------------------|-------------------------|----------------|-----------------------------|-----------------------|--------------------|------------------------------|
| <input type="radio"/> |                         | AWS account    | Department=Marketing, Sales | LF-Tag key value pair | -                  | Describe                     |
| <input type="radio"/> |                         | AWS account    | Department=Marketing, Sales | LF-Tag key value pair | -                  | Associate                    |
| <input type="radio"/> | arn:aws:iam::( ):/Admin | IAM role       | Department                  | LF-Tag                | Alter, Drop        | -                            |
| <input type="radio"/> | arn:aws:iam::( ):/Admin | IAM role       | Department                  | LF-Tag                | -                  | Describe                     |
| <input type="radio"/> | arn:aws:iam::( ):/Admin | IAM role       | Department                  | LF-Tag                | -                  | Associate                    |
| <input type="radio"/> | arn:aws:iam::( ):/Admin | IAM role       | Department                  | LF-Tag                | -                  | Grant with LF-Tag expression |
| <input type="radio"/> | arn:aws:iam::( ):/Admin | IAM role       | LF-Test                     | LF-Tag                | -                  | Describe                     |
| <input type="radio"/> | arn:aws:iam::( ):/Admin | IAM role       | LF-Test                     | LF-Tag                | -                  | Associate                    |

1. Wählen Sie im Navigationsbereich unter Berechtigungen, Datenberechtigungen die Option Grant aus.
2. Wählen Sie auf der Seite Berechtigungen gewähren die Option IAM-Benutzer und -Rollen aus.
3. Wählen Sie als Nächstes die IAM-Benutzer und -Rollen in Ihrem Konto aus, um Zugriff auf die gemeinsam genutzten Datenbanken/Tabellen zu gewähren.
4. Wählen Sie als Nächstes für LF-Tags oder Katalogressourcen die Option Ressourcen, denen LF-Tags zugeordnet sind.
5. Wählen Sie als Nächstes den Schlüssel und die Werte des LF-Tags aus, das mit Ihnen geteilt wird.
6. Wählen Sie als Nächstes die Datenbank- und Tabellenberechtigungen aus, die Sie den IAM-Benutzern und -Rollen gewähren möchten. Sie können auch Grantable Permissions auswählen, sodass die IAM-Benutzer und -Rollen anderen Benutzer/Rollen Berechtigungen gewähren können.
7. Wählen Sie Grant (Erteilen).
8. Sie können die erteilten Berechtigungen unter Datenberechtigungen in der Lake Formation Formation-Konsole einsehen.

## Kontoübergreifender Datenaustausch mithilfe der benannten Ressourcenmethode

Sie können direkt den Hauptbenutzern des anderen AWS Kontos oder externen AWS-Konten Benutzern oder Berechtigungen erteilen. AWS Organizations Die Erteilung Lake Formation Formation-Berechtigungen an Organizations oder Organisationseinheiten entspricht der Erteilung der Erlaubnis AWS-Konto an alle Mitglieder dieser Organisation oder Organisationseinheit.

Wenn Sie externen Konten oder Organisationen Berechtigungen gewähren, müssen Sie die Option Erteilbare Berechtigungen einbeziehen. Nur der Data Lake-Administrator im externen Konto kann auf die gemeinsam genutzten Ressourcen zugreifen, bis der Administrator anderen Prinzipalen im externen Konto Berechtigungen für die gemeinsam genutzten Ressourcen erteilt.

### Note

Die Option „Gewährbare Berechtigungen“ wird nicht unterstützt, wenn IAM-Prinzipalen direkt von externen Konten aus Berechtigungen erteilt werden.

Folgen Sie den Anweisungen unter [Erteilen von Datenbankberechtigungen mit der benannten Ressourcenmethode](#), um kontoübergreifende Berechtigungen mithilfe der benannten Ressourcenmethode zu gewähren.

## Erteilen von Berechtigungen für eine Datenbank oder Tabelle, die mit Ihrem Konto geteilt wird

Nachdem eine Data Catalog-Ressource, die zu einem anderen AWS Konto gehört, für Ihr AWS Konto freigegeben wurde, können Sie als Data Lake-Administrator anderen Prinzipalen in Ihrem Konto Berechtigungen für die gemeinsam genutzte Ressource gewähren. Sie können jedoch anderen AWS Konten oder Organisationen keine Berechtigungen für die Ressource gewähren.

Sie können die AWS Lake Formation Konsole, die API oder die AWS Command Line Interface (AWS CLI) verwenden, um die Berechtigungen zu erteilen.

Um Berechtigungen für eine gemeinsam genutzte Datenbank zu gewähren (benannte Ressourcenmethode, Konsole)

- Folgen Sie den Anweisungen in [Erteilen von Datenbankberechtigungen mit der benannten Ressourcenmethode](#). Stellen Sie sicher, dass Sie in der Datenbankliste unter LF-Tags oder

Katalogressourcen die Datenbank im externen Konto auswählen und keinen Ressourcenlink für die Datenbank.

Wenn Sie die Datenbank nicht in der Liste der Datenbanken sehen, stellen Sie sicher, dass Sie die Einladung AWS Resource Access Manager (AWS RAM) zur gemeinsamen Nutzung von Ressourcen für die Datenbank akzeptiert haben. Weitere Informationen finden Sie unter [Annahme einer Einladung zur gemeinsamen Nutzung von Ressourcen AWS RAM](#).

Folgen Sie für die ALTER Berechtigungen CREATE\_TABLE und den Anweisungen unter und achten Sie darauf [Erteilen von Datenspeicherberechtigungen \(dasselbe Konto\)](#), dass Sie die ID des Eigentümerkontos in das Feld Standort des registrierten Kontos eingeben.

So gewähren Sie Berechtigungen für eine gemeinsam genutzte Tabelle (benannte Ressourcenmethode, Konsole)

- Folgen Sie den Anweisungen in [Erteilen von Tabellenberechtigungen mithilfe der benannten Ressourcenmethode](#). Stellen Sie sicher, dass Sie in der Datenbankliste unter LF-Tags oder Katalogressourcen die Datenbank im externen Konto auswählen und keinen Ressourcenlink für die Datenbank.

Wenn Sie die Tabelle nicht in der Tabellenliste sehen, stellen Sie sicher, dass Sie die Einladung zur gemeinsamen Nutzung der AWS RAM Ressource für die Tabelle akzeptiert haben. Weitere Informationen finden Sie unter [Annahme einer Einladung zur gemeinsamen Nutzung von Ressourcen AWS RAM](#).

Folgen Sie für die ALTER Erteilung der Genehmigung außerdem den Anweisungen unter und achten Sie darauf [Erteilen von Datenspeicherberechtigungen \(dasselbe Konto\)](#), dass Sie die Konto-ID des Besitzers in das Feld Standort des registrierten Kontos eingeben.

So gewähren Sie Berechtigungen für gemeinsam genutzte Ressourcen (LF-TBAC-Methode, Konsole)

- Folgen Sie den Anweisungen in [Erteilen von Datenkatalogberechtigungen](#). Gewähren Sie im Abschnitt LF-Tags oder Katalogressourcen genau den LF-Tag-Ausdruck, den das externe Konto Ihrem Konto gewährt hat, oder eine Teilmenge dieses Ausdrucks.

Wenn beispielsweise ein externes Konto Ihrem Konto mit der Grant-Option den LF-Tag-Ausdruck `module=customers AND environment=production` gewährt hat, können Sie als Data Lake-Administrator denselben Ausdruck oder `module=customers` oder

`environment=production` einem Prinzipal in Ihrem Konto gewähren. Sie können nur dieselben oder nur einen Teil der Lake Formation Formation-Berechtigungen (z. B., usw.) gewähren `SELECTALTER`, die für Ressourcen über den LF-Tag-Ausdruck erteilt wurden.

Um Berechtigungen für eine gemeinsam genutzte Tabelle zu erteilen (benannte Ressourcenmethode,) AWS CLI

- Verwenden Sie einen Befehl ähnlich dem folgenden. In diesem Beispiel:
  - Ihre AWS Konto-ID lautet 1111-2222-3333.
  - Das Konto, dem die Tabelle gehört und das sie Ihrem Konto gewährt hat, ist 1234-5678-9012.
  - Die `SELECT` Berechtigung wird dem Benutzer für die gemeinsam genutzte Tabelle erteilt. `pageviews datalake_user1` Dieser Benutzer ist ein Hauptbenutzer in Ihrem Konto.
  - Die `pageviews` Tabelle befindet sich in der `analytics` Datenbank, die dem Konto 1234-5678-9012 gehört.

```
aws lakeformation grant-permissions --principal
DataLakePrincipalIdentifier=arn:aws:iam::111122223333:user/datalake_user1
--permissions "SELECT" --resource '{ "Table": {"CatalogId":"123456789012",
"DatabaseName":"analytics", "Name":"pageviews"}}'
```

Beachten Sie, dass das Eigentümerkonto in der Eigenschaft im Argument angegeben werden muss. `CatalogId resource`

## Erteilen von Ressourcenverknüpfungsberechtigungen

Gehen Sie wie folgt vor, um einem Prinzipal in Ihrem AWS Konto AWS Lake Formation Berechtigungen für eine oder mehrere Ressourcenlinks zu erteilen.

Nachdem Sie einen Ressourcenlink erstellt haben, können nur Sie ihn anzeigen und darauf zugreifen. (Dabei wird vorausgesetzt, dass „Nur IAM-Zugriffssteuerung für neue Tabellen in dieser Datenbank verwenden“ für die Datenbank nicht aktiviert ist.) Um anderen Hauptbenutzern in Ihrem Konto den Zugriff auf den Ressourcenlink zu ermöglichen, erteilen Sie mindestens die `DESCRIBE` entsprechende Berechtigung.

 **Important**

Durch das Erteilen von Berechtigungen für einen Ressourcenlink werden keine Berechtigungen für die (verknüpfte) Zieldatenbank oder -tabelle gewährt. Sie müssen Berechtigungen für das Ziel separat gewähren.

Sie können Berechtigungen mithilfe der Lake Formation Formation-Konsole, der API oder der AWS Command Line Interface (AWS CLI) gewähren.

console

So gewähren Sie Resource Link-Berechtigungen mithilfe der Lake Formation Formation-Konsole

1. Führen Sie eine der folgenden Aktionen aus:
  - Gehen Sie für Links zu Datenbankressourcen wie unter [Erteilen von Datenbankberechtigungen mit der benannten Ressourcenmethode](#), beschrieben vor, um Folgendes zu tun:
    1. Wählen Sie den Ressourcenlink aus der Datenbankliste unter Datenkatalog, Datenbanken aus.
    2. Wählen Sie Grant, um die Seite „Berechtigungen gewähren“ zu öffnen.
    3. Geben Sie Principals an, denen Berechtigungen erteilt werden sollen.
    4. Die Felder Kataloge und Datenbanken sind gefüllt.
  - Gehen Sie bei Links [Erteilen von Tabellenberechtigungen mithilfe der benannten Ressourcenmethode](#) zu Tabellenressourcen wie folgt vor:
    1. Wählen Sie den Ressourcenlink aus der Tabellenliste unter Datenkatalog, Tabellen aus.
    2. Öffnen Sie die Seite „Berechtigungen gewähren“.
    3. Geben Sie die Hauptbenutzer an.
    4. Die Felder Kataloge, Datenbanken, Tabellen sind gefüllt.
    5. Geben Sie die Hauptbenutzer an.
2. Wählen Sie unter Berechtigungen die zu erteilenden Berechtigungen aus. Wählen Sie optional erteilbare Berechtigungen aus.

## LF-Tags or catalog resources

Choose a method to grant permissions.

☐ **Resources matched by LF-Tags (recommended)**  
Manage permissions indirectly for resources or data matched by a specific set of LF-Tags.

☒ **Named Data Catalog resources**  
Manage permissions for specific databases or tables, in addition to fine-grained data access.

### Catalogs

Choose catalogs

Default catalog

### Databases

Select one or more databases.

Choose databases

resourcelink

### Tables - optional

Select one or more tables.

Choose tables

### Views - optional

Select one or more views.

Choose views

### Data filters - optional

Select one or more data filters.

Choose data filters

Load more

Create new

[Manage data filters](#)

## Resource link permissions

### Resource link permissions

Choose specific access permissions to grant.

☐ Describe ☐ Drop

### Grantable permissions

Choose the permission that can be granted to others.

☐ Describe ☐ Drop

Cancel

Grant

### 3. Wählen Sie Grant (Erteilen).

## AWS CLI

Um Ressourcenverknüpfungsberechtigungen zu gewähren, verwenden Sie AWS CLI

- Führen Sie den `grant-permissions` Befehl aus und geben Sie einen Ressourcenlink als Ressource an.

### Example

In diesem Beispiel wird `DESCRIBE datalake_user1` dem Benutzer für die Tabelle ein Ressourcenlink `incidents-link` in der Datenbank `issues` im AWS Konto `1111-2222-3333` gewährt.

```
aws lakeformation grant-permissions --principal
DataLakePrincipalIdentifier=arn:aws:iam::111122223333:user/datalake_user1
--permissions "DESCRIBE" --resource '{ "Table": {"DatabaseName":"issues",
"Name":"incidents-link"}}'
```

 Weitere Informationen finden Sie unter:

- [Ressourcenlinks erstellen](#)
- [Referenz zu den Genehmigungen von Lake Formation](#)

## Zugreifen auf die zugrunde liegenden Daten einer gemeinsam genutzten Tabelle

Gehen Sie davon aus, dass AWS Konto A gemeinsam mit Konto B eine Datenkatalogtabelle verwendet, z. B. indem Konto B `SELECT` mit der `Grant`-Option für die Tabelle eine Genehmigung erteilt wird, damit ein Hauptbenutzer in Konto B die der gemeinsam genutzten Tabelle zugrunde liegenden Daten lesen kann, müssen die folgenden Bedingungen erfüllt sein:

- Der Data Lake-Administrator in Konto B muss die gemeinsame Nutzung akzeptieren. (Dies ist nicht erforderlich, wenn sich die Konten A und B in derselben Organisation befinden oder wenn die Gewährung mit der Tag-basierten Zugriffskontrollmethode von Lake Formation erfolgt ist.)
- Der Data Lake-Administrator muss dem Principal erneut die Lake Formation `SELECT` Formation-Berechtigung erteilen, die Konto A für die gemeinsam genutzte Tabelle erteilt hat.

- Der Principal muss über die folgenden IAM-Berechtigungen für die Tabelle, die Datenbank, die sie enthält, und das Konto A Data Catalog verfügen.

#### Note

In der folgenden IAM-Richtlinie:

- *<account-id-A>* Ersetzen Sie es durch die AWS Konto-ID von Konto A.
- *<region>* Durch eine gültige Region ersetzen.
- *<database>* Ersetzen Sie es durch den Namen der Datenbank in Konto A, die die gemeinsam genutzte Tabelle enthält.
- *<table>* Ersetzen Sie durch den Namen der gemeinsam genutzten Tabelle.

## JSON

```
{
 "Version": "2012-10-17",
 "Statement": [
 {
 "Effect": "Allow",
 "Action": [
 "glue:GetTable",
 "glue:GetTables",
 "glue:GetPartition",
 "glue:GetPartitions",
 "glue:BatchGetPartition",
 "glue:GetDatabase",
 "glue:GetDatabases"
],
 "Resource": [
 "arn:aws:glue:us-east-1:111122223333:table/<database>/<table>",
 "arn:aws:glue:us-east-1:111122223333:database/<database>",
 "arn:aws:glue:us-east-1:111122223333:catalog"
]
 },
 {
 "Effect": "Allow",
 "Action": [
 "lakeformation:GetDataAccess"
],

```



```
 "Resource": [
 "*"
]
 }
]
}
```

 Weitere Informationen finden Sie unter:

- [Annahme einer Einladung zur gemeinsamen Nutzung von Ressourcen AWS RAM](#)

## Kontoübergreifende Protokollierung CloudTrail

Lake Formation bietet einen zentralen Prüfpfad für alle kontenübergreifenden Zugriffe auf Daten in Ihrem Data Lake. Wenn ein AWS Empfängerkonto auf Daten in einer gemeinsam genutzten Tabelle zugreift, kopiert Lake Formation das CloudTrail Ereignis in die Protokolle des Eigentümerkontos CloudTrail. Zu den kopierten Ereignissen gehören Abfragen von Daten durch integrierte Services wie Amazon Athena Amazon Redshift Spectrum und Datenzugriffe durch AWS Glue Jobs.

CloudTrail Ereignisse für kontenübergreifende Operationen mit Datenkatalogressourcen werden auf ähnliche Weise kopiert.

Wenn Sie als Ressourcenbesitzer die Protokollierung auf Objektebene in Amazon S3 aktivieren, können Sie Abfragen ausführen, die CloudTrail S3-Ereignisse mit Lake Formation CloudTrail Formation-Ereignissen verknüpfen, um die Konten zu ermitteln, die auf Ihre S3-Buckets zugegriffen haben.

### Themen

- [Einbeziehung von Hauptidentitäten in kontoübergreifende Protokolle CloudTrail](#)
- [CloudTrail Logs für den kontoübergreifenden Zugriff auf Amazon S3 abfragen](#)

## Einbeziehung von Hauptidentitäten in kontoübergreifende Protokolle CloudTrail

Standardmäßig enthalten kontoübergreifende CloudTrail Ereignisse, die zu den Protokollen des Empfängers der gemeinsam genutzten Ressource hinzugefügt und in die Protokolle des Ressourcenbesitzers kopiert wurden, nur die AWS Prinzipal-ID des externen Kontoprinzipals — nicht

den menschenlesbaren Amazon-Ressourcennamen (ARN) des Prinzipals (Principal-ARN). Wenn Sie Ressourcen innerhalb vertrauenswürdiger Grenzen gemeinsam nutzen, z. B. innerhalb derselben Organisation oder desselben Teams, können Sie sich dafür entscheiden, den Haupt-ARN in die CloudTrail Ereignisse aufzunehmen. Mit Konten von Ressourcenbesitzern können dann die Principals in den Empfängerkonten nachverfolgt werden, die auf ihre eigenen Ressourcen zugreifen.

 **Important**

Wenn Sie als Empfänger gemeinsam genutzter Ressourcen den Prinzipal-ARN in Ereignissen in Ihren eigenen CloudTrail Protokollen sehen möchten, müssen Sie sich dafür entscheiden, den Prinzipal-ARN mit dem Besitzerkonto zu teilen.

Wenn der Datenzugriff über einen Ressourcenlink erfolgt, werden zwei Ereignisse im Empfängerkonto der gemeinsam genutzten Ressource protokolliert: eines für den Zugriff auf die Ressourcenverknüpfung und eines für den Zugriff auf die Zielressource. Das Ereignis für den Resource Link-Zugriff beinhaltet den Prinzipal-ARN. Das Ereignis für den Zugriff auf die Zielressource beinhaltet nicht den Prinzipal-ARN ohne das Opt-In. Das Ereignis für den Zugriff auf den Ressourcenlink wird nicht auf das Besitzerkonto kopiert.

Im Folgenden finden Sie einen Auszug aus einem kontoübergreifenden CloudTrail Standardereignis (ohne Opt-In). Das Konto, das den Datenzugriff durchführt, ist 1111-2222-3333. Dies ist das Protokoll, das sowohl im anrufenden Konto als auch im Konto des Ressourcenbesitzers angezeigt wird. Lake Formation füllt im kontenübergreifenden Fall Logs in beiden Konten aus.

```
{
 "eventVersion": "1.05",
 "userIdentity": {
 "type": "AWSAccount",
 "principalId": "AROAQGFTBBBG0BWV2EMZA:GlueJobRunnerSession",
 "accountId": "111122223333"
 },
 "eventSource": "lakeformation.amazonaws.com",
 "eventName": "GetDataAccess",
 ...
 ...
 "additionalEventData": {
 "requesterService": "GLUE_JOB",
 "lakeFormationRoleSessionName": "AWSLF-00-GL-111122223333-G13T0Rmng2"
 },
 ...
}
```

```
}
```

Wenn Sie sich als Nutzer gemeinsam genutzter Ressourcen dafür entscheiden, den Haupt-ARN einzubeziehen, lautet der Auszug wie folgt. Das `lakeFormationPrincipal` Feld steht für die Endrolle oder den Benutzer, der die Abfrage über Amazon Athena, Amazon Redshift Spectrum oder AWS Glue Jobs ausführt.

```
{
 "eventVersion": "1.05",
 "userIdentity": {
 "type": "AWSAccount",
 "principalId": "AR0AQGFTBBBG0BWV2EMZA:GlueJobRunnerSession",
 "accountId": "111122223333"
 },
 "eventSource": "lakeformation.amazonaws.com",
 "eventName": "GetDataAccess",
 ...
 ...
 "additionalEventData": {
 "requesterService": "GLUE_JOB",
 "lakeFormationPrincipal": "arn:aws:iam::111122223333:role/ETL-Glue-Role",
 "lakeFormationRoleSessionName": "AWSLF-00-GL-111122223333-G13T0Rmng2"
 },
 ...
}
```

Um sich dafür zu entscheiden, dass der Hauptbenutzer in kontoübergreifende Logs ARNs aufgenommen wird CloudTrail

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

Melden Sie sich als Administrator Benutzer oder als Benutzer mit der Administrator Access IAM-Richtlinie an.

2. Wählen Sie im Navigationsbereich Settings (Einstellungen).
3. Geben Sie auf der Seite mit den Datenkatalogeinstellungen im AWS CloudTrail Abschnitt Standardberechtigungen für Ressourcenbesitzer ein oder mehrere AWS Ressourcenbesitzerkonten IDs ein.

Drücken Sie nach jeder Konto-ID die Eingabetaste.

#### 4. Wählen Sie Speichern.

Jetzt enthalten kontenübergreifende CloudTrail Ereignisse, die in den Protokollen sowohl für den Empfänger der gemeinsam genutzten Ressource als auch für den Ressourcenbesitzer gespeichert sind, den Haupt-ARN.

### CloudTrail Logs für den kontoübergreifenden Zugriff auf Amazon S3 abfragen

Als Eigentümer gemeinsam genutzter Ressourcen können Sie CloudTrail S3-Protokolle abfragen, um die Konten zu ermitteln, die auf Ihre Amazon S3-Buckets zugegriffen haben (vorausgesetzt, Sie haben die Protokollierung auf Objektebene in Amazon S3 aktiviert). Dies gilt nur für S3-Standorte, die Sie bei Lake Formation registriert haben. Wenn Benutzer gemeinsam genutzter Ressourcen sich dafür entscheiden, Principal ARNs in Lake Formation CloudTrail Formation-Logs aufzunehmen, können Sie die Rollen oder Benutzer bestimmen, die auf die Buckets zugegriffen haben.

Wenn Sie Abfragen mit ausführen Amazon Athena, können Sie Lake Formation CloudTrail Formation-Ereignisse und CloudTrail S3-Ereignisse in der Eigenschaft Sitzungsname verknüpfen. Abfragen können auch Lake Formation Formation-Ereignisse nach `eventName="GetDataAccess"` und S3-Ereignisse nach `eventName="Get Object"` oder `filtereventName="Put Object"`.

Im Folgenden finden Sie einen Auszug aus einem kontoübergreifenden CloudTrail Ereignis in Lake Formation, bei dem auf Daten an einem registrierten S3-Standort zugegriffen wurde.

```
{
 "eventSource": "lakeformation.amazonaws.com",
 "eventName": "GetDataAccess",

 "additionalEventData": {
 "requesterService": "GLUE_JOB",
 "lakeFormationPrincipal": "arn:aws:iam::111122223333:role/ETL-Glue-Role",
 "lakeFormationRoleSessionName": "AWSLF-00-GL-111122223333-B8JSAjo5QA"
 }
}
```

Der `lakeFormationRoleSessionName` Schlüsselwert, `AWSLF-00-GL-111122223333-B8JSAjo5QA`, kann mit dem Sitzungsnamen im `principalId` Schlüssel des CloudTrail S3-Ereignisses verknüpft werden. Das Folgende ist ein Auszug aus dem CloudTrail S3-Ereignis. Es zeigt den Speicherort des Sitzungsnamens.

```
{
 "eventSource": "s3.amazonaws.com",
 "eventName": "Get Object"

 "principalId": "AROAQSOX5XXUR7D6RMYLR:AWSLF-00-GL-111122223333-B8JSAjo5QA",
 "arn": "arn:aws:sets::111122223333:assumed-role/Deformationally/AWSLF-00-GL-111122223333-B8JSAjo5QA",
 "session Context": {
 "session Issuer": {
 "type": "Role",
 "principalId": "AROAQSOX5XXUR7D6RMYLR",
 "arn": "arn:aws:iam::111122223333:role/aws-service-role/lakeformation.amazonaws.com/Deformationally",
 "accountId": "111122223333",
 "user Name": "Deformationally"
 },

 }
}
```

Der Sitzungsname ist wie folgt formatiert:

```
AWSLF-<version-number>-<query-engine-code>-<account-id>-<suffix>
```

### version-number

Die aktuelle Version dieses Formats. 00 Wenn sich das Format des Sitzungsnamens ändert, wird es die nächste Version sein01.

### query-engine-code

Gibt die Entität an, die auf die Daten zugegriffen hat. Aktuelle Werte sind:

|    |                          |
|----|--------------------------|
| GL | AWS GlueETL-Job          |
| AT | Athena                   |
| RE | Amazon Redshift Spectrum |

**account-id**

Die AWS Konto-ID, die Anmeldeinformationen von Lake Formation angefordert hat.

**suffix**

Eine zufällig generierte Zeichenfolge.

## Verwaltung kontenübergreifender Berechtigungen sowohl AWS Glue mit Lake Formation als auch mit Lake Formation

Es ist möglich, kontenübergreifenden Zugriff auf Datenkatalogressourcen und zugrunde liegende Daten zu gewähren, indem Sie entweder AWS Glue oder AWS Lake Formation verwenden.

Indem Sie einen kontenübergreifenden Zugriff mit AWS Glue gewähren, indem Sie eine Datenkatalog-Ressourcenrichtlinie erstellen oder aktualisieren. In Lake Formation gewähren Sie kontenübergreifende Berechtigungen, indem Sie das Lake Formation GRANT/REVOKE Formation-Berechtigungsmodell und den `Grant Permissions` API-Vorgang verwenden.

 **Tip**

Wir empfehlen, sich ausschließlich auf die Berechtigungen von Lake Formation zu verlassen, um Ihren Data Lake zu sichern.

Sie können kontenübergreifende Zuschüsse von Lake Formation in der Lake Formation Konsole oder der Konsole AWS Resource Access Manager (AWS RAM) anzeigen. Auf diesen Konsolenseiten werden jedoch keine kontenübergreifenden Berechtigungen angezeigt, die durch die AWS Glue Datenkatalog-Ressourcenrichtlinie gewährt wurden. In ähnlicher Weise können Sie die kontenübergreifenden Zuweisungen in der Datenkatalog-Ressourcenrichtlinie auf der Einstellungsseite der AWS Glue Konsole anzeigen, aber auf dieser Seite werden die mit Lake Formation gewährten kontenübergreifenden Berechtigungen nicht angezeigt.

Um sicherzustellen, dass Sie bei der Anzeige und Verwaltung von kontenübergreifenden Berechtigungen keine Zuschüsse verpassen, AWS Glue fordert Lake Formation und Sie auf, die folgenden Aktionen durchzuführen, um anzuzeigen, dass Sie sich der kontenübergreifenden Zuschüsse sowohl von Lake Formation als auch bewusst sind und diese zulassen. AWS Glue

Bei der Gewährung kontenübergreifender Berechtigungen mithilfe der AWS Glue Datenkatalog-Ressourcenrichtlinie

Wenn Ihr Konto (Förderkonto oder Produzentenkonto) keine kontoübergreifenden Zuschüsse gewährt hat, die AWS RAM zur gemeinsamen Nutzung der Ressourcen verwendet werden, können Sie eine Datenkatalog-Ressourcenrichtlinie wie gewohnt unter speichern. AWS Glue Wenn jedoch bereits Zuschüsse gewährt wurden, die gemeinsame Nutzung von AWS RAM Ressourcen beinhalten, müssen Sie einen der folgenden Schritte ausführen, um sicherzustellen, dass das Speichern der Ressourcenrichtlinie erfolgreich ist:

- Wenn Sie die Ressourcenrichtlinie auf der Seite Einstellungen der AWS Glue Konsole speichern, gibt die Konsole eine Warnung aus, dass die Berechtigungen in der Richtlinie zusätzlich zu den über die Lake Formation Formation-Konsole gewährten Berechtigungen gelten. Sie müssen Fortfahren wählen, um die Richtlinie zu speichern.
- Wenn Sie die Ressourcenrichtlinie mithilfe des `glue:PutResourcePolicy` API-Vorgangs speichern, müssen Sie das `EnableHybrid` Feld auf 'TRUE' (type = string) setzen.

Um eine bestehende Ressourcenrichtlinie zu aktualisieren, rufen Sie mithilfe des `glue:GetResourcePolicy` API-Vorgangs zunächst Ihre aktuelle Richtlinie ab und ändern Sie sie dann nach Bedarf, bevor Sie sie aufrufen `glue:PutResourcePolicy`.

 Note

Wenn Sie AWS Glue Ressourcenrichtlinien für den kontoübergreifenden Zugriff erstellen, gewähren Sie nur die Mindestberechtigungen, die für Ihren speziellen Anwendungsfall erforderlich sind.

Weitere Informationen finden Sie unter [PutResourcePolicy Action \(Python: put\\_resource\\_policy\)](#) im Developer Guide.AWS Glue

Bei der Gewährung kontoübergreifender Berechtigungen mithilfe der Lake Formation Formation-Methode für benannte Ressourcen

Wenn es in Ihrem Konto (Produzentenkonto) keine Datenkatalog-Ressourcenrichtlinie gibt, werden die von Ihnen gewährten kontoübergreifenden Zuschüsse von Lake Formation wie gewohnt durchgeführt. Wenn jedoch eine Datenkatalog-Ressourcenrichtlinie vorhanden ist, müssen Sie dieser die folgende Erklärung hinzufügen, damit Ihre kontoübergreifenden Zuschüsse erfolgreich sind, wenn sie mit der benannten Ressourcenmethode gewährt werden. `<region>` Ersetzen Sie es durch einen gültigen Regionsnamen und `<account-id>` durch Ihre AWS Konto-ID (Herstellerkonto-ID).

```
{
 "Effect": "Allow",
 "Action": [
 "glue:ShareResource"
],
 "Principal": {"Service": [
 "ram.amazonaws.com"
]},
 "Resource": [
 "arn:aws:glue:<region>:<account-id>:table/*/*",
 "arn:aws:glue:<region>:<account-id>:database/*",
 "arn:aws:glue:<region>:<account-id>:catalog"
]
}
```

Ohne diese zusätzliche Erklärung ist der Lake Formation Formation-Zuschuss erfolgreich, wird jedoch gesperrt AWS RAM, und das Empfängerkonto kann nicht auf die gewährte Ressource zugreifen.

#### Important

Wenn Sie die Tag-Based Access Control (LF-TBAC) -Methode von Lake Formation verwenden, um kontenübergreifende Zuschüsse zu gewähren, benötigen Sie eine Datenkatalog-Ressourcenrichtlinie mit mindestens den unter angegebenen Berechtigungen.

[Voraussetzungen](#)

#### Weitere Informationen finden Sie unter:

- [Zugriffskontrolle für Metadaten](#) (für eine Diskussion der benannten Ressourcenmethode im Vergleich zur Tag-Based Access Control (LF-TBAC) -Methode von Lake Formation).
- [Tabellen und Datenbanken des gemeinsamen Datenkatalogs anzeigen](#)
- [Arbeiten mit Datenkatalogeinstellungen auf der AWS Glue](#) Konsole im Entwicklerhandbuch AWS Glue
- [Gewähren von kontenübergreifendem Zugriff](#) im AWS Glue Entwicklerhandbuch (für Beispielrichtlinien für Datenkatalog-Ressourcen)



# Alle kontenübergreifenden Zuschüsse mithilfe des GetResourceShares API-Vorgangs anzeigen

Wenn Ihr Unternehmen kontenübergreifende Berechtigungen sowohl mithilfe einer AWS Glue Data Catalog Ressourcenrichtlinie als auch mithilfe von Lake Formation Formation-Zuschüssen gewährt, besteht die einzige Möglichkeit, alle kontenübergreifenden Zuschüsse an einem Ort anzuzeigen, darin, den `glue:GetResourceShares` API-Vorgang zu verwenden.

Wenn Sie Lake Formation mithilfe der benannten Ressourcenmethode kontenübergreifend Berechtigungen gewähren, erstellt AWS Resource Access Manager (AWS RAM) eine AWS Identity and Access Management (IAM-) Ressourcenrichtlinie und speichert sie in Ihrem AWS Konto. Die Richtlinie gewährt die für den Zugriff auf die Ressource erforderlichen Berechtigungen. AWS RAM erstellt für jeden kontenübergreifenden Zuschuss eine separate Ressourcenrichtlinie. Sie können all diese Richtlinien mithilfe des `glue:GetResourceShares` API-Vorgangs anzeigen.

## Note

Dieser Vorgang gibt auch die Datenkatalog-Ressourcenrichtlinie zurück. Wenn Sie jedoch die Metadatenverschlüsselung in den Datenkatalogeinstellungen aktiviert haben und keine Berechtigung für den AWS KMS Schlüssel haben, gibt der Vorgang die Datenkatalog-Ressourcenrichtlinie nicht zurück.

Um alle kontoübergreifenden Zuschüsse anzuzeigen

- Geben Sie den folgenden AWS CLI Befehl ein.

```
aws glue get-resource-policies
```

Im Folgenden finden Sie ein Beispiel für eine Ressourcenrichtlinie, die AWS RAM erstellt und gespeichert wird, wenn Sie dem AWS Konto 1111-2222-3333 Berechtigungen für eine Tabelle `t` in der Datenbank `db1` gewähren.

JSON

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

```
"Statement": [
 {
 "Effect": "Allow",
 "Action": [
 "glue:GetTable",
 "glue:GetTables",
 "glue:GetTableVersion",
 "glue:GetTableVersions",
 "glue:GetPartition",
 "glue:GetPartitions",
 "glue:BatchGetPartition",
 "glue:SearchTables"
],
 "Principal": {"AWS": [
 "111122223333"
]},
 "Resource": [
 "arn:aws:glue:us-east-1:111122223333:table/db1/t"
]
 }
]
```

 Weitere Informationen finden Sie auch unter:

- [GetResourceShares Action \(Python: `get\_resource\_policies`\)](#) im Developer Guide AWS Glue

## Zugreifen auf und Anzeigen von gemeinsam genutzten Datenkatalogtabellen und Datenbanken

Für den Data Lake-Administrator und für Principals, denen Berechtigungen erteilt wurden, werden Ressourcen, die mit Ihrem AWS Konto gemeinsam genutzt werden, im Datenkatalog so angezeigt, als wären sie Ressourcen in Ihrem Konto. In der Konsole wird das Konto angezeigt, dem die Ressource gehört.

Sie können Ressourcen, die mit Ihrem Konto geteilt werden, mithilfe der Lake Formation Formation-Konsole anzeigen. Sie können die Konsole AWS Resource Access Manager (AWS RAM) auch verwenden, um sowohl Ressourcen anzuzeigen, die mit Ihrem Konto gemeinsam genutzt wurden,

als auch Ressourcen, die Sie mit anderen AWS Konten geteilt haben, indem Sie die benannte Ressourcenmethode verwenden.

### Important

Wenn jemand die Methode der benannten Ressource verwendet, um Ihrem Konto oder Ihrer AWS Organisation kontenübergreifende Berechtigungen für eine Datenkatalogressource zu gewähren, verwendet Lake Formation den Dienst AWS Resource Access Manager (AWS RAM), um die Ressource gemeinsam zu nutzen. Wenn sich Ihr Konto in derselben AWS Organisation befindet wie das Erteilungskonto, steht Ihnen die gemeinsam genutzte Ressource sofort zur Verfügung.

Wenn sich Ihr Konto jedoch nicht in derselben Organisation befindet, AWS RAM sendet es eine Einladung an Ihr Konto, um die gemeinsame Nutzung der Ressource anzunehmen oder abzulehnen. Um die gemeinsam genutzte Ressource verfügbar zu machen, muss der Data Lake-Administrator in Ihrem Konto die Einladung AWS RAM über die Konsole oder CLI annehmen.

Die Lake Formation Konsole zeigt eine Warnung an, wenn eine Einladung zur gemeinsamen Nutzung von AWS RAM Ressourcen darauf wartet, akzeptiert zu werden. Nur Benutzer, die berechtigt sind, AWS RAM Einladungen anzusehen, erhalten die Warnung.

### Weitere Informationen finden Sie unter:

- [Gemeinsame Nutzung von Datenkatalogtabellen und Datenbanken für mehrere AWS Konten](#)
- [Kontoübergreifender Datenaustausch in Lake Formation](#)
- [Zugreifen auf die zugrunde liegenden Daten einer gemeinsam genutzten Tabelle](#)
- [Zugriffskontrolle für Metadaten](#) (für Informationen zur benannten Ressourcenmethode im Vergleich zur LF-TBAC-Methode zur gemeinsamen Nutzung von Ressourcen.)

