aws

Benutzerhandbuch

Amazon DataZone

Amazon DataZone: Benutzerhandbuch

Table of Contents

Was ist Amazon DataZone?

Amazon DataZone ist ein Datenverwaltungsservice, mit dem Sie Daten, die in lokalen und externen Quellen gespeichert sind, schneller und einfacher katalogisieren AWS, ermitteln, teilen und verwalten können. Mit Amazon können Administratoren DataZone, die die Datenbestände des Unternehmens überwachen, den Zugriff auf Daten mithilfe detaillierter Kontrollen verwalten und steuern. Diese Kontrollen tragen dazu bei, den Zugriff mit den richtigen Rechten und dem richtigen Kontext sicherzustellen. Amazon DataZone macht es Ingenieuren, Datenwissenschaftlern, Produktmanagern, Analysten und Geschäftsanwendern leicht, Daten im gesamten Unternehmen auszutauschen und darauf zuzugreifen, sodass sie Daten entdecken, nutzen und zusammenarbeiten können, um datengestützte Erkenntnisse zu gewinnen.

Amazon DataZone hilft Ihnen dabei, Daten direkt an Endbenutzer bereitzustellen, und vereinfacht Ihre Architektur durch die Integration von Datenverwaltungsdiensten wie Amazon Redshift, Amazon Athena, Amazon, AWS Glue QuickSight, AWS Lake Formation, lokale Quellen, Quellen von Drittanbietern und mehr.

Themen

Was kann ich mit Amazon machen DataZone?

Mit Amazon DataZone können Sie Folgendes tun:

- Steuern Sie den Datenzugriff über Unternehmensgrenzen hinweg. Mit Amazon können Sie sicherstellen DataZone, dass der richtige Benutzer gemäß den Sicherheitsbestimmungen Ihres Unternehmens für den richtigen Zweck auf die richtigen Daten zugreift, ohne sich auf individuelle Anmeldeinformationen verlassen zu müssen. Sie können auch Transparenz bei der Nutzung von Datenbeständen schaffen und Datenabonnements mit einem geregelten Arbeitsablauf genehmigen. Mithilfe von Funktionen zur Nutzungsprüfung können Sie Datenbestände auch projektübergreifend überwachen.
- Connect Datenarbeiter mithilfe gemeinsam genutzter Daten und Tools, um Geschäftseinblicke zu gewinnen. Mit Amazon können Sie die Effizienz Ihres Geschäftsteams steigern DataZone, indem Sie nahtlos teamübergreifend zusammenarbeiten und Self-Service-Zugriff auf Daten- und

Analysetools bereitstellen. Sie können Geschäftsbegriffe verwenden, um katalogisierte Daten zu suchen, zu teilen und darauf zuzugreifen AWS, die vor Ort oder bei Drittanbietern gespeichert sind. Und mithilfe der Amazon DataZone Business-Glossare können Sie mehr über die Daten erfahren, die Sie verwenden möchten.

- Automatisieren Sie die Datenermittlung und Katalogisierung mit maschinellem Lernen. Mit Amazon DataZone können Sie den Zeitaufwand für die manuelle Eingabe von Datenattributen in den Geschäftsdatenkatalog reduzieren. Umfangreichere Daten im Datenkatalog verbessern auch das Sucherlebnis.

Wie DataZone unterstützt und integriert Amazon andere AWS Dienste?

Amazon DataZone unterstützt drei Arten von Integrationen mit anderen AWS Diensten:

- Producer-Datenquellen — Sie können Datenbestände aus den in AWS Glue Data DataZone Catalog- und Amazon Redshift-Tabellen und -Ansichten gespeicherten Daten im Amazon-Katalog veröffentlichen. Sie können Objekte aus Amazon Simple Storage Service (S3) auch manuell im DataZone Amazon-Katalog veröffentlichen.
- Tools für Privatanwender — Sie können die Abfrage-Editoren von Amazon Athena oder Amazon Redshift verwenden, um auf Ihre Datenbestände zuzugreifen und diese zu analysieren.
- Zugriffskontrolle und Auftragsabwicklung — Amazon DataZone unterstützt die Gewährung des Zugriffs auf von AWS Lake Formation verwaltete AWS Glue-Tabellen und Amazon Redshift Redshift-Tabellen und -Ansichten. Für alle anderen Datenbestände DataZone veröffentlicht Amazon Standardereignisse im Zusammenhang mit Ihren Aktionen (z. B. die Genehmigung einer Abonnementanfrage) an Amazon EventBridge. Sie können diese Standardereignisse verwenden, um sie in andere AWS Dienste oder Lösungen von Drittanbietern für benutzerdefinierte Integrationen zu integrieren.

Wie kann ich auf Amazon zugreifen DataZone?

Sie können auf Amazon DataZone auf eine der folgenden Arten zugreifen:

- DataZone Amazon-Konsole

  Sie können die DataZone Amazon-Managementkonsole verwenden, um auf Ihre DataZone Amazon-Domains, -Blueprints und -Benutzer zuzugreifen und diese zu konfigurieren. Weitere

Informationen finden Sie unter https://console.aws.amazon.com/datazone. Die Amazon DataZone Management Console wird auch zur Erstellung des DataZone Amazon-Datenportals verwendet.

- DataZone Amazon-Datenportal

  Das DataZone Amazon-Datenportal ist eine browserbasierte Webanwendung, mit der Sie Daten im Self-Service-Modus katalogisieren, ermitteln, verwalten, teilen und analysieren können. Das Datenportal kann Sie mit den Anmeldeinformationen Ihres Identitätsanbieters über das AWS IAM Identity Center (Nachfolger von AWS SSO) oder mit Ihren IAM-Anmeldeinformationen authentifizieren. Sie können die URL des Datenportals abrufen, indem Sie auf die DataZone Amazon-Konsole unter https://console.aws.amazon.com/datazone zugreifen.

- DataZone Amazon-HTTPS-API

  Sie können DataZone programmgesteuert auf Amazon zugreifen, indem Sie die Amazon DataZone HTTPS-API verwenden, mit der Sie HTTPS-Anfragen direkt an den Service senden können. Weitere Informationen finden Sie in der Amazon DataZone API-Referenz.

DataZone Amazon-Terminologie und Konzepte

Wenn Sie mit Amazon beginnen DataZone, ist es wichtig, dass Sie die wichtigsten Konzepte, Terminologie und Komponenten verstehen.

Themen

DataZone Amazon-Komponenten

Amazon DataZone umfasst die folgenden vier Hauptkomponenten:

- Geschäftsdatenkatalog — Sie können diese Komponente verwenden, um Daten in Ihrem gesamten Unternehmen mit geschäftlichem Kontext zu katalogisieren und so jedem in Ihrem Unternehmen zu ermöglichen, Daten schnell zu finden und zu verstehen.
- Workflows veröffentlichen und abonnieren — Sie können diese automatisierten Workflows verwenden, um Daten zwischen Produzenten und Verbrauchern auf Self-Service-Weise zu schützen und sicherzustellen, dass jeder in Ihrem Unternehmen Zugriff auf die richtigen Daten für den richtigen Zweck hat.
- Projekte und Umgebungen
  - Bei DataZone Amazon-Projekten handelt es sich um auf geschäftliche Anwendungsfälle basierende Gruppierungen von Personen, Ressourcen (Daten) und Tools, die verwendet werden, um den Zugriff auf die Analysen zu vereinfachen. AWS Projekte bieten Bereiche, in denen Projektmitglieder zusammenarbeiten, Daten austauschen und Ressourcen gemeinsam nutzen können. Standardmäßig sind Projekte so konfiguriert, dass nur Personen, die dem Projekt explizit hinzugefügt wurden, auf die darin enthaltenen Daten- und Analysetools zugreifen können.

Projekte verwalten das Eigentum an Ressourcen, die gemäß den Projektrichtlinien erstellt wurden, damit Datennutzer darauf zugreifen können.

- Innerhalb von DataZone Amazon-Projekten sind Umgebungen Sammlungen von null oder mehr konfigurierten Ressourcen (z. B. einem Amazon S3-Bucket, einer AWS Glue Datenbank oder einer Amazon Athena Athena-Arbeitsgruppe), auf denen ein bestimmter Satz von IAM-Prinzipalen (z. B. Benutzer mit Mitwirkendenberechtigungen) arbeiten kann.

- Datenportal (außerhalb der AWS Management Console) — Dies ist eine browserbasierte Webanwendung, mit der verschiedene Benutzer Daten im Self-Service-Modus katalogisieren, ermitteln, verwalten, teilen und analysieren können. Das Datenportal authentifiziert Benutzer mit IAM-Anmeldeinformationen oder vorhandenen Anmeldeinformationen Ihres Identitätsanbieters über. AWS IAM Identity Center

Was sind DataZone Amazon-Domains?

Sie können DataZone Amazon-Domains verwenden, um Ihre Ressourcen, Benutzer und deren Projekte zu organisieren. Indem Sie zusätzliche AWS Konten mit Ihren DataZone Amazon-Domains verknüpfen, können Sie Ihre Datenquellen zusammenführen. Anschließend können Sie Inhalte aus diesen Datenquellen im Katalog Ihrer Domain veröffentlichen. Dabei stehen Metadatenformulare und Glossare zur Verbesserung der Vollständigkeit und Qualität der Metadaten zur Verfügung. Sie können diese Ressourcen auch durchsuchen, um zu sehen, welche Daten in der Domain veröffentlicht wurden. Darüber hinaus können Sie Projekten beitreten, um mit anderen Benutzern zusammenzuarbeiten, Ressourcen zu abonnieren und Projektumgebungen für den Zugriff auf Analysetools wie Amazon Athena und Amazon Redshift zu verwenden. DataZone Amazon-Domains bieten Ihnen die Flexibilität, die Daten- und Analyseanforderungen Ihrer Unternehmensstruktur zu berücksichtigen, unabhängig davon, ob Sie eine einzelne DataZone Amazon-Domain für Ihr Unternehmen oder mehrere DataZone Amazon-Domains für verschiedene Geschäftsbereiche erstellen.

Was sind DataZone Amazon-Projekte und -Umgebungen?

Amazon DataZone ermöglicht Teams und Analytics-Benutzern die Zusammenarbeit an Projekten, indem es anwendungsfallbasierte Gruppierungen von Teams, Tools und Daten erstellt.

- In Amazon DataZone ermöglichen Projekte einer Gruppe von Benutzern die Zusammenarbeit bei verschiedenen geschäftlichen Anwendungsfällen, bei denen Daten im DataZone Amazon-Katalog veröffentlicht, entdeckt, abonniert und genutzt werden. Die Projektmitglieder nutzen

Ressourcen aus dem DataZone Amazon-Katalog und erstellen mithilfe eines oder mehrerer analytischer Workflows neue Ressourcen. Projekte unterstützen die folgenden Aktivitäten innerhalb des Datenportals:

- Projekteigentümer können Mitglieder mit Inhaber- und Mitwirkendenberechtigungen hinzufügen
- Projektmitglieder können SSO-Benutzer, SSO-Gruppen und IAM-Benutzer sein
- Projektmitglieder können ein Abonnement für die Assets im Datenkatalog beantragen

  Für die Projekte werden Abonnementgenehmigungen erteilt

- In einem DataZone Amazon-Projekt sind Umgebungen Sammlungen von null oder mehr konfigurierten Ressourcen (z. B. ein Amazon S3, eine AWS Glue Datenbank oder eine Amazon Athena Athena-Arbeitsgruppe) mit einer bestimmten Gruppe von IAM-Prinzipalen, die mit diesen Ressourcen arbeiten können. Umgebungen werden mithilfe von Umgebungsprofilen erstellt. Dabei handelt es sich um vorkonfigurierte Gruppen von Ressourcen und Blueprints, die wiederverwendbare Vorlagen für die Erstellung von Umgebungen bereitstellen. Umgebungsprofile definieren Einstellungen wie die Region AWS-Konto oder die Region, in der Umgebungen bereitgestellt werden.

Was sind Amazon DataZone Blueprints?

Ein Blueprint, mit dem die Umgebung erstellt wird, definiert, AWS Glue welche AWS Tools und Dienste (z. B. Amazon Redshift) Mitglieder des Projekts, zu dem die Umgebung gehört, verwenden können, wenn sie mit Ressourcen im DataZone Amazon-Katalog arbeiten.

In der aktuellen Version von Amazon DataZone werden die folgenden Standard-Blueprints unterstützt:

Name des Blueprints	Beschreibung	Ressourcen wurden erstellt
Bauplan für Data Lake	Ermöglicht es den Mitgliede rn DataZone des Amazon-Pr ojekts, Data Lake-Dienste für Produzenten und Verbrauch er innerhalb der Umgebung zu starten.	Bietet Benutzern die Möglichkeit, Lake Formation-Tabellen mit Amazon Athena zu erstellen und abzufrage n. Amazon Athena Athena-Arbeitsgruppe, AWS Glue Datenbank mit Lake Formation Formation-Berechtigungen

Name des Blueprints	Beschreibung	Ressourcen wurden erstellt
	Als Verbraucher können DataZone Amazon-Projektmitglieder direkt in Amazon Athena und in anderen von Lake Formation unterstützten Abfrage-Engines auf eine schreibgeschützte Kopie der von Lake Formation verwalteten Assets zugreifen. Als Produzent ermöglicht es DataZone Amazon-Projektmitgliedern, mit Amazon Athena neue LakeFormation verwaltete Tabellen zu erstellen und diese im DataZone Amazon-Katalog zu veröffentlichen.	„nur lesen“, IAM-Berechtigungen „nur lesen“ und Zugriff auf Amazon S3, die vom Projekt verwaltet wird. AWS Glue Datenbank mit Lake Formation Formation-Berechtigungen „erstellen“ und „gewähren“, IAM-Berechtigungen „Lesen“ und „Schreiben“, AWS Glue ETL (Extrahieren, Transformieren und Laden) mit Tagging.

Name des Blueprints	Beschreibung	Ressourcen wurden erstellt
Bauplan für ein Data Warehouse	Als Verbraucher ermöglicht dieser Blueprint den Mitgliedern des DataZone Amazon-Projekts, eine Verbindung zu ihren eigenen Amazon Redshift-Clustern herzustellen, um Remote-Datenspeicher abzufragen und neue Datensätze zu erstellen und zu speichern. Als Produzent ermöglicht dieser Blueprint den Mitgliedern des DataZone Amazon-Projekts, sich mit ihren eigenen Amazon Redshift-Clustern zu verbinden, um Remote-Datenspeicher abzufragen, neue Datensätze zu erstellen und sie im Amazon-Katalog zu veröffentlichen. DataZone	Zugriff auf den Amazon Redshift Redshift-Abfrage-Editor, Lesezugriff auf die abonnierten Datenquellen aus dem DataZone Amazon-Katalog, die Möglichkeit, lokale Assets im konfigurierten Amazon Redshift-Cluster zu erstellen. Zugriff auf den Amazon Redshift Redshift-Abfrage-Editor, Lesezugriff auf die abonnierten Datenquellen aus dem DataZone Amazon-Katalog, die Möglichkeit, Assets aus dem konfigurierten Amazon Redshift-Cluster zu erstellen und zu veröffentlichen.

Name des Blueprints	Beschreibung	Ressourcen wurden erstellt
Amazon Sagemaker-Entwurf	Dieser Blueprint hilft Datenproduzenten und Verbrauchern dabei, nahtlos zu Amazon zu wechseln, SageMaker um an Projekten für maschinelles Lernen (ML) zusammenzuarbeiten und gleichzeitig die Zugriffss teuerung für Daten und ML-Assets durchzusetzen. Mit der neuen integrierten Integration zwischen Amazon DataZone und Amazon SageMaker können Datenkonsumenten und -produzenten die ML-Governance im gesamten Infrastrukturaufbau optimiere n, bei Geschäftsinitiativen zusammenarbeiten und Daten und ML-Assets einfach verwalten.	Sie können eine SageMaker Amazon-Domain erstellen, die Daten und ML-Assets in Amazon suchen, abonniere n und veröffentlichen kann DataZone. Kann auch AWS Glue-Datenbanken und Lake Formation wie konfiguriert abonnieren und veröffent lichen.

Was sind Amazon-Workflows für DataZone Inventar und Veröffentlichung?

Inventar-Assets für Projekte erstellen

Um Amazon für die Katalogisierung Ihrer Daten verwenden DataZone zu können, müssen Sie zunächst Ihre Daten (Assets) als Inventar Ihres Projekts in Amazon speichern DataZone. Wenn Sie ein Inventar für ein Projekt erstellen, sind die Ressourcen nur für die Mitglieder dieses Projekts auffindbar. Objekte aus dem Projektinventar stehen nicht allen Domänenbenutzern beim Suchen/Durchsuchen zur Verfügung, sofern sie nicht ausdrücklich veröffentlicht wurden. In der aktuellen

Version von Amazon DataZone können Sie dem Projektbestand auf folgende Weise Assets hinzufügen:

- Erstellen und betreiben Sie Datenquellen über das Datenportal oder mithilfe der DataZone Amazon-APIs. In der aktuellen Version von Amazon DataZone können Sie Datenquellen für AWS Glue und Amazon Redshift erstellen und ausführen. Durch das Erstellen und Ausführen von AWS Glue- oder Amazon Redshift Redshift-Datenquellen erstellen Sie Assets in einem ausgewählten Projektinventar und importieren deren technische Metadaten aus den Quelldatenbanktabellen oder Data Warehouses als Inventar in Amazon DataZone.
- Mithilfe von APIs können Sie Assets aus den verfügbaren System-Asset-Typen (AWS Glue, Amazon Redshift, Amazon S3 S3-Objekte) oder aus Ihren benutzerdefinierten Asset-Typen erstellen.
  - Erstellen Sie mithilfe der DataZone Amazon-APIs benutzerdefinierte Asset-Typen in einem Projektinventar. Zu den benutzerdefinierten Asset-Typen können ML-Modelle, Dashboards, lokale Tabellen usw. gehören.
  - Erstellen Sie mithilfe von DataZone Amazon-APIs Assets aus diesen benutzerdefinierten Asset-Typen.
- Erstellen Sie mithilfe des DataZone Amazon-Datenportals manuell Assets für S3-Objekte.

Kuratierung Ihrer Projektinventarressourcen — Nach der Erstellung eines Projektinventars können Dateneigentümer ihre Inventarressourcen mit den erforderlichen Geschäftsmetadaten kuratieren, indem sie Unternehmensnamen (Asset und Schema), Beschreibungen (Asset und Schema), Readme, Glossarbegriffe (Asset und Schema) und Metadatenformulare hinzufügen oder aktualisieren. Sie können dies über das Datenportal oder mithilfe der DataZone Amazon-APIs tun. Bei jeder Änderung an Ihrem Asset wird eine neue Inventarversion erstellt.

Veröffentlichen von Objekten aus dem Projektbestand im DataZone Amazon-Katalog

Der nächste Schritt bei der Verwendung von Amazon DataZone zur Katalogisierung Ihrer Daten besteht darin, die Inventarressourcen Ihres Projekts für die Domain-Benutzer auffindbar zu machen. Sie können dies tun, indem Sie die Inventarressourcen im DataZone Amazon-Katalog veröffentlichen. Nur die neueste Version des Inventarbestands kann im Katalog veröffentlicht werden, und nur die zuletzt veröffentlichte Version ist im Discovery-Katalog aktiv. Wenn ein Inventar-Asset aktualisiert wird, nachdem es im DataZone Amazon-Katalog veröffentlicht wurde, müssen Sie es explizit erneut veröffentlichen, damit die neueste Version im Discovery-Katalog angezeigt wird. In der aktuellen

Version von Amazon DataZone können Sie Ihre Projektinventar-Assets auf folgende Weise im DataZone Amazon-Katalog veröffentlichen:

- Veröffentlichen Sie Ihre Projektinventarressourcen manuell im DataZone Amazon-Katalog, entweder über das Datenportal oder mithilfe der DataZone Amazon-APIs.
- Aktivieren Sie im Rahmen der Erstellung oder Bearbeitung von Datenquellen die optionalen Einstellungen Veröffentlichen Sie Ihre AWS Glue-Ressourcen im Katalog oder Veröffentlichen Sie Ihre Amazon Redshift Redshift-Assets im Katalog, um sie während der geplanten oder automatisierten Datenquellenläufe zu verwenden. Wenn diese Einstellung aktiviert ist, fügt ein Datenquellenlauf Assets zum Inventar Ihres Projekts hinzu und veröffentlicht die Inventar-Assets anschließend auch im DataZone Amazon-Katalog. Beachten Sie, dass die Assets, wenn Sie direkt veröffentlichen, möglicherweise keine Geschäftsmetadaten enthalten und für alle Domain-Benutzer direkt auffindbar sind. Sie können diese Einstellung für Ihre Datenquellen entweder über das Datenportal oder mithilfe der DataZone Amazon-APIs verwenden.

Was sind DataZone Amazon-Abonnement- und Fulfillment-Workflows?

Sobald Ihre Ressourcen im DataZone Amazon-Katalog veröffentlicht wurden, können Ihre Domain-Benutzer diese Ressourcen finden, diese Ressourcen anfordern und darauf zugreifen und Amazon weiterhin verwenden, um diese Ressourcen DataZone zu verwalten, zu teilen und zu analysieren.

Benutzer beantragen Zugriff auf ein Asset, indem sie dieses Asset im Namen eines Projekts abonnieren. Sobald eine Abonnementanfrage erstellt wurde, erhalten die Eigentümer des Assets eine Benachrichtigung. Sie können die Abonnementanfrage überprüfen und entscheiden, ob sie sie genehmigen oder ablehnen möchten. Wenn die Abonnementanfrage vom Dateneigentümer genehmigt wird, erhält das abonnierende Projekt Zugriff auf dieses Asset.

Sobald eine Abonnementanfrage genehmigt wurde, DataZone startet Amazon einen Workflow zur Abonnementabwicklung, der das Asset automatisch allen entsprechenden Umgebungen innerhalb des Projekts hinzufügt, indem die erforderlichen Zuschüsse in AWS Lake Formation oder Amazon Redshift erstellt werden. Dadurch können die abonnierten Projektmitglieder das Asset mit einem der Abfragetools (Amazon Athena oder Amazon Redshift Query Editor) in ihren Umgebungen abfragen.

Amazon DataZone kann diese automatisierte Fulfillment-Logik nur für verwaltete Assets auslösen (dazu gehören AWS Glue-Tabellen und Amazon Redshift Redshift-Tabellen und -Ansichten). Für alle anderen Asset-Typen (nicht verwaltete Anlagen) DataZone kann Amazon den

Versand nicht automatisch auslösen, sondern veröffentlicht stattdessen ein Ereignis in Amazon Eventbridge mit allen erforderlichen Details in der Event-Payload, sodass Sie die erforderlichen Zuschüsse außerhalb von Amazon erstellen können. DataZone Amazon stellt DataZone auch die `updateSubscriptionStatus` API bereit, mit der Sie den Status des Abonnements aktualisieren können, sobald es außerhalb von Amazon abgewickelt wurde, DataZone sodass Amazon die Projektmitglieder darüber informieren DataZone kann, dass sie mit der Nutzung des Assets beginnen können.

Die Benutzerpersönlichkeiten von Amazon DataZone

Im Folgenden sind die wichtigsten DataZone Amazon-Benutzerrollen aufgeführt:

- Domain-Administratoren, die selbst Amazon DataZone als Analyseplattform für ihr Unternehmen einrichten.

  Im Kontext von Amazon DataZone installieren Domain-Administratoren Amazon DataZone in AWS Konten, erstellen DataZone Amazon-Domains und konfigurieren AWS Kontozuordnungen und Identitätsanbieter-Verknüpfungen mit DataZone Amazon-Domains. Domain-Administratoren verwenden auch andere AWS Servicekonsolen wie AWS Organization und Service Catalog, um Amazon zu konfigurieren DataZone.
- Datennutzer, die die Hauptnutzer von Amazon DataZone (Asset-Publisher und Abonnenten) für ihre Analyse- und Machine-Learning-Aufgaben sind.

  Zu den Datennutzern gehören Datenanalytiker, Datenwissenschaftler und Systembenutzer, die Datenbestände erstellen und nutzen. Im Kontext von Amazon erstellen DataZone Datennutzer Projekte und Umgebungen und schließen sich ihnen an, abonnieren und nutzen Datenbestände mit vorkonfigurierten Tools für Analyse oder maschinelles Lernen und veröffentlichen Ausgabedatenbestände zurück im DataZone Amazon-Domain-Katalog, um sie mit anderen zu teilen.
- Systementwickler, die benutzerdefinierte Infrastrukturvorlagen erstellen und Amazon DataZone in interne Kataloge oder Produktionssysteme integrieren.

  Im Kontext von Amazon DataZone erstellen Systementwickler als Environment-Provider Umgebungs-Blueprints (Infrastrukturvorlagen) oder Infrastructure-As-Code CI/CD-Pipeline, Daten-Pipelines zur umgebungsübergreifenden Förderung von Datenbeständen, Katalogsynchronisations- und Abonnement-Grant-Fulfillment-Adapter zur Integration mit internen Katalogen oder Integrationen zwischen DataZone Amazon-APIs und internen Benutzeroberflächen oder Produktionssystemen, falls erforderlich.

- Datenschutzbeauftragte, die für die Definitionen und Risiken der organisatorischen Sicherheits-, Datenschutz- und anderer Compliance-Richtlinien verantwortlich sind und sicherstellen, dass die Nutzung von Amazon DataZone in ihren Organisationen diesen Definitionen entspricht.

DataZone Amazon-Terminologie

Domain

Eine DataZone Amazon-Domain ist die organisierende Einheit, die Ihre Ressourcen, Benutzer und deren Projekte miteinander verbindet. Mit DataZone Amazon-Domains haben Sie die Flexibilität, die Daten- und Analyseanforderungen Ihrer Unternehmensstruktur zu berücksichtigen, unabhängig davon, ob Sie eine einzelne DataZone Amazon-Domain für Ihr Unternehmen oder mehrere Datenzonen, Domains für verschiedene Geschäftsbereiche oder Teams erstellen.

Zugeordnetes Konto

Wenn Sie Ihre AWS Konten mit DataZone Amazon-Domains verknüpfen, können Sie Daten aus diesen AWS Konten im DataZone Amazon-Katalog veröffentlichen und DataZone Amazon-Projekte erstellen, um mit Ihren Daten über mehrere AWS Konten hinweg zu arbeiten. Kontozuordnungsanfragen können nur für AWS Konten gestellt werden, die eine DataZone Amazon-Domain besitzen. Anfragen zur Kontozuweisung können nur von den administrativen Benutzern der eingeladenen AWS Konten akzeptiert werden. Sobald ein AWS Konto mit einer DataZone Amazon-Domain verknüpft ist, können Sie Ihre Datenquellen wie AWS Glue Catalog und Amazon Redshift in diesem Konto für diese Domain registrieren. Durch die Verknüpfung kann ein AWS Konto auch DataZone Amazon-Projekte und -Umgebungen erstellen.

Ein AWS-Konto kann mit einer oder mehreren DataZone Amazon-Domains verknüpft werden.

Datenquelle

In Amazon können Sie Datenquellen verwenden DataZone, um technische Metadaten von Assets (Daten) aus den Quelldatenbanken oder Data Warehouses in Amazon zu importieren DataZone. In der aktuellen Version von Amazon DataZone können Sie Datenquellen für AWS Glue und Amazon Redshift erstellen und ausführen. Durch das Erstellen einer Datenquelle stellen Sie eine Verbindung zwischen Amazon DataZone und der Quelle (AWS Glue Data Catalog oder Amazon Redshift Warehouse) her, sodass Sie technische Metadaten lesen können, einschließlich Tabellennamen, Spaltennamen und Datentypen. Durch das Erstellen einer Datenquelle starten Sie auch den ersten Datenquellenlauf, der neue Assets in Amazon erstellt oder bestehende aktualisiert DataZone. Während der Erstellung einer Datenquelle oder nachdem

die Datenquelle erfolgreich erstellt wurde, haben Sie auch die Möglichkeit, einen Zeitplan für Ihre Datenquellenläufe festzulegen.

Ausführung der Datenquelle

In Amazon DataZone ist ein Datenquellenlauf eine Aufgabe, die Amazon DataZone ausführt, um Assets in Projektinventaren zu erstellen und optional auch Projektinventar-Assets im DataZone Amazon-Katalog zu veröffentlichen. Datenquellenläufe können automatisiert (bei der ersten Erstellung einer Datenquelle gestartet), geplant oder manuell ausgeführt werden. Mit den Datenauswahlkriterien können Sie die vorhandenen und future Datensätze, die in Projektinventare oder den DataZone Amazon-Katalog aufgenommen werden sollen, sowie die Häufigkeit der Metadaten-Aktualisierungen für diese Inventar- oder Katalog-Assets optimieren.

Ziel des Abonnements

In Amazon DataZone ermöglichen Ihnen Abonnementziele den Zugriff auf die Daten, die Sie in Ihren Projekten abonniert haben. Ein Abonnementziel gibt den Speicherort (z. B. eine Datenbank oder ein Schema) und die erforderlichen Berechtigungen (z. B. eine IAM-Rolle) an, die Amazon verwenden DataZone kann, um eine Verbindung mit den Quelldaten herzustellen und die erforderlichen Zuschüsse zu erstellen, sodass Mitglieder des DataZone Amazon-Projekts mit der Abfrage der Daten beginnen können, die sie abonniert haben.

Abonnement-Anfrage

Bei Amazon DataZone ist eine Abonnementanfrage ein Prozess, dem ein DataZone Amazon-Projekt folgen muss, um Zugriff auf ein bestimmtes Asset zu erhalten. Abonnementanfragen können genehmigt, abgelehnt, widerrufen oder gewährt werden.

Komponente

In Amazon DataZone ist ein Asset eine Entität, die ein einzelnes physisches Datenobjekt (z. B. eine Tabelle, ein Dashboard, eine Datei) oder ein virtuelles Datenobjekt (z. B. eine Ansicht) darstellt.

Asset type (Objekttyp)

Asset-Typen definieren, wie Vermögenswerte im DataZone Amazon-Katalog dargestellt werden. Ein Asset-Typ definiert das Schema für einen bestimmten Asset-Typ. Wenn Assets erstellt werden, werden sie anhand des Schemas validiert, das durch ihren Asset-Typ (standardmäßig die neueste Version) definiert ist. Wenn ein Asset-Update stattfindet, DataZone erstellt Amazon eine neue Asset-Version und ermöglicht es DataZone Amazon-Benutzern, mit allen Asset-Versionen zu arbeiten.

Glossar für Unternehmen

Bei Amazon DataZone ist ein Geschäftsglossar eine Sammlung von Geschäftsbegriffen, die mit Vermögenswerten in Verbindung gebracht werden können. Ein Geschäftsglossar trägt dazu bei, dass im gesamten Unternehmen bei den verschiedenen Datenanalyseaufgaben dieselben Begriffe und Definitionen verwendet werden.

Die Begriffe in einem Geschäftsglossar können zu Assets und Spalten hinzugefügt werden, um diese Attribute bei der Suche zu klassifizieren oder ihre Identifizierung zu verbessern. Glossar kann als Wertetyp für ein Feld in einem Metadatenformular ausgewählt werden, das einem Asset zugeordnet ist. Wenn ein bestimmter Begriff als Wert für das Metadaten-Formularfeld eines Assets ausgewählt wird, können Benutzer nach dem Begriff im Unternehmensglossar suchen und die zugehörigen Ressourcen finden.

Typ des Metadaten-Formulars

Ein Metadaten-Formulartyp ist eine Vorlage, die die Metadaten definiert, die gesammelt und gespeichert werden, wenn Assets als Inventar erstellt oder in einer DataZone Amazon-Domain veröffentlicht werden. Metadaten-Formulartypen können einem Datenobjekt zugeordnet werden. Mithilfe von Metadaten-Formulartypen können Domänenadministratoren Metadatenformulare definieren, die für diese Domain benötigt werden, z. B. Compliance-Informationen, regulatorische Informationen oder Klassifizierungen. Es ermöglicht Domainadministratoren, zusätzliche Metadaten für ihre Ressourcen anzupassen. Amazon DataZone verfügt über Formulartypen für Systemmetadaten wie asset-common-details-form -type, column-business-metadata-form -type, glue-table-form-type, glue-view-form-type, redshift-table-form-type, redshift-view-form-type, s3-object-collection-form-type subscription-terms-form-type, und. suggestion-form-type

Formular für Metadaten

In Amazon DataZone definieren Metadatenformulare die Metadaten, die gesammelt und gespeichert werden, wenn Assets als Inventar erstellt oder in einer DataZone Amazon-Domain veröffentlicht werden. Metadaten-Formulardefinitionen werden in der Katalogdomäne von einem Domain-Administrator erstellt. Eine Metadaten-Formulardefinition besteht aus einer oder mehreren Felddefinitionen und unterstützt die Datentypen Boolean, Date, Decimal, Integer, String und Business Glossary.

Ein Domainadministrator wendet ein Metadatenformular auf Assets in seiner Domain an, indem er das Metadatenformular zu seiner Domain hinzufügt. Asset-Publisher geben dann alle optionalen und erforderlichen Feldwerte im Metadatenformular an.

Projekt

In Amazon DataZone ermöglichen Projekte einer Gruppe von Benutzern die Zusammenarbeit bei verschiedenen geschäftlichen Anwendungsfällen, bei denen es darum geht, Ressourcen in Projektinventaren zu erstellen und sie so für alle Projektmitglieder auffindbar zu machen und dann Ressourcen im Amazon-Katalog zu veröffentlichen, zu entdecken, zu abonnieren und zu konsumieren. DataZone Die Projektmitglieder nutzen Ressourcen aus dem DataZone Amazon-Katalog und erstellen mithilfe eines oder mehrerer analytischer Workflows neue Ressourcen. Projektmitglieder können Eigentümer oder Mitwirkende sein. Projektinhaber können andere Benutzer als Eigentümer oder Mitwirkende hinzufügen oder entfernen und Projekte ändern oder löschen. Andere Einschränkungen für Mitwirkende können mit Richtlinien definiert werden. Wenn ein Benutzer ein Projekt erstellt, wird er der erste Eigentümer dieses Projekts.

Umgebung

Eine Umgebung ist eine Sammlung konfigurierter Ressourcen (z. B. ein Amazon S3 S3-Bucket, eine AWS Glue Datenbank oder eine Amazon Athena Athena-Arbeitsgruppe) mit einer bestimmten Gruppe von IAM-Prinzipalen (mit zugewiesenen Mitwirkendenberechtigungen), die mit diesen Ressourcen arbeiten können. Jede Umgebung kann auch Benutzerprinzipale haben, die berechtigt sind, auf die Ressourcen zuzugreifen und per Abonnement und Versand Zugriff auf Daten zu erhalten. Umgebungen sind so konzipiert, dass sie verwertbare Links zu AWS Diensten und externen IDEs und Konsolen speichern. Mitglieder des Projekts können über Deep-Links, die in einer Umgebung konfiguriert sind, auf Dienste wie die Amazon Athena Athena-Konsole und mehr zugreifen. SSO- und IAM-Benutzer aus dem Projekt können weiter auf die Nutzung/den Zugriff auf bestimmte Umgebungen beschränkt werden.

Profil der Umgebung

In Amazon DataZone ist ein Umgebungsprofil eine Vorlage, mit der Sie Umgebungen erstellen können. Umgebungsprofile werden mithilfe von Blueprints erstellt.

Mithilfe von Umgebungsprofilen können Domänenadministratoren Blueprints mit vorkonfigurierten Parametern verpacken. Anschließend können Datenarbeiter schnell eine beliebige Anzahl neuer Umgebungen erstellen, indem sie vorhandene Umgebungsprofile auswählen und Namen für die neuen Umgebungen angeben. Auf diese Weise können Datenarbeiter ihre Projekte und Umgebungen effizient verwalten und gleichzeitig sicherstellen, dass sie die von ihren Domänenadministratoren durchgesetzten Datenverwaltungsrichtlinien einhalten.

Blueprint

Ein Blueprint, mit dem die Umgebung erstellt wird, definiert, AWS Glue welche AWS Tools und Dienste (z. B. Amazon Redshift) Mitglieder des Projekts, zu dem die Umgebung gehört, verwenden können, wenn sie mit Ressourcen im DataZone Amazon-Katalog arbeiten.

In der aktuellen Version von Amazon werden DataZone die folgenden Standard-Blueprints unterstützt:

- Data-Lake-Blueprint
- Bauplan für ein Data Warehouse
- Amazon Sagemaker-Entwurf

Benutzerprofil

Ein Benutzerprofil steht für DataZone Amazon-Benutzer. Amazon DataZone unterstützt sowohl IAM-Rollen als auch SSO-Identitäten, um mit der Amazon DataZone Management Console und dem Datenportal für verschiedene Zwecke zu interagieren. Domain-Administratoren verwenden IAM-Rollen, um die ersten administrativen Aufgaben im Zusammenhang mit der Domain in der Amazon DataZone Management Console auszuführen, einschließlich der Erstellung neuer DataZone Amazon-Domains, der Konfiguration von Metadaten-Formulartypen und der Implementierung von Richtlinien. Datenarbeiter verwenden ihre SSO-Unternehmensidentitäten über Identity Center, um sich beim Amazon DataZone Data Portal anzumelden und auf Projekte zuzugreifen, bei denen sie Mitglied sind.

Profil der Gruppe

Gruppenprofile stellen Gruppen von DataZone Amazon-Benutzern dar. Gruppen können manuell erstellt oder Active Directory-Gruppen von Unternehmenskunden zugeordnet werden. Bei Amazon DataZone dienen Gruppen zwei Zwecken. Erstens kann eine Gruppe einem Team von Benutzern im Organigramm zugeordnet werden und so den Verwaltungsaufwand eines DataZone Amazon-Projektinhabers reduzieren, wenn neue Mitarbeiter einem Team beitreten oder es verlassen. Zweitens verwenden Unternehmensadministratoren Active Directory-Gruppen, um Benutzerstatus zu verwalten und zu aktualisieren, sodass DataZone Amazon-Domain-Administratoren diese Gruppenmitgliedschaften verwenden können, um DataZone Amazon-Domain-Richtlinien zu implementieren.

Domain-Administrator

In Amazon DataZone ist ein IAM-Principal, der eine DataZone Amazon-Domain erstellt, der Standard-Domain-Administrator dieser Domain. Domain-Administratoren bei Amazon

DataZone führen wichtige Funktionen für die Domain aus, darunter das Erstellen von Domains, das Zuweisen anderer Domain-Administratoren, das Hinzufügen von Datenquellen und Abonnementzielen, das Erstellen von Projekten und Umgebungen sowie das Zuweisen von Projektinhabern.

Herausgeber

In Amazon DataZone veröffentlichen Verlage Assets im DataZone Amazon-Katalog und können die Metadaten der von ihnen veröffentlichten Assets bearbeiten. Wenn Verlage diese Befugnis erhalten, können sie Abonnementanfragen für die Inhalte, die sie im DataZone Amazon-Katalog veröffentlicht haben, genehmigen oder ablehnen.

Subscriber

Bei Amazon DataZone ist ein Abonnent ein DataZone Amazon-Projekt, das nach Ressourcen im DataZone Amazon-Katalog suchen, darauf zugreifen und sie nutzen möchte.

AWS-Konto owner

In Amazon DataZone erstellen AWS-Konto Eigentümer in ihren eigenen Rollen, Richtlinien und Berechtigungen, AWS-Konten die es ermöglichen, diese mit DataZone Amazon-Domains AWS-Konten zu verknüpfen.

Was ist neu bei Amazon DataZone?

In diesem Abschnitt werden neue Funktionen und Verbesserungen in Amazon DataZone nach Veröffentlichungsdatum sortiert beschrieben.

Themen

2024

Amazon DataZone startet die Integration mit Amazon SageMaker

Veröffentlicht am 05.06.2024

Amazon DataZone führt die Integration mit Amazon ein SageMaker, um Datenproduzenten und Verbrauchern zu helfen, nahtlos zu Amazon zu wechseln SageMaker , um an Projekten für maschinelles Lernen (ML) zusammenzuarbeiten und gleichzeitig die Zugriffssteuerung für Daten und ML-Assets durchzusetzen. Mit der neuen integrierten Integration zwischen Amazon DataZone und Amazon SageMaker können Datenkonsumenten und -produzenten die ML-Governance im gesamten Infrastrukturaufbau optimieren, bei Geschäftsinitiativen zusammenarbeiten und Daten und ML-Assets einfach verwalten. Weitere Informationen finden Sie unter Arbeiten mit den DataZone integrierten Blueprints von Amazon und Mit verknüpften Konten arbeiten, um Daten zu veröffentlichen und zu nutzen.

Amazon DataZone startet die Integration mit dem hybriden Zugriffsmodus von AWS Lake Formation

Veröffentlicht am 04.03.2024

Amazon DataZone hat eine Integration mit dem Hybridzugriffsmodus von AWS Lake Formation eingeführt. Diese Integration ermöglicht es Ihnen, Ihre AWS Glue-Tabellen einfach über Amazon zu veröffentlichen und zu teilen DataZone, ohne sie zuerst in AWS Lake Formation registrieren zu müssen. Zunächst aktivieren Administratoren die Einstellung für die Registrierung des Datenstandorts unter dem `DefaultDataLake` Blueprint in der DataZone Amazon-Konsole. Wenn dann ein Datenverbraucher eine AWS Glue-Tabelle abonniert, die über IAM-Berechtigungen verwaltet wird,

registriert Amazon DataZone zunächst die Amazon S3 S3-Standorte dieser Tabelle im Hybridmodus und gewährt dann dem Datenverbraucher Zugriff, indem die Berechtigungen für die Tabelle über AWS Lake Formation verwaltet werden. Dadurch wird sichergestellt, dass die IAM-Berechtigungen für die Tabelle auch mit den neu erteilten AWS Lake Formation Formation-Berechtigungen bestehen bleiben, ohne bestehende Workflows zu stören. Weitere Informationen hierzu finden Sie unter DataZone Amazon-Integration mit dem AWS Lake Formation Formation-Hybridmodus .

Amazon DataZone startet die Integration mit AWS Glue Data Quality

Veröffentlicht am 04.03.2024

Amazon DataZone startet die Integration mit AWS Glue Data Quality und bietet APIs zur Integration von Datenqualitätsmetriken aus Datenqualitätslösungen von Drittanbietern. Die neue Integration ermöglicht es Ihnen, AWS Glue Data Quality Scores automatisch im DataZone Amazon-Geschäftsdatenkatalog zu veröffentlichen. DataZone Amazon-APIs können verwendet werden, um Qualitätskennzahlen aus Quellen von Drittanbietern aufzunehmen. Nach der Veröffentlichung können Datennutzer einfach nach Datenbeständen suchen, detaillierte Qualitätskennzahlen einsehen und fehlgeschlagene Prüfungen und Regeln identifizieren, was wiederum Geschäftsentscheidungen erleichtert. Weitere Informationen hierzu finden Sie unter Datenqualität bei Amazon DataZone.

Veröffentlichung der KI-Empfehlungen für Beschreibungen in Amazon zur allgemeinen Verfügbarkeit DataZone

Veröffentlicht am 27.03.2024

Amazon DataZone kündigte die allgemeine Verfügbarkeit der neuen generativen KI-basierten Funktion zur Verbesserung der Datenerkennung, des Datenverständnisses und der Datennutzung durch die Erweiterung des Geschäftsdatenkatalogs an. Mit einem einzigen Klick können Datenproduzenten umfassende Beschreibungen und den Kontext von Geschäftsdaten generieren, aussagekräftige Spalten hervorheben und Empfehlungen zu analytischen Anwendungsfällen geben. Die Markteinführung bietet Unterstützung für APIs, mit denen Datenproduzenten programmgesteuert Beschreibungen für Ressourcen generieren können. Weitere Informationen finden Sie unter Einsatz von maschinellem Lernen und generativer KI.

Amazon DataZone führt Verbesserungen der Amazon Redshift Redshift-Integration ein

Veröffentlicht am 21.03.2024

Amazon DataZone hat mehrere Verbesserungen an seiner Amazon Redshift Redshift-Integration eingeführt, die das Veröffentlichen und Abonnieren von Amazon Redshift Redshift-Tabellen und -Ansichten vereinfachen. Diese Updates optimieren die Erfahrung sowohl für Datenproduzenten als auch für Verbraucher und ermöglichen es ihnen, schnell Data Warehouse-Umgebungen mit vorkonfigurierten Anmeldeinformationen und Verbindungsparametern zu erstellen, die von ihren DataZone Amazon-Administratoren bereitgestellt werden. Darüber hinaus gewähren diese Verbesserungen Administratoren mehr Kontrolle darüber, wer die Ressourcen in ihren AWS Konten und Amazon Redshift Redshift-Clustern nutzen kann und zu welchem Zweck.

- Blueprint-Konfiguration: Sobald Sie den `DefaultDataWarehouseBlueprint` Blueprint aktiviert haben, können Sie steuern, welche Projekte den `DefaultDataWarehouseBlueprint` Blueprint in Ihrem Konto verwenden können, um Umgebungsprofile zu erstellen, indem Sie dem aktivierten Blueprint die Verwaltung von Projekten zuweisen. Sie können darüber hinaus auch Parametersätze erstellen, `DefaultDataWarehouseBlueprint` indem Sie Parameter wie Cluster, Datenbank und einen geheimen Schlüssel angeben. AWS Sie können AWS Secrets auch von der DataZone Amazon-Konsole aus erstellen.
- Umgebungsprofil: Wenn Sie ein Umgebungsprofil erstellen, können Sie wählen, ob Sie Ihre eigenen Amazon Redshift Redshift-Parameter angeben oder einen der Parametersätze aus der Blueprint-Konfiguration verwenden möchten. Wenn Sie sich dafür entscheiden, den in der Blueprint-Konfiguration erstellten Parametersatz zu verwenden, ist für das AWS Geheimnis nur ein `AmazonDataZoneDomain` Tag erforderlich (das `AmazonDataZoneProject` Tag ist nur erforderlich, wenn Sie Ihre eigenen Parametersätze im Umgebungsprofil angeben). Im Umgebungsprofil können Sie eine Liste autorisierter Projekte angeben. Nur autorisierte Projekte können dieses Umgebungsprofil verwenden, um Data Warehouse-Umgebungen zu erstellen. Sie können auch angeben, welche Daten autorisierte Projekte veröffentlichen dürfen. Derzeit können Sie eine der folgenden Optionen wählen: 1) Aus einem beliebigen Schema veröffentlichen, 2) Aus dem Standardumgebungsschema veröffentlichen, 3) Veröffentlichung nicht zulassen.
- Umgebung: Datenproduzenten oder Verbraucher können jetzt ein Umgebungsprofil auswählen, um Umgebungen zu erstellen, ohne ihre eigenen Amazon Redshift Redshift-Parameter wie AWS Secret, Cluster, Arbeitsgruppe und Datenbank angeben zu müssen. Diese Parameter werden aus dem Umgebungsprofil in die Umgebung portiert. Neben der Erstellung der Umgebung erstellt Amazon DataZone jetzt auch ein Standardschema für die Umgebung. Mitglieder des Projekts haben Lese- und Schreibzugriff auf dieses Schema und können alle in diesem Schema erstellten Tabellen problemlos im Katalog veröffentlichen, indem sie die Standarddatenquelle ausführen, die im Rahmen der Umgebungserstellung erstellt wurde. Amazon Redshift Redshift-Parameter, die zur Erstellung der Umgebung verwendet werden, können auch zum Erstellen neuer Datenquellen

verwendet werden (anstelle von Data Producer, der bei der Erstellung der Datenquelle eigene Parameter bereitstellt).

AWS Cloud Formation-Unterstützung für Amazon DataZone

Veröffentlicht am 18.01.2024

Nutzer von Amazon DataZone können nun eine AWS CloudFormation Suite von DataZone Amazon-Ressourcen effektiv modellieren und verwalten. Dieser Ansatz ermöglicht die konsistente Bereitstellung von Ressourcen und ermöglicht gleichzeitig das Lebenszyklusmanagement mithilfe von Infrastructure-as-Code-Praktiken. Mit benutzerdefinierten Vorlagen können Sie Ihre benötigten Ressourcen und deren Interdependenzen genau definieren. Weitere Informationen finden Sie in der Referenz zum DataZone Amazon-Ressourcentyp.

Fügen Sie IAM-Prinzipale direkt als Mitglieder von Amazon-Projekten hinzu DataZone

Veröffentlicht am 01.05.2024

Sie können jetzt IAM-Prinzipale als Projektmitglieder hinzufügen, auch wenn sich diese IAM-Prinzipale noch nicht bei Amazon angemeldet haben DataZone (vorherige Anforderung). Nachdem ein Domainadministrator oder IT-Administrator die Domain-Ausführungsrolle der Domain hinzugefügt `iam:GetUser` hat, können Projekteigentümer IAM-Prinzipale als Mitglieder hinzufügen, indem sie einfach den Amazon Resource Name (ARN) der IAM-Rolle oder des IAM-Benutzers angeben. `iam:GetRole` Der IAM-Principal muss weiterhin über die IAM-Berechtigungen verfügen, die für den Zugriff auf Amazon DataZone erforderlich sind. Diese können in der IAM-Konsole konfiguriert werden. Weitere Informationen finden Sie unter Füge Mitglieder zu einem Projekt hinzu.

Support für benutzerdefinierte Asset-Typen aus dem Datenportal

Veröffentlicht am 01.05.2024

Die Unterstützung für benutzerdefinierte Ressourcen ermöglicht es Amazon DataZone , Assets über das Datenportal für unstrukturierte Daten, einschließlich Dashboards, Abfragen und Modelle, zu katalogisieren, sodass Sie benutzerdefinierte Assets zusammen mit der zuvor verfügbaren API-Unterstützung leichter direkt im Datenportal hinzufügen können. Die Möglichkeit, benutzerdefinierte Ressourcen in Amazon zu erstellen, zu aktualisieren und zu veröffentlichen DataZone, ermöglicht es Ihnen, jede Art von Asset zu teilen, zu finden und zu abonnieren und einen Geschäftsablauf zu

erstellen, der die Verwaltung dieser Ressourcen gewährleistet. Weitere Informationen finden Sie unter Erstellen Sie benutzerdefinierte Asset-Typen.

2023

Domain löschen

Veröffentlicht am 27.12.2023

Mit dieser Funktion können Sie Ihre Domains einfacher löschen. Jetzt können Sie mit dem Löschen von Domains fortfahren, auch wenn sie nicht leer ist (d. h. sie enthält Projekte, Umgebungen, Ressourcen, Datenquellen usw.). Weitere Informationen finden Sie unter Domains löschen.

Hybrider Modus

Veröffentlicht am 22.12.2023

Amazon DataZone hat Unterstützung für den AWS Lake Formation Formation-Hybridmodus hinzugefügt. Wenn Sie mit dieser Unterstützung eine AWS Glue-Tabelle auf Amazon DataZone veröffentlichen, deren AWS S3-Standort in Lake Formation im Hybridmodus registriert ist, DataZone behandelt Amazon diese Tabelle als verwaltetes Asset und kann die Abonnementzuschüsse für diese Tabelle verwalten. Vor dieser Feature-Version DataZone behandelte Amazon diese Tabelle als nicht verwaltetes Asset, d. DataZone h. Amazon konnte keine Abonnements für diese Tabelle gewähren. Weitere Informationen finden Sie unter Lake Formation Formation-Berechtigungen für Amazon konfigurieren DataZone.

HIPAA-Konformität

Veröffentlicht am 14.12.2023

Amazon DataZone entspricht jetzt dem US-amerikanischen Health Insurance Portability and Accountability Act von 1996 (HIPAA). Die Liste der AWS Dienste, die HIPAA-konform sind, finden Sie unter https://aws.amazon.com/compliance//. hipaa-eligible-services-reference

KI-Empfehlungen für Beschreibungen in Amazon DataZone (Vorschau)

Veröffentlicht am 28.11.2023

AWS kündigt die Vorschau einer neuen generativen KI-basierten Funktion in Amazon an, DataZone um die Datenerkennung, das Datenverständnis und die Datennutzung durch die Erweiterung

des Geschäftsdatenkatalogs zu verbessern. Mit einem einzigen Klick können Datenproduzenten umfassende Beschreibungen und den Kontext von Geschäftsdaten generieren, aussagekräftige Spalten hervorheben und Empfehlungen zu analytischen Anwendungsfällen geben. Mit KI-Empfehlungen für Beschreibungen in Amazon können Datenkonsumenten Datentabellen und Spalten identifizieren DataZone, die für die Analyse benötigt werden, was die Auffindbarkeit von Daten verbessert und die back-and-forth Kommunikation mit Datenproduzenten reduziert. Die Vorversion ist in DataZone Amazon-Domains verfügbar, die in den folgenden AWS Regionen bereitgestellt werden: USA Ost (Nord-Virginia), USA West (Oregon). Weitere Informationen finden Sie unter Einsatz von maschinellem Lernen und generativer KI.

DefaultDataLake Verbesserung des Blueprints

Veröffentlicht am 20.11.2023

Amazon DataZone hat dem DefaultDataLake Blueprint eine Erweiterung hinzugefügt, mit der Sie besser kontrollieren können, wer welche Daten aus Ihrem AWS Konto veröffentlichen kann. Mit der Einführung dieser Funktion wurden zwei wichtige Änderungen eingeführt.

- Sobald Sie den DefaultDataLake Blueprint aktiviert haben, können Sie in der Konsole steuern, welche Projekte den DefaultDataLake Blueprint in Ihrem Konto verwenden können, um Umgebungsprofile zu erstellen, indem Sie dem aktivierten Blueprint die Verwaltung von Projekten zuweisen.
- Die zweite Änderung betrifft das Portal. Wenn Sie mithilfe des DefaultDataLake Blueprints ein Umgebungsprofil erstellen, können Sie auch die autorisierten Projekte auswählen, die das Umgebungsprofil zum Erstellen von Umgebungen verwenden dürfen. Standardmäßig dürfen alle Projekte das Data Lake-Umgebungsprofil verwenden. Sie können das Umgebungsprofil jedoch auf bestimmte Projekte beschränken und auch steuern, welche Daten mithilfe der mit dem Profil erstellten Umgebungen veröffentlicht werden können.

Weitere Informationen finden Sie unter Erstellen Sie ein Umgebungsprofil.

Einrichtung

Um Amazon einzurichten DataZone, müssen Sie über ein AWS Konto verfügen und die erforderlichen IAM-Richtlinien und -Berechtigungen für Amazon DataZone einrichten.

Sobald Sie Ihre DataZone Amazon-Berechtigungen eingerichtet haben, wird empfohlen, dass Sie die Schritte im Abschnitt Erste Schritte ausführen, der Sie durch die Erstellung der DataZone Amazon-Domain, das Abrufen der Datenportal-URL und die grundlegenden DataZone Amazon-Workflows für Datenproduzenten und Datenkonsumenten führt.

Themen

Eröffnen Sie ein AWS Konto

Wenn Sie noch kein AWS Konto haben, führen Sie die folgenden Schritte aus, um eines zu erstellen.

Wenn Sie eine AWS Organisation haben, erstellen Sie ein Konto:

1. Melden Sie sich bei der AWS Management Console an und öffnen Sie die Organisationskonsole unter https://console.aws.amazon.com/organizations/.
2. Wählen Sie im Navigationsbereich AWS Konten aus.
3. Wählen Sie AWS Konto hinzufügen aus.
4. Wählen Sie AWS Konto erstellen und geben Sie die angeforderten Daten ein. Wählen Sie AWS Konto erstellen.

Um ein AWS Konto zu eröffnen

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

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

Wenn Sie sich für ein AWS Konto registrieren, wird ein Root-Benutzer für das AWS Konto erstellt. Der Root-Benutzer hat Zugriff auf alle AWS Dienste und Ressourcen im Konto. Als bewährte Sicherheitsmethode weisen Sie einem Administratorbenutzer Administratorzugriff zu und verwenden Sie nur den Root-Benutzer, um Aufgaben auszuführen, die Root-Benutzerzugriff erfordern.

Konfigurieren Sie die IAM-Berechtigungen, die für die Nutzung der Amazon DataZone Management Console erforderlich sind

Jeder Benutzer, jede Gruppe oder Rolle, der die Amazon DataZone Management Console verwenden möchte, muss über die erforderlichen Berechtigungen verfügen.

Themen

- Ordnen Sie einem Benutzer, einer Gruppe oder einer Rolle erforderliche und optionale Richtlinien für den Zugriff auf die DataZone Amazon-Konsole zu
- Erstellen Sie eine benutzerdefinierte Richtlinie für IAM-Berechtigungen, um die vereinfachte Rollenerstellung über die Amazon DataZone Service Console zu ermöglichen
- Erstellen Sie eine benutzerdefinierte Richtlinie für Berechtigungen zur Verwaltung eines mit einer DataZone Amazon-Domain verknüpften Kontos
- (Optional) Erstellen Sie eine benutzerdefinierte Richtlinie für AWS Identity Center-Berechtigungen, um Single Sign-On (SSO) für Ihre Domain zu aktivieren
- (Optional) Erstellen Sie eine benutzerdefinierte Richtlinie für AWS Identity Center-Berechtigungen, um SSO-Benutzer- und SSO-Gruppenzugriffe auf Ihre DataZone Amazon-Domain hinzuzufügen und zu entfernen.
- (Optional) Fügen Sie Ihren IAM-Prinzipal als Schlüsselbenutzer hinzu, um Ihre DataZone Amazon-Domain mit einem vom Kunden verwalteten Schlüssel von AWS Key Management Service (KMS) zu erstellen

Ordnen Sie einem Benutzer, einer Gruppe oder einer Rolle erforderliche und optionale Richtlinien für den Zugriff auf die DataZone Amazon-Konsole zu

Gehen Sie wie folgt vor, um einem Benutzer, einer Gruppe oder einer Rolle die erforderlichen und optionalen benutzerdefinierten Richtlinien zuzuweisen. Weitere Informationen finden Sie unter AWS verwaltete Richtlinien für Amazon DataZone.

1. Melden Sie sich bei der AWS Management Console an und öffnen Sie die IAM-Konsole unter https://console.aws.amazon.com/iam/.
2. Wählen Sie im Navigationsbereich Richtlinien.
3. Wählen Sie die folgenden Richtlinien aus, die Sie Ihrem Benutzer, Ihrer Gruppe oder einer Rolle zuordnen möchten.

   - Aktivieren Sie in der Liste der Richtlinien das Kontrollkästchen neben dem AmazonDataZoneFullAccess. Über das Menü Filter und das Suchfeld können Sie die Richtlinienliste filtern. Weitere Informationen finden Sie unter AWS verwaltete Richtlinie: AmazonDataZoneFullAccess.
   - (Optional) Erstellen Sie eine benutzerdefinierte Richtlinie für IAM-Berechtigungen, um die vereinfachte Rollenerstellung über die Amazon DataZone Service Console zu ermöglichen.
   - (Optional) Erstellen Sie eine benutzerdefinierte Richtlinie für AWS Identity Center-Berechtigungen, um Single Sign-On (SSO) für Ihre Domain zu aktivieren.
   - (Optional) Erstellen Sie eine benutzerdefinierte Richtlinie für AWS Identity Center-Berechtigungen, um SSO-Benutzer- und SSO-Gruppenzugriffe auf Ihre DataZone Amazon-Domain hinzuzufügen und zu entfernen.
4. Wählen Sie Actions (Aktionen) und dann Attach policy (Richtlinie anfügen).
5. Wählen Sie den Benutzer, die Gruppe oder die Rolle aus, der Sie die Richtlinie zuordnen möchten. Über das Menü Filter und das Suchfeld können Sie die Liste der Prinzipal-Entitäten filtern. Nachdem Sie den Benutzer, die Gruppe oder die Rolle ausgewählt haben, wählen Sie Richtlinie anhängen.

Erstellen Sie eine benutzerdefinierte Richtlinie für IAM-Berechtigungen, um die vereinfachte Rollenerstellung über die Amazon DataZone Service Console zu ermöglichen

Gehen Sie wie folgt vor, um eine benutzerdefinierte Inline-Richtlinie zu erstellen, um über die erforderlichen Berechtigungen zu verfügen DataZone , damit Amazon die erforderlichen Rollen in der AWS Management-Konsole in Ihrem Namen erstellen kann.

1. Melden Sie sich bei der AWS Management Console an und öffnen Sie die IAM-Konsole unter https://console.aws.amazon.com/iam/.
2. Wählen Sie im Navigationsbereich Benutzer oder Benutzergruppen.
3. Wählen Sie in der Liste den Namen des Benutzers oder der Gruppe, in die eine Richtlinie eingebettet werden soll.
4. Wählen Sie die Registerkarte Permissions (Berechtigungen) aus und erweitern Sie ggf. den Abschnitt Permissions policies (Berechtigungsrichtlinien).
5. Wählen Sie den Link „Berechtigungen hinzufügen“ und „Inline-Richtlinie erstellen“.
6. Wählen Sie auf dem Bildschirm Richtlinie erstellen im Abschnitt Richtlinien-Editor die Option JSON aus.

   Erstellen Sie ein Richtliniendokument mit den folgenden JSON-Anweisungen und wählen Sie dann Weiter.