## Themen

- [Annahme einer Einladung zur gemeinsamen Nutzung von Ressourcen AWS RAM](#)
- [Tabellen und Datenbanken des gemeinsamen Datenkatalogs anzeigen](#)

# Annahme einer Einladung zur gemeinsamen Nutzung von Ressourcen

## AWS RAM

Wenn eine Datenkatalogressource mit Ihrem AWS Konto geteilt wird und sich Ihr Konto nicht in derselben AWS Organisation wie das Freigabekonto befindet, haben Sie erst Zugriff auf die gemeinsam genutzte Ressource, wenn Sie eine Einladung zur Ressourcenfreigabe von AWS Resource Access Manager (AWS RAM) annehmen. Als Data Lake-Administrator müssen Sie zunächst AWS RAM nach ausstehenden Einladungen fragen und dann die Einladung annehmen.

Sie können die AWS RAM Konsole, die API oder AWS Command Line Interface (AWS CLI) verwenden, um Einladungen anzuzeigen und anzunehmen.

Um eine Einladung zur gemeinsamen Nutzung von Ressourcen von AWS RAM (Konsole) aus anzusehen und anzunehmen

1. Stellen Sie sicher, dass Sie über die erforderlichen AWS Identity and Access Management (IAM-) Berechtigungen verfügen, um Einladungen zur gemeinsamen Nutzung von Ressourcen anzuzeigen und anzunehmen.

Informationen zu den empfohlenen IAM-Richtlinien für Data Lake-Administratoren finden Sie unter [the section called “Berechtigungen des Data Lake-Administrators”](#)

2. Folgen Sie den Anweisungen unter [Einladungen annehmen und ablehnen](#) im AWS RAM Benutzerhandbuch.

So zeigen Sie eine Resource Share-Einladung von AWS RAM (AWS CLI) an und nehmen sie an

1. Stellen Sie sicher, dass Sie über die erforderlichen AWS Identity and Access Management (IAM-) Berechtigungen verfügen, um Einladungen zur gemeinsamen Nutzung von Ressourcen anzuzeigen und anzunehmen.

Informationen zu den empfohlenen IAM-Richtlinien für Data Lake-Administratoren finden Sie unter [the section called “Berechtigungen des Data Lake-Administrators”](#)

2. Geben Sie den folgenden Befehl ein, um ausstehende Einladungen zur gemeinsamen Nutzung von Ressourcen anzuzeigen.

```
aws ram get-resource-share-invitations
```

Die Ausgabe sollte folgendermaßen oder ähnlich aussehen.

```
{
 "resourceShareInvitations": [
 {
 "resourceShareInvitationArn": "arn:aws:ram:us-east-1:111122223333:resource-share-invitation/a93aa60a-1bd9-46e8-96db-a4e72eec1d9f",
 "resourceShareName": "111122223333-123456789012-uswuU",
 "resourceShareArn": "arn:aws:ram:us-east-1:111122223333:resource-share/2a4ab5fb-d859-4751-84f7-8760b35fc1fe",
 "senderAccountId": "111122223333",
 "receiverAccountId": "123456789012",
 "invitationTimestamp": 1589576601.79,
 "status": "PENDING"
 }
]
}
```

Notieren Sie sich den Status von PENDING.

3. Kopiert den Wert des `resourceShareInvitationArn` Schlüssels in die Zwischenablage.
4. Fügen Sie den Wert in den folgenden Befehl ein, ersetzen Sie ihn `<invitation-arn>`, und geben Sie den Befehl ein.

```
aws ram accept-resource-share-invitation --resource-share-invitation-arn <invitation-arn>
```

Die Ausgabe sollte folgendermaßen oder ähnlich aussehen.

```
{
 "resourceShareInvitations": [
 {
 "resourceShareInvitationArn": "arn:aws:ram:us-east-1:111122223333:resource-share-invitation/a93aa60a-1bd9-46e8-96db-a4e72eec1d9f",
 "resourceShareName": "111122223333-123456789012-uswuU",
 "resourceShareArn": "arn:aws:ram:us-east-1:111122223333:resource-share/2a4ab5fb-d859-4751-84f7-8760b35fc1fe",
 "senderAccountId": "111122223333",
 "receiverAccountId": "123456789012",
 "invitationTimestamp": 1589576601.79,
 "status": "ACCEPTED"
 }
]
}
```

```
}
]
}
```

Notieren Sie sich den Status von `ACCEPTED`.

## Tabellen und Datenbanken des gemeinsamen Datenkatalogs anzeigen

Sie können Ressourcen, die mit Ihrem Konto geteilt werden, mithilfe der Lake Formation Formation-Konsole oder AWS CLI anzeigen. Sie können auch die Konsole AWS Resource Access Manager (AWS RAM) oder die CLI verwenden, um sowohl Ressourcen anzuzeigen, die mit Ihrem Konto geteilt wurden, als auch Ressourcen, die Sie mit anderen AWS Konten geteilt haben.

So zeigen Sie gemeinsam genutzte Ressourcen mit der Lake Formation Formation-Konsole an

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

Melden Sie sich als Data Lake-Administrator oder als Benutzer an, dem Berechtigungen für eine gemeinsam genutzte Tabelle erteilt wurden.

2. Gehen Sie wie folgt vor, um Ressourcen anzuzeigen, die mit Ihrem AWS Konto gemeinsam genutzt werden:
  - Um Tabellen anzuzeigen, die mit Ihrem Konto gemeinsam genutzt werden, wählen Sie im Navigationsbereich Tabellen aus.
  - Um Datenbanken anzuzeigen, die mit Ihrem Konto gemeinsam genutzt werden, wählen Sie im Navigationsbereich Datenbanken aus.

In der Konsole wird eine Liste der Datenbanken oder Tabellen angezeigt, die sich sowohl in Ihrem Konto befinden als auch mit Ihrem Konto gemeinsam genutzt werden. Bei Ressourcen, die mit Ihrem Konto geteilt werden, zeigt die Konsole die AWS Konto-ID des Besitzers in der Spalte Besitzerkonto-ID an (die dritte Spalte im folgenden Screenshot).

**Tables (11)** ↻ Actions ▼ Create table using a crawler ↗ Create table

< 1 > ⚙️

|                       | Name ▼           | Database ▼ | Owner account ... ▼ | Shared resource ▼ | Shared resource owner ▼ |
|-----------------------|------------------|------------|---------------------|-------------------|-------------------------|
| <input type="radio"/> | adviews          | analytics  | 111122223333        | -                 | -                       |
| <input type="radio"/> | pageviews        | analytics  | 111122223333        | -                 | -                       |
| <input type="radio"/> | blackholes       | hubble     | 123456789012        | -                 | -                       |
| <input type="radio"/> | celestial-events | hubble     | 123456789012        | -                 | -                       |
| <input type="radio"/> | suns             | hubble     | 123456789012        | -                 | -                       |

- Um Ressourcen anzuzeigen, die Sie mit anderen AWS Konten oder Organisationen geteilt haben, wählen Sie im Navigationsbereich Datenberechtigungen aus.

Ressourcen, die Sie gemeinsam genutzt haben, werden auf der Seite Datenberechtigungen aufgeführt, wobei die externe Kontonummer in der Spalte Hauptbenutzer angezeigt wird, wie in der folgenden Abbildung dargestellt.

**Data permissions (4)** ↻ Revoke Grant

Choose a database or table for which to review, grant or revoke user permissions.

< 1 > ⚙️

Database: analytics X Table: clickthroughs X Clear filter

|                       | Principal ▼    | Principal type ▼ | Resource type ▼ | Resource ▼                | Owner account ID ▼ | Permissions ▼                      |
|-----------------------|----------------|------------------|-----------------|---------------------------|--------------------|------------------------------------|
| <input type="radio"/> | datalake_admin | IAM user         | Table           | clickthroughs             | 123456789012       | Super, Alter, Delete, Drop, Insert |
| <input type="radio"/> | datalake_admin | IAM user         | Column          | analytics.clickthroughs.* | 123456789012       | Select                             |
| <input type="radio"/> | 111122223333   | AWS account      | Table           | clickthroughs             | 123456789012       | Insert                             |
| <input type="radio"/> | 111122223333   | AWS account      | Column          | analytics.clickthroughs.* | 123456789012       | Select                             |

Um gemeinsam genutzte Ressourcen mit der AWS RAM Konsole anzuzeigen

- Stellen Sie sicher, dass Sie über die erforderlichen AWS Identity and Access Management (IAM-) Berechtigungen zum Anzeigen gemeinsam genutzter Ressourcen verfügen. AWS RAM

Sie benötigen mindestens die entsprechende Genehmigung. `ram:ListResources`  
Diese Berechtigung ist in der von AWS verwalteten Richtlinie enthalten.  
`AWSLakeFormationCrossAccountManager`

2. [Melden Sie sich bei der an AWS-Managementkonsole und öffnen Sie die AWS RAM Konsole zu Hause. https://console.aws.amazon.com/ram/](https://console.aws.amazon.com/ram/)
3. Führen Sie eine der folgenden Aktionen aus:
  - Um die von Ihnen freigegebenen Ressourcen anzuzeigen, wählen Sie im Navigationsbereich unter Von mir gemeinsam genutzt die Option Gemeinsam genutzte Ressourcen aus.
  - Um Ressourcen anzuzeigen, die für Sie freigegeben wurden, wählen Sie im Navigationsbereich unter Für mich freigegeben die Option Gemeinsam genutzte Ressourcen aus.

## Ressourcenlinks erstellen

Ressourcenlinks sind Datenkatalogobjekte, bei denen es sich um Links zu Metadatendatenbanken und Tabellen handelt — in der Regel zu gemeinsam genutzten Datenbanken und Tabellen aus anderen Konten. AWS ermöglicht den kontenübergreifenden Zugriff auf Daten im Data Lake in allen Regionen. AWS

### Note

Lake Formation unterstützt das Abfragen von Datenkatalogtabellen in allen AWS Regionen. Sie können von jeder AWS Region aus auf die Datenbanken und Tabellen des Datenkatalogs zugreifen, indem Sie in diesen Regionen Ressourcenlinks erstellen, die auf gemeinsam genutzte Datenbanken und Tabellen in verschiedenen Regionen verweisen.

### Themen

- [Funktionsweise von Ressourcenverbindungen in Lake Formation](#)
- [Einen Ressourcenlink zu einer gemeinsam genutzten Datenkatalogtabelle erstellen](#)
- [Einen Ressourcenlink zu einer gemeinsam genutzten Datenkatalog-Datenbank erstellen](#)
- [Umgang mit Ressourcenlinks in AWS Glue APIs](#)



## Funktionsweise von Ressourcenverbindungen in Lake Formation

Ein Ressourcenlink ist ein Datenkatalogobjekt, bei dem es sich um einen Link zu einer lokalen oder gemeinsam genutzten Datenbank oder Tabelle handelt. Nachdem Sie eine Ressourcenverknüpfung zu einer Datenbank oder Tabelle erstellt haben, können Sie den Namen der Ressourcenverknüpfung überall dort verwenden, wo Sie den Datenbank- oder Tabellennamen verwenden würden. Zusammen mit Tabellen, die Ihnen gehören, oder Tabellen, die mit Ihnen gemeinsam genutzt werden, werden Tabellenressourcen-Links von der Lake Formation Formation-Konsole zurückgegeben **glue:GetTables()** und als Einträge auf der Tabellenseite angezeigt. Ressourcenlinks zu Datenbanken verhalten sich ähnlich.

Wenn Sie eine Ressourcenverknüpfung zu einer Datenbank oder Tabelle erstellen, können Sie Folgendes tun:

- Weisen Sie einer Datenbank oder Tabelle in Ihrem Datenkatalog einen anderen Namen zu. Dies ist besonders nützlich, wenn verschiedene AWS Konten Datenbanken oder Tabellen mit demselben Namen gemeinsam nutzen oder wenn mehrere Datenbanken in Ihrem Konto Tabellen mit demselben Namen haben.
- Greifen Sie von jeder AWS Region aus auf die Datenbanken und Tabellen des Datenkatalogs zu, indem Sie in diesen Regionen Ressourcenlinks erstellen, die auf die Datenbank und Tabellen in einer anderen Region verweisen. Sie können Abfragen in jeder Region mit diesen Ressourcenlinks mithilfe von Athena und Amazon EMR ausführen und AWS Glue ETL Spark-Jobs ausführen, ohne Quelldaten oder Metadaten in Glue Data Catalog zu kopieren.
- Verwenden Sie integrierte AWS Services wie Amazon Athena Amazon Redshift Spectrum, um Abfragen auszuführen, die auf gemeinsam genutzte Datenbanken oder Tabellen zugreifen. Einige integrierte Dienste können nicht direkt kontenübergreifend auf Datenbanken oder Tabellen zugreifen. Sie können jedoch auf Ressourcenlinks in Ihrem Konto zu Datenbanken und Tabellen in anderen Konten zugreifen.

### Note

Sie müssen keinen Ressourcenlink erstellen, um in ETL-Skripts (AWS Glue Extrahieren, Transformieren und Laden) auf eine gemeinsam genutzte Datenbank oder Tabelle zu verweisen. Um jedoch Unklarheiten zu vermeiden, wenn mehrere AWS Konten eine Datenbank oder Tabelle mit demselben Namen gemeinsam nutzen, können Sie entweder

einen Ressourcenlink erstellen und verwenden oder beim Aufrufen von ETL-Vorgängen die Katalog-ID angeben.

Das folgende Beispiel zeigt die Tabellenseite der Lake Formation Formation-Konsole, auf der zwei Ressourcenlinks aufgeführt sind. Namen von Ressourcenlinks werden immer kursiv angezeigt. Jeder Ressourcenlink wird zusammen mit dem Namen und dem Besitzer der verknüpften gemeinsam genutzten Ressource angezeigt. In diesem Beispiel hat ein Data Lake-Administrator im AWS Konto 1111-2222-3333 die Tabellen `inventory` und `incidents` mit dem Konto 1234-5678-9012 geteilt. Ein Benutzer in diesem Konto hat dann Ressourcenlinks zu diesen gemeinsam genutzten Tabellen erstellt.

| Tables (30)                                           |                       |              |                              |                   |                       |
|-------------------------------------------------------|-----------------------|--------------|------------------------------|-------------------|-----------------------|
|                                                       |                       | Actions ▾    | Create table using a crawler | Create table      |                       |
| <input type="text" value="Find table by properties"/> |                       | < 1 >        |                              |                   |                       |
|                                                       | Name ▾                | Database ▾   | Owner account ... ▾          | Shared resource ▾ | Shared resource owner |
| <input type="radio"/>                                 | <i>inventory-link</i> | retail       | 123456789012                 | inventory         | 111122223333          |
| <input type="radio"/>                                 | <i>incidents-link</i> | issues-local | 123456789012                 | incidents         | 111122223333          |
| <input type="radio"/>                                 | site-logs             | logs         | 123456789012                 | -                 | -                     |
| <input type="radio"/>                                 | alexa-logs            | logs         | 123456789012                 | -                 | -                     |

Im Folgenden finden Sie Hinweise und Einschränkungen zu Ressourcenlinks:

- Ressourcenlinks sind erforderlich, damit integrierte Dienste wie Athena und Redshift Spectrum die zugrunde liegenden Daten gemeinsam genutzter Tabellen abfragen können. Abfragen in diesen integrierten Diensten werden anhand der Namen der Ressourcenlinks erstellt.
- Unter der Annahme, dass die Einstellung Nur IAM-Zugriffskontrolle für neue Tabellen in dieser Datenbank verwenden für die enthaltene Datenbank deaktiviert ist, kann nur der Prinzipal, der einen Ressourcenlink erstellt hat, ihn anzeigen und darauf zugreifen. Um anderen Prinzipalen in Ihrem Konto den Zugriff auf einen Ressourcenlink zu ermöglichen, erteilen Sie ihm die DESCRIBE entsprechende Berechtigung. Um es anderen zu ermöglichen, einen Ressourcenlink zu löschen, erteilen Sie ihm die DROP entsprechende Erlaubnis. Data Lake-Administratoren können auf alle Ressourcenlinks im Konto zugreifen. Um einen Ressourcenlink zu löschen, der von einem anderen Principal erstellt wurde, muss sich der Data Lake-Administrator zunächst selbst die DROP entsprechenden Berechtigungen für den Ressourcenlink erteilen. Weitere Informationen finden Sie unter [Referenz zu den Genehmigungen von Lake Formation](#).

 **Important**

Durch das Erteilen von Berechtigungen für einen Ressourcenlink werden keine Berechtigungen für die (verknüpfte) Zieldatenbank oder -tabelle gewährt. Sie müssen Berechtigungen für das Ziel separat gewähren.

- Um einen Ressourcenlink zu erstellen, benötigen Sie die Lake Formation `CREATE_TABLE` oder `CREATE_DATABASE` -Berechtigung sowie die `glue:CreateTable` oder `glue:CreateDatabase` AWS Identity and Access Management (IAM) -Berechtigung.
- Sie können Ressourcenlinks zu lokalen (eigenen) Datenkatalogressourcen sowie zu Ressourcen erstellen, die mit Ihrem AWS Konto gemeinsam genutzt werden.
- Wenn Sie einen Ressourcenlink erstellen, wird nicht geprüft, ob die gemeinsam genutzte Zielressource vorhanden ist oder ob Sie über kontoübergreifende Berechtigungen für die Ressource verfügen. Auf diese Weise können Sie den Ressourcenlink und die gemeinsam genutzte Ressource in beliebiger Reihenfolge erstellen.
- Wenn Sie einen Ressourcenlink löschen, wird die verknüpfte gemeinsam genutzte Ressource nicht gelöscht. Wenn Sie eine gemeinsam genutzte Ressource löschen, werden die Ressourcenlinks zu dieser Ressource nicht gelöscht.
- Es ist möglich, Linkketten für Ressourcen zu erstellen. Dies hat jedoch keinen Wert, da sie nur dem ersten Ressourcenlink APIs folgen.

 Weitere Informationen finden Sie auch unter:

- [Erteilen von Berechtigungen für Datenkatalogressourcen](#)

## Einen Ressourcenlink zu einer gemeinsam genutzten Datenkatalogtabelle erstellen

Sie können einen Ressourcenlink zu einer gemeinsam genutzten Tabelle in einer beliebigen AWS Region erstellen, indem Sie die AWS Lake Formation Konsole, die API oder AWS Command Line Interface (AWS CLI) verwenden.

Um einen Ressourcenlink zu einer gemeinsam genutzten Tabelle (Konsole) zu erstellen

1. Öffnen Sie die AWS Lake Formation Konsole unter <https://console.aws.amazon.com/lakeformation/>. Melden Sie sich als Principal an, der über die Lake Formation CREATE\_TABLE Formation-Berechtigung für die Datenbank verfügt, um den Ressourcenlink zu enthalten.
2. Wählen Sie im Navigationsbereich unter Datenkatalog die Option Tabellen und dann Erstellen, Ressourcenlink aus.
3. Geben Sie auf der Seite „Ressourcenlink erstellen“ die folgenden Informationen ein:

#### Name des Ressourcenlinks

Geben Sie einen Namen ein, der denselben Regeln entspricht wie ein Tabellename. Der Name kann mit dem Namen der gemeinsam genutzten Zieltabelle identisch sein.

#### Datenbank

Die Datenbank im lokalen Datenkatalog, die den Ressourcenlink enthalten soll.

#### Besitzer der gemeinsam genutzten Tabelle, Region

Wenn Sie den Ressourcenlink in einer anderen Region erstellen, wählen Sie die Region der gemeinsam genutzten Zieltabelle aus.

#### Gemeinsam genutzte Tabelle

Wählen Sie eine gemeinsam genutzte Tabelle aus der Liste aus, oder geben Sie einen Namen für eine lokale (eigene) oder gemeinsam genutzte Tabelle ein.

Die Liste enthält alle Tabellen, die mit Ihrem Konto geteilt wurden. Notieren Sie sich die Datenbank und die ID des Besitzerkontos, die in jeder Tabelle aufgeführt sind. Wenn Sie keine Tabelle sehen, von der Sie wissen, dass sie mit Ihrem Konto geteilt wurde, überprüfen Sie Folgendes:

- Wenn Sie kein Data Lake-Administrator sind, überprüfen Sie, ob der Data Lake-Administrator Ihnen Lake Formation Formation-Berechtigungen für die Tabelle erteilt hat.
- Wenn Sie ein Data Lake-Administrator sind und sich Ihr Konto nicht in derselben AWS Organisation wie das gewährende Konto befindet, stellen Sie sicher, dass Sie die Einladung AWS Resource Access Manager (AWS RAM) zur gemeinsamen Nutzung der Ressource für die Tabelle akzeptiert haben. Weitere Informationen finden Sie unter [Annahme einer Einladung zur gemeinsamen Nutzung von Ressourcen AWS RAM](#).

## Die Datenbank der gemeinsam genutzten Tabelle

Wenn Sie eine gemeinsam genutzte Tabelle aus der Liste ausgewählt haben, wird dieses Feld mit der Datenbank der gemeinsam genutzten Tabelle im externen Konto gefüllt. Geben Sie andernfalls eine lokale Datenbank (für einen Ressourcenlink zu einer lokalen Tabelle) oder die Datenbank der gemeinsam genutzten Tabelle in das externe Konto ein.

## Besitzer der gemeinsam genutzten Tabelle

Wenn Sie eine gemeinsam genutzte Tabelle aus der Liste ausgewählt haben, wird dieses Feld mit der Konto-ID des Besitzers der gemeinsam genutzten Tabelle gefüllt. Geben Sie andernfalls Ihre AWS Konto-ID (für einen Ressourcenlink zu einer lokalen Tabelle) oder die ID des AWS Kontos ein, das die Tabelle gemeinsam genutzt hat.

4. Wählen Sie Erstellen, um den Ressourcenlink zu erstellen.

Anschließend können Sie den Namen des Ressourcenlinks in der Spalte Name auf der Tabellenseite anzeigen.

5. (Optional) Erteilen Sie Prinzipalen, die in der Lage sein müssen, den Link anzuzeigen und auf die Zieltabelle zuzugreifen, die Lake Formation DESCRIBE Formation-Berechtigung für den Ressourcenlink.

Das Erteilen von Berechtigungen für einen Ressourcenlink gewährt jedoch keine Berechtigungen für die (verknüpfte) Zieldatenbank oder -tabelle. Sie müssen die Berechtigungen für die Zieldatenbank separat erteilen, damit der table/resource Link in Athena sichtbar ist.

Um einen Ressourcenlink zu einer gemeinsam genutzten Tabelle in derselben Region zu erstellen  
(AWS CLI)

1. Verwenden Sie einen Befehl ähnlich dem folgenden.

```
aws glue create-table --database-name myissues --table-input
'{"Name":"my_customers","TargetTable":
{"CatalogId":"111122223333","DatabaseName":"issues","Name":"customers"}}'
```

Dieser Befehl erstellt einen Ressourcenlink mit dem Namen my\_customers der gemeinsam genutzten Tabelle customers, die sich in der Datenbank issues im AWS Konto 1111-2222-3333 befindet. Der Ressourcenlink wird in der lokalen Datenbank gespeichert. myissues

2. (Optional) Erteilen Sie Prinzipalen, die in der Lage sein müssen, den Link anzuzeigen und auf die Zieltabelle zuzugreifen, die Lake Formation DESCRIBE Formation-Berechtigung für den Ressourcenlink.

Das Erteilen von Berechtigungen für einen Ressourcenlink gewährt jedoch keine Berechtigungen für die (verknüpfte) Zieltabelle. Sie müssen die Berechtigungen für die Zieldatenbank separat erteilen, damit der table/resource Link in Athena sichtbar ist.

Um einen Ressourcenlink zu einer gemeinsam genutzten Tabelle in einer anderen Region zu erstellen (AWS CLI)

1. Verwenden Sie einen Befehl ähnlich dem folgenden.

```
aws glue create-table --region eu-west-1 --cli-input-json '{
 "CatalogId": "111122223333",
 "DatabaseName": "ireland_db",
 "TableInput": {
 "Name": "rl_useast1salestb_ireland",
 "TargetTable": {
 "CatalogId": "444455556666",
 "DatabaseName": "useast1_salesdb",
 "Region": "us-east-1",
 "Name": "useast1_salestb"
 }
 }
}'
```

Mit diesem Befehl wird ein `rl_useast1salestb_ireland` in der Region Europa (Irland) benannter Ressourcenlink zu der gemeinsam genutzten Tabelle `useast1_salestb`, die sich in der Datenbank `useast1_salesdb` im AWS Konto `444455556666` in der Region USA Ost (Nord-Virginia) befindet. Der Ressourcenlink wird in der lokalen Datenbank gespeichert. `ireland_db`

2. Erteilen Sie die Lake DESCRIBE Formation den Principals, die in der Lage sein müssen, den Link zu sehen und über den Link auf das Linkziel zuzugreifen.

Das Erteilen von Berechtigungen für einen Ressourcenlink gewährt jedoch keine Berechtigungen für die (verknüpfte) Zieltabelle. Sie müssen die Berechtigungen für die Zieltabelle separat erteilen, damit der table/resource Link in Athena sichtbar ist.

 Weitere Informationen finden Sie auch unter:

- [Funktionsweise von Ressourcenverbindungen in Lake Formation](#)
- [DESCRIBE](#)

## Einen Ressourcenlink zu einer gemeinsam genutzten Datenkatalog-Datenbank erstellen

Sie können einen Ressourcenlink zu einer gemeinsam genutzten Datenbank mithilfe der AWS Lake Formation Konsole, der API oder AWS Command Line Interface (AWS CLI) erstellen.

Um einen Ressourcenlink zu einer gemeinsam genutzten Datenbank (Konsole) zu erstellen

1. Öffnen Sie die AWS Lake Formation Konsole unter <https://console.aws.amazon.com/lakeformation/>. Melden Sie sich als Data Lake-Administrator oder als Datenbankersteller an.

Ein Datenbankersteller ist ein Principal, dem die Lake Formation CREATE\_DATABASE Formation-Genehmigung erteilt wurde.

2. Wählen Sie im Navigationsbereich Datenbanken und dann Erstellen, Ressourcenlink aus.
3. Geben Sie auf der Seite „Ressourcenlink erstellen“ die folgenden Informationen ein:

Name des Ressourcenlinks

Geben Sie einen Namen ein, der denselben Regeln entspricht wie ein Datenbankname. Der Name kann mit dem der gemeinsam genutzten Zieldatenbank identisch sein.

Zielkatalog

Wählen Sie den Zielkatalog für den Datenbankressourcen-Link aus.

Gemeinsamer Datenbankbesitzer, Region

Wenn Sie den Ressourcenlink in einer anderen Region erstellen, wählen Sie die Region der gemeinsam genutzten Zieldatenbank aus.

Gemeinsam genutzte Datenbank

Wählen Sie eine Datenbank aus der Liste aus, oder geben Sie einen lokalen (eigenen) oder gemeinsamen Datenbanknamen ein.

Die Liste enthält alle Datenbanken, die mit Ihrem Konto gemeinsam genutzt werden. Notieren Sie sich die ID des Besitzerkontos, die in jeder Datenbank aufgeführt ist. Wenn Sie keine Datenbank sehen, von der Sie wissen, dass sie mit Ihrem Konto geteilt wurde, überprüfen Sie Folgendes:

- Wenn Sie kein Data Lake-Administrator sind, überprüfen Sie, ob der Data Lake-Administrator Ihnen Lake Formation-Berechtigungen für die Datenbank erteilt hat.
- Wenn Sie ein Data Lake-Administrator sind und sich Ihr Konto nicht in derselben AWS Organisation wie das gewährende Konto befindet, stellen Sie sicher, dass Sie die Einladung AWS Resource Access Manager (AWS RAM) zur gemeinsamen Nutzung von Ressourcen für die Datenbank akzeptiert haben. Weitere Informationen finden Sie unter [Annahme einer Einladung zur gemeinsamen Nutzung von Ressourcen AWS RAM](#).

#### Besitzer der gemeinsam genutzten Datenbank

Wenn Sie eine gemeinsam genutzte Datenbank aus der Liste ausgewählt haben, wird dieses Feld mit der Konto-ID des Besitzers der gemeinsam genutzten Datenbank gefüllt. Geben Sie andernfalls Ihre AWS Konto-ID (für einen Ressourcenlink zu einer lokalen Datenbank) oder die ID des AWS Kontos ein, das die Datenbank gemeinsam genutzt hat.

#### Die Katalog-ID der gemeinsam genutzten Datenbank

Geben Sie die Katalog-ID für die gemeinsam genutzte Datenbank ein. Wenn Sie einen Ressourcenlink zu einer Datenbank erstellen, die von einem anderen AWS Konto gemeinsam genutzt wird, müssen Sie diese Katalog-ID angeben, um zu identifizieren, welcher Datenkatalog die Quelldatenbank enthält.

Wenn Sie im Dropdownmenü eine gemeinsam genutzte Datenbank auswählen, gibt das System automatisch die Katalog-ID des Kontos ein, das diese Datenbank besitzt und für Sie freigegeben hat.



## Create resource link [Info](#)

### Database resource link details

Create a database resource link in the Data Catalog.

#### Resource link name

If you plan to access the database from Amazon Athena, then the name should be under 256 characters and contain only lowercase letters (a-z), numbers (0-9), and underscore (\_). For more information, see [Athena names](#).

#### Destination catalog

Select the destination catalog for the database resource link.

#### Shared database's region

Select the region of the shared database.

#### Shared database

Enter or choose a shared database.

#### Shared database's catalog ID

Enter the catalog ID of the shared database.

[Cancel](#)[Create](#)

4. Wählen Sie Erstellen, um den Ressourcenlink zu erstellen.

Anschließend können Sie den Namen des Ressourcenlinks in der Spalte Name auf der Datenbankseite anzeigen.

5. (Optional) Erteilen Sie Prinzipalen aus der Region Europa (Irland), die in der Lage sein müssen, den Link zu sehen und auf die Zieldatenbank zuzugreifen, die Lake Formation DESCRIBE Formation-Berechtigung für den Ressourcenlink.

Das Erteilen von Berechtigungen für einen Ressourcenlink gewährt jedoch keine Berechtigungen für die (verknüpfte) Zieldatenbank oder -tabelle. Sie müssen die Berechtigungen für die Zieldatenbank separat erteilen, damit der table/resource Link in Athena sichtbar ist.

Um einen Ressourcenlink zu einer gemeinsam genutzten Datenbank in derselben Region zu erstellen ()AWS CLI

1. Verwenden Sie einen Befehl ähnlich dem folgenden.

```
aws glue create-database --database-input '{"Name":"myissues","TargetDatabase":
{"CatalogId":"111122223333","DatabaseName":"issues"}}'
```

Dieser Befehl erstellt einen Ressourcenlink mit dem Namen myissues der gemeinsam genutzten Datenbank issues, die sich im AWS Konto 1111-2222-3333 befindet.

2. (Optional) Erteilen Sie die Lake Formation DESCRIBE Formation-Berechtigung den Prinzipalen für den Ressourcenlink, die in der Lage sein müssen, den Link anzuzeigen und auf die Zieldatenbank oder -tabelle zuzugreifen.

Das Erteilen von Berechtigungen für einen Ressourcenlink gewährt jedoch keine Berechtigungen für die (verknüpfte) Zieldatenbank oder -tabelle. Sie müssen die Berechtigungen für die Zieldatenbank separat erteilen, damit der table/resource Link in Athena sichtbar ist.

Um einen Ressourcenlink zu einer gemeinsam genutzten Datenbank in einer anderen Region zu erstellen ()AWS CLI

1. Verwenden Sie einen Befehl ähnlich dem folgenden.

```
aws glue create-database --region eu-west-1 --cli-input-json '{
 "CatalogId": "111122223333",
 "DatabaseInput": {
 "Name": "rl_useast1shared_irelanddb",
 "TargetDatabase": {
 "CatalogId": "444455556666",
 "DatabaseName": "useast1shared_db",
 "Region": "us-east-1"
 }
 }
}'
```

Dieser Befehl erstellt einen Ressourcenlink mit dem Namen 111122223333 rl\_useast1shared\_irelanddb in der AWS Region Europa (Irland) zur gemeinsam genutzten Datenbank useast1shared\_db, die sich im AWS Konto 444455556666 in der Region USA Ost (Nord-Virginia) befindet.

2. Erteilen Sie Principals aus der Region Europa (Irland), die in der Lage sein müssen, den Link zu sehen und über den Link auf das Linkziel zuzugreifen, die DESCRIBE Genehmigung für Lake Formation.

 Weitere Informationen finden Sie auch unter:

- [Funktionsweise von Ressourcenverbindungen in Lake Formation](#)
- [DESCRIBE](#)

## Umgang mit Ressourcenlinks in AWS Glue APIs

In den folgenden Tabellen wird erklärt, wie der AWS Glue Datenkatalog APIs mit Datenbank- und Tabellenressourcenlinks umgeht. Für alle Get \* API-Operationen werden nur Datenbanken und Tabellen zurückgegeben, für die der Aufrufer über Berechtigungen verfügt. Wenn Sie über einen Ressourcenlink auf eine Zieldatenbank oder -tabelle zugreifen, benötigen Sie außerdem sowohl AWS Identity and Access Management (IAM) als auch Lake Formation Formations-Berechtigungen sowohl für das Ziel als auch für den Ressourcenlink. Die Lake Formation Formations-Genehmigung, die für Ressourcenlinks erforderlich ist, lautet DESCRIBE. Weitere Informationen finden Sie unter [DESCRIBE](#).

### Datenbank-API-Operationen

| API-Operation  | Handhabung von Ressourcenlinks                                                                                                                                                                                                                                                                |
|----------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| CreateDatabase | Wenn es sich bei der Datenbank um einen Ressourcenlink handelt, wird der Ressourcenlink zur angegebenen Zieldatenbank erstellt.                                                                                                                                                               |
| UpdateDatabase | Wenn es sich bei der angegebenen Datenbank um einen Ressourcenlink handelt, folgt er dem Link und aktualisiert die Zieldatenbank. Wenn der Ressourcenlink geändert werden muss, um eine Verknüpfung mit einer anderen Datenbank herzustellen, müssen Sie ihn löschen und eine neue erstellen. |
| DeleteDatabase | Löscht den Ressourcenlink. Die verknüpfte (Ziel-) Datenbank wird nicht gelöscht.                                                                                                                                                                                                              |

| API-Operation | Handhabung von Ressourcenlinks                                                                                                                                                                                                                                                                                                        |
|---------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| GetDatabase   | Wenn der Aufrufer über Berechtigungen für das Ziel verfügt, folgt er dem Link, um die Eigenschaften des Ziels zurückzugeben. Andernfalls werden die Eigenschaften des Links zurückgegeben.                                                                                                                                            |
| GetDatabases  | Gibt eine Liste von Datenbanken zurück, einschließlich Ressourcenlinks. Für jeden Ressourcenlink in der Ergebnismenge folgt der Vorgang dem Link, um die Eigenschaften des Linkziels abzurufen. Sie müssen <code>ResourceShareType = angegebenALL</code> , um die Datenbanken zu sehen, die mit Ihrem Konto gemeinsam genutzt werden. |

## Tabellen-API-Operationen

| API-Operation | Handhabung von Ressourcenlinks                                                                                                                                                                                                                                                                                                                                                                          |
|---------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| CreateTable   | Wenn es sich bei der Datenbank um einen Ressourcenlink handelt, folgt er dem Datenbank-Link und erstellt eine Tabelle in der Zieldatenbank. Wenn es sich bei der Tabelle um einen Ressourcenlink handelt, erstellt der Vorgang den Ressourcenlink in der angegebenen Datenbank. Das Erstellen einer Tabellenressourcenverknüpfung über eine Datenbankressourcenverknüpfung wird nicht unterstützt.      |
| UpdateTable   | Wenn es sich bei der Tabelle oder der angegebenen Datenbank um einen Ressourcenlink handelt, wird die Zieltabelle aktualisiert. Wenn es sich sowohl bei der Tabelle als auch bei der Datenbank um Ressourcenlinks handelt, schlägt der Vorgang fehl.                                                                                                                                                    |
| DeleteTable   | Wenn es sich bei der angegebenen Datenbank um einen Ressourcenlink handelt, folgt er dem Link und löscht den Tabellen- oder Tabellenressourcenlink in der Zieldatenbank. Wenn es sich bei der Tabelle um einen Ressourcenlink handelt, löscht der Vorgang den Tabellenressourcenlink in der angegebenen Datenbank. Durch das Löschen eines Tabellenressourcenlinks wird die Zieltabelle nicht gelöscht. |

| API-Operation           | Handhabung von Ressourcenlinks                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                        |
|-------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| BatchDeleteTable        | Entspricht DeleteTable .                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                              |
| GetTable                | Wenn es sich bei der angegebenen Datenbank um einen Ressourcenlink handelt, folgt er dem Datenbank-Link und gibt den Tabellen- oder Tabellenressourcen-Link aus der Zieldatenbank zurück. Andernfalls, wenn es sich bei der Tabelle um einen Ressourcenlink handelt, folgt der Vorgang dem Link und gibt die Eigenschaften der Zieltabelle zurück.                                                                                                                                                                                                                                                                                                                                                                    |
| GetTables               | Wenn es sich bei der angegebenen Datenbank um einen Ressourcenlink handelt, folgt er dem Datenbank-Link und gibt die Tabellen und Tabellenressourcen-Links aus der Zieldatenbank zurück. Wenn es sich bei der Zieldatenbank um eine gemeinsam genutzte Datenbank eines anderen AWS Kontos handelt, gibt der Vorgang nur die gemeinsam genutzten Tabellen in dieser Datenbank zurück. Sie folgt nicht den Tabellenressourcen-Links in der Zieldatenbank. Andernfalls, wenn es sich bei der angegebenen Datenbank um eine lokale (eigene) Datenbank handelt, gibt der Vorgang alle Tabellen in der lokalen Datenbank zurück und folgt jedem Tabellenressourcenlink, um die Eigenschaften der Zieltabelle zurückzugeben. |
| SearchTables            | Gibt Tabellen und Tabellenressourcenlinks zurück. Es folgt keinen Links, um die Eigenschaften der Zieltabelle zurückzugeben. Sie müssen ResourceShareType = angeben, um Tabellen ALL zu sehen, die mit Ihrem Konto geteilt wurden.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                    |
| GetTableVersion         | Entspricht GetTable.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                  |
| GetTableVersions        | Entspricht GetTable.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                  |
| DeleteTableVersion      | Entspricht DeleteTable .                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                              |
| BatchDeleteTableVersion | Entspricht DeleteTable .                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                              |

## API-Operationen partitionieren

| API-Operation        | Handhabung von Ressourcenlinks                                                                                                                                                                                                                                                                                                                                                                                                                                                               |
|----------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| CreatePartition      | Wenn es sich bei der angegebenen Datenbank um einen Ressourcenlink handelt, folgt er dem Datenbank-Link und erstellt eine Partition in der angegebenen Tabelle in der Zieldatenbank. Wenn es sich bei der Tabelle um einen Ressourcenlink handelt, folgt der Vorgang dem Ressourcenlink und erstellt die Partition in der Zieltabelle. Das Erstellen einer Partition sowohl über einen Tabellenressourcenlink als auch über einen Datenbankressourcenlink wird nicht unterstützt.            |
| BatchCreatePartition | Entspricht CreatePartition .                                                                                                                                                                                                                                                                                                                                                                                                                                                                 |
| UpdatePartition      | Wenn es sich bei der angegebenen Datenbank um einen Ressourcenlink handelt, folgt er dem Datenbank-Link und aktualisiert die Partition in der angegebenen Tabelle in der Zieldatenbank. Wenn es sich bei der Tabelle um einen Ressourcenlink handelt, folgt der Vorgang dem Ressourcenlink und aktualisiert die Partition in der Zieltabelle. Das Aktualisieren einer Partition sowohl über einen Tabellenressourcenlink als auch über einen Datenbankressourcenlink wird nicht unterstützt. |
| DeletePartition      | Wenn es sich bei der angegebenen Datenbank um einen Ressourcenlink handelt, folgt er dem Datenbank-Link und löscht die Partition in der angegebenen Tabelle in der Zieldatenbank. Wenn es sich bei der Tabelle um einen Ressourcenlink handelt, folgt der Vorgang dem Ressourcenlink und löscht die Partition in der Zieltabelle. Das Löschen einer Partition sowohl über einen Tabellenressourcenlink als auch über einen Datenbankressourcenlink wird nicht unterstützt.                   |
| BatchDeletePartition | Entspricht DeletePartition .                                                                                                                                                                                                                                                                                                                                                                                                                                                                 |
| GetPartition         | Wenn es sich bei der angegebenen Datenbank um einen Ressourcenlink handelt, folgt er dem Datenbank-Link und gibt                                                                                                                                                                                                                                                                                                                                                                             |

| API-Operation     | Handhabung von Ressourcenlinks                                                                                                                                                                                                                                                                                                                                                                                                                                                          |
|-------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
|                   | Partitionsinformationen aus der angegebenen Tabelle zurück. Andernfalls, wenn es sich bei der Tabelle um einen Ressourcenlink handelt, folgt der Vorgang dem Link und gibt Partitionsinformationen zurück. Wenn es sich sowohl bei der Tabelle als auch bei der Datenbank um Ressourcenlinks handelt, wird eine leere Ergebnismenge zurückgegeben.                                                                                                                                      |
| GetPartitions     | Wenn es sich bei der angegebenen Datenbank um einen Ressourcenlink handelt, folgt er dem Datenbank-Link und gibt Partitionsinformationen für alle Partitionen in der angegebenen Tabelle zurück. Andernfalls, wenn es sich bei der Tabelle um einen Ressourcenlink handelt, folgt der Vorgang dem Link und gibt Partitionsinformationen zurück. Wenn es sich sowohl bei der Tabelle als auch bei der Datenbank um Ressourcenlinks handelt, wird eine leere Ergebnismenge zurückgegeben. |
| BatchGetPartition | Entspricht GetPartition .                                                                                                                                                                                                                                                                                                                                                                                                                                                               |

### API-Operationen mit benutzerdefinierten Funktionen

| API-Operation          | Handhabung von Ressourcenlinks                                                                                                              |
|------------------------|---------------------------------------------------------------------------------------------------------------------------------------------|
| (Alle API-Operationen) | Wenn es sich bei der Datenbank um einen Ressourcenlink handelt, folgt er dem Ressourcenlink und führt den Vorgang in der Zieldatenbank aus. |

 Weitere Informationen finden Sie auch unter:

- [Funktionsweise von Ressourcenverbindungen in Lake Formation](#)

# Regionsübergreifender Zugriff auf Tabellen

Lake Formation unterstützt das Abfragen von Datenkatalogtabellen in allen AWS Regionen. Sie können mit Amazon Athena, Amazon EMR und AWS Glue ETL von anderen Regionen aus auf Daten in einer Region zugreifen, indem Sie [Ressourcenlinks in anderen Regionen erstellen](#), die auf die Quelldatenbanken und -tabellen verweisen. Mit regionsübergreifendem Tabellenzugriff können Sie regionsübergreifend auf Daten zugreifen, ohne die zugrunde liegenden Daten oder Metadaten in den Datenkatalog kopieren zu müssen.

Sie können beispielsweise eine Datenbank oder Tabelle in einem Produzentenkonto für ein Verbraucherkonto in Region A gemeinsam nutzen. Nachdem Sie die Einladung zur gemeinsamen Nutzung von Ressourcen in Region A angenommen haben, kann der Data Lake-Administrator des Verbraucherkontos Ressourcenlinks zu der gemeinsam genutzten Ressource in Region B erstellen. Der Administrator des Verbraucherkontos kann den IAM-Prinzipalen in diesem Konto in Region A Berechtigungen für die gemeinsam genutzte Ressource gewähren und kann Ressourcenverknüpfungsberechtigungen in Region B gewähren. Mithilfe des Ressourcenlinks können die Prinzipale im Verbraucherkonto fragen Sie die gemeinsam genutzten Daten aus Region B ab.

Sie können die Amazon S3 S3-Datenquelle in Region A auch in einem Produzentenkonto hosten und den Datenstandort in einem zentralen Konto in Region B registrieren. Sie können Datenkatalogressourcen im zentralen Konto erstellen, Lake Formation Formation-Berechtigungen einrichten und Daten mit Verbrauchern in Ihrem Konto oder mit externen Konten in Region B teilen. Die regionsübergreifende Funktion ermöglicht Benutzern den Zugriff auf diese Datenkatalogtabellen von Region C aus über Ressourcenlinks.

Mit dieser Funktion können Sie Verbunddatenbanken in Apache Hive-Metastores regionsübergreifend abfragen und beim Ausführen von Abfragen auch Tabellen in der lokalen Region mit Tabellen in einer anderen Region verbinden.

Lake Formation unterstützt die folgenden Funktionen mit regionsübergreifendem Tabellenzugriff:

- Zugriffskontrolle auf Basis von LF-Tags
- Fein abgestufte Zugriffsberechtigungen
- Schreibvorgänge in der gemeinsam genutzten Datenbank oder Tabelle mit den entsprechenden Berechtigungen
- Kontoübergreifender Datenaustausch auf Kontoebene und direkt mit IAM-Prinzipalen



Benutzer ohne Administratorrechte mit `Create_Database` und `-Berechtigungen` können regionsübergreifende Ressourcenlinks erstellen. `Create_Table`

 Note

Sie können regionsübergreifende Ressourcenlinks in jeder Region erstellen und auf Daten zugreifen, ohne Lake Formation Formation-Berechtigungen anzuwenden. Für Quelldaten in Amazon S3, die nicht bei Lake Formation registriert sind, wird der Zugriff durch IAM-Berechtigungsrichtlinien für Amazon S3 und AWS Glue Aktionen bestimmt.

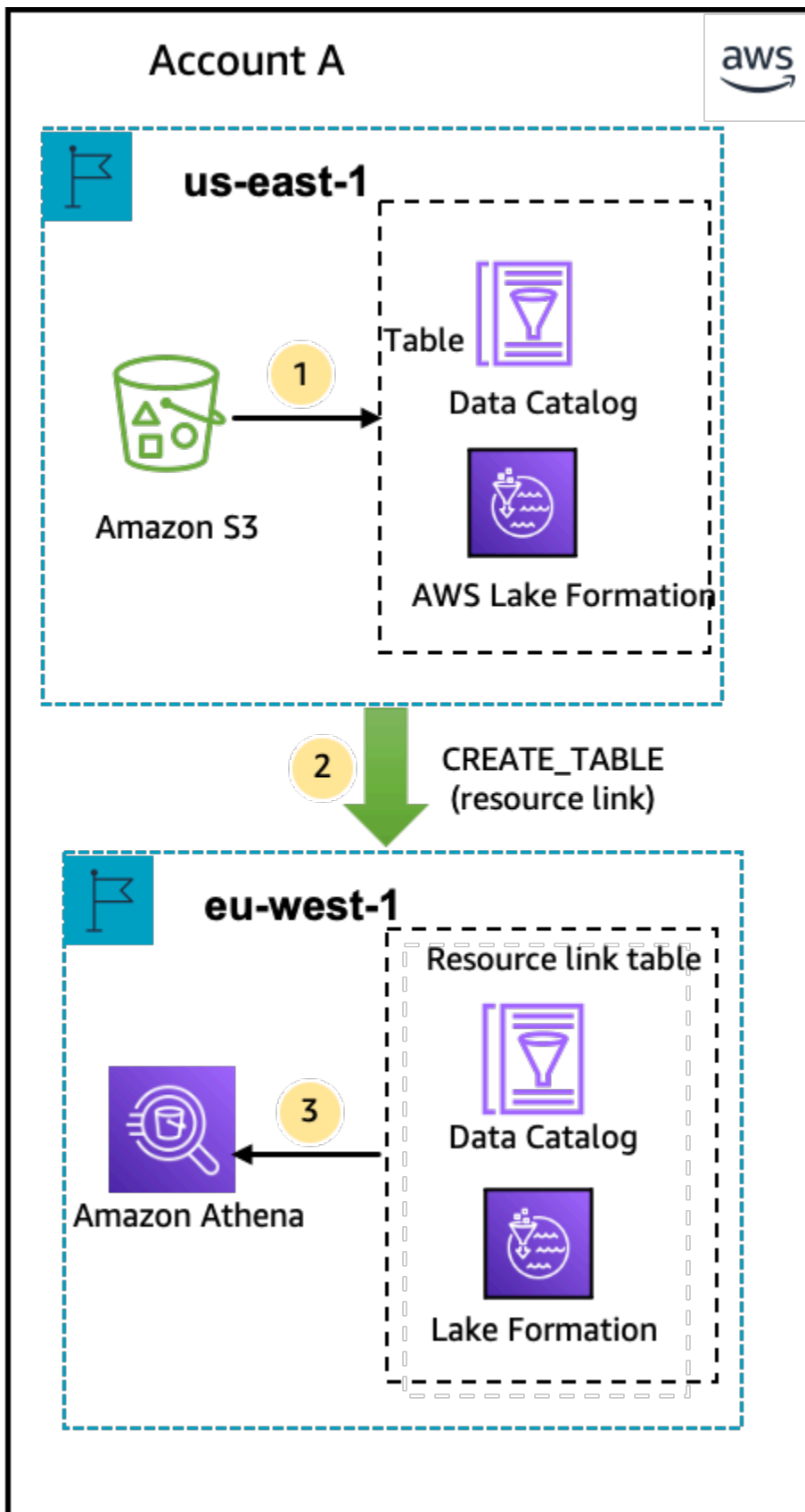
Einschränkungen finden Sie unter [Regionsübergreifende Beschränkungen des Datenzugriffs](#).

## Arbeitsabläufe

Die folgenden Diagramme zeigen die Workflows für den Zugriff auf Daten in verschiedenen AWS Regionen von demselben AWS Konto und von einem externen Konto aus.

Workflow für den Zugriff auf Tabellen, die innerhalb desselben AWS Kontos gemeinsam genutzt werden

In der Abbildung unten werden die Daten mit einem Benutzer desselben AWS Kontos in der Region USA Ost (Nord-Virginia) geteilt, und der Benutzer fragt die gemeinsam genutzten Daten aus der Region Europa (Irland) ab.



Der Data Lake-Administrator führt die folgenden Aktivitäten aus (Schritte 1—2):

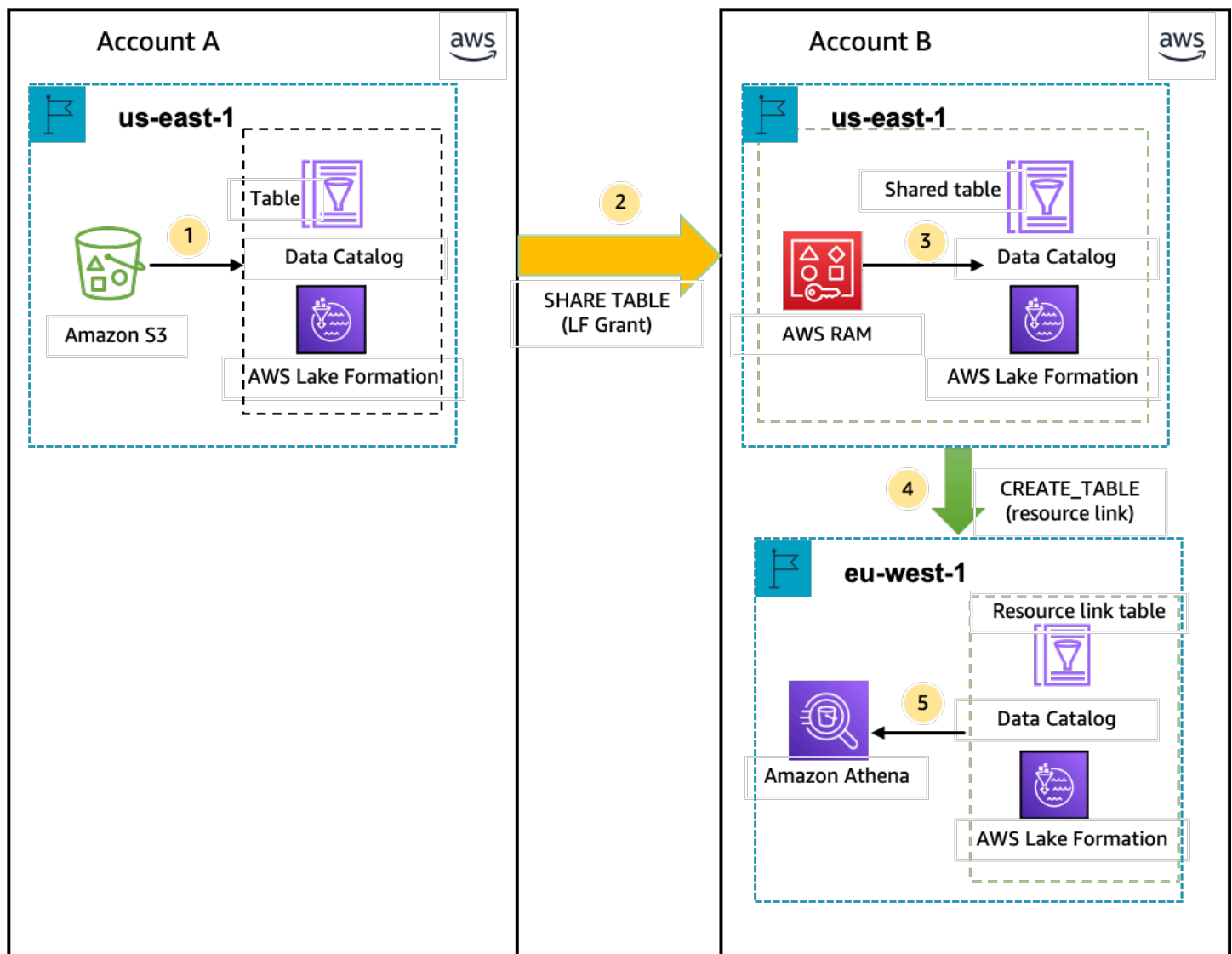
1. Ein Data Lake-Administrator richtet ein AWS Konto bei den Data Catalog-Datenbanken und -Tabellen ein und registriert einen Amazon S3 S3-Datenstandort bei Lake Formation in der Region USA Ost (Nord-Virginia).

Erteilt einem Principal (Benutzer) desselben Kontos die `Select` Berechtigung für eine Datenkatalogressource (Produkttable im Diagramm).

2. Erstellt einen Ressourcenlink in der Region Europa (Irland), der auf die Quelltable in der Region USA Ost (Nord-Virginia) verweist. Erteilt dem Auftraggeber die `DESCRIBE` Genehmigung für den Ressourcenlink von der Region Europa (Irland).
3. Der Benutzer fragt die Table mit Athena aus der Region Europa (Irland) ab.

Workflow für den Zugriff auf Tabellen, die mit einem externen AWS Konto gemeinsam genutzt werden

In der Abbildung unten hostet das Produzentenkonto (Konto A) den Amazon S3 S3-Bucket, registriert den Datenstandort und teilt eine Datenkatalogtable mit einem Verbraucherkonto (Konto B) in der Region USA Ost (Nord-Virginia), und ein Benutzer des Verbraucherkontos (Konto B) fragt die Table aus der Region Europa (Irland) ab.



1. Ein Data Lake-Administrator richtet ein AWS Konto (Producer-Konto) mit den Data Catalog-Ressourcen und einem Amazon S3 S3-Datenstandort ein, der bei Lake Formation in der Region USA Ost (Nord-Virginia) registriert ist.
2. Der Data Lake-Administrator des Produzentenkontos teilt eine Datenkatalogtabelle mit einem Kundenkonto.
3. Der Data Lake-Administrator des Verbraucherkontos nimmt die Einladung zur gemeinsamen Nutzung von Daten in der Region USA Ost (Nord-Virginia) an und erteilt einem Principal aus derselben Region die `Select` Erlaubnis für die gemeinsam genutzte Tabelle.
4. Der Data Lake-Administrator des Verbraucherkontos erstellt einen Ressourcenlink in der Region Europa (Irland), der auf die gemeinsam genutzte Zieltabelle in der Region USA Ost (Nord-Virginia)

verweist, und erteilt dem Benutzer die DESCRIBE Berechtigung für den Ressourcenlink aus der Region Europa (Irland).

5. Der Benutzer fragt die Daten aus der Region Europa (Irland) mit Athena ab.

## Einrichtung des regionsübergreifenden Tabellenzugriffs

Um auf Daten aus einer anderen Region zuzugreifen, müssen Sie zunächst die Datenkatalog-Datenbanken und -Tabellen in der Region einrichten, in der Sie Ihren Amazon S3 S3-Datenstandort registrieren. Sie können die Data Catalog-Datenbanken und -Tabellen mit Principals in Ihrem Konto oder in einem anderen Konto teilen. Anschließend müssen Sie Data Lake-Administratoren einrichten, die Ressourcenlinks erstellen können, die auf den gemeinsam genutzten Zieldatenspeicherort in den Regionen verweisen, in denen Benutzer die Daten abfragen.

Um innerhalb desselben Kontos gemeinsam genutzte Daten aus einer anderen Region abzufragen

In diesem Abschnitt wird die gemeinsam genutzte Zieltabelle Region als Region A bezeichnet, und Benutzer führen Abfragen aus Region B aus.

### 1. Kontoeinrichtung in Region A (wo Sie die Daten erstellen und teilen)

Ein Data Lake-Administrator muss die folgenden Aktionen ausführen:

- a. Registrieren Sie einen Amazon S3 S3-Datenstandort.

Weitere Informationen finden Sie unter [Hinzufügen eines Amazon S3 S3-Standorts zu Ihrem Data Lake](#).

- b. Erstellen Sie Datenbanken und Tabellen im Konto. Dies kann auch von einem Benutzer ohne Administratorrechte ausgeführt werden, der über die Berechtigungen zum Erstellen von Datenbanken und Tabellen verfügt.
- c. Erteilen Sie den Prinzipalen Datenberechtigungen für eine Tabelle mit. `Grantable permissions`

Weitere Informationen finden Sie unter [Erteilen von Berechtigungen für Datenkatalogressourcen](#).

### 2. Kontoeinrichtung in Region B (wo Sie auf die Daten zugreifen)

Ein Data Lake-Administrator muss die folgenden Aktionen ausführen:

- a. Erstellen Sie in Region B einen Ressourcenlink, der auf die gemeinsam genutzte Zieltabelle in Region A verweist. Geben Sie auf dem Bildschirm Tabelle erstellen die Region des Besitzers der gemeinsamen Tabelle an.

## Create table

### Table details

Create a table in the AWS Glue Data Catalog.

☐ **Table**  
Create a table in my account.

☒ **Resource link**  
Create a resource link to a shared table.

**Resource link name**  
  
Name may contain letters (A-Z), numbers (0-9), hyphens (-), or underscores (\_), and must be less than 256 characters long.

**Database**  
Resource link will be contained in this database.

**Shared table owner region**  
Select the region where the table is shared  

US West (N. California) ▼

**Shared table**  
Enter or choose a shared table.

**Shared table's database**  
Enter the database containing the shared table.

**Shared table's owner ID**  
Enter the AWS account ID of the shared table owner.

**Cancel** **Create**

Anweisungen zum Erstellen von Ressourcenlinks zu Datenbanken und Tabellen finden Sie unter [Ressourcenlinks erstellen](#).

- b. Erteilen Sie IAM-Prinzipalen die `Describe` Berechtigung für den Ressourcenlink in Region B.

Weitere Informationen zum Erteilen von Berechtigungen für Ressourcenlinks finden Sie unter [Erteilen von Ressourcenverknüpfungsberechtigungen](#)

IAM-Prinzipale in Region B können die Zieltabelle über den Link mit Athena abfragen.

Um auf kontenübergreifende Daten aus einer anderen Region zuzugreifen

## 1. Einrichtung eines Kontos für Produzent/Förderer

Ein Data Lake-Administrator muss die folgenden Aktionen ausführen:

- a. Richten Sie das `producer/grantor` Konto in Region A ein.
- b. Registrieren Sie einen Amazon S3 S3-Datenstandort in Region A.
- c. Erstellen Sie Datenbanken und Tabellen. Dies kann von einem Benutzer ohne Administratorrechte ausgeführt werden, der über die Berechtigungen zum Erstellen von Tabellen verfügt.
- d. Erteilen Sie dem `consumer/grantee` Konto Datenberechtigungen für eine Tabelle in Region A mit `Grantable permissions`.

Weitere Informationen finden Sie unter [Gemeinsame Nutzung von Datenkatalogtabellen und Datenbanken für mehrere AWS-Konten IAM-Prinzipale von externen Konten aus](#).

## 2. Einrichtung eines Verbraucher-/Empfängerkontos

Ein Data Lake-Administrator muss die folgenden Aktionen ausführen:

- a. Nehmen Sie die Einladung zur gemeinsamen Nutzung von Ressourcen aus AWS RAM Region A an.
- b. Erstellen Sie einen Ressourcenlink in Region B, der auf die gemeinsam genutzte Tabelle verweist. In Region B möchten Benutzer die Tabelle abfragen.
- c. Erteilen Sie IAM-Prinzipalen in Region A Datenberechtigungen für die gemeinsam genutzte Tabelle.

 Note

Sie müssen Berechtigungen für die gemeinsam genutzte Tabelle in derselben Region gewähren, in der die Tabelle gemeinsam genutzt wurde.

- d. Erteilen Sie den Prinzipalen Berechtigungen für den Ressourcenlink in Region B.

Principals im Verbraucherkonto in Region B fragen dann mithilfe von Athena die gemeinsam genutzte Tabelle aus Region B ab.



# Sicherheit in AWS Lake Formation

Cloud-Sicherheit AWS hat höchste Priorität. Als AWS Kunde profitieren Sie von einer Rechenzentrums- und Netzwerkarchitektur, die darauf ausgelegt sind, die Anforderungen der sicherheitssensibelsten Unternehmen zu erfüllen.

Sicherheit ist eine gemeinsame Verantwortung von Ihnen AWS und Ihnen. Das [Modell der geteilten Verantwortung](#) beschreibt dies als Sicherheit der Cloud und Sicherheit in der Cloud:

- **Sicherheit der Cloud** — AWS ist verantwortlich für den Schutz der Infrastruktur, die AWS Dienste in der AWS Cloud ausführt. AWS bietet Ihnen auch Dienste, die Sie sicher nutzen können. Auditoren von Drittanbietern testen und überprüfen die Effektivität unserer Sicherheitsmaßnahmen im Rahmen der [AWS -Compliance-Programme](#) regelmäßig. Weitere Informationen zu den Compliance-Programmen, die für gelten AWS Lake Formation, finden Sie unter [AWS Services in Umfang nach Compliance-Programmen](#).
- **Sicherheit in der Cloud** — Ihre Verantwortung richtet sich nach dem AWS Dienst, den Sie nutzen. Sie sind auch für andere Faktoren verantwortlich, etwa für die Vertraulichkeit Ihrer Daten, für die Anforderungen Ihres Unternehmens und für die geltenden Gesetze und Vorschriften.

Diese Dokumentation hilft Ihnen zu verstehen, wie Sie das Modell der gemeinsamen Verantwortung bei der Verwendung von Lake Formation anwenden können. In den folgenden Themen erfahren Sie, wie Sie Lake Formation konfigurieren, um Ihre Sicherheits- und Compliance-Ziele zu erreichen. Sie lernen auch, wie Sie andere AWS Dienste nutzen können, mit denen Sie Ihre Lake Formation Formation-Ressourcen überwachen und sichern können.

## Topics

- [Datenschutz bei Lake Formation](#)
- [Infrastruktursicherheit in AWS Lake Formation](#)
- [Serviceübergreifende Confused-Deputy-Prävention](#)
- [Anmeldung bei Sicherheitsereignissen AWS Lake Formation](#)

## Datenschutz bei Lake Formation

Das AWS [Modell](#) der gilt für den Datenschutz in AWS Lake Formation. 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 Informationen zur Verwendung von CloudTrail Pfaden zur Erfassung von AWS Aktivitäten finden Sie unter [Arbeiten mit CloudTrail Pfaden](#) im AWS CloudTrail Benutzerhandbuch.
- 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 140-3-validierte kryptografische Module benötigen, verwenden Sie einen FIPS-Endpunkt. Weitere Informationen über verfügbare FIPS-Endpunkte finden Sie unter [Federal Information Processing Standard \(FIPS\) 140-3](#).

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 Lake Formation oder anderen AWS-Services über die Konsole AWS CLI, API oder arbeiten AWS SDKs. 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

AWS Lake Formation unterstützt Datenverschlüsselung in den folgenden Bereichen:

- Daten in Ihrem Amazon Simple Storage Service (Amazon S3) Data Lake.

Lake Formation unterstützt Datenverschlüsselung mit [AWS Key Management Service](#) (AWS KMS). Daten werden in der Regel mit folgenden Methoden in den Data Lake geschrieben: AWS Glue Extrahieren, Transformieren und Laden (ETL) Jobs. Für Informationen zur Verschlüsselung von Daten, die geschrieben wurden von AWS Glue Jobs, finden Sie unter [Verschlüsselung von Daten, die von Crawlern, Jobs und Entwicklungsendpunkten geschrieben wurden im Entwicklerhandbuch](#). AWS Glue

- Der AWS Glue Data Catalog, wo Lake Formation Metadatatabellen speichert, die Daten im Data Lake beschreiben.

Weitere Informationen finden Sie unter [Verschlüsseln Ihres Datenkatalogs](#) im AWS Glue Entwicklerhandbuch.

Um einen Amazon S3 S3-Standort als Speicher in Ihrem Data Lake hinzuzufügen, registrieren Sie den Standort bei AWS Lake Formation. Anschließend können Sie Lake Formation Berechtigungen für eine detaillierte Zugriffskontrolle auf AWS Glue Data Catalog Objekte verwenden, die auf diese Position verweisen, und auf die zugrunde liegenden Daten in der Position.

Lake Formation unterstützt die Registrierung eines Amazon S3 S3-Standorts, der verschlüsselte Daten enthält. Weitere Informationen finden Sie unter [Registrierung eines verschlüsselten Amazon S3 S3-Standorts](#).

## Infrastruktursicherheit in AWS Lake Formation

Als verwalteter Service AWS Lake Formation ist er durch die AWS globalen Netzwerksicherheitsverfahren geschützt, die im Whitepaper [Amazon Web Services: Sicherheitsprozesse im Überblick](#) beschrieben sind.

Sie verwenden AWS veröffentlichte API-Aufrufe, um über das Netzwerk auf Lake Formation zuzugreifen. Kunden müssen Transport Layer Security (TLS) 1.0 oder neuer unterstützen. Wir empfehlen TLS 1.2 oder höher. Clients müssen außerdem Verschlüsselungssammlungen mit PFS (Perfect Forward Secrecy) wie DHE (Ephemeral Diffie-Hellman) oder ECDHE (Elliptic Curve

Ephemeral Diffie-Hellman) unterstützen. 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.

## Serviceübergreifende Confused-Deputy-Prävention

Das Confused-Deputy-Problem ist ein Sicherheitsproblem, bei dem eine juristische Stelle, die nicht über die Berechtigung zum Ausführen einer Aktion verfügt, eine privilegiertere juristische Stelle zwingen kann, die Aktion auszuführen. In AWS, dienstübergreifender Identitätswechsel kann zum Problem des verwirrten Stellvertreters führen. Ein dienstübergreifender Identitätswechsel kann auftreten, wenn ein Dienst (der Anruf-Dienst) einen anderen Dienst anruft (den aufgerufenen Dienst). Der Anruf-Dienst kann so manipuliert werden, dass er seine Berechtigungen verwendet, um auf die Ressourcen eines anderen Kunden zu reagieren, auf die er sonst nicht zugreifen dürfte. Um dies zu verhindern, AWS bietet Tools, mit denen Sie Ihre Daten für alle Dienste mit Dienstprinzipalen schützen können, denen Zugriff auf Ressourcen in Ihrem Konto gewährt wurde.

Wir empfehlen die Verwendung der globalen Bedingungskontext-Schlüssel [aws:SourceArn](#) und [aws:SourceAccount](#) in ressourcenbasierten Richtlinien, um die Berechtigungen, die AWS Lake Formation einem anderen Service erteilt, auf eine bestimmte Ressource einzuschränken. Wenn Sie beide globalen Bedingungskontextschlüssel verwenden, müssen der `aws:SourceAccount`-Wert und das Konto im `aws:SourceArn`-Wert dieselbe Konto-ID verwenden, wenn sie in derselben Richtlinienanweisung verwendet werden.

Derzeit unterstützt `aws:SourceArn` Lake Formation nur das folgende Format:

```
arn:aws:lakeformation:aws-region:account-id:*
```

Das folgende Beispiel zeigt, wie Sie die Kontextschlüssel `aws:SourceArn` und die `aws:SourceAccount` globalen Bedingungsschlüssel in Lake Formation verwenden können, um das Problem des verwirrten Stellvertreters zu verhindern.

JSON

```
{
```

```

"Version": "2012-10-17",
"Statement": [
 {
 "Sid": "ConfusedDeputyPreventionExamplePolicy",
 "Effect": "Allow",
 "Principal": {
 "Service": "lakeformation.amazonaws.com"
 },
 "Action": [
 "sts:AssumeRole"
],
 "Condition": {
 "StringEquals": {
 "aws:SourceAccount": "123456789012"
 },
 "ArnEquals": {
 "aws:SourceArn": "arn:aws:lakeformation:aws-region:123456789012:*"
 }
 }
 }
]
}

```

## Anmeldung bei Sicherheitsereignissen AWS Lake Formation

AWS Lake Formation ist in einen Dienst integriert AWS CloudTrail, der eine Aufzeichnung der Aktionen bereitstellt, die von einem Benutzer, einer Rolle oder einem AWS Dienst in Lake Formation ausgeführt wurden. CloudTrail erfasst alle API-Aufrufe für Lake Formation als Ereignisse. Zu den erfassten Aufrufen gehören Aufrufe von der Lake Formation Formation-Konsole AWS Command Line Interface, die und Codeaufrufen an die Lake Formation Formation-API-Operationen.

Weitere Informationen zur Ereignisprotokollierung in Lake Formation finden Sie unter [Protokollieren AWS Lake Formation Formation-API-Aufrufen mit AWS CloudTrail](#).

### Note

GetTableObjectsUpdateTableObjects, und GetWorkUnitResults sind Datenebenenoperationen mit hohem Datenvolumen. Anrufe an diese APIs werden derzeit nicht protokolliert. CloudTrail Weitere Informationen zu Vorgängen auf Datenebene finden Sie

unter [Protokollieren von Datenereignissen für Pfade](#) im AWS CloudTrail Benutzerhandbuch.  
CloudTrail  
Änderungen in der Lake Formation zur Unterstützung zusätzlicher CloudTrail  
Veranstaltungen werden unter dokumentiert [Dokumentenverlauf für AWS Lake Formation](#).

# Integration von Diensten von Drittanbietern mit Lake Formation

Durch die Integration mit AWS Lake Formation können Drittanbieter-Services sicher auf Daten in ihren Amazon S3 S3-basierten Data Lakes zugreifen. Sie können Lake Formation als Autorisierungs-Engine verwenden, um Berechtigungen für Ihren Data Lake mit integrierten AWS Services wie AWS Glue ETL, Amazon Athena, Amazon EMR und Redshift Spectrum zu verwalten oder durchzusetzen. Lake Formation bietet zwei Optionen für die Integration von Diensten:

1. Die Anwendungsintegrationseinstellungen von Lake Formation: Lake Formation kann begrenzte temporäre Anmeldeinformationen in Form von AWS STS-Token an registrierte Amazon S3 S3-Standorte auf der Grundlage der geltenden Berechtigungen verkaufen, sodass autorisierte Anwendungen im Namen von Benutzern auf Daten zugreifen können.
2. Zentrale Durchsetzung: Bei [API-Abfragen](#) von Lake Formation werden Daten aus Amazon S3 abgerufen und die Ergebnisse anhand effektiver Berechtigungen gefiltert. Die Engine oder Anwendung, die in den abfragenden API-Vorgang integriert wird, kann sich darauf verlassen, dass Lake Formation die Berechtigungen der aufrufenden Identität auswertet und die Daten auf der Grundlage dieser Berechtigungen sicher filtert. Abfrage-Engines von Drittanbietern können nur gefilterte Daten sehen und verarbeiten.

Der Verkauf von Anmeldedaten von Lake Formation lässt sich nicht in Spark-SQL-Abfragen integrieren. Der Verkauf von Anmeldeinformationen funktioniert nur mit Abfragen, die über die AWS Glue ETL-Bibliothek ausgeführt werden.

## Themen

- [Verwenden der Anwendungsintegration von Lake Formation](#)

## Verwenden der Anwendungsintegration von Lake Formation

Lake Formation ermöglicht es Drittanbietern, sich in Lake Formation zu integrieren und im Namen ihrer Benutzer durch Nutzung [GetTemporaryGlueTableCredentials](#) und [GetTemporaryGluePartitionCredentials](#) Betrieb temporären Zugriff auf Amazon S3 S3-Daten zu erhalten. Auf diese Weise können Dienste von Drittanbietern dieselbe Autorisierungs- und Verkaufsfunktion für Anmeldeinformationen verwenden wie die übrigen AWS Analysedienste. In

diesem Abschnitt wird beschrieben, wie Sie diese API-Operationen verwenden, um eine Abfrage-Engine eines Drittanbieters zu integrieren. Lake Formation

Diese API-Operationen sind standardmäßig deaktiviert. Es gibt zwei Möglichkeiten, Lake Formation zur Integration von Anwendungen zu autorisieren:

- Konfigurieren Sie IAM-Sitzungs-Tags, die bei jedem Aufruf der API-Operationen für die Anwendungsintegration validiert werden

Weitere Informationen finden Sie unter [Aktivierung von Berechtigungen für eine Abfrage-Engine eines Drittanbieters zum Aufrufen von API-Operationen für die Anwendungsintegration](#).