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Action": [
                "iam:CreatePolicy",
                "iam:CreateRole"
            ],
            "Resource": [
                "arn:aws:iam::*:policy/service-role/AmazonDataZone*",
                "arn:aws:iam::*:role/service-role/AmazonDataZone*"
            ]
        },
        {
```

```
            "Effect": "Allow",
            "Action": "iam:AttachRolePolicy",
            "Resource": "arn:aws:iam::*:role/service-role/AmazonDataZone*",
            "Condition": {
                "ArnLike": {
                    "iam:PolicyARN": [
                        "arn:aws:iam::aws:policy/AmazonDataZone*",
                        "arn:aws:iam::*:policy/service-role/AmazonDataZone*"
                    ]
                }
            }
        }
    ]
}
```

7. Geben Sie auf dem Bildschirm „Richtlinie überprüfen“ einen Namen für die Richtlinie ein. Wenn Sie mit der Richtlinie zufrieden sind, klicken Sie auf Create policy (Richtlinie erstellen). Stellen Sie sicher, dass in dem roten Feld am oberen Bildschirmrand keine Fehler angezeigt werden. Korrigieren Sie etwaige Fehler.

Erstellen Sie eine benutzerdefinierte Richtlinie für Berechtigungen zur Verwaltung eines mit einer DataZone Amazon-Domain verknüpften Kontos

Gehen Sie wie folgt vor, um eine benutzerdefinierte Inline-Richtlinie zu erstellen, damit Sie in einem zugehörigen AWS Konto über die erforderlichen Berechtigungen verfügen, um gemeinsam genutzte Ressourcen einer Domain aufzulisten, zu akzeptieren und abzulehnen und anschließend Umgebungs-Blueprints im zugehörigen Konto zu aktivieren, zu konfigurieren und zu deaktivieren. Um die optionale vereinfachte Rollenerstellung der Amazon DataZone Service Console zu aktivieren, die während der Blueprint-Konfiguration verfügbar ist, müssen Sie außerdemErstellen Sie eine benutzerdefinierte Richtlinie für IAM-Berechtigungen, um die vereinfachte Rollenerstellung über die Amazon DataZone Service Console zu ermöglichen .

1. Melden Sie sich bei der AWS Management Console an und öffnen Sie die IAM-Konsole unter https://console.aws.amazon.com/iam/.
2. Wählen Sie im Navigationsbereich Benutzer oder Benutzergruppen.
3. Wählen Sie in der Liste den Namen des Benutzers oder der Gruppe, in die eine Richtlinie eingebettet werden soll.

4. Wählen Sie die Registerkarte Permissions (Berechtigungen) aus und erweitern Sie ggf. den Abschnitt Permissions policies (Berechtigungsrichtlinien).
5. Wählen Sie den Link „Berechtigungen hinzufügen“ und „Inline-Richtlinie erstellen“.
6. Wählen Sie auf dem Bildschirm Richtlinie erstellen im Abschnitt Richtlinien-Editor die Option JSON aus. Erstellen Sie ein Richtliniendokument mit den folgenden JSON-Anweisungen und wählen Sie dann Weiter.

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Action": [
                "datazone:ListEnvironmentBlueprintConfigurations",
                "datazone:PutEnvironmentBlueprintConfiguration",
                "datazone:GetDomain",
                "datazone:ListDomains",
                "datazone:GetEnvironmentBlueprintConfiguration",
                "datazone:ListEnvironmentBlueprints",
                "datazone:GetEnvironmentBlueprint",
                "datazone:ListAccountEnvironments",
                "datazone:DeleteEnvironmentBlueprintConfiguration"
            ],
            "Resource": "*"
        },
        {
            "Effect": "Allow",
            "Action": "iam:PassRole",
            "Resource": [
                "arn:aws:iam::*:role/AmazonDataZone",
                "arn:aws:iam::*:role/service-role/AmazonDataZone*"
            ],
            "Condition": {
                "StringEquals": {
                    "iam:passedToService": "datazone.amazonaws.com"
                }
            }
        },
        {
            "Effect": "Allow",
            "Action": "iam:AttachRolePolicy",
```

```
            "Resource": "arn:aws:iam::*:role/service-role/AmazonDataZone*",
            "Condition": {
                "ArnLike": {
                    "iam:PolicyARN": [
                        "arn:aws:iam::aws:policy/AmazonDataZone*",
                        "arn:aws:iam::*:policy/service-role/AmazonDataZone*"
                    ]
                }
            }
        },
        {
            "Effect": "Allow",
            "Action": "iam:ListRoles",
            "Resource": "*"
        },
        {
            "Effect": "Allow",
            "Action": [
                "iam:CreatePolicy",
                "iam:CreateRole"
            ],
            "Resource": [
                "arn:aws:iam::*:policy/service-role/AmazonDataZone*",
                "arn:aws:iam::*:role/service-role/AmazonDataZone*"
            ]
        },
        {
            "Effect": "Allow",
            "Action": [
                "ram:AcceptResourceShareInvitation",
                "ram:RejectResourceShareInvitation",
                "ram:GetResourceShareInvitations"
            ],
            "Resource": "*"
        },
        {
            "Effect": "Allow",
            "Action": [
                "s3:ListAllMyBuckets",
                "s3:ListBucket",
                "s3:GetBucketLocation"
            ],
            "Resource": "*"
        },
```

```
        {
            "Effect": "Allow",
            "Action": "s3:CreateBucket",
            "Resource": "arn:aws:s3:::amazon-datazone*"
        }
    ]
}
```

7. Geben Sie auf dem Bildschirm „Richtlinie überprüfen“ einen Namen für die Richtlinie ein. Wenn Sie mit der Richtlinie zufrieden sind, klicken Sie auf Create policy (Richtlinie erstellen). Stellen Sie sicher, dass in dem roten Feld am oberen Bildschirmrand keine Fehler angezeigt werden. Korrigieren Sie etwaige Fehler.

(Optional) Erstellen Sie eine benutzerdefinierte Richtlinie für AWS Identity Center-Berechtigungen, um Single Sign-On (SSO) für Ihre Domain zu aktivieren

Gehen Sie wie folgt vor, um eine benutzerdefinierte Inline-Richtlinie zu erstellen, damit Sie über die erforderlichen Berechtigungen verfügen, um Single Sign-On (SSO) mithilfe des AWS IAM Identity Center in Amazon zu aktivieren. DataZone

1. Melden Sie sich bei der AWS Management Console an und öffnen Sie die IAM-Konsole unter https://console.aws.amazon.com/iam/.
2. Wählen Sie im Navigationsbereich Benutzer oder Benutzergruppen.
3. Wählen Sie in der Liste den Namen des Benutzers oder der Gruppe, in die eine Richtlinie eingebettet werden soll.
4. Wählen Sie die Registerkarte Permissions (Berechtigungen) aus und erweitern Sie ggf. den Abschnitt Permissions policies (Berechtigungsrichtlinien).
5. Wählen Sie Berechtigungen hinzufügen und Inline-Richtlinie erstellen aus.
6. Wählen Sie auf dem Bildschirm Richtlinie erstellen im Abschnitt Richtlinien-Editor die Option JSON aus.

   Erstellen Sie ein Richtliniendokument mit den folgenden JSON-Anweisungen und wählen Sie dann Weiter.

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Action": [
                "sso:DeleteManagedApplicationInstance",
                "sso:CreateManagedApplicationInstance",
                "sso:PutApplicationAssignmentConfiguration"
            ],
            "Resource": "*"
        }
    ]
}
```

7. Geben Sie auf dem Bildschirm „Richtlinie überprüfen“ einen Namen für die Richtlinie ein. Wenn Sie mit der Richtlinie zufrieden sind, klicken Sie auf Create policy (Richtlinie erstellen). Stellen Sie sicher, dass in dem roten Feld am oberen Bildschirmrand keine Fehler angezeigt werden. Korrigieren Sie etwaige Fehler.

(Optional) Erstellen Sie eine benutzerdefinierte Richtlinie für AWS Identity Center-Berechtigungen, um SSO-Benutzer- und SSO-Gruppenzugriffe auf Ihre DataZone Amazon-Domain hinzuzufügen und zu entfernen.

Gehen Sie wie folgt vor, um eine benutzerdefinierte Inline-Richtlinie zu erstellen, damit Sie über die erforderlichen Berechtigungen verfügen, um SSO-Benutzer- und SSO-Gruppenzugriffe auf Ihre DataZone Amazon-Domain hinzuzufügen und zu entfernen.

1. Melden Sie sich bei der AWS Management Console an und öffnen Sie die IAM-Konsole unter https://console.aws.amazon.com/iam/.
2. Wählen Sie im Navigationsbereich Benutzer oder Benutzergruppen.
3. Wählen Sie in der Liste den Namen des Benutzers oder der Gruppe, in die eine Richtlinie eingebettet werden soll.
4. Wählen Sie die Registerkarte Permissions (Berechtigungen) aus und erweitern Sie ggf. den Abschnitt Permissions policies (Berechtigungsrichtlinien).
5. Wählen Sie Berechtigungen hinzufügen und Inline-Richtlinie erstellen aus.

6. Wählen Sie auf dem Bildschirm Richtlinie erstellen im Abschnitt Richtlinien-Editor die Option JSON aus.

   Erstellen Sie ein Richtliniendokument mit den folgenden JSON-Anweisungen und wählen Sie dann Weiter.

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Action": [
        "sso:GetManagedApplicationInstance",
        "sso:ListProfiles",
        "sso:GetProfiles",
        "sso:AssociateProfile",
        "sso:DisassociateProfile",
        "sso:GetProfile"
      ],
      "Resource": "*"
    }
  ]
}
```

7. Geben Sie auf dem Bildschirm „Richtlinie überprüfen“ einen Namen für die Richtlinie ein. Wenn Sie mit der Richtlinie zufrieden sind, klicken Sie auf Create policy (Richtlinie erstellen). Stellen Sie sicher, dass in dem roten Feld am oberen Bildschirmrand keine Fehler angezeigt werden. Korrigieren Sie etwaige Fehler.

(Optional) Fügen Sie Ihren IAM-Prinzipal als Schlüsselbenutzer hinzu, um Ihre DataZone Amazon-Domain mit einem vom Kunden verwalteten Schlüssel von AWS Key Management Service (KMS) zu erstellen

Bevor Sie Ihre DataZone Amazon-Domain optional mit einem vom Kunden verwalteten Schlüssel (CMK) vom AWS Key Management Service (KMS) erstellen können, führen Sie das folgende Verfahren durch, um Ihren IAM-Principal zum Benutzer Ihres KMS-Schlüssels zu machen.

1. Melden Sie sich bei der AWS Management Console an und öffnen Sie die KMS-Konsole unter https://console.aws.amazon.com/kms/.
2. Zum Anzeigen der Schlüssel in Ihrem Konto, die Sie erstellen und verwalten, wählen Sie im Navigationsbereich Customer managed keys (Vom Kunden verwaltete Schlüssel) aus.
3. Wählen Sie in der Liste der KMS-Schlüssel den Alias oder die Schlüssel-ID des KMS-Schlüssels aus, den Sie untersuchen möchten.
4. Verwenden Sie die Steuerelemente im Abschnitt Hauptbenutzer der Seite, um Schlüsselbenutzer hinzuzufügen oder zu entfernen und externen AWS Konten die Verwendung des KMS-Schlüssels zu gestatten oder zu verbieten. Schlüsselbenutzer können den KMS-Schlüssel in kryptografischen Produktionen verwenden, wie beispielsweise der Verschlüsselung, Entschlüsselung, erneuten Verschlüsselung und Generierung von Datenschlüsseln.

Konfigurieren Sie die IAM-Berechtigungen, die für die Nutzung des DataZone Amazon-Datenportals erforderlich sind

Jeder Benutzer, jede Gruppe oder Rolle, der das DataZone Amazon-Datenportal oder den Amazon-Katalog verwenden möchte, muss über die erforderlichen Berechtigungen verfügen.

Themen

- Hängen Sie die erforderliche Richtlinie an einen Benutzer, eine Gruppe oder eine Rolle für den Zugriff auf das DataZone Amazon-Datenportal an
- Ordnen Sie einem Benutzer, einer Gruppe oder einer Rolle die erforderliche Richtlinie für den Zugriff auf den DataZone Amazon-Katalog zu
- Fügen Sie einem Benutzer, einer Gruppe oder einer Rolle eine optionale Richtlinie für den Zugriff auf das DataZone Amazon-Datenportal oder den Amazon-Katalog hinzu, wenn Ihre Domain mit einem vom Kunden verwalteten Schlüssel von AWS Key Management Service (KMS) verschlüsselt ist

Hängen Sie die erforderliche Richtlinie an einen Benutzer, eine Gruppe oder eine Rolle für den Zugriff auf das DataZone Amazon-Datenportal an

Sie können auf das DataZone Amazon-Datenportal zugreifen, indem Sie entweder Ihre AWS Anmeldeinformationen oder Ihre Single Sign-On (SSO) -Anmeldeinformationen verwenden. Folgen Sie den Anweisungen im folgenden Abschnitt, um die Berechtigungen einzurichten, die für den Zugriff

auf das Datenportal mit Ihren AWS Anmeldeinformationen erforderlich sind. Weitere Informationen zur Verwendung von Amazon DataZone mit SSO finden Sie unterAWS IAM Identity Center für Amazon einrichten DataZone.

> **Note**
>
> Nur IAM-Prinzipale im AWS Konto Ihrer Domain können auf das Datenportal der Domain zugreifen. IAM-Prinzipale anderer AWS Konten können nicht auf das Datenportal der Domain zugreifen.

Gehen Sie wie folgt vor, um die erforderliche Richtlinie einem Benutzer, einer Gruppe oder einer Rolle zuzuweisen. Weitere Informationen finden Sie unter AWS verwaltete Richtlinien für Amazon DataZone.

1. Melden Sie sich bei der AWS Management Console an und öffnen Sie die IAM-Konsole unter https://console.aws.amazon.com/iam/.
2. Wählen Sie im Navigationsbereich Benutzer, Benutzergruppen oder Rollen aus.
3. Wählen Sie in der Liste den Namen des Benutzers, der Gruppe oder der Rolle aus, in die eine Richtlinie eingebettet werden soll.
4. Wählen Sie die Registerkarte Permissions (Berechtigungen) aus und erweitern Sie ggf. den Abschnitt Permissions policies (Berechtigungsrichtlinien).
5. Wählen Sie den Link „Berechtigungen hinzufügen“ und „Inline-Richtlinie erstellen“.
6. Wählen Sie auf dem Bildschirm Richtlinie erstellen im Abschnitt Richtlinien-Editor die Option JSON aus. Erstellen Sie ein Richtliniendokument mit den folgenden JSON-Anweisungen und wählen Sie dann Weiter.

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Action": [
                "datazone:GetIamPortalLoginUrl"
            ],
            "Resource": [
                "*"
```

```
            ]
        }
    ]
}
```

7. Geben Sie auf dem Bildschirm „Richtlinie überprüfen“ einen Namen für die Richtlinie ein. Wenn Sie mit der Richtlinie zufrieden sind, klicken Sie auf Create policy (Richtlinie erstellen). Stellen Sie sicher, dass in dem roten Feld am oberen Bildschirmrand keine Fehler angezeigt werden. Korrigieren Sie etwaige Fehler.

Ordnen Sie einem Benutzer, einer Gruppe oder einer Rolle die erforderliche Richtlinie für den Zugriff auf den DataZone Amazon-Katalog zu

> **Note**
>
> Nur IAM-Principals im AWS Konto Ihrer Domain können auf den Katalog der Domain zugreifen. IAM-Prinzipale anderer AWS Konten können nicht auf den Katalog der Domain zugreifen.

Mit dem folgenden Verfahren können Sie Ihren IAM-Identitäten über die API und das SDK Zugriff auf den Katalog Ihrer DataZone Amazon-Domain gewähren. Wenn Sie möchten, dass diese IAM-Identitäten auch Zugriff auf das DataZone Amazon-Datenportal haben, gehen Sie zusätzlich wie oben beschrieben vor. Hängen Sie die erforderliche Richtlinie an einen Benutzer, eine Gruppe oder eine Rolle für den Zugriff auf das DataZone Amazon-Datenportal an Weitere Informationen finden Sie unter AWS verwaltete Richtlinien für Amazon DataZone.

1. Melden Sie sich bei der AWS Management Console an und öffnen Sie die IAM-Konsole unter https://console.aws.amazon.com/iam/.
2. Wählen Sie im Navigationsbereich Richtlinien.
3. Wählen Sie in der Liste der Richtlinien das Optionsfeld neben der AmazonDataZoneFullUserAccessRichtlinie aus. Über das Menü Filter und das Suchfeld können Sie die Richtlinienliste filtern. Weitere Informationen finden Sie unter AWS verwaltete Richtlinie: AmazonDataZoneFullUserAccess.
4. Wählen Sie Actions (Aktionen) und dann Attach policy (Richtlinie anfügen).

5. Wählen Sie den Benutzer, die Gruppe oder die Rolle aus, der Sie die Richtlinie zuordnen möchten, indem Sie das Kontrollkästchen neben jedem Prinzipal aktivieren. Über das Menü Filter und das Suchfeld können Sie die Liste der Prinzipal-Entitäten filtern. Nachdem Sie den Benutzer, die Gruppe oder die Rolle ausgewählt haben, wählen Sie Richtlinie anhängen aus.

Fügen Sie einem Benutzer, einer Gruppe oder einer Rolle eine optionale Richtlinie für den Zugriff auf das DataZone Amazon-Datenportal oder den Amazon-Katalog hinzu, wenn Ihre Domain mit einem vom Kunden verwalteten Schlüssel von AWS Key Management Service (KMS) verschlüsselt ist

Wenn Sie Ihre DataZone Amazon-Domain mit Ihrem eigenen KMS-Schlüssel für die Datenverschlüsselung erstellen, müssen Sie auch eine Inline-Richtlinie mit den folgenden Berechtigungen erstellen und diese an Ihre IAM-Prinzipale anhängen, damit diese auf das DataZone Amazon-Datenportal oder den Amazon-Katalog zugreifen können.

1. Melden Sie sich bei der AWS Management Console an und öffnen Sie die IAM-Konsole unter https://console.aws.amazon.com/iam/.
2. Wählen Sie im Navigationsbereich Benutzer, Benutzergruppen oder Rollen aus.
3. Wählen Sie in der Liste den Namen des Benutzers, der Gruppe oder der Rolle aus, in die eine Richtlinie eingebettet werden soll.
4. Wählen Sie die Registerkarte Permissions (Berechtigungen) aus und erweitern Sie ggf. den Abschnitt Permissions policies (Berechtigungsrichtlinien).
5. Wählen Sie den Link „Berechtigungen hinzufügen“ und „Inline-Richtlinie erstellen“.
6. Wählen Sie auf dem Bildschirm Richtlinie erstellen im Abschnitt Richtlinien-Editor die Option JSON aus. Erstellen Sie ein Richtliniendokument mit den folgenden JSON-Anweisungen und wählen Sie dann Weiter.

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Action": [
                "kms:Decrypt",
```

```
                "kms:GenerateDataKey",
                "kms:DescribeKey"
            ],
            "Resource": "*"
        }
    ]
}
```

7. Geben Sie auf dem Bildschirm „Richtlinie überprüfen“ einen Namen für die Richtlinie ein. Wenn Sie mit der Richtlinie zufrieden sind, klicken Sie auf Create policy (Richtlinie erstellen). Stellen Sie sicher, dass in dem roten Feld am oberen Bildschirmrand keine Fehler angezeigt werden. Korrigieren Sie etwaige Fehler.

AWS IAM Identity Center für Amazon einrichten DataZone

> **Note**
>
> AWS Identity Center muss in derselben AWS Region wie Ihre DataZone Amazon-Domain aktiviert sein. Derzeit kann AWS Identity Center nur in einer einzigen AWS Region aktiviert werden.

Sie können auf das DataZone Amazon-Datenportal zugreifen, indem Sie entweder Ihre Single Sign-On (SSO) -Anmeldeinformationen oder AWS Anmeldeinformationen verwenden. Folgen Sie den Anweisungen in diesem Abschnitt, um AWS IAM Identity Center für Amazon DataZone einzurichten. Weitere Informationen zur Verwendung von Amazon DataZone mit Ihren AWS Anmeldeinformationen finden Sie unterKonfigurieren Sie die IAM-Berechtigungen, die für die Nutzung der Amazon DataZone Management Console erforderlich sind.

Sie können die Verfahren in diesem Abschnitt überspringen, wenn Sie AWS IAM Identity Center (Nachfolger von AWS Single Sign-On) bereits in derselben AWS Region aktiviert und konfiguriert haben, in der Sie Ihre DataZone Amazon-Domain erstellen möchten.

Gehen Sie wie folgt vor, um AWS IAM Identity Center (Nachfolger von AWS Single Sign-On) zu aktivieren.

1. Um AWS IAM Identity Center zu aktivieren, müssen Sie sich mit den Anmeldeinformationen Ihres AWS AWS Organisationsverwaltungskontos bei der Management Console anmelden. Sie

können IAM Identity Center nicht aktivieren, während Sie mit den Anmeldeinformationen eines Mitgliedskontos einer AWS Organizations angemeldet sind. Weitere Informationen finden Sie unter Organisation erstellen und verwalten im AWS Organizations User Guide.

2. Öffnen Sie die AWS IAM Identity Center-Konsole (Nachfolger von AWS Single Sign-On) und wählen Sie mit der Regionsauswahl in der oberen Navigationsleiste die AWS Region aus, in der Sie Ihre Amazon-Domain erstellen möchten. DataZone
3. Wählen Sie Enable (Aktivieren) aus.
4. Wählen Sie Ihre Identitätsquelle.

   Standardmäßig erhalten Sie einen IAM Identity Center Store für eine schnelle und einfache Benutzerverwaltung. Optional können Sie stattdessen einen externen Identitätsanbieter verbinden. In diesem Verfahren verwenden wir den standardmäßigen IAM Identity Center-Speicher.

   Weitere Informationen finden Sie unter Wählen Sie Ihre Identitätsquelle.
5. Wählen Sie im Navigationsbereich von IAM Identity Center die Option Gruppen und anschließend Gruppe erstellen aus. Geben Sie den Gruppennamen ein und wählen Sie Create aus.
6. Wählen Sie im Navigationsbereich von IAM Identity Center die Option Benutzer aus.
7. Geben Sie auf dem Bildschirm „Benutzer hinzufügen“ die erforderlichen Informationen ein und wählen Sie „Dem Benutzer eine E-Mail mit Anweisungen zur Einrichtung des Passworts senden“. Der Benutzer sollte eine E-Mail mit den nächsten Einrichtungsschritten erhalten.
8. Wählen Sie Weiter: Gruppen, wählen Sie die gewünschte Gruppe aus und klicken Sie auf Benutzer hinzufügen. Benutzer sollten eine E-Mail erhalten, in der sie zur Verwendung von SSO eingeladen werden. In dieser E-Mail müssen sie Einladung annehmen auswählen und das Passwort festlegen.

Nachdem Sie Ihre DataZone Amazon-Domain erstellt haben, können Sie AWS Identity Center for Amazon aktivieren DataZone und Zugriff auf Ihre SSO-Benutzer und SSO-Gruppen gewähren. Weitere Informationen finden Sie unter IAM Identity Center für Amazon aktivieren DataZone.

Erste Schritte

Die Informationen in diesem Abschnitt helfen Ihnen bei den ersten Schritten mit Amazon DataZone. Wenn Sie neu bei Amazon sind DataZone, sollten Sie sich zunächst mit den Konzepten und der Terminologie in vertraut machen DataZone Amazon-Terminologie und Konzepte.

In diesem Abschnitt „Erste Schritte“ werden Sie durch die folgenden DataZone Amazon-Schnellstart-Workflows geführt:

Themen

- DataZone Amazon-Schnellstart mit AWS Glue-Daten
- DataZone Amazon-Schnellstart mit Amazon Redshift-Daten
- DataZone Amazon-Schnellstart mit Beispielskripten

> **Important**
>
> Bevor Sie mit den Schritten in einem dieser Schnellstart-Workflows beginnen, müssen Sie die im Abschnitt Einrichtung dieses Handbuchs beschriebenen Verfahren abschließen. Wenn Sie ein brandneues AWS Konto verwenden, müssen Sie die für die Nutzung der Amazon DataZone Management Console erforderlichen Berechtigungen konfigurieren. Wenn Sie ein AWS Konto verwenden, das bereits über AWS Glue Data Catalog-Objekte verfügt, müssen Sie auch Lake Formation Formation-Berechtigungen für Amazon konfigurieren DataZone.

DataZone Amazon-Schnellstart mit AWS Glue-Daten

Themen

- Schritt 1 — DataZone Amazon-Domain und Datenportal erstellen
- Schritt 2 — Erstellen Sie das Veröffentlichungsprojekt
- Schritt 3 — Erstellen Sie die Umgebung
- Schritt 4: Erzeugen Sie Daten für die Veröffentlichung
- Schritt 5 — Metadaten aus AWS Glue sammeln
- Schritt 6 — Kuratieren und veröffentlichen Sie das Daten-Asset
- Schritt 7 — Erstellen Sie das Projekt für die Datenanalyse

- Schritt 8 — Erstellen Sie eine Umgebung für die Datenanalyse
- Schritt 9: Durchsuchen Sie den Datenkatalog und abonnieren Sie Daten
- Schritt 10 — Genehmigen Sie die Abonnementanfrage
- Schritt 11 — Erstellen Sie eine Abfrage und analysieren Sie Daten in Amazon Athena

Schritt 1 — DataZone Amazon-Domain und Datenportal erstellen

In diesem Abschnitt werden die Schritte zum Erstellen einer DataZone Amazon-Domain und eines Datenportals für diesen Workflow beschrieben.

Gehen Sie wie folgt vor, um eine DataZone Amazon-Domain zu erstellen. Weitere Informationen zu DataZone Amazon-Domains finden Sie unter DataZone Amazon-Terminologie und Konzepte.

1. Navigieren Sie zur DataZone Amazon-Konsole unter https://console.aws.amazon.com/datazone, melden Sie sich an und wählen Sie dann Create domain aus.

   > **Note**
   >
   > Wenn Sie eine bestehende DataZone Amazon-Domain für diesen Workflow verwenden möchten, wählen Sie Domains anzeigen, wählen Sie dann die Domain aus, die Sie verwenden möchten, und fahren Sie dann mit Schritt 2 der Erstellung eines Veröffentlichungsprojekts fort.

2. Geben Sie auf der Seite „Domain erstellen“ Werte für die folgenden Felder ein:

   - Name — geben Sie einen Namen für Ihre Domain an. Für die Zwecke dieses Workflows können Sie diese Domain Marketing nennen.
   - Beschreibung — Geben Sie eine optionale Domainbeschreibung an.
   - Datenverschlüsselung — Ihre Daten werden standardmäßig mit einem Schlüssel verschlüsselt, der Ihnen AWS gehört und der für Sie verwaltet wird. Für diesen Anwendungsfall können Sie die Standardeinstellungen für die Datenverschlüsselung beibehalten.

     Weitere Informationen zur Verwendung von vom Kunden verwalteten Schlüsseln finden Sie unterDatenverschlüsselung im Ruhezustand für Amazon DataZone. Wenn Sie Ihren eigenen KMS-Schlüssel für die Datenverschlüsselung verwenden, müssen Sie die folgende Anweisung in Ihre Standardeinstellung aufnehmenAmazonDataZoneDomainExecutionRole.

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Action": [
        "kms:Decrypt",
        "kms:GenerateDataKey"
      ],
      "Resource": "*"
    }
  ]
}
```

- Dienstzugriff — lassen Sie die standardmäßig ausgewählte Option Standardrolle verwenden unverändert.

> **Note**
>
> Wenn Sie eine bestehende DataZone Amazon-Domain für diesen Workflow verwenden, können Sie die Option Bestehende Servicerolle verwenden und dann eine bestehende Rolle aus dem Drop-down-Menü auswählen.

- Wählen Sie unter Schnelleinrichtung die Option Dieses Konto für Datenverbrauch und -veröffentlichung einrichten aus. Diese Option aktiviert die integrierten DataZone Amazon-Blueprints von Data Lake und Data Warehouse und konfiguriert die erforderlichen Berechtigungen, Ressourcen, ein Standardprojekt und standardmäßige Data Lake- und Data Warehouse-Umgebungsprofile für dieses Konto. Weitere Informationen zu Amazon DataZone Blueprints finden Sie unter DataZone Amazon-Terminologie und Konzepte.
- Lassen Sie die übrigen Felder unter den Berechtigungsdetails unverändert.

> **Note**
>
> Wenn Sie über eine bestehende DataZone Amazon-Domain verfügen, können Sie die Option Eine bestehende Servicerolle verwenden und dann eine vorhandene Rolle aus

dem Drop-down-Menü für die Rollen Glue Manage Access, Redshift Manage Access und Provisioning auswählen.

- Lassen Sie die Felder unter Tags unverändert.
- Wählen Sie Domain erstellen aus.

3. Sobald die Domain erfolgreich erstellt wurde, wählen Sie diese Domain aus und notieren Sie sich auf der Übersichtsseite der Domain die Datenportal-URL für diese Domain. Sie können diese URL verwenden, um auf Ihr DataZone Amazon-Datenportal zuzugreifen, um die restlichen Schritte in diesem Workflow abzuschließen. Sie können auch zum Datenportal navigieren, indem Sie Datenportal öffnen wählen.

> **Note**
>
> In der aktuellen Version von Amazon DataZone kann die für das Datenportal generierte URL nach der Erstellung der Domain nicht mehr geändert werden.

Die Erstellung der Domain kann mehrere Minuten dauern. Warten Sie, bis die Domain den Status Verfügbar hat, bevor Sie mit dem nächsten Schritt fortfahren.

Schritt 2 — Erstellen Sie das Veröffentlichungsprojekt

In diesem Abschnitt werden die Schritte beschrieben, die erforderlich sind, um das Veröffentlichungsprojekt für diesen Workflow zu erstellen.

1. Sobald Sie Schritt 1 oben abgeschlossen und eine Domain erstellt haben, sehen Sie die Meldung Willkommen bei Amazon DataZone! Fenster. Wählen Sie in diesem Fenster Projekt erstellen.
2. Geben Sie den Projektnamen für diesen Workflow an. Sie können ihn benennen SalesDataPublishingProject, dann die restlichen Felder unverändert lassen und dann Erstellen wählen.

Schritt 3 — Erstellen Sie die Umgebung

In diesem Abschnitt werden die Schritte beschrieben, die zum Erstellen einer Umgebung für diesen Workflow erforderlich sind.

1. Sobald Sie Schritt 2 oben abgeschlossen und Ihr Projekt erstellt haben, wird das Fenster Ihr Projekt ist einsatzbereit angezeigt. Wählen Sie in diesem Fenster die Option Umgebung erstellen.
2. Geben Sie auf der Seite Umgebung erstellen Folgendes an und wählen Sie dann Umgebung erstellen aus.
3. Geben Sie Werte für Folgendes an:
   - Name — geben Sie den Namen für die Umgebung an. Für diese exemplarische Vorgehensweise können Sie ihn `Default data lake environment` aufrufen.
   - Beschreibung — Geben Sie eine Beschreibung für die Umgebung an.
   - Umgebungsprofil — wählen Sie das DataLakeProfileUmgebungsprofil aus. Auf diese Weise können Sie Amazon DataZone in diesem Workflow verwenden, um mit Daten in Amazon S3, AWS Glue Catalog und Amazon Athena zu arbeiten.
   - Lassen Sie für diese exemplarische Vorgehensweise die restlichen Felder unverändert.
4. Wählen Sie Create environment (Umgebung erstellen) aus.

Schritt 4: Erzeugen Sie Daten für die Veröffentlichung

In diesem Abschnitt werden die Schritte beschrieben, die erforderlich sind, um Daten für die Veröffentlichung in diesem Workflow zu erstellen.

1. Nachdem Sie Schritt 3 oben abgeschlossen haben, wählen Sie in Ihrem `SalesDataPublishingProject` Projekt im rechten Bereich unter Analytics-Tools Amazon Athena aus. Dadurch wird der Athena-Abfrageeditor geöffnet, der die Anmeldeinformationen Ihres Projekts zur Authentifizierung verwendet. Vergewissern Sie sich, dass Ihre Veröffentlichungsumgebung in der Dropdownliste DataZone Amazon-Umgebung und die `<environment_name>%_pub_db` Datenbank wie im Abfrage-Editor ausgewählt ist.
2. In dieser exemplarischen Vorgehensweise verwenden Sie das CTAS-Abfrageskript (Create Table as Select), um eine neue Tabelle zu erstellen, die Sie auf Amazon veröffentlichen möchten. DataZone Führen Sie dieses CTAS-Skript in Ihrem Abfrage-Editor aus, um eine `mkt_sls_table` Tabelle zu erstellen, die Sie veröffentlichen und für die Suche und das Abonnement zur Verfügung stellen können.

```
CREATE TABLE mkt_sls_table AS
```

```
SELECT 146776932 AS ord_num, 23 AS sales_qty_sld, 23.4 AS wholesale_cost, 45.0 as
 lst_pr, 43.0 as sell_pr, 2.0 as disnt, 12 as ship_mode,13 as warehouse_id, 23 as
 item_id, 34 as ctlg_page, 232 as ship_cust_id, 4556 as bill_cust_id
UNION ALL SELECT 46776931, 24, 24.4, 46, 44, 1, 14, 15, 24, 35, 222, 4551
UNION ALL SELECT 46777394, 42, 43.4, 60, 50, 10, 30, 20, 27, 43, 241, 4565
UNION ALL SELECT 46777831, 33, 40.4, 51, 46, 15, 16, 26, 33, 40, 234, 4563
UNION ALL SELECT 46779160, 29, 26.4, 50, 61, 8, 31, 15, 36, 40, 242, 4562
UNION ALL SELECT 46778595, 43, 28.4, 49, 47, 7, 28, 22, 27, 43, 224, 4555
UNION ALL SELECT 46779482, 34, 33.4, 64, 44, 10, 17, 27, 43, 52, 222, 4556
UNION ALL SELECT 46779650, 39, 37.4, 51, 62, 13, 31, 25, 31, 52, 224, 4551
UNION ALL SELECT 46780524, 33, 40.4, 60, 53, 18, 32, 31, 31, 39, 232, 4563
UNION ALL SELECT 46780634, 39, 35.4, 46, 44, 16, 33, 19, 31, 52, 242, 4557
UNION ALL SELECT 46781887, 24, 30.4, 54, 62, 13, 18, 29, 24, 52, 223, 4561
```

Stellen Sie sicher, dass die Tabelle mkt_sls_table erfolgreich im Abschnitt Tabellen und Ansichten auf der linken Seite erstellt wurde. Jetzt haben Sie ein Datenobjekt, das im DataZone Amazon-Katalog veröffentlicht werden kann.

Schritt 5 — Metadaten aus AWS Glue sammeln

In diesem Abschnitt wird der Schritt des Sammelns von Metadaten aus AWS Glue für diesen Workflow beschrieben.

1. Nachdem Sie Schritt 4 oben abgeschlossen haben, wählen Sie im DataZone Amazon-Datenportal das `SalesDataPublishingProject` Projekt, dann die Registerkarte Daten und dann im linken Bereich Datenquellen aus.
2. Wählen Sie die Quelle aus, die im Rahmen der Erstellung der Umgebung erstellt wurde.
3. Wählen Sie neben dem Dropdownmenü „Aktion“ die Option „Ausführen“ und klicken Sie dann auf die Schaltfläche „Aktualisieren“. Sobald der Datenquellenlauf abgeschlossen ist, werden die Assets dem DataZone Amazon-Inventar hinzugefügt.

Schritt 6 — Kuratieren und veröffentlichen Sie das Daten-Asset

In diesem Abschnitt werden die Schritte zum Kuratieren und Veröffentlichen des Datenbestands in diesem Workflow beschrieben.

1. Nachdem Sie Schritt 5 oben abgeschlossen haben, wählen Sie im DataZone Amazon-Datenportal das `SalesDataPublishingProject` Projekt aus, das Sie im vorherigen Schritt

erstellt haben, wählen Sie die Registerkarte Daten, wählen Sie im linken Bereich Inventardaten aus und suchen Sie die `mkt_sls_table` Tabelle.

2. Öffnen Sie die Seite mit den `mkt_sls_table` Asset-Details, um die automatisch generierten Unternehmensnamen zu sehen. Wählen Sie das Symbol Automatisch generierte Metadaten, um die automatisch generierten Namen für Assets und Spalten anzuzeigen. Sie können entweder jeden Namen einzeln akzeptieren oder ablehnen oder Alle akzeptieren wählen, um die generierten Namen zu übernehmen. Optional können Sie Ihrem Asset auch das verfügbare Metadatenformular hinzufügen und Glossarbegriffe auswählen, um Ihre Daten zu klassifizieren.
3. Wählen Sie Asset veröffentlichen, um das Asset zu veröffentlichen. `mkt_sls_table`

Schritt 7 — Erstellen Sie das Projekt für die Datenanalyse

In diesem Abschnitt werden die Schritte zur Erstellung des Projekts für die Datenanalyse beschrieben. Dies ist der Beginn der Datenverbraucherschritte dieses Workflows.

1. Nachdem Sie Schritt 6 oben abgeschlossen haben, wählen Sie im DataZone Amazon-Datenportal im Drop-down-Menü Projekt die Option Projekt erstellen aus.
2. Geben Sie auf der Seite Projekt erstellen den Projektnamen an. Sie können beispielsweise für diesen Workflow einen Namen angeben MarketingDataAnalysisProject, dann die restlichen Felder unverändert lassen und dann Erstellen wählen.

Schritt 8 — Erstellen Sie eine Umgebung für die Datenanalyse

In diesem Abschnitt werden die Schritte zum Erstellen einer Umgebung für die Datenanalyse beschrieben.

1. Nachdem Sie Schritt 7 oben abgeschlossen haben, wählen Sie im DataZone Amazon-Datenportal das `MarketingDataAnalysisProject` Projekt, dann die Registerkarte Umgebungen und dann Umgebung erstellen aus.
2. Geben Sie auf der Seite Umgebung erstellen Folgendes an und wählen Sie dann Umgebung erstellen aus.

   - Name — geben Sie den Namen für die Umgebung an. Für diese exemplarische Vorgehensweise können Sie ihn `Default data lake environment` aufrufen.
   - Beschreibung — Geben Sie eine Beschreibung für die Umgebung an.
   - Umgebungsprofil — wählen Sie das integrierte DataLakeProfileUmgebungsprofil aus.

- Lassen Sie für diese exemplarische Vorgehensweise die restlichen Felder unverändert.

Schritt 9: Durchsuchen Sie den Datenkatalog und abonnieren Sie Daten

In diesem Abschnitt werden die Schritte zum Durchsuchen des Datenkatalogs und zum Abonnieren von Daten beschrieben.

1. Nachdem Sie Schritt 8 oben abgeschlossen haben, wählen Sie im DataZone Amazon-Datenportal das DataZone Amazon-Symbol und suchen Sie im DataZone Amazon-Suchfeld mithilfe von Schlüsselwörtern (z. B. „Katalog“ oder „Verkauf“) in der Suchleiste des Datenportals nach Datenbeständen.

   Wenden Sie bei Bedarf Filter oder Sortierungen an. Sobald Sie das Asset mit den Produktverkaufsdaten gefunden haben, können Sie es auswählen, um die Detailseite des Assets zu öffnen.
2. Wählen Sie auf der Detailseite des Assets „Katalog-Verkaufsdaten“ die Option Abonnieren aus.
3. Wählen Sie im Dialogfeld Abonnieren Ihr MarketingDataAnalysisProjectVerbraucherprojekt aus der Dropdownliste aus, geben Sie dann den Grund für Ihre Abonnementanfrage an und wählen Sie dann Abonnieren aus.

Schritt 10 — Genehmigen Sie die Abonnementanfrage

In diesem Abschnitt werden die Schritte zur Genehmigung der Abonnementanfrage beschrieben.

1. Nachdem Sie Schritt 9 oben abgeschlossen haben, wählen Sie im DataZone Amazon-Datenportal das SalesDataPublishingProjectProjekt aus, mit dem Sie Ihr Asset veröffentlicht haben.
2. Wählen Sie die Registerkarte Daten, dann Veröffentlichte Daten und dann Eingehende Anfragen aus.
3. Jetzt können Sie die Zeile für die neue Anfrage sehen, für die eine Genehmigung erforderlich ist. Wählen Sie Anfrage anzeigen. Geben Sie einen Grund für die Genehmigung an und wählen Sie Genehmigen.

Schritt 11 — Erstellen Sie eine Abfrage und analysieren Sie Daten in Amazon Athena

Nachdem Sie ein Asset erfolgreich im DataZone Amazon-Katalog veröffentlicht und abonniert haben, können Sie es analysieren.

1. Wählen Sie im DataZone Amazon-Datenportal Ihr MarketingDataAnalysisProjectVerbraucherprojekt aus und wählen Sie dann im rechten Bereich unter Analytics-Tools den Link Daten abfragen mit Amazon Athena aus. Dadurch wird der Amazon Athena Athena-Abfrage-Editor geöffnet, der die Anmeldeinformationen Ihres Projekts zur Authentifizierung verwendet. Wählen Sie die MarketingDataAnalysisProjectVerbraucherumgebung aus der Dropdownliste Amazon DataZone Environment im Abfrage-Editor und wählen Sie dann Ihre Projekte `<environment_name>%sub_db` aus der Datenbank-Dropdown-Liste aus.
2. Sie können jetzt Abfragen für die abonnierte Tabelle ausführen. Sie können die Tabelle aus Tabellen und Ansichten auswählen und dann „Vorschau“ wählen, damit die SELECT-Anweisung auf dem Editor-Bildschirm angezeigt wird. Führen Sie die Abfrage aus, um die Ergebnisse zu sehen.

DataZone Amazon-Schnellstart mit Amazon Redshift-Daten

Themen

Schritt 1 — DataZone Amazon-Domain und Datenportal erstellen

Gehen Sie wie folgt vor, um eine DataZone Amazon-Domain zu erstellen. Weitere Informationen zu DataZone Amazon-Domains finden Sie unter DataZone Amazon-Terminologie und Konzepte.

1. Navigieren Sie zur DataZone Amazon-Konsole unter https://console.aws.amazon.com/datazone, melden Sie sich an und wählen Sie dann Create domain aus.

   > **Note**
   >
   > Wenn Sie eine bestehende DataZone Amazon-Domain für diesen Workflow verwenden möchten, wählen Sie Domains anzeigen, wählen Sie dann die Domain aus, die Sie verwenden möchten, und fahren Sie dann mit Schritt 2 der Erstellung eines Veröffentlichungsprojekts fort.

2. Geben Sie auf der Seite „Domain erstellen“ Werte für die folgenden Felder ein:

   - Name — geben Sie einen Namen für Ihre Domain an. Für die Zwecke dieses Workflows können Sie diese Domain aufrufen`Marketing`.
   - Beschreibung — Geben Sie eine optionale Domänenbeschreibung an.
   - Datenverschlüsselung — Ihre Daten werden standardmäßig mit einem Schlüssel verschlüsselt, der Ihnen AWS gehört und der für Sie verwaltet wird. Für diese exemplarische Vorgehensweise können Sie die Standardeinstellungen für die Datenverschlüsselung beibehalten.

     Weitere Informationen zur Verwendung von vom Kunden verwalteten Schlüsseln finden Sie unterDatenverschlüsselung im Ruhezustand für Amazon DataZone. Wenn Sie Ihren eigenen KMS-Schlüssel für die Datenverschlüsselung verwenden, müssen Sie die folgende Anweisung in Ihre Standardeinstellung aufnehmenAmazonDataZoneDomainExecutionRole.

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Action": [
        "kms:Decrypt",
        "kms:GenerateDataKey"
```

```
      ],
      "Resource": "*"
    }
  ]
}
```

- Dienstzugriff — Wählen Sie die Option Benutzerdefinierte Servicerolle verwenden und wählen Sie dann im Dropdownmenü die AmazonDataZoneDomainExecutionRoleaus.
- Wählen Sie unter Schnelleinrichtung die Option Dieses Konto für Datenverbrauch und -veröffentlichung einrichten aus. Diese Option aktiviert die integrierten DataZone Amazon-Blueprints von Data Lake und Data Warehouse und konfiguriert die erforderlichen Berechtigungen und Ressourcen, um die restlichen Schritte in diesem Workflow abzuschließen. Weitere Informationen zu Amazon DataZone Blueprints finden Sie unter DataZone Amazon-Terminologie und Konzepte.
- Lassen Sie die übrigen Felder unter „Berechtigungsdetails“ und „Tags“ unverändert und wählen Sie dann „Domain erstellen“.

3. Sobald die Domain erfolgreich erstellt wurde, wählen Sie diese Domain aus und notieren Sie sich auf der Übersichtsseite der Domain die Datenportal-URL für diese Domain. Sie können diese URL verwenden, um auf Ihr DataZone Amazon-Datenportal zuzugreifen, um die restlichen Schritte in diesem Workflow abzuschließen.

> **Note**
>
> In der aktuellen Version von Amazon DataZone kann die für das Datenportal generierte URL nach der Erstellung der Domain nicht mehr geändert werden.

Die Erstellung der Domain kann mehrere Minuten dauern. Warten Sie, bis die Domain den Status Verfügbar hat, bevor Sie mit dem nächsten Schritt fortfahren.

Schritt 2 — Erstellen Sie das Veröffentlichungsprojekt

Im folgenden Abschnitt werden die Schritte zum Erstellen des Veröffentlichungsprojekts in diesem Workflow beschrieben.

1. Sobald Sie Schritt 1 abgeschlossen haben, navigieren Sie mit der DataZone Datenportal-URL zum Amazon-Datenportal und melden Sie sich mit Ihren Single Sign-On- (SSO) - oder AWS IAM-Anmeldeinformationen an.
2. Wählen Sie „Projekt erstellen“, geben Sie den Projektnamen an, z. B. für diesen Workflow. Sie können ihm einen Namen geben SalesDataPublishingProject, die restlichen Felder unverändert lassen und dann „Erstellen“ wählen.

Schritt 3 — Erstellen Sie die Umgebung

Im folgenden Abschnitt werden die Schritte zum Erstellen einer Umgebung in diesem Workflow beschrieben.

1. Nachdem Sie Schritt 2 abgeschlossen haben, wählen Sie im DataZone Amazon-Datenportal das `SalesDataPublishingProject` Projekt aus, das Sie im vorherigen Schritt erstellt haben, wählen Sie dann die Registerkarte Umgebungen und dann Umgebung erstellen aus.
2. Geben Sie auf der Seite Umgebung erstellen Folgendes an und wählen Sie dann Umgebung erstellen aus.

   - Name — geben Sie den Namen für die Umgebung an. Für diese exemplarische Vorgehensweise können Sie ihn `Default data warehouse environment` aufrufen.
   - Beschreibung — Geben Sie eine Beschreibung für die Umgebung an.
   - Umgebungsprofil — wählen Sie das DataWarehouseProfileUmgebungsprofil aus.
   - Geben Sie den Namen Ihres Amazon Redshift Redshift-Clusters, den Datenbanknamen und den geheimen ARN für den Amazon Redshift Redshift-Cluster an, in dem Ihre Daten gespeichert sind.

   > **Note**
   >
   > Stellen Sie sicher, dass Ihr Secret in AWS Secrets Manager die folgenden Tags (Schlüssel/Wert) enthält:
   >
   > - Für Amazon Redshift Redshift-Cluster — datazone.rs.cluster: <cluster_name:database name>
   >
   >   Für Amazon Redshift Serverless Workgroup — datazone.rs.workgroup: <workgroup_name:database_name>
   > - AmazonDataZoneProject: <projectID>

- AmazonDataZoneDomain: <domainID>

Weitere Informationen finden Sie unter Speichern von Datenbankanmeldedaten in AWS Secrets Manager.

Der Datenbankbenutzer, den Sie im AWS Secrets Manager angeben, muss über Superuser-Rechte verfügen.

Schritt 4 — Daten für die Veröffentlichung erstellen

Im folgenden Abschnitt werden die Schritte zur Erstellung von Daten für die Veröffentlichung in diesem Workflow beschrieben.

1. Nachdem Sie Schritt 3 abgeschlossen haben, wählen Sie im DataZone Amazon-Datenportal das `SalesDataPublishingProject` Projekt aus und wählen Sie dann im rechten Bereich unter Analytics-Tools Amazon Redshift aus. Dadurch wird der Amazon Redshift Redshift-Abfrage-Editor geöffnet, der die Anmeldeinformationen Ihres Projekts zur Authentifizierung verwendet.
2. In dieser exemplarischen Vorgehensweise verwenden Sie das CTAS-Abfrageskript (Create Table as Select), um eine neue Tabelle zu erstellen, die Sie auf Amazon veröffentlichen möchten. DataZone Führen Sie dieses CTAS-Skript in Ihrem Abfrage-Editor aus, um eine `mkt_sls_table` Tabelle zu erstellen, die Sie veröffentlichen und für die Suche und das Abonnement zur Verfügung stellen können.

```
CREATE TABLE mkt_sls_table AS
SELECT 146776932 AS ord_num, 23 AS sales_qty_sld, 23.4 AS wholesale_cost, 45.0 as
 lst_pr, 43.0 as sell_pr, 2.0 as disnt, 12 as ship_mode,13 as warehouse_id, 23 as
 item_id, 34 as ctlg_page, 232 as ship_cust_id, 4556 as bill_cust_id
UNION ALL SELECT 46776931, 24, 24.4, 46, 44, 1, 14, 15, 24, 35, 222, 4551
UNION ALL SELECT 46777394, 42, 43.4, 60, 50, 10, 30, 20, 27, 43, 241, 4565
UNION ALL SELECT 46777831, 33, 40.4, 51, 46, 15, 16, 26, 33, 40, 234, 4563
UNION ALL SELECT 46779160, 29, 26.4, 50, 61, 8, 31, 15, 36, 40, 242, 4562
UNION ALL SELECT 46778595, 43, 28.4, 49, 47, 7, 28, 22, 27, 43, 224, 4555
UNION ALL SELECT 46779482, 34, 33.4, 64, 44, 10, 17, 27, 43, 52, 222, 4556
UNION ALL SELECT 46779650, 39, 37.4, 51, 62, 13, 31, 25, 31, 52, 224, 4551
UNION ALL SELECT 46780524, 33, 40.4, 60, 53, 18, 32, 31, 31, 39, 232, 4563
UNION ALL SELECT 46780634, 39, 35.4, 46, 44, 16, 33, 19, 31, 52, 242, 4557
UNION ALL SELECT 46781887, 24, 30.4, 54, 62, 13, 18, 29, 24, 52, 223, 4561
```

Stellen Sie sicher, dass die Tabelle mkt_sls_table erfolgreich erstellt wurde. Jetzt haben Sie ein Datenobjekt, das im DataZone Amazon-Katalog veröffentlicht werden kann.

Schritt 5 — Metadaten aus Amazon Redshift sammeln

Im folgenden Abschnitt werden die Schritte zum Sammeln von Metadaten aus Amazon Redshift beschrieben.

1. Nachdem Sie Schritt 4 abgeschlossen haben, wählen Sie im DataZone Amazon-Datenportal das `SalesDataPublishingProject` Projekt, dann die Registerkarte Daten und dann Datenquellen aus.
2. Wählen Sie die Quelle aus, die im Rahmen der Erstellung der Umgebung erstellt wurde.
3. Wählen Sie neben dem Dropdownmenü „Aktion“ die Option „Ausführen“ und klicken Sie dann auf die Schaltfläche „Aktualisieren“. Sobald der Datenquellenlauf abgeschlossen ist, werden die Assets dem DataZone Amazon-Inventar hinzugefügt.

Schritt 6 — Kuratieren und veröffentlichen Sie das Daten-Asset

Im folgenden Abschnitt werden die Schritte zum Kuratieren und Veröffentlichen des Datenbestands in diesem Workflow beschrieben.

1. Nachdem Sie Schritt 5 abgeschlossen haben, wählen Sie im DataZone Amazon-Datenportal das `SalesDataPublishingProject` Projekt aus, wählen Sie dann die Registerkarte Daten, wählen Sie Inventardaten aus und suchen Sie die `mkt_sls_table` Tabelle.
2. Öffnen Sie die Seite mit den `mkt_sls_table` Asset-Details, um die automatisch generierten Unternehmensnamen zu sehen. Wählen Sie das Symbol Automatisch generierte Metadaten, um die automatisch generierten Namen für Assets und Spalten anzuzeigen. Sie können entweder jeden Namen einzeln akzeptieren oder ablehnen oder Alle akzeptieren wählen, um die generierten Namen zu übernehmen. Optional können Sie Ihrem Asset auch das verfügbare Metadatenformular hinzufügen und Glossarbegriffe auswählen, um Ihre Daten zu klassifizieren.
3. Wählen Sie Veröffentlichen, um das Asset zu veröffentlichen. `mkt_sls_table`

Schritt 7 — Erstellen Sie das Projekt für die Datenanalyse

Im folgenden Abschnitt werden die Schritte zum Erstellen des Projekts für die Datenanalyse in diesem Workflow beschrieben.

1. Nachdem Sie Schritt 6 abgeschlossen haben, wählen Sie im DataZone Amazon-Datenportal die Option Projekt erstellen aus.
2. Geben Sie auf der Seite Projekt erstellen den Projektnamen an, z. B. für diesen Workflow. Sie können ihm einen Namen geben MarketingDataAnalysisProject, dann die restlichen Felder unverändert lassen und dann Create wählen.

Schritt 8 — Erstellen Sie eine Umgebung für die Datenanalyse

Im folgenden Abschnitt werden die Schritte zum Erstellen einer Umgebung für die Datenanalyse in diesem Workflow beschrieben.

1. Nachdem Sie Schritt 7 abgeschlossen haben, wählen Sie im DataZone Amazon-Datenportal das `MarketingDataAnalysisProject` Projekt aus, das Sie im vorherigen Schritt erstellt haben, wählen Sie dann die Registerkarte Umgebungen und dann Umgebung hinzufügen.
2. Geben Sie auf der Seite Umgebung erstellen Folgendes an und wählen Sie dann Umgebung erstellen aus.

   - Name — geben Sie den Namen für die Umgebung an. Für diese exemplarische Vorgehensweise können Sie ihn `Default data warehouse environment` aufrufen.
   - Beschreibung — Geben Sie eine Beschreibung für die Umgebung an.
   - Umgebungsprofil — wählen Sie ein DataWarehouseProfileUmgebungsprofil.
   - Geben Sie den Namen Ihres Amazon Redshift Redshift-Clusters, den Datenbanknamen und den geheimen ARN für den Amazon Redshift Redshift-Cluster an, in dem Ihre Daten gespeichert sind.

   > **Note**
   >
   > Stellen Sie sicher, dass Ihr Secret in AWS Secrets Manager die folgenden Tags (Schlüssel/Wert) enthält:
   >
   > - Für Amazon Redshift Redshift-Cluster — datazone.rs.cluster: <cluster_name:database name>

Für Amazon Redshift Serverless Workgroup — datazone.rs.workgroup: <workgroup_name:database_name>

- AmazonDataZoneProject: <projectID>
- AmazonDataZoneDomain: <domainID>

Weitere Informationen finden Sie unter Speichern von Datenbankanmeldedaten in AWS Secrets Manager.

Der Datenbankbenutzer, den Sie im AWS Secrets Manager angeben, muss über Superuser-Rechte verfügen.

- Lassen Sie für diese exemplarische Vorgehensweise die restlichen Felder unverändert.

Schritt 9: Durchsuchen Sie den Datenkatalog und abonnieren Sie Daten

Im folgenden Abschnitt werden die Schritte zum Durchsuchen des Datenkatalogs und zum Abonnieren von Daten beschrieben.

1. Nachdem Sie Schritt 8 abgeschlossen haben, suchen Sie im DataZone Amazon-Datenportal mithilfe von Schlüsselwörtern (z. B. „Katalog“ oder „Verkauf“) in der Suchleiste des Datenportals nach Datenbeständen.

   Wenden Sie bei Bedarf Filter oder Sortierungen an. Sobald Sie das Asset mit den Produktverkaufsdaten gefunden haben, können Sie es auswählen, um die Detailseite des Assets zu öffnen.
2. Wählen Sie auf der Detailseite des Assets „Produktverkaufsdaten“ die Option Abonnieren aus.
3. Wählen Sie im Dialogfeld Ihr Verbraucherprojekt aus der Dropdownliste aus, geben Sie den Grund für die Zugriffsanfrage an und wählen Sie dann Abonnieren aus.

Schritt 10 — Genehmigen Sie die Abonnementanfrage

Im folgenden Abschnitt werden die Schritte zur Genehmigung der Abonnementanfrage in diesem Workflow beschrieben.

1. Nachdem Sie Schritt 9 abgeschlossen haben, wählen Sie im DataZone Amazon-Datenportal das SalesDataPublishingProjectProjekt aus, mit dem Sie Ihr Asset veröffentlicht haben.
2. Wählen Sie die Registerkarte Daten, dann Veröffentlichte Daten und dann Eingehende Anfragen.

3. Wählen Sie den Link „Anfrage anzeigen“ und dann „Genehmigen“.

Schritt 11 — Erstellen Sie eine Abfrage und analysieren Sie Daten in Amazon Redshift

Nachdem Sie ein Asset erfolgreich im DataZone Amazon-Katalog veröffentlicht und abonniert haben, können Sie es analysieren.

1. Klicken Sie im DataZone Amazon-Datenportal im rechten Bereich auf den Link Amazon Redshift. Dadurch wird der Amazon Redshift Redshift-Abfrage-Editor geöffnet, der die Anmeldeinformationen des Projekts zur Authentifizierung verwendet.
2. Sie können jetzt eine Abfrage (Select-Anweisung) für die abonnierte Tabelle ausführen. Sie können auf die Tabelle klicken (three-vertical-dots Option) und „Vorschau“ wählen, damit die ausgewählte Anweisung auf dem Editor-Bildschirm angezeigt wird. Führen Sie die Abfrage aus, um die Ergebnisse zu sehen.

DataZone Amazon-Schnellstart mit Beispielskripten

Im folgenden Abschnitt werden Beispielskripts beschrieben, die verschiedene DataZone Amazon-APIs aufrufen, mit denen Sie die folgenden Aufgaben ausführen können:

Themen

Erstellen Sie eine DataZone Amazon-Domain und ein Datenportal

Sie können das folgende Beispielskript verwenden, um eine DataZone Amazon-Domain zu erstellen. Weitere Informationen zu DataZone Amazon-Domains finden Sie unter DataZone Amazon-Terminologie und Konzepte.

```
import sys
import boto3

// Initialize datazone client
region = 'us-east-1'
dzclient = boto3.client(service_name='datazone', region_name='us-east-1')

// Create DataZone domain
def create_domain(name):
    return dzclient.create_domain(
        name = name,
        description = "this is a description",
        domainExecutionRole = "arn:aws:iam::<account>:role/
AmazonDataZoneDomainExecutionRole",
    )
```

Erstellen Sie ein Veröffentlichungsprojekt

Sie können das folgende Beispielskript verwenden, um ein Veröffentlichungsprojekt in Amazon zu erstellen DataZone.

```
// Create Project
def create_project(domainId):
    return dzclient.create_project(
        domainIdentifier = domainId,
        name = "sample-project"
    )
```

Erstellen Sie ein Umgebungsprofil

Sie können die folgenden Beispielskripts verwenden, um ein Umgebungsprofil in Amazon zu erstellen DataZone.

Diese Beispielnutzlast wird verwendet, wenn die `CreateEnvironmentProfile` API aufgerufen wird:

```
Sample Payload
{
    "Content":{
        "project_name": "Admin_project",
        "domain_name": "Drug-Research-and-Development",
        "blueprint_account_region": [
            {
                "blueprint_name": "DefaultDataLake",
                "account_id": ["066535990535",
                "413878397724",
                "676266385322",
                "747721550195",
                "755347404384"
                ],
                "region": ["us-west-2", "us-east-1"]
            },
            {
                "blueprint_name": "DefaultDataWarehouse",
                "account_id": ["066535990535",
                "413878397724",
                "676266385322",
                "747721550195",
                "755347404384"
                ],
                "region":["us-west-2", "us-east-1"]
            }
        ]
    }
}
```

Dieses Beispielskript ruft die API auf: `CreateEnvironmentProfile`

```
def create_environment_profile(domain_id, project_id, env_blueprints)
        try:
            response = dz.list_environment_blueprints(
                domainIdentifier=domain_id,
                managed=True
```

```
            )
            env_blueprints = response.get("items")
            env_blueprints_map = {}
            for i in env_blueprints:
                env_blueprints_map[i["name"]] = i['id']

            print("Environment Blueprint map", env_blueprints_map)
            for i in blueprint_account_region:
                print(i)
                for j in i["account_id"]:
                    for k in i["region"]:
                        print("The env blueprint name is", i['blueprint_name'])
                        dz.create_environment_profile(
                            description='This is a test environment profile created via
 lambda function',
                            domainIdentifier=domain_id,
                            awsAccountId=j,
                            awsAccountRegion=k,

 environmentBlueprintIdentifier=env_blueprints_map.get(i["blueprint_name"]),
                            name=i["blueprint_name"] + j + k + "_profile",
                            projectIdentifier=project_id
                        )
        except Exception as e:
            print("Failed to created Environment Profile")
            raise e
```

Dies ist die Beispielausgabe-Payload, sobald die `CreateEnvironmentProfile` API aufgerufen wurde:

```
{
    "Content":{
        "project_name": "Admin_project",
        "domain_name": "Drug-Research-and-Development",
        "blueprint_account_region": [
            {
                "blueprint_name": "DefaultDataWarehouse",
                "account_id": ["111111111111"],
                "region":["us-west-2"],
                "user_parameters":[
                    {
```

```
                        "name": "dataAccessSecretsArn",
                        "value": ""
                    }
                ]
            }
        ]
    }
}
```

Erstellen einer Umgebung

Sie können das folgende Beispielskript verwenden, um eine Umgebung in Amazon zu erstellen DataZone.

```
def create_environment(domain_id, project_id,blueprint_account_region ):
         try:
            #refer to get_domain_id and get_project_id for fetching ids using names.
            sts_client = boto3.client("sts")
            # Get the current account ID
            account_id = sts_client.get_caller_identity()["Account"]
            print("Fetching environment profile ids")
            env_profile_map = get_env_profile_map(domain_id, project_id)

            for i in blueprint_account_region:
                for j in i["account_id"]:
                    for k in i["region"]:
                        print(" env blueprint name", i['blueprint_name'])
                        profile_name = i["blueprint_name"] + j + k + "_profile"
                        env_name = i["blueprint_name"] + j + k + "_env"
                        description = f'This is environment is created for
 {profile_name}, Account {account_id} and region {i["region"]}'
                        try:
                            dz.create_environment(
                                description=description,
                                domainIdentifier=domain_id,

 environmentProfileIdentifier=env_profile_map.get(profile_name),
                                name=env_name,
                                projectIdentifier=project_id
                            )
                            print(f"Environment created - {env_name}")
```

```
                        except:
                            dz.create_environment(
                                description=description,
                                domainIdentifier=domain_id,

 environmentProfileIdentifier=env_profile_map.get(profile_name),
                                name=env_name,
                                projectIdentifier=project_id,
                                userParameters= i["user_parameters"]
                            )
                            print(f"Environment created - {env_name}")
        except Exception as e:
            print("Failed to created Environment")
            raise e
```

Metadaten von AWS Glue sammeln

Sie können dieses Beispielskript verwenden, um Metadaten aus AWS Glue zu sammeln. Dieses Skript wird nach einem Standardzeitplan ausgeführt. Sie können die Parameter aus dem Beispielskript abrufen und sie global machen. Rufen Sie das Projekt, die Umgebung und die Domain-ID mithilfe von Standardfunktionen ab. Die AWS Glue-Datenquelle wird zu einer Standardzeit erstellt und ausgeführt, die im Cron-Abschnitt des Skripts aktualisiert werden kann.

```
def crcreate_data_source(domain_id, project_id,data_source_name)
        print("Creating Data Source")
        data_source_creation = dz.create_data_source(
            # Define data source : Customize the data source to which you'd like to
 connect
            # define the name of the Data source to create, example: name
 ='TestGlueDataSource'
            name=data_source_name,
            # give a description for the datasource (optional), example:
 description='This is a dorra test for creation on DZ datasources'
            description=data_source_description,
            # insert the domain identifier corresponding to the domain to which the
 datasource will belong, example: domainIdentifier= 'dzd_6f3gst5jjmrrmv'
            domainIdentifier=domain_id,
            # give environment identifier , example: environmentIdentifier=
 '3weyt6hhn8qcvb'
            environmentIdentifier=environment_id,
```

```
            # give corresponding project identifier, example: projectIdentifier=
'6tl4csoyrg16ef',
            projectIdentifier=project_id,
            enableSetting="ENABLED",
            # publishOnImport used to select whether assets are added to the inventory
and/or discovery catalog .
            # publishOnImport = True : Assets will be added to project's inventory as
well as published to the discovery catalog
            # publishOnImport = False : Assets will only be added to project's
inventory.
            # You can later curate the metadata of the assets and choose subscription
terms to publish them from the inventory to the discovery catalog.
            publishOnImport=False,
            # Automated business name generation : Use AI to automatically generate
metadata for assets as they are published or updated by this data source run.
            # Automatically generated metadata can be be approved, rejected, or edited
by data publishers.
            # Automatically generated metadata is badged with a small icon next to the
corresponding metadata field.
            recommendation={"enableBusinessNameGeneration": True},
            type="GLUE",
            configuration={
                "glueRunConfiguration": {
                    "dataAccessRole": "arn:aws:iam::"
                    + account_id
                    + ":role/service-role/AmazonDataZoneGlueAccess-"
                    + current_region
                    + "-"
                    + domain_id
                    + "",
                    "relationalFilterConfigurations": [
                        {
                            #
                            "databaseName": glue_database_name,
                            "filterExpressions": [
                                {"expression": "*", "type": "INCLUDE"},
                            ],
                            #    "schemaName": "TestSchemaName",
                        },
                    ],
                },
            },
            # Add metadata forms to the data source (OPTIONAL).
```

```
            # Metadata forms will be automatically applied to any assets that are
 created by the data source.
            # assetFormsInput=[
            #     {
            #         "content": "string",
            #         "formName": "string",
            #         "typeIdentifier": "string",
            #         "typeRevision": "string",
            #     },
            # ],
            schedule={
                "schedule": "cron(5 20 * * ? *)",
                "timezone": "UTC",
            },
        )
        # This is a suggested syntax to return values
        #        return_values["data_source_creation"] = data_source_creation["items"]
        print("Data Source Created")


//This is the sample response payload after the CreateDataSource API is invoked:

{
    "Content":{
        "project_name": "Admin",
        "domain_name": "Drug-Research-and-Development",
        "env_name": "GlueEnvironment",
        "glue_database_name": "test",
        "data_source_name" : "test",
        "data_source_description" : "This is a test data source"
    }
}
```

Kuratieren und veröffentlichen Sie ein Datenobjekt

Sie können die folgenden Beispielskripts verwenden, um Datenbestände in Amazon DataZone zu kuratieren und zu veröffentlichen.