- Aktivieren Sie die Option, die externen Engines den Zugriff auf Daten an Amazon S3 S3-Standorten mit vollständigem Tabellenzugriff ermöglicht

Diese Option ermöglicht es Abfrage-Engines und Anwendungen, Anmeldeinformationen ohne IAM-Sitzungs-Tags abzurufen, wenn der Benutzer vollen Tabellenzugriff hat. Sie bietet Leistungsvorteile für Abfrage-Engines und Anwendungen und vereinfacht den Datenzugriff. Amazon EMR auf Amazon EC2 kann diese Einstellung nutzen.

Weitere Informationen finden Sie unter [Anwendungsintegration für vollständigen Tabellenzugriff](#).

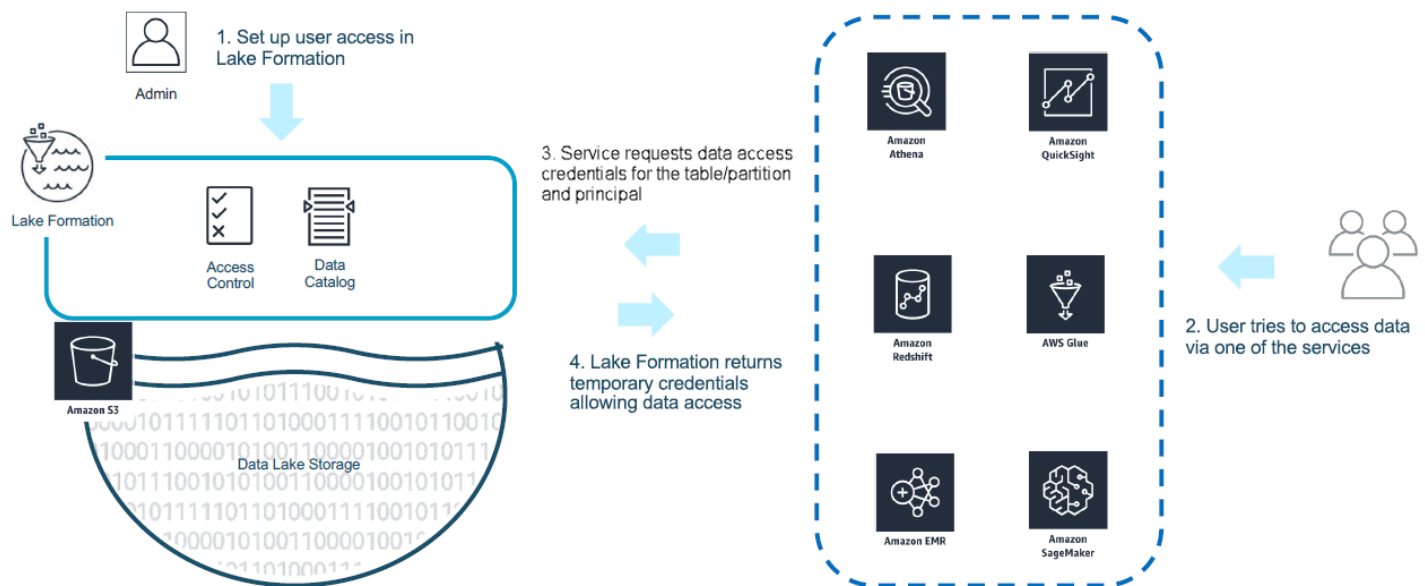
## Themen

- [So funktioniert die Anwendungsintegration von Lake Formation](#)
- [Rollen und Verantwortlichkeiten bei der Anwendungsintegration von Lake Formation](#)
- [Lake FormationWorkflow für API-Operationen zur Anwendungsintegration](#)
- [Registrierung einer Query-Engine eines Drittanbieters](#)
- [Aktivierung von Berechtigungen für eine Abfrage-Engine eines Drittanbieters zum Aufrufen von API-Operationen für die Anwendungsintegration](#)
- [Anwendungsintegration für vollständigen Tabellenzugriff](#)

## So funktioniert die Anwendungsintegration von Lake Formation

In diesem Abschnitt wird beschrieben, wie API-Operationen zur Anwendungsintegration verwendet werden, um eine Drittanbieteranwendung (Abfrage-Engine) zu integrierenLake Formation.





## 1. Der Lake Formation Administrator führt die folgenden Aktivitäten aus:

- Registriert einen Amazon S3 S3-Standort bei Lake Formation, indem eine IAM-Rolle (für Verkaufsberechtigungen) bereitgestellt wird, die über die entsprechenden Berechtigungen für den Zugriff auf Daten innerhalb des Amazon S3 S3-Standorts verfügt
- Registriert eine Drittanbieteranwendung, um die API-Operationen für den Verkauf von Anmeldeinformationen von Lake Formation aufrufen zu können. Siehe [the section called "Registrierung einer Query-Engine eines Drittanbieters"](#)
- Gewährt Benutzern Berechtigungen für den Zugriff auf Datenbanken und Tabellen

Wenn Sie beispielsweise einen Datensatz für Benutzersitzungen veröffentlichen möchten, der einige Spalten mit personenbezogenen Daten (PII) enthält, weisen Sie diesen Spalten zur Einschränkung des Zugriffs ein [LF-TBAC-Tag](#) mit dem Namen „Klassifizierung“ mit dem Wert „vertraulich“ zu. Als Nächstes definieren Sie eine Berechtigung, die es einem Geschäftsanalysten ermöglicht, auf die Daten der Benutzersitzungen zuzugreifen, aber die Spalten, die mit `classification = sensitive` gekennzeichnet sind, ausschließen.

2. Ein Principal (Benutzer) sendet eine Anfrage an einen integrierten Dienst.
3. Die integrierte Anwendung sendet die Anfrage an Lake Formation und bittet um Tabelleninformationen und Anmeldeinformationen für den Zugriff auf die Tabelle.
4. Wenn der abfragende Prinzipal autorisiert ist, auf die Tabelle zuzugreifen, gibt Lake Formation die Anmeldeinformationen an die integrierte Anwendung zurück, die den Datenzugriff ermöglicht.

 Note

Lake Formation greift beim Verkauf von Anmeldeinformationen nicht auf die zugrunde liegenden Daten zu.

5. Der integrierte Service liest Daten aus Amazon S3, filtert Spalten auf der Grundlage der empfangenen Richtlinien und gibt die Ergebnisse an den Principal zurück.

 Important

Lake Formation-API-Operationen für den Verkauf von Anmeldedaten ermöglichen eine verteilte Durchsetzung mit einem expliziten Modell der Ablehnung bei einem Ausfall (Fail-Close). Dadurch wird ein Dreiparteien-Sicherheitsmodell zwischen Kunden, Drittanbieterdiensten und Lake Formation eingeführt. Integrierten Diensten wird bei der ordnungsgemäßen Durchsetzung von Lake Formation Berechtigungen vertraut (verteilte Durchsetzung).

Der integrierte Service ist dafür verantwortlich, die aus Amazon S3 gelesenen Daten auf der Grundlage der Richtlinien zu filtern, die Lake Formation vor der Rückgabe der gefilterten Daten an den Benutzer zurückgegeben wurden. Integrierte Dienste folgen einem Fail-Close-Modell, was bedeutet, dass sie die Abfrage nicht bestehen müssen, wenn sie die erforderlichen Lake Formation Berechtigungen nicht durchsetzen können.

## Rollen und Verantwortlichkeiten bei der Anwendungsintegration von Lake Formation

Im Folgenden sind die Rollen und die damit verbundenen Verantwortlichkeiten für die Integration von Drittanbieteranwendungen mit aufgeführt AWS Lake Formation.

| Rolle     | Verantwortung                                                                                                                                                                                                                   |
|-----------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Der Kunde | <ul style="list-style-type: none"><li>• Aktivieren Sie Lake Formation Formation-Anwendungsintegrationseinstellung (siehe <a href="#">the section called “Registrierung einer Query-Engine eines Drittanbieters”</a>).</li></ul> |

| Rolle              | Verantwortung                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                  |
|--------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
|                    | <ul style="list-style-type: none"> <li>• Registriert ausdrücklich zugelassene Dritte bei Lake Formation (siehe <a href="#">the section called “Registrierung einer Query-Engine eines Drittanbieters”</a>).</li> <li>• Testet und validiert Lösungen von Drittanbietern mit Lake Formation Formation-Berechtigungen.</li> <li>• Überwacht und prüft die Nutzung der API-Operationen für den Verkauf von Anmeldedaten von Lake Formation durch Dritte.</li> </ul>                                                                                                                                                                                                                                                                                               |
| Der Drittanbieter  | <ul style="list-style-type: none"> <li>• Dokumentiert öffentlich die unterstützten Funktionen für jede Softwareversion und stellt Anweisungen zur korrekten Aktivierung bereit.</li> <li>• Werbt beim Aufrufen von Lake Formation Credential Vending API-Operationen genau für die unterstützten Funktionen (gemäß der Dokumentation).</li> <li>• Speichert und verarbeitet verkaufte Anmeldeinformationen auf sichere Weise, um Datenlecks und die Eskalation von Rechten zu vermeiden.</li> <li>• Erzwingt Berechtigungen auf der Grundlage der unterstützten Funktionen und gibt nur gefilterte Daten an Benutzer zurück</li> <li>• Die Abfrage schlägt fehl, wenn die erforderlichen Berechtigungen nicht ordnungsgemäß erzwungen werden können</li> </ul> |
| AWS Lake Formation | <ul style="list-style-type: none"> <li>• Leitet die effektiven Berechtigungen für einen bestimmten Prinzipal korrekt ab und gibt sie zurück.</li> <li>• Überprüft die von Drittanbietern unterstützten Funktionen auf call-by-call API-Betriebsbasis.</li> <li>• Gibt nur dann nach unten abgegrenzte IAM-Anmeldeinformationen zurück, wenn die angekündigten Funktionen der Engine mit den in den Katalogressourcen definierten Funktionen übereinstimmen. Andernfalls wird ein Fehler zurückgegeben.</li> </ul>                                                                                                                                                                                                                                              |

## Lake FormationWorkflow für API-Operationen zur Anwendungsintegration

Im Folgenden ist der Arbeitsablauf für API-Operationen zur Anwendungsintegration dargestellt:

1. Ein Benutzer sendet eine Abfrage oder Datenanforderung mithilfe einer integrierten Abfrage-Engine eines Drittanbieters. Die Abfrage-Engine nimmt eine IAM-Rolle an, die den Benutzer oder eine Benutzergruppe repräsentiert, und ruft vertrauenswürdige Anmeldeinformationen ab, die beim Aufrufen der API-Operationen für die Anwendungsintegration verwendet werden.
2. Die Abfrage-Engine ruft auf `GetUnfilteredTableMetadata`, und wenn es sich um eine partitionierte Tabelle handelt, ruft die Abfrage-Engine auf, `GetUnfilteredPartitionsMetadata` um Metadaten und Richtlinieninformationen aus dem Datenkatalog abzurufen.
3. Lake Formation führt die Autorisierung für die Anfrage durch. Wenn der Benutzer nicht über die entsprechenden Berechtigungen für die Tabelle verfügt, `AccessDeniedException` wird ausgelöst.
4. Als Teil der Anfrage sendet die Abfrage-Engine die Filterung, die sie unterstützt. Es gibt zwei Flags, die innerhalb eines Arrays gesendet werden können: `COLUMN_PERMISSIONS` und `CELL_FILTER_PERMISSION`. Wenn die Abfrage-Engine keine dieser Funktionen unterstützt und in der Tabelle für die Funktion eine Richtlinie vorhanden ist, wird eine `PermissionTypeMismatchException` ausgelöst und die Abfrage schlägt fehl. Dies dient dazu, Datenlecks zu vermeiden.
5. Die zurückgegebene Antwort enthält Folgendes:
  - Das gesamte Schema für die Tabelle, sodass Abfrage-Engines es verwenden können, um die Daten aus dem Speicher zu analysieren.
  - Eine Liste der autorisierten Spalten, auf die der Benutzer Zugriff hat. Wenn die Liste der autorisierten Spalten leer ist, bedeutet dies, dass der Benutzer zwar über `DESCRIBE` Berechtigungen, aber nicht über `SELECT` Berechtigungen verfügt, und die Abfrage schlägt fehl.
  - Eine Flagge `IsRegisteredWithLakeFormation`, die angibt, ob Lake Formation Anmeldeinformationen für diese Ressourcendaten weitergeben kann. Wenn dies den Wert `False` zurückgibt, sollten die Anmeldeinformationen des Kunden für den Zugriff auf Amazon S3 verwendet werden.
  - Eine Liste, `CellFilters` falls vorhanden, die auf Datenzeilen angewendet werden sollen. Diese Liste enthält Spalten und einen Ausdruck zur Auswertung jeder Zeile. Dies sollte nur aufgefüllt werden, wenn `CELL_FILTER_PERMISSION` als Teil der Anfrage gesendet wird und ein Datenfilter für die Tabelle für den aufrufenden Benutzer vorhanden ist.
6. Nachdem die Metadaten abgerufen wurden, ruft die Abfrage-Engine `GetTemporaryGlueTableCredentials` oder `GetTemporaryGluePartitionCredentials` auf, um AWS Anmeldeinformationen zum Abrufen von Daten vom Amazon S3 S3-Standort abzurufen.

7. Die Abfrage-Engine liest relevante Objekte aus Amazon S3, filtert die Daten auf der Grundlage der Richtlinien, die sie in Schritt 2 erhalten hat, und gibt die Ergebnisse an den Benutzer zurück.

Die API-Operationen für die Anwendungsintegration für Lake Formation enthalten zusätzliche Inhalte für die Konfiguration der Integration mit Abfrage-Engines von Drittanbietern. Die Einzelheiten zu den Vorgängen finden Sie im [Abschnitt „Credential Vending API Operations“](#).

Dies `QuerySessionContext` ist eine Struktur, an die Abfrage-Engines Lake Formation für diese API-Operationen zur Anwendungsintegration zusätzlich senden können. Sie ermöglicht Lake Formation das Speichern und Verwenden von zusätzlichem Kontext für eine bestimmte Abfrage. Im Folgenden finden Sie ein Beispiel dafür, wie es verwendet werden [QuerySessionContext](#) sollte:

1. Die Abfrage-Engine `GetInternalUnfilteredMetadata` ruft auf und übergibt eine QSC-Struktur, die eine eindeutige Abfrage-ID in der Anfrage enthält:

```
{
 "QuerySessionContext": {
 "QueryId": "your-unique-identifier-here"
 }
}
```

2. Der `GetInternalUnfilteredMetadata` Aufruf wird in der Antwort eine `QueryAuthorizationId` Zeichenfolge zurückgegeben haben. Beim nächsten (und jedem nachfolgenden) Abfrageaufruf, der eine QSC-Struktur in der Eingabe akzeptiert, übergibt die Abfrage-Engine dieselbe QSC-Struktur, die jetzt auch das `QueryAuthorizationId` zurückgegebene von enthält. Lake Formation Nehmen wir an, dieser nächste Aufruf ist `GetTemporaryGlueTableCredentials`; die Anfrage wird Folgendes enthalten:

```
{
 "QuerySessionContext": {
 "QueryAuthorizationId": "lf-returned-query-authz-id-here",
 "QueryId": "your-unique-identifier-here"
 },
}
```

## Registrierung einer Query-Engine eines Drittanbieters

Bevor eine Abfrage-Engine eines Drittanbieters die API-Operationen für die Anwendungsintegration verwenden kann, müssen Sie der Abfrage-Engine explizit Berechtigungen zum Aufrufen der API-Operationen in Ihrem Namen gewähren. Dies ist in wenigen Schritten erledigt:

1. Sie müssen die AWS Konten und IAM-Sitzungs-Tags angeben, für die eine Genehmigung zum Aufrufen der API-Operationen für die Anwendungsintegration über die AWS Lake Formation Konsole, die AWS CLI oder das API/SDK erforderlich ist.
2. Wenn die Drittanbieter-Abfrage-Engine die Ausführungsrolle in Ihrem Konto übernimmt, muss die Abfrage-Engine ein Sitzungs-Tag anhängen, das bei Lake Formation registriert ist und die Drittanbieter-Engine darstellt. Lake Formation verwendet dieses Tag, um zu überprüfen, ob die Anfrage von einer zugelassenen Engine stammt. Weitere Informationen zu Sitzungs-Tags finden Sie unter [Sitzungs-Tags](#) im IAM-Benutzerhandbuch.
3. Wenn Sie eine Ausführungsrolle für die Query Engine eines Drittanbieters einrichten, müssen Sie in der IAM-Richtlinie über die folgenden Mindestberechtigungen verfügen:

JSON

```
{
 "Version": "2012-10-17",
 "Statement": {
 "Effect": "Allow",
 "Action": [
 "lakeformation:GetDataAccess",
 "glue:GetTable",
 "glue:GetTables",
 "glue:GetDatabase",
 "glue:GetDatabases",
 "glue>CreateDatabase",
 "glue:GetUserDefinedFunction",
 "glue:GetUserDefinedFunctions",
 "glue:GetPartition",
 "glue:GetPartitions"
],
 "Resource": "*"
 }
}
```

4. Richten Sie eine Rollenvertrauensrichtlinie für die Ausführungsrolle der Abfrage-Engine ein, um genau kontrollieren zu können, welches Schlüssel-Wert-Paar für das Sitzungs-Tag an diese Rolle

angehängt werden kann. Im folgenden Beispiel darf dieser Rolle nur der Sitzungs-Tag-Schlüssel "LakeFormationAuthorizedCaller" und der Sitzungs-Tag-Wert "engine1" angehängt werden, und es ist kein anderes Sitzungstag-Schlüssel-Wert-Paar zulässig.

```
{
 "Sid": "AllowPassSessionTags",
 "Effect": "Allow",
 "Principal": {
 "AWS": "arn:aws:iam::111122223333:role/query-execution-role"
 },
 "Action": "sts:TagSession",
 "Condition": {
 "StringLike": {
 "aws:RequestTag/LakeFormationAuthorizedCaller": "engine1"
 }
 }
}
```

Wenn der LakeFormationAuthorizedCaller AssumeRole API-Vorgang STS: aufgerufen wird, um Anmeldeinformationen für die Abfrageengine abzurufen, muss das Sitzungs-Tag in der [AssumeRole Anforderung](#) enthalten sein. Die zurückgegebenen temporären Anmeldeinformationen können verwendet werden, um API-Anfragen zur Lake Formation Anwendungsintegration zu stellen.

Lake FormationFür API-Operationen zur Anwendungsintegration muss der aufrufende Prinzipal eine IAM-Rolle sein. Die IAM-Rolle muss ein Sitzungs-Tag mit einem vordefinierten Wert enthalten, mit dem registriert wurde. Lake Formation Mit diesem Tag kann Lake Formation überprüft werden, ob die Rolle, die zum Aufrufen der API-Operationen für die Anwendungsintegration verwendet wird, dazu berechtigt ist.

## Aktivierung von Berechtigungen für eine Abfrage-Engine eines Drittanbieters zum Aufrufen von API-Operationen für die Anwendungsintegration

Gehen Sie wie folgt vor, damit eine Query-Engine eines Drittanbieters API-Operationen für die Anwendungsintegration über die AWS Lake Formation Konsole, die AWS CLI oder API/SDK aufrufen kann.

## Console

So registrieren Sie Ihr Konto für die externe Datenfilterung:

1. Melden Sie sich bei an AWS-Managementkonsole und öffnen Sie die Lake Formation Formation-Konsole unter <https://console.aws.amazon.com/lakeformation/>.
2. Erweitern Sie in der linken Navigationsleiste die Option Administration und wählen Sie dann Anwendungsintegrationseinstellung aus.
3. Wählen Sie auf der Einstellungsseite für die Anwendungsintegration die Option Zulassen, dass externe Engines Daten an Amazon S3 S3-Standorten filtern, bei denen Sie registriert sindLake Formation.
4. Geben Sie die Sitzungs-Tags ein, die Sie für die Drittanbieter-Engine erstellt haben. Informationen zu Sitzungs-Tags finden Sie im AWS Identity and Access Management Benutzerhandbuch unter [Übergeben von Sitzungs-Tags in AWS STS](#).
5. Geben Sie das Konto IDs für Benutzer ein, die mit der Drittanbieter-Engine auf ungefilterte Metadateninformationen und die Datenzugriffsanmeldeinformationen der Ressourcen im aktuellen Konto zugreifen können.

Sie können das AWS Konto-ID-Feld auch für die Konfiguration des kontoübergreifenden Zugriffs verwenden.



# Application integration settings [Learn more](#)

## Application integration settings

Use the options below to control which third-party engines are allowed to read and filter data in Amazon S3 locations registered with Lake Formation.

### ☒ Allow external engines to filter data in Amazon S3 locations registered with Lake Formation

Check this box to allow third-party engines to access data in Amazon S3 locations that are registered with Lake Formation.

#### Session tag values

Enter one or more strings that match the LakeFormationAuthorizedCaller session tag defined for third-party engines.

Clear all

engine 1 ✕

engine 2 ✕

session 1 ✕

Enter one or several string values separated by comma.

#### AWS account IDs

Enter the external AWS account IDs from where third-party engines are allowed to access locations registered with Lake Formation.

Clear all

11111111111 ✕  
Account

22222222222 ✕  
Account

Enter one or more AWS account IDs. Press enter after each ID.

### ☐ Allow external engines to access data in Amazon S3 locations with full table access.

When you enable this option, Lake Formation will return credentials to the integrated application directly without IAM session tag validation.

Cancel

Save

## CLI

Verwenden Sie den `put-data-lake-settings` CLI-Befehl, um die folgenden Parameter festzulegen.

Bei Verwendung dieses AWS CLI Befehls müssen drei Felder konfiguriert werden:

- `allow-external-data-filtering` — (boolean) Gibt an, dass eine Engine eines Drittanbieters auf ungefilterte Metadateninformationen und Datenzugriffsanmeldeinformationen von Ressourcen im aktuellen Konto zugreifen kann.
- `external-data-filtering-allow-list`— (Array) Eine Liste von Konten IDs , die auf ungefilterte Metadateninformationen und Datenzugriffsanmeldeinformationen von Ressourcen im aktuellen Konto zugreifen können, wenn eine Engine eines Drittanbieters verwendet wird.

Wenn auf „true“ gesetzt `AllowExternalDataFiltering` ist, muss die `ExternalDataFilteringAllowList` Eigenschaft mindestens eine Konto-ID enthalten. Eine leere Liste ist nicht zulässig.

- `authorized-sessions-tag-value-list`— (Array) Eine Liste von autorisierten Sitzungs-Tag-Werten (Zeichenketten). Wenn eine IAM-Rollenanmeldeberechtigung mit einem autorisierten Schlüssel-Wert-Paar verknüpft wurde und das Sitzungs-Tag in der Liste enthalten ist, erhält die Sitzung Zugriff auf ungefilterte Metadateninformationen und Datenzugriffsanmeldeinformationen für Ressourcen im konfigurierten Konto. Der Tag-Schlüssel für die autorisierte Sitzung ist definiert als `*LakeFormationAuthorizedCaller*`
- `AllowFullTableExternalDataAccess`— (boolean) Ob einer Abfrage-Engine eines Drittanbieters erlaubt werden soll, Datenzugriffsanmeldeinformationen ohne Sitzungs-Tags abzurufen, wenn ein Aufrufer über volle Datenzugriffsberechtigungen verfügt.

Beispiel:

```
aws lakeformation put-data-lake-settings --cli-input-json file://
datalakesettings.json

{
 "DataLakeSettings": {
 "DataLakeAdmins": [
 {
 "DataLakePrincipalIdentifier": "arn:aws:iam::111111111111:user/lakeAdmin"
 }
],
 "CreateDatabaseDefaultPermissions": [],
 "CreateTableDefaultPermissions": [],
 "TrustedResourceOwners": [],
 "AllowExternalDataFiltering": true,
 "ExternalDataFilteringAllowList": [
 {"DataLakePrincipalIdentifier": "111111111111"}
],
 "AuthorizedSessionTagValueList": ["engine1"],
 "AllowFullTableExternalDataAccess": false
 }
}
```

## API/SDK

Verwenden Sie den `PutDataLakeSetting` API-Vorgang, um die folgenden Parameter festzulegen.

Bei Verwendung dieses API-Vorgangs müssen drei Felder konfiguriert werden:

- `AllowExternalDataFiltering`— (Boolean) Gibt an, ob eine Engine eines Drittanbieters auf ungefilterte Metadateninformationen und Datenzugriffsanmeldeinformationen von Ressourcen im aktuellen Konto zugreifen kann.
- `ExternalDataFilteringAllowList`— (Array) Eine Liste von Konten IDs , die mithilfe einer Drittanbieter-Engine auf ungefilterte Metadateninformationen und die Datenzugriffsanmeldeinformationen von Ressourcen im aktuellen Konto zugreifen können.
- `AuthorizedSectionsTagValueList`— (Array) Eine Liste autorisierter Tag-Werte (Zeichenketten). Wenn eine IAM-Rollenberechtigung mit einem autorisierten Tag verknüpft wurde, erhält die Sitzung Zugriff auf ungefilterte Metadateninformationen und die Datenzugriffsanmeldeinformationen für Ressourcen im konfigurierten Konto. Der Tag-Schlüssel für die autorisierte Sitzung ist definiert als. `*LakeFormationAuthorizedCaller*`
- `AllowFullTableExternalDataAccess`— (boolean) Ob einer Abfrage-Engine eines Drittanbieters erlaubt werden soll, Datenzugriffsanmeldeinformationen ohne Sitzungs-Tags abzurufen, wenn ein Aufrufer über volle Datenzugriffsberechtigungen verfügt.

Beispiel:

```
//Enable session tag on existing data lake settings
public void sessionTagSetUpForExternalFiltering(AWSLakeFormationClient
lakeformation) {
 GetDataLakeSettingsResult getDataLakeSettingsResult =
 lfClient.getDataLakeSettings(new GetDataLakeSettingsRequest());
 DataLakeSettings dataLakeSettings =
 getDataLakeSettingsResult.getDataLakeSettings();

 //set account level flag to allow external filtering
 dataLakeSettings.setAllowExternalDataFiltering(true);

 //set account that are allowed to call credential vending or Glue
 GetFilteredMetadata API
 List<DataLakePrincipal> allowlist = new ArrayList<>();
 allowlist.add(new
 DataLakePrincipal().withDataLakePrincipalIdentifier("111111111111"));
}
```

```
dataLakeSettings.setWhitelistedForExternalDataFiltering(allowlist);

//set registered session tag values
List<String> registeredTagValues = new ArrayList<>();
registeredTagValues.add("engine1");
dataLakeSettings.setAuthorizedSessionTagValueList(registeredTagValues);

lakeformation.putDataLakeSettings(new
PutDataLakeSettingsRequest().withDataLakeSettings(dataLakeSettings));
}
```

## Anwendungsintegration für vollständigen Tabellenzugriff

Gehen Sie wie folgt vor, damit Abfrage-Engines von Drittanbietern auf Daten zugreifen können, ohne dass das IAM-Sitzungs-Tag überprüft wird:

### Console

1. Melden Sie sich bei der Lake Formation Formation-Konsole unter an <https://console.aws.amazon.com/lakeformation/>.
2. Erweitern Sie in der linken Navigationsleiste die Option Administration und wählen Sie Anwendungsintegrationseinstellungen aus.
3. Wählen Sie auf der Seite mit den Einstellungen für die Anwendungsintegration die Option Externen Engines den Zugriff auf Daten an Amazon S3 S3-Standorten mit vollständigem Tabellenzugriff erlauben.

Wenn Sie diese Option aktivieren, gibt Lake Formation Anmeldeinformationen ohne Überprüfung des IAM-Sitzungstags direkt an die abfragende Anwendung zurück.

# Application integration settings [Learn more](#)

## Application integration settings

Use the options below to control which third-party engines are allowed to read and filter data in Amazon S3 locations registered with Lake Formation.

### ☐ Allow external engines to filter data in Amazon S3 locations registered with Lake Formation

Check this box to allow third-party engines to access data in Amazon S3 locations that are registered with Lake Formation.

#### Session tag values

Enter one or more strings that match the LakeFormationAuthorizedCaller session tag defined for third-party engines.

[Clear all](#)




Enter one or several string values separated by comma.

#### AWS account IDs

Enter the external AWS account IDs from where third-party engines are allowed to access locations registered with Lake Formation.

[Clear all](#)


Account

Account

Enter one or more AWS account IDs. Press enter after each ID.

### ☒ Allow external engines to access data in Amazon S3 locations with full table access.

When you enable this option, Lake Formation will return credentials to the integrated application directly without IAM session tag validation.

[Cancel](#)
[Save](#)

## AWS CLI

Verwenden Sie den `put-data-lake-settings` CLI-Befehl, um den `AllowFullTableExternalDataAccess` Parameter festzulegen.

```
aws lakeformation put-data-lake-settings --cli-input-json file:///put-data-lake-
settings.json --region ap-northeast-1
{
 "DataLakeSettings": {
 "DataLakeAdmins": [
 {
 "DataLakePrincipalIdentifier": "arn:aws:iam::111111111111:user/
lakeAdmin"
 }
]
 }
}
```

```
],
 "AllowFullTableExternalDataAccess": true
 }
}
```

# Zusammenarbeit mit anderen AWS Diensten

AWS Dienste wie Amazon Athena AWS Glue, Amazon Redshift Spectrum und Amazon EMR können für den sicheren Zugriff auf Daten AWS Lake Formation an Amazon S3 S3-Standorten verwendet werden, die bei Lake Formation registriert sind. Mit Lake Formation können Sie feinkörnige Zugriffssteuerungsberechtigungen (FGAC) für Ihre Tabellen in der definieren und verwalten. AWS Glue Data Catalog Jeder dieser AWS Dienste ist ein vertrauenswürdiger Anrufer für Lake Formation, und Lake Formation bietet über temporäre Anmeldeinformationen Zugriff auf in Amazon S3 gespeicherte Daten. Weitere Informationen finden Sie unter [So funktioniert die Anwendungsintegration von Lake Formation](#).

Um diese Funktionen nutzen zu können, müssen Sie bei Lake Formation zunächst den Amazon S3 S3-Standort registrieren und dem IAM-Prinzipal die entsprechenden Berechtigungen für den Zugriff auf die Tabelle, die Datenbank und den Amazon S3 S3-Standort zuweisen. Weitere Informationen finden Sie unter [Verwaltung von Lake Formation Formation-Berechtigungen](#).

In der folgenden Tabelle sind die Typen von Lake Formation Formation-Berechtigungen aufgeführt, die von Amazon Athena AWS Glue, Amazon EMR und Amazon Redshift Spectrum für den Zugriff auf Daten aus AWS Glue Standardtabellen und Transaktionstabellen ([Apache Iceberg](#), [Apache Hudi](#) und [Linux Foundation Delta Lake](#)) mit in Amazon S3 gespeicherten Daten und Tabellenmetadaten im Datenkatalog unterstützt werden.

AWS Dienste und unterstützte Berechtigungstypen für Standardtabellen und -ansichten AWS Glue

| AWS Dienst                                                                                           | Berechtigungen auf Tabellenebene | Berechtigungen auf Spaltenebene | Berechtigungen auf Zeilen- und Zellenebene |
|------------------------------------------------------------------------------------------------------|----------------------------------|---------------------------------|--------------------------------------------|
| <a href="#">Athena SQL</a>                                                                           | Lese-/Schreibzugriff             | Lesezugriff                     | Lesezugriff                                |
| Athena Spark                                                                                         | Nicht unterstützt                | Nicht unterstützt               | Nicht unterstützt                          |
| <a href="#">Redshift Spectrum</a> auf einem bereitgestellten Cluster oder Amazon Redshift serverless | Lese-/Schreibzugriff             | Lesezugriff                     | Lesezugriff                                |

| AWS Dienst                                        | Berechtigungen auf Tabellenebene | Berechtigungen auf Spaltenebene                  | Berechtigungen auf Zeilen- und Zellenebene       |
|---------------------------------------------------|----------------------------------|--------------------------------------------------|--------------------------------------------------|
| <a href="#">Apache Spark auf Amazon EMR (EC2)</a> | Lese-/Schreibzugriff             | Lesezugriff                                      | Lesezugriff                                      |
| <a href="#">Apache Hive auf Amazon EMR (EC2)</a>  | Lese-/Schreibzugriff             | Lesezugriff                                      | Nicht unterstützt                                |
| <a href="#">Apache Spark auf EMR Serverless</a>   | Lese-/Schreibzugriff             | Lesezugriff                                      | Lesezugriff                                      |
| Apache Hive auf EMR Serverless                    | Nicht unterstützt                | Nicht unterstützt                                | Nicht unterstützt                                |
| Amazon EMR auf EKS                                | Nicht unterstützt                | Nicht unterstützt                                | Nicht unterstützt                                |
| <a href="#">AWS Glue ETL</a>                      | Lese-/Schreibzugriff             | AWS Glue 5.0 oder höher unterstützt Lesezugriff. | AWS Glue 5.0 oder höher unterstützt Lesezugriff. |

## Überlegungen und Einschränkungen

- Athena Spark unterstützt keine Abfragen von Datenkatalogtabellen mit Lake Formation Formation-Berechtigungen.
- SAML-basierte Benutzer von Athena können Datenquellen lesen, die mit Lake Formation Formation-Berechtigungen gesichert sind, indem sie den SAML 2.0-basierten Verbund aktivieren. SAML-Benutzer können Daten in Parquet-Tabellen einfügen.
- Apache Spark on EMR Serverless unterstützt das Abfragen von Datenkatalogansichten nicht.
- Apache Hive on EMR Serverless unterstützt das Abfragen von Tabellen mit Lake Formation Formation-Berechtigungen nicht.
- AWS Glue 5.0 oder höher unterstützt detaillierte Zugriffskontrollen für Iceberg- und Hive-Tabellen im Datenkatalog, die von S3 unterstützt werden. Mit dieser Funktion können Sie Zugriffskontrollen auf Tabellen-, Zeilen-, Spalten- und Zellenebene für Leseabfragen innerhalb Ihrer AWS Glue Apache Spark-Jobs konfigurieren.



Weitere Informationen finden Sie unter [AWS Glue -Versionen](#).

## AWS Dienste und unterstützte Berechtigungstypen für Transaktionstabellenformate

| AWS Dienst                                                           | Iceberg                                                                                                                                                          | Hudi                                                                                                                                                                     | Delta-See (einheimisch)                                                                                                                                                                    | Delta Lake (Symlink-Tabellen)                                                                                                                                                                  |
|----------------------------------------------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <a href="#">Athena SQL</a>                                           | Unterstützt das Lesen von Tabellen mit Berechtigungen auf Tabellen-, Spalten-, Zeilen- und Zellenebene. Schreibvorgänge erfordern vollständigen Tabellenzugriff. | Unterstützt Lese- und Erstellungsoperationen für Tabellen mit Berechtigungen auf Tabellen-, Spalten-, Zeilen- und Zellenebene. Schreibvorgänge werden nicht unterstützt. | Athena (Engine-Version 3) unterstützt das Lesen nativer Delta Lake-Tabellen mit Berechtigungen auf Tabellen-, Spalten-, Zeilen- und Zellenebene. Schreibvorgänge werden nicht unterstützt. | Athena (Engine-Version 3) unterstützt das Lesen von Symlink-Delta-Lake-Tabellen mit Berechtigungen auf Tabellen-, Spalten-, Zeilen- und Zellenebene. Schreibvorgänge werden nicht unterstützt. |
| <a href="#">Redshift Spectrum</a> auf einem bereitgestellten Cluster | Unterstützt das Lesen von Tabellen mit Berechtigungen auf Tabellen-, Spalten-, Zeilen- und Zellenebene. Schreibvorgänge werden nicht unterstützt.                | Unterstützt das Lesen von Tabellen mit Berechtigungen auf Tabellen-, Spalten-, Zeilen- und Zellenebene. Schreibvorgänge werden nicht unterstützt.                        | Nicht unterstützt                                                                                                                                                                          | Unterstützt das Lesen von Delta Lake-Tabellen über ein Symlink-Manifest mit Berechtigungen auf Tabellen-, Spalten-, Zeilen- und Zellenebene. Schreibvorgänge werden nicht unterstützt.         |

| AWS Dienst                                        | Iceberg                                                                                                                                                          | Hudi                                                                                                                                                             | Delta-See<br>(einheimisch)                                                                                                                        | Delta Lake<br>(Symlink-<br>Tabellen)                                                                                                                             |
|---------------------------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <a href="#">Apache Spark auf Amazon EMR (EC2)</a> | Unterstützt das Lesen von Tabellen mit Berechtigungen auf Tabellen-, Spalten-, Zeilen- und Zellenebene. Schreibvorgänge erfordern vollständigen Tabellenzugriff. | Unterstützt das Lesen von Tabellen mit Berechtigungen auf Tabellen-, Spalten-, Zeilen- und Zellenebene. Schreibvorgänge erfordern vollständigen Tabellenzugriff. | Unterstützt das Lesen von Tabellen mit Berechtigungen auf Tabellen-, Spalten-, Zeilen- und Zellenebene. Schreibvorgänge werden nicht unterstützt. | Unterstützt das Lesen von Tabellen mit Berechtigungen auf Tabellen-, Spalten-, Zeilen- und Zellenebene. Schreibvorgänge erfordern vollständigen Tabellenzugriff. |
| <a href="#">AWS Glue ETL</a>                      | AWS Glue 5.0 oder höher unterstützt das Lesen von Tabellen mit Berechtigungen auf Tabellen-, Spalten-, Zeilen- und Zellenebene.                                  | Unterstützt Tabellen mit read/write Berechtigungen auf Tabellenebene.                                                                                            | Unterstützt Tabellen mit read/write Berechtigungen auf Tabellenebene.                                                                             | Unterstützt Tabellen mit read/write Berechtigungen auf Tabellenebene.                                                                                            |

## Themen

- [Verwendung AWS Lake Formation mit Amazon Athena](#)
- [Verwendung AWS Lake Formation mit Amazon Redshift Spectrum](#)
- [Verwenden mit AWS Lake Formation AWS Glue](#)
- [Verwendung AWS Lake Formation mit Amazon EMR](#)
- [Verwendung mit Quick AWS Lake Formation](#)
- [Verwendung AWS Lake Formation mit AWS CloudTrail Lake](#)

# Verwendung AWS Lake Formation mit Amazon Athena

[Amazon Athena](#) ist ein serverloser Abfrageservice, der Sie bei der Analyse strukturierter, halbstrukturierter und unstrukturierter Daten unterstützt, die in Amazon S3 gespeichert sind. Sie können Athena SQL verwenden, um Daten aus den Datenformaten CSV, JSON, Parquet und Avro abzufragen. [Athena SQL unterstützt auch Tabellenformate wie Apache Hive, ApacheHudi und Apache Iceberg](#). Athena lässt sich in die integrieren AWS Glue Data Catalog, um Metadaten Ihrer Datensätze in Amazon S3 zu speichern. Athena kann Lake Formation verwenden, um Zugriffskontrollrichtlinien für diese Datensätze zu definieren und zu verwalten.

Hier sind einige häufige Anwendungsfälle, in denen Sie Lake Formation mit Athena verwenden können.

- Verwenden Sie Lake Formation Formation-Berechtigungen für den Zugriff auf die Datenkatalogressourcen (Datenbank und Tabellen) von Athena. Sie können entweder die Methode der benannten Ressource oder LF-Tags verwenden, um Berechtigungen für Datenbanken und Tabellen zu definieren. Weitere Informationen finden Sie unter:
  - [Erteilen von Datenbankberechtigungen mit der benannten Ressourcenmethode](#)
  - [Tag-basierte Zugangskontrolle von Lake Formation](#)

## Note

Lake Formation Formation-Berechtigungen gelten nur, wenn Athena SQL verwendet wird, um Quelldaten aus Amazon S3 und Metadaten im Datenkatalog abzufragen. Athena Spark unterstützt keine Abfragen von Datenkatalogtabellen mit Lake Formation Formation-Berechtigungen. Lake Formation Formation-Berechtigungen unterstützen sowohl Lese- als auch Schreiboperationen für Datenbanken und Tabellen.

## Note

Sie können keine Datenfilter anwenden, wenn Sie LF-Tags verwenden, um Berechtigungen für Datenkatalogressourcen zu verwalten.

- Steuern Sie die Abfrageergebnisse [Datenfilter in Lake Formation](#), indem Sie Tabellen in Ihren Amazon S3 S3-Data Lakes sichern, indem Sie Berechtigungen auf Spalten-, Zeilen- und

Zellenebene gewähren. Informationen zu den [Einschränkungen bei der Partitionsprojektion](#) finden Sie im Amazon Athena Athena-Benutzerhandbuch.

- Erzwingen Sie bei der Ausführung von Verbundabfragen eine differenzierte Zugriffskontrolle für die Daten, die dem SAML-basierten Athena-Benutzer zur Verfügung stehen.

Die JDBC- und ODBC-Treiber von Athena unterstützen die Konfiguration des Verbundzugriffs auf Ihre Datenquelle mithilfe eines SAML-basierten Identity Providers (IdP). Verwenden Sie Quick integriert in Lake Formation mit Ihren vorhandenen IAM-Rollen- oder SAML-Benutzern oder -Gruppen, um Athena-Abfrageergebnisse zu visualisieren.

 Note

Lake Formation Formations-Berechtigungen für SAML-Benutzer und -Gruppen gelten nur, wenn Sie mithilfe des JDBC- oder ODBC-Treibers Anfragen an Athena senden.

Weitere Informationen finden Sie unter [Verwenden von Lake Formation und den Athena JDBC- und ODBC-Treibern für den Verbundzugriff](#) auf Athena.

 Note

Derzeit wird die Autorisierung des Zugriffs auf SAML-Identitäten in Lake Formation in den folgenden Regionen nicht unterstützt:

- Naher Osten (Bahrain) – me-south-1
- Asien-Pazifik (Hongkong) – ap-east-1
- Afrika (Kapstadt) – af-south-1
- China (Ningxia) – cn-northwest-1
- Asien-Pazifik (Osaka) – ap-northeast-3

- Wird verwendet [Kontoübergreifender Datenaustausch in Lake Formation](#), um Tabellen in einem anderen Konto abzufragen.

**Note**

Weitere Informationen zu Einschränkungen bei der Verwendung von Lake Formation Formation-Berechtigungen für finden Sie unter [Überlegungen und Einschränkungen](#). Views

## Support für Transaktionstabellenformate

Durch die Anwendung Lake Formation Formation-Berechtigungen können Sie Ihre Transaktionsdaten in Ihren Amazon S3 S3-basierten Data Lakes sichern. In der folgenden Tabelle sind Transaktionstabellenformate aufgeführt, die in den Berechtigungen Athena und Lake Formation unterstützt werden. Lake Formation erzwingt diese Berechtigungen, wenn Athena-Benutzer ihre Abfragen ausführen.

| Tabellenformat | Beschreibung und zulässige Operationen                                                                                                                                                                                                                                                                                                                                                                                                                                        | In Athena werden Lake Formation Formation-Berechtigungen unterstützt                                                                                                                                           |
|----------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Apache Hudi    | <p>Ein Format, das zur Vereinfachung der inkrementellen Datenverarbeitung und der Entwicklung von Datenleitungen verwendet wird.</p> <p>Athena unterstützt Erstellungs- und Lesevorgänge mit Apache Hudi-Tabellenformaten auf Amazon S3 S3-Datensätzen für die Hudi-Tabellentypen Copy on Write (CoW) und Merge On Read (MoR). Athena unterstützt keine Schreiboperationen auf Hudi-Tabellen.</p> <p>Verwenden Sie <a href="#">Athena, um Hudi-Datensätze abzufragen</a>.</p> | <p>Wird verwendet <a href="#">Datenfilterung und Sicherheit auf Zellebene in Lake Formation</a>, um Hudi-Tabellen mithilfe von Berechtigungen auf Tabellen-, Spalten-, Zeilen- und Zellenebene zu sichern.</p> |

| Tabellenformat | Beschreibung und zulässige Operationen                                                                                                                                                                                                                                                                                                                                            | In Athena werden Lake Formation Formations-Berechtigungen unterstützt                                                                                                                                                                                                 |
|----------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Apache Iceberg | <p>Ein offenes Tabellenformat, das große Sammlungen von Dateien als Tabellen verwaltet und moderne analytische Data Lake-Operationen wie Einfügen, Aktualisieren, Löschen und Zeitreiseabfragen auf Datensatzebene unterstützt.</p> <p><a href="#">Weitere Informationen zur Unterstützung von Iceberg-Tabellen durch Athena finden Sie unter Iceberg-Tabellen verwenden.</a></p> | <p>Berechtigungen auf Tabellen-, Spalten-, Zeilen- und Zellenebene werden unterstützt. Derzeit unterstützt Lake Formation die Verwaltung von Berechtigungen für Schreiboperationen wie VACUUMMERGE, UPDATE und OPTIMIZE für Tabellen in Open Table Formats nicht.</p> |

| Tabellenformat              | Beschreibung und zulässige Operationen                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                   | In Athena werden Lake Formation Formations-Berechtigungen unterstützt                                                                   |
|-----------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------|
| Linux Foundation Delta Lake | <p>Delta Lake ist ein Open-Source-Projekt, das bei der Implementierung moderner Data-Lake-Architekturen hilft, die üblicherweise auf Amazon S3 oder Hadoop Distributed File System (HDFS) basieren.</p> <p>Athena unterstützt Delta-Lake-Tabellen, die mithilfe einer Symlink-basierten Manifest-Tabellendefinition AWS Glue Data Catalog aus einer Delta Lake-Tabelle erstellt wurden.</p> <p>Weitere Informationen finden Sie unter <a href="#">Delta Lake-Tabellen mithilfe von Crawlern crawlen</a>.</p> <p>AWS Glue</p> <p>Athena (Engine-Version 3) unterstützt das Lesen nativer Delta Lake-Tabellen.</p> <p>Weitere Informationen finden Sie unter <a href="#">Einführung der systemeigenen Unterstützung für Delta Lake-Tabellen mit AWS Glue Crawlern</a>.</p> | Berechtigungen auf Tabellen-, Spalten-, Zeilen- und Zellenebene werden für Symlink-Tabellen und native Delta Lake-Tabellen unterstützt. |

## Weitere Ressourcen

Blogbeiträge, Videos und Workshops

- [Fragen Sie mit Amazon Athena einen Apache Hudi-Datensatz in einem Amazon S3 S3-Data Lake ab](#)
- [Erstellen Sie einen Apache Iceberg Data Lake mit Amazon Athena, Amazon EMR und AWS Glue](#)
- [Einfügen, Aktualisieren, Löschen auf Amazon S3 mit Athena und Apache Iceberg](#)
- Lake Formation-Workshop zur [LF-Tag-basierten Zugangskontrolle](#) zum Abfragen eines Data Lakes.

## Verwendung AWS Lake Formation mit Amazon Redshift Spectrum

Mit [Amazon Redshift Spectrum](#) können Sie Daten in Amazon S3 S3-Datenseen abfragen und abrufen, ohne Daten in Amazon Redshift Redshift-Clusterknoten laden zu müssen.

Redshift Spectrum unterstützt zwei Möglichkeiten zur Registrierung eines externen AWS Glue Datenkatalogs, der mit Lake Formation aktiviert wurde.

- Verwenden einer an einen Cluster angegliederten IAM-Rolle, die über Berechtigungen für den Datenkatalog verfügt

Gehen Sie wie im Folgenden beschrieben vor, um eine IAM-Rolle zu erstellen.

### [Steuern des Zugriffs auf AWS Glue Data Catalog](#)

- Verwenden einer föderierten IAM-Identität, die für die Verwaltung des Zugriffs auf externe Ressourcen konfiguriert ist AWS Glue Data Catalog

Redshift Spectrum unterstützt das Abfragen von Lake Formation-Tabellen mithilfe föderierter IAM-Identitäten. Bei den IAM-Identitäten kann es sich um einen IAM-Benutzer oder eine IAM-Rolle handeln. Weitere Informationen zum IAM-Identitätsverbund in Redshift Spectrum finden Sie unter [Verwenden einer föderierten Identität zur Verwaltung des Amazon Redshift Redshift-Zugriffs auf lokale Ressourcen und externe Redshift Spectrum-Tabellen](#).

Mit der Integration von Lake Formation in Redshift Spectrum können Sie Zugriffsberechtigungen auf Zeilen-, Spalten- und Zellenebene für Tabellen definieren, nachdem Ihre Daten bei Lake Formation registriert wurden.



Weitere Informationen finden Sie unter [Redshift Spectrum verwenden mit AWS Lake Formation](#).

Redshift Spectrum unterstützt Lesevorgänge oder SELECT Abfragen in den von Lake Formation verwalteten externen Schematabellen.

Weitere Informationen finden Sie unter [Externe Schemas für Redshift Spectrum erstellen](#).

## Support für Transaktionstabellentypen

In dieser Tabelle sind die in Redshift Spectrum unterstützten Transaktionstabellenformate und die entsprechenden Lake Formation Formation-Berechtigungen aufgeführt.

### Unterstützte Tabellenformate

| Tabellenformat | Beschreibung und zulässige Operationen                                                                                                                                                                                                                                                                                                                                                                                                | In Redshift Spectrum unterstützte Lake Formation Formation-Berechtigungen                                                                                                                                      |
|----------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Apache Hudi    | <p>Ein Format, das zur Vereinfachung der inkrementellen Datenverarbeitung und der Entwicklung von Datenpipelines verwendet wird.</p> <p>Redshift Spectrum unterstützt Einfüge-, Lösch- und Upsert-Schreibvorgänge im Tabellenformat Apache Hudi <a href="#">Copy on Write (CoW)</a> auf Amazon S3.</p> <p>Weitere Informationen finden Sie unter <a href="#">Erstellen externer Tabellen für in Apache Hudi verwaltete Daten</a>.</p> | <p>Wird verwendet <a href="#">Datenfilterung und Sicherheit auf Zellebene in Lake Formation</a>, um Hudi-Tabellen mithilfe von Berechtigungen auf Tabellen-, Spalten-, Zeilen- und Zellenebene zu sichern.</p> |
| Apache Iceberg | <p>Ein offenes Tabellenformat, das große Sammlungen von Dateien als Tabellen verwaltet und moderne analytische Data Lake-Oper</p>                                                                                                                                                                                                                                                                                                     | <p>Redshift Spectrum unterstützt Apache Iceberg-Tabellen für Abfragen.</p>                                                                                                                                     |

| Tabellenformat              | Beschreibung und zulässige Operationen                                                                                                                                                                                                                                                                                                                                                                   | In Redshift Spectrum unterstützte Lake Formation Formations-Berechtigungen          |
|-----------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-------------------------------------------------------------------------------------|
|                             | <p>ationen wie Einfügen, Aktualisieren, Löschen und Zeitreise abfragen auf Datensatzebene unterstützt.</p> <p>Weitere Informationen finden Sie unter <a href="#">Verwenden von Apache Iceberg-Tabellen mit Amazon Redshift</a>.</p>                                                                                                                                                                      |                                                                                     |
| Linux Foundation Delta Lake | <p>Delta Lake ist ein Open-Source-Projekt, das bei der Implementierung moderner Data-Lake-Architekturen hilft, die üblicherweise auf Amazon S3 oder Hadoop Distributed File System (HDFS) basieren.</p> <p>Redshift Spectrum unterstützt die Abfrage von Delta Lake-Tabellen. Weitere Informationen finden Sie unter <a href="#">Erstellen externer Tabellen für in Delta Lake verwaltete Daten</a>.</p> | Berechtigungen auf Tabellen-, Spalten-, Zeilen- und Zellenebene werden unterstützt. |

## Weitere Ressourcen

### Blogbeiträge und Workshops

- [Zentralisieren Sie die Governance für Ihren Data Lake mithilfe von Amazon Redshift Spectrum und ermöglichen Sie AWS Lake Formation gleichzeitig eine moderne Datenarchitektur](#)
- [Verwenden Sie Redshift Spectrum, um Apache HUDI Copy On Write \(CoW\) -Tabellen in Amazon S3 Data Lake abzufragen](#)

# Verwenden mit AWS Lake Formation AWS Glue

Dateningenieure und DevOps Experten verwenden AWS Glue Extract, Transform and Load (ETL) mit Apache Spark, um Transformationen an ihren Datensätzen in Amazon S3 durchzuführen und die transformierten Daten für Analysen, maschinelles Lernen und Anwendungsentwicklung in Data Lakes und Data Warehouses zu laden. Da verschiedene Teams auf denselben Datensatz in Amazon S3 zugreifen, ist es unerlässlich, Berechtigungen basierend auf ihren Rollen zu gewähren und einzuschränken.

AWS Lake Formation ist darauf aufgebaut AWS Glue, und die Dienste interagieren auf folgende Weise:

- Lake Formation und AWS Glue teilen denselben Datenkatalog.
- Die folgenden Funktionen der Lake Formation Konsole rufen die AWS Glue Konsole auf:
  - Jobs — Weitere Informationen finden Sie im AWS Glue Developer Guide unter [Jobs hinzufügen](#).
  - Crawler — Weitere Informationen finden Sie unter [Katalogisieren von Tabellen mit einem Crawler im AWS Glue Entwicklerhandbuch](#).
- Bei den Workflows, die generiert werden, wenn Sie einen Lake Formation-Blueprint verwenden, handelt es sich um AWS Glue Workflows. Sie können diese Workflows sowohl in der Lake Formation Konsole als auch in der AWS Glue Konsole anzeigen und verwalten.
- Transformationen für maschinelles Lernen werden mit Lake Formation bereitgestellt und basieren auf AWS Glue API-Operationen. Sie erstellen und verwalten Transformationen für maschinelles Lernen auf der AWS Glue Konsole. Weitere Informationen finden Sie unter [Machine Learning Transforms](#) im AWS Glue Developer Guide.

Sie können die detaillierte Zugriffskontrolle von Lake Formation verwenden, um Ihre vorhandenen Datenkatalogressourcen und Amazon-S3-Datenstandorte zu verwalten.

## Note

AWS Glue 5.0 oder höher unterstützt detaillierte Zugriffskontrollen für Iceberg- und Hive-Tabellen, die von S3 unterstützt werden. Mit dieser Funktion können Sie Zugriffskontrollen auf Tabellen-, Zeilen-, Spalten- und Zellenebene für Leseabfragen innerhalb Ihrer AWS Glue Apache Spark-Jobs konfigurieren.

## Support für Transaktionstabellentypen

Durch die Anwendung Lake Formation Formation-Berechtigungen können Sie Ihre Transaktionsdaten in Ihren Amazon S3 S3-basierten Data Lakes sichern. In der folgenden Tabelle sind die in unterstützten Transaktionstabellenformate AWS Glue und die Lake Formation Formation-Berechtigungen aufgeführt. Lake Formation setzt diese AWS Glue Betriebsgenehmigungen durch.

### Unterstützte Tabellenformate

| Tabellenformat              | Beschreibung und zulässige Operationen                                                                                                                                                                                                            | Lake Formation Formation-Berechtigungen werden unterstützt in AWS Glue                                                                                                                                                                                                                              |
|-----------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Apache Hudi                 | <p>Ein offenes Tabellenformat, das zur Vereinfachung der inkrementellen Datenverarbeitung und der Entwicklung von Datenpipelines verwendet wird.</p> <p>Beispiele finden Sie unter <a href="#">Verwenden des Hudi-Frameworks in AWS Glue</a>.</p> | <p>Für Hudi-Tabellen sind Berechtigungen auf Tabellenebene verfügbar.</p> <p>Weitere Informationen finden Sie unter <a href="#">Limitations</a>.</p>                                                                                                                                                |
| Apache Iceberg              | <p>Ein offenes Tabellenformat, das große Sammlungen von Dateien als Tabellen verwaltet.</p> <p>Beispiele finden Sie unter <a href="#">Verwenden des Iceberg-Frameworks in AWS Glue</a>.</p>                                                       | <p>AWS Glue Mit Version 5.0 und höher können Sie Zugriffskontrollen auf Tabellen-, Zeilen-, Spalten- und Zellenebene für Leseabfragen innerhalb Ihrer Apache Spark-Jobs AWS Glue für Iceberg-Tabellen konfigurieren.</p> <p>Weitere Informationen finden Sie unter <a href="#">Limitations</a>.</p> |
| Linux Foundation Delta Lake | Delta Lake ist ein Open-Source-Projekt, das bei der Implementierung moderner                                                                                                                                                                      | Für Delta Lake-Tabellen sind Berechtigungen auf Tabellenebene verfügbar.                                                                                                                                                                                                                            |

| Tabellenformat | Beschreibung und zulässige Operationen                                                                                                                                                                                       | Lake Formation -Berechtigungen werden unterstützt in AWS Glue              |
|----------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|----------------------------------------------------------------------------|
|                | <p>Data-Lake-Architekturen hilft, die üblicherweise auf Amazon S3 oder Hadoop Distributed File System (HDFS) basieren.</p> <p>Beispiele finden Sie unter <a href="#">Verwenden des Delta Lake-Frameworks</a> in AWS Glue</p> | <p>Weitere Informationen finden Sie unter <a href="#">Limitations</a>.</p> |

## Weitere Ressourcen

### Blogbeiträge und Repositorien

- [Verwenden Sie den AWS Glue Konnektor, um Apache Iceberg-Tabellen mit ACID-Transaktionen zu lesen und zu schreiben und Zeitreisen durchzuführen](#)
- [Schreiben in Apache Hudi-Tabellen mit einem benutzerdefinierten Konnektor AWS Glue](#)
- AWS Repository mit [Cloudformation-Vorlage und Pyspark-Codebeispiel](#) zur Analyse von Streaming-Daten mit AWS Glue Apache Hudi und Amazon S3.

## Verwendung AWS Lake Formation mit Amazon EMR

Amazon EMR ist eine flexible AWS verwaltete Cluster-Plattform, auf der Sie beliebigen benutzerdefinierten Code auf unterstützten Big-Data-Frameworks wie Hadoop Map-Reduce, Spark, Hive, Presto usw. ausführen können. Organizations verwenden Amazon EMR auch, um Batch- und Stream-Datenverarbeitungsanwendungen in einem stark verteilten Cluster auszuführen. Mit Apache Spark auf Amazon EMR können Sie Ihre Datentransformationen und Ihren benutzerdefinierten Code in Datenbanken und Tabellen ausführen, deren Berechtigungen von Lake Formation verwaltet werden.

Es gibt drei Optionen für die Bereitstellung von Amazon EMR:

- EMR in EC2
- EMR Serverlos

- Amazon EMR auf EKS

Weitere Informationen finden Sie unter [Integrieren von Amazon EMR mit Lake Formation](#) oder [Verwenden von EMR Serverless mit AWS Lake Formation für](#) eine differenzierte Zugriffskontrolle

## Support für Transaktionstabellenformate

Die Amazon EMR-Versionen 6.15.0 und höher bieten Unterstützung für die Zugriffskontrolle auf Tabellen-, Zeilen-, Spalten- und Zellenebene von Lake Formation in den Tabellenformaten [Apache Hudi](#), [Apache Iceberg](#) und [Delta Lake](#), wenn Sie Daten mit Spark SQL lesen und schreiben.

Informationen zu Einschränkungen finden Sie unter [Überlegungen zu Amazon EMR with Lake Formation](#).

### Unterstützte Tabellenformate

| Tabellenformat | Beschreibung und zulässige Operationen                                                                                                                                                                                                                                | In Amazon EMR unterstützte Lake Formation Formation-Berechtigungen                                                |
|----------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-------------------------------------------------------------------------------------------------------------------|
| Apache Hudi    | <p>Ein offenes Tabellenformat, das zur Vereinfachung der inkrementellen Datenverarbeitung und der Entwicklung von Datenpipelines verwendet wird.</p> <p>Eine Liste der unterstützten Operationen finden Sie unter <a href="#">Apache Hudi und Lake Formation</a>.</p> | Amazon EMR unterstützt die Zugriffskontrolle auf Tabellen-, Zeilen-, Spalten- und Zellenebene mit Apache Hudi.    |
| Apache Iceberg | <p>Ein offenes Tabellenformat, das große Sammlungen von Dateien als Tabellen verwaltet.</p> <p>Eine Liste der unterstützten Operationen finden Sie unter</p>                                                                                                          | Amazon EMR unterstützt die Zugriffskontrolle auf Tabellen-, Zeilen-, Spalten- und Zellenebene mit Apache Iceberg. |

| Tabellenformat              | Beschreibung und zulässige Operationen                                                                                                                                                                                                                                                                                  | In Amazon EMR unterstützte Lake Formation Formation-Berechtigungen                                                     |
|-----------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|------------------------------------------------------------------------------------------------------------------------|
|                             | <a href="#">Apache Iceberg und Lake Formation.</a>                                                                                                                                                                                                                                                                      |                                                                                                                        |
| Linux Foundation Delta Lake | <p>Delta Lake ist ein Open-Source-Projekt, das bei der Implementierung moderner Data-Lake-Architekturen hilft, die üblicherweise auf Amazon S3 oder Hadoop Distributed File System (HDFS) basieren.</p> <p>Eine Liste der unterstützten Operationen finden Sie unter <a href="#">Delta Lake und Lake Formation.</a></p> | Amazon EMR unterstützt die Zugriffskontrolle auf Tabellen-, Zeilen-, Spalten- und Zellenebene mit Delta Lake-Tabellen. |

## Weitere Ressourcen

Benutzerhandbuch, Blogbeiträge und Workshops

- [Integration mit Amazon EMR mithilfe von Runtime Roles](#)
- [Schneller Start mit Apache Hudi, Apache Iceberg und Delta Lake mit Amazon EMR auf EKS](#)
- [Verwenden von Delta Lake OSS mit EMR Serverless](#)

## Verwendung mit Quick AWS Lake Formation

Quick unterstützt die Erkundung von Datensätzen, die mit Lake Formation Formation-Berechtigungen in Amazon S3 verwaltet werden, mithilfe von Athena.

Sowohl Benutzer der Standard- als auch der Enterprise Edition von Quick integrieren sich in Lake Formation, jedoch etwas anders.

- Enterprise Edition — Gewähren Sie einzelnen Quick-Benutzern und Gruppen detaillierte Zugriffssteuerungsberechtigungen (FGAC) für den Zugriff auf Datenbanken und Tabellen.
- Standard Edition — Erteilen Sie IAM-Rollen Berechtigungen für den Zugriff auf Datenbanken und Tabellen.

#### Note

Standardmäßig verwendet Quick eine Rolle mit dem Namen `aws-quicksight-service-role-v0`. Sie können auch benutzerdefinierte Rollen mit den erforderlichen Berechtigungen definieren, die den schnellen Zugriff auf Athena ermöglichen.

Weitere Informationen finden Sie unter [Autorisieren von Verbindungen](#) über AWS Lake Formation

## Weitere Ressourcen

### Blog-Posts

- [Aktivieren Sie detaillierte Berechtigungen für Schnellautoren in AWS Lake Formation](#)
- [Analysieren Sie Ihre Daten sicher mit AWS Lake Formation und Quick](#)

## Verwendung AWS Lake Formation mit AWS CloudTrail Lake

AWS CloudTrail Lake unterstützt das Durchsuchen von Ereignisdatenspeichern Amazon Athena mithilfe detaillierter Berechtigungen in AWS Lake Formation

#### Note

CloudTrail Lake kann nur abgefragt werden. Amazon Athena

Informationen zur Registrierung Ihres CloudTrail Lake-Ereignisdatenspeichers bei Lake Formation finden Sie [unter Einen Ereignisdatenspeicher verbinden](#).



# Protokollieren AWS Lake Formation Formation-API-Aufrufen mit AWS CloudTrail

AWS Lake Formation ist in einen Dienst integriert AWS CloudTrail, der eine Aufzeichnung der Aktionen bereitstellt, die von einem Benutzer, einer Rolle oder einem AWS Dienst in Lake Formation ausgeführt wurden. CloudTrail erfasst alle Lake Formation API-Aufrufe als Ereignisse. Zu den erfassten Aufrufen gehören Aufrufe von der Lake Formation Formation-Konsole AWS Command Line Interface, die und Code-Aufrufe der Lake Formation Formation-API-Aktionen. Wenn Sie einen Trail erstellen, können Sie die kontinuierliche Bereitstellung von CloudTrail Ereignissen an einen Amazon S3 S3-Bucket aktivieren, einschließlich Ereignissen für Lake Formation. Wenn Sie keinen Trail konfigurieren, können Sie die neuesten Ereignisse trotzdem in der CloudTrail Konsole im Ereignisverlauf anzeigen. Anhand der von gesammelten Informationen können Sie die Anfrage CloudTrail, die an Lake Formation gestellt wurde, die IP-Adresse, von der aus die Anfrage gestellt wurde, wer die Anfrage gestellt hat, wann sie gestellt wurde, und weitere Details ermitteln.

Weitere Informationen CloudTrail dazu finden Sie im [AWS CloudTrail Benutzerhandbuch](#).

## Informationen Lake Formation in CloudTrail

CloudTrail ist standardmäßig aktiviert, wenn Sie ein neues AWS Konto erstellen. Wenn in Lake Formation eine Aktivität auftritt, wird diese Aktivität zusammen mit anderen CloudTrail AWS Serviceereignissen in der Ereignishistorie als Ereignis aufgezeichnet. 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. Darüber hinaus enthält jedes Ereignis oder jeder Protokolleintrag Informationen darüber, wer die Anfrage generiert hat. Die Identitätsinformationen unterstützen Sie bei der Ermittlung der folgenden Punkte:

- Ob die Anfrage mit Root- oder AWS Identity and Access Management (IAM-) Benutzeranmeldedaten gestellt wurde.
- Gibt an, ob die Anforderung mit temporären Sicherheitsanmeldeinformationen für eine Rolle oder einen Verbundbenutzer gesendet wurde.
- Ob die Anfrage von einem anderen AWS Dienst gestellt wurde.

Weitere Informationen finden Sie unter [CloudTrail -Element userIdentity](#).

Sie können aktuelle Ereignisse für Ihr AWS Konto ansehen, suchen und herunterladen. Weitere Informationen finden Sie unter [Ereignisse mit dem CloudTrail Ereignisverlauf anzeigen](#).

Für eine fortlaufende Aufzeichnung der Ereignisse in Ihrem AWS Konto, einschließlich der Ereignisse für Lake Formation, erstellen Sie einen Trail. Ein Trail ermöglicht CloudTrail die Übermittlung von Protokolldateien an einen Amazon S3 S3-Bucket. Standardmäßig gilt ein in der Konsole erstellter Trail für alle AWS -Regionen. Der Trail protokolliert Ereignisse aus allen Regionen der AWS Partition und übermittelt die Protokolldateien an den von Ihnen angegebenen Amazon S3 S3-Bucket.

Darüber hinaus können Sie weitere AWS Dienste konfigurieren, z. B. Amazon Athena um die in den CloudTrail Protokollen gesammelten Ereignisdaten weiter zu analysieren und darauf zu reagieren. CloudTrail kann auch Protokolldateien an Amazon CloudWatch Logs and CloudWatch Events liefern.

Weitere Informationen finden Sie hier:

- [Übersicht zum Erstellen eines Trails](#)
- [CloudTrail unterstützte Dienste und Integrationen](#)
- [Konfiguration von Amazon SNS SNS-Benachrichtigungen für CloudTrail](#)
- [Empfangen von CloudTrail Protokolldateien aus mehreren Regionen](#) und [Empfangen von CloudTrail Protokolldateien von mehreren Konten](#)

## Lake Formation Formation-Ereignisse verstehen

Alle Lake Formation API-Aktionen werden vom Developer Guide protokolliert CloudTrail und sind im AWS Lake Formation Developer Guide dokumentiert. Beispielsweise generieren Aufrufe der `RevokePermissions` Aktionen `PutDataLakeSettingsGrantPermissions`, und Einträge in den CloudTrail Protokolldateien.

Das folgende Beispiel zeigt ein CloudTrail Ereignis für die `GrantPermissions` Aktion. Der Eintrag enthält den Benutzer, der die Berechtigung erteilt hat (`datalake_admin`), den Prinzipal, dem die Berechtigung erteilt wurde (`datalake_user1`), und die erteilte Berechtigung (`CREATE_TABLE`). Der Eintrag zeigt auch, dass die Erteilung fehlgeschlagen ist, weil die Zieldatenbank im `resource` Argument nicht angegeben wurde.

```
{
 "eventVersion": "1.08",
 "userIdentity": {
 "type": "IAMUser",
 "principalId": "AIDAZKE67KM3P775X74U2",
```

```

 "arn": "arn:aws:iam::111122223333:user/datalake_admin",
 "accountId": "111122223333",
 "accessKeyId": "...",
 "userName": "datalake_admin"
 },
 "eventTime": "2021-02-06T00:43:21Z",
 "eventSource": "lakeformation.amazonaws.com",
 "eventName": "GrantPermissions",
 "awsRegion": "us-east-1",
 "sourceIPAddress": "72.21.198.65",
 "userAgent": "aws-cli/1.19.0 Python/3.6.12
Linux/4.9.230-0.1.ac.223.84.332.metal1.x86_64 botocore/1.20.0",
 "errorCode": "InvalidInputException",
 "errorMessage": "Resource must have one of the have either the catalog, table or
database field populated.",
 "requestParameters": {
 "principal": {
 "dataLakePrincipalIdentifier": "arn:aws:iam::111122223333:user/
datalake_user1"
 },
 "resource": {},
 "permissions": [
 "CREATE_TABLE"
]
 },
 "responseElements": null,
 "requestID": "b85e863f-e75d-4fc0-9ff0-97f943f706e7",
 "eventID": "8d2cceff0-55f3-42d3-9ede-3a6faedaa5c1",
 "readOnly": false,
 "eventType": "AwsApiCall",
 "managementEvent": true,
 "eventCategory": "Management",
 "recipientAccountId": "111122223333"
}

```

Das nächste Beispiel zeigt einen CloudTrail Protokolleintrag für die GetDataAccess Aktion. Prinzipale rufen diese API nicht direkt auf. Wird vielmehr protokolliert, GetDataAccess wenn ein Principal oder ein integrierter AWS Dienst temporäre Anmeldeinformationen für den Zugriff auf Daten an einem Data Lake-Standort anfordert, der bei Lake Formation registriert ist.

```

{
 "eventVersion": "1.05",
 "userIdentity": {

```

```
 "type": "AWSAccount",
 "principalId": "AR0AQGFTBBBG0BWV2EMZA:GlueJobRunnerSession",
 "accountId": "111122223333"
 },
 "eventSource": "lakeformation.amazonaws.com",
 "eventName": "GetDataAccess",
 ...
 ...
 "additionalEventData": {
 "requesterService": "GLUE_JOB",
 "lakeFormationPrincipal": "arn:aws:iam::111122223333:role/ETL-Glue-Role",
 "lakeFormationRoleSessionName": "AWSLF-00-GL-111122223333-G13T0Rmng2"
 },
 ...
}
```

## Überwachung des Verbundkatalogzugriffs mit Amazon Redshift

Verbundkataloge von Amazon Redshift in den Protokollen generieren AWS Glue Data Catalog keine GetDataAccess Ereignisse in Lake Formation Formation-Protokollen. CloudTrail Um den Datenzugriff für Amazon Redshift Redshift-Tabellen im Datenkatalog zu verfolgen, überwachen GetTable und BatchGetTable Ereignisse, die Metadaten-Zugriffsmuster für Redshift-Verbundtabellen erfassen, einschließlich Tabellename, Datenbankname und Katalog-ID-Informationen.

 Weitere Informationen finden Sie unter:

- [Kontoübergreifende Protokollierung CloudTrail](#)

# Bewährte Methoden, Überlegungen und Einschränkungen von Lake Formation

In diesem Abschnitt finden Sie schnell bewährte Methoden, Überlegungen und Einschränkungen AWS Lake Formation.

Die maximale Anzahl von [Serviceressourcen](#) oder Vorgängen für Sie finden Sie unter Servicekontingenten AWS-Konto.

## Themen

- [Bewährte Methoden und Überlegungen für den kontenübergreifenden Datenaustausch](#)
- [Einschränkungen für dienstbezogene Rollen](#)
- [Regionsübergreifende Beschränkungen des Datenzugriffs](#)
- [Überlegungen und Einschränkungen im Datenkatalog](#)
- [Einschränkungen bei der Datenfilterung](#)
- [Überlegungen und Einschränkungen des hybriden Zugriffsmodus](#)
- [Einschränkungen beim Einbringen von Amazon Redshift Data Warehouse-Daten in die AWS Glue Data Catalog](#)
- [Einschränkungen bei der Integration von S3-Tabellen](#)
- [Überlegungen und Einschränkungen beim Datenaustausch im Hive-Metadatenpeicher](#)
- [Einschränkungen beim Datenaustausch mit Amazon Redshift](#)
- [Einschränkungen bei der IAM Identity Center-Integration](#)
- [Bewährte Methoden und Überlegungen zur Tag-basierten Zugriffskontrolle von Lake Formation](#)
- [Überlegungen zur attributbasierten Zugriffskontrolle, Einschränkungen und unterstützte Regionen](#)

## Bewährte Methoden und Überlegungen für den kontenübergreifenden Datenaustausch

Die kontoübergreifenden Funktionen von Lake Formation ermöglichen es Benutzern AWS-Konten, verteilte Data Lakes sicher über mehrere AWS Organisationen hinweg oder direkt mit IAM-Prinzipalen in einem anderen Konto zu teilen und bieten so einen detaillierten Zugriff auf die Data Catalog-Metadaten und die zugrunde liegenden Daten.

Beachten Sie die folgenden bewährten Methoden, wenn Sie den kontoübergreifenden Datenaustausch mit Lake Formation verwenden:

- Die Anzahl der Genehmigungen für Lake Formation, die Sie Schulleitern in Ihrem eigenen AWS Konto gewähren können, ist unbegrenzt. Lake Formation verwendet jedoch die Kapazität AWS Resource Access Manager (AWS RAM) für kontoübergreifende Zuschüsse, die Ihr Konto mit der benannten Ressourcenmethode gewähren kann. Um die AWS RAM Kapazität zu maximieren, folgen Sie diesen bewährten Methoden für die Methode der benannten Ressourcen:
- Verwenden Sie den neuen kontenübergreifenden Grant-Modus (Version 3 und höher unter Einstellungen für kontoübergreifende Version), um eine Ressource für externe AWS-Konto Benutzer freizugeben. Weitere Informationen finden Sie unter [Aktualisierung der Versionseinstellungen für die kontenübergreifende gemeinsame Nutzung von Daten](#).
- Ordnen Sie AWS Konten in Organisationen an und gewähren Sie Organisationen oder Organisationseinheiten Berechtigungen. Ein Zuschuss für eine Organisation oder Organisationseinheit gilt als ein Zuschuss.