Sie können das folgende Skript verwenden, um benutzerdefinierte Formulartypen zu erstellen:

```
def create_form_type(domainId, projectId):
```

```
    return dzclient.create_form_type(
        domainIdentifier = domainId,
        name = "customForm",
        model = {
            "smithy": "structure customForm { simple: String }"
        },
        owningProjectIdentifier = projectId,
        status = "ENABLED"
    )
```

Sie können das folgende Beispielskript verwenden, um benutzerdefinierte Asset-Typen zu erstellen:

```
def create_custom_asset_type(domainId, projectId):
    return dzclient.create_asset_type(
        domainIdentifier = domainId,
        name = "userCustomAssetType",
        formsInput = {
            "Model": {
                "typeIdentifier": "customForm",
                "typeRevision": "1",
                "required": False
            }
        },
        owningProjectIdentifier = projectId,
    )
```

Sie können das folgende Beispielskript verwenden, um benutzerdefinierte Assets zu erstellen:

```
def create_custom_asset(domainId, projectId):
    return dzclient.create_asset(
        domainIdentifier = domainId,
        name = 'custom asset',
        description = "custom asset",
        owningProjectIdentifier = projectId,
        typeIdentifier = "userCustomAssetType",
        formsInput = [
            {
                "formName": "UserCustomForm",
                "typeIdentifier": "customForm",
```

```
                "content": "{\"simple\":\"sample-catalogId\"}"
            }
        ]
    )
```

Sie können das folgende Beispielskript verwenden, um ein Glossar zu erstellen:

```
def create_glossary(domainId, projectId):
    return dzclient.create_glossary(
        domainIdentifier = domainId,
        name = "test7",
        description = "this is a test glossary",
        owningProjectIdentifier = projectId
    )
```

Sie können das folgende Beispielskript verwenden, um einen Glossarbegriff zu erstellen:

```
def create_glossary_term(domainId, glossaryId):
    return dzclient.create_glossary_term(
        domainIdentifier = domainId,
        name = "soccer",
        shortDescription = "this is a test glossary",
        glossaryIdentifier = glossaryId,
    )
```

Sie können das folgende Beispielskript verwenden, um ein Asset mithilfe eines systemdefinierten Asset-Typs zu erstellen:

```
def create_asset(domainId, projectId):
    return dzclient.create_asset(
        domainIdentifier = domainId,
        name = 'sample asset name',
        description = "this is a glue table asset",
        owningProjectIdentifier = projectId,
        typeIdentifier = "amazon.datazone.GlueTableAssetType",
        formsInput = [
```

```
            {
                "formName": "GlueTableForm",
                "content": "{\"catalogId\":\"sample-catalogId\",\"columns\":
[{\"columnDescription\":\"sample-columnDescription\",\"columnName\":\"sample-
columnName\",\"dataType\":\"sample-dataType\",\"lakeFormationTags\":{\"sample-
key1\":\"sample-value1\",\"sample-key2\":\"sample-value2\"}}],\"compressionType\":
\"sample-compressionType\",\"lakeFormationDetails\":{\"lakeFormationManagedTable
\":false,\"lakeFormationTags\":{\"sample-key1\":\"sample-value1\",\"sample-key2\":
\"sample-value2\"}},\"primaryKeys\":[\"sample-Key1\",\"sample-Key2\"],\"region\":
\"us-east-1\",\"sortKeys\":[\"sample-sortKey1\"],\"sourceClassification\":\"sample-
sourceClassification\",\"sourceLocation\":\"sample-sourceLocation\",\"tableArn\":
\"sample-tableArn\",\"tableDescription\":\"sample-tableDescription\",\"tableName\":
\"sample-tableName\"}"
            }
        ]
    )
```

Sie können das folgende Beispielskript verwenden, um eine Asset-Revision zu erstellen und einen Glossarbegriff anzuhängen:

```
def create_asset_revision(domainId, assetId):
    return dzclient.create_asset_revision(
        domainIdentifier = domainId,
        identifier = assetId,
        name = 'glue table asset 7',
        description = "glue table asset description update",
        formsInput = [
            {
                "formName": "GlueTableForm",
                "content": "{\"catalogId\":\"sample-catalogId\",\"columns\":
[{\"columnDescription\":\"sample-columnDescription\",\"columnName\":\"sample-
columnName\",\"dataType\":\"sample-dataType\",\"lakeFormationTags\":{\"sample-
key1\":\"sample-value1\",\"sample-key2\":\"sample-value2\"}}],\"compressionType\":
\"sample-compressionType\",\"lakeFormationDetails\":{\"lakeFormationManagedTable
\":false,\"lakeFormationTags\":{\"sample-key1\":\"sample-value1\",\"sample-key2\":
\"sample-value2\"}},\"primaryKeys\":[\"sample-Key1\",\"sample-Key2\"],\"region\":
\"us-east-1\",\"sortKeys\":[\"sample-sortKey1\"],\"sourceClassification\":\"sample-
sourceClassification\",\"sourceLocation\":\"sample-sourceLocation\",\"tableArn\":
\"sample-tableArn\",\"tableDescription\":\"sample-tableDescription\",\"tableName\":
\"sample-tableName\"}"
            }
```

```
        ],
        glossaryTerms = ["<glossaryTermId:>"]
    )
```

Sie können das folgende Beispielskript verwenden, um ein Asset zu veröffentlichen:

```
def publish_asset(domainId, assetId):
    return dzclient.create_listing_change_set(
        domainIdentifier = domainId,
        entityIdentifier = assetId,
        entityType = "ASSET",
        action = "PUBLISH",
    )
```

Durchsuchen Sie den Datenkatalog und abonnieren Sie Daten

Sie können die folgenden Beispielskripts verwenden, um den Datenkatalog zu durchsuchen und Daten zu abonnieren:

```
def search_asset(domainId, projectId, text):
    return dzclient.search(
        domainIdentifier = domainId,
        owningProjectIdentifier = projectId,
        searchScope = "ASSET",
        searchText = text,
    )
```

Sie können das folgende Beispielskript verwenden, um die Listing-ID für das Asset abzurufen:

```
def search_listings(domainId, assetName, assetId):
    listings = dzclient.search_listings(
        domainIdentifier=domainId,
        searchText=assetName,
        additionalAttributes=["FORMS"]
    )
```

```
    assetListing = None
    for listing in listings['items']:
        if listing['assetListing']['entityId'] == assetId:
            assetListing = listing

    return listing['assetListing']['listingId']
```

Sie können die folgenden Beispielskripts verwenden, um mithilfe der Listing-ID eine Abonnementanfrage zu erstellen:

```
create_subscription_response = def create_subscription_request(domainId, projectId,
 listingId):
    return dzclient.create_subscription_request(
        subscribedPrincipals=[{
            "project": {
                "identifier": projectId
            }
        }],
        subscribedListings=[{
            "identifier": listingId
        }],
        requestReason="Give request reason here."
    )
```

Rufen Sie mithilfe der `create_subscription_response` obigen Anweisungen das `subscription_request_id` Abonnement ab und akzeptieren/genehmigen Sie es anschließend mithilfe des folgenden Beispielskripts:

```
subscription_request_id = create_subscription_response["id"]

def accept_subscription_request(domainId, subscriptionRequestId):
    return dzclient.accept_subscription_request(
        domainIdentifier=domainId,
        identifier=subscriptionRequestId
    )
```

Andere nützliche Beispielskripte

Sie können die folgenden Beispielskripts verwenden, um verschiedene Aufgaben zu erledigen, während Sie mit Ihren Daten in Amazon arbeiten DataZone.

Verwenden Sie das folgende Beispielskript, um bestehende DataZone Amazon-Domains aufzulisten:

```
def list_domains():
    datazone = boto3.client('datazone')
    response = datazone.list_domains(status='AVAILABLE')
    [print("%12s | %16s | %12s | %52s" % (item['id'], item['name'],
 item['managedAccountId'], item['portalUrl'])) for item in response['items']]
    return
```

Verwenden Sie das folgende Beispielskript, um bestehende DataZone Amazon-Projekte aufzulisten:

```
def list_projects(domain_id):
    datazone = boto3.client('datazone')
    response = datazone.list_projects(domainIdentifier=domain_id)
    [print("%12s | %16s " % (item['id'], item['name'])) for item in response['items']]
    return
```

Verwenden Sie das folgende Beispielskript, um bestehende DataZone Amazon-Metadatenformulare aufzulisten:

```
def list_metadata_forms(domain_id):
    datazone = boto3.client('datazone')
    response = datazone.search_types(domainIdentifier=domain_id,
        managed=False,
        searchScope='FORM_TYPE')
    [print("%16s | %16s | %3s | %8s" % (item['formTypeItem']['name'],
 item['formTypeItem']['owningProjectId'],item['formTypeItem']['revision'],
 item['formTypeItem']['status'])) for item in response['items']]
    return
```

Verwaltung von DataZone Amazon-Domains und Benutzerzugriff

Themen

Domains erstellen

> **Note**
>
> Wenn Sie Amazon DataZone mit AWS Identity Center verwenden, um SSO-Benutzern und -Gruppen Zugriff zu gewähren, muss sich Ihre DataZone Amazon-Domain derzeit in derselben AWS Region wie Ihre AWS Identity Center-Instance befinden.

Amazon DataZone, eine Domain, ist eine Organisationseinheit, die Ihre Ressourcen, Benutzer und deren Projekte miteinander verbindet. Weitere Informationen finden Sie unter DataZone Amazon-Terminologie und Konzepte.

Um eine DataZone Amazon-Domain zu erstellen, müssen Sie eine IAM-Rolle im Konto mit Administratorberechtigungen annehmen. Konfigurieren Sie die IAM-Berechtigungen, die für die Nutzung der Amazon DataZone Management Console erforderlich sindum die Mindestberechtigungen zu erhalten, die für die Erstellung einer Domain erforderlich sind.

Zusätzliche IAM-Rollen werden von Amazon benötigt DataZone , um Aktionen im Namen von Domain-Benutzern mit einer Standardkonfiguration durchzuführen. Sie können diese IAM-Rollen im Voraus erstellen oder sie von Amazon für Sie DataZone erstellen lassen. Wenn Sie

möchten DataZone , dass Amazon diese IAM-Rollen während des Domainerstellungsprozesses für Sie erstellt, müssen Sie für die Domainerstellung eine IAM-Rolle mit Berechtigungen zur Rollenerstellung annehmen. Siehe Erstellen Sie eine benutzerdefinierte Richtlinie für IAM-Berechtigungen, um die vereinfachte Rollenerstellung über die Amazon DataZone Service Console zu ermöglichen . Abhängig von Ihren Optionen zur Domainerstellung erstellt Amazon DataZone bis zu vier neue IAM-Rollen für Sie: AmazonDataZoneDomainExecutionRole, AmazonDataZoneGlueManageAccessRoleAmazonDataZoneRedshiftManageAccessRole, und AmazonDataZoneProvisioningRole.

Gehen Sie wie folgt vor, um eine DataZone Amazon-Domain zu erstellen.

1. Navigieren Sie zur DataZone Amazon-Konsole unter https://console.aws.amazon.com/datazone und wählen Sie mit der Regionsauswahl in der oberen Navigationsleiste die entsprechende AWS Region aus.
2. Wählen Sie Create Domain und geben Sie Werte für die folgenden Felder ein:

   - Name — geben Sie einen benutzerfreundlichen Namen für die Domain an. Sobald die Domain erstellt wurde, kann dieser Name nicht mehr geändert werden.
   - Beschreibung — (optional) geben Sie eine Domainbeschreibung an.
   - Datenverschlüsselung — Ihre DataZone Amazon-Domain, Metadaten und Berichtsdaten werden vom AWS Key Management Service (KMS) mit einem für Ihr Amazon spezifischen Schlüssel verschlüsselt DataZone. Verwenden Sie dieses Feld, um anzugeben, ob Sie einen AWS eigenen Schlüssel verwenden oder einen anderen AWS KMS-Schlüssel wählen möchten.

     Weitere Informationen zur Verwendung von kundenverwalteten Schlüsseln finden Sie unterDatenverschlüsselung im Ruhezustand für Amazon DataZone. Wenn Sie Ihren eigenen KMS-Schlüssel für die Datenverschlüsselung verwenden, müssen Sie die folgende Anweisung in Ihre Standardeinstellung aufnehmenAmazonDataZoneDomainExecutionRole.

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Sid": "Statement1",
      "Effect": "Allow",
      "Action": [
        "kms:Decrypt",
```