Durch die Gewährung an Organisationen oder Organisationseinheiten entfällt auch die Notwendigkeit, eine AWS Resource Access Manager (AWS RAM) Einladung zur gemeinsamen Nutzung des Zuschusses anzunehmen. Weitere Informationen finden Sie unter [Zugreifen auf und Anzeigen von gemeinsam genutzten Datenkatalogtabellen und Datenbanken](#).

- Anstatt Berechtigungen für viele einzelne Tabellen in einer Datenbank zu gewähren, verwenden Sie den speziellen Platzhalter Alle Tabellen, um Berechtigungen für alle Tabellen in der Datenbank zu gewähren. Die Erteilung für alle Tabellen gilt als eine einzige Erteilung. Weitere Informationen finden Sie unter [Erteilen von Berechtigungen für Datenkatalogressourcen](#).

#### Note

Weitere Informationen zur Beantragung einer höheren Obergrenze für die Anzahl der Ressourcenfreigaben finden Sie unter [AWS Servicekontingenten](#) im Allgemeine AWS-Referenz. AWS RAM

- Sie müssen einen Ressourcenlink zu einer gemeinsam genutzten Datenbank erstellen, damit diese Datenbank in den Abfrage-Editoren Amazon Athena und Amazon Redshift Spectrum angezeigt wird. Ebenso müssen Sie Ressourcenlinks zu den Tabellen erstellen, um gemeinsam genutzte Tabellen mit Athena und Redshift Spectrum abfragen zu können. Die Ressourcenlinks werden dann in der Tabellenliste der Abfrage-Editoren angezeigt.

Anstatt Ressourcenlinks für viele einzelne Tabellen für Abfragen zu erstellen, können Sie den Platzhalter Alle Tabellen verwenden, um Berechtigungen für alle Tabellen in einer Datenbank zu gewähren. Wenn Sie dann einen Ressourcenlink für diese Datenbank erstellen und diesen Datenbankressourcen-Link im Abfrage-Editor auswählen, haben Sie Zugriff auf alle Tabellen in dieser Datenbank für Ihre Abfrage. Weitere Informationen finden Sie unter [Ressourcenlinks erstellen](#).

- Wenn Sie Ressourcen direkt mit Principals in einem anderen Konto teilen, ist der IAM-Prinzipal im Empfängerkonto möglicherweise nicht berechtigt, Ressourcenlinks zu erstellen, um die gemeinsam genutzten Tabellen mit Athena und Amazon Redshift Spectrum abfragen zu können. Anstatt für jede gemeinsam genutzte Tabelle einen Ressourcenlink zu erstellen, kann der Data Lake-Administrator eine Platzhalterdatenbank erstellen und der Gruppe Berechtigungen erteilen `CREATE_TABLE`. `ALLIAMPrincipal` Anschließend können alle IAM-Prinzipale im Empfängerkonto Ressourcenlinks in der Platzhalterdatenbank erstellen und mit der Abfrage der gemeinsam genutzten Tabellen beginnen.

Sehen Sie sich den CLI-Beispielbefehl zum Erteilen von Berechtigungen für `ALLIAMPrincipal` in an [Erteilen von Datenbankberechtigungen mit der benannten Ressourcenmethode](#).

- Wenn kontoübergreifende Berechtigungen direkt einem Prinzipal erteilt werden, kann nur der Empfänger der Zuweisung diese Berechtigungen einsehen. Der Data Lake-Administrator im AWS Konto des Empfängers kann diese direkten Zuschüsse nicht einsehen.
- Athena und Redshift Spectrum unterstützen die Zugriffskontrolle auf Spaltenebene, jedoch nur zur Inklusion, nicht zum Ausschluss. Die Zugriffskontrolle auf Spaltenebene wird in ETL-Jobs nicht unterstützt. AWS Glue
- Wenn eine Ressource mit Ihrem AWS Konto geteilt wird, können Sie nur Benutzern in Ihrem Konto Berechtigungen für die Ressource gewähren. Sie können anderen AWS Konten, Organisationen (nicht einmal Ihrer eigenen Organisation) oder der `IAMAllowedPrincipals` Gruppe keine Berechtigungen für die Ressource gewähren.
- Sie können einem externen Konto keine Rechte `DR0P` oder `Super` für eine Datenbank gewähren.
- Widerrufen Sie kontoübergreifende Berechtigungen, bevor Sie eine Datenbank oder Tabelle löschen. Andernfalls müssen Sie verwaiste Ressourcenanteile in löschen. AWS Resource Access Manager

 Weitere Informationen finden Sie auch unter

- [Bewährte Methoden und Überlegungen zur Tag-basierten Zugriffskontrolle von Lake Formation](#)
- [CREATE\\_TABLE](#) in der Liste finden Sie weitere Regeln und Einschränkungen [Referenz zu den Genehmigungen von Lake Formation](#) für den kontoübergreifenden Zugriff.

## Einschränkungen für dienstbezogene Rollen

Eine serviceverknüpfte Rolle ist eine spezielle Art von IAM-Rolle, mit der direkt verknüpft ist. AWS Lake Formation Diese Rolle verfügt über vordefinierte Berechtigungen, die es Lake Formation ermöglichen, in Ihrem Namen AWS dienstübergreifende Aktionen auszuführen.

Die folgenden Einschränkungen gelten, wenn Sie eine Service-Linked Role (SLR) verwenden, um Datenstandorte bei Lake Formation zu registrieren.

- Sie können Richtlinien für dienstverknüpfte Rollen nicht mehr ändern, sobald sie einmal erstellt wurden.
- Eine mit einem Dienst verknüpfte Rolle unterstützt keine kontenübergreifende gemeinsame Nutzung verschlüsselter Katalogressourcen. Verschlüsselte Ressourcen erfordern bestimmte AWS KMS Schlüsselberechtigungen. Mit Diensten verknüpfte Rollen verfügen über vordefinierte Berechtigungen, die nicht die Möglichkeit beinhalten, kontenübergreifend mit verschlüsselten Katalogressourcen zu arbeiten.
- Wenn Sie mehrere Amazon S3 S3-Standorte registrieren, kann die Verwendung einer serviceverknüpften Rolle dazu führen, dass Sie Ihre IAM-Richtliniengrenzen schnell überschreiten. Das passiert, weil bei serviceverknüpften Rollen die Richtlinie für Sie AWS geschrieben wird und sie dann zu einem großen Block inkrementiert wird, der all Ihre Registrierungen umfasst. Sie können vom Kunden verwaltete Richtlinien effizienter erstellen, Berechtigungen auf mehrere Richtlinien verteilen oder unterschiedliche Rollen für verschiedene Regionen verwenden.
- Amazon EMR on EC2 kann nicht auf Daten zugreifen, bei denen Sie Datenstandorte mit serviceverknüpften Rollen registrieren.
- Bei Vorgängen mit servicebezogenen Rollen werden Ihre AWS Richtlinien zur Servicesteuerung umgangen.



- Wenn Sie Datenstandorte mit einer serviceverknüpften Rolle registrieren, werden die IAM-Richtlinien letztendlich konsistent aktualisiert. Weitere Informationen finden Sie in der Dokumentation zur [IAM-Fehlerbehebung im IAM-Benutzerhandbuch](#).
- Sie können `SET_CONTEXT = TRUE` in Lake Formation Data Lake-Einstellungen nicht festlegen, wenn Sie serviceverknüpfte Rollen verwenden und Sie IAM Identity Center verwenden. Der Grund dafür ist, dass serviceverknüpfte Rollen unveränderliche Vertrauensrichtlinien haben, die nicht mit der vertrauenswürdigen Identitätsverbreitung kompatibel sind, die für die `SetContext` Überwachung mit IAM Identity Center-Prinzipalen erforderlich ist.

## Regionsübergreifende Beschränkungen des Datenzugriffs

Lake Formation unterstützt das Abfragen von Datenkatalogtabellen in allen Bereichen AWS-Regionen. Sie können mithilfe Amazon Athena von Amazon EMR und AWS Glue ETL von anderen Regionen aus auf Daten in einer Region zugreifen, indem Sie Ressourcenlinks in anderen Regionen erstellen, die auf die Quelldatenbanken und -tabellen verweisen. Mit regionsübergreifendem Tabellenzugriff können Sie auf Daten aus verschiedenen Regionen zugreifen, ohne die zugrunde liegenden Daten oder Metadaten in den Datenkatalog kopieren zu müssen.

Die folgenden Einschränkungen gelten für den regionsübergreifenden Tabellenzugriff.

- Lake Formation unterstützt das Abfragen von Datenkatalogtabellen aus einer anderen Region mit Amazon Redshift Spectrum nicht.
- In der Lake Formation Formation-Konsole zeigen die Datenbank- und Tabellenansichten die Datenbank-/Tabellenamen der Quellregion nicht an.
- Um die Liste der Tabellen in einer gemeinsam genutzten Datenbank aus einer anderen Region anzuzeigen, müssen Sie zuerst einen Ressourcenlink zu der gemeinsam genutzten Datenbank erstellen, dann den Ressourcenlink auswählen und Tabellen anzeigen auswählen.
- Lake Formation unterstützt keine regionsübergreifenden Resource Link-Aufrufe von SAML-Benutzern.
- Für die regionsübergreifende Funktion von Lake Formation fallen keine zusätzlichen Gebühren für Datenübertragungen an.

## Überlegungen und Einschränkungen im Datenkatalog

Die folgenden Überlegungen und Einschränkungen gelten für Datenkatalogansichten.

- Sie können keine Datenkatalogansicht von der Lake Formation Formation-Konsole aus erstellen. Sie können Ansichten mit dem AWS CLI oder SDK erstellen.
- Sie können Datenkatalogansichten aus 10 Tabellen erstellen. Es ist eine harte Grenze. Die einer Ansicht zugrunde liegenden Referenztabelle können zu derselben Datenbank oder zu verschiedenen Datenbanken innerhalb desselben AWS Kontos gehören.
- Weitere Überlegungen und Einschränkungen speziell für die Erstellung von Datenkatalogansichten mit Redshift finden Sie im Abschnitt [Überlegungen und Einschränkungen zu Datenkatalogansichten](#) im Amazon Redshift Database Developer Guide. Informationen zu Athena finden Sie im Abschnitt [Überlegungen und Einschränkungen zu Datenkatalogansichten](#) im Amazon Athena Benutzerhandbuch.
- Sie können Datenkatalogansichten für Tabellen erstellen, die bei Lake Formation registriert sind, sowohl im Hybridzugriffsmodus als auch im Lake Formation Modus.

Bei der Verwendung von Datenkatalogansichten im Lake Formation Hybridzugriffsmodus wird empfohlen, sicherzustellen, dass die Hauptbenutzer, die die Ansicht verwenden, für Lake Formation Berechtigungen für die in der Ansicht referenzierten Basistabellen aktiviert sind, ohne Zugriff zu gewähren. Dadurch wird sichergestellt, dass die Basistabellen den Verbrauchern nicht über AWS Glue IAM-Berechtigungen zugänglich gemacht werden.

- Bei der Version mit kontenübergreifendem Teilen von Ansichten gibt es keine Einschränkungen.
- Ansichten werden genauso wie Datenkatalogtabellen versioniert, wenn Sie die `ALTER VIEW` Anweisung für einen bereits erstellten Ansichtsdiagnostik verwenden. Sie können nicht zu einer vorherigen Ansicht zurückkehren, da sich die Version der Ansicht mit den zugrunde liegenden Datenänderungen ändert. Sie können eine View-Version löschen und es wird standardmäßig die nächste verfügbare neueste Version verwendet. Wenn Sie die Ansichtsversion ändern, stellen Sie sicher, dass Ihre Daten mit dem ausgewählten Ansichtsversionsschema synchronisiert sind.
- Es werden keine neuen Datenkataloge eingeführt. Die vorhandenen `CreateTableUpdateTable`, `DeleteTable` und `GetTable` APIs werden aktualisiert.
- Amazon Redshift erstellt immer Ansichten mit Varchar-Spalten aus Tabellen mit Zeichenfolgen. Wenn Sie Dialekte aus anderen Engines hinzufügen, müssen Sie Zeichenketten-spalten mit einer expliziten Länge in Varchar umwandeln.
- Die Gewährung von Data Lake-Berechtigungen `ALL tables` innerhalb einer Datenbank führt dazu, dass der Empfänger über Berechtigungen für alle Tabellen und Ansichten in der Datenbank verfügt.
- Sie können keine Ansichten erstellen:
  - Diese verweisen auf andere Ansichten.

- Wenn die Referenztabelle ein Ressourcenlink ist.
- Wenn sich die Referenztabelle in einem anderen Konto befindet.
- Aus externen Hive-Metastoren.
- Kontoübergreifende Definerrollen werden für Redshift Spectrum Dialect-Ansichten nicht unterstützt.
- Ressourcenlinks für den Athena-Dialekt im Athena-Abfrageeditor werden nicht unterstützt. Um kontenübergreifende Definerrollen für den Athena-Dialekt zu verwenden, fügen Sie das Konto, das die Basistabellen hostet, als Datenquelle in Athena hinzu.

## Einschränkungen bei der Datenfilterung

Wenn Sie Lake Formation-Berechtigungen für eine Datenkatalogtabelle gewähren, können Sie Datenfilterspezifikationen hinzufügen, um den Zugriff auf bestimmte Daten in Abfrageergebnissen und in Lake Formation integrierten Engines einzuschränken. Lake Formation verwendet Datenfilterung, um Sicherheit auf Spaltenebene, Sicherheit auf Zeilenebene und Sicherheit auf Zellebene zu erreichen. Sie können Datenfilter definieren und auf verschachtelte Spalten anwenden, wenn Ihre Quelldaten verschachtelte Strukturen enthalten.

## Hinweise und Einschränkungen für die Filterung auf Spaltenebene

Es gibt drei Möglichkeiten, die Spaltenfilterung festzulegen:

- Durch die Verwendung von Datenfiltern
- Mithilfe einfacher Spaltenfilterung oder verschachtelter Spaltenfilterung.
- Durch die Verwendung TAGs von.

Einfache Spaltenfilterung gibt lediglich eine Liste von Spalten an, die ein- oder ausgeschlossen werden sollen. Sowohl die Lake Formation Konsole als auch die API AWS CLI unterstützen einfache Spaltenfilterung. Ein Beispiel finden Sie unter [Grant with Simple Column Filtering](#).

Die folgenden Hinweise und Einschränkungen gelten für die Spaltenfilterung:

- AWS Glue 5.0 oder höher unterstützt eine differenzierte Zugriffskontrolle über Lake Formation nur für Apache Hive- und Apache Iceberg-Tabellen.

- Für die Gewährung SELECT mit der Grant-Option und der Spaltenfilterung müssen Sie eine Einschlussliste und keine Ausschlussliste verwenden. Ohne die Option „Gewährung“ können Sie entweder Einschluss- oder Ausschlusslisten verwenden.
- Um für eine Tabelle mit Spaltenfilterung eine Gewährung zu gewährenSELECT, müssen Sie für die Tabelle mit der Grant-Option und ohne Zeileneinschränkungen eine Erteilung erhalten SELECT haben. Sie müssen Zugriff auf alle Zeilen haben.
- Wenn Sie die SELECT Gewährungsoption und die Spaltenfilterung für einen Hauptbenutzer in Ihrem Konto verwenden, muss dieser Hauptbenutzer bei der Gewährung an einen anderen Hauptbenutzer die Spaltenfilterung für dieselben Spalten oder eine Teilmenge der gewährten Spalten angeben. Wenn Sie die SELECT Gewährungsoption und die Spaltenfilterung für ein externes Konto verwenden, kann der Data Lake-Administrator des externen Kontos für alle Spalten einem anderen Prinzipal in seinem Konto gewährenSELECT. Aber selbst bei SELECT „Alle Spalten“ hat dieser Hauptbenutzer nur Zugriff auf die Spalten, die dem externen Konto zugewiesen wurden.
- Sie können die Spaltenfilterung nicht auf Partitionsschlüssel anwenden.
- Einem Prinzipal mit der SELECT Berechtigung für eine Teilmenge von Spalten in einer Tabelle kann dieALTER, DROPDELETE, oder INSERT -Berechtigung für diese Tabelle nicht erteilt werden. Wenn Sie einem Prinzipal mit der INSERT Berechtigung ALTER DROPDELETE,, oder für eine Tabelle die SELECT Berechtigung mit Spaltenfilterung erteilen, hat dies keine Auswirkung.

Die folgenden Hinweise und Einschränkungen gelten für die Filterung verschachtelter Spalten:

- Sie können fünf Ebenen verschachtelter Felder in einen Datenfilter einbeziehen oder ausschließen.

#### Example

Spal1.Col1\_1.Col1\_1\_1.Col1\_1\_1\_1.Col1\_1\_1\_1\_1

- Sie können keine Spaltenfilterung auf verschachtelte Felder in Partitionsspalten anwenden.
- Wenn Ihr Tabellenschema einen Spaltennamen auf oberster Ebene enthält („Kunde“). „Adresse“), das dasselbe Muster einer verschachtelten Felddarstellung innerhalb eines Datenfilters aufweist (eine verschachtelte Spalte mit einem Spaltennamen der obersten Ebene customer und einem verschachtelten Feldnamen address wird wie "customer"."address" in einem Datenfilter angegeben), können Sie den Zugriff auf eine Spalte der obersten Ebene oder ein verschachteltes Feld nicht explizit angeben, da beide in den Listen nach demselben Muster dargestellt werden. inclusion/exclusion Dies ist mehrdeutig, und Lake Formation kann keine Lösung finden, wenn Sie die Spalte auf oberster Ebene oder das verschachtelte Feld angeben.

- Wenn eine Spalte oder ein verschachteltes Feld auf oberster Ebene ein doppeltes Anführungszeichen im Namen enthält, müssen Sie ein zweites doppeltes Anführungszeichen angeben, wenn Sie den Zugriff auf ein verschachteltes Feld in der Ein- und Ausschlussliste eines Datenzellenfilters angeben.

#### Example

Beispiel für einen verschachtelten Spaltennamen mit doppelten Anführungszeichen —  
`a.b.double"quote`

#### Example

Beispiel für eine Darstellung verschachtelter Spalten in einem Datenfilter —  
`"a"."b"."double""quote"`

## Einschränkungen bei der Filterung auf Zellebene

Beachten Sie die folgenden Hinweise und Einschränkungen für die Filterung auf Zeilen- und Zellebene.

- Sicherheit auf Zellebene wird für verschachtelte Spalten, Ansichten und Ressourcenlinks nicht unterstützt.
- Alle Ausdrücke, die in Spalten der obersten Ebene unterstützt werden, werden auch in verschachtelten Spalten unterstützt. Bei der Definition verschachtelter Ausdrücke auf Zeilenebene sollte jedoch NICHT auf verschachtelte Felder unter Partitionsspalten verwiesen werden.
- Sicherheit auf Zellebene ist in allen Regionen verfügbar, wenn Sie Athena Engine Version 3 oder Amazon Redshift Spectrum verwenden. Für andere Dienste ist die Sicherheit auf Zellebene nur in den Regionen verfügbar, die auf der aufgeführt sind. [Unterstützte Regionen](#)
- `SELECT INTO`-Anweisungen werden nicht unterstützt.
- Die `array map` Datentypen werden in Zeilenfilterausdrücken nicht unterstützt. Der `struct` Datentyp wird unterstützt.
- Die Anzahl der Datenfilter, die für eine Tabelle definiert werden können, ist unbegrenzt, aber es gibt eine Obergrenze von 100 Datenfiltern für einen einzelnen Prinzipal in einer Tabelle.
- Um einen Datenfilter mit einem Zeilenfilterausdruck anzuwenden, müssen `SELECT` Sie die `Grant`-Option auf alle Tabellenspalten anwenden. Diese Einschränkung gilt nicht für Administratoren in externen Konten, als die Gewährung für das externe Konto gewährt wurde.

- Wenn ein Principal Mitglied einer Gruppe ist und sowohl dem Prinzipal als auch der Gruppe Berechtigungen für eine Teilmenge von Zeilen erteilt werden, sind die effektiven Zeilenberechtigungen des Prinzipals die Vereinigung der Berechtigungen des Prinzipals und der Gruppenberechtigungen.
- Die folgenden Spaltennamen sind in einer Tabelle für die Filterung auf Zeilen- und Zellenebene eingeschränkt:
  - ctid
  - oid
  - xmin
  - cmin
  - xmax
  - cmax
  - Tischoide
  - xid einfügen
  - xid löschen
  - importoid
  - eindeutige ID von redcat
- Wenn Sie den Filterausdruck für alle Zeilen gleichzeitig mit anderen Filterausdrücken mit Prädikaten auf eine Tabelle anwenden, hat der Ausdruck für alle Zeilen Vorrang vor allen anderen Filterausdrücken.
- Wenn einem externen AWS Konto Berechtigungen für eine Teilmenge von Zeilen erteilt werden und der Data Lake-Administrator des externen Kontos diese Berechtigungen einem Prinzipal in diesem Konto erteilt, ist das effektive Filterprädikat des Prinzipals die Schnittmenge zwischen dem Prädikat des Kontos und allen Prädikaten, die dem Prinzipal direkt erteilt wurden.

Wenn das Konto beispielsweise über Zeilenberechtigungen mit dem Prädikat verfügt `dept='hr'` und dem Prinzipal separat die Berechtigung erteilt wurde `country='us'`, hat der Principal nur Zugriff auf Zeilen mit `dept='hr' country='us'`

Weitere Informationen zur Filterung auf Zellenebene finden Sie unter. [Datenfilterung und Sicherheit auf Zellebene in Lake Formation](#)

Hinweise und Einschränkungen bei der Abfrage von Tabellen mithilfe von Amazon Redshift Spectrum mit Sicherheitsrichtlinien auf Zeilenebene finden Sie unter [Überlegungen und Einschränkungen bei der Verwendung von RLS-Richtlinien](#) im Amazon Redshift Database Developer Guide.

## Überlegungen und Einschränkungen des hybriden Zugriffsmodus

Der Hybridzugriffsmodus bietet die Flexibilität, selektiv Lake Formation Formation-Berechtigungen für Datenbanken und Tabellen in Ihrem AWS Glue Data Catalog zu aktivieren.

Mit dem Hybridzugriffsmodus verfügen Sie jetzt über einen inkrementellen Pfad, mit dem Sie Lake Formation Formation-Berechtigungen für eine bestimmte Gruppe von Benutzern festlegen können, ohne die Berechtigungsrichtlinien anderer vorhandener Benutzer oder Workloads zu unterbrechen.

Die folgenden Überlegungen und Einschränkungen gelten für den hybriden Zugriffsmodus.

### Einschränkungen

- Amazon S3 S3-Standortregistrierung aktualisieren — Sie können die Parameter eines Standorts, der mit einer serviceverknüpften Rolle bei Lake Formation registriert ist, nicht bearbeiten.
- Opt-in-Option bei der Verwendung von LF-Tags — Wenn Sie Lake Formation Formation-Berechtigungen mithilfe von LF-Tags gewähren können, können Sie Principals aktivieren, um Lake Formation Formation-Berechtigungen in einem aufeinanderfolgenden Schritt durchzusetzen, indem Sie Datenbanken und Tabellen auswählen, denen LF-Tags angehängt sind.
- Zugriff im hybriden Zugriffsmodus — Der Zugriff auf den hybriden Zugriffsmodus in Lake Formation ist auf Benutzer mit Data Lake-Administrator- oder Nur-Lese-Administratorrechten beschränkt.
- Opt-In Principals — Derzeit kann nur eine Data Lake-Administratorrolle Principals für Ressourcen aktivieren.
- Alle Tabellen in einer Datenbank zulassen — Wenn Sie bei kontoübergreifenden Zuweisungen Berechtigungen gewähren und sich für alle Tabellen in einer Datenbank anmelden, müssen Sie sich auch für die Datenbank anmelden, damit die Berechtigungen funktionieren.

### Überlegungen

- Aktualisierung des bei Lake Formation registrierten Amazon S3-Standorts auf den Hybridzugriffsmodus — Wir empfehlen nicht, einen Amazon S3 S3-Datenstandort, der bereits bei Lake Formation registriert ist, in den Hybridzugriffsmodus zu konvertieren, obwohl dies möglich ist.
- API-Verhalten, wenn ein Datenstandort im Hybridzugriffsmodus registriert ist

- **CreateTable** — Der Standort gilt unabhängig von der Flagge für den hybriden Zugriffsmodus und dem Opt-In-Status als bei Lake Formation registriert. Daher benötigt der Benutzer die Datenstandortberechtigung, um eine Tabelle zu erstellen.
- **CreatePartition/BatchCreatePartitions/UpdatePartitions**(wenn der Partitionsstandort so aktualisiert wird, dass er auf den mit Hybrid registrierten Standort verweist) — Der Amazon S3 S3-Standort gilt unabhängig von der Markierung für den hybriden Zugriffsmodus und dem Opt-in-Status als bei Lake Formation registriert. Daher benötigt der Benutzer die Datenstandortberechtigung, um eine Datenbank zu erstellen oder zu aktualisieren.
- **CreateDatabase/UpdateDatabase** (wenn der Datenbankstandort so aktualisiert wird, dass er auf den im Hybridzugriffsmodus registrierten Standort verweist) — Der Standort gilt unabhängig von der Markierung für den Hybridzugriffsmodus und dem Opt-In-Status als bei Lake Formation registriert. Daher benötigt der Benutzer die Datenstandortberechtigung, um eine Datenbank zu erstellen oder zu aktualisieren.
- **UpdateTable** (wenn ein Tabellenstandort so aktualisiert wird, dass er auf den Standort verweist, der im Hybridzugriffsmodus registriert ist) — Der Standort gilt unabhängig von der Markierung für den hybriden Zugriffsmodus und dem Opt-in-Status als bei Lake Formation registriert. Daher benötigt der Benutzer eine Datenstandortberechtigung, um die Tabelle zu aktualisieren. Wenn der Tabellenstandort nicht aktualisiert wird oder auf einen Speicherort verweist, der nicht bei Lake Formation registriert ist, benötigt der Benutzer keine Datenstandortberechtigung, um die Tabelle zu aktualisieren.

## Einschränkungen beim Einbringen von Amazon Redshift Data Warehouse-Daten in die AWS Glue Data Catalog

Mit dem können Sie den Zugriff auf Analysedaten in Amazon Redshift Data Warehouses katalogisieren und verwalten. AWS Glue Data Catalog Die folgenden Einschränkungen gelten:

- Kontoübergreifendes Teilen wird auf Ebene des Verbundkatalogs nicht unterstützt. Sie können jedoch einzelne Datenbanken und Tabellen innerhalb eines Verbundkatalogs für mehrere Benutzer gemeinsam nutzen. AWS-Konto
- Sie müssen über die kontoübergreifende Version der Versionseinstellungen Version 4 oder höher verfügen, um Datenbanken oder Tabellen im Verbundkatalog für mehrere AWS-Konto Benutzer gemeinsam nutzen zu können.
- Der Datenkatalog unterstützt nur die Erstellung von Katalogen der obersten Ebene.



- Sie können nur die Beschreibung von Katalogen im Redshift Managed Storage (RMS) aktualisieren.
- Das Einrichten von Berechtigungen für Verbundkataloge sowie für Datenbanken und Tabellen im Verbundkatalog zur Gruppierung wird nicht unterstützt. `IAMAllowedPrincipals`
- DDL-Operationen (Data Definition Language) für den Katalog von Engines wie Athena, Amazon EMR Spark oder anderen, einschließlich der Einstellung von Katalogkonfigurationen, werden nicht unterstützt.
- Die Ausführung von DDL-Vorgängen an RMS-Tabellen mit Athena wird nicht unterstützt.
- Das Erstellen materialisierter Ansichten wird nicht unterstützt, unabhängig davon, ob es über Athena, Apache Spark AWS Glue Data Catalog, den oder den Amazon Redshift Redshift-Consumer erfolgt.
- Athena unterstützt kein Erlebnis mit mehreren Katalogen. Es kann jeweils nur eine Verbindung zu einem einzelnen, bestimmten Katalog herstellen. Athena kann nicht gleichzeitig auf mehrere Kataloge zugreifen oder Abfragen durchführen.
- Tagging- und Verzweigungsvorgänge auf Iceberg-Tabellen über Athena und Amazon Redshift werden nicht unterstützt.
- Time Travel auf RMS-Tabellen wird nicht unterstützt.
- Mehrstufige Kataloge mit Data-Lake-Tabellen werden nicht unterstützt. Alle in Amazon S3 zur Verwendung mit Data-Lake-Tabellen gespeicherten Daten müssen sich in der AWS Glue Data Catalog Standardversion befinden und können nicht in Katalogen mit mehreren Ebenen organisiert werden.
- In Amazon Redshift werden Datashares nicht zum registrierten Namespace hinzugefügt. Cluster und Namespaces sind synonym. Sobald Sie einen Cluster im veröffentlicht haben, können Sie keine neuen Daten mehr hinzufügen. AWS Glue Data Catalog
- Amazon EMR on EC2 unterstützt keine Verknüpfung zwischen RMS-Tabellen und Amazon S3-Tabellen. Nur EMR Serverless unterstützt diese Funktion.
- Externe Schemas und Tabellen werden nicht unterstützt.
- Auf RMS-Tabellen kann nur vom Erweiterungsendpunkt im AWS Glue Iceberg REST Catalog aus zugegriffen werden.
- Auf Hive-Tabellen kann nicht über Engines von Drittanbietern zugegriffen werden, die mit dem AWS Glue Iceberg REST-Katalog verbunden sind.
- Die Isolationsstufe `read_committed` für RMS-Tabellen über Spark wird unterstützt.

- Redshift-Datenbanknamen werden in der ohne Berücksichtigung von Groß- und Kleinschreibung behandelt AWS Glue Data Catalog, sind auf 128 Zeichen beschränkt und können alphanumerisch mit Bindestrichen (-) und Unterstrichen (\_) sein.
- Bei den Katalognamen wird nicht zwischen Groß- und Kleinschreibung unterschieden, sie sind auf 50 Zeichen beschränkt und können alphanumerisch mit Bindestrichen (-) und Unterstrichen (\_) sein.
- Amazon Redshift unterstützt nicht die Verwendung der Befehle GRANT und REVOKE im Lake Formation SQL-Stil zur Verwaltung von Zugriffsberechtigungen für Tabellen, die in der veröffentlicht wurden. AWS Glue Data Catalog
- Richtlinien für Sicherheit auf Zeilenebene und dynamische Datenmaskierung, die an den Amazon Redshift Redshift-Produzenten- (Quell-) Cluster angehängt sind, werden nicht durchgesetzt. Stattdessen werden die in Lake Formation definierten Zugriffsberechtigungen für die gemeinsam genutzten Daten durchgesetzt.
- Das Ausführen von Vorgängen in Data Definition Language (DDL) und Data Manipulation Language (DML) für Tabellenlinks wird nicht unterstützt.
- Wenn reservierte Schlüsselwörter nicht ordnungsgemäß maskiert werden, führt dies zu Ausfällen oder Fehlern.
- Die Verschlüsselung von Daten in Szenarien mit mehreren Katalogen wird nicht unterstützt.

## Einschränkungen bei der Integration von S3-Tabellen

Amazon S3 Tables ist in AWS Glue Data Catalog (Data Catalog) integriert und registriert den Katalog als Lake Formation Formation-Datenspeicherort. Sie können diese Registrierung über die Lake Formation Formation-Konsole oder mithilfe des Dienstes einrichten APIs.

### Note

Wenn Sie über eine ressourcenbasierte Richtlinie für IAM oder S3-Tabellen verfügen, die IAM-Benutzer und IAM-Rollen auf der Grundlage von Prinzipal-Tags einschränkt, müssen Sie der IAM-Rolle, die Lake Formation für den Zugriff auf Ihre S3-Daten verwendet, dieselben Prinzipal-Tags zuordnen (z. B. LakeFormationDataAccessRole) und dieser Rolle die erforderlichen Berechtigungen erteilen. Dies ist erforderlich, damit Ihre tagbasierte Zugriffskontrollrichtlinie ordnungsgemäß mit Ihrer Analyseintegration von S3 Tables funktioniert.

Die folgenden Einschränkungen gelten für die Integration des S3 Tables-Katalogs mit Data Catalog und Lake Formation:

- AWS Glue und Lake Formation unterstützen keine Spaltennamen mit gemischter Groß- und Kleinschreibung und konvertieren alle Spaltennamen in Kleinbuchstaben. Sie müssen sicherstellen, dass die Namen der Tabellenspalten eindeutig sind, wenn sie in Kleinbuchstaben umgewandelt werden. Verwenden Sie `customer_id` anstelle von `customerId`. Die Verwendung von Spaltennamen mit Groß- und Kleinschreibung wurde nur in der Vorschauversion unterstützt.
- Die `CreateCatalog` API kann in Amazon S3 keine Tabellen-Buckets erstellen.
- Die `SearchTables` API kann S3-Tabellen nicht durchsuchen.

## Überlegungen und Einschränkungen beim Datenaustausch im Hive-Metadatenpeicher

Mit dem AWS Glue Data Catalog Metadatenverbund (Data Catalog Federation) können Sie den Datenkatalog mit externen Metastores verbinden, die Metadaten für Ihre Amazon S3 S3-Daten speichern, und Datenzugriffsberechtigungen mithilfe von AWS Lake Formation sicher verwalten.

Die folgenden Überlegungen und Einschränkungen gelten für Verbunddatenbanken, die aus Hive-Datenbanken erstellt werden:

### Überlegungen

- AWS SAM Anwendungssupport — Sie sind verantwortlich für die Verfügbarkeit der bereitgestellten Anwendungsressourcen (Amazon API Gateway und AWS SAM der Lambda-Funktion). Stellen Sie sicher, dass die Verbindung zwischen dem AWS Glue Data Catalog und dem Hive-Metastore funktioniert, wenn Benutzer Abfragen ausführen.
- Versionsanforderung für Hive Metastore — Sie können Verbunddatenbanken nur mit Apache Hive Version 3 und höher erstellen.
- Anforderung einer zugewiesenen Datenbank — Jede Hive-Datenbank muss einer neuen Datenbank in Lake Formation zugeordnet werden.
- Verbundunterstützung auf Datenbankebene — Sie können nur auf Datenbankebene eine Verbindung zu Hive Metastore herstellen.
- Berechtigungen für Verbunddatenbanken — Die Berechtigungen, die auf eine Verbunddatenbank oder Tabellen unter einer Verbunddatenbank angewendet werden, bleiben auch dann bestehen,

wenn eine Quelltable oder eine Datenbank gelöscht wird. Wenn die Quelldatenbank oder -table neu erstellt wird, müssen Sie die Berechtigungen nicht erneut gewähren. Wenn eine Verbundtable mit Lake Formation Formation-Berechtigungen an der Quelle gelöscht wird, sind Lake Formation Formation-Berechtigungen weiterhin sichtbar, und Sie können sie bei Bedarf widerrufen.

Wenn ein Benutzer eine Verbunddatenbank löscht, gehen alle zugehörigen Berechtigungen verloren. Durch das Neuerstellen derselben Datenbank mit demselben Namen werden die Lake Formation Formation-Berechtigungen nicht wiederhergestellt. Benutzer müssen erneut neue Berechtigungen einrichten.

- **IAMAllowedHauptgruppenberechtigungen für Verbunddatenbanken** — Basierend auf dem `DataLakeSettings` kann Lake Formation Berechtigungen für alle Datenbanken und Tabellen einer virtuellen Gruppe mit dem Namen `IAMAllowedPrincipal` zuweisen. Das `IAMAllowedPrincipal` bezieht sich auf alle IAM-Prinzipale, die über IAM-Prinzipalrichtlinien und Ressourcenrichtlinien Zugriff auf Datenkatalogressourcen haben. AWS Glue Wenn diese Berechtigungen für eine Datenbank oder Tabelle vorhanden sind, erhalten alle Prinzipale Zugriff auf die Datenbank oder Tabelle.

Lake Formation erlaubt jedoch keine `IAMAllowedPrincipal` Berechtigungen für Tabellen in Verbunddatenbanken. Wenn Sie Verbunddatenbanken erstellen, stellen Sie sicher, dass Sie den `CreateTableDefaultPermissions` Parameter als leere Liste übergeben.

Weitere Informationen finden Sie unter [Ändern der Standardeinstellungen für Ihren Data Lake](#).

- **Tabellen in Abfragen verknüpfen** — Sie können Hive-Metastore-Tabellen mit systemeigenen Data Catalog-Tabellen verbinden, um Abfragen auszuführen.

## Einschränkungen

- **Einschränkung bei der Synchronisierung von Metadaten zwischen dem AWS Glue Data Catalog und dem Hive-Metastore** — Nachdem Sie die Hive-Metastore-Verbindung hergestellt haben, müssen Sie eine Verbunddatenbank erstellen, um Metadaten im Hive-Metastore mit dem zu synchronisieren. AWS Glue Data Catalog Die Tabellen in der Verbunddatenbank werden zur Laufzeit synchronisiert, wenn Benutzer Abfragen ausführen.
- **Einschränkung beim Erstellen neuer Tabellen in einer Verbunddatenbank** — Sie können keine neuen Tabellen in einer Verbunddatenbank erstellen.
- **Einschränkung von Datenberechtigungen** — Support für Berechtigungen für Hive-Metastore-Tabellenansichten ist nicht verfügbar.

# Einschränkungen beim Datenaustausch mit Amazon Redshift

AWS Lake Formation ermöglicht es Ihnen, Daten in einem Datashare von Amazon Redshift sicher zu verwalten. Amazon Redshift ist ein vollständig verwalteter Data-Warehouse-Service im Petabyte-Bereich in der Cloud. AWS Mithilfe der Funktion zur gemeinsamen Nutzung von Daten hilft Ihnen Amazon Redshift dabei, Daten gemeinsam zu nutzen. AWS-Konten Weitere Informationen zur gemeinsamen Nutzung von Amazon Redshift-Daten finden Sie unter [Überblick über die gemeinsame Nutzung von Daten in Amazon Redshift](#).

Die folgenden Hinweise und Einschränkungen gelten für Verbunddatenbanken, die aus Amazon Redshift-Datenfreigaben erstellt wurden:

- Anforderung einer zugewiesenen Datenbank — Jeder Amazon Redshift Redshift-Datenaustausch muss einer neuen Datenbank in Lake Formation zugeordnet werden. Dies ist erforderlich, um eindeutige Tabellennamen beizubehalten, wenn die Darstellung der Datashare-Objekte in der Datenkatalogdatenbank vereinfacht wird.
- Einschränkung beim Erstellen neuer Tabellen in einer Verbunddatenbank — Sie können keine neuen Tabellen in Verbunddatenbanken erstellen.
- Berechtigungen für die Verbunddatenbanken — Die Berechtigungen, die auf eine Verbunddatenbank oder Tabellen in einer Verbunddatenbank angewendet werden, bleiben auch dann bestehen, wenn eine Quelltable oder eine Datenbank gelöscht wird. Wenn die Quelldatenbank oder -table neu erstellt wird, müssen Sie die Berechtigungen nicht erneut gewähren. Wenn eine Verbundtable mit Lake Formation Formation-Berechtigungen an der Quelle gelöscht wird, sind Lake Formation Formation-Berechtigungen weiterhin sichtbar und Sie können sie bei Bedarf widerrufen.

Wenn ein Benutzer eine Verbunddatenbank löscht, gehen alle zugehörigen Berechtigungen verloren. Durch das Neuerstellen derselben Datenbank mit demselben Namen werden die Lake Formation Formation-Berechtigungen nicht wiederhergestellt. Benutzer müssen erneut neue Berechtigungen einrichten.

- IAMAllowedHauptgruppenberechtigungen für Verbunddatenbanken — Basierend auf dem DataLakeSettings kann Lake Formation Berechtigungen für alle Datenbanken und Tabellen einer virtuellen Gruppe mit dem Namen IAMAllowedPrincipal zuweisen. Das IAMAllowedPrincipal bezieht sich auf alle IAM-Prinzipale, die über IAM-Prinzipalrichtlinien und Ressourcenrichtlinien Zugriff auf Datenkatalogressourcen haben. AWS Glue Wenn diese Berechtigungen für eine Datenbank oder Tabelle vorhanden sind, erhalten alle Prinzipale Zugriff auf die Datenbank oder Tabelle.

Lake Formation erlaubt jedoch keine `IAMAllowedPrincipal` Berechtigungen für Tabellen in Verbunddatenbanken. Wenn Sie Verbunddatenbanken erstellen, stellen Sie sicher, dass Sie den `CreateTableDefaultPermissions` Parameter als leere Liste übergeben.

Weitere Informationen finden Sie unter [Ändern der Standardeinstellungen für Ihren Data Lake](#).

- **Datenfilterung** — In Lake Formation können Sie Berechtigungen für eine Tabelle in einer Verbunddatenbank mit Filterung auf Spalten- und Zeilenebene gewähren. Sie können jedoch keine Filterung auf Spalten- und Zeilenebene kombinieren, um den Zugriff auf Tabellen in Verbunddatenbanken auf Zellenebene einzuschränken.
- **Kennung für Groß- und Kleinschreibung** — Amazon Redshift Redshift-Datashare-Objekte, die von Lake Formation verwaltet werden, unterstützen Tabellen- und Spaltennamen nur in Kleinbuchstaben. Aktivieren Sie die Groß- und Kleinschreibung nicht für Datenbanken, Tabellen und Spalten in Amazon Redshift Redshift-Datenfreigaben, wenn diese mit Lake Formation gemeinsam genutzt und verwaltet werden.
- **Abfrageunterstützung** — Sie können Amazon Redshift-Datenfreigaben, die von Lake Formation verwaltet werden, mit Amazon Redshift abfragen. Athena unterstützt nicht die Abfrage von Amazon Redshift-Datenfreigaben, die von Lake Formation verwaltet werden.

Weitere Informationen zu Einschränkungen bei der Arbeit mit Datenfreigaben in Amazon Redshift finden Sie unter [Einschränkungen für die gemeinsame Nutzung von Daten](#) im Amazon Redshift Database Developer Guide.

## Einschränkungen bei der IAM Identity Center-Integration

Mit AWS IAM Identity Center können Sie eine Verbindung zu Identitätsanbietern (IdPs) herstellen und den Zugriff für Benutzer und Gruppen über AWS Analysedienste hinweg zentral verwalten. Sie können die Anwendung in IAM Identity Center AWS Lake Formation als aktivierte Anwendung konfigurieren, und Data Lake-Administratoren können autorisierten Benutzern und Gruppen detaillierte Berechtigungen für Ressourcen gewähren. AWS Glue Data Catalog

Die folgenden Einschränkungen gelten für die Integration von Lake Formation mit IAM Identity Center:

- Sie können IAM Identity Center-Benutzer und -Gruppen in Lake Formation nicht als Data Lake-Administratoren oder Administratoren mit Schreibschutz zuweisen.

Benutzer und Gruppen von IAM Identity Center können verschlüsselte Datenkatalogressourcen abfragen, wenn Sie eine IAM-Rolle verwenden, die in Ihrem Namen die Verschlüsselung und Entschlüsselung des Datenkatalogs übernehmen AWS Glue kann. AWS verwaltete Schlüssel unterstützen keine vertrauenswürdige Identitätsweitergabe.

- Benutzer und Gruppen von IAM Identity Center können nur API-Operationen aufrufen, die in der von IAM Identity Center bereitgestellten `AWSIAMIdentityCenterAllowListForIdentityContext` Richtlinie aufgeführt sind.
- Lake Formation ermöglicht es IAM-Rollen von externen Konten, im Namen von IAM Identity Center-Benutzern und -Gruppen als Trägerrollen für den Zugriff auf Datenkatalogressourcen zu fungieren. Berechtigungen können jedoch nur für Datenkatalogressourcen innerhalb des Eigentümerkontos erteilt werden. Wenn Sie versuchen, Benutzern und Gruppen von IAM Identity Center Berechtigungen für Datenkatalogressourcen in einem externen Konto zu gewähren, gibt Lake Formation die folgende Fehlermeldung aus: „Kontoübergreifende Zuweisungen werden für den Prinzipal nicht unterstützt“.
- Wenn Sie Lake Formation mit IAM Identity Center verwenden, ist die Konfiguration der Anwendungszuweisung `false` standardmäßig auf eingestellt. Wenn Sie diese Konfiguration direkt über die [IAM Identity Center-API](#) ändern, müssen Sie anschließend alle Anwendungszuweisungen manuell mithilfe der API verwalten. Lake Formation synchronisiert oder verwaltet Zuweisungsänderungen, die außerhalb der Standardworkflows vorgenommen wurden, nicht automatisch, was sich auf die Zugriffsmuster und Autorisierungsabläufe in Ihrer Data-Lake-Umgebung auswirken kann.

## Bewährte Methoden und Überlegungen zur Tag-basierten Zugriffskontrolle von Lake Formation

Sie können LF-Tags erstellen, verwalten und zuweisen, um den Zugriff auf Datenbanken, Tabellen und Spalten im Datenkatalog zu kontrollieren.

Beachten Sie bei der Verwendung der tagbasierten Zugriffskontrolle von Lake Formation die folgenden bewährten Methoden:

- Alle LF-Tags müssen vordefiniert sein, bevor sie Datenkatalogressourcen zugewiesen oder Prinzipalen gewährt werden können.



Der Data Lake-Administrator kann Tag-Management-Aufgaben delegieren, indem er LF-Tag-Ersteller mit den erforderlichen IAM-Berechtigungen erstellt. Dateningenieure und Analysten entscheiden über die Eigenschaften und Beziehungen von LF-Tags. Die LF-Tag-Ersteller erstellen und verwalten dann die LF-Tags in Lake Formation.

- Sie können Datenkatalogressourcen mehrere LF-Tags zuweisen. Einer bestimmten Ressource kann nur ein Wert für einen bestimmten Schlüssel zugewiesen werden.

Sie können beispielsweise `module=Orders`, `region=Westdivision=Consumer`, usw. einer Datenbank, Tabelle oder Spalte zuweisen. Sie können nichts zuweisen `module=Orders, Customers`.

- Sie können Ressourcen keine LF-Tags zuweisen, wenn Sie die Ressource erstellen. Sie können LF-Tags nur vorhandenen Ressourcen hinzufügen.
- Sie können einem Prinzipal LF-Tag-Ausdrücke und nicht nur einzelne LF-Tags zuweisen.

Ein LF-Tag-Ausdruck sieht ungefähr wie folgt aus (in Pseudocode).

```
module=sales AND division=(consumer OR commercial)
```

Ein Prinzipal, dem dieser LF-Tag-Ausdruck erteilt wurde, kann nur auf zugewiesene Datenkatalogressourcen (Datenbanken, Tabellen und Spalten) zugreifen und entweder `module=sales` oder `division=consumer` oder `division=commercial`. Wenn Sie möchten, dass der Prinzipal auf Ressourcen zugreifen kann, die über `module=sales` oder `division=commercial` verfügen, sollten Sie nicht beide in dieselbe Zuweisung einbeziehen. Vergeben Sie zwei Zuschüsse, einen für `module=sales` und einen für `division=commercial`.

Der einfachste LF-Tag-Ausdruck besteht aus nur einem LF-Tag, z. B. `module=sales`.

- Ein Prinzipal, dem Berechtigungen für ein LF-Tag mit mehreren Werten erteilt wurden, kann mit einem dieser Werte auf Datenkatalogressourcen zugreifen. Wenn einem Benutzer beispielsweise ein LF-Tag mit `key=module` und `values=` gewährt wird, hat der Benutzer Zugriff auf `orders`, `customers` Ressourcen, denen entweder `module=orders` oder `module=customers` zugewiesen ist.
- Sie benötigen die `Grant with LF-Tag expressions` Berechtigung, Datenberechtigungen für Datenkatalogressourcen mithilfe der LF-TBAC-Methode zu erteilen. Der Data Lake-Administrator und der LF-Tag-Ersteller erhalten diese Berechtigung implizit. Ein Prinzipal, der über die `Grant with LF-Tag expressions` entsprechende Berechtigung verfügt, kann Datenberechtigungen für die Ressourcen gewähren, indem er:



- die benannte Ressourcenmethode
- die LF-TBAC-Methode, aber nur unter Verwendung desselben LF-Tag-Ausdrucks

Gehen Sie beispielsweise davon aus, dass der Data Lake-Administrator den folgenden Zuschuss erteilt (in Pseudocode).

```
GRANT (SELECT ON TABLES) ON TAGS module=customers, region=west,south TO user1 WITH
GRANT OPTION
```

In diesem Fall `user1` kann anderen Prinzipalen mithilfe `SELECT` der LF-TBAC-Methode eine Genehmigung für Tabellen erteilt werden, jedoch nur mit dem vollständigen LF-Tag-Ausdruck. `module=customers, region=west,south`

- Wenn einem Prinzipal sowohl mit der LF-TBAC-Methode als auch mit der benannten Ressourcenmethode Berechtigungen für eine Ressource erteilt werden, sind die Berechtigungen, die der Prinzipal für die Ressource besitzt, die Vereinigung der von beiden Methoden erteilten Berechtigungen.
- Lake Formation unterstützt die kontenübergreifende Gewährung `DESCRIBE` und `ASSOCIATE` Aktivierung von LF-Tags sowie die kontenübergreifende Erteilung von Berechtigungen für Datenkatalogressourcen mithilfe der LF-TBAC-Methode. In beiden Fällen ist der Principal eine Konto-ID. AWS

#### Note

Lake Formation unterstützt kontenübergreifende Zuschüsse für Organisationen und Organisationseinheiten mithilfe der LF-TBAC-Methode. Um diese Funktion nutzen zu können, müssen Sie die Einstellungen für die kontenübergreifende Version auf Version 3 aktualisieren.

Weitere Informationen finden Sie unter [Kontoübergreifender Datenaustausch in Lake Formation](#).

- Datenkatalogressourcen, die in einem Konto erstellt wurden, können nur mit LF-Tags gekennzeichnet werden, die in demselben Konto erstellt wurden. In einem Konto erstellte LF-Tags können nicht mit gemeinsam genutzten Ressourcen aus einem anderen Konto verknüpft werden.
- Wenn Sie die Tag-Based Access Control (LF-TBAC) von Lake Formation verwenden, um kontenübergreifenden Zugriff auf Datenkatalogressourcen zu gewähren, sind Ergänzungen der

Datenkatalog-Ressourcenrichtlinie für Ihr Konto erforderlich. AWS Weitere Informationen finden Sie unter [Voraussetzungen](#).

- LF-Tag-Schlüssel und LF-Tag-Werte dürfen eine Länge von 50 Zeichen nicht überschreiten.
- Die maximale Anzahl von LF-Tags, die einer Datenkatalogressource zugewiesen werden können, beträgt 50.
- Bei den folgenden Grenzwerten handelt es sich um weiche Grenzwerte:
  - Die maximale Anzahl von LF-Tags, die erstellt werden können, beträgt 1000.
  - Die maximale Anzahl von Werten, die für ein LF-Tag definiert werden können, ist 1000.
- Tags, Schlüssel und Werte werden beim Speichern ausschließlich in Kleinbuchstaben umgewandelt.
- Einer bestimmten Ressource kann nur ein Wert für ein LF-Tag zugewiesen werden.
- Wenn einem Principal mit einem einzigen Grant mehrere LF-Tags gewährt werden, kann der Principal nur auf Datenkatalogressourcen zugreifen, die über alle LF-Tags verfügen.
- Wenn eine Auswertung eines LF-Tag-Ausdrucks dazu führt, dass nur auf eine Teilmenge von Tabellenspalten zugegriffen wird, die bei einer Übereinstimmung erteilte Lake Formation-Berechtigung jedoch eine der Berechtigungen ist, die vollen Spaltenzugriff erforderten, nämlich, `oder,,,,,,,,Alter,,Drop,,Insert,,Delete,,`, dann wird keine dieser Berechtigungen gewährt. Stattdessen wird nur `Describe` gewährt. Wenn die erteilte Erlaubnis `All (Super)` lautet, dann `Describe` werden nur `Select` und erteilt.
- Platzhalter werden nicht mit LF-Tags verwendet. Um allen Spalten einer Tabelle ein LF-Tag zuzuweisen, weisen Sie der Tabelle das LF-Tag zu, und alle Spalten in der Tabelle erben das LF-Tag. Um allen Tabellen in einer Datenbank ein LF-Tag zuzuweisen, weisen Sie der Datenbank das LF-Tag zu, und alle Tabellen in der Datenbank erben dieses LF-Tag.
- Sie können bis zu 1000 LF-Tag-Ausdrücke in einem Konto erstellen.
- Sie können bis zu 50 LF-Tag-Ausdrücke verwenden, um einem Prinzipal Berechtigungen für die Datenkatalogressourcen zu erteilen.
- Beim Erteilen oder Widerrufen von Berechtigungen für einen Inline-LF-Tag-Ausdruck darf die Größe des LF-Tag-Ausdrucks 900 Byte nicht überschreiten. Verwenden Sie die gespeicherten LF-Tag-Ausdrücke, um Berechtigungen für größere LF-Tag-Ausdrücke zu erteilen. Weitere Informationen finden Sie unter [LF-Tag-Ausdrücke erstellen](#).
- Um LF-Tag zu bestehenden Redshift-Verbundkatalogen hinzuzufügen, die vor der allgemeinen Verfügbarkeit der LF-Tag-Unterstützung für Verbundkataloge erstellt wurden, müssen Sie sich an das Support-Team wenden, um Unterstützung zu erhalten. AWS

# Überlegungen zur attributbasierten Zugriffskontrolle, Einschränkungen und unterstützte Regionen

Die folgenden Überlegungen und Einschränkungen gelten für die attributbasierte Zugriffskontrolle (ABAC).

- ABAC unterstützt die Gewährung von Zugriff mithilfe von LF-Tag-Richtlinien nicht.
- Erteilbare Berechtigungen sind bei ABAC nicht verfügbar.
- ABAC unterstützt die Erteilung von Berechtigungen für IAM Identity Center-Benutzer nicht.
- Wenn Sie ABAC-Grants für eine Tabelle in Lake Formation verwenden, gewährt Lake Formation keine DESCRIBE Berechtigungen für die übergeordnete Datenbank oder den übergeordneten Katalog. Dies unterscheidet sich von Nicht-ABAC-Szenarien, in denen Lake Formation implizite DESCRIBE Berechtigungen für übergeordnete Ressourcen bereitstellt.
- Alle Principals mit dem AmazonDataZoneProject Tag-Schlüssel werden für alle Datenkatalogressourcen immer so behandelt, als ob sie bei Lake Formation angemeldet sind.
- ABAC unterstützt nur Zeichenkettenattribute.

# Fehlerbehebung bei der Lake Formation

Wenn Sie bei der Arbeit mit AWS Lake Formation auf Probleme stoßen, lesen Sie die Themen in diesem Abschnitt.

## Topics

- [Allgemeine Problembehebung](#)
- [Problembehandlung beim kontoübergreifenden Zugriff](#)
- [Problembehandlung bei Blueprints und Workflows](#)
- [Bekannte Probleme für AWS Lake Formation](#)
- [Die Fehlermeldung wurde aktualisiert](#)

## Allgemeine Problembehebung

Verwenden Sie die Informationen hier, um verschiedene Probleme mit der Lake Formation zu diagnostizieren und zu beheben.

### Fehler: Unzureichende Lake Formation Formation-Berechtigungen für <Amazon S3 location>

Es wurde versucht, eine Datenkatalogressource ohne Datenspeicherberechtigungen an dem Amazon S3 S3-Standort zu erstellen oder zu ändern, auf den die Ressource verweist.

Wenn eine Data Catalog-Datenbank oder -Tabelle auf einen Amazon S3 S3-Standort verweist, müssen Sie, wenn Sie Lake Formation Berechtigungen CREATE\_TABLE oder gewährenALTER, auch die DATA\_LOCATION\_ACCESS Berechtigung für den Standort erteilen. Wenn Sie diese Berechtigungen externen Konten oder Organisationen gewähren, müssen Sie die Option „Erteilen“ angeben.

Nachdem diese Berechtigungen einem externen Konto erteilt wurden, muss der Data Lake-Administrator für dieses Konto die Berechtigungen den Prinzipalen (Benutzern oder Rollen) im Konto gewähren. Wenn Sie die von einem anderen Konto erhaltene DATA\_LOCATION\_ACCESS Berechtigung erteilen, müssen Sie die Katalog-ID (AWS Konto-ID) des Besitzerkontos angeben. Das Besitzerkonto ist das Konto, mit dem der Standort registriert wurde.

Weitere Informationen erhalten Sie unter [Zugrundeliegende Datenzugriffskontrolle](#) und [Erteilung von Berechtigungen zum Speicherort von Daten](#).

## Fehler: „Unzureichende Verschlüsselungsschlüsselberechtigungen für die Glue-API“

Es wurde versucht, Lake Formation Berechtigungen ohne AWS Identity and Access Management (IAM) -Berechtigungen für den AWS KMS Verschlüsselungsschlüssel für einen verschlüsselten Datenkatalog zu gewähren.

## Meine Amazon Athena oder Amazon Redshift Redshift-Abfrage, die Manifeste verwendet, schlägt fehl

Lake Formation unterstützt keine Abfragen, die Manifeste verwenden.

## Fehler: „Unzureichende Lake Formation Formation-Berechtigungen: Erforderlich, Tag im Katalog erstellen“

Der user/role muss ein Data Lake-Administrator sein.

## Fehler beim Löschen ungültiger Data Lake-Administratoren

Sie sollten alle ungültigen Data Lake-Administratoren (gelöschte IAM-Rollen, die als Data Lake-Administratoren definiert sind) gleichzeitig löschen. Wenn Sie versuchen, ungültige Data Lake-Administratoren separat zu löschen, gibt Lake Formation einen ungültigen Prinzipalfehler aus.

## Problembehandlung beim kontoübergreifenden Zugriff

Verwenden Sie die Informationen hier, um Probleme mit dem kontenübergreifenden Zugriff zu diagnostizieren und zu beheben.

### Themen

- [Ich habe eine kontoübergreifende Lake Formation Formation-Genehmigung erteilt, aber der Empfänger kann die Ressource nicht sehen](#)
- [Principals im Empfängerkonto können die Datenkatalogressource sehen, aber nicht auf die zugrunde liegenden Daten zugreifen](#)

- Fehler: „Die Zuordnung ist fehlgeschlagen, weil der Anrufer nicht autorisiert war“ beim Annehmen einer AWS RAM Einladung zur gemeinsamen Nutzung von Ressourcen
- Fehler: „Nicht berechtigt, Berechtigungen für die Ressource zu erteilen“
- Fehler: „Zugriff zum Abrufen von AWS Unternehmensinformationen verweigert“
- Fehler: „Organisation <organization-ID>nicht gefunden“
- Fehler: „Unzureichende Lake Formation Formation-Berechtigungen: Unzulässige Kombination“
- `ConcurrentModificationException` bei grant/revoke Anfragen an externe Konten
- Fehler bei der Verwendung von Amazon EMR für den Zugriff auf kontoübergreifende Daten

## Ich habe eine kontoübergreifende Lake Formation Formation-Genehmigung erteilt, aber der Empfänger kann die Ressource nicht sehen

- Ist der Benutzer im Empfängerkonto ein Data Lake-Administrator? Nur Data Lake-Administratoren können die Ressource zum Zeitpunkt der Freigabe sehen.
- Verwenden Sie die Methode der benannten Ressource für ein Konto außerhalb Ihrer Organisation? In diesem Fall muss der Data Lake-Administrator des Empfängerkontos eine Einladung zur gemeinsamen Nutzung von Ressourcen in AWS Resource Access Manager (AWS RAM) annehmen.

Weitere Informationen finden Sie unter [the section called “Annahme einer Einladung AWS RAM zur gemeinsamen Nutzung von Ressourcen”](#).

- Verwenden Sie Ressourcenrichtlinien auf Kontoebene (Datenkatalog) in? AWS Glue Falls ja, dann müssen Sie, wenn Sie die Methode der benannten Ressourcen verwenden, eine spezielle Erklärung in die Richtlinie aufnehmen, die berechtigt, Richtlinien in Ihrem Namen AWS RAM weiterzugeben.

Weitere Informationen finden Sie unter [the section called “Verwaltung kontenübergreifender Berechtigungen sowohl AWS Glue mit Lake Formation als auch mit Lake Formation”](#).

- Verfügen Sie über die erforderlichen AWS Identity and Access Management (IAM-) Berechtigungen, um kontenübergreifenden Zugriff zu gewähren?

Weitere Informationen finden Sie unter [the section called “Voraussetzungen”](#).

- Für die Ressource, für die Sie Berechtigungen erteilt haben, dürfen der `IAMAllowedPrincipals` Gruppe keine Lake Formation Formation-Berechtigungen erteilt werden.
- Gibt es in der deny Richtlinie auf Kontoebene eine Erklärung zu der Ressource?

Principals im Empfängerkonto können die Datenkatalogressource sehen, aber nicht auf die zugrunde liegenden Daten zugreifen

Die Prinzipale im Empfängerkonto müssen über die erforderlichen AWS Identity and Access Management (IAM-) Berechtigungen verfügen. Details hierzu finden Sie unter [Zugreifen auf die zugrunde liegenden Daten einer gemeinsam genutzten Tabelle](#).

## Fehler: „Die Zuordnung ist fehlgeschlagen, weil der Anrufer nicht autorisiert war“ beim Annehmen einer AWS RAM Einladung zur gemeinsamen Nutzung von Ressourcen

Wenn das empfangende Konto versucht, die Einladung zur gemeinsamen Nutzung anzunehmen, schlägt die Aktion fehl, nachdem einem anderen Konto Zugriff auf eine Ressource gewährt wurde.

```
$ aws ram get-resource-share-associations --association-type PRINCIPAL --resource-
share-arns arn:aws:ram:aws-region:444444444444:resource-share/e1d1f4ba-xxxx-xxxx-xxxx-
xxxxxxxx5d8d
{
 "resourceShareAssociations": [
 {
 "resourceShareArn": "arn:aws:ram:aws-region:444444444444:resource-share/
e1d1f4ba-xxxx-xxxx-xxxx-xxxxxxxx5d8d
",
 "resourceShareName": "LakeFormation-MMCC0XQBH3Y",
 "associatedEntity": "5815803XXXXX",
 "associationType": "PRINCIPAL",
 "status": "FAILED",
 "statusMessage": "Association failed because the caller was not
authorized.",
 "creationTime": "2021-07-12T02:20:10.267000+00:00",
 "lastUpdatedTime": "2021-07-12T02:20:51.830000+00:00",
 "external": true
 }
]
}
```

Der Fehler tritt auf, weil der aufgerufen `glue:PutResourcePolicy` wird, AWS Glue wenn das Empfängerkonto die Einladung zur gemeinsamen Nutzung von Ressourcen annimmt. Um das Problem zu lösen, lassen Sie die `glue:PutResourcePolicy` Aktion der Rolle zu, die vom producer/grantor Konto verwendet wird.

## Fehler: „Nicht berechtigt, Berechtigungen für die Ressource zu erteilen“

Es wurde versucht, kontenübergreifende Berechtigungen für eine Datenbank oder Tabelle zu gewähren, die einem anderen Konto gehört. Wenn eine Datenbank oder Tabelle mit Ihrem Konto gemeinsam genutzt wird, können Sie als Data Lake-Administrator nur Benutzern in Ihrem Konto Berechtigungen dafür gewähren.

## Fehler: „Zugriff zum Abrufen von AWS Unternehmensinformationen verweigert“

Ihr Konto ist ein Verwaltungskonto für AWS Organizations und Sie verfügen nicht über die erforderlichen Berechtigungen zum Abrufen von Organisationsinformationen, z. B. Organisationseinheiten im Konto.

Weitere Informationen finden Sie unter [Required permissions for cross-account grants](#).

## Fehler: „Organisation <organization-ID>nicht gefunden“

Es wurde versucht, eine Ressource für eine Organisation freizugeben, aber die gemeinsame Nutzung für Organisationen ist nicht aktiviert. Aktivieren Sie die gemeinsame Nutzung von Ressourcen mit Organisationen.

Weitere Informationen finden Sie unter [Aktivieren der gemeinsamen Nutzung mit AWS Organizations](#) im AWS RAM Benutzerhandbuch.

## Fehler: „Unzureichende Lake Formation Formation-Berechtigungen: Unzulässige Kombination“

Ein Benutzer hat eine Datenkatalogressource gemeinsam genutzt, während der IAMAllowedPrincipals Gruppe Lake Formation Formation-Berechtigungen für die Ressource gewährt wurden. Der Benutzer muss alle Lake Formation Formation-Berechtigungen widerrufen, IAMAllowedPrincipals bevor er die Ressource teilen kann.

## ConcurrentModificationException bei grant/revoke Anfragen an externe Konten

Wenn Benutzer in LF-Tag-Richtlinien mehrere Anfragen gleichzeitig zum and/or Widerruf von Genehmigungen für einen Principal stellen, werden sie von Lake Formation ausgelöst. ConcurrentModificationException Benutzer müssen die Ausnahme catch und die



fehlgeschlagene grant/revoke Anfrage erneut versuchen. Verwendung von Batch-Versionen der `GrantPermissions/RevokePermissions`-API-Operationen — [BatchGrantPermissions](#) und [BatchRevokePermissions](#) behebt dieses Problem bis zu einem gewissen Grad, indem die Anzahl gleichzeitiger grant/revoke Anfragen reduziert wird.

## Fehler bei der Verwendung von Amazon EMR für den Zugriff auf kontoübergreifende Daten

Wenn Sie Amazon EMR verwenden, um auf Daten zuzugreifen, die von einem anderen Konto aus mit Ihnen geteilt wurden, versuchen einige Spark-Bibliotheken, den `Glue:GetUserDefinedFunctions`-API-Vorgang aufzurufen. Da die Versionen 1 und 2 der AWS RAM verwalteten Berechtigungen diese Aktion nicht unterstützen, erhalten Sie die folgende Fehlermeldung:

```
"ERROR: User: arn:aws:sts::012345678901:assumed-role/my-
spark-role/i-06ab8c2b59299508a is not authorized to perform:
glue:GetUserDefinedFunctions on resource: arn:exampleCatalogResource
because no resource-based policy allows the glue:GetUserDefinedFunctions
action"
```

Um diesen Fehler zu beheben, muss der Data Lake-Administrator, der die Ressourcenfreigabe erstellt hat, die AWS RAM verwalteten Berechtigungen aktualisieren, die der Ressourcenfreigabe zugeordnet sind. Version 3 der von AWS RAM verwalteten Berechtigungen ermöglicht es Prinzipalen, die `glue:GetUserDefinedFunctions`-Aktion auszuführen.

Wenn Sie eine neue Ressourcenfreigabe erstellen, wendet Lake Formation standardmäßig die neueste Version der AWS RAM verwalteten Berechtigung an, sodass Sie nichts unternehmen müssen. Um den kontoübergreifenden Datenzugriff für bestehende Ressourcenfreigaben zu ermöglichen, müssen Sie die AWS RAM verwalteten Berechtigungen auf Version 3 aktualisieren.

Die AWS RAM Berechtigungen, die Ressourcen zugewiesen wurden, die mit Ihnen geteilt wurden, finden Sie unter AWS RAM. Die folgenden Berechtigungen sind in Version 3 enthalten:

### Databases

- `AWSRAMPermissionGlueDatabaseReadWriteForCatalog`
- `AWSRAMPermissionGlueDatabaseReadWrite`

### Tables

- `AWSRAMPermissionGlueTableReadWriteForCatalog`
- `AWSRAMPermissionGlueTableReadWriteForDatabase`

**AllTables**

```
AWSRAMPermissionGlueAllTablesReadWriteForCatalog
AWSRAMPermissionGlueAllTablesReadWriteForDatabase
```

Um die Version mit AWS RAM verwalteten Berechtigungen vorhandener Ressourcenfreigaben zu aktualisieren

Sie (Data Lake-Administrator) können entweder [AWS RAM verwaltete Berechtigungen auf eine neuere Version aktualisieren](#), indem Sie den Anweisungen im AWS RAM Benutzerhandbuch folgen, oder Sie können alle vorhandenen Berechtigungen für den Ressourcentyp widerrufen und sie erneut gewähren. Wenn Sie Berechtigungen widerrufen, wird die mit dem AWS RAM Ressourcentyp verknüpfte Ressourcenfreigabe AWS RAM gelöscht. Wenn Sie Berechtigungen erneut gewähren, AWS RAM erstellt es neue Ressourcenfreigaben, denen die neueste Version der verwalteten Berechtigungen angehängt wird. AWS RAM

## Problembehandlung bei Blueprints und Workflows

Verwenden Sie die Informationen hier, um Blueprint- und Workflow-Probleme zu diagnostizieren und zu beheben.

### Themen

- [<role-ARN>Mein Blueprint schlug fehl mit der Meldung „User: <user-ARN>is not authorized to perform: iam: PassRole on resource:“](#)
- [<role-ARN>Mein Workflow ist mit „User: <user-ARN>is not authorized to perform: iam: PassRole on resource:“ fehlgeschlagen](#)
- [Ein Crawler in meinem Workflow ist mit der Meldung „Die Ressource ist nicht vorhanden oder der Anforderer ist nicht berechtigt, auf die angeforderten Berechtigungen zuzugreifen“ fehlgeschlagen](#)
- [Ein Crawler in meinem Workflow ist mit der Meldung „Beim Aufrufen der CreateTable Operation... ist ein Fehler aufgetreten \(AccessDeniedException\)“ fehlgeschlagen](#)

**<role-ARN>Mein Blueprint schlug fehl mit der Meldung „User: <user-ARN>is not authorized to perform: iam: PassRole on resource:“**

Es wurde versucht, einen Blueprint von einem Benutzer zu erstellen, der nicht über ausreichende Berechtigungen verfügt, um die gewählte Rolle zu bestehen.

Aktualisieren Sie die IAM-Richtlinie des Benutzers, um die Rolle weitergeben zu können, oder bitten Sie den Benutzer, eine andere Rolle mit den erforderlichen Passrole-Berechtigungen auszuwählen.

Weitere Informationen finden Sie unter [the section called “Referenz zu Personas und IAM-Berechtigungen in Lake Formation”](#).

<role-ARN>Mein Workflow ist mit „User: <user-ARN>is not authorized to perform: iam: PassRole on resource:“ fehlgeschlagen

Für die Rolle, die Sie für den Workflow angegeben haben, gab es keine Inline-Richtlinie, die es der Rolle ermöglichte, sich selbst weiterzugeben.

Weitere Informationen finden Sie unter [the section called “\(Optional\) Erstellen Sie eine IAM-Rolle für Workflows”](#).

Ein Crawler in meinem Workflow ist mit der Meldung „Die Ressource ist nicht vorhanden oder der Anforderer ist nicht berechtigt, auf die angeforderten Berechtigungen zuzugreifen“ fehlgeschlagen

Eine mögliche Ursache ist, dass die übergebene Rolle nicht über ausreichende Berechtigungen verfügte, um eine Tabelle in der Zieldatenbank zu erstellen. Erteilen Sie der Rolle die CREATE\_TABLE Berechtigung für die Datenbank.

Ein Crawler in meinem Workflow ist mit der Meldung „Beim Aufrufen der CreateTable Operation... ist ein Fehler aufgetreten (AccessDeniedException)“ fehlgeschlagen

Eine mögliche Ursache ist, dass die Workflow-Rolle keine Datenspeicherberechtigungen für den Zielspeicherort hatte. Erteilen Sie der Rolle Berechtigungen für den Datenspeicherort.

Weitere Informationen finden Sie unter [the section called “DATA\\_LOCATION\\_ACCESS”](#).

## Bekannte Probleme für AWS Lake Formation

Überprüfen Sie diese bekannten Probleme auf AWS Lake Formation.

### Themen

- [Einschränkung beim Filtern von Tabellenmetadaten](#)
- [Problem beim Umbenennen einer ausgeschlossenen Spalte](#)
- [Problem beim Löschen von Spalten in CSV-Tabellen](#)
- [Tabellenpartitionen müssen unter einem gemeinsamen Pfad hinzugefügt werden](#)
- [Problem beim Erstellen einer Datenbank während der Workflow-Erstellung](#)
- [Problem beim Löschen und erneuten Erstellen eines Benutzers](#)
- [Bei API-Vorgängen für den Datenkatalog wird der Wert für den `IsRegisteredWithLakeFormation` Parameter nicht aktualisiert](#)
- [Lake Formation Formation-Operationen unterstützen AWS Glue Schema Registry nicht](#)

## Einschränkung beim Filtern von Tabellenmetadaten

AWS Lake Formation Berechtigungen auf Spaltenebene können verwendet werden, um den Zugriff auf bestimmte Spalten in einer Tabelle einzuschränken. Wenn ein Benutzer mithilfe der Konsole oder einer API Metadaten über die Tabelle abrufen `glue:GetTable`, enthält die Spaltenliste im Tabellenobjekt nur die Felder, auf die er Zugriff hat. Es ist wichtig, die Einschränkungen dieser Metadatenfilterung zu verstehen.

Lake Formation stellt zwar Metadaten über Spaltenberechtigungen für integrierte Dienste zur Verfügung, das eigentliche Filtern von Spalten in Abfrageantworten liegt jedoch in der Verantwortung des integrierten Dienstes. Lake Formation-Clients, die Filterung auf Spaltenebene unterstützen, darunter Amazon Athena, Amazon Redshift Spectrum und Amazon EMR, filtern die Daten auf der Grundlage der bei Lake Formation registrierten Spaltenberechtigungen. Benutzer können keine Daten lesen, auf die sie keinen Zugriff haben sollten. Derzeit unterstützt AWS Glue ETL keine Spaltenfilterung.

### Note

EMR-Cluster werden nicht vollständig von AWS verwaltet. Daher liegt es in der Verantwortung der EMR-Administratoren, die Cluster ordnungsgemäß zu sichern, um unbefugten Zugriff auf Daten zu verhindern.