```
        "kms:DescribeKey",
        "kms:GenerateDataKey"
      ],
      "Resource": [
        "*"
      ]
    }
  ]
}
```

- Servicezugriff — wählen Sie aus, ob Amazon eine neue DomainExecutionRolefür Sie DataZone erstellen und verwenden soll, oder wählen Sie eine bestehende IAM-Rolle.
- Schnelle Einrichtung — (optional) Markieren Sie dieses Kästchen, um schneller loszulegen, indem Sie Amazon Ihr Konto für den Datenverbrauch und die Veröffentlichung DataZone einrichten lassen. Amazon DataZone wird drei IAM-Rollen für die Bereitstellung, Aufnahme und Verwaltung des Zugriffs auf AWS Glue- und Amazon Redshift Redshift-Ressourcen einrichten, einen neuen Amazon S3 S3-Bucket erstellen, ein administratives DataZone Amazon-Projekt erstellen und Umgebungsprofile für die Standard-Blueprints von Data Lake und Data Warehouse erstellen.
- Tags — (optional) geben Sie AWS Tags (Schlüssel- und Wertepaare) für die Domain an.
- Sobald die Domain erfolgreich erstellt wurde, sollte Ihr Browser aktualisiert werden, sodass die Detailseite Ihrer neuen DataZone Amazon-Domain angezeigt wird.

Domains bearbeiten

Bei Amazon ist eine Domain eine Organisationseinheit DataZone, die Ihre Ressourcen, Benutzer und deren Projekte miteinander verbindet. Weitere Informationen finden Sie unter DataZone Amazon-Terminologie und Konzepte.

Nachdem Sie eine DataZone Amazon-Domain erstellt haben, können Sie die Domain später bearbeiten, um: die Beschreibung zu ändern, IAM Identity Center zu aktivieren und Tag-Schlüssel und deren Werte hinzuzufügen, zu bearbeiten oder zu entfernen. Um eine DataZone Amazon-Domain zu bearbeiten, müssen Sie eine IAM-Rolle in dem Konto mit Administratorberechtigungen annehmen. Konfigurieren Sie die IAM-Berechtigungen, die für die Nutzung der Amazon DataZone Management Console erforderlich sindum die Mindestberechtigungen zu erhalten, die für die Bearbeitung einer Domain erforderlich sind.

Gehen Sie wie folgt vor, um eine Domain zu bearbeiten:

1. Melden Sie sich bei der AWS Management Console an und öffnen Sie die DataZone Amazon-Konsole unter https://console.aws.amazon.com/datazone.
2. Wählen Sie Domains anzeigen und wählen Sie den Namen der Domain aus der Liste aus. Der Name ist ein Hyperlink.
3. Wählen Sie auf der Detailseite für die Domain die Option Bearbeiten aus.
4.
   - Bearbeiten Sie die Beschreibung.
   - Legen Sie die IAM Identity Center-Einstellungen fest. Weitere Informationen zu diesen Einstellungen finden Sie unterAWS IAM Identity Center für Amazon einrichten DataZone.
   - Tag-Schlüssel und ihre Werte hinzufügen, bearbeiten oder entfernen.
5. Sobald Sie Ihre Änderungen vorgenommen haben, wählen Sie Domain aktualisieren.

Domains löschen

Bei Amazon ist eine Domain eine Organisationseinheit DataZone, die Ihre Ressourcen, Benutzer und deren Projekte miteinander verbindet. Weitere Informationen finden Sie unter DataZone Amazon-Terminologie und Konzepte.

Das Löschen einer Domain ist endgültig. Durch das Löschen werden alle DataZone Amazon-Entitäten unwiderruflich entfernt, einschließlich Datenquellen, Projekte, Umgebungen, Ressourcen, Glossare und Metadatenformulare. Durch das Löschen werden keine DataZone AWS Ressourcen gelöscht, die nicht zu Amazon gehören und bei deren Erstellung Amazon Ihnen DataZone möglicherweise geholfen hat, wie IAM-Rollen, S3-Buckets, AWS Glue-Datenbanken und Abonnementzuschüsse über LakeFormation oder Redshift. Wenn Sie diese Ressourcen nicht mehr benötigen, löschen Sie sie im jeweiligen Service. AWS

Um zu verhindern, dass jemand eine Domain böswillig löscht, erfordert das Löschen einer Domain administrative IAM-Berechtigungen für Amazon DataZone, die Sie mit IAM konfigurieren können. Um zu verhindern, dass jemand versehentlich eine Domain löscht, erfordert das Löschen einer Domain ein Bestätigungswort (in der DataZone Amazon-Konsole).

Gehen Sie wie folgt vor, um eine Domain zu löschen:

1. Melden Sie sich bei der AWS Management Console an und öffnen Sie die DataZone Amazon-Konsole unter https://console.aws.amazon.com/datazone.

2. Wählen Sie Domains anzeigen und wählen Sie den Namen der Domain aus der Liste aus. Der Name ist ein Hyperlink.
3. Wählen Sie Löschen und überprüfen Sie die Informationswarnungen.
4. Geben Sie den angeforderten Text ein, um zu bestätigen, dass Sie diese Warnungen verstanden haben. Wählen Sie Löschen aus.

Important

Das Löschen Ihrer Domain ist eine unwiderrufliche Aktion, die weder von Ihnen noch von rückgängig gemacht werden kann. AWS

Note

Wenn Sie oder Ihre Domain-Benutzer eine Umgebung in einem Projekt erstellen, DataZone erstellt Amazon AWS Ressourcen in Ihrer Domain oder den zugehörigen Konten, um Ihnen und Ihren Domain-Benutzern Funktionen zur Verfügung zu stellen. Unten finden Sie eine Liste der AWS Ressourcen, die Amazon für Projekte in Ihrer Domain erstellen DataZone kann, zusammen mit dem Standardnamen. Durch das Löschen einer Domain werden keine dieser AWS Ressourcen in Ihren AWS Konten gelöscht.

- <environmentId>IAM-Rollen: datazone_usr_.
- <environmentName>Glue-Datenbanken: (1) <environmentName>_pub_db-*, (2) _sub_db-*. Wenn es bereits eine Datenbank mit diesem Namen gab, DataZone fügt Amazon die Umgebungs-ID hinzu.
- <environmentName>Athena-Arbeitsgruppen: -*. Wenn es bereits eine Arbeitsgruppe mit diesem Namen gab, fügt Amazon DataZone die Umgebungs-ID hinzu.
- CloudWatch Protokollgruppe: datazone_ <environmentId>

IAM Identity Center für Amazon aktivieren DataZone

> **Note**
>
> Um dieses Verfahren abzuschließen, muss AWS IAM Identity Center in derselben AWS Region wie Ihre DataZone Amazon-Domain aktiviert sein.

Mithilfe von AWS IAM Identity Center können Sie SSO-Benutzern und -Gruppen Zugriff auf Ihr DataZone Amazon-Datenportal gewähren. Nach Abschluss AWS IAM Identity Center für Amazon einrichten DataZone können Sie Ihren SSO-Benutzern und -Gruppen den Zugriff auf Ihr DataZone Amazon-Domain-Datenportal ermöglichen.

Um AWS IAM Identity Center für die Verwendung mit Ihrer DataZone Amazon-Domain zu aktivieren, müssen Sie eine IAM-Rolle in dem Konto mit Administratorberechtigungen annehmen. Konfigurieren Sie die IAM-Berechtigungen, die für die Nutzung der Amazon DataZone Management Console erforderlich sindund Erstellen Sie eine benutzerdefinierte Richtlinie für IAM-Berechtigungen, um die vereinfachte Rollenerstellung über die Amazon DataZone Service Console zu ermöglichen um die Mindestberechtigungen zu erhalten, die erforderlich sind, um IAM Identity Center für die Verwendung mit Amazon DataZone zu aktivieren.

Gehen Sie wie folgt vor, um das AWS IAM Identity Center für Amazon DataZone zu aktivieren.

1. Melden Sie sich bei der AWS Management Console an und öffnen Sie die DataZone Konsole unter https://console.aws.amazon.com/datazone.
2. Wählen Sie Domains anzeigen und wählen Sie den Namen der Domain aus der Liste aus. Der Name ist ein Hyperlink.
3. Wählen Sie auf der Detailseite der Domain die Option Bearbeiten aus.
    - Aktivieren Sie das Kontrollkästchen für Benutzer in IAM Identity Center aktivieren.
    - Wählen Sie zwischen den beiden Benutzerzuweisungsmodi. Sobald Ihre Domain mit Ihrer Auswahl aktualisiert wurde, kann sie später nicht mehr geändert werden.
        - Mit der impliziten Benutzerzuweisung kann jeder Benutzer, der zu Ihrem IAM Identity Center-Verzeichnis hinzugefügt wurde, auf Ihre DataZone Amazon-Domain zugreifen.
        - Mit der expliziten Benutzerzuweisung fügen Sie bestimmte Benutzer oder Gruppen aus Ihrem IAM Identity Center-Verzeichnis hinzu, um ihnen Zugriff auf Ihre DataZone Amazon-

Domain zu gewähren. Sie werden diese Benutzer und Gruppen später in der DataZone Amazon-Konsole hinzufügen und entfernen.

4. Wenn Sie mit Ihrer Auswahl zufrieden sind, wählen Sie Domain aktualisieren.

IAM Identity Center für Amazon deaktivieren DataZone

Durch die Deaktivierung von AWS IAM Identity Center für eine DataZone Amazon-Domain wird der Zugriff für alle SSO-Benutzer aufgehoben.

> **Note**
>
> Durch die Deaktivierung von IAM Identity Center wird die Abrechnung für SSO-Benutzer nicht beendet. Um die Abrechnung für SSO-Benutzer zu beenden, müssen Sie sie in Ihrer Domain deaktivieren. Die Abrechnung dauert bis zum Ende des Monats, in dem ein Benutzer deaktiviert wird. Informationen zum Deaktivieren von Benutzern finden Sie unterBenutzer in der DataZone Amazon-Konsole verwalten.

Mithilfe von AWS IAM Identity Center können Sie SSO-Benutzern und -Gruppen Zugriff auf Ihr DataZone Amazon-Datenportal gewähren. Wenn Sie AWS IAM Identity Center für Amazon aktiviert haben DataZone, können Sie später den Zugriff für alle Benutzer deaktivieren.

Um AWS IAM Identity Center für die Verwendung mit Ihrer DataZone Amazon-Domain zu deaktivieren, müssen Sie eine IAM-Rolle in dem Konto mit Administratorberechtigungen annehmen. Konfigurieren Sie die IAM-Berechtigungen, die für die Nutzung der Amazon DataZone Management Console erforderlich sindund Erstellen Sie eine benutzerdefinierte Richtlinie für IAM-Berechtigungen, um die vereinfachte Rollenerstellung über die Amazon DataZone Service Console zu ermöglichen um die Mindestberechtigungen zu erhalten, die erforderlich sind, um die Verwendung von IAM Identity Center mit Amazon DataZone zu deaktivieren.

Gehen Sie wie folgt vor, um das AWS IAM Identity Center für Amazon DataZone zu deaktivieren.

1. Melden Sie sich bei der AWS Management Console an und öffnen Sie die DataZone Konsole unter https://console.aws.amazon.com/datazone.
2. Wählen Sie Domains anzeigen und wählen Sie den Namen der Domain aus der Liste aus. Der Name ist ein Hyperlink.

3. <regionName><accountId><domainName>Kopieren Sie den Amazon-Ressourcennamen (ARN) für Ihre Domain, der mit arn:aws:datazone: ::domain/ beginnt.
4. Öffnen Sie die IAM Identity Center-Konsole unter https://console.aws.amazon.com/singlesignon/.
5. Wählen Sie Applications (Anwendungen).
6. Wählen Sie die Domain aus, für die Sie AWS IAM Identity Center deaktivieren möchten. Dadurch wird allen SSO-Benutzern der Zugriff auf das Datenportal der Domain entzogen. Sie können das Menü Filter und das Suchfeld verwenden, um die Liste der Anwendungen zu filtern.
7. Wählen Sie im Menü Aktionen die Option Deaktivieren.
8. SSO-Benutzer verlieren den Zugriff auf die DataZone Amazon-Domain.
9. Um AWS IAM Identity Center für die DataZone Amazon-Domain erneut zu aktivieren, wählen Sie die Domain aus, für die Sie AWS IAM Identity Center erneut aktivieren möchten, und klicken Sie im Menü Aktionen auf Aktivieren.

Benutzer in der DataZone Amazon-Konsole verwalten

Ihre Benutzer können entweder mit ihren AWS Anmeldeinformationen oder mit Single Sign-On (SSO) -Anmeldeinformationen auf das DataZone Amazon-Datenportal zugreifen. Um Benutzer in der DataZone Amazon-Konsole für eine DataZone Amazon-Domain zu verwalten, müssen Sie eine IAM-Rolle im Konto mit Administratorberechtigungen annehmen. Konfigurieren Sie die IAM-Berechtigungen, die für die Nutzung der Amazon DataZone Management Console erforderlich sindum die Mindestberechtigungen zu erhalten, die für die Verwaltung von Benutzern in der DataZone Amazon-Konsole erforderlich sind.

Themen

- IAM-Rollen und -Benutzer verwalten
- SSO-Benutzer verwalten
- SSO-Gruppen verwalten

IAM-Rollen und -Benutzer verwalten

IAM-Rollen und -Benutzer werden mithilfe von AWS Identity and Access Management (IAM) erstellt und erhalten Zugriff auf Ihre DataZone Amazon-Domains über Berechtigungen, die ihnen über Richtlinien zugewiesen sind. Weitere Informationen finden Sie unter Konfigurieren Sie die IAM-Berechtigungen, die für die Nutzung des DataZone Amazon-Datenportals erforderlich sind. Sie

können die Liste der IAM-Rollen und -Benutzer einsehen, die ihr DataZone Amazon-Domain-Abonnement aktiviert haben, ihren Zugriff deaktivieren und ihren Zugriff aktivieren, falls er zuvor deaktiviert wurde.

1. Melden Sie sich bei der AWS Management Console an und öffnen Sie die DataZone Konsole unter https://console.aws.amazon.com/datazone.
2. Wählen Sie Domains anzeigen und wählen Sie den Namen der Domain aus der Liste aus. Der Name ist ein Hyperlink.
3. Wählen Sie auf der Detailseite für die Domain die Option Benutzerverwaltung aus.
4. Wählen Sie als Benutzertyp IAM-Benutzer aus, um die aktuelle Liste der aktivierten und deaktivierten IAM-Benutzer und -Rollen anzuzeigen.
   - In der Spalte Name wird der ARN des IAM-Benutzers oder der IAM-Rolle angezeigt.
   - In der Spalte Status wird der aktuelle Status des IAM-Benutzers oder der IAM-Rolle in der Domäne angezeigt.
     - Aktiviert bedeutet, dass der IAM-Benutzer oder die IAM-Rolle eine API aufgerufen, einen Befehl (über die Befehlszeilenschnittstelle) ausgegeben oder auf das DataZone Amazon-Portal für Ihre Domain zugegriffen hat und Ihnen das Abonnement des Benutzers in Rechnung gestellt wird.
     - Deaktiviert bedeutet, dass der Zugriff des IAM-Benutzers oder der IAM-Rolle auf Ihre DataZone Amazon-Domain gesperrt ist.
5. Um einen aktuell aktivierten IAM-Benutzer oder eine IAM-Rolle zu deaktivieren, markieren Sie das Kästchen neben dem Benutzer und wählen Sie im Menü Aktionen die Option Deaktivieren aus. Der Benutzer verliert den Zugriff auf die DataZone Amazon-Domain. Die Abrechnung für den Benutzer endet am Ende des aktuellen Kalendermonats.
6. Um einen aktuell deaktivierten IAM-Benutzer oder eine IAM-Rolle zu aktivieren, klicken Sie das Kästchen neben dem Benutzer an und wählen Sie im Menü Aktionen die Option Aktivieren aus. Der Benutzer erhält Zugriff auf die DataZone Amazon-Domain, wenn der IAM-Benutzer oder die IAM-Rolle über die entsprechenden Berechtigungen verfügt. Die Abrechnung für den Benutzer beginnt erneut.

SSO-Benutzer verwalten

SSO-Benutzer werden in AWS IAM Identity Center erstellt oder mit Ihrem Identitätsanbieter synchronisiert. Weitere Informationen finden Sie unter AWS IAM Identity Center für Amazon

einrichten DataZone und IAM Identity Center für Amazon aktivieren DataZone zur Aktivierung und Konfiguration von AWS IAM Identity Center für Amazon DataZone. Sie können die Liste der SSO-Benutzer anzeigen, die der Domain zugewiesen sind, SSO-Benutzer hinzufügen und SSO-Benutzer entfernen.

1. Melden Sie sich bei der AWS Management Console an und öffnen Sie die DataZone Konsole unter https://console.aws.amazon.com/datazone.
2. Wählen Sie Domains anzeigen und wählen Sie den Namen der Domain aus der Liste aus. Der Name ist ein Hyperlink.
3. Scrollen Sie auf der Detailseite für die Domain nach unten und wählen Sie Benutzerverwaltung aus.
4. Wählen Sie als Benutzertyp die Option SSO-Benutzer aus, um die aktuelle Liste der SSO-Benutzer anzuzeigen.

   - In der Spalte Name wird der Name des SSO-Benutzers angezeigt.
   - In der Spalte Status wird der aktuelle Status des SSO-Benutzers in der Domain angezeigt.
     - Zugewiesen bedeutet, dass der SSO-Benutzer der Domain explizit zugewiesen wurde. Dadurch hat der Benutzer Zugriff auf Amazon DataZone. Dieser Status wird nur verwendet, wenn der Identity-Provider-Modus Ihrer Domain auf explizite Zuweisung eingestellt ist.
     - Aktiviert bedeutet, dass der SSO-Benutzer auf das DataZone Amazon-Portal für die Domain zugegriffen hat und Ihnen das Abonnement des Benutzers in Rechnung gestellt wird. Die Aktivierung erfolgt automatisch.
     - Deaktiviert bedeutet, dass der Zugriff des SSO-Benutzers auf das Datenportal der Domain gesperrt ist. Die Abrechnung für den Benutzer endete am Ende des Monats, in dem sein Zugang deaktiviert wurde.
     - Entfernt bedeutet, dass der SSO-Benutzer der Domain zuvor zugewiesen, aber entfernt wurde, bevor er überhaupt darauf zugegriffen hat.
5. Fügen Sie SSO-Benutzer hinzu, indem Sie Hinzufügen und Benutzer hinzufügen wählen. Diese Option ist nicht verfügbar, wenn die Domain auf implizite Benutzerzuweisung eingestellt ist, was bedeutet, dass alle Benutzer im Identitätspool Zugriff auf die DataZone Amazon-Domain haben.

   - Suchen Sie auf der Seite Benutzer hinzufügen nach den Aliasnamen der Benutzer, die Sie hinzufügen möchten. Unter dem Suchfeld wird eine Liste mit möglichen Treffern angezeigt.
   - Wählen Sie den Benutzer aus, den Sie hinzufügen möchten. Ihr Alias wird als Chip unter dem Suchfeld angezeigt.

- Wenn Sie mit der Liste der Benutzer, die Sie hinzufügen möchten, zufrieden sind, wählen Sie Benutzer hinzufügen.
- Die Benutzer werden der DataZone Amazon-Domain mit dem Status Zugewiesen zugewiesen.
- Wenn der Benutzer zum ersten Mal auf das Datenportal der Domain zugegriffen hat, ändert sich der Status automatisch in Aktiviert, und Ihnen wird das Abonnement des Benutzers in Rechnung gestellt.

6. Entfernen Sie einen zugewiesenen SSO-Benutzer, indem Sie den Benutzer auswählen und im Menü Aktionen die Option Deaktivieren wählen. Infolgedessen verliert der Benutzer den Zugriff auf die DataZone Amazon-Domain. Der Status des Benutzers wird als Entfernt angezeigt. Diese Option ist nicht verfügbar, wenn die Domäne auf implizite Benutzerzuweisung eingestellt ist.
7. Deaktivieren Sie einen aktivierten SSO-Benutzer, indem Sie den Benutzer auswählen und im Menü Aktionen die Option Deaktivieren wählen. Infolgedessen geht der Zugriff des Benutzers auf die DataZone Amazon-Domain verloren und wird blockiert. Die Abrechnung für das Abonnement des Benutzers wird bis Ende des Monats fortgesetzt. Der Status des Benutzers wird als Deaktiviert angezeigt.
8. Aktivieren Sie einen deaktivierten SSO-Benutzer, indem Sie den Benutzer auswählen und im Menü Aktionen die Option Aktivieren wählen. Dadurch erhält der Benutzer wieder Zugriff auf die DataZone Amazon-Domain. Die Abrechnung beginnt sofort. Die des Benutzers wird als Aktiviert angezeigt.

SSO-Gruppen verwalten

SSO-Gruppen werden in AWS IAM Identity Center erstellt oder mit Ihrem Identitätsanbieter synchronisiert. Weitere Informationen finden Sie unter AWS IAM Identity Center für Amazon einrichten DataZone und IAM Identity Center für Amazon aktivieren DataZone zur Aktivierung und Konfiguration von AWS IAM Identity Center für Amazon DataZone. Sie können die Liste der SSO-Gruppen anzeigen, die der Domain zugewiesen sind, SSO-Gruppen hinzufügen und SSO-Gruppen entfernen.

1. Melden Sie sich bei der AWS Management Console an und öffnen Sie die DataZone Konsole unter https://console.aws.amazon.com/datazone.
2. Wählen Sie Domains anzeigen und wählen Sie den Namen der Domain aus der Liste aus. Der Name ist ein Hyperlink.
3. Scrollen Sie auf der Detailseite für die Domain nach unten und wählen Sie Benutzerverwaltung aus.

4. Wählen Sie als Benutzertyp SSO-Gruppen aus, um die aktuelle Liste der SSO-Gruppen anzuzeigen.

   - In der Spalte Name wird der Name der SSO-Gruppe angezeigt.
   - In der Spalte Status wird der aktuelle Status der SSO-Gruppe in der Domain angezeigt.
     - Zugewiesen bedeutet, dass die SSO-Gruppe der Domain explizit zugewiesen wurde. Dadurch haben alle Benutzer in der Gruppe Zugriff auf das Datenportal der Domain (sofern der Benutzer nicht deaktiviert ist).
     - Nicht zugewiesen bedeutet, dass die SSO-Gruppe aus der Domain entfernt wurde. Benutzer in der Gruppe haben über ihre Mitgliedschaft in dieser Gruppe keinen Zugriff auf das Datenportal der Domain.
5. Fügen Sie SSO-Gruppen hinzu, indem Sie Hinzufügen und Gruppen hinzufügen auswählen. Diese Option ist nicht verfügbar, wenn die Domain auf implizite Benutzerzuweisung eingestellt ist, was bedeutet, dass alle Benutzer im Identitätspool unabhängig von ihrer Gruppenmitgliedschaft Zugriff auf die DataZone Amazon-Domain haben.

   - Suchen Sie auf der Seite Gruppen hinzufügen nach den Aliasnamen der Gruppen, die Sie hinzufügen möchten. Unter dem Suchfeld wird eine Liste mit möglichen Treffern angezeigt.
   - Wählen Sie die Gruppe aus, die Sie hinzufügen möchten. Ihr Alias wird als Chip unter dem Suchfeld angezeigt.
   - Wenn Sie mit der Liste der Gruppen, die Sie hinzufügen möchten, zufrieden sind, wählen Sie Gruppe (n) hinzufügen.
   - Die Gruppen werden der DataZone Amazon-Domain mit dem Status Zugewiesen zugewiesen.
   - Wenn ein Mitglied der Gruppe auf das Datenportal der Domain zugreift, ändert sich der Status automatisch in Aktiviert, und Ihnen wird das Abonnement des Benutzers in Rechnung gestellt.
6. Entfernen Sie eine zugewiesene SSO-Gruppe, indem Sie die Gruppe auswählen und im Menü Aktionen die Option Zuweisung aufheben wählen. Infolgedessen verliert die Gruppe den Zugriff auf die DataZone Amazon-Domain. Der Status der Gruppe wird als Nicht zugewiesen angezeigt. Benutzer, die ihren Zugriff auf Amazon DataZone über ihre Mitgliedschaft in dieser Gruppe erhalten haben, verlieren den Zugriff. Diese Option ist nicht verfügbar, wenn die Domain auf implizite Benutzerzuweisung eingestellt ist. Um die Abrechnung für Benutzer zu beenden, deren Zugriff durch Aufheben der Gruppenzuweisung aufgehoben wurde, müssen Sie als Nächstes ihre Benutzerprofile manuell auswählen und deaktivieren.

Benutzerberechtigungen im DataZone Amazon-Datenportal verwalten

In der aktuellen Version von Amazon DataZone ermöglicht der Standard-Autorisierungsmechanismus allen authentifizierten Benutzern (IAM und SSO) der DataZone Amazon-Domains, Projekte zu erstellen, Entitäten innerhalb der Projekte zu erstellen und Suchen durchzuführen. Die Projektmitglieder müssen sich weiterhin an die Berechtigungen halten, die ihnen in den Rollen als Projekteigentümer oder Projektmitwirkender erteilt wurden.

Arbeiten mit den DataZone integrierten Blueprints von Amazon

Ein Blueprint, mit dem eine Umgebung erstellt wird, definiert, welche Tools und Dienste Mitglieder des Projekts, zu dem die Umgebung gehört, verwenden können, wenn sie mit Ressourcen im DataZone Amazon-Katalog arbeiten. In der aktuellen Version von Amazon DataZone gibt es die folgenden integrierten Blueprints:

- Bauplan für einen Data Lake
- Bauplan für ein Data Warehouse
- SageMaker Amazon-Entwurf

Themen

Aktivieren Sie integrierte Blueprints in dem AWS Konto, dem die DataZone Amazon-Domain gehört

Ein Blueprint, mit dem eine Umgebung erstellt wird, definiert, welche Tools und Dienste Mitglieder des Projekts, zu dem die Umgebung gehört, verwenden können, wenn sie mit Ressourcen im DataZone Amazon-Katalog arbeiten.

In der aktuellen Version von Amazon DataZone gibt es mehrere integrierte Blueprints: Data Lake-Blueprint, Data Warehouse-Blueprint und Amazon-Blueprint. SageMaker

- Der Data Lake-Blueprint enthält die Definition für den Start und die Konfiguration einer Reihe von Diensten (AWS Glue, AWS Lake Formation, Amazon Athena) zur Veröffentlichung und Verwendung von Data Lake-Assets im DataZone Amazon-Katalog.
- Der Data Warehouse-Blueprint enthält die Definition für den Start und die Konfiguration einer Reihe von Diensten (Amazon Redshift) zur Veröffentlichung und Verwendung von Amazon Redshift Redshift-Assets im Amazon-Katalog. DataZone

- Amazon SageMaker Blueprint enthält die Definition für den Start und die Konfiguration einer Reihe von Diensten (Amazon SageMaker Studio) zur Veröffentlichung und Verwendung von SageMaker Amazon-Ressourcen im DataZone Amazon-Katalog.

Weitere Informationen finden Sie unter DataZone Amazon-Terminologie und Konzepte.

Bei der Erstellung einer DataZone Amazon-Domain haben Sie die Möglichkeit, das Schnell-Setup zu wählen, das automatisch den Standard-Data Lake und die integrierten Standard-Data Warehouse-Blueprints als Teil des Domain-Erstellungsprozesses aktiviert. Quick Setup erstellt mithilfe dieser integrierten Blueprints auch Standardumgebungsprofile und Standardumgebungen für Sie.

Wenn Sie bei der Erstellung Ihrer DataZone Amazon-Domain nicht die Option Schnelleinrichtung wählen, können Sie wie folgt vorgehen, um die verfügbaren integrierten Blueprints in dem AWS Konto zu aktivieren, das diese DataZone Amazon-Domain beherbergt. Sie müssen diese integrierten Blueprints aktivieren, bevor Sie sie verwenden können, um Umgebungsprofile und Umgebungen in dieser Domain zu erstellen.

Um integrierte Blueprints in einer DataZone Amazon-Domain über die DataZone Amazon-Managementkonsole zu aktivieren, müssen Sie eine IAM-Rolle in dem Konto mit Administratorberechtigungen annehmen. Konfigurieren Sie die IAM-Berechtigungen, die für die Nutzung der Amazon DataZone Management Console erforderlich sindum die Mindestberechtigungen zu erhalten.

Integrierte Blueprints in einer DataZone Amazon-Domain aktivieren

1. Rufen Sie die DataZone Amazon-Konsole unter https://console.aws.amazon.com/datazone auf und melden Sie sich mit Ihren Kontoanmeldeinformationen an.
2. Wählen Sie Domains anzeigen und wählen Sie die Domain aus, für die Sie einen oder mehrere integrierte Blueprints aktivieren möchten.
3. Navigieren Sie auf der Seite mit den Domain-Details zur Registerkarte Blueprints.
4. Wählen Sie aus der Blueprint-Liste entweder den DefaultDataLakeoder den oder den DefaultDataWarehouse SageMakerAmazon-Blueprint aus.
5. Wählen Sie auf der Detailseite des ausgewählten Blueprints die Option In diesem Konto aktivieren aus.
6. Geben Sie auf der Seite „Berechtigungen und Ressourcen“ Folgendes an:

    - Wenn Sie den DefaultDataLakeBlueprint aktivieren, geben Sie für die Rolle Glue Manage Access eine neue oder bestehende Servicerolle an, die Amazon die DataZone Autorisierung

erteilt, den Zugriff auf Tabellen in AWS Glue und AWS Lake Formation aufzunehmen und zu verwalten.

- Wenn Sie den DefaultDataWarehouseBlueprint aktivieren, geben Sie für die Rolle Redshift Manage Access eine neue oder bestehende Servicerolle an, die Amazon die DataZone Autorisierung erteilt, den Zugriff auf Datashares, Tabellen und Ansichten in Amazon Redshift aufzunehmen und zu verwalten.
- Wenn Sie den SageMakerAmazon-Blueprint aktivieren, geben Sie für die Rolle „Zugriff SageMaker verwalten“ eine neue oder bestehende Servicerolle an, die Amazon DataZone Berechtigungen zur Veröffentlichung von SageMaker Amazon-Daten im Katalog erteilt. Es gibt Amazon auch die DataZone Erlaubnis, Zugriff auf von Amazon SageMaker veröffentlichte Assets im Katalog zu gewähren oder den Zugriff zu widerrufen.

  > **Important**
  >
  > Wenn Sie den SageMakerAmazon-Blueprint aktivieren, DataZone prüft Amazon, ob die folgenden IAM-Rollen für Amazon im aktuellen Konto und in der Region DataZone existieren. Wenn diese Rollen nicht existieren, erstellt Amazon sie DataZone automatisch.
  >
  > - AmazonDataZoneGlueAccess- <region>- <domainId>
  > - AmazonDataZoneRedshiftAccess- <region>- <domainId>

- Geben Sie für die Bereitstellungsrolle eine neue oder bestehende Servicerolle an, die Amazon die DataZone Autorisierung erteilt, Umgebungsressourcen mithilfe AWS CloudFormation des Umgebungskontos und der Region zu erstellen und zu konfigurieren.
- Wenn Sie den SageMakerAmazon-Blueprint aktivieren, geben Sie für die Datenquelle Amazon S3-Bucket SageMaker für -Glue einen Amazon S3 S3-Bucket an, der von allen SageMaker Umgebungen im AWS Konto verwendet werden soll. Das von Ihnen angegebene Bucket-Präfix muss eines der folgenden sein:
  - Amazon-Datazone*
  - Datazone-Sagemaker*
  - Sagemaker-Datazone*
  - DataZone-Sagemaker*
  - Salbeimacher- * DataZone
  - DataZone-SageMaker*
  - SageMaker-DataZone*

7. Wählen Sie Blueprint aktivieren.

Sobald Sie die ausgewählten Blueprints aktiviert haben, können Sie steuern, welche Projekte die Blueprints in Ihrem Konto verwenden können, um Umgebungsprofile zu erstellen. Sie können dies tun, indem Sie der Konfiguration des Blueprints die Verwaltung von Projekten zuweisen.

Geben Sie die Verwaltung von Projekten auf aktivierten Blueprints an

1. Rufen Sie die DataZone Amazon-Konsole unter https://console.aws.amazon.com/datazone auf und melden Sie sich mit Ihren Kontoanmeldeinformationen an.
2. Wählen Sie „Domains anzeigen“ und wählen Sie dann die Domain aus, zu der Sie die Verwaltungsprojekte für die ausgewählten Blueprints hinzufügen möchten.
3. Wählen Sie die Registerkarte Blueprints und dann den Blueprint aus, mit dem Sie arbeiten möchten.
4. Standardmäßig können alle Projekte innerhalb der Domain die DefaultDataLake oder oder die SageMaker Amazon-Blueprints im Konto verwenden DefaultDataWareshouse, um Umgebungsprofile zu erstellen. Sie können dies jedoch einschränken, indem Sie den Blueprints die Verwaltung von Projekten zuweisen. Um Verwaltungsprojekte hinzuzufügen, wählen Sie Verwaltungsprojekt auswählen aus, wählen Sie dann im Dropdownmenü die Projekte aus, die Sie als Verwaltungsprojekte hinzufügen möchten, und wählen Sie dann Verwaltungsprojekte auswählen aus.

Sobald Sie den DefaultDataWarehouse Blueprint in Ihrem AWS Konto aktiviert haben, können Sie der Blueprint-Konfiguration Parametersätze hinzufügen. Ein Parametersatz ist eine Gruppe von Schlüsseln und Werten, die Amazon benötigt, um eine Verbindung DataZone zu Ihrem Amazon Redshift Redshift-Cluster herzustellen, und wird zur Erstellung von Data Warehouse-Umgebungen verwendet. Zu diesen Parametern gehören der Name Ihres Amazon Redshift Redshift-Clusters, die Datenbank und das AWS Geheimnis, das die Anmeldeinformationen für den Cluster enthält.

Hinzufügen von Parametersätzen zum Blueprint DefaultDataWarehouse

1. Rufen Sie die DataZone Amazon-Konsole unter https://console.aws.amazon.com/datazone auf und melden Sie sich mit Ihren Kontoanmeldeinformationen an.
2. Wählen Sie Domains anzeigen und wählen Sie dann die Domain aus, zu der Sie den Parametersatz hinzufügen möchten.

3. Wählen Sie die Registerkarte Blueprints und dann den DefaultDataWareshouse Blueprint aus, um die Blueprint-Detailseite zu öffnen.
4. Wählen Sie auf der Blueprint-Detailseite auf der Registerkarte Parametersätze die Option Parametersatz erstellen aus.
   - Geben Sie einen Namen für den Parametersatz ein.
   - Geben Sie optional eine Beschreibung für den Parametersatz ein.
   - Region auswählen
   - Wählen Sie entweder Amazon Redshift Cluster oder Amazon Redshift Serverless aus.
   - Wählen Sie den AWS geheimen ARN aus, der die Anmeldeinformationen für den ausgewählten Amazon Redshift-Cluster oder die Amazon Redshift Serverless-Arbeitsgruppe enthält. Das AWS Geheimnis muss mit dem `AmazonDataZoneDomain : [Domain_ID]` Tag gekennzeichnet sein, um innerhalb eines Parametersatzes verwendet werden zu können.
     - Wenn Sie noch kein AWS Geheimnis haben, können Sie auch ein neues Geheimnis erstellen, indem Sie Neues AWS Geheimnis erstellen wählen. Dadurch wird ein Dialogfeld geöffnet, in dem Sie den Namen des Geheimnisses, den Benutzernamen und das Passwort angeben können. Sobald Sie Create New AWS Secret wählen, DataZone erstellt Amazon ein neues Secret im AWS Secrets Manager-Service und stellt sicher, dass das Secret mit der Domain gekennzeichnet ist, in der Sie versuchen, den Parametersatz zu erstellen.
   - Wenn Sie im obigen Schritt Amazon Redshift Redshift-Cluster ausgewählt haben, wählen Sie jetzt einen Cluster aus der Drop-down-Liste aus. Wenn Sie im obigen Schritt die Amazon Redshift Redshift-Arbeitsgruppe ausgewählt haben, wählen Sie jetzt eine Arbeitsgruppe aus dem Drop-down-Menü aus.
   - Geben Sie den Namen der Datenbank innerhalb des ausgewählten Amazon Redshift-Clusters oder der Amazon Redshift Serverless-Arbeitsgruppe ein.
   - Wählen Sie Parametersatz erstellen.

Sobald Sie den SageMaker Amazon-Blueprint in Ihrem AWS Konto aktiviert haben, können Sie der Blueprint-Konfiguration Parametersätze hinzufügen. Ein Parametersatz ist eine Gruppe von Schlüsseln und Werten, die Amazon benötigt, um eine Verbindung DataZone zu Ihrem Amazon herzustellen, SageMaker und wird verwendet, um Sagemaker-Umgebungen zu erstellen.

Hinzufügen von Parametersätzen zum SageMaker Amazon-Blueprint

1. Rufen Sie die DataZone Amazon-Konsole unter https://console.aws.amazon.com/datazone auf und melden Sie sich mit Ihren Kontoanmeldeinformationen an.
2. Wählen Sie Domains anzeigen und wählen Sie dann die Domain aus, die den aktivierten Blueprint enthält, zu dem Sie den Parametersatz hinzufügen möchten.
3. Wählen Sie die Registerkarte Blueprints und dann den SageMaker Amazon-Blueprint aus, um die Detailseite des Blueprints zu öffnen.
4. Wählen Sie auf der Blueprint-Detailseite auf der Registerkarte Parametersätze die Option Parametersatz erstellen aus und geben Sie dann Folgendes an:
   - Geben Sie einen Namen für den Parametersatz ein.
   - Geben Sie optional eine Beschreibung für den Parametersatz ein.
   - Geben Sie den SageMaker Amazon-Domain-Authentifizierungstyp an. Sie können entweder IAM oder IAM Identity Center (SSO) wählen.
   - Geben Sie eine Region an AWS .
   - Geben Sie einen AWS KMS-Schlüssel für die Datenverschlüsselung an. Sie können einen vorhandenen Schlüssel auswählen oder einen neuen Schlüssel erstellen.
   - Geben Sie unter Umgebungsparameter Folgendes an:
     - VPC-ID — die ID, die Sie für die VPC der SageMaker Amazon-Umgebung verwenden. Sie können eine bestehende VPC angeben oder eine neue erstellen.
     - Subnetze — eine oder mehrere IDs für einen Bereich von IP-Adressen für bestimmte Ressourcen innerhalb Ihrer VPC.
     - Netzwerkzugriff — wählen Sie entweder „Nur VPC“ oder „Nur öffentliches Internet“.
     - Sicherheitsgruppe — Die Sicherheitsgruppe, die bei der Konfiguration von VPC und Subnetzen verwendet werden soll.
   - Wählen Sie unter Datenquellenparameter eine der folgenden Optionen aus:
     - AWS Nur Glue
     - AWS Glue + Amazon Redshift Serverless. Wenn Sie diese Option wählen, geben Sie Folgendes an:
       - Geben Sie den AWS geheimen ARN an, der die Anmeldeinformationen für den ausgewählten Amazon Redshift Redshift-Cluster enthält. Der AWS geheime Schlüssel muss mit dem `AmazonDataZoneDomain : [Domain_ID]` Tag gekennzeichnet sein, um innerhalb eines Parametersatzes verwendet werden zu können.

Wenn Sie noch kein AWS Geheimnis haben, können Sie auch ein neues Geheimnis erstellen, indem Sie Neues AWS Geheimnis erstellen wählen. Dadurch wird ein Dialogfeld geöffnet, in dem Sie den Namen des Geheimnisses, den Benutzernamen und das Passwort angeben können. Sobald Sie Create New AWS Secret wählen, DataZone erstellt Amazon ein neues Secret im AWS Secrets Manager-Service und stellt sicher, dass das Secret mit der Domain gekennzeichnet ist, in der Sie versuchen, den Parametersatz zu erstellen.

- Geben Sie die Amazon Redshift Redshift-Arbeitsgruppe an, die Sie beim Erstellen von Umgebungen verwenden möchten.
- Geben Sie den Namen der Datenbank (innerhalb der von Ihnen ausgewählten Arbeitsgruppe) an, die Sie beim Erstellen von Umgebungen verwenden möchten.

- AWS Nur Glue + Amazon Redshift Cluster
  - Geben Sie den AWS geheimen ARN an, der die Anmeldeinformationen für den ausgewählten Amazon Redshift Redshift-Cluster enthält. Der AWS geheime Schlüssel muss mit dem `AmazonDataZoneDomain : [Domain_ID]` Tag gekennzeichnet sein, um innerhalb eines Parametersatzes verwendet werden zu können.

    Wenn Sie noch kein AWS Geheimnis haben, können Sie auch ein neues Geheimnis erstellen, indem Sie Neues AWS Geheimnis erstellen wählen. Dadurch wird ein Dialogfeld geöffnet, in dem Sie den Namen des Geheimnisses, den Benutzernamen und das Passwort angeben können. Sobald Sie Create New AWS Secret wählen, DataZone erstellt Amazon ein neues Secret im AWS Secrets Manager-Service und stellt sicher, dass das Secret mit der Domain gekennzeichnet ist, in der Sie versuchen, den Parametersatz zu erstellen.
  - Geben Sie den Amazon Redshift Redshift-Cluster an, den Sie beim Erstellen von Umgebungen verwenden möchten.
  - Geben Sie den Namen der Datenbank (innerhalb des von Ihnen ausgewählten Clusters) an, die Sie beim Erstellen von Umgebungen verwenden möchten.

5. Wählen Sie Parametersatz erstellen aus.

Fügen Sie Amazon SageMaker als vertrauenswürdigen Service zu dem AWS Konto hinzu, dem die DataZone Amazon-Domain gehört

Wenn Sie den SageMaker Amazon-Blueprint aktiviert haben, müssen Sie ihn auch SageMaker als einen der vertrauenswürdigen Dienste innerhalb von Amazon DataZone hinzufügen. Gehen Sie dazu wie folgt vor:

1. Rufen Sie die DataZone Amazon-Konsole unter https://console.aws.amazon.com/datazone auf und melden Sie sich mit Ihren Kontoanmeldeinformationen an.
2. Wählen Sie Domains anzeigen und wählen Sie dann die Domain aus, die den aktivierten SageMaker Blueprint enthält.
3. Wählen Sie die Trusted Services, dann Amazon SageMaker und dann Enable aus.

Mit verknüpften Konten arbeiten, um Daten zu veröffentlichen und zu nutzen

Wenn Sie Ihre AWS Konten mit Ihrer DataZone Amazon-Domain verknüpfen, können Domain-Benutzer Daten aus diesen AWS Konten veröffentlichen und nutzen. Die Einrichtung einer Kontoverknüpfung besteht aus drei Schritten.

- Teilen Sie zunächst die Domain mit dem gewünschten AWS Konto, indem Sie eine Zuordnung beantragen. Amazon DataZone verwendet AWS Resource Access Manager (RAM), wenn sich das AWS Konto vom AWS Konto der Domain unterscheidet. Eine Kontoverknüpfung kann nur von der DataZone Amazon-Domain initiiert werden.
- Zweitens bitten Sie den Kontoinhaber, die Zuordnungsanfrage anzunehmen.
- Drittens bitten Sie den Kontoinhaber, die gewünschten Umgebungs-Blueprints zu aktivieren. Durch die Aktivierung eines Blueprints stellt der Kontoinhaber den Benutzern in der Domain die IAM-Rollen und Ressourcenkonfigurationen zur Verfügung, die für die Erstellung und den Zugriff auf Ressourcen in ihrem Konto erforderlich sind, z. B. AWS Glue-Datenbanken und Amazon Redshift Redshift-Cluster.

Themen

Beantragen Sie die Verknüpfung mit anderen Konten AWS

> **Note**
>
> Wenn Sie eine Zuordnungsanfrage an ein anderes AWS Konto senden, teilen Sie Ihre Domain mit dem anderen AWS Konto mit AWS Resource Access Manager (RAM). Achten Sie darauf, die Richtigkeit der eingegebenen Konto-ID zu überprüfen.

Um eine Verknüpfung mit anderen AWS Konten in der DataZone Amazon-Konsole für eine DataZone Amazon-Domain zu beantragen, müssen Sie eine IAM-Rolle in dem Konto mit Administratorberechtigungen annehmen. Konfigurieren Sie die IAM-Berechtigungen, die für die Nutzung der Amazon DataZone Management Console erforderlich sindum die Mindestberechtigungen zu erhalten, die für die Beantragung einer Kontoverknüpfung erforderlich sind.

Gehen Sie wie folgt vor, um eine Verknüpfung mit anderen AWS Konten zu beantragen.

1. Melden Sie sich bei der AWS Management Console an und öffnen Sie die Amazon DataZone Management Console unter https://console.aws.amazon.com/datazone.
2. Wählen Sie Domains anzeigen und wählen Sie den Namen der Domain aus der Liste aus. Der Name ist ein Hyperlink.
3. Scrollen Sie nach unten zum Tab Verknüpfte Konten und wählen Sie Verknüpfung anfordern aus.
4. Geben Sie die IDs der Konten ein, deren Zuordnung Sie beantragen möchten. Wenn Sie mit der Liste der Konto-IDs zufrieden sind, wählen Sie Zuordnung anfordern aus.
5. Amazon DataZone erstellt im Namen Ihres Kontos eine AWS Ressourcenfreigabe im Resource Access Manager, wobei die eingegebenen Konto-ID (s) als Principals verwendet werden.
6. Sie müssen den Besitzer der anderen AWS Konten benachrichtigen, damit er Ihre Anfrage annehmen kann. Einladungen laufen nach sieben (7) Tagen ab.

Gewähren Sie Kontozugriff auf Ihren vom Kunden verwalteten KMS-Schlüssel

DataZone Amazon-Domains und ihre Metadaten werden entweder (standardmäßig) mit einem Schlüssel verschlüsselt, der von einem Kunden verwaltet wird AWS, oder (optional) mit einem vom

Kunden verwalteten Schlüssel von AWS Key Management Service (KMS), den Sie besitzen und den Sie bei der Domainerstellung angeben. Wenn Ihre Domain mit einem vom Kunden verwalteten Schlüssel verschlüsselt ist, gehen Sie wie folgt vor, um dem zugehörigen Konto die Erlaubnis zur Verwendung des KMS-Schlüssels zu erteilen.

1. Melden Sie sich bei der AWS Management Console an und öffnen Sie die KMS-Konsole unter https://console.aws.amazon.com/kms/.
2. Zum Anzeigen der Schlüssel in Ihrem Konto, die Sie erstellen und verwalten, wählen Sie im Navigationsbereich Customer managed keys (Vom Kunden verwaltete Schlüssel) aus.
3. Zum Anzeigen der Schlüssel in Ihrem Konto, die Sie erstellen und verwalten, wählen Sie im Navigationsbereich Customer managed keys (Vom Kunden verwaltete Schlüssel) aus.
4. Wählen Sie in der Liste der KMS-Schlüssel den Alias oder die Schlüssel-ID des KMS-Schlüssels aus, den Sie untersuchen möchten.
5. Verwenden Sie die Steuerelemente im Abschnitt Andere AWS AWS Konten der Seite, um externen Konten die Verwendung des KMS-Schlüssels zu gestatten oder zu verbieten. IAM-Prinzipale in diesen Konten (die selbst über die entsprechenden KMS-Berechtigungen verfügen) können den KMS-Schlüssel für kryptografische Operationen verwenden, z. B. beim Verschlüsseln, Entschlüsseln, erneuten Verschlüsseln und Generieren von Datenschlüsseln.

Akzeptieren Sie eine Kontozuordnungsanfrage von einer DataZone Amazon-Domain und aktivieren Sie einen Umgebungs-Blueprint

Um in der DataZone Amazon-Managementkonsole die Zuordnung zu einer DataZone Amazon-Domain zu akzeptieren, müssen Sie eine IAM-Rolle in dem Konto mit Administratorberechtigungen annehmen. Konfigurieren Sie die IAM-Berechtigungen, die für die Nutzung der Amazon DataZone Management Console erforderlich sindum die Mindestberechtigungen zu erhalten.

Gehen Sie wie folgt vor, um die Zuordnung zu einer DataZone Amazon-Domain zu akzeptieren.

1. Melden Sie sich bei der AWS Management Console an und öffnen Sie die Amazon DataZone Management Console unter https://console.aws.amazon.com/datazone.
2. Wählen Sie Anfragen anzeigen und wählen Sie die einladende Domain aus der Liste aus. Der Status der Einladung sollte „Angefragt“ lauten. Wählen Sie „Anfrage überprüfen“.
3. Wählen Sie aus, ob die standardmäßigen Blueprints für die Data Lake- und/oder Data Warehouse-Umgebung aktiviert werden sollen, indem Sie keines, beide oder eines der Felder auswählen. Sie können dies später tun.

- Der Data Lake-Umgebungs-Blueprint ermöglicht es Domain-Benutzern, AWS Glue-, Amazon S3- und Amazon Athena Athena-Ressourcen zu erstellen und zu verwalten, um sie von einem Data Lake aus zu veröffentlichen und zu nutzen.
- Der Blueprint für die Data Warehouse-Umgebung ermöglicht es Domain-Benutzern, Amazon Redshift Redshift-Ressourcen zu erstellen und zu verwalten, um sie von einem Data Warehouse aus zu veröffentlichen und zu nutzen.

4. Wenn Sie einen oder beide Standardumgebungs-Blueprints auswählen möchten, konfigurieren Sie die folgenden Berechtigungen und Ressourcen.

   - Die IAM-Rolle „Zugriff verwalten“ gewährt Amazon Berechtigungen DataZone, damit Domain-Benutzer den Zugriff auf Tabellen wie AWS Glue und Amazon Redshift aufnehmen und verwalten können. Sie können wählen, ob Amazon eine neue IAM-Rolle DataZone erstellen und verwenden soll, oder Sie können aus einer Liste vorhandener IAM-Rollen wählen.
   - Die IAM-Rolle Provisioning gewährt Amazon Berechtigungen DataZone, damit Domain-Benutzer Umgebungsressourcen wie AWS Glue-Datenbanken erstellen und konfigurieren können. Sie können wählen, ob Amazon eine neue IAM-Rolle DataZone erstellen und verwenden soll, oder Sie können aus einer Liste vorhandener IAM-Rollen wählen.
   - Der Amazon S3 S3-Bucket für Data Lake ist der Bucket oder Pfad, den Amazon DataZone verwendet, wenn Domain-Benutzer Data Lake-Daten speichern. Sie können den von Amazon ausgewählten Standard-Bucket verwenden DataZone oder Ihren eigenen vorhandenen Amazon S3 S3-Pfad wählen, indem Sie dessen Pfadzeichenfolge eingeben. Wenn Sie Ihren eigenen Amazon S3 S3-Pfad wählen, müssen Sie die IAM-Richtlinien aktualisieren, um Amazon die DataZone entsprechenden Nutzungsberechtigungen zu gewähren.

5. Wenn Sie mit Ihren Konfigurationen zufrieden sind, wählen Sie Accept and configure association.

Eine Kontozuordnungsanfrage von einer DataZone Amazon-Domain ablehnen

Um eine Zuordnungsanfrage in der DataZone Amazon-Managementkonsole von einer DataZone Amazon-Domain abzulehnen, müssen Sie eine IAM-Rolle in dem Konto mit Administratorberechtigungen annehmen. Konfigurieren Sie die IAM-Berechtigungen, die für die Nutzung der Amazon DataZone Management Console erforderlich sindum die Mindestberechtigungen zu erhalten.

Gehen Sie wie folgt vor, um eine Zuordnungsanfrage von einer DataZone Amazon-Domain abzulehnen.

1. Melden Sie sich bei der AWS Management Console an und öffnen Sie die Amazon DataZone Management Console unter https://console.aws.amazon.com/datazone.
2. Wählen Sie Anfragen anzeigen und wählen Sie die einladende Domain aus der Liste aus. Der Status der Einladung sollte „Angefragt“ lauten. Wählen Sie Zuordnung ablehnen aus. Bestätigen Sie Ihre Auswahl, indem Sie Zuordnung ablehnen wählen.

Aktivieren Sie einen Umgebungs-Blueprint in einem zugehörigen Konto AWS

Um einen Umgebungs-Blueprint in der Amazon DataZone Management Console zu aktivieren, müssen Sie eine IAM-Rolle in dem Konto mit Administratorberechtigungen annehmen. Konfigurieren Sie die IAM-Berechtigungen, die für die Nutzung der Amazon DataZone Management Console erforderlich sindum die Mindestberechtigungen zu erhalten.

Gehen Sie wie folgt vor, um einen Blueprint in einer zugehörigen Domäne zu aktivieren.

1. Melden Sie sich bei der AWS Management Console an und öffnen Sie die Amazon DataZone Management Console unter https://console.aws.amazon.com/datazone.
2. Öffnen Sie den linken Navigationsbereich und wählen Sie Assoziierte Domains aus.
3. Wählen Sie die Domain aus, für die Sie einen Umgebungs-Blueprint aktivieren möchten.
4. Wählen Sie aus der Blueprint-Liste entweder den DefaultDataLakeoder den oder den DefaultDataWarehouse SageMakerAmazon-Blueprint aus.
5. Wählen Sie auf der Detailseite des ausgewählten Blueprints die Option In diesem Konto aktivieren aus.
6. Geben Sie auf der Seite „Berechtigungen und Ressourcen“ Folgendes an:

   - Wenn Sie den DefaultDataLakeBlueprint aktivieren, geben Sie für die Rolle Glue Manage Access eine neue oder bestehende Servicerolle an, die Amazon die DataZone Autorisierung erteilt, den Zugriff auf Tabellen in AWS Glue und AWS Lake Formation aufzunehmen und zu verwalten.
   - Wenn Sie den DefaultDataWarehouseBlueprint aktivieren, geben Sie für die Rolle Redshift Manage Access eine neue oder bestehende Servicerolle an, die Amazon die DataZone

Autorisierung erteilt, den Zugriff auf Datashares, Tabellen und Ansichten in Amazon Redshift aufzunehmen und zu verwalten.

- Wenn Sie den SageMakerAmazon-Blueprint aktivieren, geben Sie für die Rolle „Zugriff SageMaker verwalten“ eine neue oder bestehende Servicerolle an, die Amazon DataZone Berechtigungen zur Veröffentlichung von SageMaker Amazon-Daten im Katalog erteilt. Es gibt Amazon auch die DataZone Erlaubnis, Zugriff auf von Amazon SageMaker veröffentlichte Assets im Katalog zu gewähren oder den Zugriff zu widerrufen.

  > **Important**
  >
  > Wenn Sie den SageMakerAmazon-Blueprint aktivieren, DataZone prüft Amazon, ob die folgenden IAM-Rollen für Amazon im aktuellen Konto und in der Region DataZone existieren. Wenn diese Rollen nicht existieren, erstellt Amazon sie DataZone automatisch.
  >
  > - AmazonDataZoneGlueAccess- <region>- <domainId>
  > - AmazonDataZoneRedshiftAccess- <region>- <domainId>

- Geben Sie für die Bereitstellungsrolle eine neue oder bestehende Servicerolle an, die Amazon die DataZone Autorisierung erteilt, Umgebungsressourcen mithilfe AWS CloudFormation des Umgebungskontos und der Region zu erstellen und zu konfigurieren.
- Wenn Sie den SageMakerAmazon-Blueprint aktivieren, geben Sie für die Datenquelle Amazon S3-Bucket SageMaker für -Glue einen Amazon S3 S3-Bucket an, der von allen SageMaker Umgebungen im AWS Konto verwendet werden soll. Das von Ihnen angegebene Bucket-Präfix muss eines der folgenden sein:
  - Amazon-Datazone*
  - Datazone-Sagemaker*
  - Sagemaker-Datazone*
  - DataZone-Sagemaker*
  - Salbeimacher- * DataZone
  - DataZone-SageMaker*
  - SageMaker-DataZone*

7. Wählen Sie Blueprint aktivieren.

Sobald Sie die ausgewählten Blueprints aktiviert haben, können Sie steuern, welche Projekte die Blueprints in Ihrem Konto verwenden können, um Umgebungsprofile zu erstellen. Sie können dies tun, indem Sie der Konfiguration des Blueprints die Verwaltung von Projekten zuweisen.

Geben Sie die Verwaltung von Projekten auf „Enabled“ oder „Blueprint“ DefaultDataLake an DefaultDataWarehouse

1. Rufen Sie die DataZone Amazon-Konsole unter https://console.aws.amazon.com/datazone auf und melden Sie sich mit Ihren Kontoanmeldeinformationen an.
2. Öffnen Sie den linken Navigationsbereich und wählen Sie Assoziierte Domains und dann die Domain aus, der Sie Verwaltungsprojekte hinzufügen möchten.
3. Wählen Sie die Registerkarte Blueprints und dann DefaultDataLake oder DefaultDataWareshouse Blueprint aus.
4. Standardmäßig können alle Projekte innerhalb der Domain den DefaultDataWareshouse Blueprint DefaultDataLake oder im Konto verwenden, um Umgebungsprofile zu erstellen. Sie können dies jedoch einschränken, indem Sie dem Blueprint die Verwaltung von Projekten zuweisen. Um Verwaltungsprojekte hinzuzufügen, wählen Sie Verwaltungsprojekt auswählen aus, wählen Sie dann im Dropdownmenü die Projekte aus, die Sie als Verwaltungsprojekte hinzufügen möchten, und wählen Sie dann Verwaltungsprojekte auswählen aus.

Sobald Sie den DefaultDataWarehouse Blueprint in Ihrem AWS Konto aktiviert haben, können Sie der Blueprint-Konfiguration Parametersätze hinzufügen. Ein Parametersatz ist eine Gruppe von Schlüsseln und Werten, die Amazon benötigt, um eine Verbindung DataZone zu Ihrem Amazon Redshift Redshift-Cluster herzustellen, und wird zur Erstellung von Data Warehouse-Umgebungen verwendet. Zu diesen Parametern gehören der Name Ihres Amazon Redshift Redshift-Clusters, die Datenbank und das AWS Geheimnis, das die Anmeldeinformationen für den Cluster enthält.

Hinzufügen von Parametersätzen zum Blueprint DefaultDataWarehouse

1. Rufen Sie die DataZone Amazon-Konsole unter https://console.aws.amazon.com/datazone auf und melden Sie sich mit Ihren Kontoanmeldeinformationen an.
2. Öffnen Sie den linken Navigationsbereich und wählen Sie Associated Domains und dann die Domain aus, zu der Sie Parametersätze hinzufügen möchten.
3. Wählen Sie die Registerkarte Blueprints und dann den DefaultDataWareshouse Blueprint aus, um die Blueprint-Detailseite zu öffnen.

4. Wählen Sie auf der Blueprint-Detailseite auf der Registerkarte Parametersätze die Option Parametersatz erstellen aus.

   - Geben Sie einen Namen für den Parametersatz ein.
   - Geben Sie optional eine Beschreibung für den Parametersatz ein.
   - Region auswählen
   - Wählen Sie entweder Amazon Redshift Cluster oder Amazon Redshift Serverless aus.
   - Wählen Sie den AWS geheimen ARN aus, der die Anmeldeinformationen für den ausgewählten Amazon Redshift-Cluster oder die Amazon Redshift Serverless-Arbeitsgruppe enthält. Das AWS Geheimnis muss mit dem `AmazonDataZoneDomain : [Domain_ID]` Tag gekennzeichnet sein, um innerhalb eines Parametersatzes verwendet werden zu können.
     - Wenn Sie noch kein AWS Geheimnis haben, können Sie auch ein neues Geheimnis erstellen, indem Sie Neues AWS Geheimnis erstellen wählen. Dadurch wird ein Dialogfeld geöffnet, in dem Sie den Namen des Geheimnisses, den Benutzernamen und das Passwort angeben können. Sobald Sie Create New AWS Secret wählen, DataZone erstellt Amazon ein neues Secret im AWS Secrets Manager-Service und stellt sicher, dass das Secret mit der Domain gekennzeichnet ist, in der Sie versuchen, den Parametersatz zu erstellen.
   - Wählen Sie entweder Amazon Redshift-Cluster oder Amazon Redshift Serverless Workgroup aus.
   - Geben Sie den Namen der Datenbank innerhalb des ausgewählten Amazon Redshift-Clusters oder der Amazon Redshift Serverless-Arbeitsgruppe ein.
   - Wählen Sie Parametersatz erstellen aus.

Sobald Sie den SageMaker Amazon-Blueprint in Ihrem AWS Konto aktiviert haben, können Sie der Blueprint-Konfiguration Parametersätze hinzufügen. Ein Parametersatz ist eine Gruppe von Schlüsseln und Werten, die Amazon benötigt, um eine Verbindung DataZone zu Ihrem Amazon herzustellen, SageMaker und wird verwendet, um Sagemaker-Umgebungen zu erstellen.

Hinzufügen von Parametersätzen zum SageMaker Amazon-Blueprint

1. Rufen Sie die DataZone Amazon-Konsole unter https://console.aws.amazon.com/datazone auf und melden Sie sich mit Ihren Kontoanmeldeinformationen an.
2. Wählen Sie Domains anzeigen und wählen Sie dann die Domain aus, die den aktivierten Blueprint enthält, zu dem Sie den Parametersatz hinzufügen möchten.

3. Wählen Sie die Registerkarte Blueprints und dann den SageMaker Amazon-Blueprint aus, um die Detailseite des Blueprints zu öffnen.
4. Wählen Sie auf der Blueprint-Detailseite auf der Registerkarte Parametersätze die Option Parametersatz erstellen aus und geben Sie dann Folgendes an:

   - Geben Sie einen Namen für den Parametersatz ein.
   - Geben Sie optional eine Beschreibung für den Parametersatz ein.
   - Geben Sie den SageMaker Amazon-Domain-Authentifizierungstyp an. Sie können entweder IAM oder IAM Identity Center (SSO) wählen.
   - Geben Sie eine Region an AWS .
   - Geben Sie einen AWS KMS-Schlüssel für die Datenverschlüsselung an. Sie können einen vorhandenen Schlüssel auswählen oder einen neuen Schlüssel erstellen.
   - Geben Sie unter Umgebungsparameter Folgendes an:
     - VPC-ID — die ID, die Sie für die VPC der SageMaker Amazon-Umgebung verwenden. Sie können eine bestehende VPC angeben oder eine neue erstellen.
     - Subnetze — eine oder mehrere IDs für einen Bereich von IP-Adressen für bestimmte Ressourcen innerhalb Ihrer VPC.
     - Netzwerkzugriff — wählen Sie entweder „Nur VPC“ oder „Nur öffentliches Internet“.
     - Sicherheitsgruppe — Die Sicherheitsgruppe, die bei der Konfiguration von VPC und Subnetzen verwendet werden soll.
   - Wählen Sie unter Datenquellenparameter eine der folgenden Optionen aus:
     - AWS Nur Glue
     - AWS Glue + Amazon Redshift Serverless. Wenn Sie diese Option wählen, geben Sie Folgendes an:
       - Geben Sie den AWS geheimen ARN an, der die Anmeldeinformationen für den ausgewählten Amazon Redshift Redshift-Cluster enthält. Der AWS geheime Schlüssel muss mit dem `AmazonDataZoneDomain : [Domain_ID]` Tag gekennzeichnet sein, um innerhalb eines Parametersatzes verwendet werden zu können.

         Wenn Sie noch kein AWS Geheimnis haben, können Sie auch ein neues Geheimnis erstellen, indem Sie Neues AWS Geheimnis erstellen wählen. Dadurch wird ein Dialogfeld geöffnet, in dem Sie den Namen des Geheimnisses, den Benutzernamen und das Passwort angeben können. Sobald Sie Create New AWS Secret wählen, DataZone erstellt Amazon ein neues Secret im AWS Secrets Manager-Service und stellt sicher, dass

das Secret mit der Domain gekennzeichnet ist, in der Sie versuchen, den Parametersatz zu erstellen.

- Geben Sie die Amazon Redshift Redshift-Arbeitsgruppe an, die Sie beim Erstellen von Umgebungen verwenden möchten.
- Geben Sie den Namen der Datenbank (innerhalb der von Ihnen ausgewählten Arbeitsgruppe) an, die Sie beim Erstellen von Umgebungen verwenden möchten.

- AWS Nur Glue + Amazon Redshift Cluster
  - Geben Sie den AWS geheimen ARN an, der die Anmeldeinformationen für den ausgewählten Amazon Redshift Redshift-Cluster enthält. Der AWS geheime Schlüssel muss mit dem `AmazonDataZoneDomain : [Domain_ID]` Tag gekennzeichnet sein, um innerhalb eines Parametersatzes verwendet werden zu können.

    Wenn Sie noch kein AWS Geheimnis haben, können Sie auch ein neues Geheimnis erstellen, indem Sie Neues AWS Geheimnis erstellen wählen. Dadurch wird ein Dialogfeld geöffnet, in dem Sie den Namen des Geheimnisses, den Benutzernamen und das Passwort angeben können. Sobald Sie Create New AWS Secret wählen, DataZone erstellt Amazon ein neues Secret im AWS Secrets Manager-Service und stellt sicher, dass das Secret mit der Domain gekennzeichnet ist, in der Sie versuchen, den Parametersatz zu erstellen.
  - Geben Sie den Amazon Redshift Redshift-Cluster an, den Sie beim Erstellen von Umgebungen verwenden möchten.
  - Geben Sie den Namen der Datenbank (innerhalb des von Ihnen ausgewählten Clusters) an, die Sie beim Erstellen von Umgebungen verwenden möchten.

5. Wählen Sie Parametersatz erstellen aus.

Fügen Sie Amazon SageMaker als vertrauenswürdigen Service zum zugehörigen AWS Konto hinzu

Wenn Sie den SageMaker Amazon-Blueprint aktiviert haben, müssen Sie ihn auch SageMaker als einen der vertrauenswürdigen Dienste innerhalb von Amazon DataZone hinzufügen. Führen Sie dazu das folgende Verfahren aus:

1. Rufen Sie die DataZone Amazon-Konsole unter https://console.aws.amazon.com/datazone auf und melden Sie sich mit Ihren Kontoanmeldeinformationen an.

2. Wählen Sie Domains anzeigen und wählen Sie dann die Domain aus, die den aktivierten SageMaker Blueprint enthält.
3. Wählen Sie die Trusted Services, dann Amazon SageMaker und dann Enable aus.

Entfernen Sie ein zugeordnetes Konto

Um ein zugeordnetes AWS Konto in der Amazon DataZone Management Console zu entfernen, müssen Sie eine IAM-Rolle in dem Konto mit Administratorberechtigungen annehmen. Konfigurieren Sie die IAM-Berechtigungen, die für die Nutzung der Amazon DataZone Management Console erforderlich sindum die Mindestberechtigungen zu erhalten.

Gehen Sie wie folgt vor, um ein zugeordnetes Konto aus Ihrer Domain zu entfernen.

1. Melden Sie sich bei der AWS Management Console an und öffnen Sie die Amazon DataZone Management Console unter https://console.aws.amazon.com/datazone.
2. Wählen Sie „Domains anzeigen“ und wählen Sie den Namen der Domain aus der Liste aus. Der Name ist ein Hyperlink.
3. Scrollen Sie nach unten zum Tab Zugeordnete Konten. Wählen Sie die Konto-ID für das AWS Konto, das Sie entfernen möchten.
4. Wählen Sie Disassociate (Zuordnung aufheben) aus. Bestätigen Sie Ihre Auswahl, indem Sie Disassociate in das Feld eingeben und Disassociate auswählen.
5. Das Konto ist jetzt aus Ihrer Domain entfernt und kann von den Benutzern der Domain nicht zum Veröffentlichen und Konsumieren von Daten verwendet werden.

Arbeiten mit dem DataZone Amazon-Datenkatalog

Sie können den DataZone Amazon-Geschäftsdatenkatalog verwenden, um Daten in Ihrem gesamten Unternehmen mit geschäftlichem Kontext zu katalogisieren und so jedem in Ihrem Unternehmen zu ermöglichen, Daten schnell zu finden und zu verstehen. Weitere Informationen finden Sie unter DataZone Amazon-Terminologie und Konzepte.

Themen

Ein Geschäftsglossar erstellen, bearbeiten oder löschen

Bei Amazon DataZone ist ein Geschäftsglossar eine Sammlung von Geschäftsbegriffen (Wörtern), die mit Vermögenswerten (Daten) verknüpft werden können. Es enthält geeignete Vokabeln mit einer Liste von Geschäftsbegriffen und ihren Definitionen für Geschäftsanwender, um sicherzustellen, dass bei der Datenanalyse im gesamten Unternehmen dieselben Definitionen verwendet werden. Unternehmensglossare werden in der Katalogdomäne erstellt und können auf Ressourcen und Spalten angewendet werden, um die wichtigsten Merkmale dieser Ressource oder Spalte besser zu verstehen. Es können ein oder mehrere Glossarbegriffe verwendet werden. Ein Geschäftsglossar kann eine einfache Liste von Begriffen sein, wobei jeder Begriff im Geschäftsglossar mit einer Unterliste anderer Begriffe verknüpft werden kann. Weitere Informationen finden Sie unter DataZone Amazon-Terminologie und Konzepte. Um ein Glossar in Ihrer DataZone Amazon-Domain zu erstellen, zu bearbeiten oder zu löschen, müssen Sie Mitglied des Eigentümerprojekts mit den richtigen Berechtigungen für diese Domain sein.

Gehen Sie wie folgt vor, um ein Glossar zu erstellen:

1. Navigieren Sie mithilfe der DataZone Datenportal-URL zum Amazon-Datenportal und melden Sie sich mit Ihrem SSO oder Ihren AWS Anmeldeinformationen an. Wenn Sie ein DataZone Amazon-Administrator sind, können Sie die Datenportal-URL abrufen, indem Sie auf die DataZone Amazon-Konsole unter https://console.aws.amazon.com/datazone in dem AWS Konto zugreifen, in dem die DataZone Amazon-Domain erstellt wurde.
2. Navigieren Sie in der oberen Navigationsleiste neben Suchen zum Katalogmenü.

3. Wählen Sie im Amazon DataZone Data Portal Glossare und dann Glossar erstellen aus.
4. Geben Sie einen Namen, eine Beschreibung und einen Besitzer für das Glossar an und wählen Sie dann Glossar erstellen.
5. Aktivieren Sie das neue Glossar, indem Sie den Schalter Aktiviert wählen.
6. Auf der Detailseite des Glossars können Sie Readme erstellen wählen, um zusätzliche Informationen zu diesem Glossar hinzuzufügen.

Gehen Sie wie folgt vor, um ein Geschäftsglossar zu deaktivieren oder zu aktivieren:

1. Navigieren Sie mithilfe der DataZone Datenportal-URL zum Amazon-Datenportal und melden Sie sich mit Ihrem SSO oder Ihren AWS Anmeldeinformationen an. Wenn Sie ein DataZone Amazon-Administrator sind, können Sie die Datenportal-URL abrufen, indem Sie auf die DataZone Amazon-Konsole unter https://console.aws.amazon.com/datazone in dem AWS Konto zugreifen, in dem die DataZone Amazon-Domain erstellt wurde.
2. Navigieren Sie in der oberen Navigationsleiste neben Suchen zum Katalogmenü.
3. Wählen Sie im Amazon DataZone Data Portal Glossaries aus und suchen Sie das Geschäftsglossar, das Sie deaktivieren/aktivieren möchten.
4. Suchen Sie auf der Seite mit den Glossardetails den Schalter Aktivieren/Deaktivieren und verwenden Sie ihn, um Ihr ausgewähltes Glossar zu aktivieren oder zu deaktivieren.

> **Note**
>
> Wenn Sie ein Glossar deaktivieren, werden auch alle darin enthaltenen Begriffe deaktiviert.

Gehen Sie wie folgt vor, um ein Geschäftsglossar zu bearbeiten:

1. Navigieren Sie mithilfe der DataZone Datenportal-URL zum Amazon-Datenportal und melden Sie sich mit Ihrem SSO oder Ihren AWS Anmeldeinformationen an. Wenn Sie ein DataZone Amazon-Administrator sind, können Sie die Datenportal-URL abrufen, indem Sie auf die DataZone Amazon-Konsole unter https://console.aws.amazon.com/datazone in dem AWS Konto zugreifen, in dem die DataZone Amazon-Domain erstellt wurde.
2. Navigieren Sie in der oberen Navigationsleiste neben Suchen zum Katalogmenü.
3. Wählen Sie im Amazon DataZone Data Portal Glossaries aus und suchen Sie das Geschäftsglossar, das Sie bearbeiten möchten.

4. Erweitern Sie auf der Seite mit den Glossardetails die Option Aktionen und wählen Sie dann Bearbeiten, um das Glossar zu bearbeiten.
5. Nehmen Sie die gewünschten Änderungen am Namen und der Beschreibung vor und wählen Sie dann Speichern aus.

Gehen Sie wie folgt vor, um ein Unternehmensglossar zu löschen:

1. Navigieren Sie mithilfe der DataZone Datenportal-URL zum Amazon-Datenportal und melden Sie sich mit Ihrem SSO oder Ihren AWS Anmeldeinformationen an. Wenn Sie ein DataZone Amazon-Administrator sind, können Sie die Datenportal-URL abrufen, indem Sie auf die DataZone Amazon-Konsole unter https://console.aws.amazon.com/datazone in dem AWS Konto zugreifen, in dem die DataZone Amazon-Domain erstellt wurde.
2. Navigieren Sie in der oberen Navigationsleiste neben Suchen zum Katalogmenü.
3. Wählen Sie im Amazon DataZone Data Portal Glossaries aus und suchen Sie das Geschäftsglossar, das Sie löschen möchten.
4. Erweitern Sie auf der Seite mit den Glossardetails die Option Aktionen und wählen Sie dann Löschen, um das Glossar zu löschen.

   > **Note**
   >
   > Sie müssen alle vorhandenen Begriffe im Glossar löschen, bevor Sie das Glossar löschen können.

5. Bestätigen Sie das Löschen des Glossars, indem Sie Löschen wählen.

Einen Begriff in einem Glossar erstellen, bearbeiten oder löschen

Bei Amazon DataZone ist ein Geschäftsglossar eine Sammlung von Geschäftsbegriffen, die mit Vermögenswerten (Daten) verknüpft sein können. Weitere Informationen finden Sie unter DataZone Amazon-Terminologie und Konzepte. Um Begriffe in einem Glossar in Ihrer DataZone Amazon-Domain zu erstellen, zu bearbeiten oder zu löschen, müssen Sie Mitglied des jeweiligen Projekts sein und über die entsprechenden Berechtigungen für diese Domain verfügen.

Bei Amazon DataZone können Begriffe aus dem Geschäftsglossar sehr genau beschrieben werden. Um den Kontext eines bestimmten Begriffs festzulegen, können Sie Beziehungen zwischen Begriffen angeben. Wenn Sie eine Beziehung für einen Begriff definieren, wird sie automatisch zur

Definition des verwandten Begriffs hinzugefügt. Zu den bei Amazon verfügbaren Glossarbegriffen „Beziehungen“ DataZone gehören:

- Ist ein Typ von — gibt an, dass es sich bei dem aktuellen Begriff um einen Typ des identifizierten Begriffs handelt. Zeigt an, dass der identifizierte Begriff dem aktuellen Begriff übergeordnet ist.
- Hat Typen — gibt an, dass es sich bei dem aktuellen Begriff um einen Oberbegriff für den oder die angegebenen spezifischen Begriffe handelt. Diese Beziehung kann untergeordnete Begriffe für den generischen Begriff bezeichnen.

Gehen Sie wie folgt vor, um einen neuen Begriff zu erstellen:

1. Navigieren Sie mithilfe der DataZone Datenportal-URL zum Amazon-Datenportal und melden Sie sich mit Ihrem SSO oder Ihren AWS Anmeldeinformationen an. Wenn Sie ein DataZone Amazon-Administrator sind, können Sie die Datenportal-URL abrufen, indem Sie auf die DataZone Amazon-Konsole unter https://console.aws.amazon.com/datazone in dem AWS Konto zugreifen, in dem die DataZone Amazon-Domain erstellt wurde.
2. Navigieren Sie in der oberen Navigationsleiste neben Suchen zum Katalogmenü.
3. Wählen Sie im Amazon DataZone Data Portal Glossaries und dann das Glossar aus, in dem Sie den neuen Begriff erstellen möchten.
4. Geben Sie einen Namen, eine Beschreibung und einen Eigentümer für den Begriff ein und wählen Sie dann Begriff erstellen.
5. Aktivieren Sie den neuen Begriff, indem Sie den Schalter Aktiviert auswählen.
6. Um eine Readme-Datei hinzuzufügen, navigieren Sie zur Seite mit den Begriffsdetails. Wählen Sie dann Create Readme aus, um zusätzliche Informationen zu diesem Glossar hinzuzufügen.
7. Um Beziehungen hinzuzufügen, navigieren Sie zur Seite mit den Begriffsdetails, wählen Sie den Abschnitt Termbeziehungen und dann Glossarbegriffe hinzufügen aus. Wählen Sie im Dialogfeld die Beziehung und die Begriffe aus, die Sie verknüpfen möchten, und klicken Sie dann auf Schließen, um dem entsprechenden Beziehungstyp einen Begriff hinzuzufügen. Diese Beziehung wird auch zu allen Begriffen hinzugefügt, die Sie miteinander verknüpft haben.

Gehen Sie wie folgt vor, um einen Begriff in einem Glossar zu bearbeiten:

1. Navigieren Sie mithilfe der DataZone Datenportal-URL zum Amazon-Datenportal und melden Sie sich mit Ihrem SSO oder Ihren AWS Anmeldeinformationen an. Wenn Sie ein DataZone Amazon-Administrator sind, können Sie die Datenportal-URL abrufen, indem Sie auf die

DataZone Amazon-Konsole unter https://console.aws.amazon.com/datazone in dem AWS Konto zugreifen, in dem die DataZone Amazon-Domain erstellt wurde.

2. Navigieren Sie in der oberen Navigationsleiste neben Suchen zum Katalogmenü.
3. Wählen Sie im Amazon DataZone Data Portal Glossaries aus, suchen Sie das Glossar, das den Begriff enthält, den Sie bearbeiten möchten, und wählen Sie dann diesen Begriff aus.
4. Erweitern Sie auf der Seite mit den Begriffsdetails die Option Aktionen und wählen Sie dann Bearbeiten, um den Begriff zu bearbeiten.
5. Nehmen Sie die gewünschten Änderungen an dem Namen und der Beschreibung vor und wählen Sie dann Speichern aus.

Gehen Sie wie folgt vor, um einen Begriff in einem Glossar zu löschen:

1. Navigieren Sie mithilfe der DataZone Datenportal-URL zum Amazon-Datenportal und melden Sie sich mit Ihrem SSO oder Ihren AWS Anmeldeinformationen an. Wenn Sie ein DataZone Amazon-Administrator sind, können Sie die Datenportal-URL abrufen, indem Sie auf die DataZone Amazon-Konsole unter https://console.aws.amazon.com/datazone in dem AWS Konto zugreifen, in dem die DataZone Amazon-Domain erstellt wurde.
2. Navigieren Sie in der oberen Navigationsleiste neben Suchen zum Katalogmenü.
3. Wählen Sie im Amazon DataZone Data Portal Glossaries aus, suchen Sie das Glossar, das den Begriff enthält, den Sie löschen möchten, und wählen Sie dann diesen Begriff aus.
4. Erweitern Sie auf der Seite mit den Glossardetails die Option Aktionen und wählen Sie dann Löschen, um den Begriff zu löschen.
5. Bestätigen Sie das Löschen des Begriffs, indem Sie Löschen wählen.

Metadatenformulare erstellen, bearbeiten oder löschen

In Amazon sind Metadatenformulare einfache Formulare DataZone, um den Asset-Metadaten im Katalog zusätzlichen Geschäftskontext hinzuzufügen. Es dient als erweiterbarer Mechanismus für Dateneigentümer, um die Ressource mit Informationen anzureichern, die Datennutzern beim Suchen und Finden dieser Daten helfen können. Metadatenformulare können auch als Mechanismus dienen, um die Konsistenz aller im DataZone Amazon-Katalog veröffentlichten Assets durchzusetzen.

Eine Metadaten-Formulardefinition besteht aus einer oder mehreren Felddefinitionen und unterstützt die Datentypen Boolean, Date, Decimal, Integer, String und Business Glossary. Weitere Informationen finden Sie unter DataZone Amazon-Terminologie und Konzepte. Um

Metadatenformulare in Ihrer DataZone Amazon-Domain zu erstellen, zu bearbeiten oder zu löschen, müssen Sie Mitglied des jeweiligen Projekts sein und über die richtigen Anmeldeinformationen verfügen.

Gehen Sie wie folgt vor, um ein Metadatenformular zu erstellen:

1. Navigieren Sie mithilfe der DataZone Datenportal-URL zum Amazon-Datenportal und melden Sie sich mit Ihrem SSO oder Ihren AWS Anmeldeinformationen an. Wenn Sie ein DataZone Amazon-Administrator sind, können Sie die Datenportal-URL abrufen, indem Sie auf die DataZone Amazon-Konsole unter https://console.aws.amazon.com/datazone in dem AWS Konto zugreifen, in dem die DataZone Amazon-Domain erstellt wurde.
2. Navigieren Sie in der oberen Navigationsleiste neben Suchen zum Katalogmenü.
3. Wählen Sie im Amazon DataZone Data Portal Metadata Forms und dann Create form aus.
4. Geben Sie den Namen, die Beschreibung und den Eigentümer des Metadatenformulars an und wählen Sie dann Formular erstellen.

Gehen Sie wie folgt vor, um ein Metadatenformular zu bearbeiten:

1. Navigieren Sie mithilfe der DataZone Datenportal-URL zum Amazon-Datenportal und melden Sie sich mit Ihrem SSO oder Ihren AWS Anmeldeinformationen an. Wenn Sie ein DataZone Amazon-Administrator sind, können Sie die Datenportal-URL abrufen, indem Sie auf die DataZone Amazon-Konsole unter https://console.aws.amazon.com/datazone in dem AWS Konto zugreifen, in dem die DataZone Amazon-Domain erstellt wurde.
2. Navigieren Sie in der oberen Navigationsleiste neben Suchen zum Katalogmenü.
3. Wählen Sie im Amazon DataZone Data Portal Metadata Forms aus und suchen Sie dann das Metadaten-Formular, das Sie bearbeiten möchten.
4. Erweitern Sie auf der Detailseite des Metadatenformulars die Option Aktionen und wählen Sie dann Bearbeiten aus.
5. Nehmen Sie Ihre Aktualisierungen an den Feldern Name, Beschreibung und Besitzer vor und wählen Sie dann Formular aktualisieren aus.

Gehen Sie wie folgt vor, um ein Metadatenformular zu löschen:

> **Note**
>
> Bevor Sie ein Metadatenformular löschen können, müssen Sie es aus allen Asset-Typen oder Assets entfernen, auf die es angewendet wurde.

1. Navigieren Sie mithilfe der DataZone Datenportal-URL zum Amazon-Datenportal und melden Sie sich mit Ihrem SSO oder Ihren AWS Anmeldeinformationen an. Wenn Sie ein DataZone Amazon-Administrator sind, können Sie die Datenportal-URL abrufen, indem Sie auf die DataZone Amazon-Konsole unter https://console.aws.amazon.com/datazone in dem AWS Konto zugreifen, in dem die DataZone Amazon-Domain erstellt wurde.
2. Navigieren Sie in der oberen Navigationsleiste neben Suchen zum Katalogmenü.
3. Wählen Sie im Amazon DataZone Data Portal Metadata Forms aus und suchen Sie dann das Metadaten-Formular, das Sie löschen möchten.
4. Wenn das Metadatenformular, das Sie löschen möchten, aktiviert ist, deaktivieren Sie das Metadatenformular, indem Sie den Schalter Aktiviert wählen.
5. Erweitern Sie auf der Detailseite des Metadatenformulars die Option Aktionen und wählen Sie dann Löschen aus.
6. Bestätigen Sie den Löschvorgang, indem Sie Löschen wählen.

Felder in Metadatenformularen erstellen, bearbeiten oder löschen

In Amazon sind Metadatenformulare einfache Formulare DataZone, um den Asset-Metadaten im Katalog zusätzlichen Geschäftskontext hinzuzufügen. Es dient als erweiterbarer Mechanismus für Dateneigentümer, um die Ressource mit Informationen anzureichern, die Datennutzern beim Suchen und Finden dieser Daten helfen können. Metadatenformulare können auch als Mechanismus dienen, um die Konsistenz aller im DataZone Amazon-Katalog veröffentlichten Assets durchzusetzen.

Eine Metadaten-Formulardefinition besteht aus einer oder mehreren Felddefinitionen und unterstützt die Datentypen Boolean, Date, Decimal, Integer, String und Business Glossary. Weitere Informationen finden Sie unter DataZone Amazon-Terminologie und Konzepte. Um Felder in Metadatenformularen in Ihrer DataZone Amazon-Domain zu erstellen, zu bearbeiten oder zu löschen, müssen Sie Mitglied des jeweiligen Projekts sein und über die richtigen Anmeldeinformationen verfügen.

Gehen Sie wie folgt vor, um ein Feld in einem Metadatenformular zu erstellen:

1. Navigieren Sie mithilfe der DataZone Datenportal-URL zum Amazon-Datenportal und melden Sie sich mit Ihrem SSO oder Ihren AWS Anmeldeinformationen an. Wenn Sie ein DataZone Amazon-Administrator sind, können Sie die Datenportal-URL abrufen, indem Sie auf die DataZone Amazon-Konsole unter https://console.aws.amazon.com/datazone in dem AWS Konto zugreifen, in dem die DataZone Amazon-Domain erstellt wurde.
2. Navigieren Sie in der oberen Navigationsleiste neben Suchen zum Katalogmenü.
3. Wählen Sie im Amazon DataZone Data Portal Metadata Forms und dann das Metadaten-Formular aus, in dem Sie Feld (er) erstellen möchten.
4. Wählen Sie auf der Detailseite des Formulars die Option Feld erstellen aus.
5. Geben Sie den Feldnamen, die Beschreibung und den Typ an und geben Sie an, ob es sich um ein Pflichtfeld handelt, und wählen Sie dann Feld erstellen aus.

Gehen Sie wie folgt vor, um ein Feld in einem Metadatenformular zu bearbeiten:

1. Navigieren Sie mithilfe der DataZone Datenportal-URL zum Amazon-Datenportal und melden Sie sich mit Ihrem SSO oder Ihren AWS Anmeldeinformationen an. Wenn Sie ein DataZone Amazon-Administrator sind, können Sie die Datenportal-URL abrufen, indem Sie auf die DataZone Amazon-Konsole unter https://console.aws.amazon.com/datazone in dem AWS Konto zugreifen, in dem die DataZone Amazon-Domain erstellt wurde.
2. Navigieren Sie in der oberen Navigationsleiste neben Suchen zum Katalogmenü.
3. Wählen Sie im Amazon DataZone Data Portal Metadata Forms und dann das Metadaten-Formular aus, in dem Sie Feld (er) bearbeiten möchten.
4. Wählen Sie auf der Detailseite des Formulars das Feld aus, das Sie bearbeiten möchten, erweitern Sie dann Aktionen und wählen Sie Bearbeiten aus.
5. Aktualisieren Sie den Feldnamen, die Beschreibung, den Typ und geben Sie an, ob es sich um ein Pflichtfeld handelt, und wählen Sie dann Feld aktualisieren aus.

Gehen Sie wie folgt vor, um ein Feld in einem Metadatenformular zu löschen:

1. Navigieren Sie mithilfe der DataZone Datenportal-URL zum Amazon-Datenportal und melden Sie sich mit Ihrem SSO oder Ihren AWS Anmeldeinformationen an. Wenn Sie ein DataZone Amazon-Administrator sind, können Sie die Datenportal-URL abrufen, indem Sie auf die DataZone Amazon-Konsole unter https://console.aws.amazon.com/datazone in dem AWS Konto zugreifen, in dem die DataZone Amazon-Domain erstellt wurde.
2. Navigieren Sie in der oberen Navigationsleiste neben Suchen zum Katalogmenü.

3. Wählen Sie im Amazon DataZone Data Portal Metadata Forms und dann das Metadaten-Formular aus, in dem Sie Feld (er) löschen möchten.
4. Wählen Sie auf der Detailseite des Formulars das Feld aus, das Sie löschen möchten, erweitern Sie dann Aktionen und wählen Sie Löschen aus.
5. Bestätigen Sie den Löschvorgang, indem Sie Löschen wählen.

Arbeiten mit Projekten und Umgebungen in Amazon DataZone

In Amazon DataZone ermöglichen Projekte einer Gruppe von Benutzern die Zusammenarbeit bei verschiedenen geschäftlichen Anwendungsfällen, die das Veröffentlichen, Entdecken, Abonnieren und Verwenden von Datenbeständen im DataZone Amazon-Katalog beinhalten. Für jedes DataZone Amazon-Projekt gelten eine Reihe von Zugriffskontrollen, sodass nur autorisierte Personen, Gruppen und Rollen auf das Projekt und die Datenbestände zugreifen können, die dieses Projekt abonniert, und nur die Tools verwenden können, die durch die Projektberechtigungen definiert sind. Projekte agieren als Identitätsprinzipal, der Zugriffsberechtigungen auf zugrunde liegende Ressourcen erhält, sodass Amazon DataZone innerhalb der Infrastruktur eines Unternehmens arbeiten kann, ohne sich auf die Anmeldeinformationen einzelner Benutzer verlassen zu müssen. Weitere Informationen finden Sie unter DataZone Amazon-Terminologie und Konzepte.

Themen

Erstellen Sie ein Umgebungsprofil

In Amazon DataZone ist ein Umgebungsprofil eine Vorlage, mit der Sie Umgebungen erstellen können. Der Zweck eines Umgebungsprofils besteht darin, die Erstellung von Umgebungen zu vereinfachen, indem Platzierungsinformationen wie AWS Konto und Region in die Profile eingebettet

werden. Weitere Informationen finden Sie unter DataZone Amazon-Terminologie und Konzepte.
Um Umgebungsprofile in einer DataZone Amazon-Domain zu erstellen, müssen Sie zu einem DataZone Amazon-Projekt gehören. Alle Umgebungsprofile gehören Projekten und können von allen autorisierten Benutzern aus jedem Projekt verwendet werden, um neue Umgebungen zu erstellen.

Um ein Umgebungsprofil zu erstellen

1. Navigieren Sie mithilfe der DataZone Datenportal-URL zum Amazon-Datenportal und melden Sie sich mit Ihrem SSO oder Ihren AWS Anmeldeinformationen an. Wenn Sie ein DataZone Amazon-Administrator sind, können Sie die Datenportal-URL abrufen, indem Sie auf die DataZone Amazon-Konsole unter https://console.aws.amazon.com/datazone in dem AWS Konto zugreifen, in dem die DataZone Amazon-Domain erstellt wurde.
2. Wählen Sie im Datenportal die Option Projekte durchsuchen und wählen Sie das Projekt aus, in dem Sie das Umgebungsprofil erstellen möchten.
3. Navigieren Sie innerhalb des Projekts zur Registerkarte Umgebungen und wählen Sie dann Umgebungsprofil erstellen aus.
4. Konfigurieren Sie die folgenden Felder:

   - Name — Der Name für Ihr Umgebungsprofil.
   - Beschreibung — (Optional) Eine Beschreibung für Ihr Umgebungsprofil.
   - Besitzerprojekt — Das Projekt, in dem das Profil erstellt wird, ist standardmäßig in diesem Feld ausgewählt.
   - Blueprint — Der Blueprint, für den dieses Profil erstellt wurde. Sie können einen der DataZone Standard-Amazon-Blueprints (Data Lake oder Data Warehouse) wählen.

     Wenn Sie den Data Warehouse-Blueprint angegeben haben, gehen Sie wie folgt vor:

     - Geben Sie einen Parametersatz an. Um einen vorhandenen Parametersatz auszuwählen, wählen Sie die Option Parametersatz auswählen. Wenn Sie Ihre eigenen Parameter eingeben möchten, wählen Sie Meine eigenen eingeben.
     - Wenn Sie einen vorhandenen Parameter auswählen möchten, gehen Sie wie folgt vor:
       - Wählen Sie ein AWS Konto aus der Drop-down-Liste aus.
       - Wählen Sie einen Parametersatz aus der Drop-down-Liste aus.
     - Wenn Sie Ihre eigenen Parameter eingeben möchten, gehen Sie wie folgt vor:
       - Geben Sie die AWS Parameter an, indem Sie das AWS Konto und die Region aus der Dropdownliste auswählen.

- Geben Sie die Redshift Data Warehoue-Parameter an:
  - Wählen Sie entweder Amazon Redshift Cluster oder Amazon Redshift Serverless
  - Geben Sie den AWS geheimen ARN ein, der die Anmeldeinformationen für den ausgewählten Amazon Redshift-Cluster oder die Amazon Redshift Serverless-Arbeitsgruppe enthält. Das AWS Geheimnis muss mit der Domain-ID und der Projekt-ID gekennzeichnet sein, mit der Sie das Umgebungsprofil erstellen.
    - `AmazonDataZoneDomain: [Domain_ID]`
    - `AmazonDataZoneProject: [Project_ID]`
  - Geben Sie den Namen des Amazon Redshift-Clusters oder der Amazon Redshift Serverless Workgroup ein.
  - Geben Sie den Namen der Datenbank innerhalb des ausgewählten Amazon Redshift-Clusters oder der Amazon Redshift Serverless-Arbeitsgruppe ein.
- Geben Sie im Abschnitt Autorisierte Projekte die Projekte an, die das Umgebungsprofil zum Erstellen von Umgebungen verwenden können. Standardmäßig können alle Projekte innerhalb der Domäne die Umgebungsprofile im Konto verwenden, um Umgebungen zu erstellen. Um diese Standardeinstellung beizubehalten, wählen Sie Alle Projekte. Sie können dies jedoch einschränken, indem Sie der Umgebung autorisierte Projekte zuweisen. Wählen Sie dazu Nur autorisierte Projekte aus und geben Sie dann Projekte an, die dieses Projektprofil zum Erstellen von Umgebungen verwenden können.
- Wählen Sie im Bereich Veröffentlichen entweder eine der folgenden Optionen aus:
  - Aus einem beliebigen Schema veröffentlichen: Wenn Sie diese Option wählen, können Umgebungen, die mit diesem Umgebungsprofil erstellt wurden, verwendet werden, um aus jedem Schema innerhalb der Datenbank zu veröffentlichen, das in den oben angegebenen Redshift-Parametern ausgewählt wurde. Benutzer der Umgebung, die mit diesen Umgebungsprofilen erstellt wurde, können auch ihre eigenen Amazon Redshift Redshift-Parameter angeben, um sie aus einem beliebigen Schema innerhalb des AWS Kontos und der Region zu veröffentlichen, die im Umgebungsprofil ausgewählt wurden.
  - Nur aus dem Standardumgebungsschema veröffentlichen: Wenn Sie diese Option wählen, können Umgebungen, die mit diesem Schema erstellt wurden, verwendet werden, um nur anhand des von Amazon DataZone für diese Umgebung erstellten Standardschemas zu veröffentlichen. Benutzer der Umgebung, die mit diesen Umgebungsprofilen erstellt wurde, können keine eigenen Amazon Redshift Redshift-Parameter angeben.

- Veröffentlichung nicht zulassen: Wenn Sie diese Option wählen, können Umgebungen, die mit diesem Umgebungsprofil erstellt wurden, nur zum Abonnieren und Verwenden von Daten verwendet werden. Umgebungen können überhaupt nicht zum Veröffentlichen von Daten verwendet werden.

Wenn Sie den Data Lake-Blueprint angegeben haben, gehen Sie wie folgt vor:

- Geben Sie im Abschnitt AWS Kontoparameter die AWS Kontonummer und die AWS Kontoregion an, in der die potenziellen Umgebungen erstellt werden sollen.
- Geben Sie im Abschnitt Autorisierte Projekte die Projekte an, die das Umgebungsprofil mit dem integrierten Data Lake-Umgebungsprofil zum Erstellen von Umgebungen verwenden können. Standardmäßig können alle Projekte innerhalb der Domäne den Data Lake-Blueprint im Konto verwenden, um Umgebungsprofile zu erstellen. Um diese Standardeinstellung beizubehalten, wählen Sie Alle Projekte aus. Sie können dies jedoch einschränken, indem Sie dem Blueprint Projekte zuweisen. Wählen Sie dazu Nur autorisierte Projekte aus und geben Sie dann Projekte an, die dieses Projektprofil zum Erstellen von Umgebungen verwenden können.
- Wählen Sie im Abschnitt Datenbanken entweder Beliebige Datenbank aus, um die Veröffentlichung aus einer beliebigen Datenbank innerhalb des AWS Kontos und der Region zu ermöglichen, in der die Umgebung erstellt wurde, oder wählen Sie Nur Standarddatenbank, um die Veröffentlichung nur aus der Standard-Veröffentlichungsdatenbank zu ermöglichen, die mit der Umgebung erstellt wurde.

5. Wählen Sie „Umgebungsprofil erstellen“.

Bearbeiten Sie ein Umgebungsprofil

In Amazon DataZone ist ein Umgebungsprofil eine Vorlage, mit der Sie Umgebungen erstellen können. Weitere Informationen finden Sie unter DataZone Amazon-Terminologie und Konzepte. Um ein vorhandenes Umgebungsprofil in einer DataZone Amazon-Domain zu bearbeiten, müssen Sie zu einem DataZone Amazon-Projekt gehören.

Um ein Umgebungsprofil zu bearbeiten

1. Navigieren Sie zur URL des DataZone Amazon-Datenportals und melden Sie sich mit Single Sign-On (SSO) oder Ihren AWS Anmeldeinformationen an. Wenn Sie ein DataZone Amazon-Administrator sind, können Sie unter https://console.aws.amazon.com/datazone zur DataZone

Amazon-Konsole navigieren und sich dort anmelden, AWS-Konto wo die Domain erstellt wurde, und dann Datenportal öffnen wählen.

2. Wählen Sie im Datenportal die Option Projekte durchsuchen und wählen Sie das Projekt aus, in dem Sie das Umgebungsprofil bearbeiten möchten.
3. Navigieren Sie innerhalb des Projekts zur Registerkarte Umgebungen, wählen Sie dann Umgebungsprofile und dann das Umgebungsprofil aus, das Sie bearbeiten möchten.

   Wenn Sie ein Data Warehouse-Umgebungsprofil bearbeiten, können Sie nur den Namen und die Beschreibung eines vorhandenen Umgebungsprofils bearbeiten.

   Wenn Sie ein Data Lake-Umgebungsprofil bearbeiten, können Sie den Namen und die Beschreibung des Profils bearbeiten. Sie können auch die Projekte bearbeiten, die berechtigt sind, dieses Profil zum Erstellen von Umgebungen zu verwenden, und Sie können Datenbanken bearbeiten. Gehen Sie wie folgt vor, um diese Einstellungen zu bearbeiten:

   - Geben Sie im Abschnitt Autorisierte Projekte die Projekte an, die das Umgebungsprofil mit dem integrierten Data Lake-Umgebungsprofil zum Erstellen von Umgebungen verwenden können. Standardmäßig können alle Projekte innerhalb der Domäne den Data Lake-Blueprint im Konto verwenden, um Umgebungsprofile zu erstellen. Um diese Standardeinstellung beizubehalten, wählen Sie Alle Projekte aus. Sie können dies jedoch einschränken, indem Sie dem Blueprint Projekte zuweisen. Wählen Sie dazu Nur autorisierte Projekte aus und geben Sie dann Projekte an, die dieses Projektprofil zum Erstellen von Umgebungen verwenden können.
   - Wählen Sie im Abschnitt Datenbanken entweder Beliebige Datenbank aus, um die Veröffentlichung aus einer beliebigen Datenbank innerhalb des AWS Kontos und der Region zu ermöglichen, in der die Umgebung erstellt wurde, oder wählen Sie Nur Standarddatenbank, um die Veröffentlichung nur aus der Standard-Veröffentlichungsdatenbank zu ermöglichen, die mit der Umgebung erstellt wurde.

   Wenn Sie Ihre Änderungen abgeschlossen haben, wählen Sie Umgebungsprofil bearbeiten aus.

Löschen Sie ein Umgebungsprofil

In Amazon DataZone ist ein Umgebungsprofil eine Vorlage, mit der Sie Umgebungen erstellen können. Der Zweck eines Umgebungsprofils besteht darin, die Erstellung von Umgebungen zu vereinfachen, indem Platzierungsinformationen wie AWS Konto und Region in die Profile eingebettet

werden. Weitere Informationen finden Sie unter DataZone Amazon-Terminologie und Konzepte. Um Umgebungsprofile in einer DataZone Amazon-Domain zu löschen, müssen Sie zu einem DataZone Amazon-Projekt gehören.

> **Note**
>
> Wenn Sie ein Umgebungsprofil löschen, können Sie mit diesem Profil keine weiteren Umgebungen erstellen.

Um ein Umgebungsprofil zu löschen

1. Navigieren Sie zur URL des DataZone Amazon-Datenportals und melden Sie sich mit Single Sign-On (SSO) oder Ihren AWS Anmeldeinformationen an. Wenn Sie ein DataZone Amazon-Administrator sind, können Sie unter https://console.aws.amazon.com/datazone zur DataZone Amazon-Konsole navigieren und sich dort anmelden, AWS-Konto wo die Domain erstellt wurde, und dann Datenportal öffnen wählen.
2. Wählen Sie im Datenportal die Option Projekte durchsuchen und wählen Sie das Projekt aus, in dem Sie das Umgebungsprofil löschen möchten.
3. Navigieren Sie innerhalb des Projekts zur Registerkarte Umgebungen, wählen Sie dann Umgebungsprofile und dann das Umgebungsprofil aus, das Sie löschen möchten.
4. Wählen Sie das Umgebungsprofil aus, das Sie löschen möchten, und wählen Sie dann Aktionen, Löschen und bestätigen Sie den Löschvorgang.

Erstellen einer neuen Umgebung

In DataZone Amazon-Projekten sind Umgebungen Sammlungen konfigurierter Ressourcen (z. B. ein Amazon S3-Bucket, eine AWS Glue-Datenbank oder eine Amazon Athena Athena-Arbeitsgruppe) mit einem bestimmten Satz von IAM-Prinzipalen (Umgebungsbenutzerrollen) mit zugewiesenen Inhaber- oder Mitwirkendenberechtigungen, die mit diesen Ressourcen arbeiten können. Weitere Informationen finden Sie unter DataZone Amazon-Terminologie und Konzepte.

Jeder DataZone Amazon-Benutzer mit den erforderlichen Zugriffsberechtigungen für das Datenportal kann innerhalb eines Projekts eine DataZone Amazon-Umgebung erstellen.

Gehen Sie wie folgt vor, um eine neue Umgebung zu erstellen.

1. Navigieren Sie zur URL des DataZone Amazon-Datenportals und melden Sie sich mit Single Sign-On (SSO) oder Ihren AWS Anmeldeinformationen an. Wenn Sie ein DataZone Amazon-Administrator sind, können Sie unter https://console.aws.amazon.com/datazone zur DataZone Amazon-Konsole navigieren und sich dort anmelden, AWS-Konto wo die Domain erstellt wurde, und dann Datenportal öffnen wählen.
2. Wählen Sie Alle Projekte durchsuchen und wählen Sie das Projekt aus, in dem Sie eine neue Umgebung erstellen möchten.
3. Wählen Sie Umgebung erstellen, geben Sie Werte für die folgenden Felder ein und wählen Sie dann Umgebung erstellen aus:

   - Name — der Name der Umgebung
   - Beschreibung — eine Beschreibung der Umgebung
   - Umgebungsprofil — wählen Sie ein vorhandenes Umgebungsprofil aus oder erstellen Sie ein neues. Ein Umgebungsprofil ist eine Vorlage, mit der Sie Umgebungen erstellen können. Weitere Informationen finden Sie unter DataZone Amazon-Terminologie und Konzepte.

     Nachdem Sie das Umgebungsprofil ausgewählt haben, geben Sie im Abschnitt Parameter die Werte für die Felder an, die Teil dieses Umgebungsprofils sind.

Bearbeiten Sie eine Umgebung

In DataZone Amazon-Projekten sind Umgebungen Sammlungen konfigurierter Ressourcen (z. B. ein Amazon S3-Bucket, eine AWS Glue-Datenbank oder eine Amazon Athena Athena-Arbeitsgruppe) mit einem bestimmten Satz von IAM-Prinzipalen (mit zugewiesenen Mitwirkendenberechtigungen), die mit diesen Ressourcen arbeiten können. Weitere Informationen finden Sie unter DataZone Amazon-Terminologie und Konzepte.

Jeder DataZone Amazon-Benutzer mit den erforderlichen Zugriffsberechtigungen für das Datenportal kann eine DataZone Amazon-Umgebung innerhalb eines Projekts bearbeiten.

Gehen Sie wie folgt vor, um eine bestehende Umgebung zu bearbeiten.

1. Navigieren Sie zur URL des DataZone Amazon-Datenportals und melden Sie sich mit Single Sign-On (SSO) oder Ihren AWS Anmeldeinformationen an. Wenn Sie ein DataZone Amazon-Administrator sind, können Sie unter https://console.aws.amazon.com/datazone zur DataZone Amazon-Konsole navigieren und sich dort anmelden, AWS-Konto wo die Domain erstellt wurde, und dann Datenportal öffnen wählen.

2. Wählen Sie im oberen Navigationsbereich die Option Projekte durchsuchen und wählen Sie das Projekt aus, das die Umgebung enthält, die Sie bearbeiten möchten.
3. Suchen Sie die Umgebung und wählen Sie sie aus, um die zugehörige Detailseite zu öffnen. Erweitern Sie dann Aktionen und wählen Sie Umgebung bearbeiten aus.
4. Nehmen Sie Ihre Änderungen am Namen und der Beschreibung der Umgebung vor und wählen Sie dann Änderungen speichern.

Löschen Sie eine Umgebung

In DataZone Amazon-Projekten sind Umgebungen Sammlungen konfigurierter Ressourcen (z. B. ein Amazon S3-Bucket, eine AWS Glue-Datenbank oder eine Amazon Athena Athena-Arbeitsgruppe) mit einem bestimmten Satz von IAM-Prinzipalen (mit zugewiesenen Mitwirkendenberechtigungen), die mit diesen Ressourcen arbeiten können. Weitere Informationen finden Sie unter DataZone Amazon-Terminologie und Konzepte.

Jeder DataZone Amazon-Benutzer mit den erforderlichen Zugriffsberechtigungen für das Datenportal kann eine DataZone Amazon-Umgebung innerhalb eines Projekts löschen.

Gehen Sie wie folgt vor, um eine bestehende Umgebung zu löschen.

1. Navigieren Sie zur URL des DataZone Amazon-Datenportals und melden Sie sich mit Single Sign-On (SSO) oder Ihren AWS Anmeldeinformationen an. Wenn Sie ein DataZone Amazon-Administrator sind, können Sie unter https://console.aws.amazon.com/datazone zur DataZone Amazon-Konsole navigieren und sich dort anmelden, AWS-Konto wo die Domain erstellt wurde, und dann Datenportal öffnen wählen.
2. Wählen Sie im oberen Navigationsbereich die Option Projekt durchsuchen und wählen Sie das Projekt aus, das die Umgebung enthält, die Sie löschen möchten.
3. Suchen Sie die Umgebung und wählen Sie sie aus, um die zugehörige Detailseite zu öffnen. Erweitern Sie dann Aktionen und wählen Sie Umgebung löschen aus.
4. Bestätigen Sie im Popupfenster Umgebung löschen den Löschvorgang, indem Sie `Delete` etwas in das Feld eingeben und dann Umgebung löschen wählen.

   Sie können eine Umgebung erst erfolgreich löschen, nachdem alle Entitäten, die von dieser Umgebung abhängig sind, gelöscht wurden. Um eine Umgebung zu löschen, müssen Sie zuerst alle zugehörigen Datenquellen und Abonnementziele löschen.

Erstellen eines neuen Projekts

In Amazon DataZone ermöglichen Projekte einer Gruppe von Benutzern die Zusammenarbeit bei verschiedenen geschäftlichen Anwendungsfällen, die das Veröffentlichen, Entdecken, Abonnieren und Verwenden von Datenbeständen im DataZone Amazon-Katalog beinhalten. Weitere Informationen finden Sie unter DataZone Amazon-Terminologie und Konzepte.

Jeder DataZone Amazon-Benutzer mit den erforderlichen Zugriffsberechtigungen für das Datenportal kann ein DataZone Amazon-Projekt erstellen.

Gehen Sie wie folgt vor, um ein neues Projekt zu erstellen.

1. Navigieren Sie zur URL des DataZone Amazon-Datenportals und melden Sie sich mit Single Sign-On (SSO) oder Ihren AWS Anmeldeinformationen an. Wenn Sie ein DataZone Amazon-Administrator sind, können Sie unter https://console.aws.amazon.com/datazone zur DataZone Amazon-Konsole navigieren und sich dort anmelden, AWS-Konto wo die Domain erstellt wurde, und dann Datenportal öffnen wählen.
2. Wählen Sie im DataZone Amazon-Datenportal die Option Create Project aus.
3. Geben Sie Werte für die folgenden Felder an und wählen Sie dann Projekt erstellen aus:
   - Name — Der Projektname.
   - Beschreibung — Eine Beschreibung des Projekts.

Projekt bearbeiten

In Amazon DataZone ermöglichen Projekte einer Gruppe von Benutzern die Zusammenarbeit bei verschiedenen geschäftlichen Anwendungsfällen, die das Veröffentlichen, Entdecken, Abonnieren und Verwenden von Datenbeständen im DataZone Amazon-Katalog beinhalten. Weitere Informationen finden Sie unter DataZone Amazon-Terminologie und Konzepte. Um ein DataZone Amazon-Projekt bearbeiten zu können, müssen Sie der Eigentümer dieses Projekts oder der Domain-Administrator der Domain sein, die dieses Projekt enthält.

Gehen Sie wie folgt vor, um ein vorhandenes Projekt zu bearbeiten.

1. Navigieren Sie zur URL des DataZone Amazon-Datenportals und melden Sie sich mit Single Sign-On (SSO) oder Ihren AWS Anmeldeinformationen an. Wenn Sie ein DataZone Amazon-Administrator sind, können Sie unter https://console.aws.amazon.com/datazone zur DataZone

Amazon-Konsole navigieren und sich dort anmelden, AWS-Konto wo die Domain erstellt wurde, und dann Datenportal öffnen wählen.

2. Wählen Sie Projekte durchsuchen.
3. Wählen Sie das Projekt aus, das Sie bearbeiten möchten. Wenn Sie es nicht ohne weiteres in der Projektliste finden, können Sie danach suchen, indem Sie den Projektnamen im Feld Projekt suchen angeben.
4. Erweitern Sie Aktionen und wählen Sie Projekt bearbeiten.
5. Aktualisieren Sie den Projektnamen und die Beschreibung und wählen Sie dann Speichern.

Projekt löschen

In Amazon DataZone ermöglichen Projekte einer Gruppe von Benutzern die Zusammenarbeit bei verschiedenen geschäftlichen Anwendungsfällen, die das Veröffentlichen, Entdecken, Abonnieren und/oder Verwenden von Datenbeständen im DataZone Amazon-Katalog beinhalten. Weitere Informationen finden Sie unter DataZone Amazon-Terminologie und Konzepte.

Das Löschen eines Projekts ist endgültig. Durch das Löschen werden die Inhalte des Projekts, einschließlich Datenquellen, Umgebungen, Ressourcen, Glossare und Metadatenformulare, unwiderruflich gelöscht. Amazon DataZone widerruft Zuschüsse, die Amazon DataZone über Lake Formation und Amazon Redshift für verwaltete Vermögenswerte gewährt hat. Durch das Löschen eines Projekts werden keine DataZone AWS Ressourcen gelöscht, die nicht von Amazon stammen und bei deren Erstellung Amazon Ihnen DataZone möglicherweise geholfen hat. Wenn Sie diese AWS Ressourcen nicht mehr benötigen, löschen Sie sie in ihrem jeweiligen AWS Service und Konto.

Um ein DataZone Amazon-Projekt zu löschen, müssen Sie Eigentümer des Projekts sein.

Gehen Sie wie folgt vor, um ein vorhandenes Projekt zu löschen.

1. Navigieren Sie zur URL des DataZone Amazon-Datenportals und melden Sie sich mit Single Sign-On (SSO) oder Ihren AWS Anmeldeinformationen an. Ein IAM-Principal kann unter https://console.aws.amazon.com/datazone zur DataZone Amazon-Konsole navigieren und sich dort anmelden, AWS-Konto wo die Domain erstellt wurde, und dann Datenportal öffnen auswählen.
2. Wählen Sie im oberen Navigationsbereich die Option Projekte durchsuchen aus.
3. Wählen Sie das Projekt aus, das Sie löschen möchten. Wenn Sie es nicht in der Projektliste sehen, können Sie danach suchen, indem Sie den Projektnamen im Feld Projekt suchen angeben.

4. Erweitern Sie Aktionen und wählen Sie Projekt löschen.

   Lesen Sie die Informationswarnungen zu den möglichen Auswirkungen des Löschens des Projekts.

5. Wenn Sie die Warnungen akzeptieren, geben Sie den Bestätigungstext ein und wählen Sie Löschen.

> **Important**
>
> Das Löschen eines Projekts ist eine unwiderrufliche Aktion, die weder von Ihnen noch von rückgängig gemacht werden kann. AWS

> **Note**
>
> Wenn Sie oder Ihre Domain-Benutzer eine Umgebung in einem Projekt erstellen, DataZone erstellt Amazon AWS Ressourcen in Ihrer Domain oder den zugehörigen Konten, um Ihnen und Ihren Domain-Benutzern Funktionen zur Verfügung zu stellen. Im Folgenden finden Sie eine Liste der AWS Ressourcen, die Amazon für ein Projekt erstellen DataZone kann, zusammen mit dem Standardnamen. Durch das Löschen eines Projekts werden keine dieser AWS Ressourcen in Ihren AWS Konten gelöscht.
>
> - <environmentId>IAM-Rollen: datazone_usr_.
> - <environmentName>Glue-Datenbanken: (1) <environmentName>_pub_db-*, (2) _sub_db-*. Wenn es bereits eine Datenbank mit diesem Namen gab, DataZone fügt Amazon die Umgebungs-ID hinzu.
> - <environmentName>Athena-Arbeitsgruppen: -*. Wenn es bereits eine Arbeitsgruppe mit diesem Namen gab, fügt Amazon DataZone die Umgebungs-ID hinzu.
> - CloudWatch Protokollgruppe: datazone_ <environmentId>

Projekt verlassen

In Amazon DataZone ermöglichen Projekte einer Gruppe von Benutzern die Zusammenarbeit bei verschiedenen geschäftlichen Anwendungsfällen, die das Veröffentlichen, Entdecken,

Abonnieren und Verwenden von Datenbeständen im DataZone Amazon-Katalog beinhalten. Weitere Informationen finden Sie unter DataZone Amazon-Terminologie und Konzepte.

Gehen Sie wie folgt vor, um ein bestehendes Projekt zu verlassen.

1. Navigieren Sie zur URL des DataZone Amazon-Datenportals und melden Sie sich mit Single Sign-On (SSO) oder Ihren AWS Anmeldeinformationen an. Wenn Sie ein DataZone Amazon-Administrator sind, können Sie unter https://console.aws.amazon.com/datazone zur DataZone Amazon-Konsole navigieren und sich dort anmelden, AWS-Konto wo die Domain erstellt wurde, und dann Datenportal öffnen wählen.
2. Wählen Sie im oberen Navigationsbereich die Option Projekt auswählen und wählen Sie das Projekt aus.
3. Wählen Sie das Projekt aus, das Sie verlassen möchten. Wenn Sie es nicht ohne weiteres in der Projektliste finden, können Sie danach suchen, indem Sie den Projektnamen im Feld Projekt suchen angeben.
4. Erweitern Sie Aktionen und wählen Sie Projekt verlassen aus.

Füge Mitglieder zu einem Projekt hinzu

In Amazon DataZone ermöglichen Projekte einer Gruppe von Benutzern die Zusammenarbeit bei verschiedenen geschäftlichen Anwendungsfällen, die das Veröffentlichen, Entdecken, Abonnieren und Verwenden von Datenbeständen im DataZone Amazon-Katalog beinhalten. Weitere Informationen finden Sie unter DataZone Amazon-Terminologie und Konzepte.

Sie müssen Projektinhaber oder Mitwirkender sein, um Mitglieder zu einem Projekt hinzufügen zu können. Sie können SSO-Gruppen, SSO-Benutzer oder IAM-Prinzipale (Rollen oder Benutzer) als Projektmitglieder hinzufügen.

Gehen Sie wie folgt vor, um Mitglieder zu einem bestehenden Projekt hinzuzufügen.

1. Navigieren Sie zur URL des DataZone Amazon-Datenportals und melden Sie sich mit Single Sign-On (SSO) oder Ihren AWS Anmeldeinformationen an. Wenn Sie ein DataZone Amazon-Administrator sind, können Sie unter https://console.aws.amazon.com/datazone zur DataZone Amazon-Konsole navigieren und sich dort anmelden, AWS-Konto wo die Domain erstellt wurde, und dann Datenportal öffnen wählen.
2. Wählen Sie im oberen Navigationsbereich die Option Projekt auswählen und wählen Sie das Projekt aus.

3. Wählen Sie das Projekt aus, zu dem Sie Mitglieder hinzufügen möchten. Wenn Sie es nicht ohne weiteres in der Projektliste finden, können Sie danach suchen, indem Sie den Projektnamen im Feld Projekt suchen angeben.
4. Wählen Sie auf der Detailseite des Projekts die Registerkarte Mitglieder und dann den Knoten Alle Mitglieder auswählen aus.
5. Wählen Sie auf der Registerkarte Projektmitglieder die Option Mitglieder hinzufügen aus.
6. Geben Sie im Popup-Fenster Mitglieder zum Projekt hinzufügen die Benutzer an, die Sie hinzufügen möchten, und geben Sie deren Rolle innerhalb des Projekts an (Eigentümer oder Mitwirkender). Wählen Sie dann Mitglieder hinzufügen aus.

> **Note**
>
> Sie können einen IAM-Prinzipal als Projektmitglied hinzufügen, wenn dieser Principal bereits über ein DataZone Amazon-Benutzerprofil in der Domain verfügt. Amazon erstellt DataZone automatisch ein Benutzerprofil für einen IAM-Principal, wenn dieser erfolgreich über das Portal, die API oder die CLI mit der Domain interagiert. Sie können kein Benutzerprofil für einen IAM-Principal erstellen. Um IAM-Prinzipale als Projektmitglieder hinzuzufügen, falls der IAM-Principal kein vorhandenes DataZone Amazon-Benutzerprofil in der Domain hat, bitten Sie Ihren Administrator, die folgenden beiden IAM-Berechtigungen zu Ihren Domains AmazonDataZoneDomainExecutionRolein der IAM-Konsole hinzuzufügen: und. `iam:GetUser` `iam:GetRole` Unabhängig davon muss der IAM-Principal über die entsprechenden IAM-Berechtigungen für solche Aktionen verfügen, um Aktionen in der Domain ausführen zu können.

Mitglieder aus einem Projekt entfernen

In Amazon DataZone ermöglichen Projekte einer Gruppe von Benutzern die Zusammenarbeit bei verschiedenen geschäftlichen Anwendungsfällen, die das Veröffentlichen, Entdecken, Abonnieren und Verwenden von Datenbeständen im DataZone Amazon-Katalog beinhalten. Weitere Informationen finden Sie unter DataZone Amazon-Terminologie und Konzepte. Sie müssen ein Projekteigentümer sein, um Mitglieder aus einem Projekt entfernen zu können.

Gehen Sie wie folgt vor, um Mitglieder aus einem bestehenden Projekt zu entfernen.

1. Navigieren Sie mithilfe der DataZone Datenportal-URL zum Amazon-Datenportal und melden Sie sich mit Ihrem SSO oder Ihren AWS Anmeldeinformationen an. Wenn Sie ein DataZone Amazon-Administrator sind, können Sie die Datenportal-URL abrufen, indem Sie auf die DataZone Amazon-Konsole unter https://console.aws.amazon.com/datazone in dem AWS Konto zugreifen, in dem die DataZone Amazon-Domain erstellt wurde.
2. Wählen Sie im oberen Navigationsbereich die Option Projekt auswählen und wählen Sie das Projekt aus.
3. Wählen Sie das Projekt aus, aus dem Sie Mitglieder entfernen möchten. Wenn Sie es nicht ohne weiteres in der Projektliste finden, können Sie danach suchen, indem Sie den Projektnamen im Feld Projekt suchen angeben.
4. Wählen Sie auf der Detailseite des Projekts die Registerkarte Mitglieder und dann den Knoten Alle Mitglieder auswählen aus.
5. Wählen Sie auf der Registerkarte Projektmitglieder die Mitglieder aus, die Sie aus dem Projekt entfernen möchten, und klicken Sie dann auf Entfernen.
6. Bestätigen Sie im Popupfenster Mitglieder entfernen das Entfernen, indem Sie Mitglieder entfernen wählen.

Inventar erstellen und Daten in Amazon veröffentlichen DataZone

In diesem Abschnitt werden die Aufgaben und Verfahren beschrieben, die Sie ausführen möchten, um ein Inventar Ihrer Daten bei Amazon zu erstellen DataZone und Ihre Daten bei Amazon zu veröffentlichen DataZone.

Um Amazon für die Katalogisierung Ihrer Daten verwenden DataZone zu können, müssen Sie zunächst Ihre Daten (Assets) als Inventar Ihres Projekts in Amazon speichern DataZone. Durch die Erstellung eines Inventars für ein bestimmtes Projekt sind die Ressourcen nur für die Mitglieder dieses Projekts auffindbar. Objekte aus dem Projektinventar stehen nicht allen Domänenbenutzern beim Suchen/Durchsuchen zur Verfügung, sofern sie nicht ausdrücklich veröffentlicht wurden. Nach der Erstellung eines Projektinventars können Dateneigentümer ihre Inventarressourcen mit den erforderlichen Geschäftsmetadaten kuratieren, indem sie Unternehmensnamen (Asset und Schema), Beschreibungen (Asset und Schema), Readme, Glossarbegriffe (Asset und Schema) und Metadatenformulare hinzufügen oder aktualisieren.

Der nächste Schritt bei der Verwendung von Amazon DataZone zur Katalogisierung Ihrer Daten besteht darin, die Inventarressourcen Ihres Projekts für die Domain-Benutzer auffindbar zu machen. Sie können dies tun, indem Sie die Inventarressourcen im DataZone Amazon-Katalog veröffentlichen. Nur die neueste Version des Inventarbestands kann im Katalog veröffentlicht werden, und nur die zuletzt veröffentlichte Version ist im Discovery-Katalog aktiv. Wenn ein Inventar-Asset aktualisiert wird, nachdem es im DataZone Amazon-Katalog veröffentlicht wurde, müssen Sie es explizit erneut veröffentlichen, damit die neueste Version im Discovery-Katalog angezeigt wird.

Themen

- Veröffentlichung eines Assets aus dem DataZone Amazon-Katalog rückgängig machen
- Löschen Sie ein DataZone Amazon-Asset
- Manuelles Starten einer Datenquellenausführung in Amazon DataZone
- Überarbeitungen von Vermögenswerten bei Amazon DataZone
- Datenqualität bei Amazon DataZone
- Einsatz von maschinellem Lernen und generativer KI

Lake Formation Formation-Berechtigungen für Amazon konfigurieren DataZone

Wenn Sie eine Umgebung mit dem integrierten Data Lake-Blueprint (DefaultDataLake) erstellen, wird eine AWS Glue-Datenbank in Amazon DataZone als Teil des Erstellungsprozesses dieser Umgebung hinzugefügt. Wenn Sie Assets aus dieser AWS Glue-Datenbank veröffentlichen möchten, sind keine zusätzlichen Berechtigungen erforderlich.

Wenn Sie jedoch Assets aus einer Glue-Datenbank veröffentlichen und Assets aus einer AWS Glue-Datenbank abonnieren möchten, die außerhalb Ihrer DataZone Amazon-Umgebung existiert, müssen Sie Amazon DataZone ausdrücklich die Berechtigungen für den Zugriff auf Tabellen in dieser externen AWS Glue-Datenbank gewähren. Dazu müssen Sie die folgenden Einstellungen in AWS Lake Formation vornehmen und die erforderlichen Lake Formation Formation-Berechtigungen an den anhängenAmazonDataZoneGlueAccess- <region>- <domainId>.

- Konfigurieren Sie den Amazon S3 S3-Standort für Ihren Data Lake in AWS Lake Formation mit dem Lake Formation Formation-Berechtigungsmodus oder dem Hybrid-Zugriffsmodus. Weitere Informationen finden Sie unter https://docs.aws.amazon.com/lake-formation/latest/dg/ register-data-lake .html.
- Entfernen Sie die `IAMAllowedPrincipals` Berechtigung aus den Amazon Lake Formation-Tabellen, für die Amazon Berechtigungen DataZone verwaltet. Weitere Informationen finden Sie unter https://docs.aws.amazon.com/lake-formation/latest/dg/ upgrade-glue-lake-formation - background.html.
- Hängen Sie die folgenden AWS Lake Formation Formation-Berechtigungen anAmazonDataZoneGlueAccess- <region>- <domainId>:
  - `Describe`und `Describe grantable` Berechtigungen für die Datenbank, in der die Tabellen existieren

- `Describe`, `SelectDescribe Grantable`, `Select Grantable` Berechtigungen für alle Tabellen in der obigen Datenbank, deren Zugriff Sie in Ihrem Namen verwalten möchten DataZone .

> **Note**
>
> Amazon DataZone unterstützt den AWS Lake Formation Hybrid-Modus. Der Lake Formation-Hybridmodus ermöglicht es Ihnen, mit der Verwaltung von Berechtigungen für Ihre AWS Glue-Datenbanken und -Tabellen über Lake Formation zu beginnen und gleichzeitig alle vorhandenen IAM-Berechtigungen für diese Tabellen und Datenbanken beizubehalten. Weitere Informationen finden Sie unter DataZone Amazon-Integration mit dem AWS Lake Formation Formation-Hybridmodus .

Weitere Informationen finden Sie unter Fehlerbehebung bei AWS Lake Formation Formation-Berechtigungen für Amazon DataZone.

DataZone Amazon-Integration mit dem AWS Lake Formation Formation-Hybridmodus

Amazon DataZone ist in den AWS Lake Formation Formation-Hybridmodus integriert. Diese Integration ermöglicht es Ihnen, Ihre AWS Glue-Tabellen einfach über Amazon zu veröffentlichen und zu teilen, DataZone ohne sie zuerst in AWS Lake Formation registrieren zu müssen. Im Hybridmodus können Sie mit der Verwaltung von Berechtigungen für Ihre AWS Glue-Tabellen über AWS Lake Formation beginnen und gleichzeitig alle vorhandenen IAM-Berechtigungen für diese Tabellen beibehalten.

Zu Beginn können Sie die Einstellung für die Registrierung des Datenstandorts unter dem DefaultDataLakeBlueprint in der DataZone Amazon-Managementkonsole aktivieren.

Aktivieren Sie die Integration mit dem AWS Lake Formation Formation-Hybridmodus

1. Rufen Sie die DataZone Amazon-Konsole unter https://console.aws.amazon.com/datazone auf und melden Sie sich mit Ihren Kontoanmeldeinformationen an.
2. Wählen Sie Domänen anzeigen und wählen Sie die Domain aus, in der Sie die Integration mit dem AWS Lake Formation Formation-Hybridmodus aktivieren möchten.
3. Navigieren Sie auf der Seite mit den Domänendetails zur Registerkarte Blueprints.

4. Wählen Sie in der Blueprint-Liste den DefaultDataLakeBlueprint aus.
5. Stellen Sie sicher, dass der DefaultDataLake Blueprint aktiviert ist. Wenn es nicht aktiviert ist, folgen Sie den Schritten unter, Aktivieren Sie integrierte Blueprints in dem AWS Konto, dem die DataZone Amazon-Domain gehört um es in Ihrem AWS Konto zu aktivieren.
6. Öffnen Sie auf der DefaultDataLake Detailseite den Tab Provisioning und wählen Sie in der oberen rechten Ecke der Seite die Schaltfläche Bearbeiten aus.
7. Aktivieren Sie unter Registrierung des Datenstandorts das Kontrollkästchen, um die Registrierung des Datenstandorts zu aktivieren.
8. Für die Datenstandortverwaltungsrolle können Sie eine neue IAM-Rolle erstellen oder eine vorhandene IAM-Rolle auswählen. Amazon DataZone verwendet diese Rolle, um den Lese-/Schreibzugriff auf die ausgewählten Amazon S3 S3-Buckets für Data Lake im AWS Lake Formation Formation-Hybridzugriffsmodus zu verwalten. Weitere Informationen finden Sie unter AmazonDataZone<region>S3 Manage- - <domainId>.
9. Optional können Sie bestimmte Amazon S3 S3-Standorte ausschließen, wenn Sie nicht möchten, dass Amazon DataZone sie automatisch im Hybridmodus registriert. Führen Sie dazu die folgenden Schritte aus:

    - Wählen Sie die Umschaltfläche, um bestimmte Amazon S3 S3-Standorte auszuschließen.
    - Geben Sie die URI des Amazon S3 S3-Buckets an, den Sie ausschließen möchten.
    - Um weitere Buckets hinzuzufügen, wählen Sie S3-Standort hinzufügen.

    > **Note**
    >
    > Amazon erlaubt DataZone nur den Ausschluss eines Root-S3-Standorts. Alle S3-Standorte innerhalb des Pfads eines S3-Stammstandorts werden automatisch von der Registrierung ausgeschlossen.

    - Wählen Sie Änderungen speichern aus.

Sobald Sie die Einstellung für die Registrierung des Datenstandorts in Ihrem AWS Konto aktiviert haben und ein Datenverbraucher eine über IAM-Berechtigungen verwaltete AWS Glue-Tabelle abonniert, registriert Amazon zunächst die Amazon S3 S3-Standorte dieser Tabelle im Hybridmodus und gewährt dann dem Datenverbraucher Zugriff, indem die Berechtigungen für die Tabelle über AWS Lake Formation verwaltet DataZone werden. Dadurch wird sichergestellt, dass die IAM-Berechtigungen für die Tabelle auch mit den neu erteilten AWS Lake Formation Formation-Berechtigungen bestehen bleiben, ohne bestehende Workflows zu stören.

Umgang mit verschlüsselten Amazon S3 S3-Standorten bei der Aktivierung der AWS Lake Formation Formation-Hybridmodus-Integration in Amazon DataZone

Wenn Sie einen Amazon S3 S3-Standort verwenden, der mit einem vom Kunden verwalteten oder AWS verwalteten KMS-Schlüssel verschlüsselt ist, muss die AmazonDataZoneS3Manage-Rolle über die Berechtigung verfügen, Daten mit dem KMS-Schlüssel zu verschlüsseln und zu entschlüsseln, oder die KMS-Schlüsselrichtlinie muss Berechtigungen für den Schlüssel für die Rolle gewähren.

Wenn Ihr Amazon S3 S3-Standort mit einem AWS verwalteten Schlüssel verschlüsselt ist, fügen Sie der AmazonDataZoneDataLocationManagementRolle die folgende Inline-Richtlinie hinzu:

```
 {
"Version": "2012-10-17",
"Statement": [
  {
    "Effect": "Allow",
    "Action": [
      "kms:Encrypt",
      "kms:Decrypt",
      "kms:ReEncrypt*",
      "kms:GenerateDataKey*",
      "kms:DescribeKey"
    ],
    "Resource": "<AWS managed key ARN>"
  }
]
```

Wenn Ihr Amazon S3 S3-Standort mit einem vom Kunden verwalteten Schlüssel verschlüsselt ist, gehen Sie wie folgt vor:

1. Öffnen Sie die AWS KMS-Konsole unter https://console.aws.amazon.com/kms und melden Sie sich als Administrator für AWS Identity and Access Management (IAM) an oder als Benutzer, 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 die AmazonDataZoneDataLocationManagementRolle hinzu.
   - Wenn die Schlüsselrichtlinie (JSON) angezeigt wird, bearbeiten Sie die Richtlinie, um dem Objekt „Verwendung des Schlüssels zulassen“ AmazonDataZoneDataLocationManagementeine Rolle hinzuzufügen, wie im folgenden Beispiel gezeigt

```
...
        {
            "Sid": "Allow use of the key",
            "Effect": "Allow",
            "Principal": {
                "AWS": [
                    "arn:aws:iam::111122223333:role/service-role/
AmazonDataZoneDataLocationManage-<region>-<domain-id>",
                    "arn:aws:iam::111122223333:user/keyuser"
                ]
            },
            "Action": [
                "kms:Encrypt",
                "kms:Decrypt",
                "kms:ReEncrypt*",
                "kms:GenerateDataKey*",
                "kms:DescribeKey"
            ],
            "Resource": "*"
        },
        ...
```

> **Note**
>
> Wenn sich der KMS-Schlüssel oder der Amazon S3 S3-Standort nicht in demselben AWS Konto wie der Datenkatalog befinden, folgen Sie den Anweisungen unter AWS Kontoübergreifende Registrierung eines verschlüsselten Amazon S3 S3-Standorts.

Erstellen Sie benutzerdefinierte Asset-Typen

In Amazon DataZone stellen Assets bestimmte Arten von Datenressourcen wie Datenbanktabellen, Dashboards oder Modelle für maschinelles Lernen dar. Um Konsistenz und Standardisierung bei der Beschreibung von Katalog-Assets zu gewährleisten, muss eine DataZone Amazon-Domain über eine Reihe von Asset-Typen verfügen, die definieren, wie Assets im Katalog dargestellt werden. Ein Asset-Typ definiert das Schema für einen bestimmten Asset-Typ. Ein Asset-Typ hat eine Reihe erforderlicher und optionaler benennbarer Metadaten-Formulartypen (z. B. GovForm oder). GovernanceFormType Die Asset-Typen in Amazon DataZone sind versioniert. Wenn Assets erstellt werden, werden sie anhand des Schemas validiert, das durch ihren Asset-Typ (in der Regel die neueste Version) definiert ist. Wenn eine ungültige Struktur angegeben wird, schlägt die Asset-Erstellung fehl.

System-Asset-Typen — DataZone Amazon stellt serviceeigene System-Asset-Typen (einschließlich GlueTableAssetType GlueViewAssetType RedshiftTableAssetType, RedshiftViewAssetType,, und S3ObjectCollectionAssetType) und Systemformtypen (einschließlich DataSourceReferenceFormType AssetCommonDetailsFormType, und SubscriptionTermsFormType) bereit. System-Asset-Typen können nicht bearbeitet werden.

Benutzerdefinierte Asset-Typen — Um benutzerdefinierte Asset-Typen zu erstellen, erstellen Sie zunächst die erforderlichen Metadaten-Formulartypen und Glossare, die in den Formulartypen verwendet werden sollen. Anschließend können Sie benutzerdefinierte Asset-Typen erstellen, indem Sie den Namen, die Beschreibung und die zugehörigen Metadatenformulare angeben, die erforderlich oder optional sein können.

Bei Assettypen mit strukturierten Daten können Sie zur Darstellung des Spaltenschemas im Datenportal die verwenden, `RelationalTableFormType` um Ihren Spalten die technischen Metadaten hinzuzufügen (einschließlich Spaltennamen, Beschreibungen und Datentypen) und die, `ColumnBusinessMetadataForm` um die Unternehmensbeschreibungen der Spalten hinzuzufügen, einschließlich Unternehmensnamen, Glossarbegriffen und benutzerdefinierten Schlüsselwertpaaren.

Gehen Sie wie folgt vor, um über das Datenportal einen benutzerdefinierten Asset-Typ zu erstellen:

1. Navigieren Sie zur URL des DataZone Amazon-Datenportals und melden Sie sich mit Single Sign-On (SSO) oder Ihren AWS Anmeldeinformationen an. Wenn Sie ein DataZone Amazon-Administrator sind, können Sie unter https://console.aws.amazon.com/datazone zur DataZone Amazon-Konsole navigieren und sich dort anmelden, AWS-Konto wo die Domain erstellt wurde, und dann Datenportal öffnen wählen.
2. Wählen Sie im oberen Navigationsbereich die Option Projekt auswählen und wählen Sie das Projekt aus, für das Sie einen benutzerdefinierten Asset-Typ erstellen möchten.
3. Navigieren Sie zur Registerkarte Daten für das Projekt.
4. Wählen Sie im linken Navigationsbereich die Option Asset-Typen und anschließend Asset-Typ erstellen aus.
5. Geben Sie Folgendes an und wählen Sie dann „Erstellen“.
   - Name — der Name des benutzerdefinierten Asset-Typs
   - Beschreibung — die Beschreibung des benutzerdefinierten Asset-Typs.
   - Wählen Sie Metadatenformulare hinzufügen, um diesem benutzerdefinierten Asset-Typ Metadatenformulare hinzuzufügen.
6. Sobald der benutzerdefinierte Asset-Typ erstellt wurde, können Sie ihn zum Erstellen von Assets verwenden.

Gehen Sie wie folgt vor, um über die APIs einen benutzerdefinierten Asset-Typ zu erstellen:

1. Erstellen Sie einen Metadaten-Formulartyp, indem Sie die `CreateFormType` API-Aktion aufrufen.

   Das Folgende ist ein SageMaker Amazon-Beispiel:

```
m_model = "

structure SageMakerModelFormType {
   @required
   @amazon.datazone#searchable
   modelName: String

   @required
   modelArn: String
```

```
   @required
   creationTime: String
}
"

CreateFormType(
    domainIdentifier="my-dz-domain",
    owningProjectIdentifier="d4bywm0cja1dbb",
    name="SageMakerModelFormType",
    model=m_model
    status="ENABLED"
    )
```

2. Als Nächstes können Sie einen Asset-Typ erstellen, indem Sie die `CreateAssetType` API-Aktion aufrufen. Sie können Asset-Typen nur über DataZone Amazon-APIs erstellen, indem Sie die verfügbaren Systemformulartypen (`SubscriptionTermsFormType`im folgenden Beispiel) oder Ihre benutzerdefinierten Formulartypen verwenden. Bei Systemformulartypen muss der Typname mit beginnen`amazon.datazone`.

```
CreateAssetType(
    domainIdentifier="my-dz-domain",
    owningProjectIdentifier="d4bywm0cja1dbb",
    name="SageMakerModelAssetType",
    formsInput={
        "ModelMetadata": {
            "typeIdentifier": "SageMakerModelMetadataFormType",
            "typeRevision": 7,
            "required": True,
        },
        "SubscriptionTerms": {
            "typeIdentifier": "amazon.datazone.SubscriptionTermsFormType",
            "typeRevision": 1,
            "required": False,
        },
    },
)
```

Im Folgenden finden Sie ein Beispiel für die Erstellung eines Asset-Typs für strukturierte Daten:

```
CreateAssetType(
    domainIdentifier="my-dz-domain",
    owningProjectIdentifier="d4bywm0cja1dbb",
    name="OnPremMySQLAssetType",
    formsInput={
        "OnpremMySQLForm": {
            "typeIdentifier": "OnpremMySQLFormType",
            "typeRevision": 5,
            "required": True,
        },
        "RelationalTableForm": {
            "typeIdentifier": "RelationalTableFormType",
            "typeRevision": 1,
            "required": True,
        },
        "ColumnBusinessMetadataForm": {
            "typeIdentifier": "ColumnBusinessMetadataForm",
            "typeRevision": 1,
            "required": False,
        },
        "SubscriptionTerms": {
            "typeIdentifier": "SubscriptionTermsFormType",
            "typeRevision": 1,
            "required": False,
        },
    },
)
```

3. Und jetzt können Sie ein Asset mit den benutzerdefinierten Asset-Typen erstellen, die Sie in den obigen Schritten erstellt haben.

```
CreateAsset(
   domainIdentifier="my-dz-domain",
   owningProjectIdentifier="d4bywm0cja1dbb",
   owningProjectIdentifier="my-project",
   name="MyModelAsset",
```

```
   glossaryTerms="xxx",
   formsInput=[{
        "formName": "SageMakerModelForm",
        "typeIdentifier": "SageMakerModelForm",
        "typeRevision": "5",
        "content": "{\n \"ModelName\" : \"sample-ModelName\",\n \"ModelArn\" :
 \"999999911111\"\n}"
        }
        ]
)
```

Und in diesem Beispiel erstellen Sie ein strukturiertes Daten-Asset:

```
CreateAsset(
   domainIdentifier="my-dz-domain",
   owningProjectIdentifier="d4bywm0cja1dbb",
   name="MyModelAsset",
   glossaryTerms="xxx",
   formsInput=[{
        "formName": "RelationalTableForm",
        "typeIdentifier": "amazon.datazone.RelationalTableForm",
        "typeRevision": "1",
        "content": ".."
        },
        {
        "formName": "mySQLTableForm",
        "typeIdentifier": "mySQLTableForm",
        "typeRevision": "6",
        "content": ".."
        },
        {
        "formName": "mySQLTableForm",
        "typeIdentifier": "mySQLTableForm",
        "typeRevision": "1",
        "content": ".."
        },
        .....
        ]
)
```

Erstellen und betreiben Sie eine DataZone Amazon-Datenquelle für die AWS Glue Data Catalog

In Amazon können Sie eine AWS Glue Data Catalog Datenquelle erstellen DataZone, aus der Sie technische Metadaten von Datenbanktabellen importieren können AWS Glue. Um eine Datenquelle für hinzuzufügen AWS Glue Data Catalog, muss die Quelldatenbank bereits in vorhanden sein AWS Glue.

Wenn Sie eine AWS Glue Datenquelle erstellen und ausführen, fügen Sie dem Inventar Ihres DataZone Amazon-Projekts Assets aus der AWS Glue Quelldatenbank hinzu. Sie können Ihre AWS Glue Datenquellen nach einem festgelegten Zeitplan oder bei Bedarf ausführen, um die technischen Metadaten Ihrer Assets zu erstellen oder zu aktualisieren. Während der Datenquellenläufe können Sie sich optional dafür entscheiden, Ihre Assets im DataZone Amazon-Katalog zu veröffentlichen und sie so für alle Domain-Benutzer auffindbar zu machen. Sie können die Ressourcen Ihres Projektinventars auch veröffentlichen, nachdem Sie deren Geschäftsmetadaten bearbeitet haben. Domain-Benutzer können nach Ihren veröffentlichten Ressourcen suchen und diese entdecken und Abonnements für diese Ressourcen beantragen.

Um eine AWS Glue Datenquelle hinzuzufügen

1. Navigieren Sie zur URL des DataZone Amazon-Datenportals und melden Sie sich mit Single Sign-On (SSO) oder Ihren AWS Anmeldeinformationen an. Wenn Sie ein DataZone Amazon-Administrator sind, können Sie unter https://console.aws.amazon.com/datazone zur DataZone Amazon-Konsole navigieren und sich dort anmelden, AWS-Konto wo die Domain erstellt wurde, und dann Datenportal öffnen wählen.
2. Wählen Sie im oberen Navigationsbereich die Option Projekt auswählen und wählen Sie das Projekt aus, zu dem Sie die Datenquelle hinzufügen möchten.
3. Navigieren Sie zur Registerkarte Daten für das Projekt.
4. Wählen Sie im linken Navigationsbereich Datenquellen und dann Datenquelle erstellen aus.
5. Konfigurieren Sie die folgenden Felder:
   - Name — Der Name der Datenquelle.
   - Beschreibung — Die Beschreibung der Datenquelle.
6. Wählen Sie unter Datenquellentyp die Option AWS Glue.
7. Geben Sie unter Umgebung auswählen eine Umgebung an, in der die AWS Glue Tabellen veröffentlicht werden sollen.

8. Geben Sie unter Datenauswahl eine AWS Glue Datenbank an und geben Sie Ihre Tabellenauswahlkriterien ein. Wenn Sie beispielsweise Include und Enter wählen`*corporate`, enthält die Datenbank alle Quelltabellen, die mit dem Wort enden`corporate`.

   Sie können entweder eine AWS Glue Datenbank aus der Dropdownliste auswählen oder einen Datenbanknamen eingeben. Die Dropdownliste umfasst zwei Datenbanken: die Veröffentlichungsdatenbank und die Abonnementdatenbank der Umgebung. Wenn Sie Elemente aus einer Datenbank übernehmen möchten, die nicht von der Umgebung erstellt wurde, müssen Sie den Namen der Datenbank eingeben, anstatt sie aus der Dropdownliste auszuwählen.

   Sie können mehrere Ein- und Ausschlussregeln für Tabellen innerhalb einer einzigen Datenbank hinzufügen. Sie können auch mehrere Datenbanken hinzufügen, indem Sie auf die Schaltfläche Weitere Datenbank hinzufügen klicken.

9. Unter Datenqualität können Sie wählen, ob Sie die Datenqualität für diese Datenquelle aktivieren möchten. Wenn Sie dies tun, DataZone importiert Amazon Ihre bestehende AWS Glue-Datenqualitätsausgabe in Ihren DataZone Amazon-Katalog. Standardmäßig DataZone importiert Amazon die letzten vorhandenen 100 Qualitätsberichte ohne Verfallsdatum von AWS Glue.

   Die Datenqualitätskennzahlen in Amazon DataZone helfen Ihnen dabei, die Vollständigkeit und Genauigkeit Ihrer Datenquellen zu verstehen. Amazon DataZone ruft diese Datenqualitätskennzahlen von AWS Glue ab, um zu einem bestimmten Zeitpunkt einen Kontext bereitzustellen, z. B. bei einer Suche nach einem Geschäftsdatenkatalog. Datennutzer können sehen, wie sich die Datenqualitätskennzahlen für ihre abonnierten Ressourcen im Laufe der Zeit ändern. Datenproduzenten können die Datenqualitätswerte von AWS Glue nach einem Zeitplan aufnehmen. Der DataZone Amazon-Geschäftsdatenkatalog kann über Datenqualitäts-APIs auch Datenqualitätskennzahlen aus Systemen von Drittanbietern anzeigen. Weitere Informationen finden Sie unter Datenqualität bei Amazon DataZone.
10. Wählen Sie Weiter aus.
11. Wählen Sie unter Veröffentlichungseinstellungen aus, ob Assets im Geschäftsdatenkatalog sofort auffindbar sind. Wenn Sie sie nur zum Inventar hinzufügen, können Sie später Abonnementbedingungen auswählen und sie im Geschäftsdatenkatalog veröffentlichen. Weitere Informationen finden Sie unter the section called “Bestehende Datenquellen verwalten”.
12. Wählen Sie unter Automatisierte Generierung von Unternehmensnamen aus, ob Metadaten für Assets automatisch generiert werden sollen, wenn diese aus der Quelle importiert werden.
13. (Optional) Fügen Sie für Metadaten-Formulare Formulare hinzu, um die Metadaten zu definieren, die gesammelt und gespeichert werden, wenn die Assets in Amazon importiert werden

DataZone. Weitere Informationen finden Sie unter the section called “Metadatenformulare erstellen, bearbeiten oder löschen”.

14. Wählen Sie unter Einstellung „Ausführen“ aus, wann die Datenquelle ausgeführt werden soll.
    - Nach einem Zeitplan ausführen — Geben Sie Datum und Uhrzeit für die Ausführung der Datenquelle an.
    - Bei Bedarf ausführen — Sie können Datenquellenläufe manuell starten.
15. Wählen Sie Weiter aus.
16. Überprüfen Sie Ihre Datenquellenkonfiguration und wählen Sie Erstellen aus.

Eine DataZone Amazon-Datenquelle für Amazon Redshift erstellen und ausführen

In Amazon können Sie eine Amazon Redshift-Datenquelle erstellen DataZone, um technische Metadaten von Datenbanktabellen und Ansichten aus dem Amazon Redshift Data Warehouse zu importieren. Um eine DataZone Amazon-Datenquelle für Amazon Redshift hinzuzufügen, muss das Quell-Data Warehouse bereits in Amazon Redshift vorhanden sein.

Wenn Sie eine Amazon Redshift Redshift-Datenquelle erstellen und ausführen, fügen Sie dem Inventar Ihres DataZone Amazon-Projekts Assets aus dem Amazon Redshift Redshift-Quell-Data Warehouse hinzu. Sie können Ihre Amazon Redshift Redshift-Datenquellen nach einem festgelegten Zeitplan oder bei Bedarf ausführen, um die technischen Metadaten Ihrer Assets zu erstellen oder zu aktualisieren. Während der Datenquellenläufe können Sie sich optional dafür entscheiden, Ihre Projektinventarressourcen im DataZone Amazon-Katalog zu veröffentlichen und sie so für alle Domain-Benutzer auffindbar zu machen. Sie können Ihre Inventarressourcen auch veröffentlichen, nachdem Sie deren Geschäftsmetadaten bearbeitet haben. Domain-Benutzer können nach Ihren veröffentlichten Assets suchen und diese entdecken und Abonnements für diese Assets beantragen.

So fügen Sie eine Amazon Redshift Redshift-Datenquelle hinzu

1. Navigieren Sie zur URL des DataZone Amazon-Datenportals und melden Sie sich mit Single Sign-On (SSO) oder Ihren AWS Anmeldeinformationen an. Wenn Sie ein DataZone Amazon-Administrator sind, können Sie unter https://console.aws.amazon.com/datazone zur DataZone Amazon-Konsole navigieren und sich dort anmelden, AWS-Konto wo die Domain erstellt wurde, und dann Datenportal öffnen wählen.

2. Wählen Sie im oberen Navigationsbereich die Option Projekt auswählen und wählen Sie das Projekt aus, zu dem Sie die Datenquelle hinzufügen möchten.
3. Navigieren Sie zur Registerkarte Daten für das Projekt.
4. Wählen Sie im linken Navigationsbereich Datenquellen und dann Datenquelle erstellen aus.
5. Konfigurieren Sie die folgenden Felder:

   - Name — Der Name der Datenquelle.
   - Beschreibung — Die Beschreibung der Datenquelle.
6. Wählen Sie unter Datenquellentyp Amazon Redshift aus.
7. Geben Sie unter Umgebung auswählen eine Umgebung an, in der die Amazon Redshift Redshift-Tabellen veröffentlicht werden sollen.
8. Abhängig von der ausgewählten Umgebung wendet Amazon DataZone automatisch die Amazon Redshift Redshift-Anmeldeinformationen und andere Parameter direkt aus der Umgebung an oder gibt Ihnen die Möglichkeit, Ihre eigenen auszuwählen.

   - Wenn Sie eine Umgebung ausgewählt haben, die nur das Veröffentlichen aus dem Amazon Redshift Redshift-Standardschema der Umgebung erlaubt, wendet Amazon DataZone automatisch die Amazon Redshift Redshift-Anmeldeinformationen und andere Parameter an, darunter den Namen des Amazon Redshift Redshift-Clusters oder der Arbeitsgruppe, den AWS geheimen Schlüssel, den Datenbanknamen und den Schemanamen. Sie können diese automatisch ausgefüllten Parameter nicht bearbeiten.
   - Wenn Sie eine Umgebung auswählen, in der keine Daten veröffentlicht werden können, können Sie nicht mit der Erstellung der Datenquelle fortfahren.
   - Wenn Sie eine Umgebung auswählen, die das Veröffentlichen von Daten aus einem beliebigen Schema ermöglicht, sehen Sie die Option, entweder die Anmeldeinformationen und andere Amazon Redshift Redshift-Parameter aus der Umgebung zu verwenden oder Ihre eigenen Anmeldeinformationen/Parameter einzugeben.
9. Wenn Sie Ihre eigenen Anmeldeinformationen verwenden möchten, um die Datenquelle zu erstellen, geben Sie die folgenden Details an:

   - Wählen Sie unter Amazon Redshift-Anmeldeinformationen bereitstellen aus, ob Sie einen bereitgestellten Amazon Redshift Redshift-Cluster oder einen Amazon Redshift Serverless Workspace als Datenquelle verwenden möchten.
   - Wählen Sie je nach Ihrer Auswahl im obigen Schritt Ihren Amazon Redshift Redshift-Cluster oder Workspace aus dem Drop-down-Menü aus und wählen Sie dann das Geheimnis in AWS

Secrets Manager aus, das für die Authentifizierung verwendet werden soll. Sie können ein vorhandenes Geheimnis auswählen oder ein neues erstellen.

- Damit das bestehende Geheimnis in der Drop-down-Liste angezeigt wird, stellen Sie sicher, dass Ihr Geheimnis in AWS Secrets Manager die folgenden Tags (Schlüssel/Wert) enthält:
  - AmazonDataZoneProject: <projectID>
  - AmazonDataZoneDomain: <domainID>

  Wenn Sie sich dafür entscheiden, ein neues Geheimnis zu erstellen, wird das Geheimnis automatisch mit den oben genannten Tags versehen, sodass keine zusätzlichen Schritte erforderlich sind. Weitere Informationen finden Sie unter Speichern von Datenbankanmeldedaten in AWS Secrets Manager.

  Amazon Redshift Redshift-Benutzer, die sich in dem für die Erstellung der Datenquelle angegebenen AWS Secret befinden, müssen über `SELECT` Berechtigungen für die Tabellen verfügen, die veröffentlicht werden sollen. Wenn Sie möchten DataZone , dass Amazon auch die Abonnements (den Zugriff) in Ihrem Namen verwaltet, müssen die Datenbankbenutzer in The AWS Secret außerdem über die folgenden Berechtigungen verfügen:
  - `CREATE DATASHARE`
  - `ALTER DATASHARE`
  - `DROP DATASHARE`

10. Geben Sie unter Datenauswahl eine Amazon Redshift Redshift-Datenbank und ein Schema an und geben Sie Ihre Auswahlkriterien für Tabelle oder Ansicht ein. Wenn Sie beispielsweise Include wählen und Enter eingeben**`*corporate`**, enthält das Asset alle Quelltabellen, die mit dem Wort **`corporate`** enden.

    Sie können mehrere Include-Regeln für Tabellen innerhalb einer einzigen Datenbank hinzufügen. Sie können auch mehrere Datenbanken hinzufügen, indem Sie auf die Schaltfläche Weitere Datenbank hinzufügen klicken.
11. Wählen Sie Weiter aus.
12. Wählen Sie unter Veröffentlichungseinstellungen aus, ob Assets im Datenkatalog sofort auffindbar sind. Wenn Sie sie nur zum Inventar hinzufügen, können Sie später Abonnementbedingungen auswählen und sie im Geschäftsdatenkatalog veröffentlichen. Weitere Informationen finden Sie unter the section called “Bestehende Datenquellen verwalten”.

13. Wählen Sie unter Automatisierte Generierung von Unternehmensnamen aus, ob Metadaten für Assets automatisch generiert werden sollen, sobald diese veröffentlicht und anhand der Quelle aktualisiert werden.
14. (Optional) Fügen Sie für Metadaten-Formulare Formulare hinzu, um die Metadaten zu definieren, die gesammelt und gespeichert werden, wenn die Assets in Amazon importiert werden DataZone. Weitere Informationen finden Sie unter the section called “Metadatenformulare erstellen, bearbeiten oder löschen”.
15. Wählen Sie unter Einstellung „Ausführen“ aus, wann die Datenquelle ausgeführt werden soll.
    - Nach einem Zeitplan ausführen — Geben Sie Datum und Uhrzeit für die Ausführung der Datenquelle an.
    - Bei Bedarf ausführen — Sie können Datenquellenläufe manuell starten.
16. Wählen Sie Weiter aus.
17. Überprüfen Sie Ihre Datenquellenkonfiguration und wählen Sie Erstellen aus.

Bestehende DataZone Amazon-Datenquellen verwalten

Nachdem Sie eine DataZone Amazon-Datenquelle erstellt haben, können Sie sie jederzeit ändern, um die Quelldetails oder die Datenauswahlkriterien zu ändern. Wenn Sie eine Datenquelle nicht mehr benötigen, können Sie sie löschen.

Um diese Schritte ausführen zu können, muss Ihnen die AmazonDataZoneFullAccess AWS verwaltete Richtlinie angehängt sein. Weitere Informationen finden Sie unter the section called “AWS verwaltete Richtlinien”.

Themen

- Bearbeiten Sie eine Datenquelle
- Löschen einer Datenquelle

Bearbeiten Sie eine Datenquelle

Sie können eine DataZone Amazon-Datenquelle bearbeiten, um ihre Datenauswahleinstellungen zu ändern, einschließlich Hinzufügen, Entfernen oder Ändern der Tabellenauswahlkriterien. Sie können auch Datenbanken hinzufügen und entfernen. Sie können den Datenquellentyp oder die Umgebung, in der eine Datenquelle veröffentlicht wird, nicht ändern.

So bearbeiten Sie eine Datenquelle:

1. Navigieren Sie zur URL des DataZone Amazon-Datenportals und melden Sie sich mit Single Sign-On (SSO) oder Ihren AWS Anmeldeinformationen an. Wenn Sie ein DataZone Amazon-Administrator sind, können Sie unter https://console.aws.amazon.com/datazone zur DataZone Amazon-Konsole navigieren und sich dort anmelden, AWS-Konto wo die Domain erstellt wurde, und dann Datenportal öffnen wählen.
2. Wählen Sie im oberen Navigationsbereich die Option Projekt auswählen und wählen Sie das Projekt aus, zu dem die Datenquelle gehört.
3. Navigieren Sie zur Registerkarte Daten für das Projekt.
4. Wählen Sie im linken Navigationsbereich Datenquellen und dann die Datenquelle aus, die Sie ändern möchten.
5. Navigieren Sie zur Registerkarte Datenquellendefinition und wählen Sie Bearbeiten aus.
6. Nehmen Sie Ihre Änderungen an der Datenquellendefinition vor. Sie können die Datenquellendetails aktualisieren und Änderungen an den Datenauswahlkriterien vornehmen.
7. Wenn Sie die gewünschten Änderungen vorgenommen haben, wählen Sie Save (Speichern) aus.

Löschen einer Datenquelle

Wenn Sie eine DataZone Amazon-Datenquelle nicht mehr benötigen, können Sie sie dauerhaft entfernen. Nachdem Sie eine Datenquelle gelöscht haben, sind alle Assets, die aus dieser Datenquelle stammen, weiterhin im Katalog verfügbar, und Benutzer können sie weiterhin abonnieren. Die Assets erhalten jedoch keine Updates mehr von der Quelle. Es wird empfohlen, die abhängigen Assets zunächst in eine andere Datenquelle zu verschieben, bevor Sie sie löschen.

> **Note**
>
> Sie müssen alle Fulfillments aus der Datenquelle entfernen, bevor Sie sie löschen können. Weitere Informationen finden Sie unter Daten in Amazon entdecken, abonnieren und nutzen DataZone.

So löschen Sie eine Datenquelle:

1. Wählen Sie auf der Registerkarte Daten für das Projekt im linken Navigationsbereich die Option Datenquellen aus.
2. Wählen Sie die Datenquelle aus, die Sie löschen möchten.
3. Wählen Sie Aktionen, Datenquelle löschen und bestätigen Sie den Löschvorgang.

Veröffentlichen Sie Assets aus dem Projektinventar im DataZone Amazon-Katalog

Sie können DataZone Amazon-Ressourcen und ihre Metadaten aus Projektbeständen im DataZone Amazon-Katalog veröffentlichen. Sie können nur die neueste Version eines Assets im Katalog veröffentlichen.

Beachten Sie beim Veröffentlichen von Assets im Katalog Folgendes:

- Um ein Asset im Katalog zu veröffentlichen, müssen Sie der Eigentümer oder Mitwirkende des Projekts sein.
- Stellen Sie für Amazon Redshift Redshift-Assets sicher, dass die Amazon Redshift Redshift-Cluster, die sowohl Publisher- als auch Abonnenten-Clustern zugeordnet sind, alle Anforderungen für die gemeinsame Nutzung von Amazon Redshift Redshift-Daten erfüllen, damit Amazon DataZone den Zugriff auf Redshift-Tabellen und -Ansichten verwalten kann. Weitere Informationen finden Sie unter Konzepte zur gemeinsamen Nutzung von Daten für Amazon Redshift.
- Amazon unterstützt DataZone nur die Zugriffsverwaltung für Assets, die AWS Glue Data Catalog über Amazon Redshift veröffentlicht wurden. Für alle anderen Ressourcen, wie z. B. Amazon S3 S3-Objekte, verwaltet Amazon den Zugriff für zugelassene Abonnenten DataZone nicht. Wenn Sie diese nicht verwalteten Ressourcen abonnieren, werden Sie mit der folgenden Meldung benachrichtigt:

  ```
  Subscription approval does not provide access to data. Subscription
  grants on this asset are not managed by Amazon DataZone. For more
  information or help, reach out to your administrator.
  ```

Veröffentlichen Sie ein Asset

Wenn Sie sich bei der Erstellung einer Datenquelle nicht dafür entschieden haben, dass Assets sofort im Datenkatalog auffindbar sind, führen Sie die folgenden Schritte aus, um sie zu einem späteren Zeitpunkt zu veröffentlichen.

Um ein Asset zu veröffentlichen

1. Navigieren Sie zur URL des DataZone Amazon-Datenportals und melden Sie sich mit Single Sign-On (SSO) oder Ihren AWS Anmeldeinformationen an. Wenn Sie ein DataZone Amazon-Administrator sind, können Sie unter https://console.aws.amazon.com/datazone zur DataZone Amazon-Konsole navigieren und sich dort anmelden, AWS-Konto wo die Domain erstellt wurde, und dann Datenportal öffnen wählen.
2. Wählen Sie im oberen Navigationsbereich die Option Projekt auswählen und wählen Sie das Projekt aus, zu dem das Asset gehört.
3. Navigieren Sie zur Registerkarte Daten für das Projekt.
4. Wählen Sie im linken Navigationsbereich Inventardaten und dann das Asset aus, das Sie veröffentlichen möchten.

   > **Note**
   >
   > Standardmäßig ist für alle Assets eine Abonnementgenehmigung erforderlich, was bedeutet, dass ein Dateneigentümer alle Abonnementanfragen für das Asset genehmigen muss. Wenn Sie diese Einstellung ändern möchten, bevor Sie das Asset veröffentlichen, öffnen Sie die Asset-Details und wählen Sie neben Abonnementgenehmigung die Option Bearbeiten aus. Sie können diese Einstellung später ändern, indem Sie das Asset ändern und erneut veröffentlichen.

5. Wählen Sie Asset veröffentlichen. Das Asset wird direkt im Katalog veröffentlicht.

   Wenn Sie Änderungen an dem Asset vornehmen, z. B. die Genehmigungsanforderungen ändern, können Sie die Option Erneut veröffentlichen auswählen, um die Aktualisierungen im Katalog zu veröffentlichen.

Inventar verwalten und Ressourcen kuratieren

Um Amazon für die Katalogisierung Ihrer Daten verwenden DataZone zu können, müssen Sie zunächst Ihre Daten (Assets) als Inventar Ihres Projekts in Amazon speichern DataZone. Durch die Erstellung eines Inventars für ein bestimmtes Projekt sind die Ressourcen nur für die Mitglieder dieses Projekts auffindbar.

Sobald die Assets im Projektinventar erstellt wurden, können ihre Metadaten kuratiert werden. Sie können beispielsweise den Namen und die Beschreibung des Assets bearbeiten oder mich lesen. Bei jeder Bearbeitung des Assets wird eine neue Version des Assets erstellt. Sie können die Registerkarte Verlauf auf der Detailseite des Assets verwenden, um alle Asset-Versionen anzuzeigen.

Sie können den Abschnitt „Read Me“ bearbeiten und ausführliche Beschreibungen für das Asset hinzufügen. Der Abschnitt „Read Me“ unterstützt Markdown, sodass Sie Ihre Beschreibungen nach Bedarf formatieren und Verbrauchern wichtige Informationen zu einem Vermögenswert beschreiben können.

Glossarbegriffe können auf Anlageebene hinzugefügt werden, indem Sie die verfügbaren Formulare ausfüllen.

Um das Schema zu kuratieren, können Sie die Spalten überprüfen, Unternehmensnamen und Beschreibungen hinzufügen und Glossarbegriffe auf Spaltenebene hinzufügen.

Wenn die automatische Generierung von Metadaten bei der Erstellung der Datenquelle aktiviert ist, können die Unternehmensnamen für Assets und Spalten einzeln oder alle gleichzeitig überprüft und akzeptiert oder abgelehnt werden.

Sie können auch die Abonnementbedingungen bearbeiten, um anzugeben, ob eine Genehmigung für das Asset erforderlich ist oder nicht.

Mit Metadatenformularen DataZone in Amazon können Sie das Metadatenmodell eines Datenbestands erweitern, indem Sie benutzerdefinierte Attribute hinzufügen (z. B. Verkaufsregion, Verkaufsjahr und Verkaufsquartal). Die Metadatenformulare, die an einen Asset-Typ angehängt sind, werden auf alle Assets angewendet, die mit diesem Asset-Typ erstellt wurden. Sie können einzelnen Assets auch zusätzliche Metadatenformulare als Teil des Datenquellenlaufs oder nach deren Erstellung hinzufügen. Informationen zum Erstellen neuer Formulare finden Sie unterthe section called “Metadatenformulare erstellen, bearbeiten oder löschen”.

Um die Metadaten eines Assets zu aktualisieren, müssen Sie Eigentümer oder Mitwirkender des Projekts sein, zu dem das Asset gehört.

Um die Metadaten eines Assets zu aktualisieren

1. Navigieren Sie zur URL des DataZone Amazon-Datenportals und melden Sie sich mit Single Sign-On (SSO) oder Ihren AWS Anmeldeinformationen an. Wenn Sie ein DataZone Amazon-Administrator sind, können Sie unter https://console.aws.amazon.com/datazone zur DataZone Amazon-Konsole navigieren und sich dort anmelden, AWS-Konto wo die Domain erstellt wurde, und dann Datenportal öffnen wählen.
2. Wählen Sie im oberen Navigationsbereich die Option Projekt auswählen und wählen Sie das Projekt aus, das das Asset enthält, dessen Metadaten Sie aktualisieren möchten.
3. Navigieren Sie zur Registerkarte Daten für das Projekt.
4. Wählen Sie im linken Navigationsbereich Inventardaten und dann den Namen des Assets aus, dessen Metadaten Sie aktualisieren möchten.
5. Wählen Sie auf der Seite mit den Asset-Details unter Metadatenformulare die Option Bearbeiten aus und bearbeiten Sie die vorhandenen Formulare nach Bedarf. Sie können dem Asset auch zusätzliche Metadatenformulare anhängen. Weitere Informationen finden Sie unter the section called “Fügen Sie zusätzliche Metadatenformulare an Assets an”.
6. Wenn Sie mit den Aktualisierungen fertig sind, wählen Sie Formular speichern.

   Wenn Sie das Formular speichern, DataZone generiert Amazon eine neue Inventarversion des Assets. Um die aktualisierte Version im Katalog zu veröffentlichen, wählen Sie Asset erneut veröffentlichen.

Fügen Sie zusätzliche Metadatenformulare an Assets an

Standardmäßig werden Metadatenformulare, die an eine Domain angehängt sind, an alle in dieser Domain veröffentlichten Assets angehängt. Datenherausgeber können einzelnen Assets zusätzliche Metadatenformulare zuordnen, um zusätzlichen Kontext bereitzustellen.

Um zusätzliche Metadatenformulare an ein Asset anzuhängen

1. Navigieren Sie zur URL des DataZone Amazon-Datenportals und melden Sie sich mit Single Sign-On (SSO) oder Ihren AWS Anmeldeinformationen an. Wenn Sie ein DataZone Amazon-Administrator sind, können Sie unter https://console.aws.amazon.com/datazone zur DataZone

Amazon-Konsole navigieren und sich dort anmelden, AWS-Konto wo die Domain erstellt wurde, und dann Datenportal öffnen wählen.

2. Wählen Sie im oberen Navigationsbereich die Option Projekt auswählen und wählen Sie das Projekt aus, das das Asset enthält, dessen Metadaten Sie hinzufügen möchten.
3. Navigieren Sie zur Registerkarte Daten für das Projekt.
4. Wählen Sie im linken Navigationsbereich Inventardaten und dann den Namen des Assets aus, dessen Metadaten Sie hinzufügen möchten.
5. Wählen Sie auf der Seite mit den Asset-Details unter Metadatenformulare die Option Formulare hinzufügen aus.
6. Wählen Sie die Formulare aus, die Sie dem Asset hinzufügen möchten, und wählen Sie dann Formulare hinzufügen aus.
7. Geben Sie Werte für jedes der Metadatenfelder ein und wählen Sie dann Formular speichern.

   Wenn Sie das Formular speichern, DataZone generiert Amazon eine neue Inventarversion des Assets. Um die aktualisierte Version im Katalog zu veröffentlichen, wählen Sie Asset erneut veröffentlichen.

Veröffentlichen Sie das Asset nach der Kuration im Katalog

Sobald der Dateneigentümer mit der Asset-Kuration zufrieden ist, kann er eine Asset-Version im DataZone Amazon-Katalog veröffentlichen und sie so für alle Domain-Benutzer auffindbar machen. Das Asset zeigt die Inventarversion und die veröffentlichte Version. Im Discovery-Katalog wird nur die zuletzt veröffentlichte Version angezeigt. Wenn die Metadaten nach der Veröffentlichung aktualisiert werden, steht eine neue Inventarversion für die Veröffentlichung im Katalog zur Verfügung.

Erstellen Sie manuell ein Asset

In Amazon DataZone ist ein Asset eine Entität, die ein einzelnes physisches Datenobjekt (z. B. eine Tabelle, ein Dashboard, eine Datei) oder ein virtuelles Datenobjekt (z. B. eine Ansicht) darstellt. Weitere Informationen finden Sie unter DataZone Amazon-Terminologie und Konzepte. Das manuelle Veröffentlichen eines Assets ist ein einmaliger Vorgang. Sie geben keinen Ausführungsplan für das Asset an, sodass es nicht automatisch aktualisiert wird, wenn sich seine Quelle ändert.

Um ein Asset manuell über ein Projekt zu erstellen, müssen Sie der Eigentümer oder Mitwirkender dieses Projekts sein.

Um ein Asset manuell zu erstellen

1. Navigieren Sie zur URL des DataZone Amazon-Datenportals und melden Sie sich mit Single Sign-On (SSO) oder Ihren AWS Anmeldeinformationen an. Wenn Sie ein DataZone Amazon-Administrator sind, können Sie unter https://console.aws.amazon.com/datazone zur DataZone Amazon-Konsole navigieren und sich dort anmelden, AWS-Konto wo die Domain erstellt wurde, und dann Datenportal öffnen wählen.
2. Wählen Sie im oberen Navigationsbereich die Option Projekt auswählen und wählen Sie das Projekt aus, für das Sie das Asset erstellen möchten.
3. Navigieren Sie zur Registerkarte Daten für das Projekt.
4. Wählen Sie im linken Navigationsbereich Datenquellen und dann Datenbestand erstellen aus.
5. Konfigurieren Sie für Asset-Details die folgenden Einstellungen:
   - Asset-Typ — Der Asset-Typ.
   - Name — Der Name des Vermögenswerts.
   - Beschreibung — Eine Beschreibung des Assets.
6. Geben Sie für den S3-Standort den Amazon-Ressourcennamen (ARN) des Quell-S3-Buckets ein.

   Geben Sie optional einen S3-Zugangspunkt ein. Weitere Informationen finden Sie unter Verwalten des Datenzugriffs mit Amazon-S3-Zugriffspunkten.
7. Wählen Sie unter Veröffentlichungseinstellungen aus, ob Assets im Katalog sofort auffindbar sind. Wenn Sie sie nur zum Inventar hinzufügen, können Sie später Abonnementbedingungen wählen, um sie im Katalog zu veröffentlichen.
8. Wählen Sie Erstellen.

   Sobald das Asset erstellt wurde, wird es entweder direkt als aktives Asset im Katalog veröffentlicht oder im Inventar gespeichert, bis Sie sich entscheiden, es zu veröffentlichen.

Veröffentlichung eines Assets aus dem DataZone Amazon-Katalog rückgängig machen

Wenn Sie die Veröffentlichung eines DataZone Amazon-Assets aus dem Katalog rückgängig machen, wird es nicht mehr in den globalen Suchergebnissen angezeigt. Neue Benutzer können die

Asset-Liste im Katalog nicht finden oder abonnieren, aber alle bestehenden Abonnements bleiben unverändert.

Um die Veröffentlichung eines Assets rückgängig zu machen, müssen Sie Eigentümer oder Mitwirkender des Projekts sein, zu dem das Asset gehört:

Um die Veröffentlichung eines Assets rückgängig zu machen

1. Navigieren Sie zur URL des DataZone Amazon-Datenportals und melden Sie sich mit Single Sign-On (SSO) oder Ihren AWS Anmeldeinformationen an. Wenn Sie ein DataZone Amazon-Administrator sind, können Sie unter https://console.aws.amazon.com/datazone zur DataZone Amazon-Konsole navigieren und sich dort anmelden, AWS-Konto wo die Domain erstellt wurde, und dann Datenportal öffnen wählen.
2. Wählen Sie im oberen Navigationsbereich die Option Projekt auswählen und wählen Sie das Projekt aus, zu dem das Asset gehört.
3. Navigieren Sie zur Registerkarte Daten für das Projekt.
4. Wählen Sie im linken Navigationsbereich Veröffentlichte Daten aus.
5. Suchen Sie das Asset in der Liste der veröffentlichten Assets und wählen Sie dann Veröffentlichung rückgängig machen aus.

   Das Asset wird aus dem Katalog entfernt. Sie können das Asset jederzeit erneut veröffentlichen, indem Sie Veröffentlichen wählen.

Löschen Sie ein DataZone Amazon-Asset

Wenn Sie ein Asset bei Amazon nicht mehr benötigen DataZone, können Sie es dauerhaft löschen. Das Löschen eines Assets unterscheidet sich vom Rückgängigmachen der Veröffentlichung eines Assets aus dem Katalog. Sie können ein Asset und den zugehörigen Eintrag im Katalog löschen, sodass es in den Suchergebnissen nicht mehr sichtbar ist. Um die Asset-Liste zu löschen, müssen Sie zunächst alle zugehörigen Abonnements kündigen.

Um ein Asset zu löschen, müssen Sie der Eigentümer oder Mitwirkender des Projekts sein, zu dem das Asset gehört:

> **Note**
>
> Um eine Asset-Liste zu löschen, müssen Sie zunächst alle bestehenden Abonnements für das Asset kündigen. Sie können einen Asset-Eintrag, der bereits Abonnenten hat, nicht löschen.

Um ein Asset zu löschen

1. Navigieren Sie zur URL des DataZone Amazon-Datenportals und melden Sie sich mit Single Sign-On (SSO) oder Ihren AWS Anmeldeinformationen an. Wenn Sie ein DataZone Amazon-Administrator sind, können Sie unter https://console.aws.amazon.com/datazone zur DataZone Amazon-Konsole navigieren und sich dort anmelden, AWS-Konto wo die Domain erstellt wurde, und dann Datenportal öffnen wählen.
2. Wählen Sie im oberen Navigationsbereich die Option Projekt auswählen und wählen Sie das Projekt aus, das das Asset enthält, das Sie löschen möchten.
3. Navigieren Sie zur Registerkarte Daten für das Projekt.
4. Wählen Sie im linken Navigationsbereich die Option Veröffentlichte Daten aus, suchen Sie dann das Asset, das Sie löschen möchten, und wählen Sie es aus. Dadurch wird die Seite mit den Asset-Details geöffnet.
5. Wählen Sie Aktionen, Löschen und bestätigen Sie den Löschvorgang.

   Sobald das Asset gelöscht wurde, kann es nicht mehr angezeigt werden und Benutzer können es nicht abonnieren.

Manuelles Starten einer Datenquellenausführung in Amazon DataZone

Wenn Sie eine Datenquelle ausführen, DataZone ruft Amazon alle neuen oder geänderten Metadaten aus der Quelle ab und aktualisiert die zugehörigen Ressourcen im Inventar. Wenn Sie Amazon eine Datenquelle hinzufügen DataZone, geben Sie die Ausführungspräferenz der Quelle an, die definiert, ob die Quelle nach einem Zeitplan oder bei Bedarf ausgeführt wird. Wenn Ihre Quelle bei Bedarf ausgeführt wird, müssen Sie eine Datenquellenausführung manuell initiieren.

Auch wenn Ihre Quelle nach einem Zeitplan ausgeführt wird, können Sie sie jederzeit manuell ausführen. Nachdem Sie Geschäftsmetadaten zu den Assets hinzugefügt haben, können Sie

Assets auswählen und sie im DataZone Amazon-Katalog veröffentlichen, damit diese Assets von allen Domain-Benutzern gefunden werden können. Nur veröffentlichte Assets können von anderen Domain-Benutzern durchsucht werden.

Um eine Datenquelle manuell auszuführen

1. Navigieren Sie zur URL des DataZone Amazon-Datenportals und melden Sie sich mit Single Sign-On (SSO) oder Ihren AWS Anmeldeinformationen an. Wenn Sie ein DataZone Amazon-Administrator sind, können Sie unter https://console.aws.amazon.com/datazone zur DataZone Amazon-Konsole navigieren und sich dort anmelden, AWS-Konto wo die Domain erstellt wurde, und dann Datenportal öffnen wählen.
2. Wählen Sie im oberen Navigationsbereich die Option Projekt auswählen und wählen Sie das Projekt aus, zu dem die Datenquelle gehört.
3. Navigieren Sie zur Registerkarte Daten für das Projekt.
4. Wählen Sie im linken Navigationsbereich Datenquellen aus, suchen Sie dann die Datenquelle, die Sie ausführen möchten, und wählen Sie sie aus. Dadurch wird die Seite mit den Datenquellendetails geöffnet.
5. Wählen Sie Bei Bedarf ausführen aus.

   Der Status der Datenquelle ändert sich in, `Running` wenn Amazon die Asset-Metadaten mit den neuesten Daten aus der Quelle DataZone aktualisiert. Sie können den Status des Laufs auf der Registerkarte Datenquellenläufe überwachen.

Überarbeitungen von Vermögenswerten bei Amazon DataZone

Amazon DataZone erhöht die Revision eines Assets, wenn Sie dessen geschäftliche oder technische Metadaten bearbeiten. Zu diesen Änderungen gehören die Änderung des Asset-Namens, der Beschreibung, der Glossarbegriffe, der Spaltennamen, der Metadatenformulare und der Feldwerte des Metadatenformulars. Diese Änderungen können auf manuelle Änderungen, die Ausführung von Datenquellen-Jobs oder API-Operationen zurückzuführen sein. Amazon generiert jedes Mal, wenn Sie das Asset bearbeiten, DataZone automatisch eine neue Asset-Revision.

Nachdem Sie ein Asset aktualisiert haben und eine neue Version generiert wurde, müssen Sie die neue Version im Katalog veröffentlichen, damit sie aktualisiert und für Abonnenten verfügbar ist. Weitere Informationen finden Sie unter the section called “Veröffentlichen Sie Elemente aus dem Projektinventar im Katalog”. Sie können nur die neueste Version eines Assets im Katalog veröffentlichen.

Um frühere Versionen eines Assets einzusehen

1. Navigieren Sie zur URL des DataZone Amazon-Datenportals und melden Sie sich mit Single Sign-On (SSO) oder Ihren AWS Anmeldeinformationen an. Wenn Sie ein DataZone Amazon-Administrator sind, können Sie unter https://console.aws.amazon.com/datazone zur DataZone Amazon-Konsole navigieren und sich dort anmelden, AWS-Konto wo die Domain erstellt wurde, und dann Datenportal öffnen wählen.
2. Wählen Sie im oberen Navigationsbereich die Option Projekt auswählen und wählen Sie das Projekt aus, das das Asset enthält.
3. Navigieren Sie zur Registerkarte Daten für das Projekt, suchen Sie das Asset und wählen Sie es aus. Dadurch wird die Seite mit den Asset-Details geöffnet.
4. Navigieren Sie zur Registerkarte Verlauf, auf der eine Liste der vergangenen Versionen des Assets angezeigt wird.

Datenqualität bei Amazon DataZone

Datenqualitätskennzahlen in Amazon DataZone helfen Ihnen dabei, die verschiedenen Qualitätskennzahlen wie Vollständigkeit, Aktualität und Genauigkeit Ihrer Datenquellen zu verstehen. Amazon ist in AWS Glue Data Quality DataZone integriert und bietet APIs zur Integration von Datenqualitätsmetriken aus Datenqualitätslösungen von Drittanbietern. Datennutzer können sehen, wie sich die Datenqualitätskennzahlen für ihre abonnierten Ressourcen im Laufe der Zeit ändern. Um die Datenqualitätsregeln zu erstellen und auszuführen, können Sie das Datenqualitätstool Ihrer Wahl wie AWS Glue Data Quality verwenden. Mit Datenqualitätsmetriken in Amazon DataZone können Datenkonsumenten die Datenqualitätswerte für die Ressourcen und Spalten visualisieren und so Vertrauen in die Daten aufbauen, die sie für Entscheidungen verwenden.

Voraussetzungen und Änderungen der IAM-Rollen

Wenn Sie die AWS verwalteten Richtlinien DataZone von Amazon verwenden, gibt es keine zusätzlichen Konfigurationsschritte und diese verwalteten Richtlinien werden automatisch aktualisiert, um die Datenqualität zu unterstützen. Wenn Sie Ihre eigenen Richtlinien für die Rollen verwenden, die Amazon die erforderlichen Berechtigungen für DataZone die Zusammenarbeit mit unterstützten Diensten gewähren, müssen Sie die mit diesen Rollen verknüpften Richtlinien aktualisieren, um die Unterstützung für das Lesen der AWS Glue-Datenqualitätsinformationen in der AWS verwaltete Richtlinie: AmazonDataZoneGlueManageAccessRolePolicy und die Unterstützung für die Zeitreihen-APIs in AWS verwaltete Richtlinie: AmazonDataZoneDomainExecutionRolePolicy und die AWS verwaltete Richtlinie: AmazonDataZoneFullUserAccess zu aktivieren.

Datenqualität für AWS Glue-Assets aktivieren

Amazon DataZone bezieht die Datenqualitätskennzahlen von AWS Glue, um zu einem bestimmten Zeitpunkt Kontext bereitzustellen, z. B. bei einer Suche nach einem Geschäftsdatenkatalog. Datennutzer können sehen, wie sich die Datenqualitätskennzahlen für ihre abonnierten Ressourcen im Laufe der Zeit ändern. Datenproduzenten können die Datenqualitätswerte von AWS Glue nach einem Zeitplan aufnehmen. Der DataZone Amazon-Geschäftsdatenkatalog kann über Datenqualitäts-APIs auch Datenqualitätskennzahlen aus Systemen von Drittanbietern anzeigen. Weitere Informationen finden Sie unter AWS Glue Data Quality und Erste Schritte mit AWS Glue Data Quality für den Datenkatalog.

Sie können Datenqualitätsmetriken für Ihre DataZone Amazon-Ressourcen auf folgende Weise aktivieren:

- Verwenden Sie das Datenportal oder die DataZone Amazon-APIs, um die Datenqualität für Ihre AWS Glue-Datenquelle über das DataZone Amazon-Datenportal zu aktivieren, während Sie entweder eine neue AWS Glue-Datenquelle erstellen oder eine bestehende bearbeiten.

  Weitere Informationen zur Aktivierung der Datenqualität für eine Datenquelle über das Portal finden Sie unter Erstellen und betreiben Sie eine DataZone Amazon-Datenquelle für die AWS Glue Data Catalog undBestehende DataZone Amazon-Datenquellen verwalten.

  > **Note**
  >
  > Sie können das Datenportal verwenden, um die Datenqualität nur für Ihre AWS Glue-Inventarressourcen zu aktivieren. In dieser Version von Amazon wird DataZone die Aktivierung der Datenqualität für Amazon Redshift oder Assets mit benutzerdefinierten Typen über das Datenportal nicht unterstützt.

  Sie können die APIs auch verwenden, um die Datenqualität für Ihre neuen oder vorhandenen Datenquellen zu aktivieren. Sie können dies tun, indem Sie das CreateDataSourceoder aufrufen UpdateDataSourceund den `autoImportDataQualityResult` Parameter auf „True“ setzen.

  Nachdem die Datenqualität aktiviert wurde, können Sie die Datenquelle bei Bedarf oder nach einem Zeitplan ausführen. Bei jedem Lauf können bis zu 100 Messwerte pro Asset erfasst werden. Es ist nicht erforderlich, Formulare zu erstellen oder Metriken manuell hinzuzufügen, wenn die Datenquelle aus Gründen der Datenqualität verwendet wird. Wenn das Asset veröffentlicht wird,

werden die Aktualisierungen, die am Datenqualitätsformular vorgenommen wurden (bis zu 30 Datenpunkte pro historischer Regel), in der Liste für die Verbraucher wiedergegeben. Anschließend wird jedes neue Hinzufügen von Metriken zum Asset automatisch zur Liste hinzugefügt. Es ist nicht erforderlich, das Asset erneut zu veröffentlichen, um den Verbrauchern die neuesten Ergebnisse zur Verfügung zu stellen.

Aktivierung der Datenqualität für benutzerdefinierte Asset-Typen

Sie können die DataZone Amazon-APIs verwenden, um die Datenqualität für jedes Ihrer benutzerdefinierten Assets zu aktivieren. Weitere Informationen finden Sie hier:

- PostTimeSeriesDataPoints
- ListTimeSeriesDataPoints
- GetTimeSeriesDataPoint
- DeleteTimeSeriesDataPoints

Die folgenden Schritte bieten ein Beispiel für die Verwendung von APIs oder CLI zum Importieren von Drittanbieter-Metriken für Ihre Assets in Amazon DataZone:

1. Rufen Sie die `PostTimeSeriesDataPoints` API wie folgt auf:

```
aws datazone post-time-series-data-points  \
--cli-input-json file://createTimeSeriesPayload.json \
```

mit der folgenden Nutzlast:

```
{
"domainIdentifier": "dzd_bqqlk3nz21zp2f",
"entityIdentifier": "4nwl5ew0dsu27b",
"entityType": "ASSET",
"forms": [
{
"content": "{\n \"evaluationsCount\" : 11,\n \"evaluations\" : [ {\n \"description
\" : \"IsComplete \\\"Id\\\"\",\n \"details\" : {\n \"STATISTIC_NAME\" :
 \"Completeness\",\n \"COLUMN_NAME\" : \"Id\"\n },\n \"status\" : \"PASS\"\n },
```

```
 {\n \"description\" : \"Uniqueness \\\"Id\\\" > 0.95\",\n \"details\" : {\n
 \"STATISTIC_NAME\" : \"Uniqueness\",\n \"COLUMN_NAME\" : \"Id\"\n },\n \"status
\" : \"PASS\"\n }, {\n \"description\" : \"ColumnLength \\\"Id\\\" = 18\",\n
 \"details\" : {\n \"STATISTIC_NAME\" : \"MinimumLength,MaximumLength\",\n
 \"COLUMN_NAME\" : \"Id,Id\"\n },\n \"status\" : \"PASS\"\n }, {\n \"description
\" : \"IsComplete \\\"IsDeleted\\\"\",\n \"details\" : {\n \"STATISTIC_NAME\" :
 \"Completeness\",\n \"COLUMN_NAME\" : \"IsDeleted\"\n },\n \"status\" : \"PASS
\"\n }, {\n \"description\" : \"Completeness \\\"Type\\\" >= 0.59\",\n \"details
\" : {\n \"STATISTIC_NAME\" : \"Completeness\",\n \"COLUMN_NAME\" : \"Type\"\n },
\n \"status\" : \"PASS\"\n }, {\n \"description\" : \"ColumnValues \\\"Type\
\\" in [\\\"Customer - Direct\\\",\\\"Customer - Channel\\\"] with threshold
 >= 0.8\",\n \"details\" : {\n \"STATISTIC_NAME\" : \"\",\n \"COLUMN_NAME\" :
 \"\"\n },\n \"status\" : \"PASS\"\n }, {\n \"description\" : \"ColumnLength \\
\"Type\\\" <= 18\",\n \"details\" : {\n \"STATISTIC_NAME\" : \"MaximumLength\",\n
 \"COLUMN_NAME\" : \"Type\"\n },\n \"status\" : \"PASS\"\n }, {\n \"description
\" : \"ColumnLength \\\"ParentId\\\" <= 18\",\n \"details\" : {\n \"STATISTIC_NAME
\" : \"MaximumLength\",\n \"COLUMN_NAME\" : \"ParentId\"\n },\n \"status\" :
 \"PASS\"\n }, {\n \"description\" : \"Completeness \\\"AnnualRevenue\\\" >=
 0.28\",\n \"details\" : {\n \"STATISTIC_NAME\" : \"Completeness\",\n \"COLUMN_NAME
\" : \"AnnualRevenue\"\n },\n \"status\" : \"PASS\"\n }, {\n \"description
\" : \"StandardDeviation \\\"AnnualRevenue\\\" between 1658483123.39 and
 1833060294.28\",\n \"details\" : {\n \"STATISTIC_NAME\" : \"StandardDeviation
\",\n \"COLUMN_NAME\" : \"AnnualRevenue\"\n },\n \"status\" : \"PASS\"\n }, {\n
 \"description\" : \"ColumnValues \\\"AnnualRevenue\\\" between 29999999 and
 5600000001\",\n \"details\" : {\n \"STATISTIC_NAME\" : \"Minimum,Maximum\",\n
 \"COLUMN_NAME\" : \"AnnualRevenue,AnnualRevenue\"\n },\n \"status\" : \"PASS
\"\n } ],\n \"passingPercentage\" : 1.0\n}",
"formName": "GREAT_EXPECTATION_NEW",
"typeIdentifier": "amazon.datazone.DataQualityResultFormType",
"timestamp": 1608969556
}
]
}
```

2. Rufen Sie die `DeleteTimeSeriesDataPoints` API wie folgt auf:

```
aws datazone delete-time-series-data-points\
--domain-identifier dzd_bqqlk3nz21zp2f \
--entity-identifier dzd_bqqlk3nz21zp2f \
--entity-type ASSET \
--form-name rulesET1 \
```

Einsatz von maschinellem Lernen und generativer KI

> **Note**
>
> Bereitgestellt von Amazon Bedrock: AWS implementiert automatisierte Missbrauchserkennung. Da die KI-Empfehlungen für Beschreibungsfunktionen in Amazon DataZone auf Amazon Bedrock basieren, übernehmen die Benutzer die in Amazon Bedrock implementierten Kontrollen, um Sicherheit und den verantwortungsvollen Umgang mit KI durchzusetzen.

In der aktuellen Version von Amazon können Sie die Funktion KI-Empfehlungen für Beschreibungen verwenden DataZone, um die Datenermittlung und Katalogisierung zu automatisieren. Die Support für generative KI und maschinelles Lernen in Amazon DataZone erstellt Beschreibungen für Ressourcen und Spalten. Sie können diese Beschreibungen verwenden, um Ihren Daten einen Geschäftskontext hinzuzufügen und Analysen für Datensätze zu empfehlen, was zu besseren Ergebnissen bei der Datenermittlung beitragen kann.

Die KI-Empfehlungen für Datenbestandsbeschreibungen in Amazon basieren auf den großen Sprachmodellen von Amazon Bedrock und DataZone helfen Ihnen dabei, sicherzustellen, dass Ihre Daten verständlich und leicht auffindbar sind. Die KI-Empfehlungen schlagen auch die relevantesten Analyseanwendungen für Datensätze vor. Durch die Reduzierung manueller Dokumentationsaufgaben und Hinweise zur angemessenen Datennutzung können automatisch generierte Beschreibungen Ihnen helfen, die Vertrauenswürdigkeit Ihrer Daten zu erhöhen und das Übersehen wertvoller Daten zu minimieren, um eine fundierte Entscheidungsfindung zu beschleunigen.

> **Important**
>
> In der aktuellen DataZone Amazon-Version wird die Funktion KI-Empfehlungen für Beschreibungen nur in den folgenden Regionen unterstützt:
>
> - USA Ost (Nord-Virginia)
> - USA West (Oregon)
> - Europa (Frankfurt)

- Asien-Pazifik (Tokio)

Das folgende Verfahren beschreibt, wie KI-Empfehlungen für Beschreibungen in Amazon generiert werden DataZone:

1. Navigieren Sie zur URL des DataZone Amazon-Datenportals und melden Sie sich dann mit Single Sign-On (SSO) oder Ihren AWS Anmeldeinformationen an. Wenn Sie ein DataZone Amazon-Administrator sind, navigieren Sie zur DataZone Amazon-Konsole unter https://console.aws.amazon.com/datazone und melden Sie sich mit dem AWS-Konto Ort an, an dem die Domain erstellt wurde, und wählen Sie dann Datenportal öffnen.
2. Wählen Sie im oberen Navigationsbereich die Option Projekt auswählen und wählen Sie dann das Projekt aus, das das Asset enthält, für das Sie KI-Empfehlungen für Beschreibungen generieren möchten.
3. Navigieren Sie zur Registerkarte Daten für das Projekt.
4. Wählen Sie im linken Navigationsbereich Inventardaten und dann den Namen des Assets aus, für das Sie KI-Empfehlungen für Beschreibungen für das Asset generieren möchten.
5. Wählen Sie auf der Detailseite des Assets auf der Registerkarte Geschäftsmetadaten die Option Beschreibungen generieren aus.
6. Sobald die Beschreibungen generiert wurden, können Sie sie entweder bearbeiten, akzeptieren oder ablehnen. Neben jeder automatisch generierten Metadatenbeschreibung für das Datenobjekt werden grüne Symbole angezeigt. Auf der Registerkarte Geschäftsmetadaten können Sie das grüne Symbol neben der automatisch generierten Zusammenfassung auswählen und dann Bearbeiten, Akzeptieren oder Ablehnen wählen, um auf die generierte Beschreibung einzugehen. Sie können auch die Optionen Alle akzeptieren oder Alle ablehnen auswählen, die oben auf der Seite angezeigt werden, wenn der Tab Geschäftsmetadaten ausgewählt ist, und so die ausgewählte Aktion für alle automatisch generierten Beschreibungen ausführen.

   Sie können auch die Registerkarte Schema wählen und dann automatisch generierte Beschreibungen einzeln adressieren, indem Sie das grüne Symbol für jeweils eine Spaltenbeschreibung auswählen und dann Akzeptieren oder Ablehnen wählen. Auf der Registerkarte Schema können Sie auch Alle akzeptieren oder Alle ablehnen wählen und so die ausgewählte Aktion für alle automatisch generierten Beschreibungen ausführen.
7. Um das Asset mit den generierten Beschreibungen im Katalog zu veröffentlichen, wählen Sie Asset veröffentlichen und bestätigen Sie diese Aktion, indem Sie im Popup-Fenster Asset veröffentlichen erneut auf Asset veröffentlichen klicken.

> **Note**
>
> Wenn Sie die generierten Beschreibungen für ein Asset nicht akzeptieren oder ablehnen und dieses Asset dann veröffentlichen, sind diese ungeprüften, automatisch generierten Metadaten nicht im veröffentlichten Daten-Asset enthalten.

Daten in Amazon entdecken, abonnieren und nutzen DataZone

Sobald ein Asset in einer Domain veröffentlicht wurde, können Abonnenten bei Amazon DataZone dieses Asset finden und ein Abonnement für dieses Asset beantragen. Der Abonnementprozess beginnt damit, dass ein Abonnent im Katalog nach einem gewünschten Asset sucht und es durchsucht. Über das DataZone Amazon-Portal entscheiden sie sich dafür, das Asset zu abonnieren, indem sie eine Abonnementanfrage einreichen, die eine Begründung und den Grund für die Anfrage enthält. Der Genehmigungsberechtigte für das Abonnement, wie in der Veröffentlichungsvereinbarung definiert, prüft dann die Zugriffsanfrage. Er kann die Anfrage entweder genehmigen oder ablehnen.

Nachdem ein Abonnement gewährt wurde, beginnt ein Fulfillment-Prozess, der dem Abonnenten den Zugriff auf das Asset erleichtert. Es gibt zwei Hauptmodi für die Zugriffskontrolle und DataZone -abwicklung von Vermögenswerten: die für von Amazon verwaltete Vermögenswerte und die für Anlagen, die nicht von Amazon DataZone verwaltet werden.

- Verwaltete Ressourcen — Amazon DataZone kann den Versand und die Berechtigungen für verwaltete Ressourcen wie AWS Glue Tabellen und Amazon Redshift Redshift-Tabellen und -Ansichten verwalten.
- Nicht verwaltete Ressourcen — Amazon DataZone veröffentlicht Standardereignisse im Zusammenhang mit Ihren Aktionen (z. B. die Genehmigung einer Abonnementanfrage) an Amazon EventBridge. Sie können diese Standardereignisse verwenden, um sie in andere AWS Dienste oder Lösungen von Drittanbietern für benutzerdefinierte Integrationen zu integrieren.

Themen

Daten entdecken

In den folgenden Aufgaben werden verschiedene Möglichkeiten beschrieben, Daten in Amazon zu ermitteln DataZone.

Themen

Suchen Sie nach Ressourcen im Katalog und sehen Sie sich diese an

Amazon DataZone bietet eine optimierte Methode zur Suche nach Daten. Jeder DataZone Amazon-Benutzer mit Zugriffsberechtigungen für das Datenportal kann im DataZone Amazon-Katalog nach Assets suchen und die Asset-Namen und die ihnen zugewiesenen Metadaten einsehen. Sie können sich ein Asset genauer ansehen, indem Sie sich dessen Detailseite ansehen.

> **Note**
>
> Um die tatsächlichen Daten zu sehen, die ein Asset enthält, müssen Sie das Asset zunächst abonnieren und Ihre Abonnementanfrage genehmigen und den Zugriff gewähren lassen. Weitere Informationen finden Sie unter Daten abonnieren.

Um im Katalog nach Assets zu suchen

1. Navigieren Sie zur URL des DataZone Amazon-Datenportals und melden Sie sich mit Single Sign-On (SSO) oder Ihren AWS Anmeldeinformationen an. Wenn Sie ein DataZone Amazon-Administrator sind, können Sie unter https://console.aws.amazon.com/datazone zur DataZone Amazon-Konsole navigieren und sich dort anmelden, AWS-Konto wo die Domain erstellt wurde, und dann Datenportal öffnen wählen.
2. Sie können den Namen des Assets, nach dem Sie suchen, in die Suchleiste auf der Startseite des Datenportals eingeben.
3. Um Namespaces zu durchsuchen, wählen Sie oben rechts auf der Seite „Katalog“ aus, um den Katalog zu öffnen. Der Katalog bietet ein vielseitiges Sucherlebnis, mit dem Sie Assets anhand von Kriterien wie Dateneigentümer und Glossarbegriffen finden können.
4. Geben Sie Ihren Suchbegriff in eines der Suchfelder ein. Nachdem Sie eine Suche ausgeführt haben, können Sie verschiedene Filter anwenden, um die Ergebnisse einzugrenzen. Zu den

Filtern gehören der Anlagentyp, das Quellkonto und das Objekt, AWS-Region zu dem das Asset gehört.

5. Um Details zu einem bestimmten Asset anzuzeigen, wählen Sie das Asset aus, um die zugehörige Detailseite zu öffnen. Die Detailseite enthält die folgenden Informationen:

   - Der Asset-Name, die Datenquelle (AWS Glue Amazon Redshift oder Amazon S3), der Typ (Tabelle, Ansicht oder S3-Objekt), die Anzahl der Spalten und die Größe.
   - Eine Beschreibung des Assets.
   - Die aktuell veröffentlichte Version des Assets, der Besitzer, ob für Abonnements eine Genehmigung erforderlich ist, der Namespace und der Aktualisierungsverlauf.
   - Eine Registerkarte „Übersicht“, die Glossarbegriffe und Metadatenformulare enthält.
   - Eine Registerkarte „Schema“, auf der das Schema des Assets angezeigt wird, einschließlich geschäftlicher und technischer Spaltennamen, Datentypen und Geschäftsbeschreibungen der Spalten. Die Registerkarte Schema ist nur für Tabellen und Ansichten sichtbar (nicht für Amazon S3 S3-Objekte).
   - Eine Registerkarte „Abonnements“, die eine Liste der Abonnenten der Domain enthält.
   - Eine Registerkarte „Verlauf“, die eine Liste früherer Versionen des Assets enthält.

Daten abonnieren

Die folgenden Aufgaben enthalten Einzelheiten zum Abonnieren von Ressourcen bei Amazon DataZone.

Themen

Fordern Sie ein Abonnement für Ressourcen an

Amazon DataZone ermöglicht es Ihnen, die Ressourcen im DataZone Amazon-Katalog zu finden, darauf zuzugreifen und sie zu nutzen. Wenn Sie im Katalog ein Asset finden, auf das Sie zugreifen möchten, müssen Sie das Asset abonnieren, wodurch eine Abonnementanfrage erstellt wird. Ein Genehmiger kann Ihre Anfrage dann genehmigen oder anfordern.

Sie müssen Mitglied eines Projekts sein, um ein Abonnement für ein Asset innerhalb dieses Projekts beantragen zu können.

Um ein Asset zu abonnieren

1. Navigieren Sie zur URL des DataZone Amazon-Datenportals und melden Sie sich mit Single Sign-On (SSO) oder Ihren AWS Anmeldeinformationen an. Wenn Sie ein DataZone Amazon-Administrator sind, können Sie unter https://console.aws.amazon.com/datazone zur DataZone Amazon-Konsole navigieren und sich dort anmelden, AWS-Konto wo die Domain erstellt wurde, und dann Datenportal öffnen wählen.
2. Verwenden Sie die Suchleiste, um nach dem Asset zu suchen und es auszuwählen, das Sie abonnieren möchten, und wählen Sie dann Abonnieren.
3. Geben Sie im Popup-Fenster „Abonnieren“ die folgenden Informationen ein:
   - Das Projekt, für das Sie das Asset abonnieren möchten.
   - Eine kurze Begründung für Ihre Abonnementanfrage.
4. Wählen Sie Subscribe (Abonnieren) aus.

   Sie erhalten im Datenportal eine Benachrichtigung, wenn der Verlag Ihre Anfrage genehmigt.

Um den Status der Abonnementanfrage einzusehen, suchen Sie das Projekt, mit dem Sie das Asset abonniert haben, und wählen Sie es aus. Navigieren Sie zur Registerkarte Daten für das Projekt und wählen Sie dann im linken Navigationsbereich die Option Angeforderte Daten aus. Auf dieser Seite werden die Ressourcen aufgeführt, für die das Projekt Zugriff angefordert hat. Sie können die Liste nach dem Status der Anfrage filtern.

Genehmigen oder lehnen Sie eine Abonnementanfrage ab

Amazon DataZone ermöglicht es Ihnen, die Ressourcen im DataZone Amazon-Katalog zu finden, darauf zuzugreifen und sie zu nutzen. Wenn Sie im Katalog ein Asset finden, auf das Sie zugreifen

möchten, müssen Sie das Asset abonnieren, wodurch eine Abonnementanfrage erstellt wird. Ein Genehmiger kann Ihre Anfrage dann genehmigen oder ablehnen.

Sie müssen Mitglied des Projekts sein, das Eigentümer ist (das Projekt, das das Asset veröffentlicht hat), um eine Abonnementanfrage genehmigen oder ablehnen zu können.

Um eine Abonnementanfrage zu genehmigen oder abzulehnen

1. Navigieren Sie zur URL des DataZone Amazon-Datenportals und melden Sie sich mit Single Sign-On (SSO) oder Ihren AWS Anmeldeinformationen an. Wenn Sie ein DataZone Amazon-Administrator sind, können Sie unter https://console.aws.amazon.com/datazone zur DataZone Amazon-Konsole navigieren und sich dort anmelden, AWS-Konto wo die Domain erstellt wurde, und dann Datenportal öffnen wählen.
2. Wählen Sie im Datenportal die Option Projektliste durchsuchen und wählen Sie das Projekt aus, das das Asset mit der Abonnementanfrage enthält.
3. Navigieren Sie zur Registerkarte Daten und wählen Sie dann im linken Navigationsbereich Eingehende Anfragen aus.
4. Suchen Sie die Anfrage und wählen Sie Anfrage anzeigen aus. Sie können nach Ausstehend filtern, um nur Anfragen zu sehen, die noch offen sind.
5. Prüfen Sie die Abonnementanfrage und den Grund für den Zugriff und entscheiden Sie, ob Sie sie genehmigen oder ablehnen möchten.
6. (Optional) Geben Sie eine Antwort ein, in der Sie den Grund für die Annahme oder Ablehnung der Anfrage erläutern.
7. Wählen Sie entweder Genehmigen oder Ablehnen.

Als Projektinhaber können Sie das Abonnement jederzeit kündigen. Weitere Informationen finden Sie unter the section called “Widerrufen Sie ein bestehendes Abonnement”.

Eine Übersicht aller Abonnementanfragen finden Sie unterArbeiten mit DataZone Amazon-Ereignissen und -Benachrichtigungen.

Widerrufen Sie ein bestehendes Abonnement

Amazon DataZone ermöglicht es Ihnen, die Ressourcen im DataZone Amazon-Katalog zu finden, darauf zuzugreifen und sie zu nutzen. Wenn Sie im Katalog ein Asset finden, auf das Sie zugreifen möchten, müssen Sie das Asset abonnieren, wodurch eine Abonnementanfrage erstellt wird. Ein Genehmiger kann Ihre Anfrage dann genehmigen oder anfordern. Möglicherweise müssen Sie ein

Abonnement kündigen, nachdem Sie es genehmigt haben, entweder weil die Genehmigung ein Fehler war oder weil der Abonnent keinen Zugriff mehr auf das Asset benötigt.

Sie müssen Mitglied des Projekts sein, das Eigentümer ist (das Projekt, das das Asset veröffentlicht hat), um ein Abonnement zu kündigen.

Um ein Abonnement zu kündigen

1. Navigieren Sie zur URL des DataZone Amazon-Datenportals und melden Sie sich mit Single Sign-On (SSO) oder Ihren AWS Anmeldeinformationen an. Wenn Sie ein DataZone Amazon-Administrator sind, können Sie unter https://console.aws.amazon.com/datazone zur DataZone Amazon-Konsole navigieren und sich dort anmelden, AWS-Konto wo die Domain erstellt wurde, und dann Datenportal öffnen wählen.
2. Wählen Sie im oberen Navigationsbereich die Option Projekt auswählen und wählen Sie das Projekt aus, das das Abonnement enthält, das Sie kündigen möchten.
3. Navigieren Sie zur Registerkarte Daten und wählen Sie dann im linken Navigationsbereich Eingehende Anfragen aus.
4. Suchen Sie das Abonnement, das Sie kündigen möchten, und wählen Sie Abonnement anzeigen aus.
5. (Optional) Aktivieren Sie das Kontrollkästchen, damit der Abonnent das Asset in den Abonnementzielen des Projekts behalten kann. Ein Abonnementziel ist ein Verweis auf eine Reihe von Ressourcen, über die abonnierte Daten innerhalb einer Umgebung verfügbar gemacht werden können.

   Wenn Sie dem Abonnementziel zu einem späteren Zeitpunkt den Zugriff auf das Asset entziehen möchten, müssen Sie dies unter tun. AWS Lake Formation
6. Wählen Sie Abonnement widerrufen aus.

Sie können ein Abonnement nicht erneut genehmigen, nachdem Sie es widerrufen haben. Der Abonnent muss das Asset erneut abonnieren, damit Sie es genehmigen können.

Stornieren Sie eine Abonnementanfrage

Amazon DataZone ermöglicht es Ihnen, die Ressourcen im DataZone Amazon-Katalog zu finden, darauf zuzugreifen und sie zu nutzen. Wenn Sie im Katalog ein Asset finden, auf das Sie zugreifen möchten, müssen Sie das Asset abonnieren, wodurch eine Abonnementanfrage erstellt wird. Ein Genehmiger kann Ihre Anfrage dann genehmigen oder anfordern. Möglicherweise müssen Sie eine

ausstehende Abonnementanfrage stornieren, entweder weil Sie sie versehentlich eingereicht haben oder weil Sie keinen Lesezugriff mehr auf das Asset benötigen.

Um eine Abonnementanfrage zu stornieren, müssen Sie entweder Projektinhaber oder Mitwirkender sein.

Um eine Abonnementanfrage zu stornieren

1. Navigieren Sie zur URL des DataZone Amazon-Datenportals und melden Sie sich mit Single Sign-On (SSO) oder Ihren AWS Anmeldeinformationen an. Wenn Sie ein DataZone Amazon-Administrator sind, können Sie unter https://console.aws.amazon.com/datazone zur DataZone Amazon-Konsole navigieren und sich dort anmelden, AWS-Konto wo die Domain erstellt wurde, und dann Datenportal öffnen wählen.
2. Wählen Sie im oberen Navigationsbereich die Option Projekt auswählen und wählen Sie das Projekt aus, das die Abonnementanfrage enthält.
3. Navigieren Sie zur Registerkarte Daten für das Projekt und wählen Sie dann im linken Navigationsbereich die Option Angeforderte Daten aus. Auf dieser Seite werden die Ressourcen aufgeführt, für die das Projekt Zugriff angefordert hat.
4. Filtern Sie nach Angefordert, um nur Anfragen zu sehen, die noch ausstehen. Suchen Sie die Anfrage und wählen Sie Anfrage anzeigen aus.
5. Überprüfen Sie die Abonnementanfrage und wählen Sie Anfrage stornieren.

Wenn Sie das Asset (oder ein anderes Asset) erneut abonnieren möchten, finden Sie weitere Informationen unterthe section called “Fordern Sie ein Abonnement für Ressourcen an”.

Ein Asset abbestellen

Amazon DataZone ermöglicht es Ihnen, die Ressourcen im DataZone Amazon-Katalog zu finden, darauf zuzugreifen und sie zu nutzen. Wenn Sie im Katalog ein Asset finden, auf das Sie zugreifen möchten, müssen Sie das Asset abonnieren, wodurch eine Abonnementanfrage erstellt wird. Ein Genehmiger kann Ihre Anfrage dann genehmigen oder anfordern. Möglicherweise müssen Sie ein Asset abbestellen, entweder weil Sie es versehentlich abonniert haben und dafür eine Genehmigung erhalten haben, oder weil Sie keinen Lesezugriff mehr für das Asset benötigen.

Sie müssen Mitglied eines Projekts sein, um eines seiner Assets abbestellen zu können.

Um sich von einem Asset abzumelden

1. Navigieren Sie zur URL des DataZone Amazon-Datenportals und melden Sie sich mit Single Sign-On (SSO) oder Ihren AWS Anmeldeinformationen an. Wenn Sie ein DataZone Amazon-Administrator sind, können Sie unter https://console.aws.amazon.com/datazone zur DataZone Amazon-Konsole navigieren und sich dort anmelden, AWS-Konto wo die Domain erstellt wurde, und dann Datenportal öffnen wählen.
2. Wählen Sie im oberen Navigationsbereich die Option Projekt auswählen und wählen Sie das Projekt aus, das das Asset enthält, von dem Sie sich abmelden möchten.
3. Navigieren Sie zur Registerkarte Daten für das Projekt und wählen Sie dann im linken Navigationsbereich die Option Angeforderte Daten aus. Auf dieser Seite werden die Ressourcen aufgeführt, für die das Projekt Zugriff angefordert hat.
4. Filtern Sie nach Genehmigt, um nur Anfragen zu sehen, die genehmigt wurden. Suchen Sie die Anfrage und wählen Sie Abonnement anzeigen aus.
5. Prüfen Sie das Abonnement und wählen Sie Abbestellen.

Wenn Sie das Asset (oder ein anderes Asset) erneut abonnieren möchten, finden Sie weitere Informationen unterthe section called “Fordern Sie ein Abonnement für Ressourcen an”.

Nutzung vorhandener IAM-Rollen zur Erfüllung von Amazon-Abonnements DataZone

In der aktuellen Version DataZone unterstützt Amazon Sie dabei, Ihre vorhandenen IAM-Rollen zu verwenden, um Zugriff auf die Daten zu erhalten. Um dies zu erreichen, können Sie in der DataZone Amazon-Umgebung, die Sie für die Erfüllung Ihres Abonnements verwenden, ein Abonnementziel erstellen. Um ein Abonnementziel für eine Umgebung in einem der zugehörigen AWS Konten zu erstellen, können Sie die folgenden Schritte ausführen:

Schritt 1: Stellen Sie sicher, dass Ihre DataZone Amazon-Domain Version 2 oder höher der RAM-Richtlinie verwendet

1. Navigieren Sie in der AWS RAM-Konsole zur Seite Shared by me: Resource Shares.
2. Da AWS RAM-Ressourcenfreigaben in bestimmten AWS Regionen existieren, wählen Sie die entsprechende AWS Region aus der Dropdownliste in der oberen rechten Ecke der Konsole aus.
3. Wählen Sie den Resource Share aus, der Ihrer DataZone Amazon-Domain entspricht, und klicken Sie dann auf Ändern. Sie können die RAM-Freigabe für die DataZone Amazon-Domain

anhand des Namens oder der ID der Domain identifizieren, da die RAM-Freigabe mit dem Namen erstellt wird:`DataZone-<domain-name>-<domain-id>`.

4. Wählen Sie Weiter, um mit dem nächsten Schritt fortzufahren, in dem Sie die Version der RAM-Richtlinie überprüfen und ändern können.
5. Stellen Sie sicher, dass die Version der RAM-Richtlinie Version 2 oder höher ist. Wenn nicht, verwenden Sie das Dropdownmenü, um Version 2 oder höher auszuwählen.
6. Wählen Sie Weiter zu Schritt 4: Überprüfen und aktualisieren.
7. Wählen Sie „Ressourcenfreigabe aktualisieren“.

Schritt 2: Erstellen Sie ein Abonnementziel aus einem verknüpften Konto

- In der aktuellen Version DataZone unterstützt Amazon die Erstellung von Abonnementzielen nur mithilfe von APIs. Im Folgenden finden Sie einige Beispiele für die Payload, die Sie verwenden können, um ein Abonnementziel für die Erfüllung von Abonnements für Ihre AWS Glue-Tabellen und Amazon Redshift Redshift-Tabellen oder -Ansichten zu erstellen. Weitere Informationen finden Sie unter. CreateSubscriptionTarget

  Beispiel für ein Abonnementziel für AWS Glue

```
{
        "domainIdentifier": "<DOMAIN_ID>",
        "environmentIdentifier": "<ENVIRONMENT_ID>",
        "name": "<SUBSCRIPTION_TARGET_NAME>",
        "type": "GlueSubscriptionTargetType",
        "authorizedPrincipals" : ["IAM_ROLE_ARN"],
        "subscriptionTargetConfig" : [{"content": "{\"databaseName\":
 \"<DATABASE_NAME>\"}", "formName": "GlueSubscriptionTargetConfigForm"}],
        "manageAccessRole": "<GLUE_DATA_ACCESS_ROLE_IN_ASSOCIATED_ACCOUNT_ARN>",
        "applicableAssetTypes" : ["GlueTableAssetType"],
        "provider": "Amazon DataZone"
}
```

  Beispiel für ein Abonnementziel für Amazon Redshift:

```
{
        "domainIdentifier": "<DOMAIN_ID>",
```

```
        "environmentIdentifier": "<ENVIRONMENT_ID>",
        "name": "<SUBSCRIPTION_TARGET_NAME>",
        "type": "RedshiftSubscriptionTargetType",
        "authorizedPrincipals" : ["REDSHIFT_DATABASE_ROLE_NAME"],
        "subscriptionTargetConfig" : [{"content": "{\"databaseName\":
 \"<DATABASE_NAME>\", \"secretManagerArn\": \"<SECRET_MANAGER_ARN>
\",\"clusterIdentifier\": \"<CLUSTER_IDENTIFIER>\"}", "formName":
 "RedshiftSubscriptionTargetConfigForm"}],
        "manageAccessRole":
 "<REDSHIFT_DATA_ACCESS_ROLE_IN_ASSOCIATED_ACCOUNT_ARN>",
        "applicableAssetTypes" : ["RedshiftViewAssetType",
 "RedshiftTableAssetType"],
        "provider": "Amazon DataZone"
}
```

Important

- Der EnvironmentIdentifier, den Sie im obigen API-Aufruf verwenden, sollte in demselben verknüpften Konto vorhanden sein, von dem aus Sie den API-Aufruf tätigen. Andernfalls ist der API-Aufruf nicht erfolgreich.
- Die IAM-Rolle ARN, die Sie in den „AuthorizedPrincipals“ verwenden, ist die Rolle, auf die Amazon DataZone Zugriff gewährt, nachdem ein abonniertes Asset zum Abonnementziel hinzugefügt wurde. Diese autorisierten Principals müssen demselben Konto angehören wie die Umgebung, in der das Abonnementziel erstellt wird.
- Der Wert für das Anbieterfeld muss „Amazon DataZone“ lauten DataZone , damit Amazon die Abonnementabwicklung abschließen kann.
- Der in angegebene Datenbankname subscriptionTargetConfig sollte in dem Konto, in dem das Ziel erstellt wird, bereits vorhanden sein. Amazon DataZone wird diese Datenbank nicht erstellen. Stellen Sie außerdem sicher, dass die Rolle „Zugriff verwalten“ über die CREATE TABLE-Berechtigung für diese Datenbank verfügt.
- Stellen Sie außerdem sicher, dass die Rollen (IAM-Rolle für AWS Glue und Datenbankrolle für Amazon Redshift) bereitgestellt werden, da die autorisierten Prinzipale bereits im Umgebungskonto vorhanden sind. Für Amazon Redshift Redshift-Abonnementziele sind zusätzliche Updates für die Rolle erforderlich, die bei der Verbindung mit dem Cluster übernommen wird. Dieser Rolle muss ein RedshiftDbRoles Tag zugewiesen sein. Der Wert des Tags kann eine durch Kommas

getrennte Liste sein. Der Wert sollte die Datenbankrolle sein, die bei der Erstellung des Abonnementziels als autorisierter Prinzipal angegeben wurde.

Schritt 3: Abonnieren Sie eine neue Tabelle und schließen Sie das Abonnement für das neue Ziel ab

- Sobald Sie das Abonnementziel erstellt haben, können Sie eine neue Tabelle abonnieren und Amazon DataZone wird es bis zum oben genannten Ziel erfüllen. Weitere Informationen finden Sie unter Daten abonnieren.

Zugriff auf Daten gewähren

Die folgenden Aufgaben enthalten Einzelheiten zur Gewährung des Zugriffs auf genehmigte Abonnements für Ressourcen in Amazon DataZone.

Bei Amazon DataZone werden Abonnementanfragen und genehmigte oder gewährte Abonnements für den Lesezugriff auf die Ressourcen von Abonnementgenehmigern verwaltet. Ein Abonnement-Genehmiger für ein Asset wird durch die Veröffentlichungsvereinbarung bestimmt, mit der dieses Asset im DataZone Amazon-Katalog veröffentlicht wurde.

Themen

- Gewähren Sie Zugriff auf verwaltete Ressourcen AWS Glue Data Catalog
- Zugriff auf verwaltete Amazon Redshift Redshift-Assets gewähren
- Gewähren Sie genehmigten Abonnements Zugriff auf nicht verwaltete Ressourcen

Gewähren Sie Zugriff auf verwaltete Ressourcen AWS Glue Data Catalog

> **Note**
>
> Die Zugriffsverwaltung für die AWS Glue Data Catalog Ressourcen mithilfe der AWS Lake Formation LF-TBAC-Methode wird nicht unterstützt.
> Die Support für die regionsübergreifende gemeinsame Nutzung von Ressourcen AWS Glue Data Catalog wird nicht unterstützt.

Sobald eine Abonnementanfrage für verwaltete AWS Glue Data Catalog Ressourcen genehmigt wurde, fügt Amazon diese Ressourcen DataZone automatisch allen vorhandenen Data-Lake-

Umgebungen im Projekt hinzu. Amazon gewährt und verwaltet DataZone dann in Ihrem Namen Zugriff auf die genehmigten AWS Glue Data Catalog Tabellen über AWS Lake Formation. Für das Abonnentenprojekt werden die gewährten Ressourcen in Ihrem Konto AWS Glue Data Catalog als Ressourcen angezeigt. Anschließend können Sie Amazon Athena verwenden, um die Tabellen abzufragen.

> **Note**
>
> Wenn dem Projekt eine neue Data Lake-Umgebung hinzugefügt wird, nachdem die abonnierten AWS Glue Data Catalog Ressourcen automatisch zu den vorhandenen Data Lake-Umgebungen hinzugefügt wurden, müssen Sie diese abonnierten AWS Glue Data Catalog Ressourcen manuell zu dieser neuen Data-Lake-Umgebung hinzufügen. Sie können dies tun, indem Sie auf der Übersichtsseite des Projekts im Amazon-Datenportal auf der Registerkarte DataZone Daten die Option Zuschuss hinzufügen auswählen.

Damit Amazon DataZone Zugriff auf AWS Glue Data Catalog-Tabellen gewähren kann, müssen die folgenden Bedingungen erfüllt sein.

- Die AWS Glue-Tabelle muss von Lake Formation verwaltet werden, da Amazon Zugriff DataZone gewährt, indem es Lake Formation Formation-Berechtigungen verwaltet.
- Die Zugriffsrolle „Zugriff verwalten“ für die Data Lake-Umgebung, die zur Veröffentlichung der AWS Glue Data Catalog-Tabelle verwendet wird, muss über die folgenden Lake Formation Formation-Berechtigungen verfügen:
  - `DESCRIBE`und `DESCRIBE GRANTABLE` Berechtigungen für die AWS Glue-Datenbank, die die veröffentlichte Tabelle enthält.
  - `DESCRIBE`, `SELECTDESCRIBE GRANTABLE`, `SELECT GRANTABLE` Berechtigungen in Lake Formation für die veröffentlichte Tabelle selbst.

Weitere Informationen finden Sie im AWS Lake Formation Entwicklerhandbuch unter Erteilen und Widerrufen von Berechtigungen für Katalogressourcen.

Zugriff auf verwaltete Amazon Redshift Redshift-Assets gewähren

Wenn ein Abonnement für eine Amazon Redshift Redshift-Tabelle oder -Ansicht genehmigt wurde, DataZone kann Amazon das abonnierte Asset automatisch zu allen Data Warehouse-Umgebungen innerhalb des Projekts hinzufügen, sodass Mitglieder des Projekts die Daten über den Amazon

Redshift Redshift-Abfrage-Editor-Link in ihren Umgebungen abfragen können. Unter der Haube sorgt Amazon DataZone für die erforderlichen Zuschüsse und Datenfreigaben zwischen der Quelle und dem Abonnementziel.

Das Verfahren zur Gewährung des Zugriffs hängt davon ab, wo sich die Quelldatenbank (Herausgeber) und die Zieldatenbank (Abonnent) befinden.

- Derselbe Cluster, dieselbe Datenbank — wenn Daten innerhalb derselben Datenbank gemeinsam genutzt werden müssen, DataZone gewährt Amazon Berechtigungen direkt für die Quelltabelle.
- Derselbe Cluster, andere Datenbank — Wenn Daten von zwei Datenbanken innerhalb desselben Clusters gemeinsam genutzt werden müssen, DataZone erstellt Amazon eine Ansicht in der Zieldatenbank und Berechtigungen werden für die erstellte Ansicht gewährt.
- Gleiches Konto, anderer Cluster — Amazon DataZone erstellt einen Datenaustausch zwischen dem Quell- und dem Zielcluster und erstellt eine Ansicht über der gemeinsam genutzten Tabelle. Für die Ansicht werden Berechtigungen erteilt.
- Kontoübergreifend — wie oben, aber es ist ein zusätzlicher Schritt erforderlich, um die kontenübergreifende Datenfreigabe auf der Producer-Cluster-Seite zu autorisieren, und ein weiterer Schritt, um die Datenfreigabe auf der Consumer-Cluster-Seite zuzuordnen.

> **Note**
>
> Wenn dem Projekt eine neue Data Warehouse-Umgebung hinzugefügt wird, nachdem die abonnierten Amazon Redshift Redshift-Assets automatisch zu den vorhandenen Data Warehouse-Umgebungen hinzugefügt wurden, müssen Sie diese abonnierten Amazon Redshift Redshift-Assets manuell zu dieser neuen Data Warehouse-Umgebung hinzufügen. Sie können dies tun, indem Sie auf der Übersichtsseite des Projekts im Amazon-Datenportal auf der Registerkarte DataZone Daten die Option Zuschuss hinzufügen auswählen.

Stellen Sie sicher, dass Ihre Amazon Redshift Redshift-Cluster, die Sie veröffentlichen und abonnieren, alle Anforderungen für Amazon Redshift Redshift-Datenfreigaben erfüllen. Weitere Informationen finden Sie im Amazon Redshift Developer Guide.

> **Note**
>
> Amazon DataZone unterstützt die automatische Gewährung von Abonnements für Amazon Redshift Cluster- und Amazon Redshift Serverless-Assets.

Der regionsübergreifende Datenaustausch mit Amazon Redshift wird nicht unterstützt.

> **Note**
>
> In der aktuellen Version DataZone kann Amazon den Zugriff auf Amazon Redshift Redshift-Tabellen und -Ansichten nur verwalten, wenn sich die Amazon Redshift Redshift-Quell- und Ziel-Cluster oder -Arbeitsgruppen in den AWS Konten befinden, die derselben Organisation angehören. AWS

Gewähren Sie genehmigten Abonnements Zugriff auf nicht verwaltete Ressourcen

Amazon DataZone ermöglicht es Benutzern, jede Art von Asset im Geschäftsdatenkatalog zu veröffentlichen. Für einige dieser Ressourcen DataZone kann Amazon Zugriffsberechtigungen automatisch verwalten. Diese Ressourcen werden als verwaltete Assets bezeichnet und umfassen von Lake Formation verwaltete AWS Glue Data Catalog-Tabellen sowie Amazon Redshift Redshift-Tabellen und -Ansichten. Alle anderen Ressourcen, für die Amazon nicht automatisch Abonnements gewähren DataZone kann, werden als nicht verwaltet bezeichnet.

Amazon DataZone bietet Ihnen eine Möglichkeit, Zugriffsberechtigungen für Ihre nicht verwalteten Vermögenswerte zu verwalten. Wenn ein Abonnement für ein Asset im Geschäftsdatenkatalog vom Dateneigentümer genehmigt wird, DataZone veröffentlicht Amazon ein Ereignis in Amazon EventBridge in Ihrem Konto zusammen mit allen erforderlichen Informationen in der Payload, mit denen Sie die Zugriffsberechtigungen zwischen der Quelle und dem Ziel erstellen können. Wenn Sie dieses Ereignis erhalten, können Sie einen benutzerdefinierten Handler auslösen, der die in dem Ereignis enthaltenen Informationen verwenden kann, um die erforderlichen Zuschüsse oder Genehmigungen zu erstellen. Sobald Sie den Zugriff gewährt haben, können Sie den Status des Abonnements in Amazon zurückmelden und aktualisieren, DataZone sodass die Benutzer, die das Asset abonniert haben, darüber informiert werden, dass sie das Asset nutzen können. Weitere Informationen finden Sie unter Arbeiten mit DataZone Amazon-Ereignissen und -Benachrichtigungen.

Daten werden konsumiert

Die folgenden Aufgaben enthalten Einzelheiten zur Nutzung von Daten, die Sie bei Amazon DataZone abonniert haben.

Themen

Daten in Amazon Athena oder Amazon Redshift abfragen

Sobald ein Abonnent in Amazon DataZone Zugriff auf ein Asset im Katalog hat, kann er es mit Amazon Athena oder dem Amazon Redshift Query Editor v2 nutzen (abfragen und analysieren). Sie müssen ein Projektinhaber oder Mitwirkender sein, um diese Aufgabe abschließen zu können. Abhängig von den im Projekt aktivierten Blueprints DataZone stellt Amazon Links zu Amazon Athena und/oder Amazon Redshift Query Editor v2 im rechten Bereich der Projektseite im Datenportal bereit.

1. Navigieren Sie zur URL des DataZone Amazon-Datenportals und melden Sie sich mit Single Sign-On (SSO) oder Ihren AWS Anmeldeinformationen an. Wenn Sie ein DataZone Amazon-Administrator sind, können Sie unter https://console.aws.amazon.com/datazone zur DataZone Amazon-Konsole navigieren und sich dort anmelden, AWS-Konto wo die Domain erstellt wurde, und dann Datenportal öffnen wählen.
2. Wählen Sie im DataZone Amazon-Datenportal die Option Projektliste durchsuchen und suchen Sie dann das Projekt, in dem Sie die Daten haben, die Sie analysieren möchten, und wählen Sie es aus.
3. Wenn der Data Lake-Blueprint für dieses Projekt aktiviert ist, wird im rechten Seitenbereich auf der Startseite des Projekts ein Link zu Amazon Athena angezeigt.

   Wenn der Data Warehouse-Blueprint für dieses Projekt aktiviert ist, wird im rechten Seitenbereich auf der Startseite des Projekts ein Link zum Abfrage-Editor angezeigt.

   > **Note**
   >
   > Blueprints werden in dem Umgebungsprofil definiert, mit dem ein Projekt erstellt wird.

Themen

Daten mit Amazon Athena abfragen

Wählen Sie den Amazon Athena Athena-Link, um den Amazon Athena Athena-Abfrage-Editor auf einer neuen Registerkarte im Browser zu öffnen und dabei die Anmeldeinformationen des Projekts für die Authentifizierung zu verwenden. Das DataZone Amazon-Projekt, mit dem Sie arbeiten, wird im Abfrage-Editor automatisch als aktuelle Arbeitsgruppe ausgewählt.

Schreiben Sie Ihre Abfragen im Amazon Athena Athena-Abfrage-Editor und führen Sie sie aus. Zu den häufigsten Aufgaben gehören:

- Fragen Sie Ihre abonnierten Ressourcen ab und analysieren Sie sie
- Neue Tabellen erstellen
- Erstellen Sie eine Tabelle aus Abfrageergebnissen (CTAS) aus einem externen S3-Bucket

Fragen Sie Ihre abonnierten Ressourcen ab und analysieren Sie sie

Wenn der Zugriff auf die Ressourcen, die Ihr Projekt abonniert hat, nicht automatisch von Amazon gewährt wird DataZone, müssen Sie berechtigt sein, auf die zugrunde liegenden Daten zuzugreifen. Weitere Informationen darüber, wie Sie Zugriff auf diese Ressourcen gewähren können, finden Sie unterGewähren Sie genehmigten Abonnements Zugriff auf nicht verwaltete Ressourcen.

Wenn der Zugriff auf die Ressourcen, die Ihr Projekt abonniert hat, automatisch von Amazon gewährt wird DataZone, können Sie SQL-Abfragen für die Tabellen ausführen und die Ergebnisse in Amazon Athena anzeigen. Weitere Informationen zur Verwendung von SQL in Amazon Athena finden Sie unter SQL-Referenz für Athena.

Wenn Sie zum Amazon Athena Athena-Abfrage-Editor navigieren, nachdem Sie den Amazon Athena Athena-Link im rechten Bereich auf der Startseite des Projekts ausgewählt haben, wird in der oberen rechten Ecke des Amazon Athena Athena-Abfrage-Editors ein Projekt-Drop-down-Menü angezeigt und Ihr Projektkontext wird automatisch ausgewählt.

In der Dropdownliste „Datenbank“ können Sie die folgenden Datenbanken sehen:

- Eine Veröffentlichungsdatenbank (*{environmentname}*_pub_db). Der Zweck dieser Datenbank besteht darin, Ihnen eine Umgebung zu bieten, in der Sie im Kontext Ihres Projekts neue Daten erstellen und diese Daten dann im DataZone Amazon-Katalog veröffentlichen können. Projekteigentümer und Mitwirkende haben Lese- und Schreibzugriff auf diese Datenbank. Projektbetrachter haben nur Lesezugriff auf diese Datenbank.

- Eine Abonnementdatenbank (*{environmentname}*_sub_db). Der Zweck dieser Datenbank besteht darin, Ihnen die Daten, die Sie als Projektmitglied im DataZone Amazon-Katalog abonniert haben, zur Verfügung zu stellen und es Ihnen zu ermöglichen, diese Daten abzufragen.

Neue Tabellen erstellen

Wenn Sie eine Verbindung zu einem externen S3-Bucket hergestellt haben, können Sie Amazon Athena verwenden, um die Ressourcen aus einem externen Amazon S3 S3-Bucket abzufragen und zu analysieren. In diesem Szenario DataZone hat Amazon keine Berechtigungen, um direkten Zugriff auf die zugrunde liegenden Daten im externen Amazon S3 S3-Bucket zu gewähren, und die externen Amazon S3 S3-Daten, die außerhalb des Projekts erstellt wurden, werden nicht automatisch in Lake Formation verwaltet und können auch nicht von Amazon verwaltet werden DataZone. Eine Alternative besteht darin, die Daten mithilfe einer `CREATE TABLE` Anweisung in Amazon Athena aus dem externen Amazon S3-Bucket in eine neue Tabelle im Amazon S3 S3-Bucket des Projekts zu kopieren. Wenn Sie eine `CREATE TABLE` Abfrage in Amazon Athena ausführen, registrieren Sie Ihre Tabelle bei der AWS Glue Data Catalog.

Zur Angabe des Pfads zu Ihren Daten in Amazon S3 verwenden Sie die `LOCATION`-Eigenschaft, wie im folgenden Beispiel gezeigt:

```
CREATE EXTERNAL TABLE 'test_table'(
...
)
ROW FORMAT ...
STORED AS INPUTFORMAT ...
OUTPUTFORMAT ...
LOCATION 's3://bucketname/folder/'
```

Weitere Informationen finden Sie unter Tabellenposition in Amazon S3.

Erstellen Sie eine Tabelle aus Abfrageergebnissen (CTAS) aus einem externen S3-Bucket

Wenn Sie ein Asset abonnieren, ist der Zugriff auf die zugrunde liegenden Daten schreibgeschützt. Sie können Amazon Athena verwenden, um eine Kopie der Tabelle zu erstellen. In Amazon Athena erstellt `A CREATE TABLE AS SELECT (CTAS)` Query eine neue Tabelle in Amazon Athena aus den Ergebnissen einer `SELECT` Anweisung aus einer anderen Abfrage. Informationen zur CTAS-Syntax finden Sie unter CREATE TABLE AS.

Das folgende Beispiel erstellt eine Tabelle durch Kopieren aller Spalten aus einer Tabelle:

```
CREATE TABLE new_table AS
SELECT *
FROM old_table;
```

In der folgenden Variante des gleichen Beispiels enthält Ihre SELECT-Anweisung auch eine WHERE-Klausel. In diesem Fall wählt die Abfrage nur die Zeilen aus der Tabelle aus, die die WHERE-Klausel erfüllen:

```
CREATE TABLE new_table AS
SELECT *
FROM old_table WHERE condition;
```

Das folgende Beispiel erstellt eine neue Abfrage, die auf einer Reihe von Spalten aus einer anderen Tabelle ausgeführt wird:

```
CREATE TABLE new_table AS
SELECT column_1, column_2, ... column_n
FROM old_table;
```

Diese Variation des gleichen Beispiels erstellt eine neue Tabelle aus bestimmten Spalten aus mehreren Tabellen:

```
CREATE TABLE new_table AS
SELECT column_1, column_2, ... column_n
FROM old_table_1, old_table_2, ... old_table_n;
```

Diese neu erstellten Tabellen sind jetzt Teil der AWS Glue Datenbank Ihrer Projekte und können für andere auffindbar gemacht und mit anderen DataZone Amazon-Projekten geteilt werden, indem Sie die Daten als Asset im DataZone Amazon-Katalog veröffentlichen.

Daten mit Amazon Redshift abfragen

Öffnen Sie im DataZone Amazon-Datenportal eine Umgebung, die den Data Warehouse-Blueprint verwendet. Wählen Sie den Amazon Redshift Redshift-Link im rechten Bereich auf der Umgebungsseite. Dadurch wird ein Bestätigungsdialogfeld mit den erforderlichen Details geöffnet, die Ihnen helfen, eine Verbindung zum Amazon Redshift-Cluster oder zur Amazon Redshift Serverless-Arbeitsgruppe Ihrer Umgebung im Amazon Redshift Query Editor v2.0 herzustellen. Sobald Sie die erforderlichen Details für den Verbindungsaufbau identifiziert haben, klicken Sie auf die Schaltfläche Amazon Redshift öffnen. Dadurch wird der Amazon Redshift Redshift-Abfrage-Editor v2.0 in einer neuen Registerkarte im Browser geöffnet, wobei temporäre Anmeldeinformationen der DataZone Amazon-Umgebung verwendet werden.

Führen Sie im Abfrage-Editor die folgenden Schritte aus, je nachdem, ob Ihre Umgebung eine Amazon Redshift Serverless-Arbeitsgruppe oder einen Amazon Redshift Redshift-Cluster verwendet.

Für eine serverlose Amazon Redshift Redshift-Arbeitsgruppe

1. Identifizieren Sie im Abfrage-Editor die Amazon Redshift Serverless-Arbeitsgruppe Ihrer DataZone Amazon-Umgebung, klicken Sie mit der rechten Maustaste darauf und wählen Sie Verbindung erstellen.
2. Wählen Sie Federated User für die Authentifizierung aus.
3. Geben Sie den Namen der Datenbank der DataZone Amazon-Umgebung an.
4. Wählen Sie Create Connection (Verbindung erstellen) aus.

Für einen Amazon Redshift Redshift-Cluster:

1. Identifizieren Sie im Abfrage-Editor den Amazon Redshift-Cluster Ihrer DataZone Amazon-Umgebung, klicken Sie mit der rechten Maustaste darauf und wählen Sie Verbindung erstellen.
2. Wählen Sie Temporäre Anmeldeinformationen mit Ihrer IAM-Identität zur Authentifizierung aus.
3. Wenn die oben genannte Authentifizierungsmethode nicht verfügbar ist, öffnen Sie die Kontoeinstellungen, indem Sie auf das Zahnrad in der unteren linken Ecke klicken, mit IAM-Anmeldeinformationen authentifizieren wählen und speichern. Dies ist eine one-time-only Einstellung.
4. Geben Sie den Namen der Datenbank der DataZone Amazon-Umgebung an, um die Verbindung herzustellen.
5. Wählen Sie Create Connection (Verbindung erstellen) aus.

Jetzt können Sie mit der Abfrage der Tabellen und Ansichten innerhalb des Amazon Redshift-Clusters oder der Amazon Redshift Serverless-Arbeitsgruppe beginnen, die für Ihre Amazon-Umgebung konfiguriert sind. DataZone

Alle Amazon Redshift-Tabellen oder -Ansichten, die Sie abonniert haben, sind mit dem Amazon Redshift Redshift-Cluster oder der Amazon Redshift Serverless-Arbeitsgruppe verknüpft, die für die Umgebung konfiguriert ist. Sie können die Tabellen und Ansichten abonnieren sowie alle neuen Tabellen und Ansichten veröffentlichen, die Sie im Cluster oder in der Datenbank Ihrer Umgebung erstellen.

Nehmen wir zum Beispiel ein Szenario, in dem eine Umgebung mit einem Amazon Redshift Redshift-Cluster verknüpft ist, der in diesem Cluster aufgerufen wird, `redshift-cluster-1` und einer Datenbank, die `dev` in diesem Cluster aufgerufen wird. Mithilfe des DataZone Amazon-Datenportals können Sie die Tabellen und Ansichten abfragen, die zu Ihrer Umgebung hinzugefügt wurden. Im `Analytics tools` Bereich auf der rechten Seite des Datenportals können Sie den Amazon Redshift Redshift-Link für diese Umgebung auswählen, wodurch der Abfrage-Editor geöffnet wird. Sie können dann mit der rechten Maustaste auf den `redshift-cluster-1` Cluster klicken und mithilfe temporärer Anmeldeinformationen unter Verwendung Ihrer IAM-Identität eine Verbindung herstellen. Sobald die Verbindung hergestellt ist, können Sie in der Dev-Datenbank alle Tabellen und Ansichten sehen, auf die Ihre Umgebung Zugriff hat.

Arbeiten mit DataZone Amazon-Ereignissen und -Benachrichtigungen

Amazon DataZone informiert Sie über wichtige Aktivitäten in Ihrem Datenportal, wie Abonnementanfragen, Updates, Kommentare und Systemereignisse. Amazon DataZone stellt Ihnen diese Informationen zur Verfügung, indem es Nachrichten in den dafür vorgesehenen Posteingang im Datenportal oder über den EventBridge Amazon-Standardbus zustellt.

Themen

Arbeiten mit Ereignissen über den speziellen Posteingang im DataZone Amazon-Datenportal

Amazon DataZone stellt im Datenportal einen eigenen Posteingang bereit, in dem Sie Ihre Nachrichten einsehen und entsprechende Maßnahmen ergreifen können. Aktuelle Nachrichten werden auch auf der Startseite, der Projektseite und der Katalogseite angezeigt. Wenn ein Benutzer beispielsweise Zugriff auf ein Datenobjekt anfordert, sehen die Eigentümer und Mitwirkenden des Veröffentlichungsprojekts die Anfrage im Datenportal. Sobald eine Aktion ausgeführt wurde, wird den Projektmitgliedern des abonnierten Projekts, das sich auf diese Anfrage bezieht, die Benachrichtigung im Datenportal angezeigt. Es gibt zwei Arten von Nachrichten:

- Aufgaben — Diese Nachrichten informieren den Empfänger darüber, dass irgendwo etwas unternommen werden muss. Sie haben ein optionales Statusfeld, das Sie zur Nachverfolgung verwenden können.
- Ereignisse — Diese Nachrichten sind informativ und haben keinen zugewiesenen Status. Ereignisse bieten einen Prüfpfad der letzten Aktualisierungen.

In Amazon DataZone werden Nachrichten für die folgenden Ereignistypen generiert:

Ereigniskategorie	Ereignisname	Beschreibung des Ereignisses	Ereignistyp
Abonnement	Abonnementanfrage erstellt	Das Ereignis wird generiert, wenn eine Abonnementanfrage erstellt wird	Aufgabe
Abonnement	Abonnementanfrage akzeptiert	Das Ereignis wird generiert, wenn eine Abonnementanfrage akzeptiert wird	Ereignis
Abonnement	Abonnementanfrage abgelehnt	Das Ereignis wird generiert, wenn eine Abonnementanfrage abgelehnt wird	Ereignis
Abonnement	Die Abonnemen tanfrage wurde gelöscht	Das Ereignis wird generiert, wenn eine Abonnementanfrage gelöscht wird	Ereignis
Projekt	Die Projekterstellung war erfolgreich	Das Ereignis wird generiert, wenn die Projekterstellung erfolgreich ist	Ereignis
Mitgliedschaft im Projekt	Die Aufnahme eines Projektmitglieds war erfolgreich	Das Ereignis wird generiert, wenn ein neues Mitglied zu einem Projekt hinzugefügt wird	Ereignis
Mitgliedschaft im Projekt	Die Entfernung des Projektmitglieds war erfolgreich	Das Ereignis wird generiert, wenn ein Mitglied aus einem Projekt entfernt wird	Ereignis

Ereigniskategorie	Ereignisname	Beschreibung des Ereignisses	Ereignistyp
Mitgliedschaft im Projekt	Die Änderung der Rolle des Projektmitglieds war erfolgreich	Das Ereignis wurde generiert. Die Rolle eines Mitglieds im Projekt wurde geändert	Ereignis
Umgebung	Die Bereitstellung der Umgebung wurde gestartet	Das Ereignis wird generiert, wenn eine Umgebungsbereitstellung initiiert wird	Ereignis
Umgebung	Die Bereitstellung der Umgebung ist abgeschlossen	Das Ereignis wird generiert, wenn eine Umgebungsbereitstellung erfolgreich abgeschlossen wurde	Ereignis
Umgebung	Die Bereitstellung der Umgebung ist fehlgeschlagen	Das Ereignis wird generiert, wenn eine Umgebungsbereitstellung fehlschlägt	Ereignis
Umgebung	Benutzerdefinierter Workflow zur Bereitstellung der Umgebung wurde initiiert	Das Ereignis wird generiert, wenn eine Umgebung mit einem benutzerdefinierten Workflow initiiert wird	Ereignis

Ereigniskategorie	Ereignisname	Beschreibung des Ereignisses	Ereignistyp
Datenbestand	Anlage wurde zum Inventar hinzugefügt	Das Ereignis wird generiert, wenn ein neues Datenobje kt zum Inventar hinzugefügt wird, d. h. wenn es dem Katalog im Entwurfsstatus hinzugefügt wird	Ereignis
Datenbestand	Anlage veröffentlicht	Das Ereignis wird generiert, wenn ein neues Datenobjekt veröffentlicht wird, d. h. es kann abonniert werden	Ereignis
Datenbestand	Das Asset-Schema wurde geändert	Das Ereignis wird generiert, wenn sich ein Asset-Schema seit dem letzten Aufnahmejob geändert hat	Ereignis
Abonnieren	Das Abonnement wurde erstellt	Das Ereignis wird generiert, wenn jemand das Abonnieren eines Datenbestands anfordert	Aufgabe

Ereigniskategorie	Ereignisname	Beschreibung des Ereignisses	Ereignistyp
Abonnieren	Abonnement genehmigt	Das Ereignis wird generiert, wenn ein Abonnement vom Eigentümer oder Mitwirkenden des Veröffentlichungsprojekts genehmigt wird	Ereignis
Abonnieren	Abonnement abgelehnt	Ein Ereignis wird generiert, wenn ein Abonnement vom Eigentümer oder Mitwirkenden des Veröffentlichungsprojekts abgelehnt wird	Ereignis
Abonnieren	Das Abonnement wurde gelöscht	Das Ereignis wird generiert, wenn ein Abonnement vom Abonnenten gekündigt wird	Ereignis
Abonnieren	Abonnementzuschuss beantragt	Das Ereignis wird generiert, wenn eine Person Zugriff auf ein Asset anfordert	Ereignis

Ereigniskategorie	Ereignisname	Beschreibung des Ereignisses	Ereignistyp
Abonnieren	Abonnementzuschuss abgeschlossen	Ein Ereignis wird generiert, wenn einem Abonnement vom Eigentümer oder Mitwirkenden des Veröffentlichungsprojekts Zugriff auf das Asset gewährt wird	Ereignis
Abonnieren	Die Abonnementgewährung ist fehlgeschlagen	Ein Ereignis wird generiert, wenn eine Abonnementgewährung fehlschlägt	Ereignis
Abonnieren	Widerruf des Abonnementzuschusses angefordert	Ein Ereignis wird generiert, wenn der Eigentümer oder Mitwirkender des veröffentlichenden Projekts einen widerrufenen Abonnementzuschuss initiiert	Ereignis
Abonnieren	Der Widerruf der Subskription ist abgeschlossen	Das Ereignis wird generiert, wenn der Widerruf eines Abonnementzuschusses abgeschlossen ist	Ereignis

Ereigniskategorie	Ereignisname	Beschreibung des Ereignisses	Ereignistyp
Abonnieren	Widerruf der Abonnemen tgewährung ist fehlgeschlagen	Das Ereignis wird generiert, wenn der Widerruf einer Abonnemen tgewährung fehlschlä gt	Ereignis
Automatisierte Generierung von Firmennamen	Der generierte Firmenname war erfolgreich	Das Ereignis wird generiert, wenn der automatisch generiert e Auftrag für den Geschäftsnamen erfolgreich abgeschlo ssen wurde	Ereignis
Automatisierte Generierung von Firmennamen	Fehler beim Generieren des Firmennamens	Das Ereignis wird generiert, wenn der automatisch generiert e Auftrag für den Geschäftsnamen fehlschlägt	Ereignis
Datenquelle ausführen	Datenquelle wurde erstellt	Das Ereignis wird generiert, wenn eine neue Datenquelle erstellt wird	Ereignis
Datenquelle ausführen	Datenquelle wurde aktualisiert	Das Ereignis wird generiert, wenn eine vorhandene Datenquelle aktualisi ert wird	Ereignis

Ereigniskategorie	Ereignisname	Beschreibung des Ereignisses	Ereignistyp
Datenquelle ausführen	Datenquellenlauf ausgelöst	Das Ereignis wird generiert, wenn ein Datenquellenlauf initiiert wird	Ereignis
Datenquellenlauf	Die Ausführung der Datenquelle war erfolgreich	Das Ereignis wird generiert, wenn eine Datenquellenausführung erfolgreich war	Ereignis
Datenquellenlauf	Die Ausführung der Datenquelle ist fehlgeschlagen	Das Ereignis wird generiert, wenn ein Datenquellenlauf fehlschlägt	Ereignis

Gehen Sie wie folgt vor, um Aufgaben in Ihrem Datenportal-Posteingang anzuzeigen:

1. Navigieren Sie mithilfe der DataZone Datenportal-URL zum Amazon-Datenportal und melden Sie sich mit Ihrem SSO oder Ihren AWS Anmeldeinformationen an. Wenn Sie ein DataZone Amazon-Administrator sind, können Sie die Datenportal-URL abrufen, indem Sie auf die DataZone Amazon-Konsole unter https://console.aws.amazon.com/datazone in dem AWS Konto zugreifen, in dem die DataZone Amazon-Domain erstellt wurde.
2. Um im Datenportal ein Pop-up mit den letzten Aufgaben anzuzeigen, wählen Sie das Glockensymbol neben der Suchleiste aus.
3. Wählen Sie Alle anzeigen aus, um alle Aufgaben anzuzeigen. Sie können die Ansicht ändern und alle Ereignisse anzeigen, indem Sie die Registerkarte Ereignisse auswählen.
4. Sie können die Suche nach dem Thema der Veranstaltung, dem Status „Aktiv“ oder „Inaktiv“ oder dem Zeitraum filtern.
5. Wählen Sie eine einzelne Aufgabe aus, um zu dem Ort zu navigieren, an dem Sie auf die Aufgabe antworten können.

Gehen Sie wie folgt vor, um Ereignisse in Ihrem Datenportal-Posteingang anzuzeigen:

1. Navigieren Sie mithilfe der DataZone Datenportal-URL zum Amazon-Datenportal und melden Sie sich mit Ihrem SSO oder Ihren AWS Anmeldeinformationen an. Wenn Sie ein DataZone Amazon-Administrator sind, können Sie die Datenportal-URL abrufen, indem Sie auf die DataZone Amazon-Konsole unter https://console.aws.amazon.com/datazone in dem AWS Konto zugreifen, in dem die DataZone Amazon-Root-Domain erstellt wurde.
2. Wählen Sie im Datenportal das Glockensymbol neben der Suchleiste aus, um das Pop-up für die letzten Ereignisse anzuzeigen.
3. Wählen Sie Alle anzeigen aus, um alle Ereignisse anzuzeigen. Sie können die Ansicht ändern und alle Aufgaben anzeigen, indem Sie die Registerkarte Aufgaben auswählen.
4. Filtern Sie die Suche nach dem Thema oder dem Zeitraum der Veranstaltung.
5. Wählen Sie ein einzelnes Ereignis aus, um zu dem Ort zu gelangen, an dem Sie Details zu diesem Ereignis anzeigen können.

Arbeiten mit Ereignissen über den EventBridge Amazon-Standardbus

Zusätzlich zum Senden von Nachrichten an Ihren speziellen Posteingang im Datenportal werden diese Nachrichten DataZone auch an Ihren EventBridge Amazon-Standard-Event-Bus in demselben AWS Konto gesendet, in dem Ihre DataZone Amazon-Root-Domain gehostet wird. Dies ermöglicht eine ereignisgesteuerte Automatisierung, z. B. die Abonnementabwicklung oder benutzerdefinierte Integrationen mit anderen Tools. Sie können Regeln erstellen, die eingehenden EventBridge Amazon-Ereignissen entsprechen, und diese zur Verarbeitung an EventBridge Amazon-Ziele senden. Eine einzelne Regel kann ein Ereignis an mehrere Ziele senden, die dann parallel ausgeführt werden können.

Hier ist ein Beispielereignis:

```
{
  "version": "0",
  "id": "bd3d6239-2877-f464-0572-b1d76760e085",
  "detail-type": "Subscription Request Created",
  "source": "aws.datazone",
  "account": "111111111111",
  "time": "2023-11-13T17:57:00Z",
  "region": "us-east-1",
  "resources": [],
```

```
  "detail": {
    "version": "655",
    "metadata": {
      "domain": "dzd_bc8e1ez8r2a6xz",
      "user": "44f864b8-50a1-70cc-736f-c1f763934ab7",
      "id": "5jbc0lie0sr99j",
      "version": "1",
      "typeName": "SubscriptionRequestEntityType",
      "owningProjectId": "6oy92hwk937pgn",
      "awsAccountId": "111111111111",
      "clientToken": "e781b7b5-78c5-4608-961e-3792a6c3ff0d"
    },
    "data": {
      "autoApproved": true,
      "requesterId": "44f864b8-50a1-70cc-736f-c1f763934ab7",
      "status": "PENDING",
      "subscribedListings": [
        {
          "id": "ayzstznnx4dxyf",
          "ownerProjectId": "5a3se66qm88947",
          "version": "12"
        }
      ],
      "subscribedPrincipals": [
        {
          "id": "6oy92hwk937pgn",
          "type": "PROJECT"
        }
      ]
    }
  }
}
```


Die vollständige Liste der von Amazon DataZone unterstützten Detailtypen umfasst:

- Abonnementanfrage wurde erstellt
- Abonnementanfrage akzeptiert
- Abonnementanfrage abgelehnt
- Abonnementanfrage wurde gelöscht
- Abonnementzuschuss beantragt

- Abonnementzuschuss abgeschlossen
- Die Abonnementgewährung ist fehlgeschlagen
- Widerruf der Abonnementgewährung angefordert
- Widerruf der Abonnementgewährung abgeschlossen
- Widerruf der Abonnementgewährung ist fehlgeschlagen
- Anlage wurde zum Inventar hinzugefügt
- Anlage wurde zum Katalog hinzugefügt
- Das Asset-Schema wurde geändert
- Änderung des Datenquellenstatus
- Datenquelle wurde erstellt
- Datenquelle wurde aktualisiert
- Datenquellenlauf ausgelöst
- Die Ausführung der Datenquelle war erfolgreich
- Die Ausführung der Datenquelle ist fehlgeschlagen
- Die Erstellung der Domäne war erfolgreich
- Die Domänenerstellung ist fehlgeschlagen
- Das Löschen der Domäne war erfolgreich
- Das Löschen der Domäne ist fehlgeschlagen
- Die Bereitstellung der Umgebung wurde gestartet
- Die Bereitstellung der Umgebung ist abgeschlossen
- Die Bereitstellung der Umgebung ist fehlgeschlagen
- Das Löschen der Umgebung wurde gestartet
- Das Löschen der Umgebung wurde abgeschlossen
- Das Löschen der Umgebung ist fehlgeschlagen
- Die Projekterstellung war erfolgreich
- Das Hinzufügen eines Projektmitglieds war erfolgreich
- Das Entfernen des Projektmitglieds war erfolgreich
- Die Änderung der Rolle des Projektmitglieds war erfolgreich
- Der Kunden-Workflow zur Bereitstellung der Umgebung wurde initiiert
- Die Generierung des Firmennamens war erfolgreich

- Die Generierung des Firmennamens ist fehlgeschlagen

Weitere Informationen finden Sie auf Amazon EventBridge.

Sicherheit bei Amazon DataZone

Cloud-Sicherheit AWS hat höchste Priorität. Als AWS Kunde profitieren Sie von Rechenzentren und Netzwerkarchitekturen, die darauf ausgelegt sind, die Anforderungen der sicherheitssensibelsten Unternehmen zu erfüllen.

Sicherheit ist eine gemeinsame AWS Verantwortung von Ihnen und Ihnen. Das Modell der geteilten Verantwortung beschreibt dies als Sicherheit der Cloud selbst und Sicherheit in der Cloud:

- Sicherheit der Cloud — AWS ist verantwortlich für den Schutz der Infrastruktur, auf der AWS Dienste in der ausgeführt AWS Cloud werden. AWS bietet Ihnen auch Dienste, die Sie sicher nutzen können. Externe Prüfer testen und verifizieren regelmäßig die Wirksamkeit unserer Sicherheitsmaßnahmen im Rahmen der AWS . Weitere Informationen zu den Compliance-Programmen, die für Amazon gelten DataZone, finden Sie unter AWS Services im Bereich nach Compliance-Programm AWS .
- Sicherheit in der Cloud — Ihre Verantwortung richtet sich nach dem AWS Service, den Sie nutzen. Sie sind auch für andere Faktoren verantwortlich, etwa für die Vertraulichkeit Ihrer Daten, für die Anforderungen Ihres Unternehmens und für die geltenden Gesetze und Vorschriften.

Diese Dokumentation hilft Ihnen zu verstehen, wie Sie das Modell der gemeinsamen Verantwortung bei der Nutzung von Amazon anwenden können DataZone. In den folgenden Themen erfahren Sie, wie Sie Amazon konfigurieren DataZone , um Ihre Sicherheits- und Compliance-Ziele zu erreichen. Sie erfahren auch, wie Sie andere AWS Dienste nutzen können, die Ihnen helfen, Ihre DataZone Amazon-Ressourcen zu überwachen und zu sichern.

Themen

- Konfiguration und Schwachstellenanalyse für Amazon DataZone

Datenschutz bei Amazon DataZone

Das AWS Modell der gilt für den Datenschutz bei Amazon DataZone. Wie in diesem Modell beschrieben, AWS ist verantwortlich für den Schutz der globalen Infrastruktur, auf der alle Systeme laufen AWS Cloud. Sie sind dafür verantwortlich, die Kontrolle über Ihre in dieser Infrastruktur gehosteten Inhalte zu behalten. Sie sind auch für die Sicherheitskonfiguration und die Verwaltungsaufgaben für die von Ihnen verwendeten AWS-Services verantwortlich. Weitere Informationen zum Datenschutz finden Sie unter Häufig gestellte Fragen zum Datenschutz. Informationen zum Datenschutz in Europa finden Sie im Blog-Beitrag AWS -Modell der geteilten Verantwortung und in der DSGVO im AWS -Sicherheitsblog.

Aus Datenschutzgründen empfehlen wir, dass Sie AWS-Konto Anmeldeinformationen schützen und einzelne Benutzer mit AWS IAM Identity Center oder AWS Identity and Access Management (IAM) einrichten. So erhält jeder Benutzer nur die Berechtigungen, die zum Durchführen seiner Aufgaben erforderlich sind. Außerdem empfehlen wir, die Daten mit folgenden Methoden schützen:

- Verwenden Sie für jedes Konto die Multi-Faktor-Authentifizierung (MFA).
- Verwenden Sie SSL/TLS, um mit Ressourcen zu kommunizieren. AWS Wir benötigen TLS 1.2 und empfehlen TLS 1.3.
- Richten Sie die API und die Protokollierung von Benutzeraktivitäten mit ein. AWS CloudTrail
- Verwenden Sie AWS Verschlüsselungslösungen zusammen mit allen darin enthaltenen Standardsicherheitskontrollen AWS-Services.
- Verwenden Sie erweiterte verwaltete Sicherheitsservices wie Amazon Macie, die dabei helfen, in Amazon S3 gespeicherte persönliche Daten zu erkennen und zu schützen.
- Wenn Sie für den Zugriff AWS über eine Befehlszeilenschnittstelle oder eine API FIPS 140-2-validierte kryptografische Module benötigen, verwenden Sie einen FIPS-Endpunkt. Weitere Informationen über verfügbare FIPS-Endpunkte finden Sie unter Federal Information Processing Standard (FIPS) 140-2.

Wir empfehlen dringend, in Freitextfeldern, z. B. im Feld Name, keine vertraulichen oder sensiblen Informationen wie die E-Mail-Adressen Ihrer Kunden einzugeben. Dies gilt auch, wenn Sie mit Amazon DataZone oder anderen zusammenarbeiten und die Konsole AWS CLI, API oder AWS SDKs AWS-Services verwenden. 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.

Datenverschlüsselung

Bei der Erteilung von Berechtigungen entscheiden Sie, wer welche Berechtigungen für welche DataZone Amazon-Ressourcen erhält. Sie aktivieren die spezifischen Aktionen, die daraufhin für die betreffenden Ressourcen erlaubt sein sollen. Aus diesem Grund sollten Sie nur Berechtigungen gewähren, die zum Ausführen einer Aufgabe erforderlich sind. Die Implementierung der geringstmöglichen Zugriffsrechte ist eine grundlegende Voraussetzung zum Reduzieren des Sicherheitsrisikos und der Auswirkungen, die aufgrund von Fehlern oder böswilligen Absichten entstehen könnten.

Verschlüsselung im Ruhezustand

Amazon DataZone verschlüsselt alle Ihre Daten standardmäßig mit einem AWS Key Management Service (AWS KMS) -Schlüssel, der Ihnen AWS gehört und für Sie verwaltet. Sie können die im DataZone Amazon-Katalog gespeicherten Daten auch mit Schlüsseln verschlüsseln, die Sie mit AWS KMS verwalten.

Wenn Sie eine Domain in Amazon erstellen DataZone, können Sie Verschlüsselungseinstellungen angeben, indem Sie unter Datenverschlüsselung das Kontrollkästchen neben Verschlüsselungseinstellungen anpassen (erweitert) aktivieren und einen KMS-Schlüssel angeben.

Verschlüsselung während der Übertragung

Amazon DataZone verwendet Transport Layer Security (TLS) und clientseitige Verschlüsselung für die Verschlüsselung bei der Übertragung. Die Kommunikation mit Amazon DataZone erfolgt immer über HTTPS, sodass Ihre Daten bei der Übertragung immer verschlüsselt werden.

Datenschutz für den Datenverkehr zwischen Netzwerken

Um Verbindungen zwischen Konten zu sichern, DataZone verwendet Amazon Service- und IAM-Rollen, um eine sichere Verbindung zu Kundenkonten herzustellen und Vorgänge im Namen des Kunden auszuführen.

Themen

- Datenverschlüsselung im Ruhezustand für Amazon DataZone

- Verwenden von Interface VPC-Endpunkten für Amazon DataZone

Datenverschlüsselung im Ruhezustand für Amazon DataZone

Die standardmäßige Verschlüsselung von Daten im Ruhezustand trägt dazu bei, den betrieblichen Aufwand und die Komplexität zu reduzieren, die mit dem Schutz vertraulicher Daten verbunden sind. Gleichzeitig können Sie damit sichere Anwendungen erstellen, die strenge Verschlüsselungsvorschriften und gesetzliche Auflagen erfüllen.

Amazon DataZone verwendet AWS eigene Standardschlüssel, um Ihre Daten im Ruhezustand automatisch zu verschlüsseln. Sie können die Verwendung AWS eigener Schlüssel nicht einsehen, verwalten oder überprüfen. Weitere Informationen finden Sie unter AWS Eigene Schlüssel.

Sie können diese Verschlüsselungsebene zwar nicht deaktivieren oder einen anderen Verschlüsselungstyp auswählen, aber Sie können eine zweite Verschlüsselungsebene über den vorhandenen AWS eigenen Verschlüsselungsschlüsseln hinzufügen, indem Sie bei der Erstellung Ihrer DataZone Amazon-Domains einen vom Kunden verwalteten Schlüssel auswählen. Amazon DataZone unterstützt die Verwendung symmetrischer, vom Kunden verwalteter Schlüssel, die Sie erstellen, besitzen und verwalten können, um der vorhandenen AWS eigenen Verschlüsselung eine zweite Verschlüsselungsebene hinzuzufügen. Da Sie die volle Kontrolle über diese Verschlüsselungsebene haben, können Sie darin die folgenden Aufgaben ausführen:

- Legen Sie wichtige Richtlinien fest und pflegen Sie sie
- Einrichtung und Pflege von IAM-Richtlinien und -Zuschüssen
- Aktivieren und deaktivieren Sie wichtige Richtlinien
- Rotieren Sie das kryptografische Schlüsselmaterial
- Tags hinzufügen
- Schlüsselaliase erstellen
- Planen Sie das Löschen von Schlüsseln ein

Weitere Informationen finden Sie unter Vom Kunden verwaltete Schlüssel.

> **Note**
>
> Amazon aktiviert DataZone automatisch die Verschlüsselung im Ruhezustand mithilfe AWS eigener Schlüssel, um Kundendaten kostenlos zu schützen.

AWS Für die Verwendung von vom Kunden verwalteten Schlüsseln fallen KMS-Gebühren an. Weitere Informationen zur Preisgestaltung finden Sie unter Preise für den AWS Key Management Service.

So DataZone verwendet Amazon Zuschüsse in AWS KMS

Amazon DataZone benötigt drei Zuschüsse, um Ihren vom Kunden verwalteten Schlüssel verwenden zu können. Wenn Sie eine DataZone Amazon-Domain erstellen, die mit einem vom Kunden verwalteten Schlüssel verschlüsselt ist, DataZone erstellt Amazon in Ihrem Namen Zuschüsse und Unterzuschüsse, indem es CreateGrantAnfragen an AWS KMS sendet. Zuschüsse in AWS KMS werden verwendet, um Amazon DataZone Zugriff auf einen KMS-Schlüssel in Ihrem Konto zu gewähren. Amazon gewährt DataZone die folgenden Zuschüsse, um Ihren vom Kunden verwalteten Schlüssel für die folgenden internen Operationen zu verwenden:

Ein Zuschuss für die Verschlüsselung Ihrer Daten im Ruhezustand für die folgenden Vorgänge:

- Senden Sie DescribeKeyAnfragen an AWS KMS, um zu überprüfen, ob die symmetrische, vom Kunden verwaltete KMS-Schlüssel-ID, die Sie bei der Erstellung einer DataZone Amazon-Domainsammlung eingegeben haben, gültig ist.
- Senden Sie GenerateDataKeyrequestsan AWS KMS, um Datenschlüssel zu generieren, die mit Ihrem vom Kunden verwalteten Schlüssel verschlüsselt sind.
- Senden Sie Entschlüsselungsanforderungen an AWS KMS, um die verschlüsselten Datenschlüssel zu entschlüsseln, sodass sie zur Verschlüsselung Ihrer Daten verwendet werden können.
- RetireGrantum den Zuschuss zurückzuziehen, wenn die Domain gelöscht wird.

Zwei Zuschüsse für die Suche und Entdeckung Ihrer Daten:

- Zuschuss 2:
  - DescribeKey
  - GenerateDataKey
  - Verschlüsseln, Entschlüsseln, ReEncrypt
  - CreateGrantum Zuschüsse für Kinder für AWS Dienste zu gewähren, die intern von genutzt werden. DataZone
  - RetireGrant
- Zuschuss 3:

- GenerateDataKey
- Decrypt
- RetireGrant

Sie können den Zugriff auf die Genehmigung jederzeit widerrufen oder den Zugriff des Services auf den vom Kunden verwalteten Schlüssel entfernen. Wenn Sie dies tun, kann Amazon auf DataZone keine der mit dem vom Kunden verwalteten Schlüssel verschlüsselten Daten zugreifen, was sich auf Vorgänge auswirkt, die von diesen Daten abhängig sind. Wenn Sie beispielsweise versuchen, Datenbestandsdetails abzurufen, auf die Amazon nicht zugreifen DataZone kann, gibt der Vorgang einen `AccessDeniedException` Fehler zurück.

Einen kundenverwalteten Schlüssel erstellen

Sie können mithilfe der AWS Management Console oder der AWS KMS-APIs einen symmetrischen, vom Kunden verwalteten Schlüssel erstellen.

Um einen symmetrischen, vom Kunden verwalteten Schlüssel zu erstellen, folgen Sie den Schritten unter Erstellen eines symmetrischen kundenverwalteten Schlüssels im AWS Key Management Service Developer Guide.

Schlüsselrichtlinie — Wichtige Richtlinien regeln den Zugriff auf Ihren vom Kunden verwalteten Schlüssel. Jeder vom Kunden verwaltete Schlüssel muss über genau eine Schlüsselrichtlinie verfügen, die aussagt, wer den Schlüssel wie verwenden kann. Wenn Sie Ihren vom Kunden verwalteten Schlüssel erstellen, können Sie eine Schlüsselrichtlinie angeben. Weitere Informationen finden Sie unter Verwaltung des Zugriffs auf vom Kunden verwaltete Schlüssel im AWS Key Management Service Developer Guide.

Um Ihren vom Kunden verwalteten Schlüssel mit Ihren DataZone Amazon-Ressourcen zu verwenden, müssen die folgenden API-Operationen in der Schlüsselrichtlinie zulässig sein:

- kms: CreateGrant — fügt einem vom Kunden verwalteten Schlüssel einen Zuschuss hinzu. Gewährt Kontrollzugriff auf einen bestimmten KMS-Schlüssel, der den Zugriff auf von Amazon DataZone benötigte Grant-Operationen ermöglicht. Weitere Informationen zur Verwendung von Grants finden Sie im AWS Key Management Service Developer Guide.
- kms: DescribeKey — stellt dem Kunden verwaltete Schlüsseldetails zur Verfügung, damit Amazon DataZone den Schlüssel validieren kann.
- kms: GenerateDataKey — gibt einen eindeutigen symmetrischen Datenschlüssel zur Verwendung außerhalb von AWS KMS zurück.

- kms:Decrypt — entschlüsselt Chiffretext, der mit einem KMS-Schlüssel verschlüsselt wurde.

Im Folgenden finden Sie Beispiele für Richtlinienerklärungen, die Sie für Amazon hinzufügen können DataZone:

```
"Statement" : [
    {
      "Sid" : "Allow access to principals authorized to manage Amazon DataZone",
      "Effect" : "Allow",
      "Principal" : {
        "AWS" : "arn:aws:iam::<account_id>:root"
      },
      "Action" : [
        "kms:DescribeKey",
        "kms:CreateGrant",
        "kms:GenerateDataKey",
        "kms:Decrypt"
      ],
      "Resource" : "arn:aws:kms:region:<account_id>:key/key_ID",
    }
  ]
```

> **Note**
>
> Die KMS-Richtlinie „Deny on the KMS“ wird nicht für Ressourcen angewendet, auf die über das DataZone Amazon-Datenportal zugegriffen wird.

Weitere Informationen zur Angabe von Berechtigungen in einer Richtlinie finden Sie im AWS Key Management Service Developer Guide.

Weitere Informationen zur Problembehandlung beim Schlüsselzugriff finden Sie im AWS Key Management Service Developer Guide.

Einen vom Kunden verwalteten Schlüssel für Amazon angeben DataZone

DataZone Amazon-Verschlüsselungskontext

Ein Verschlüsselungskontext ist ein optionaler Satz von Schlüssel-Wert-Paaren, die zusätzliche kontextbezogene Informationen zu den Daten enthalten.

AWS KMS verwendet den Verschlüsselungskontext als zusätzliche authentifizierte Daten, um die authentifizierte Verschlüsselung zu unterstützen. Wenn Sie einen Verschlüsselungskontext in eine Anforderung zur Datenverschlüsselung aufnehmen, bindet AWS KMS den Verschlüsselungskontext an die verschlüsselten Daten. Zur Entschlüsselung von Daten müssen Sie denselben Verschlüsselungskontext in der Anfrage übergeben.

Amazon DataZone verwendet den folgenden Verschlüsselungskontext:

```
"encryptionContextSubset": {
    "aws:datazone:domainId": "{root-domain-uuid}"
}
```

Verwendung des Verschlüsselungskontextes für die Überwachung — Wenn Sie einen symmetrischen, vom Kunden verwalteten Schlüssel zur Verschlüsselung von Amazon verwenden DataZone, können Sie den Verschlüsselungskontext auch in Prüfaufzeichnungen und Protokollen verwenden, um festzustellen, wie der vom Kunden verwaltete Schlüssel verwendet wird. Der Verschlüsselungskontext erscheint auch in Protokollen, die von Amazon CloudWatch Logs generiert wurden AWS CloudTrail .

Verwendung des Verschlüsselungskontextes zur Steuerung des Zugriffs auf Ihren vom Kunden verwalteten Schlüssel — Sie können den Verschlüsselungskontext in Schlüsselrichtlinien und IAM-Richtlinien als Bedingungen für die Steuerung des Zugriffs auf Ihren symmetrischen, vom Kunden verwalteten Schlüssel verwenden. Sie können Verschlüsselungskontext-Einschränkungen auch in einer Genehmigung verwenden.

Amazon DataZone verwendet bei Zuschüssen eine Einschränkung des Verschlüsselungskontextes, um den Zugriff auf den vom Kunden verwalteten Schlüssel in Ihrem Konto oder Ihrer Region zu kontrollieren. Eine Genehmigungseinschränkung erfordert, dass durch die Genehmigung ermöglichte Vorgänge den angegebenen Verschlüsselungskontext verwenden.

Im Folgenden finden Sie Beispiele für Schlüsselrichtlinienanweisungen zur Gewährung des Zugriffs auf einen vom Kunden verwalteten Schlüssel für einen bestimmten Verschlüsselungskontext. Die Bedingung in dieser Richtlinienanweisung setzt voraus, dass die Genehmigungen eine Einschränkung des Verschlüsselungskontextes haben, die den Verschlüsselungskontext spezifiziert.

```
{
    "Sid": "Enable DescribeKey",
    "Effect": "Allow",
    "Principal": {
        "AWS": "arn:aws:iam::111122223333:role/ExampleReadOnlyRole"
     },
     "Action": "kms:DescribeKey",
     "Resource": "*"
},{
    "Sid": "Enable Decrypt, GenerateDataKey",
     "Effect": "Allow",
     "Principal": {
        "AWS": "arn:aws:iam::111122223333:role/ExampleReadOnlyRole"
     },
     "Action": [
        "kms:Decrypt",
        "kms:GenerateDataKey"
     ],
     "Resource": "*",
     "Condition": {
        "StringEquals": {
            "kms:EncryptionContext:aws:datazone:domainId": "{root-domain-uuid}"
        }
    }
}
```

Überwachung Ihrer Verschlüsselungsschlüssel für Amazon DataZone

Wenn Sie einen AWS vom Kunden verwalteten KMS-Schlüssel mit Ihren DataZone Amazon-Ressourcen verwenden, können Sie AWS CloudTraildamit Anfragen verfolgen, die Amazon DataZone an AWS KMS sendet. Die folgenden Beispiele sind AWS CloudTrail Ereignisse für`CreateGrant`,`GenerateDataKey`, und `DescribeKey` zur Überwachung von KMS-Vorgängen`Decrypt`, die von Amazon aufgerufen wurden, DataZone um auf Daten zuzugreifen, die mit Ihrem vom Kunden verwalteten Schlüssel verschlüsselt wurden. Wenn Sie einen AWS

vom Kunden verwalteten KMS-Schlüssel zur Verschlüsselung Ihrer DataZone Amazon-Domain verwenden, DataZone sendet Amazon in Ihrem Namen eine `CreateGrant` Anfrage, um auf den KMS-Schlüssel in Ihrem AWS Konto zuzugreifen. Zuschüsse, die Amazon DataZone erstellt, sind spezifisch für die Ressource, die dem vom Kunden verwalteten AWS KMS-Schlüssel zugeordnet ist. Darüber hinaus DataZone verwendet Amazon den `RetireGrant` Vorgang, um einen Zuschuss zu entfernen, wenn Sie eine Domain löschen. Das folgende Beispielereignis zeichnet den Vorgang `CreateGrant` auf:

```
{
    "eventVersion": "1.08",
    "userIdentity": {
        "type": "AssumedRole",
        "principalId": "AROAIGDTESTANDEXAMPLE:Sampleuser01",
        "arn": "arn:aws:sts::111122223333:assumed-role/Admin/Sampleuser01",
        "accountId": "111122223333",
        "accessKeyId": "AKIAIOSFODNN7EXAMPLE3",
        "sessionContext": {
            "sessionIssuer": {
                "type": "Role",
                "principalId": "AROAIGDTESTANDEXAMPLE:Sampleuser01",
                "arn": "arn:aws:sts::111122223333:assumed-role/Admin/Sampleuser01",
                "accountId": "111122223333",
                "userName": "Admin"
            },
            "webIdFederationData": {},
            "attributes": {
                "mfaAuthenticated": "false",
                "creationDate": "2021-04-22T17:02:00Z"
            }
        },
        "invokedBy": "datazone.amazonaws.com"
    },
    "eventTime": "2021-04-22T17:07:02Z",
    "eventSource": "kms.amazonaws.com",
    "eventName": "CreateGrant",
    "awsRegion": "us-west-2",
    "sourceIPAddress": "172.12.34.56",
    "userAgent": "ExampleDesktop/1.0 (V1; OS)",
    "requestParameters": {
        "constraints": {
            "encryptionContextSubset": {
```

```
                "aws:datazone:domainId": "SAMPLE-root-domain-uuid"
            }
        },
        "keyId": "arn:aws:kms:us-
west-2:111122223333:key/1234abcd-12ab-34cd-56ef-123456SAMPLE",
        "operations": [
            "Decrypt",
            "GenerateDataKey",
            "RetireGrant",
            "DescribeKey"
        ],
        "granteePrincipal": "datazone.us-west-2.amazonaws.com"
    },
    "responseElements": {
        "grantId":
 "0ab0ac0d0b000f00ea00cc0a0e00fc00bce000c000f0000000c0bc0a0000aaafSAMPLE",
        "keyId": "arn:aws:kms:us-
west-2:111122223333:key/1234abcd-12ab-34cd-56ef-123456SAMPLE"
    },
    "requestID": "ff000af-00eb-00ce-0e00-ea000fb0fba0SAMPLE",
    "eventID": "ff000af-00eb-00ce-0e00-ea000fb0fba0SAMPLE",
    "readOnly": false,
    "resources": [
        {
            "accountId": "111122223333",
            "type": "AWS::KMS::Key",
            "ARN": "arn:aws:kms:us-
west-2:111122223333:key/1234abcd-12ab-34cd-56ef-123456SAMPLE"
        }
    ],
    "eventType": "AwsApiCall",
    "managementEvent": true,
    "eventCategory": "Management",
    "recipientAccountId": "111122223333"
}
```


Erstellen von Data Lake-Umgebungen mit verschlüsselten AWS Glue-Katalogen

In fortgeschrittenen Anwendungsfällen müssen Sie, wenn Sie mit einem verschlüsselten AWS Glue-Katalog arbeiten, Zugriff auf den DataZone Amazon-Service gewähren, um Ihren vom Kunden verwalteten KMS-Schlüssel verwenden zu können. Sie können dies tun, indem Sie Ihre benutzerdefinierte KMS-Richtlinie aktualisieren und dem Schlüssel ein Tag hinzufügen. Gehen

Sie wie folgt vor, um Zugriff auf den DataZone Amazon-Service für die Arbeit mit Daten in einem verschlüsselten AWS Glue-Katalog zu gewähren:

- Fügen Sie Ihrem benutzerdefinierten KMS-Schlüssel die folgende Richtlinie hinzu. Weitere Informationen finden Sie unter Changing a key policy (Ändern einer Schlüsselrichtlinie).

```
{
  "Sid": "Allow datazone environment roles to use the key",
  "Effect": "Allow",
  "Principal": {
    "AWS": "*"
  },
  "Action": [
    "kms:Decrypt",
    "kms:Describe*",
    "kms:Get*"
  ],
  "Resource": "*",
  "Condition": {
    "StringLike": {
      "aws:PrincipalArn": "arn:aws:iam::*:role/*datazone_usr*"
    }
  }
}
```

- Fügen Sie Ihrem benutzerdefinierten KMS-Schlüssel das folgende Tag hinzu. Weitere Informationen finden Sie unter Verwenden von Tags zur Steuerung des Zugriffs auf KMS-Schlüssel.

```
key: AmazonDataZoneEnvironment
value: all
```

Verwenden von Interface VPC-Endpunkten für Amazon DataZone

Wenn Sie Amazon Virtual Private Cloud (Amazon VPC) zum Hosten Ihrer AWS Ressourcen verwenden, können Sie eine Verbindung zwischen Ihrer Amazon VPC und Amazon herstellen.

DataZone Sie können diese Verbindung mit Amazon nutzen, DataZone ohne das öffentliche Internet zu überqueren.

Mit Amazon VPC können Sie AWS Ressourcen in einem benutzerdefinierten virtuellen Netzwerk starten. Mit einer VPC können Sie Netzwerkeinstellungen, wie IP-Adressbereich, Subnetze, Routing-Tabellen und Netzwerk-Gateways, steuern. Weitere Informationen zu VPCs finden Sie im Amazon-VPC-Benutzerhandbuch.

Um Ihre Amazon VPC mit Amazon zu verbinden DataZone, müssen Sie zunächst einen VPC-Schnittstellen-Endpunkt definieren, über den Sie Ihre VPC mit anderen Services verbinden können. AWS Der Endpunkt bietet eine zuverlässige, skalierbare Konnektivität, ohne dass ein Internet-Gateway, eine NAT-Instance (Network Address Translation) oder eine VPN-Verbindung erforderlich ist. Weitere Informationen und detaillierte Schritte zur Erstellung eines VPC-Endpoints finden Sie unter Interface VPC Endpoints (AWS PrivateLink) im Amazon VPC-Benutzerhandbuch.

> **Important**
>
> In VPC ist eine Endpunktrichtlinie eine ressourcenbasierte Richtlinie, die Sie an einen VPC-Endpunkt anhängen können, um zu steuern, welche AWS Principals den Endpunkt für den Zugriff auf einen Dienst verwenden können. AWS
> In der aktuellen Version von Amazon DataZone wird die Verwendung von Endpunktrichtlinien für den Aufbau und die Nutzung von Verbindungen zwischen Ihrer Amazon VPC und Amazon DataZone nicht unterstützt. Amazon DataZone Access Management basiert auf der RAM-Konfiguration und den IAM-Prinzipalrichtlinien, die auf Service-Ebene definiert sind.

Autorisierung bei Amazon DataZone

DataZoneDie Benutzeroberfläche von Amazon besteht aus einer internen Verwaltungskonsole AWS und einer externen Webanwendung (Datenportal).

Die Amazon DataZone Management Console kann von AWS Administratoren für top-level-resource APIs verwendet werden, einschließlich der Erstellung und Verwaltung von Domains, AWS Kontozuordnungen für diese Domains und Datenquellen, für die Sie die Zugriffsverwaltung an Amazon DataZone delegieren möchten. Sie können die Amazon DataZone Management Console verwenden, um alle IAM-Rollen und Konfigurationen zu verwalten, die erforderlich sind, um die Zugriffsverwaltungssteuerung für die explizit AWS konfigurierten Konten an den DataZone Amazon-Service zu delegieren. Das DataZone Amazon-Datenportal ist eine AWS Identity Center-Anwendung

von Erstanbietern für SSO-Benutzer. Wenn diese Option aktiviert ist, kann die Konsole auch von autorisierten IAM-Prinzipalen verwendet werden, um sich mit dem Datenportal zu verbinden, anstatt eine SSO-Identität zu verwenden.

DataZoneDas Datenportal von Amazon ist so konzipiert, dass es hauptsächlich von Benutzern mit AWS IAM Identity Center-Authentifizierung verwendet werden kann, um den Zugriff auf Daten zu verwalten und Aufgaben in den Bereichen Datenveröffentlichung, Erkennung, Abonnement und Analyse durchzuführen.

Autorisierung in der DataZone Amazon-Konsole

Das Autorisierungsmodell der DataZone Amazon-Konsole verwendet die IAM-Autorisierung. Die Konsole wird von Administratoren hauptsächlich für die Einrichtung verwendet. Amazon DataZone verwendet das Konzept eines AWS Domain-Administratorkontos und AWS Mitgliedskonten, und die Konsole wird von all diesen Konten aus verwendet, um Vertrauensbeziehungen aufzubauen und gleichzeitig die AWS Unternehmensgrenzen zu respektieren.

Autorisierung im DataZone Amazon-Portal

Das Autorisierungsmodell für das Amazon DataZone Data Portal ist eine hierarchische ACL mit statischen Rollenarchetypen (Profilen), zu denen Administratoren und Zuschauer gehören. Benutzer können beispielsweise ein Administrator- oder Benutzerprofil haben. Auf Domänenebene können sie als Domänenbenutzer die Bezeichnung Dateneigentümer haben. Auf Projektebene kann ein Benutzer Eigentümer oder Mitwirkender sein. Diese Profile können als einer von zwei Typen konfiguriert werden: Benutzer und Gruppen. Diese Profile werden dann mit Domänen und Projekten verknüpft, und der Status dieser Berechtigungen wird in einer Zuordnungstabelle gespeichert.

Im Rahmen dieses Autorisierungsmodells DataZone ermöglicht Amazon Benutzern die Verwaltung von Benutzer- und Gruppenberechtigungen. Benutzer verwalten die Projektmitgliedschaft, beantragen Mitgliedschaften für Projekte und genehmigen Mitgliedschaften. Benutzer veröffentlichen Daten, definieren Genehmigungsberechtigte für Datenabonnements, abonnieren Daten und genehmigen Abonnements.

Benutzer führen Datenanalysen in bestimmten Projekten durch, wenn ihr Datenportal-Client Anmeldeinformationen für IAM-Sitzungen anfordert, die Amazon auf der Grundlage des effektiven Benutzerprofils im jeweiligen Projektkontext DataZone generiert. Diese Sitzung hängt sowohl von den Benutzerberechtigungen als auch von den Ressourcen des jeweiligen Projekts ab. Benutzer wechseln dann zu Athena oder Redshift, um die relevanten Daten abzufragen, und die gesamte zugrunde liegende IAM-Arbeit wird vollständig abstrahiert.

DataZone Amazon-Profile und -Rollen

Sobald ein Benutzer authentifiziert ist, wird der authentifizierte Kontext einer Benutzerprofil-ID zugeordnet. Dieses Benutzerprofil kann mehrere, unterschiedliche Verknüpfungen haben (Projekteigentümer, Domänenadministrator usw.), die für die Autorisierung von Benutzern verwendet werden. Jede Assoziation (z. B. Projekteigentümer, Domainadministrator usw.) hat je nach Kontext Berechtigungen für bestimmte Aktivitäten. Beispielsweise kann ein Benutzer, der über eine Domain-Admin-Zuordnung verfügt, zusätzliche Domains erstellen, der Domain andere Domain-Administratoren zuweisen und Projektvorlagen innerhalb seiner Domain erstellen. Ein Projektinhaber kann Projektmitglieder für sein Projekt hinzufügen oder entfernen, er kann Veröffentlichungsvereinbarungen mit einer Domain abschließen und Inhalte in einer Domain veröffentlichen.

Steuern des Zugriffs auf DataZone Amazon-Ressourcen mithilfe von IAM

Sie benötigen AWS Identity and Access Management (IAM), um die folgenden sicherheitsrelevanten Aufgaben zu erledigen:

- Erstellen Sie Benutzer und Gruppen unter Ihrem. AWS-Konto
- Weisen Sie jedem Benutzer unter Ihrem eigene eindeutige Sicherheitsanmeldedaten zu AWS-Konto.
- Kontrollieren Sie die Berechtigungen der einzelnen Benutzer zur Ausführung von Aufgaben mit AWS Ressourcen.
- Erlauben Sie den Benutzern in einem anderen AWS-Konto Bereich, Ihre AWS Ressourcen gemeinsam zu nutzen.
- Erstellen Sie Rollen für Sie AWS-Konto und definieren Sie die Benutzer oder Dienste, die diese Rollen übernehmen können.
- Verwenden Sie bestehende Identitäten für Ihr Unternehmen, um Berechtigungen zur Ausführung von Aufgaben unter Verwendung von AWS Ressourcen zu erteilen

Weitere Informationen zu IAM finden Sie unter:

- AWS Identity and Access Management (IAM)
- Erste Schritte

- IAM Benutzerhandbuch

In den folgenden Abschnitten werden die Richtlinien und Berechtigungen beschrieben, die für die Einrichtung von Amazon DataZone und seiner Komponenten wie Domains (einschließlich der Domain), zugehörige Konten, Projekte und Datenquellen erforderlich sind. Weitere Informationen finden Sie unter DataZone Amazon-Terminologie und Konzepte.

Inhalt

AWS verwaltete Richtlinien für Amazon DataZone

Eine AWS verwaltete Richtlinie ist eine eigenständige Richtlinie, die von erstellt und verwaltet wird AWS. AWS Verwaltete Richtlinien sind so konzipiert, dass sie Berechtigungen für viele gängige Anwendungsfälle bereitstellen, sodass Sie damit beginnen können, Benutzern, Gruppen und Rollen Berechtigungen zuzuweisen.

Beachten Sie, dass AWS verwaltete Richtlinien für Ihre speziellen Anwendungsfälle möglicherweise keine Berechtigungen mit den geringsten Rechten gewähren, da sie allen AWS Kunden zur Verfügung stehen. Wir empfehlen Ihnen, die Berechtigungen weiter zu reduzieren, indem Sie kundenverwaltete Richtlinien definieren, die speziell auf Ihre Anwendungsfälle zugeschnitten sind.

Sie können die in AWS verwalteten Richtlinien definierten Berechtigungen nicht ändern. Wenn die in einer AWS verwalteten Richtlinie definierten Berechtigungen AWS aktualisiert werden, wirkt sich das Update auf alle Prinzidentitäten (Benutzer, Gruppen und Rollen) aus, denen die Richtlinie zugeordnet ist. AWS aktualisiert eine AWS verwaltete Richtlinie höchstwahrscheinlich, wenn eine neue Richtlinie eingeführt AWS-Service wird oder neue API-Operationen für bestehende Dienste verfügbar werden.

Weitere Informationen finden Sie unter Von AWS verwaltete Richtlinien im IAM-Benutzerhandbuch.

Inhalt

- AWS verwaltete Richtlinie: AmazonDataZoneCustomEnvironmentDeploymentPolicy
- AWS verwaltete Richtlinie: AmazonDataZoneEnvironmentRolePermissionsBoundary
- AWS verwaltete Richtlinie: AmazonDataZoneRedshiftGlueProvisioningPolicy
- AWS verwaltete Richtlinie: AmazonDataZoneGlueManageAccessRolePolicy
- AWS verwaltete Richtlinie: AmazonDataZoneRedshiftManageAccessRolePolicy
- Von AWS verwaltete Richtlinie: AmazonDataZoneCrossAccountAdmin
- AWS verwaltete Richtlinie: AmazonDataZoneDomainExecutionRolePolicy
- AWS verwaltete Richtlinie: AmazonDataZoneSageMakerProvisioning
- AWS verwaltete Richtlinie: AmazonDataZoneSageMakerAccess
- AWS verwaltete Richtlinie: AmazonDataZoneSageMakerEnvironmentRolePermissionsBoundary
- DataZone Aktualisierungen der AWS verwalteten Richtlinien durch Amazon

AWS verwaltete Richtlinie: AmazonDataZoneFullAccess

Sie können die `AmazonDataZoneFullAccess`-Richtlinie an Ihre IAM-Identitäten anfügen.

Diese Richtlinie bietet vollen Zugriff auf Amazon DataZone über die AWS Management Console.

Details zu Berechtigungen

Diese Richtlinie umfasst die folgenden Berechtigungen:

- `datazone`— gewährt Schulleitern vollen Zugriff auf Amazon DataZone über die AWS Management Console.
- `kms`— Ermöglicht es Prinzipalen, Aliase aufzulisten und Schlüssel zu beschreiben.
- `s3`— Ermöglicht Prinzipalen die Auswahl vorhandener oder die Erstellung neuer S3-Buckets zum Speichern von DataZone Amazon-Daten.
- `ram`— Ermöglicht Prinzipalen die gemeinsame Nutzung von DataZone Amazon-Domains. AWS-Konten
- `iam`— Ermöglicht es Prinzipalen, Rollen aufzulisten und weiterzugeben und Richtlinien abzurufen.
- `sso`— Ermöglicht Prinzipalen, die Regionen abzurufen, in denen diese Option aktiviert AWS IAM Identity Center ist.

```
{
```

```
  "Version": "2012-10-17",
  "Statement": [
    {
      "Sid": "AmazonDataZoneStatement",
      "Effect": "Allow",
      "Action": [
        "datazone:*"
      ],
      "Resource": [
        "*"
      ]
    },
    {
      "Sid": "ReadOnlyStatement",
      "Effect": "Allow",
      "Action": [
        "kms:DescribeKey",
        "kms:ListAliases",
        "iam:ListRoles",
        "sso:DescribeRegisteredRegions",
        "s3:ListAllMyBuckets",
        "redshift:DescribeClusters",
        "redshift-serverless:ListWorkgroups",
        "ec2:DescribeSecurityGroups",
        "ec2:DescribeSubnets",
        "ec2:DescribeVpcs",
        "secretsmanager:ListSecrets"
      ],
      "Resource": [
        "*"
      ]
    },
    {
      "Sid": "BucketReadOnlyStatement",
      "Effect": "Allow",
      "Action": [
        "s3:ListBucket",
        "s3:GetBucketLocation"
      ],
      "Resource": "arn:aws:s3:::*"
    },
    {
      "Sid": "CreateBucketStatement",
      "Effect": "Allow",
```

```
      "Action": "s3:CreateBucket",
      "Resource": "arn:aws:s3:::amazon-datazone*"
    },
    {
      "Sid": "RamCreateResourceStatement",
      "Effect": "Allow",
      "Action": [
        "ram:CreateResourceShare"
      ],
      "Resource": "*",
      "Condition": {
        "StringEqualsIfExists": {
          "ram:RequestedResourceType": "datazone:Domain"
        }
      }
    },
    {
      "Sid": "RamResourceStatement",
      "Effect": "Allow",
      "Action": [
        "ram:DeleteResourceShare",
        "ram:AssociateResourceShare",
        "ram:DisassociateResourceShare",
        "ram:RejectResourceShareInvitation"
      ],
      "Resource": "*",
      "Condition": {
        "StringLike": {
          "ram:ResourceShareName": [
            "DataZone*"
          ]
        }
      }
    },
    {
      "Sid": "RamResourceReadOnlyStatement",
      "Effect": "Allow",
      "Action": [
        "ram:GetResourceShares",
        "ram:GetResourceShareInvitations",
        "ram:GetResourceShareAssociations"
      ],
      "Resource": "*"
    },
```

```
    {
      "Sid": "IAMPassRoleStatement",
      "Effect": "Allow",
      "Action": "iam:PassRole",
      "Resource": [
        "arn:aws:iam::*:role/AmazonDataZone*",
        "arn:aws:iam::*:role/service-role/AmazonDataZone*"
      ],
      "Condition": {
        "StringEquals": {
          "iam:passedToService": "datazone.amazonaws.com"
        }
      }
    },
    {
      "Sid": "IAMGetPolicyStatement",
      "Effect": "Allow",
      "Action": "iam:GetPolicy",
      "Resource": [
        "arn:aws:iam::*:policy/service-role/AmazonDataZoneRedshiftAccessPolicy*"
      ]
    },
    {
      "Sid": "DataZoneTagOnCreate",
      "Effect": "Allow",
      "Action": [
        "secretsmanager:TagResource"
      ],
      "Resource": "arn:aws:secretsmanager:*:*:secret:AmazonDataZone-*",
      "Condition": {
        "ForAllValues:StringEquals": {
          "aws:TagKeys": [
            "AmazonDataZoneDomain"
          ]
        },
        "StringLike": {
          "aws:RequestTag/AmazonDataZoneDomain": "dzd_*",
          "aws:ResourceTag/AmazonDataZoneDomain": "dzd_*"
        },
        "Null": {
          "aws:TagKeys": "false"
        }
      }
    },
```

```
    {
      "Sid": "CreateSecretStatement",
      "Effect": "Allow",
      "Action": [
        "secretsmanager:CreateSecret"
      ],
      "Resource": "arn:aws:secretsmanager:*:*:secret:AmazonDataZone-*",
      "Condition": {
        "StringLike": {
          "aws:RequestTag/AmazonDataZoneDomain": "dzd_*"
        }
      }
    }
  ]
}
```

Politische Überlegungen und Einschränkungen

Es gibt bestimmte Funktionen, die die `AmazonDataZoneFullAccess` Richtlinie nicht abdeckt.

- Wenn Sie eine DataZone Amazon-Domain mit Ihrem eigenen AWS KMS Schlüssel erstellen, müssen Sie über die erforderlichen Berechtigungen verfügen, damit die Domainerstellung erfolgreich ist und`kms:GenerateDataKey`, `kms:Decrypt` damit dieser Schlüssel andere DataZone Amazon-APIs wie `listDataSources` und `createDataSource` aufrufen kann. `kms:CreateGrant` Außerdem müssen Sie über die Berechtigungen für,, und verfügen `kms:CreateGrant` `kms:Decrypt`und`kms:GenerateDataKey`, die `kms:DescribeKey` in der Ressourcenrichtlinie dieses Schlüssels enthalten sind.

  Wenn Sie den standardmäßigen, diensteigenen KMS-Schlüssel verwenden, ist dies nicht erforderlich.

  Weitere Informationen finden Sie unter AWS Key Management Service.
- Wenn Sie die Funktionen zum Erstellen und Aktualisieren von Rollen in der DataZone Amazon-Konsole verwenden möchten, benötigen Sie Administratorrechte oder die erforderlichen IAM-Berechtigungen, um IAM-Rollen zu erstellen und Richtlinien zu erstellen/aktualisieren. Zu den erforderlichen Berechtigungen gehören`iam:CreateRole`,, `iam:CreatePolicy`iam:CreatePolicyVersion, `iam:DeletePolicyVersion` und Berechtigungen. `iam:AttachRolePolicy`
- Wenn Sie bei Amazon eine neue Domain DataZone mit aktivierter AWS IAM Identity Center Benutzeranmeldung erstellen oder wenn Sie sie für eine bestehende

Domain bei Amazon aktivieren DataZone, benötigen Sie folgende Berechtigungen: `sso:CreateManagedApplicationInstancesso:DeleteManagedApplicationInstance`, und`sso:PutApplicationAssignmentConfiguration`.

- Um eine AWS Kontozuordnungsanfrage bei Amazon annehmen zu können DataZone, benötigen Sie die `ram:AcceptResourceShareInvitation` entsprechende Genehmigung.

AWS verwaltete Richtlinie: AmazonDataZoneFullUserAccess

Diese Richtlinie gewährt vollen Zugriff auf Amazon DataZone, erlaubt jedoch nicht die Verwaltung von Domains, Benutzern oder zugehörigen Konten.

Details zu Berechtigungen

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Sid": "AmazonDataZoneUserOperations",
      "Effect": "Allow",
      "Action": [
        "datazone:GetDomain",
        "datazone:CreateFormType",
        "datazone:GetFormType",
        "datazone:GetIamPortalLoginUrl",
        "datazone:SearchUserProfiles",
        "datazone:SearchGroupProfiles",
        "datazone:GetUserProfile",
        "datazone:GetGroupProfile",
        "datazone:ListGroupsForUser",
        "datazone:DeleteFormType",
        "datazone:CreateAssetType",
        "datazone:GetAssetType",
        "datazone:DeleteAssetType",
        "datazone:CreateGlossary",
        "datazone:GetGlossary",
        "datazone:DeleteGlossary",
        "datazone:UpdateGlossary",
        "datazone:CreateGlossaryTerm",
        "datazone:GetGlossaryTerm",
        "datazone:DeleteGlossaryTerm",
        "datazone:UpdateGlossaryTerm",
```

```
        "datazone:CreateAsset",
        "datazone:GetAsset",
        "datazone:DeleteAsset",
        "datazone:CreateAssetRevision",
        "datazone:ListAssetRevisions",
        "datazone:AcceptPredictions",
        "datazone:RejectPredictions",
        "datazone:Search",
        "datazone:SearchTypes",
        "datazone:CreateListingChangeSet",
        "datazone:DeleteListing",
        "datazone:SearchListings",
        "datazone:GetListing",
        "datazone:CreateDataSource",
        "datazone:GetDataSource",
        "datazone:DeleteDataSource",
        "datazone:UpdateDataSource",
        "datazone:ListDataSources",
        "datazone:StartDataSourceRun",
        "datazone:GetDataSourceRun",
        "datazone:ListDataSourceRuns",
        "datazone:ListDataSourceRunActivities",
        "datazone:ListEnvironmentBlueprintConfigurations",
        "datazone:CreateEnvironmentBlueprint",
        "datazone:GetEnvironmentBlueprint",
        "datazone:DeleteEnvironmentBlueprint",
        "datazone:UpdateEnvironmentBlueprint",
        "datazone:ListEnvironmentBlueprints",
        "datazone:CreateProject",
        "datazone:UpdateProject",
        "datazone:GetProject",
        "datazone:DeleteProject",
        "datazone:ListProjects",
        "datazone:CreateProjectMembership",
        "datazone:DeleteProjectMembership",
        "datazone:ListProjectMemberships",
        "datazone:CreateEnvironmentProfile",
        "datazone:GetEnvironmentProfile",
        "datazone:UpdateEnvironmentProfile",
        "datazone:DeleteEnvironmentProfile",
        "datazone:ListEnvironmentProfiles",
        "datazone:CreateEnvironment",
        "datazone:GetEnvironment",
        "datazone:DeleteEnvironment",
```

```
        "datazone:UpdateEnvironment",
        "datazone:UpdateEnvironmentDeploymentStatus",
        "datazone:ListEnvironments",
        "datazone:ListAccountEnvironments",
        "datazone:GetEnvironmentActionLink",
        "datazone:GetEnvironmentCredentials",
        "datazone:GetSubscriptionTarget",
        "datazone:DeleteSubscriptionTarget",
        "datazone:ListSubscriptionTargets",
        "datazone:CreateSubscriptionRequest",
        "datazone:AcceptSubscriptionRequest",
        "datazone:UpdateSubscriptionRequest",
        "datazone:ListWarehouseMetadata",
        "datazone:RejectSubscriptionRequest",
        "datazone:GetSubscriptionRequestDetails",
        "datazone:ListSubscriptionRequests",
        "datazone:DeleteSubscriptionRequest",
        "datazone:GetSubscription",
        "datazone:CancelSubscription",
        "datazone:GetSubscriptionEligibility",
        "datazone:ListSubscriptions",
        "datazone:RevokeSubscription",
        "datazone:CreateSubscriptionGrant",
        "datazone:DeleteSubscriptionGrant",
        "datazone:GetSubscriptionGrant",
        "datazone:ListSubscriptionGrants",
        "datazone:UpdateSubscriptionGrantStatus",
        "datazone:ListNotifications",
        "datazone:StartMetadataGenerationRun",
        "datazone:GetMetadataGenerationRun",
        "datazone:CancelMetadataGenerationRun",
        "datazone:ListMetadataGenerationRuns"
      ],
      "Resource": "*"
    },
    {
      "Sid": "RAMResourceShareOperations",
      "Effect": "Allow",
      "Action": "ram:GetResourceShareAssociations",
      "Resource": "*"
    }
  ]
}
```

AWS verwaltete Richtlinie: AmazonDataZoneCustomEnvironmentDeploymentPolicy

Sie können diese Richtlinie verwenden, um die Konfiguration von Umgebungen zu aktualisieren, die mit benutzerdefinierten Blueprints erstellt wurden. Diese Richtlinie kann auch verwendet werden, um DataZone Amazon-Abonnementziele und Datenquellen zu erstellen.