Bestimmte Anwendungen oder Formate speichern möglicherweise zusätzliche Metadaten, einschließlich Spaltennamen und -typen, in der `Parameters` Map als Tabelleneigenschaften. Diese

Eigenschaften werden unverändert zurückgegeben und sind für jeden Benutzer zugänglich, der über SELECT Berechtigungen für jede Spalte verfügt.

[Avro SerDe](#) speichert beispielsweise eine JSON-Darstellung des Tabellenschemas in einer Tabelleneigenschaft mit dem Namen `avro.schema.literal`, die allen Benutzern mit Zugriff auf die Tabelle zur Verfügung steht. Wir empfehlen, das Speichern vertraulicher Informationen in Tabelleneigenschaften zu vermeiden und zu beachten, dass Benutzer das vollständige Schema von Tabellen im Avro-Format erlernen können. Diese Einschränkung gilt nur für die Metadaten einer Tabelle.

AWS Lake Formation entfernt alle Tabelleneigenschaften, beginnend mit `spark.sql.sources.schema` der Antwort auf eine `glue:GetTable` oder eine ähnliche Anfrage, wenn der Aufrufer nicht über SELECT Berechtigungen für alle Spalten in der Tabelle verfügt. Dadurch wird verhindert, dass Benutzer Zugriff auf zusätzliche Metadaten zu Tabellen erhalten, die mit Apache Spark erstellt wurden. Wenn sie auf Amazon EMR ausgeführt werden, können Apache Spark-Anwendungen diese Tabellen immer noch lesen, aber bestimmte Optimierungen werden möglicherweise nicht angewendet, und Spaltennamen, bei denen Groß- und Kleinschreibung beachtet wird, werden nicht unterstützt. Wenn der Benutzer Zugriff auf alle Spalten in der Tabelle hat, gibt Lake Formation die Tabelle unverändert mit allen Tabelleneigenschaften zurück.

## Problem beim Umbenennen einer ausgeschlossenen Spalte

Wenn Sie Berechtigungen auf Spaltenebene verwenden, um eine Spalte auszuschließen und die Spalte dann umzubenennen, ist die Spalte nicht mehr von Abfragen ausgeschlossen, z. B. `SELECT *`

## Problem beim Löschen von Spalten in CSV-Tabellen

Wenn Sie eine Datenkatalogtabelle im CSV-Format erstellen und anschließend eine Spalte aus dem Schema löschen, können Abfragen fehlerhafte Daten zurückgeben, und die Berechtigungen auf Spaltenebene werden möglicherweise nicht eingehalten.

Problemumgehung: Erstellen Sie stattdessen eine neue Tabelle.

## Tabellenpartitionen müssen unter einem gemeinsamen Pfad hinzugefügt werden

Lake Formation erwartet, dass sich alle Partitionen einer Tabelle unter einem gemeinsamen Pfad befinden, der im Standortfeld der Tabelle festgelegt ist. Wenn Sie den Crawler verwenden, um

Partitionen zu einem Katalog hinzuzufügen, funktioniert dies problemlos. Wenn Sie Partitionen jedoch manuell hinzufügen und sich diese Partitionen nicht unter dem in der übergeordneten Tabelle festgelegten Speicherort befinden, funktioniert der Datenzugriff nicht.

## Problem beim Erstellen einer Datenbank während der Workflow-Erstellung

Wenn Sie mit der Lake Formation Konsole einen Workflow aus einem Blueprint erstellen, können Sie die Zieldatenbank erstellen, falls sie nicht existiert. Wenn Sie dies tun, erhält der angemeldete Benutzer die `CREATE_TABLE` Berechtigung für die Datenbank, die erstellt wird. Der Crawler, den der Workflow generiert, übernimmt jedoch die Rolle des Workflows, wenn er versucht, eine Tabelle zu erstellen. Dies schlägt fehl, da die Rolle nicht über die erforderlichen `CREATE_TABLE` Berechtigungen für die Datenbank verfügt.

Problemumgehung: Wenn Sie die Datenbank während der Workflow-Einrichtung über die Konsole erstellen, müssen Sie vor dem Ausführen des Workflows der Rolle, die mit dem Workflow verknüpft ist, die `CREATE_TABLE` Berechtigung für die Datenbank erteilen, die Sie gerade erstellt haben.

## Problem beim Löschen und erneuten Erstellen eines Benutzers

Das folgende Szenario führt zu fehlerhaften Lake Formation Berechtigungen, die zurückgegeben werden von: `lakeformation:ListPermissions`

1. Erstellen Sie einen Benutzer und gewähren Sie Lake Formation Berechtigungen.
2. Löschen Sie den Benutzer.
3. Erstellen Sie den Benutzer mit demselben Namen erneut.

`ListPermissions` gibt zwei Einträge zurück, einen für den alten Benutzer und einen für den neuen Benutzer. Wenn Sie versuchen, dem alten Benutzer erteilte Berechtigungen zu entziehen, werden die Berechtigungen dem neuen Benutzer entzogen.

## Bei API-Vorgängen für den Datenkatalog wird der Wert für den **IsRegisteredWithLakeFormation** Parameter nicht aktualisiert

Es gibt eine bekannte Einschränkung, dass Datenkatalog-API-Operationen, wie z. B. `GetTables` und `SearchTables` nicht, den Wert für den `IsRegisteredWithLakeFormation` Parameter aktualisieren und den Standardwert zurückgeben, der falsch ist. Es wird empfohlen, die `GetTable` API zu verwenden, um den richtigen Wert für den `IsRegisteredWithLakeFormation` Parameter anzuzeigen.

## Lake Formation Formation-Operationen unterstützen AWS Glue Schema Registry nicht

Lake Formation Formation-Operationen unterstützen keine AWS Glue Tabellen, die ein SchemaReference in der [Schemaregistry StorageDescriptor](#) zu verwenden enthalten.

## Die Fehlermeldung wurde aktualisiert

AWS Lake Formation hat die ressourcenspezifischen Ausnahmen auf allgemeine EntityNotFound Fehlermeldungen für die folgenden API-Operationen aktualisiert, um die Sicherheits- und Compliance-Ziele zu erfüllen.

- RevokePermissions
- GrantPermissions
- GetResourceLFTags
- GetTable
- GetDatabase

# AWS Lake Formation API

## Note

Die aktualisierte [API-Referenz](#) für den AWS Lake Formation Dienst ist jetzt verfügbar.

## Inhalt

- [Genehmigungen APIs](#)
  - [Operationen](#)
  - [Datentypen](#)
- [Data Lake-Einstellungen APIs](#)
  - [Operationen](#)
  - [Datentypen](#)
- [IAM Identity Center-Integration APIs](#)
  - [Operationen](#)
  - [Datentypen](#)
- [Hybrider Zugriffsmodus APIs](#)
  - [Operationen](#)
  - [Datentypen](#)
- [Verkauf von Zugangsdaten APIs](#)
  - [Operationen](#)
  - [Datentypen](#)
- [Taggen APIs](#)
  - [Operationen](#)
  - [Datentypen](#)
- [Datenfilter APIs](#)
  - [Operationen](#)
  - [Datentypen](#)
- [Gängige Datentypen](#)
  - [ErrorDetail Struktur](#)



- [Zeichenfolgemuster](#)

## Genehmigungen APIs

Im Abschnitt Permissions API werden Vorgänge und Datentypen beschrieben, die für das Erteilen und Widerrufen von Berechtigungen in erforderlich sind. AWS Lake Formation Alle [API-Operationen und Datentypen finden Sie im Lake Formation AWS Lake Formation API-Referenzhandbuch](#).

## Operationen

- [GrantPermissions](#)
- [RevokePermissions](#)
- [BatchGrantPermissions](#)
- [BatchRevokePermissions](#)
- [GetEffectivePermissionsForPath](#)
- [ListPermissions](#)
- [GetDataLakePrincipal](#)

## Datentypen

- [Ressource](#)
- [DatabaseResource](#)
- [TableResource](#)
- [TableWithColumnsResource](#)
- [DataCellsFilterResource](#)
- [DataLocationResource](#)
- [DataLakePrincipal](#)
- [PrincipalPermissions](#)
- [PrincipalResourcePermissions](#)
- [DetailsMap](#)
- [ColumnWildcard](#)
- [BatchPermissionsRequestEntry](#)

- [BatchPermissionsFailureEntry](#)

## Data Lake-Einstellungen APIs

Dieser Abschnitt enthält die API-Operationen und Datentypen für die Verwaltung der Data Lake-Administratoren für die Data Lake-Einstellungen.

### Operationen

- [GetDataLakeSettings](#)
- [PutDataLakeSettings](#)

### Datentypen

- [DataLakeSettings](#)

## IAM Identity Center-Integration APIs

Dieser Abschnitt enthält die Operationen zum Erstellen und Verwalten der Lake Formation Formation-Integration mit IAM Identity Center.

### Operationen

- [CreateLakeFormationIdentityCenterConfiguration](#)
- [DeleteLakeFormationIdentityCenterConfiguration](#)
- [DescribeLakeFormationIdentityCenterConfiguration](#)
- [UpdateLakeFormationIdentityCenterConfiguration](#)

### Datentypen

- [ExternalFilteringConfiguration](#)

# Hybrider Zugriffsmodus APIs

Im API-Abschnitt für den Hybridzugriffsmodus werden Vorgänge und Datentypen beschrieben, die für die Einrichtung des Hybridzugriffsmodus erforderlich sind AWS Lake Formation. Alle [API-Operationen und Datentypen finden Sie im Lake Formation AWS Lake Formation API-Referenzhandbuch](#).

## Operationen

- [CreateLakeFormationOptIn](#)
- [DeleteLakeFormationOptIn](#)
- [ListLakeFormationOptIns](#)

## Datentypen

- [Ressource](#)
- [DatabaseResource](#)
- [TableResource](#)
- [Informationen zur Ressource](#)
- [LakeFormationOptInsInfo](#)
- [DataLocationResource](#)

# Verkauf von Zugangsdaten APIs

Im Abschnitt Credential Vending API werden die Vorgänge und Datentypen im Zusammenhang mit der Nutzung des AWS Lake Formation Dienstes zum Verkauf von Anmeldeinformationen und zur Registrierung und Verwaltung einer Data-Lake-Ressource beschrieben.

## Operationen

- [RegisterResource](#)
- [DeregisterResource](#)
- [ListResources](#)
- [GetUnfilteredTableMetadata](#)

- [GetUnfilteredPartitionsMetadata](#)
- [GetTemporaryGluePartitionCredentials](#)
- [GetTemporaryGlueTableCredentials](#)
- [UpdateResource](#)

## Datentypen

- [FilterCondition](#)
- [RowFilter](#)
- [ResourceInfo](#)

## Taggen APIs

Im Abschnitt Tagging-API werden die Operationen und Datentypen im Zusammenhang mit einer Autorisierungsstrategie beschrieben, die ein Berechtigungsmodell für Attribute oder Schlüssel-Wert-Paar-Tags definiert.

## Operationen

- [Ausdruck abrufen LFTag](#)
- [LFTagAusdrücke auflisten](#)
- [LFTagAusdruck löschen](#)
- [LFTagAusdruck aktualisieren](#)
- [LFTagAusdruck erstellen](#)
- [AdditionLFTagsToResource](#)
- [RemoveLFTagsFromResource](#)
- [GetResourceLFTags](#)
- [ListeLFTags](#)
- [CreateLFTag](#)
- [Holen LFTag](#)
- [AktualisierenLFTag](#)

- [LöschenLFTag](#)
- [SearchTablesByLFTags](#)
- [SearchDatabasesByLFTags](#)

## Datentypen

- [LFTagKeyResource](#)
- [LFTagPolicyResource](#)
- [TaggedTable](#)
- [TaggedDatabase](#)
- [LFTag](#)
- [LFTagPaar](#)
- [LFTagFehler](#)
- [SpalteLFTag](#)

## Datenfilter APIs

Der Datenfilter APIs beschreibt, wie Datenzellenfilter in verwaltet AWS Lake Formation werden.

## Operationen

- [CreateDataCellsFilter](#)
- [DeleteDataCellsFilter](#)
- [ListDataCellsFilter](#)
- [GetDataCellsFilter](#)
- [UpdateDataCellsFilter](#)

## Datentypen

- [DataCellsFilter](#)
- [RowFilter](#)

# Gängige Datentypen

Die gängigen Datentypen beschreiben verschiedene Datentypen, die in AWS Lake Formation üblich sind.

## ErrorDetail Struktur

Enthält Details über einen Fehler.

Felder

- **ErrorCode** – UTF-8-Zeichenfolge, nicht weniger als 1 oder mehr als 255 Bytes lang, passend zum [Single-line string pattern](#).

Der Code im Zusammenhang mit diesem Fehler.

- **ErrorMessage** – Beschreibende Zeichenfolge, nicht mehr als 2048 Bytes lang, passend zum [URI address multi-line string pattern](#).

Eine Meldung mit einer Beschreibung des Fehlers.

## Zeichenfolgemuster

Die API verwendet die folgenden regulären Ausdrücke, um zu definieren, welche Inhalte für verschiedene Zeichenfolgenparameter und -mitglieder gültig sind:

- Einzeiliges Zeichenfolgenmuster – "[\u0020-\uD7FF\uE000-\uFFFD\uD800\uDC00-\uDBFF\uDFFF\t]\*"
- Mehrzeiliges Zeichenfolgenmuster für URI-Adressen – "[\u0020-\uD7FF\uE000-\uFFFD\uD800\uDC00-\uDBFF\uDFFF\r\n\t]\*"
- Benutzerdefiniertes Zeichenkettenmuster #3 — "^\\w+\\.\\w+\\.\\w+\$"
- Benutzerdefiniertes Zeichenkettenmuster #4 — "^\\w+\\.\\w+\$"
- Benutzerdefiniertes Zeichenkettenmuster #5 — "arn:aws:iam::[0-9]\*:role/.\*"
- Benutzerdefiniertes Zeichenkettenmuster #6 — "arn:aws:iam::[0-9]\*:user/.\*"
- Benutzerdefiniertes Zeichenkettenmuster #7 — "arn:aws:iam::[0-9]\*:group/.\*"
- Benutzerdefiniertes Zeichenfolgenmuster #8 — "arn:aws:iam::[0-9]\*:saml-provider/.\*"
- Benutzerdefiniertes Zeichenfolgenmuster #9 — "^( [\p{L}\p{Z}\p{N}\_.:\/=+\-@%]\* )\$"

- Benutzerdefiniertes Zeichenfolgenmuster #10 – `^([\p{L}\p{Z}\p{N}_.\: \*\V/=+\-@%] *)$`
- Benutzerdefiniertes Zeichenfolgenmuster #11 – `[\p{L}\p{N}\p{P}] *`

# Unterstützte Regionen

Dieser Abschnitt enthält Informationen zur Unterstützung AWS-Regionen und Funktionalität von Lake Formation.

## Allgemeine Verfügbarkeit

Informationen zu den Diensten, die von AWS-Regionen unterstützt werden AWS Lake Formation, finden Sie in [der Liste der verfügbaren AWS Dienste nach Regionen](#).

Eine Liste der Lake Formation Service-Endpunkte für jede Region und der Lake Formation Formation-Dienstkontingente finden Sie unter [AWS Lake Formation Endpunkte und](#) Kontingente.

## AWS GovCloud (US)

Einen Überblick über die Unterschiede zwischen AWS GovCloud (US) Region und Standard AWS-Regionen finden Sie unter [Wie AWS Lake Formation unterscheidet sich](#) für. AWS GovCloud (US)

## Transaktionen und Speicheroptimierung

Die Funktionen für gesteuerte Tabellen, Transaktionsunterstützung und Speicheroptimierungen für Lake Formation sind im Folgenden AWS-Regionen verfügbar:

| Name der Region         | Regionsparameter | Endpoint                                   |
|-------------------------|------------------|--------------------------------------------|
| USA Ost (Nord-Virginia) | us-east-1        | lakeformation.us-east-1.amazonaws.com      |
|                         |                  | lakeformation-fips.us-east-1.amazonaws.com |
| USA Ost (Ohio)          | us-east-2        | lakeformation.us-east-2.amazonaws.com      |
|                         |                  | lakeformation-fips.us-east-2.amazonaws.com |



| Name der Region          | Regionsparameter | Endpoint                                                                                |
|--------------------------|------------------|-----------------------------------------------------------------------------------------|
| USA West (Oregon)        | us-west-2        | lakeformation.us-west-2.amazonaws.com<br><br>lakeformation-fips.us-west-2.amazonaws.com |
| Asien-Pazifik (Mumbai)   | ap-south-1       | lakeformation.ap-south-1.amazonaws.com                                                  |
| Asien-Pazifik (Seoul)    | ap-northeast-2   | lakeformation.ap-northeast-2.amazonaws.com                                              |
| Asien-Pazifik (Singapur) | ap-southeast-1   | lakeformation.ap-southeast-1.amazonaws.com                                              |
| Asien-Pazifik (Sydney)   | ap-southeast-2   | lakeformation.ap-southeast-2.amazonaws.com                                              |
| Asien-Pazifik (Tokio)    | ap-northeast-1   | lakeformation.ap-northeast-1.amazonaws.com                                              |
| Europa (Frankfurt)       | eu-central-1     | lakeformation.eu-central-1.amazonaws.com                                                |
| Europa (Irland)          | eu-west-1        | lakeformation.eu-west-1.amazonaws.com                                                   |
| Europa (London)          | eu-west-2        | lakeformation.eu-west-2.amazonaws.com                                                   |
| Europa (Stockholm)       | eu-north-1       | lakeformation.eu-north-1.amazonaws.com                                                  |

| Name der Region        | Regionsparameter | Endpoint                                 |
|------------------------|------------------|------------------------------------------|
| Kanada (Zentral)       | ca-central-1     | lakeformation.ca-central-1.amazonaws.com |
| Südamerika (São Paulo) | sa-east-1        | lakeformation.sa-east-1.amazonaws.com    |

# Dokumentenverlauf für AWS Lake Formation

In der folgenden Tabelle werden wichtige Änderungen an der Dokumentation für beschrieben AWS Lake Formation.

| Änderung                                                                                                  | Beschreibung                                                                                                                                                                                                                                                                                               | Datum           |
|-----------------------------------------------------------------------------------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-----------------|
| <a href="#">Die Dokumentation für die attributbasierte Zugriffskontrolle wurde aktualisiert</a>           | Lake Formation ermöglicht es Ihnen, Prinzipalen mit passenden Attributen für Datenkatalogressourcen Berechtigungen zu erteilen. Weitere Informationen finden Sie unter <a href="#">Attributbasierte Zugriffskontrolle</a> .                                                                                | 17. April 2025  |
| <a href="#">Integration Amazon S3 S3-Tabellen mit AWS Lake Formation und AWS Glue Data Catalog</a>        | Sie können jetzt S3-Tabellen als AWS Glue Data Catalog Objekte integrieren und katalogisieren und den Katalog als Lake Formation Formation -Datenspeicherort registrieren. Weitere Informationen finden Sie unter <a href="#">Erstellen eines Amazon S3-Tables-Katalogs in der AWS Glue Data Catalog</a> . | 13. März 2025   |
| <a href="#">Die AWSLakeFormationCrossAccountManager Richtlinie von Lake Formation wurde aktualisiert.</a> | Lake Formation erweiterte die <a href="#">AWSLakeFormationCrossAccountManager</a> Richtlinie, indem der StringLike Bedingungsoperator durch den ArnLike Operator ersetzt wurde, der es IAM ermöglicht                                                                                                      | 25. Januar 2025 |

t, die ARN-Formatprüfung durchzuführen.

### Änderung der Richtlinie aktualisiert

Die Änderung der [AWSLakeFormationDataAdmin](#) Richtlinie wurde dokumentiert.

03. Dezember 2024

### Updates für mehrere Kataloge

AWS Glue Data Catalog ermöglicht es Ihnen, Verbundkataloge zu erstellen und Daten aus Amazon S3 S3-Data Lakes und Amazon Redshift Redshift-Data Warehouses zu vereinheitlichen sowie Daten aus Ihren Betriebsdatenbanken wie Amazon DynamoDB und Datenquellen von Drittanbietern wie Snowflake, MySQL usw. zu integrieren. [Weitere Informationen finden Sie unter Integrieren Ihrer Daten in die AWS Glue Data Catalog](#)

03. Dezember 2024

### Die Dokumentation für LF-Tag-Ausdrücke wurde aktualisiert

Sie können LF-Tag-Ausdrücke speichern und sie wiederverwenden, um Berechtigungen für die Datenkatalogressourcen zu erteilen. Weitere Informationen finden Sie unter [LF-Tag-Ausdrücke verwalten](#).

7. November 2024

[Die Dokumentation für Datenkatalogansichten wurde aktualisiert](#)

Sie können zusätzlich zur AWS Glue Data Catalog Verwendung von Amazon Athena und Amazon Redshift auch Ansichten AWS Glue APIs in der DDLs Verwendung erstellen. Weitere Informationen finden Sie unter Ansichten für den [Gebäudedatenkatalog](#).

7. August 2024

[Es wurde eine Dokumentation für den Verkauf überprüfbarer Anmeldeinformationen hinzugefügt](#)

Lake Formation ermöglicht es Ihnen, den Kontext des IAM Identity Center-Benutzers in die CloudTrail Ereignisse einzubeziehen und dann die Benutzer zu verfolgen, die auf Ihre Ressourcen zugreifen. Weitere Informationen finden Sie unter [Einbeziehen des IAM Identity Center-Benutzerkontextes in CloudTrail Protokolle](#).

14. Juli 2024

[Änderung der Richtlinie aktualisiert](#)

[Die Änderung der AWS Lake Formation Data Admin Richtlinien wurde dokumentiert \(Erklärung hinzugefügt IDs und überflüssige Berechtigungen entfernt\). AWS Lake Formation Cross Account Manager](#)

14. März 2024

[Die Einrichtung von Lake Formation wurde aktualisiert](#)

Die Schritte im AWS Lake Formation Abschnitt „[Einrichten](#)“ wurden aktualisiert.

7. Februar 2024

### Änderung der Richtlinie aktualisiert

Der Inline-Richtlinie der serviceverknüpften Rolle wurden neue Berechtigungen hinzugefügt. Weitere Informationen finden Sie unter [Verwenden von serviceverknüpften Rollen für Lake Formation](#).

7. Februar 2024

### Änderung der Richtlinie aktualisiert

Die Änderung der [LakeFormationDataAccessServiceRolePolicy](#) Richtlinie wurde dokumentiert.

2. Februar 2024

### Einschränkungen der konsolidierten Lake Formation

Es wurde ein einheitlicher Abschnitt für Einschränkungen und Überlegungen zur Lake Formation erstellt. Weitere Informationen finden Sie unter [Einschränkungen bei der Lake Formation](#).

15. Dezember 2023

### Dokumentation für die Iceberg-Verdichtung hinzugefügt

Um die Leseleistung von AWS Analysediensten wie Athena und Amazon EMR sowie AWS Glue ETL-Jobs zu verbessern, AWS Glue Data Catalog bietet es verwaltete Komprimierung (ein Prozess, der kleine Amazon S3 S3-Objekte zu größeren Objekten komprimiert) für Iceberg-Tabellen im Datenkatalog. Weitere Informationen finden Sie unter [Optimieren von Iceberg-Tabellen](#).

25. November 2023

[Dokumentation für die IAM Identity Center-Integration hinzugefügt](#)

IAM Identity Center-Integration ermöglichen Benutzern und Gruppen den Zugriff auf Datenkatalogressourcen, wodurch Lake Formation Formation-Berechtigungen durchgesetzt werden. Weitere Informationen finden Sie unter [IAM Identity Center-Integration](#).

25. November 2023

[Dokumentation für Datenkatalogansichten hinzugefügt](#)

Sie können Ansichten in der erstellen AWS Glue Data Catalog , die auf bis zu 10 Tabellen verweisen, indem Sie SQL-Editoren für Amazon Athena oder Amazon Redshift verwenden. Weitere Informationen finden Sie unter [Ansichten erstellen](#).

25. November 2023

[Die Änderung der Richtlinie wurde aktualisiert](#)

Die Änderung der [AWSLakeFormationCrossAccountManager](#) Richtlinie wurde dokumentiert.

25. Oktober 2023

[Dokumentation für den hybriden Zugriffsmodus hinzugefügt](#)

Der Hybridzugriffsmodus bietet die Flexibilität, selektiv Lake Formation Formation-Berechtigungen für Datenbanken und Tabellen in Ihrem AWS Glue Data Catalog zu aktivieren. Mit dem Hybridzugriffsmodus verfügen Sie jetzt über einen inkrementellen Pfad, mit dem Sie Lake Formation Formation-Berechtigungen für eine bestimmte Gruppe von Benutzern festlegen können, ohne die Berechtigungsrichtlinien anderer vorhandener Benutzer oder Workloads zu unterbrechen. Weitere Informationen finden Sie unter [Hybrid-Zugriffsmodus](#).

26. September 2023

[Dokumentation zum Erstellen von Apache Iceberg-Tabellen hinzugefügt](#)

Sie können jetzt Apache Iceberg-Tabellen erstellen, die das Apache Parquet-Datenformat verwenden, AWS Glue Data Catalog wobei sich die Daten in Amazon S3 befinden. Weitere Informationen finden Sie unter [Iceberg-Tabellen erstellen](#).

16. August 2023



[Dokumentation für den  
regionsübergreifenden  
Datenzugriff hinzugefügt](#)

Lake Formation unterstützt das Abfragen von Datenkatalogtabellen in allen AWS Regionen. Sie können mit Athena und Amazon EMR von anderen Regionen aus auf Daten in einer Region zugreifen und AWS Glue ETL ausführen, indem Sie Ressourcenlinks in anderen Regionen erstellen, die auf die Quelldatenbanken und -tabellen verweisen. Sie können den Datenkatalog mit externen Metastores verbinden, die Metadaten für Ihre Amazon S3 S3-Daten speichern, und Datenzugriffsberechtigungen mithilfe von AWS Lake Formation sicher verwalten. Weitere Informationen finden Sie unter [Regionsübergreifender Zugriff auf Tabellen](#).

30. Juni 2023

[Inhalt neu organisiert](#)

Die Kapitel im Leitfaden wurden neu organisiert, um der Benutzererfahrung von Lake Formation gerecht zu werden.

15. Mai 2023

## [Dokumentation für HMS Federation hinzugefügt](#)

Sie können den Datenkatalog mit externen Metastores verbinden, die Metadaten für Ihre Amazon S3-Daten speichern, und Datenzugriffsberechtigungen mithilfe von AWS Lake Formation sicher verwalten. Weitere Informationen finden Sie unter [Verwaltung von Berechtigungen für Datensätze, die externe Metastores verwenden](#).

15. April 2023

## [Dokumentation für Amazon Redshift Data Sharing hinzugefügt](#)

Sie können jetzt Daten in einem Datashare von Amazon Redshift mithilfe von Lake Formation-Berechtigungen sicher verwalten. Lake Formation unterstützt die Lizenzierung des Zugriffs auf Ihre Daten über AWS Data Exchange. Weitere Informationen finden Sie unter [Datenfreigabe in AWS Lake Formation](#).

30. November 2022

## [Support für den kontoübergreifenden Datenaustausch direkt mit Principals](#)

Es wurden Informationen zum direkten Teilen von Daten mit IAM-Prinzipalen in einem anderen Konto hinzugefügt. Weitere Informationen finden Sie unter [kontoübergreifender Datenfreigabe](#) in AWS Lake Formation.

10. November 2022

[Support für AWS RAM aktiviert  
en Datenaustausch mit TBAC](#)

[Es wurden Informationen  
zur LF-TBAC-Methode zur  
Gewährung von Datenkata  
logberechtigungen für  
kontoübergreifende Zuschüsse  
hinzugefügt. AWS Resource  
Access Manager](#)

10. November 2022

[Es wurde ein Abschnitt  
über die Arbeit mit anderen  
Diensten hinzugefügt](#)

Es wurden Informationen darüber hinzugefügt, wie AWS Dienste wie Athena AWS Glue, Redshift Spectrum und Amazon EMR Lake Formation verwenden können, um sicher auf Daten an Amazon S3 S3-Standorten zuzugreifen, die bei Lake Formation registriert sind. Weitere Informationen finden Sie unter [Zusammenarbeit mit anderen AWS Diensten](#).

10. November 2022

[???](#)

Es wurden Informationen zur Behebung eines Fehlers bei der Verwendung von Amazon EMR für den Zugriff auf kontoübergreifende Daten hinzugefügt. Weitere Informationen finden Sie unter [Fehler bei der Verwendung von Amazon EMR für den Zugriff auf kontoübergreifende Daten](#).

7. November 2022

### [Aktualisierungen zur kontenübergreifenden Nutzung von Ressourcen](#)

Es wurde eine Beschreibung hinzugefügt, wie [kontenübergreifende Ressourcenfreigabe](#) in Lake Formation funktionieren. Die Änderung der [AWSLakeFormationCrossAccountManager](#) Richtlinie wurde dokumentiert.

6. Mai 2022

### [Neue Tutorials](#)

Es wurden neue Tutorials zum Erstellen verwalteter Tabellen, zum Sichern von Data Lakes und zum Teilen von Data Lakes hinzugefügt. Weitere Informationen finden Sie im Abschnitt [Erste Schritte](#).

20. April 2022

### [Neue Landingpage von Lake Formation](#)

Die Landingpage [von Lake Formation](#) wurde aktualisiert und enthält nun Links zu Tutorials mit step-by-step Anweisungen zum Erstellen eines Data Lakes, zum Ingestieren von Daten, zum Teilen und Sichern von Data Lakes mit Lake Formation.

20. April 2022

## [Support für den Verkauf von Anmeldeinformationen](#)

Es wurden Informationen zum Verkauf von Anmeldeinformationen hinzugefügt, das Lake Formation unterstützt, sodass Dienste von Drittanbietern mithilfe von API-Operationen für den Verkauf von Anmeldeinformationen in Lake Formation integriert werden können. Weitere Informationen finden Sie unter [So funktioniert der Verkauf von Anmeldeinformationen in Lake Formation](#).

28. Februar 2022

## [Support für verwaltete Tabellen und erweiterte Datenfilterung](#)

Es wurden Informationen zu kontrollierten Tabellen hinzugefügt, die ACID-Transaktionen, automatische Datenkomprimierung und Zeitreiseabfragen unterstützen. Es wurden Informationen zum Erstellen von Datenfiltern zur Unterstützung von Sicherheit auf Spaltenebene, Sicherheit auf Zeilenebene und Sicherheit auf Zeilenebene hinzugefügt. Weitere Informationen finden Sie unter [Verwaltete Tabellen in Lake Formation](#) und [Datenfilterung und Sicherheit auf Zeilenebene in Lake Formation](#).

30. November 2021

### Support für VPC-Schnittstellenendpunkte

Es wurden Informationen zur Erstellung eines VPC-Schnittstellenendpunkts (Virtual Private Cloud) für Lake Formation hinzugefügt, sodass die Kommunikation zwischen Ihrer VPC und Lake Formation vollständig und sicher innerhalb des AWS Netzwerks erfolgt. Weitere Informationen finden Sie unter [Verwenden von Lake Formation mit VPC-Endpunkten](#).

11. Oktober 2021

### Unterstützung für VPC-Endpunkttrichtlinien

Es wurden Informationen zur Unterstützung von Virtual Private Cloud (VPC)-Endpunkttrichtlinien in Lake Formation hinzugefügt. Weitere Informationen finden Sie unter [Verwenden von Lake Formation mit VPC-Endpunkten](#).

11. Oktober 2021

### Support für tagbasierte Zugriffskontrolle

Die tagbasierte Zugriffskontrolle von Lake Formation bietet eine neue, skalierbare Möglichkeit, den Zugriff auf Datenkatalogressourcen und die zugrunde liegenden Daten mithilfe von LF-Tags zu verwalten. Weitere Informationen finden Sie unter [Tag-Based Access Control von Lake Formation](#).

7. Mai 2021

[Neue Opt-in-Anforderung für die Datenfilterung auf Amazon EMR.](#)

Es wurden Informationen zur Anmeldepflicht hinzugefügt, damit Amazon EMR Daten filtern kann, die von Lake Formation verwaltet werden. Weitere Informationen finden Sie unter [Datenfilterung auf Amazon EMR zulassen.](#)

9. Oktober 2020

[Support für die Gewährung vollständiger kontoübergreifender Berechtigungen für Data Catalog-Datenbanken](#)

Es wurden Informationen zur AWS kontenübergreifenden Gewährung vollständiger Lake Formation Formation-Berechtigungen für Data Catalog-Datenbanken hinzugefügt, darunter CREATE\_TABLE . Weitere Informationen finden Sie unter [Gemeinsame Nutzung von Datenkatalogdatenbanken.](#)

1. Oktober 2020

[Support für Amazon Athena Benutzer, die sich über SAML authentifizieren.](#)

Es wurden Informationen zur Unterstützung für Athena-Benutzer hinzugefügt, die sich über den JDBC- oder ODBC-Treiber verbinden und sich über SAML-Identitätsanbieter wie Okta und Microsoft Active Directory Federation Service (AD FS) authentifizieren. Weitere Informationen finden Sie unter [AWS Serviceintegrationen mit Lake Formation.](#)

30. September 2020

[Support für kontoübergreifenden Zugriff mit einem verschlüsselten Datenkatalog](#)

Es wurden Informationen zur Gewährung kontoübergreifender Berechtigungen hinzugefügt, wenn der Datenkatalog verschlüsselt ist. Weitere Informationen finden Sie unter Voraussetzungen für den [kontoübergreifenden Zugriff](#).

30. Juli 2020

[Support für kontoübergreifenden Zugriff auf den Data Lake](#)

Es wurden Informationen zur Erteilung von AWS Lake Formation Berechtigungen für Datenkatalog-Datenbanken und -Tabellen für externe AWS Konten und Organisationen sowie zum Zugriff auf Datenkatalogobjekte hinzugefügt, die von externen Konten gemeinsam genutzt werden. Weitere Informationen finden Sie unter [Kontoübergreifender Zugriff](#).

7. Juli 2020



### Integration mit Amazon Quick

Es wurden Informationen darüber hinzugefügt, wie Benutzern der Quick Enterprise Edition Lake Formation-Formation-Berechtigungen erteilt werden können, damit sie auf Datensätze zugreifen können, die sich an registrierten Amazon S3 Standorten befinden. Weitere Informationen finden Sie unter [Erteilen von Datenkatalogberechtigungen](#).

29. Juni 2020

### Aktualisierungen der Kapitel „Einrichtung“ und „Erste Schritte“

Die Kapitel „Einrichtung“ und „Erste Schritte“ wurden neu organisiert und verbessert. Die empfohlenen AWS Identity and Access Management (IAM-) Berechtigungen für den Data Lake-Administrator wurden aktualisiert.

27. Februar 2020

## [Support für AWS Key Management Service](#)

Es wurden Informationen darüber hinzugefügt, wie die Unterstützung von Lake Formation für AWS Key Management Service (AWS KMS) die Einrichtung integrierter Dienste zum Lesen und Schreiben verschlüsselter Daten an registrierten Amazon Simple Storage Service (Amazon S3) -Standorten vereinfacht. Es wurden Informationen zur Registrierung von Amazon S3 S3-Standorten hinzugefügt, die mit verschlüsselt sind AWS KMS keys. Weitere Informationen finden Sie unter [the section called “Hinzufügen eines Amazon S3 S3-Standorts zu Ihrem Data Lake”](#).

27. Februar 2020

## [Aktualisierungen der Blueprints und der IAM-Richtlinien für Data Lake-Administratoren](#)

Die Eingabeparameter für inkrementelle Datenbank-Blueprints wurden geklärt. Die für einen Data Lake-Administrator erforderlichen IAM-Richtlinien wurden aktualisiert.

20. Dezember 2019

## [Überarbeitungen des Kapitels Sicherheit neu schreiben und aktualisieren](#)

Die Kapitel Sicherheit und Aktualisierung wurden verbessert.

29. Oktober 2019

[Die Super-Berechtigung ersetzt die Option Alle Berechtigungen](#)

Die Kapitel Sicherheit und Aktualisierung wurden aktualisiert, um der Ersetzung der Berechtigung durch Rechnung zu All stehenSuper.

10. Oktober 2019

[Ergänzungen, Korrekturen und Klarstellungen](#)

Auf der Grundlage von Rückmeldungen wurden Ergänzungen, Korrekturen und Klarstellungen vorgenommen. Das Sicherheitskapitel wurde überarbeitet. Die Kapitel Sicherheit und Aktualisierung wurden aktualisiert, um der Ersetzung der Gruppe Everyone durch Rechnung zu tragenIAMAllowe dPrincipals .

11. September 2019

[Neues Handbuch](#)

Dies ist die erste Version des AWS Lake Formation - Entwicklerhandbuchs.

8. August 2019

# AWS Glossar

Die neueste AWS Terminologie finden Sie im [AWS Glossar](#) in der AWS-Glossar Referenz.

Die vorliegende Übersetzung wurde maschinell erstellt. Im Falle eines Konflikts oder eines Widerspruchs zwischen dieser übersetzten Fassung und der englischen Fassung (einschließlich infolge von Verzögerungen bei der Übersetzung) ist die englische Fassung maßgeblich.