Details zu Berechtigungen

```
{
 "Version": "2012-10-17",
 "Statement": [
  {
   "Sid": "AmazonDataZoneCustomEnvironment",
   "Effect": "Allow",
   "Action": [
    "datazone:ListAssociatedAccounts",
    "datazone:GetAccountAssociation",
    "datazone:GetEnvironment",
    "datazone:GetEnvironmentProfile",
    "datazone:GetEnvironmentBlueprint",
    "datazone:GetProject",
    "datazone:UpdateEnvironmentConfiguration",
    "datazone:UpdateEnvironmentDeploymentStatus",
    "datazone:CreateSubscriptionTarget",
    "datazone:CreateDataSource"
   ],
   "Resource": "*"
  }
 ]
}
```

AWS verwaltete Richtlinie: AmazonDataZoneEnvironmentRolePermissionsBoundary

> **Note**
>
> Bei dieser Richtlinie handelt es sich um eine Berechtigungsgrenze. Eine Berechtigungsgrenze legt die maximalen Berechtigungen fest, die eine identitätsbasierte Richtlinie einer IAM-Entität gewähren kann. Sie sollten die Richtlinien für die Begrenzung

von DataZone Berechtigungen von Amazon nicht eigenständig verwenden und anhängen. Grenzrichtlinien für DataZone Amazon-Berechtigungen sollten nur an von Amazon DataZone verwaltete Rollen angehängt werden. Weitere Informationen zu Berechtigungsgrenzen finden Sie unter Berechtigungsgrenzen für IAM-Entitäten im IAM-Benutzerhandbuch.

Wenn Sie eine Umgebung über das DataZone Amazon-Datenportal erstellen, DataZone wendet Amazon diese Berechtigungsgrenze auf die IAM-Rollen an, die bei der Umgebungserstellung erstellt werden. Die Berechtigungsgrenze begrenzt den Umfang der Rollen, die Amazon DataZone erstellt, und aller Rollen, die Sie hinzufügen.

Amazon DataZone verwendet die `AmazonDataZoneEnvironmentRolePermissionsBoundary` verwaltete Richtlinie, um den bereitgestellten IAM-Prinzipal einzuschränken, an den sie angehängt ist. Die Principals könnten die Form der Benutzerrollen annehmen, die Amazon im Namen interaktiver Unternehmensbenutzer oder Analysedienste (zum Beispiel) übernehmen DataZone kann AWS Glue, und dann Aktionen zur Verarbeitung von Daten durchführen, z. B. das Lesen und Schreiben von Amazon S3 oder das Ausführen von Daten. AWS-Glue-Crawler

Die `AmazonDataZoneEnvironmentRolePermissionsBoundary` Richtlinie gewährt Amazon Lese- und Schreibzugriff DataZone auf Dienste wie AWS Glue Amazon S3 AWS Lake Formation, Amazon Redshift und Amazon Athena. Die Richtlinie gewährt auch Lese- und Schreibberechtigungen für einige Infrastrukturressourcen, die für die Nutzung dieser Dienste erforderlich sind, z. B. Netzwerkschnittstellen und AWS KMS Schlüssel.

Amazon DataZone wendet die `AmazonDataZoneEnvironmentRolePermissionsBoundary` AWS verwaltete Richtlinie als Berechtigungsgrenze für alle Rollen in der DataZone Amazon-Umgebung (Eigentümer und Mitwirkender) an. Diese Berechtigungsgrenze schränkt diese Rollen so ein, dass sie nur Zugriff auf die erforderlichen Ressourcen und Aktionen gewähren, die für eine Umgebung erforderlich sind.

Die Grenze umfasst die folgenden JSON-Anweisungen:

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

```
        "ec2:CreateTags",
        "ec2:DeleteTags"
      ],
      "Resource": [
        "arn:aws:ec2:*:*:network-interface/*"
      ],
      "Condition": {
        "ForAllValues:StringEquals": {
          "aws:TagKeys": [
            "aws-glue-service-resource"
          ]
        }
      }
    },
    {
      "Sid": "GlueOperations",
      "Effect": "Allow",
      "Action": [
        "glue:*DataQuality*",
        "glue:BatchCreatePartition",
        "glue:BatchDeleteConnection",
        "glue:BatchDeletePartition",
        "glue:BatchDeleteTable",
        "glue:BatchDeleteTableVersion",
        "glue:BatchGetJobs",
        "glue:BatchGetWorkflows",
        "glue:BatchStopJobRun",
        "glue:BatchUpdatePartition",
        "glue:CreateBlueprint",
        "glue:CreateConnection",
        "glue:CreateCrawler",
        "glue:CreateDatabase",
        "glue:CreateJob",
        "glue:CreatePartition",
        "glue:CreatePartitionIndex",
        "glue:CreateTable",
        "glue:CreateWorkflow",
        "glue:DeleteBlueprint",
        "glue:DeleteColumnStatisticsForPartition",
        "glue:DeleteColumnStatisticsForTable",
        "glue:DeleteConnection",
        "glue:DeleteCrawler",
        "glue:DeleteJob",
        "glue:DeletePartition",
```

```
        "glue:DeletePartitionIndex",
        "glue:DeleteTable",
        "glue:DeleteTableVersion",
        "glue:DeleteWorkflow",
        "glue:GetColumnStatisticsForPartition",
        "glue:GetColumnStatisticsForTable",
        "glue:GetConnection",
        "glue:GetDatabase",
        "glue:GetDatabases",
        "glue:GetTable",
        "glue:GetTables",
        "glue:GetPartition",
        "glue:GetPartitions",
        "glue:ListSchemas",
        "glue:ListJobs",
        "glue:NotifyEvent",
        "glue:PutWorkflowRunProperties",
        "glue:ResetJobBookmark",
        "glue:ResumeWorkflowRun",
        "glue:SearchTables",
        "glue:StartBlueprintRun",
        "glue:StartCrawler",
        "glue:StartCrawlerSchedule",
        "glue:StartJobRun",
        "glue:StartWorkflowRun",
        "glue:StopCrawler",
        "glue:StopCrawlerSchedule",
        "glue:StopWorkflowRun",
        "glue:UpdateBlueprint",
        "glue:UpdateColumnStatisticsForPartition",
        "glue:UpdateColumnStatisticsForTable",
        "glue:UpdateConnection",
        "glue:UpdateCrawler",
        "glue:UpdateCrawlerSchedule",
        "glue:UpdateDatabase",
        "glue:UpdateJob",
        "glue:UpdatePartition",
        "glue:UpdateTable",
        "glue:UpdateWorkflow"
      ],
      "Resource": "*",
      "Condition": {
        "Null": {
          "aws:ResourceTag/AmazonDataZoneEnvironment": "false"
```

```
        }
      }
    },
    {
      "Sid": "PassRole",
      "Effect": "Allow",
      "Action": [
        "iam:PassRole"
      ],
      "Resource": [
        "arn:aws:iam::*:role/datazone*"
      ],
      "Condition": {
        "StringEquals": {
          "iam:PassedToService": "glue.amazonaws.com"
        }
      }
    },
    {
      "Sid": "SameAccountKmsOperations",
      "Effect": "Allow",
      "Action": [
        "kms:DescribeKey",
        "kms:Decrypt",
        "kms:ListKeys"
      ],
      "Resource": "*",
      "Condition": {
        "StringNotEquals": {
          "aws:ResourceAccount": "${aws:PrincipalAccount}"
        }
      }
    },
    {
      "Sid": "KmsOperationsWithResourceTag",
      "Effect": "Allow",
      "Action": [
        "kms:DescribeKey",
        "kms:Decrypt",
        "kms:ListKeys",
        "kms:Encrypt",
        "kms:GenerateDataKey",
        "kms:Verify",
        "kms:Sign"
```

```
      ],
      "Resource": "*",
      "Condition": {
        "Null": {
          "aws:ResourceTag/AmazonDataZoneEnvironment": "false"
        }
      }
    },
    {
      "Sid": "AnalyticsOperations",
      "Effect": "Allow",
      "Action": [
        "datazone:*",
        "sqlworkbench:*"
      ],
      "Resource": "*"
    },
    {
      "Sid": "QueryOperations",
      "Effect": "Allow",
      "Action": [
        "athena:BatchGetNamedQuery",
        "athena:BatchGetPreparedStatement",
        "athena:BatchGetQueryExecution",
        "athena:CreateNamedQuery",
        "athena:CreateNotebook",
        "athena:CreatePreparedStatement",
        "athena:CreatePresignedNotebookUrl",
        "athena:DeleteNamedQuery",
        "athena:DeleteNotebook",
        "athena:DeletePreparedStatement",
        "athena:ExportNotebook",
        "athena:GetDatabase",
        "athena:GetDataCatalog",
        "athena:GetNamedQuery",
        "athena:GetPreparedStatement",
        "athena:GetQueryExecution",
        "athena:GetQueryResults",
        "athena:GetQueryRuntimeStatistics",
        "athena:GetTableMetadata",
        "athena:GetWorkGroup",
        "athena:ImportNotebook",
        "athena:ListDatabases",
        "athena:ListDataCatalogs",
```

```
        "athena:ListEngineVersions",
        "athena:ListNamedQueries",
        "athena:ListPreparedStatements",
        "athena:ListQueryExecutions",
        "athena:ListTableMetadata",
        "athena:ListTagsForResource",
        "athena:ListWorkGroups",
        "athena:StartCalculationExecution",
        "athena:StartQueryExecution",
        "athena:StartSession",
        "athena:StopCalculationExecution",
        "athena:StopQueryExecution",
        "athena:TerminateSession",
        "athena:UpdateNamedQuery",
        "athena:UpdateNotebook",
        "athena:UpdateNotebookMetadata",
        "athena:UpdatePreparedStatement",
        "ec2:CreateNetworkInterface",
        "ec2:DeleteNetworkInterface",
        "ec2:Describe*",
        "glue:BatchCreatePartition",
        "glue:BatchDeletePartition",
        "glue:BatchDeleteTable",
        "glue:BatchDeleteTableVersion",
        "glue:BatchGetJobs",
        "glue:BatchGetPartition",
        "glue:BatchGetWorkflows",
        "glue:BatchUpdatePartition",
        "glue:CreateBlueprint",
        "glue:CreateConnection",
        "glue:CreateCrawler",
        "glue:CreateDatabase",
        "glue:CreateJob",
        "glue:CreatePartition",
        "glue:CreatePartitionIndex",
        "glue:CreateTable",
        "glue:CreateWorkflow",
        "glue:DeleteColumnStatisticsForPartition",
        "glue:DeleteColumnStatisticsForTable",
        "glue:DeletePartition",
        "glue:DeletePartitionIndex",
        "glue:DeleteTable",
        "glue:DeleteTableVersion",
        "glue:GetColumnStatisticsForPartition",
```

```
        "glue:GetColumnStatisticsForTable",
        "glue:GetConnection",
        "glue:GetDatabase",
        "glue:GetDatabases",
        "glue:GetTable",
        "glue:GetTables",
        "glue:GetPartition",
        "glue:GetPartitions",
        "glue:ListSchemas",
        "glue:ListJobs",
        "glue:NotifyEvent",
        "glue:SearchTables",
        "glue:UpdateColumnStatisticsForPartition",
        "glue:UpdateColumnStatisticsForTable",
        "glue:UpdateDatabase",
        "glue:UpdatePartition",
        "glue:UpdateTable",
        "iam:GetRole",
        "iam:GetRolePolicy",
        "iam:ListGroups",
        "iam:ListRolePolicies",
        "iam:ListRoles",
        "iam:ListUsers",
        "logs:DescribeLogGroups",
        "logs:DescribeLogStreams",
        "logs:DescribeMetricFilters",
        "logs:DescribeQueries",
        "logs:DescribeQueryDefinitions",
        "logs:DescribeMetricFilters",
        "logs:StartQuery",
        "logs:StopQuery",
        "logs:GetLogEvents",
        "logs:GetLogGroupFields",
        "logs:GetQueryResults",
        "logs:GetLogRecord",
        "logs:PutLogEvents",
        "logs:CreateLogStream",
        "logs:FilterLogEvents",
        "lakeformation:GetDataAccess",
        "lakeformation:GetDataLakeSettings",
        "lakeformation:GetResourceLFTags",
        "lakeformation:ListPermissions",
        "redshift-data:ListTables",
        "redshift-data:DescribeTable",
```

```
        "redshift-data:ListSchemas",
        "redshift-data:ListDatabases",
        "redshift-data:ExecuteStatement",
        "redshift-data:GetStatementResult",
        "redshift-data:DescribeStatement",
        "redshift:CreateClusterUser",
        "redshift:DescribeClusters",
        "redshift:DescribeDataShares",
        "redshift:GetClusterCredentials",
        "redshift:GetClusterCredentialsWithIAM",
        "redshift:JoinGroup",
        "redshift-serverless:ListNamespaces",
        "redshift-serverless:ListWorkgroups",
        "redshift-serverless:GetNamespace",
        "redshift-serverless:GetWorkgroup",
        "redshift-serverless:GetCredentials",
        "secretsmanager:ListSecrets",
        "tag:GetResources"
      ],
      "Resource": "*"
    },
    {
      "Sid": "QueryOperationsWithResourceTag",
      "Effect": "Allow",
      "Action": [
        "athena:GetQueryResultsStream"
      ],
      "Resource": "*",
      "Condition": {
        "Null": {
          "aws:ResourceTag/AmazonDataZoneEnvironment": "false"
        }
      }
    },
    {
      "Sid": "SecretsManagerOperationsWithTagKeys",
      "Effect": "Allow",
      "Action": [
        "secretsmanager:CreateSecret",
        "secretsmanager:TagResource"
      ],
      "Resource": "arn:aws:secretsmanager:*:*:secret:AmazonDataZone-*",
      "Condition": {
        "StringLike": {
```

```
          "aws:ResourceTag/AmazonDataZoneDomain": "*",
          "aws:ResourceTag/AmazonDataZoneProject": "*"
        },
        "Null": {
          "aws:TagKeys": "false"
        },
        "ForAllValues:StringEquals": {
          "aws:TagKeys": [
            "AmazonDataZoneDomain",
            "AmazonDataZoneProject"
          ]
        }
      }
    },
    {
      "Sid": "DataZoneS3Buckets",
      "Effect": "Allow",
      "Action": [
        "s3:AbortMultipartUpload",
        "s3:DeleteObject",
        "s3:DeleteObjectVersion",
        "s3:GetObject",
        "s3:PutObject",
        "s3:PutObjectRetention",
        "s3:ReplicateObject",
        "s3:RestoreObject"
      ],
      "Resource": [
        "arn:aws:s3:::*/datazone/*"
      ]
    },
    {
      "Sid": "DataZoneS3BucketLocation",
      "Effect": "Allow",
      "Action": [
        "s3:GetBucketLocation"
      ],
      "Resource": "*"
    },
    {
      "Sid": "ListDataZoneS3Bucket",
      "Effect": "Allow",
      "Action": [
        "s3:ListBucket"
```

```
      ],
      "Resource": [
        "*"
      ],
      "Condition": {
        "StringLike": {
          "s3:prefix": [
            "*/datazone/*",
            "datazone/*"
          ]
        }
      }
    },
    {
      "Sid": "NotDeniedOperations",
      "Effect": "Deny",
      "NotAction": [
        "datazone:*",
        "sqlworkbench:*",
        "athena:BatchGetNamedQuery",
        "athena:BatchGetPreparedStatement",
        "athena:BatchGetQueryExecution",
        "athena:CreateNamedQuery",
        "athena:CreateNotebook",
        "athena:CreatePreparedStatement",
        "athena:CreatePresignedNotebookUrl",
        "athena:DeleteNamedQuery",
        "athena:DeleteNotebook",
        "athena:DeletePreparedStatement",
        "athena:ExportNotebook",
        "athena:GetDatabase",
        "athena:GetDataCatalog",
        "athena:GetNamedQuery",
        "athena:GetPreparedStatement",
        "athena:GetQueryExecution",
        "athena:GetQueryResults",
        "athena:GetQueryResultsStream",
        "athena:GetQueryRuntimeStatistics",
        "athena:GetTableMetadata",
        "athena:GetWorkGroup",
        "athena:ImportNotebook",
        "athena:ListDatabases",
        "athena:ListDataCatalogs",
        "athena:ListEngineVersions",
```

```
        "athena:ListNamedQueries",
        "athena:ListPreparedStatements",
        "athena:ListQueryExecutions",
        "athena:ListTableMetadata",
        "athena:ListTagsForResource",
        "athena:ListWorkGroups",
        "athena:StartCalculationExecution",
        "athena:StartQueryExecution",
        "athena:StartSession",
        "athena:StopCalculationExecution",
        "athena:StopQueryExecution",
        "athena:TerminateSession",
        "athena:UpdateNamedQuery",
        "athena:UpdateNotebook",
        "athena:UpdateNotebookMetadata",
        "athena:UpdatePreparedStatement",
        "ec2:CreateNetworkInterface",
        "ec2:CreateTags",
        "ec2:DeleteNetworkInterface",
        "ec2:DeleteTags",
        "ec2:Describe*",
        "glue:*DataQuality*",
        "glue:BatchCreatePartition",
        "glue:BatchDeleteConnection",
        "glue:BatchDeletePartition",
        "glue:BatchDeleteTable",
        "glue:BatchDeleteTableVersion",
        "glue:BatchGetJobs",
        "glue:BatchGetPartition",
        "glue:BatchGetWorkflows",
        "glue:BatchStopJobRun",
        "glue:BatchUpdatePartition",
        "glue:CreateBlueprint",
        "glue:CreateConnection",
        "glue:CreateCrawler",
        "glue:CreateDatabase",
        "glue:CreateJob",
        "glue:CreatePartition",
        "glue:CreatePartitionIndex",
        "glue:CreateTable",
        "glue:CreateWorkflow",
        "glue:DeleteBlueprint",
        "glue:DeleteColumnStatisticsForPartition",
        "glue:DeleteColumnStatisticsForTable",
```

```
        "glue:DeleteConnection",
        "glue:DeleteCrawler",
        "glue:DeleteJob",
        "glue:DeletePartition",
        "glue:DeletePartitionIndex",
        "glue:DeleteTable",
        "glue:DeleteTableVersion",
        "glue:DeleteWorkflow",
        "glue:GetColumnStatisticsForPartition",
        "glue:GetColumnStatisticsForTable",
        "glue:GetConnection",
        "glue:GetDatabase",
        "glue:GetDatabases",
        "glue:GetTable",
        "glue:GetTables",
        "glue:GetPartition",
        "glue:GetPartitions",
        "glue:ListSchemas",
        "glue:ListJobs",
        "glue:NotifyEvent",
        "glue:PutWorkflowRunProperties",
        "glue:ResetJobBookmark",
        "glue:ResumeWorkflowRun",
        "glue:SearchTables",
        "glue:StartBlueprintRun",
        "glue:StartCrawler",
        "glue:StartCrawlerSchedule",
        "glue:StartJobRun",
        "glue:StartWorkflowRun",
        "glue:StopCrawler",
        "glue:StopCrawlerSchedule",
        "glue:StopWorkflowRun",
        "glue:UpdateBlueprint",
        "glue:UpdateColumnStatisticsForPartition",
        "glue:UpdateColumnStatisticsForTable",
        "glue:UpdateConnection",
        "glue:UpdateCrawler",
        "glue:UpdateCrawlerSchedule",
        "glue:UpdateDatabase",
        "glue:UpdateJob",
        "glue:UpdatePartition",
        "glue:UpdateTable",
        "glue:UpdateWorkflow",
        "iam:GetRole",
```

```
        "iam:GetRolePolicy",
        "iam:List*",
        "iam:PassRole",
        "kms:DescribeKey",
        "kms:Decrypt",
        "kms:Encrypt",
        "kms:GenerateDataKey",
        "kms:ListKeys",
        "kms:Verify",
        "kms:Sign",
        "logs:DescribeLogGroups",
        "logs:DescribeLogStreams",
        "logs:DescribeMetricFilters",
        "logs:DescribeQueries",
        "logs:DescribeQueryDefinitions",
        "logs:StartQuery",
        "logs:StopQuery",
        "logs:GetLogEvents",
        "logs:GetLogGroupFields",
        "logs:GetQueryResults",
        "logs:GetLogRecord",
        "logs:PutLogEvents",
        "logs:CreateLogStream",
        "logs:FilterLogEvents",
        "lakeformation:GetDataAccess",
        "lakeformation:GetDataLakeSettings",
        "lakeformation:GetResourceLFTags",
        "lakeformation:ListPermissions",
        "redshift-data:ListTables",
        "redshift-data:DescribeTable",
        "redshift-data:ListSchemas",
        "redshift-data:ListDatabases",
        "redshift-data:ExecuteStatement",
        "redshift-data:GetStatementResult",
        "redshift-data:DescribeStatement",
        "redshift:CreateClusterUser",
        "redshift:DescribeClusters",
        "redshift:DescribeDataShares",
        "redshift:GetClusterCredentials",
        "redshift:GetClusterCredentialsWithIAM",
        "redshift:JoinGroup",
        "redshift-serverless:ListNamespaces",
        "redshift-serverless:ListWorkgroups",
        "redshift-serverless:GetNamespace",
```

```
        "redshift-serverless:GetWorkgroup",
        "redshift-serverless:GetCredentials",
        "s3:AbortMultipartUpload",
        "s3:DeleteObject",
        "s3:DeleteObjectVersion",
        "s3:GetObject",
        "s3:GetBucketLocation",
        "s3:ListBucket",
        "s3:PutObject",
        "s3:PutObjectRetention",
        "s3:ReplicateObject",
        "s3:RestoreObject",
        "secretsmanager:CreateSecret",
        "secretsmanager:ListSecrets",
        "secretsmanager:TagResource",
        "tag:GetResources"
      ],
      "Resource": [
        "*"
      ]
    }
  ]
}
```

AWS verwaltete Richtlinie: AmazonDataZoneRedshiftGlueProvisioningPolicy

Die AmazonDataZoneRedshiftGlueProvisioningPolicy Richtlinie gewährt Amazon DataZone die für die Zusammenarbeit mit AWS Glue und Amazon Redshift erforderlichen Berechtigungen.

```
{
 "Version": "2012-10-17",
 "Statement": [
  {
   "Sid": "AmazonDataZonePermissionsToCreateEnvironmentRole",
   "Effect": "Allow",
   "Action": [
    "iam:CreateRole",
    "iam:DetachRolePolicy",
    "iam:DeleteRolePolicy",
```

```
    "iam:AttachRolePolicy",
    "iam:PutRolePolicy"
   ],
   "Resource": "arn:aws:iam::*:role/datazone*",
   "Condition": {
    "StringEquals": {
     "iam:PermissionsBoundary": "arn:aws:iam::aws:policy/
AmazonDataZoneEnvironmentRolePermissionsBoundary",
     "aws:CalledViaFirst": [
      "cloudformation.amazonaws.com"
     ]
    }
   }
  },
  {
   "Sid": "IamPassRolePermissions",
   "Effect": "Allow",
   "Action": [
    "iam:PassRole"
   ],
   "Resource": [
    "arn:aws:iam::*:role/datazone*"
   ],
   "Condition": {
    "StringEquals": {
     "iam:PassedToService": [
      "glue.amazonaws.com",
      "lakeformation.amazonaws.com"
     ],
     "aws:CalledViaFirst": [
      "cloudformation.amazonaws.com"
     ]
    }
   }
  },
  {
   "Sid": "AmazonDataZonePermissionsToManageCreatedEnvironmentRole",
   "Effect": "Allow",
   "Action": [
    "iam:DeleteRole",
    "iam:GetRole"
   ],
   "Resource": "arn:aws:iam::*:role/datazone*",
   "Condition": {
```

```
    "StringEquals": {
     "aws:CalledViaFirst": [
      "cloudformation.amazonaws.com"
     ]
    }
   }
  },
  {
   "Sid": "AmazonDataZoneCFStackCreationForEnvironments",
   "Effect": "Allow",
   "Action": [
    "cloudformation:CreateStack",
    "cloudformation:TagResource"
   ],
   "Resource": [
    "arn:aws:cloudformation:*:*:stack/DataZone*"
   ],
   "Condition": {
    "ForAnyValue:StringLike": {
     "aws:TagKeys": "AmazonDataZoneEnvironment"
    },
    "Null": {
     "aws:ResourceTag/AmazonDataZoneEnvironment": "false"
    }
   }
  },
  {
   "Sid": "AmazonDataZoneCFStackManagementForEnvironments",
   "Effect": "Allow",
   "Action": [
    "cloudformation:DeleteStack",
    "cloudformation:DescribeStacks",
    "cloudformation:DescribeStackEvents"
   ],
   "Resource": [
    "arn:aws:cloudformation:*:*:stack/DataZone*"
   ]
  },
  {
   "Sid": "AmazonDataZoneEnvironmentParameterValidation",
   "Effect": "Allow",
   "Action": [
    "lakeformation:GetDataLakeSettings",
    "lakeformation:PutDataLakeSettings",
```

```
    "lakeformation:RevokePermissions",
    "lakeformation:ListPermissions",
    "glue:CreateDatabase",
    "glue:GetDatabase",
    "athena:GetWorkGroup",
    "logs:DescribeLogGroups",
    "redshift-serverless:GetNamespace",
    "redshift-serverless:GetWorkgroup",
    "redshift:DescribeClusters",
    "secretsmanager:ListSecrets"
   ],
   "Resource": "*"
  },
  {
   "Sid": "AmazonDataZoneEnvironmentLakeFormationPermissions",
   "Effect": "Allow",
   "Action": [
    "lakeformation:RegisterResource",
    "lakeformation:DeregisterResource",
    "lakeformation:GrantPermissions",
    "lakeformation:ListResources"
   ],
   "Resource": "*",
   "Condition": {
    "StringEquals": {
     "aws:CalledViaFirst": [
      "cloudformation.amazonaws.com"
     ]
    }
   }
  },
  {
   "Sid": "AmazonDataZoneEnvironmentGlueDeletePermissions",
   "Effect": "Allow",
   "Action": [
    "glue:DeleteDatabase"
   ],
   "Resource": "*",
   "Condition": {
    "StringEquals": {
     "aws:CalledViaFirst": [
      "cloudformation.amazonaws.com"
     ]
    }
```

```
    }
   },
   {
    "Sid": "AmazonDataZoneEnvironmentAthenaDeletePermissions",
    "Effect": "Allow",
    "Action": [
     "athena:DeleteWorkGroup"
    ],
    "Resource": "*",
    "Condition": {
     "StringEquals": {
      "aws:CalledViaFirst": [
       "cloudformation.amazonaws.com"
      ]
     }
    }
   },
   {
    "Sid": "AmazonDataZoneEnvironmentAthenaResourceCreation",
    "Effect": "Allow",
    "Action": [
     "athena:CreateWorkGroup",
     "athena:TagResource",
     "iam:TagRole",
     "iam:TagPolicy",
     "logs:TagLogGroup"
    ],
    "Resource": "*",
    "Condition": {
     "ForAnyValue:StringLike": {
      "aws:TagKeys": "AmazonDataZoneEnvironment"
     },
     "Null": {
      "aws:ResourceTag/AmazonDataZoneEnvironment": "false"
     },
     "StringEquals": {
      "aws:CalledViaFirst": [
       "cloudformation.amazonaws.com"
      ]
     }
    }
   },
   {
    "Sid": "AmazonDataZoneEnvironmentLogGroupCreation",
```

```
    "Effect": "Allow",
    "Action": [
     "logs:CreateLogGroup",
     "logs:DeleteLogGroup"
    ],
    "Resource": "arn:aws:logs:*:*:log-group:datazone-*",
    "Condition": {
     "ForAnyValue:StringLike": {
      "aws:TagKeys": "AmazonDataZoneEnvironment"
     },
     "Null": {
      "aws:ResourceTag/AmazonDataZoneEnvironment": "false"
     },
     "StringEquals": {
      "aws:CalledViaFirst": [
       "cloudformation.amazonaws.com"
      ]
     }
    }
   },
   {
    "Sid": "AmazonDataZoneEnvironmentLogGroupManagement",
    "Action": [
     "logs:PutRetentionPolicy"
    ],
    "Resource": "arn:aws:logs:*:*:log-group:datazone-*",
    "Effect": "Allow",
    "Condition": {
     "StringEquals": {
      "aws:CalledViaFirst": [
       "cloudformation.amazonaws.com"
      ]
     }
    }
   },
   {
    "Sid": "AmazonDataZoneEnvironmentIAMPolicyManagement",
    "Effect": "Allow",
    "Action": [
     "iam:DeletePolicy",
     "iam:CreatePolicy",
     "iam:GetPolicy",
     "iam:ListPolicyVersions"
    ],
```

```
    "Resource": [
     "arn:aws:iam::*:policy/datazone*"
    ],
    "Condition": {
     "StringEquals": {
      "aws:CalledViaFirst": [
       "cloudformation.amazonaws.com"
      ]
     }
    }
   },
   {
    "Sid": "AmazonDataZoneEnvironmentS3ValidationPermissions",
    "Effect": "Allow",
    "Action": [
     "s3:ListAllMyBuckets",
     "s3:ListBucket"
    ],
    "Resource": "arn:aws:s3:::*"
   },
   {
    "Sid": "AmazonDataZoneEnvironmentKMSDecryptPermissions",
    "Effect": "Allow",
    "Action": [
     "kms:GenerateDataKey",
     "kms:Decrypt"
    ],
    "Resource": "*",
    "Condition": {
     "Null": {
      "aws:ResourceTag/AmazonDataZoneEnvironment": "false"
     }
    }
   },
   {
    "Sid": "PermissionsToTagAmazonDataZoneEnvironmentGlueResources",
    "Effect": "Allow",
    "Action": [
     "glue:TagResource"
    ],
    "Resource": "*",
    "Condition": {
     "ForAnyValue:StringLike": {
      "aws:TagKeys": "AmazonDataZoneEnvironment"
```

```
    },
    "Null": {
     "aws:RequestTag/AmazonDataZoneEnvironment": "false"
    }
   }
  },
  {
   "Sid": "PermissionsToGetAmazonDataZoneEnvironmentBlueprintTemplates",
   "Effect": "Allow",
   "Action": "s3:GetObject",
   "Resource": "*",
   "Condition": {
    "StringNotEquals": {
     "aws:ResourceAccount": "${aws:PrincipalAccount}"
    },
    "StringEquals": {
     "aws:CalledViaFirst": [
      "cloudformation.amazonaws.com"
     ]
    }
   }
  },
  {
   "Sid": "RedshiftDataPermissions",
   "Effect": "Allow",
   "Action": [
    "redshift-data:ListSchemas",
    "redshift-data:ExecuteStatement"
   ],
   "Resource": [
    "arn:aws:redshift-serverless:*:*:workgroup/*",
    "arn:aws:redshift:*:*:cluster:*"
   ]
  },
  {
   "Sid": "DescribeStatementPermissions",
   "Effect": "Allow",
   "Action": [
    "redshift-data:DescribeStatement"
   ],
   "Resource": "*"
  },
  {
   "Sid": "GetSecretValuePermissions",
```

```
   "Effect": "Allow",
   "Action": [
    "secretsmanager:GetSecretValue"
   ],
   "Resource": "*",
   "Condition": {
    "StringLike": {
     "secretsmanager:ResourceTag/AmazonDataZoneDomain": "dzd*"
    }
   }
  }
 ]
}
```

AWS verwaltete Richtlinie: AmazonDataZoneGlueManageAccessRolePolicy

Diese Richtlinie gibt Amazon die DataZone Erlaubnis, AWS Glue-Daten im Katalog zu veröffentlichen. Es gibt Amazon auch die DataZone Erlaubnis, Zugriff auf veröffentlichte AWS Glue-Assets im Katalog zu gewähren oder den Zugriff zu widerrufen.

```
{
 "Version": "2012-10-17",
 "Statement": [
  {
   "Sid": "GlueDataQualityPermissions",
   "Effect": "Allow",
   "Action": [
    "glue:ListDataQualityResults",
    "glue:GetDataQualityResult"
   ],
   "Resource": "arn:aws:glue:*:*:dataQualityRuleset/*",
   "Condition": {
    "StringEquals": {
     "aws:ResourceAccount": "${aws:PrincipalAccount}"
    }
   }
  },
  {
   "Sid": "GlueTableDatabasePermissions",
```

```
    "Effect": "Allow",
    "Action": [
     "glue:CreateTable",
     "glue:DeleteTable",
     "glue:GetDatabases",
     "glue:GetTables"
    ],
    "Resource": [
     "arn:aws:glue:*:*:catalog",
     "arn:aws:glue:*:*:database/*",
     "arn:aws:glue:*:*:table/*"
    ],
    "Condition": {
     "StringEquals": {
      "aws:ResourceAccount": "${aws:PrincipalAccount}"
     }
    }
   },
   {
    "Sid": "LakeformationResourceSharingPermissions",
    "Effect": "Allow",
    "Action": [
     "lakeformation:BatchGrantPermissions",
     "lakeformation:BatchRevokePermissions",
     "lakeformation:CreateLakeFormationOptIn",
     "lakeformation:DeleteLakeFormationOptIn",
     "lakeformation:GrantPermissions",
     "lakeformation:GetResourceLFTags",
     "lakeformation:ListLakeFormationOptIns",
     "lakeformation:ListPermissions",
     "lakeformation:RegisterResource",
     "lakeformation:RevokePermissions",
     "glue:GetDatabase",
     "glue:GetTable",
     "organizations:DescribeOrganization",
     "ram:GetResourceShareInvitations",
     "ram:ListResources"
    ],
    "Resource": "*"
   },
   {
    "Sid": "CrossAccountRAMResourceSharingPermissions",
    "Effect": "Allow",
    "Action": [
```

```
    "glue:DeleteResourcePolicy",
    "glue:PutResourcePolicy"
   ],
   "Resource": [
    "arn:aws:glue:*:*:catalog",
    "arn:aws:glue:*:*:database/*",
    "arn:aws:glue:*:*:table/*"
   ],
   "Condition": {
    "ForAnyValue:StringEquals": {
     "aws:CalledVia": [
      "ram.amazonaws.com"
     ]
    }
   }
  },
  {
   "Sid": "CrossAccountLakeFormationResourceSharingPermissions",
   "Effect": "Allow",
   "Action": [
    "ram:CreateResourceShare"
   ],
   "Resource": "*",
   "Condition": {
    "StringEqualsIfExists": {
     "ram:RequestedResourceType": [
      "glue:Table",
      "glue:Database",
      "glue:Catalog"
     ]
    },
    "ForAnyValue:StringEquals": {
     "aws:CalledVia": [
      "lakeformation.amazonaws.com"
     ]
    }
   }
  },
  {
   "Sid": "CrossAccountRAMResourceShareInvitationPermission",
   "Effect": "Allow",
   "Action": [
    "ram:AcceptResourceShareInvitation"
   ],
```

```
    "Resource": "arn:aws:ram:*:*:resource-share-invitation/*"
   },
   {
    "Sid": "CrossAccountRAMResourceSharingViaLakeFormationPermissions",
    "Effect": "Allow",
    "Action": [
     "ram:AssociateResourceShare",
     "ram:DeleteResourceShare",
     "ram:DisassociateResourceShare",
     "ram:GetResourceShares",
     "ram:ListResourceSharePermissions",
     "ram:UpdateResourceShare"
    ],
    "Resource": "*",
    "Condition": {
     "StringLike": {
      "ram:ResourceShareName": [
       "LakeFormation*"
      ]
     },
     "ForAnyValue:StringEquals": {
      "aws:CalledVia": [
       "lakeformation.amazonaws.com"
      ]
     }
    }
   },
   {
    "Sid": "CrossAccountRAMResourceSharingViaLakeFormationHybrid",
    "Effect": "Allow",
    "Action": "ram:AssociateResourceSharePermission",
    "Resource": "*",
    "Condition": {
     "StringLike": {
      "ram:PermissionArn": "arn:aws:ram::aws:permission/AWSRAMLFEnabled*"
     },
     "ForAnyValue:StringEquals": {
      "aws:CalledVia": [
       "lakeformation.amazonaws.com"
      ]
     }
    }
   },
   {
```

```
    "Sid": "KMSDecryptPermission",
    "Effect": "Allow",
    "Action": [
     "kms:Decrypt"
    ],
    "Resource": "*",
    "Condition": {
     "StringEquals": {
      "aws:ResourceTag/datazone:projectId": "proj-all"
     }
    }
   },
   {
    "Sid": "GetRoleForDataZone",
    "Effect": "Allow",
    "Action": [
     "iam:GetRole"
    ],
    "Resource": [
     "arn:aws:iam::*:role/AmazonDataZone*",
     "arn:aws:iam::*:role/service-role/AmazonDataZone*"
    ]
   },
   {
    "Sid": "PassRoleForDataLocationRegistration",
    "Effect": "Allow",
    "Action": [
     "iam:PassRole"
    ],
    "Resource": [
     "arn:aws:iam::*:role/AmazonDataZone*",
     "arn:aws:iam::*:role/service-role/AmazonDataZone*"
    ],
    "Condition": {
     "StringEquals": {
      "iam:PassedToService": [
       "lakeformation.amazonaws.com"
      ]
     }
    }
   }
  ]
}
```

AWS verwaltete Richtlinie: AmazonDataZoneRedshiftManageAccessRolePolicy

Diese Richtlinie erteilt Amazon die DataZone Erlaubnis, Amazon Redshift Redshift-Daten im Katalog zu veröffentlichen. Es gibt Amazon auch die DataZone Erlaubnis, Zugriff auf veröffentlichte Amazon Redshift- oder Amazon Redshift Serverless-Assets im Katalog zu gewähren oder den Zugriff zu widerrufen.

```
{
 "Version": "2012-10-17",
 "Statement": [
  {
   "Sid": "redshiftDataScopeDownPermissions",
   "Effect": "Allow",
   "Action": [
    "redshift-data:BatchExecuteStatement",
    "redshift-data:DescribeTable",
    "redshift-data:ExecuteStatement",
    "redshift-data:ListTables",
    "redshift-data:ListSchemas",
    "redshift-data:ListDatabases"
   ],
   "Resource": [
    "arn:aws:redshift-serverless:*:*:workgroup/*",
    "arn:aws:redshift:*:*:cluster:*"
   ],
   "Condition": {
    "StringEquals": {
     "aws:ResourceAccount": "${aws:PrincipalAccount}"
    }
   }
  },
  {
   "Sid": "listSecretsPermission",
   "Effect": "Allow",
   "Action": "secretsmanager:ListSecrets",
   "Resource": "*"
  },
  {
   "Sid": "getWorkgroupPermission",
   "Effect": "Allow",
```

```
    "Action": "redshift-serverless:GetWorkgroup",
    "Resource": [
     "arn:aws:redshift-serverless:*:*:workgroup/*"
    ],
    "Condition": {
     "StringEquals": {
      "aws:ResourceAccount": "${aws:PrincipalAccount}"
     }
    }
   },
   {
    "Sid": "getNamespacePermission",
    "Effect": "Allow",
    "Action": "redshift-serverless:GetNamespace",
    "Resource": [
     "arn:aws:redshift-serverless:*:*:namespace/*"
    ],
    "Condition": {
     "StringEquals": {
      "aws:ResourceAccount": "${aws:PrincipalAccount}"
     }
    }
   },
   {
    "Sid": "redshiftDataPermissions",
    "Effect": "Allow",
    "Action": [
     "redshift-data:DescribeStatement",
     "redshift-data:GetStatementResult",
     "redshift:DescribeClusters"
    ],
    "Resource": "*"
   },
   {
    "Sid": "dataSharesPermissions",
    "Effect": "Allow",
    "Action": [
     "redshift:AuthorizeDataShare",
     "redshift:DescribeDataShares"
    ],
    "Resource": [
     "arn:aws:redshift:*:*:datashare:*/datazone*"
    ],
    "Condition": {
```

```
    "StringEquals": {
     "aws:ResourceAccount": "${aws:PrincipalAccount}"
    }
   }
  },
  {
   "Sid": "associateDataShareConsumerPermission",
   "Effect": "Allow",
   "Action": "redshift:AssociateDataShareConsumer",
   "Resource": "arn:aws:redshift:*:*:datashare:*/datazone*"
  }
 ]
}
```

Von AWS verwaltete Richtlinie: AmazonDataZoneCrossAccountAdmin

Sie können die AmazonDataZoneCrossAccountAdmin Richtlinie an Ihre IAM-Identitäten anhängen.

Diese Richtlinie ermöglicht es Benutzern, mit Amazon-Konten DataZone zu arbeiten.

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Action": [
                "ram:UpdateResourceShare",
                "ram:DeleteResourceShare",
                "ram:AssociateResourceShare",
                "ram:DisassociateResourceShare",
                "ram:GetResourceShares"
            ],
            "Resource": "*",
            "Condition": {
                "StringLike": {
                    "ram:ResourceShareName": [
                        "DataZone*"
                    ]
                }
            }
        },
        {
```

```
            "Effect": "Allow",
            "Action": [
                "datazone:PutEnvironmentBlueprintConfiguration",
                "datazone:GetEnvironmentBlueprintConfiguration",
                "datazone:DeleteEnvironmentBlueprintConfiguration",
                "datazone:ListEnvironmentBlueprintConfigurations",
                "datazone:ListDomains",
                "datazone:GetDomain",
                "datazone:GetEnvironmentBlueprint",
                "datazone:ListEnvironmentBlueprints",
                "datazone:ListEnvironments",
                "datazone:GetEnvironment",
                "ram:AcceptResourceShareInvitation",
                "ram:RejectResourceShareInvitation",
                "ram:Get*",
                "ram:List*"
            ],
            "Resource": "*"
        }
    ]
}
```

AWS verwaltete Richtlinie: AmazonDataZoneDomainExecutionRolePolicy

Dies ist die Standardrichtlinie für die DataZone `DomainExecutionRole` Amazon-Servicerolle. Diese Rolle wird von Amazon verwendet, DataZone um Daten in der DataZone Amazon-Domain zu katalogisieren, zu entdecken, zu verwalten, zu teilen und zu analysieren.

Sie können die AmazonDataZoneDomainExecutionRolePolicy Richtlinie an Ihre anhängen`AmazonDataZoneDomainExecutionRole`.

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Sid": "DomainExecutionRoleStatement",
      "Effect": "Allow",
      "Action": [
        "datazone:AcceptPredictions",
        "datazone:AcceptSubscriptionRequest",
        "datazone:CancelSubscription",
```

```
        "datazone:CreateAsset",
        "datazone:CreateAssetRevision",
        "datazone:CreateAssetType",
        "datazone:CreateDataSource",
        "datazone:CreateEnvironment",
        "datazone:CreateEnvironmentBlueprint",
        "datazone:CreateEnvironmentProfile",
        "datazone:CreateFormType",
        "datazone:CreateGlossary",
        "datazone:CreateGlossaryTerm",
        "datazone:CreateListingChangeSet",
        "datazone:CreateProject",
        "datazone:CreateProjectMembership",
        "datazone:CreateSubscriptionGrant",
        "datazone:CreateSubscriptionRequest",
        "datazone:DeleteAsset",
        "datazone:DeleteAssetType",
        "datazone:DeleteDataSource",
        "datazone:DeleteEnvironment",
        "datazone:DeleteEnvironmentBlueprint",
        "datazone:DeleteEnvironmentProfile",
        "datazone:DeleteFormType",
        "datazone:DeleteGlossary",
        "datazone:DeleteGlossaryTerm",
        "datazone:DeleteListing",
        "datazone:DeleteProject",
        "datazone:DeleteProjectMembership",
        "datazone:DeleteSubscriptionGrant",
        "datazone:DeleteSubscriptionRequest",
        "datazone:DeleteSubscriptionTarget",
        "datazone:GetAsset",
        "datazone:GetAssetType",
        "datazone:GetDataSource",
        "datazone:GetDataSourceRun",
        "datazone:GetDomain",
        "datazone:GetEnvironment",
        "datazone:GetEnvironmentActionLink",
        "datazone:GetEnvironmentBlueprint",
        "datazone:GetEnvironmentCredentials",
        "datazone:GetEnvironmentProfile",
        "datazone:GetFormType",
        "datazone:GetGlossary",
        "datazone:GetGlossaryTerm",
        "datazone:GetGroupProfile",
```

```
        "datazone:GetListing",
        "datazone:GetProject",
        "datazone:GetSubscription",
        "datazone:GetSubscriptionEligibility",
        "datazone:GetSubscriptionGrant",
        "datazone:GetSubscriptionRequestDetails",
        "datazone:GetSubscriptionTarget",
        "datazone:GetUserProfile",
        "datazone:ListAccountEnvironments",
        "datazone:ListAssetRevisions",
        "datazone:ListDataSourceRunActivities",
        "datazone:ListDataSourceRuns",
        "datazone:ListDataSources",
        "datazone:ListEnvironmentBlueprintConfigurations",
        "datazone:ListEnvironmentBlueprintConfigurationSummaries",
        "datazone:ListEnvironmentBlueprints",
        "datazone:ListEnvironmentProfiles",
        "datazone:ListEnvironments",
        "datazone:ListGroupsForUser",
        "datazone:ListNotifications",
        "datazone:ListProjectMemberships",
        "datazone:ListProjects",
        "datazone:ListSubscriptionGrants",
        "datazone:ListSubscriptionRequests",
        "datazone:ListSubscriptionTargets",
        "datazone:ListSubscriptions",
        "datazone:ListWarehouseMetadata",
        "datazone:RejectPredictions",
        "datazone:RejectSubscriptionRequest",
        "datazone:RevokeSubscription",
        "datazone:Search",
        "datazone:SearchGroupProfiles",
        "datazone:SearchListings",
        "datazone:SearchTypes",
        "datazone:SearchUserProfiles",
        "datazone:StartDataSourceRun",
        "datazone:UpdateDataSource",
        "datazone:UpdateEnvironment",
        "datazone:UpdateEnvironmentBlueprint",
        "datazone:UpdateEnvironmentDeploymentStatus",
        "datazone:UpdateEnvironmentProfile",
        "datazone:UpdateGlossary",
        "datazone:UpdateGlossaryTerm",
        "datazone:UpdateProject",
```

```
        "datazone:UpdateSubscriptionGrantStatus",
        "datazone:UpdateSubscriptionRequest",
        "datazone:StartMetadataGenerationRun",
        "datazone:GetMetadataGenerationRun",
        "datazone:CancelMetadataGenerationRun",
        "datazone:ListMetadataGenerationRuns"
      ],
      "Resource": "*"
    },
    {
      "Sid": "RAMResourceShareStatement",
      "Effect": "Allow",
      "Action": "ram:GetResourceShareAssociations",
      "Resource": "*"
    }
  ]
}
```

AWS verwaltete Richtlinie: AmazonDataZoneSageMakerProvisioning

Die AmazonDataZoneSageMakerProvisioning Richtlinie gewährt Amazon DataZone die für die Zusammenarbeit mit Amazon SageMaker erforderlichen Berechtigungen.

```
{
 "Version": "2012-10-17",
 "Statement": [
  {
   "Sid": "CreateSageMakerStudio",
   "Effect": "Allow",
   "Action": [
    "sagemaker:CreateDomain"
   ],
   "Resource": [
    "*"
   ],
   "Condition": {
    "StringEquals": {
     "aws:CalledViaFirst": [
      "cloudformation.amazonaws.com"
     ]
    },
    "ForAnyValue:StringEquals": {
```

```
      "aws:TagKeys": [
       "AmazonDataZoneEnvironment"
      ]
     },
     "Null": {
      "aws:TagKeys": "false",
      "aws:ResourceTag/AmazonDataZoneEnvironment": "false",
      "aws:RequestTag/AmazonDataZoneEnvironment": "false"
     }
    }
   },
   {
    "Sid": "DeleteSageMakerStudio",
    "Effect": "Allow",
    "Action": [
     "sagemaker:DeleteDomain"
    ],
    "Resource": [
     "*"
    ],
    "Condition": {
     "StringEquals": {
      "aws:CalledViaFirst": [
       "cloudformation.amazonaws.com"
      ]
     },
     "ForAnyValue:StringLike": {
      "aws:TagKeys": [
       "AmazonDataZoneEnvironment"
      ]
     },
     "Null": {
      "aws:TagKeys": "false",
      "aws:ResourceTag/AmazonDataZoneEnvironment": "false"
     }
    }
   },
   {
    "Sid": "AmazonDataZoneEnvironmentSageMakerDescribePermissions",
    "Effect": "Allow",
    "Action": [
     "sagemaker:DescribeDomain"
    ],
    "Resource": "*",
```

```
    "Condition": {
     "StringEquals": {
      "aws:CalledViaFirst": [
       "cloudformation.amazonaws.com"
      ]
     }
    }
   },
   {
    "Sid": "IamPassRolePermissions",
    "Effect": "Allow",
    "Action": [
     "iam:PassRole"
    ],
    "Resource": [
     "arn:aws:iam::*:role/sm-provisioning/datazone_usr*"
    ],
    "Condition": {
     "StringEquals": {
      "iam:PassedToService": [
       "glue.amazonaws.com",
       "lakeformation.amazonaws.com",
       "sagemaker.amazonaws.com"
      ],
      "aws:CalledViaFirst": [
       "cloudformation.amazonaws.com"
      ]
     }
    }
   },
   {
    "Sid": "AmazonDataZonePermissionsToCreateEnvironmentRole",
    "Effect": "Allow",
    "Action": [
     "iam:CreateRole",
     "iam:DetachRolePolicy",
     "iam:DeleteRolePolicy",
     "iam:AttachRolePolicy",
     "iam:PutRolePolicy"
    ],
    "Resource": [
     "arn:aws:iam::*:role/sm-provisioning/datazone_usr*"
    ],
    "Condition": {
```

```
    "StringEquals": {
     "aws:CalledViaFirst": [
      "cloudformation.amazonaws.com"
     ],
     "iam:PermissionsBoundary": "arn:aws:iam::aws:policy/
AmazonDataZoneSageMakerEnvironmentRolePermissionsBoundary"
    }
   }
  },
  {
   "Sid": "AmazonDataZonePermissionsToManageEnvironmentRole",
   "Effect": "Allow",
   "Action": [
    "iam:GetRole",
    "iam:GetRolePolicy",
    "iam:DeleteRole"
   ],
   "Resource": [
    "arn:aws:iam::*:role/sm-provisioning/datazone_usr*"
   ],
   "Condition": {
    "StringEquals": {
     "aws:CalledViaFirst": [
      "cloudformation.amazonaws.com"
     ]
    }
   }
  },
  {
   "Sid": "AmazonDataZonePermissionsToCreateSageMakerServiceRole",
   "Effect": "Allow",
   "Action": [
    "iam:CreateServiceLinkedRole"
   ],
   "Resource": [
    "arn:aws:iam::*:role/aws-service-role/sagemaker.amazonaws.com/
AWSServiceRoleForAmazonSageMakerNotebooks"
   ],
   "Condition": {
    "StringEquals": {
     "aws:CalledViaFirst": [
      "cloudformation.amazonaws.com"
     ]
    }
```

```
    }
   },
   {
    "Sid": "AmazonDataZoneEnvironmentParameterValidation",
    "Effect": "Allow",
    "Action": [
     "ec2:DescribeVpcs",
     "ec2:DescribeSubnets",
     "sagemaker:ListDomains"
    ],
    "Resource": "*"
   },
   {
    "Sid": "AmazonDataZoneEnvironmentKMSKeyValidation",
    "Effect": "Allow",
    "Action": [
     "kms:DescribeKey"
    ],
    "Resource": "arn:aws:kms:*:*:key/*",
    "Condition": {
     "Null": {
      "aws:ResourceTag/AmazonDataZoneEnvironment": "false"
     }
    }
   },
   {
    "Sid": "AmazonDataZoneEnvironmentGluePermissions",
    "Effect": "Allow",
    "Action": [
     "glue:CreateConnection",
     "glue:DeleteConnection"
    ],
    "Resource": [
     "arn:aws:glue:*:*:connection/dz-sm-athena-glue-connection-*",
     "arn:aws:glue:*:*:connection/dz-sm-redshift-cluster-connection-*",
     "arn:aws:glue:*:*:connection/dz-sm-redshift-serverless-connection-*",
     "arn:aws:glue:*:*:catalog"
    ],
    "Condition": {
     "StringEquals": {
      "aws:CalledViaFirst": [
       "cloudformation.amazonaws.com"
      ]
     }
```

```
    }
   }
  ]
}
```

AWS verwaltete Richtlinie: AmazonDataZoneSageMakerAccess

Diese Richtlinie erteilt Amazon die DataZone Erlaubnis, SageMaker Amazon-Ressourcen im Katalog zu veröffentlichen. Es gibt Amazon auch die DataZone Erlaubnis, Zugriff auf die von Amazon SageMaker veröffentlichten Assets im Katalog zu gewähren oder den Zugriff zu widerrufen.

Diese Richtlinie umfasst die folgenden Berechtigungen:

- cloudtrail — Informationen über CloudTrail Pfade abrufen.
- cloudwatch — ruft die aktuellen CloudWatch Alarme ab.
- Logs — ruft die Metrikfilter für CloudWatch Logs ab.
- sns — ruft die Liste der Abonnements für ein SNS-Thema ab.
- Config — ruft Informationen zu Konfigurationsrekordern, Ressourcen und AWS Konfigurationsregeln ab. Ermöglicht der serviceverknüpften Rolle außerdem, AWS Config-Regeln zu erstellen und zu löschen und Evaluierungen anhand der Regeln durchzuführen.
- iam — Abrufen und Generieren von Berichten über Anmeldeinformationen für Konten.
- Organisationen — ruft Informationen zu Konten und Organisationseinheiten (OU) für eine Organisation ab.
- securityhub — ruft Informationen darüber ab, wie der Security Hub Hub-Dienst, die Standards und die Kontrollen konfiguriert sind.
- Tag — ruft Informationen über Ressourcen-Tags ab.

```
{
 "Version": "2012-10-17",
 "Statement": [
  {
   "Sid": "AmazonSageMakerReadPermission",
   "Effect": "Allow",
   "Action": [
    "sagemaker:DescribeFeatureGroup",
    "sagemaker:ListModelPackages",
```

```
    "sagemaker:DescribeModelPackage",
    "sagemaker:DescribeModelPackageGroup",
    "sagemaker:DescribeAlgorithm",
    "sagemaker:ListTags",
    "sagemaker:DescribeDomain",
    "sagemaker:GetModelPackageGroupPolicy",
    "sagemaker:Search"
   ],
   "Resource": "*"
  },
  {
   "Sid": "AmazonSageMakerTaggingPermission",
   "Effect": "Allow",
   "Action": [
    "sagemaker:AddTags",
    "sagemaker:DeleteTags"
   ],
   "Resource": "*",
   "Condition": {
    "ForAnyValue:StringLike": {
     "aws:TagKeys": [
      "sagemaker:shared-with:*"
     ]
    }
   }
  },
  {
   "Sid": "AmazonSageMakerModelPackageGroupPolicyPermission",
   "Effect": "Allow",
   "Action": [
    "sagemaker:PutModelPackageGroupPolicy",
    "sagemaker:DeleteModelPackageGroupPolicy"
   ],
   "Resource": [
    "arn:*:sagemaker:*:*:model-package-group/*"
   ]
  },
  {
   "Sid": "AmazonSageMakerRAMPermission",
   "Effect": "Allow",
   "Action": [
    "ram:GetResourceShares",
    "ram:GetResourceShareInvitations",
    "ram:GetResourceShareAssociations"
```

```
    ],
    "Resource": "*"
   },
   {
    "Sid": "AmazonSageMakerRAMResourcePolicyPermission",
    "Effect": "Allow",
    "Action": [
     "sagemaker:PutResourcePolicy",
     "sagemaker:GetResourcePolicy",
     "sagemaker:DeleteResourcePolicy"
    ],
    "Resource": [
     "arn:*:sagemaker:*:*:feature-group/*"
    ]
   },
   {
    "Sid": "AmazonSageMakerRAMTagResourceSharePermission",
    "Effect": "Allow",
    "Action": [
     "ram:TagResource"
    ],
    "Resource": "arn:*:ram:*:*:resource-share/*",
    "Condition": {
     "Null": {
      "aws:RequestTag/AwsDataZoneDomainId": "false"
     }
    }
   },
   {
    "Sid": "AmazonSageMakerRAMDeleteResourceSharePermission",
    "Effect": "Allow",
    "Action": [
     "ram:DeleteResourceShare"
    ],
    "Resource": "arn:*:ram:*:*:resource-share/*",
    "Condition": {
     "Null": {
      "aws:ResourceTag/AwsDataZoneDomainId": "false"
     }
    }
   },
   {
    "Sid": "AmazonSageMakerRAMCreateResourceSharePermission",
    "Effect": "Allow",
```

```
    "Action": [
     "ram:CreateResourceShare"
    ],
    "Resource": "*",
    "Condition": {
     "StringLikeIfExists": {
      "ram:RequestedResourceType": [
       "sagemaker:*"
      ]
     },
     "Null": {
      "aws:RequestTag/AwsDataZoneDomainId": "false"
     }
    }
   },
   {
    "Sid": "AmazonSageMakerS3BucketPolicyPermission",
    "Effect": "Allow",
    "Action": [
     "s3:DeleteBucketPolicy",
     "s3:PutBucketPolicy",
     "s3:GetBucketPolicy"
    ],
    "Resource": [
     "arn:aws:s3:::sagemaker-datazone*",
     "arn:aws:s3:::SageMaker-DataZone*",
     "arn:aws:s3:::datazone-sagemaker*",
     "arn:aws:s3:::DataZone-SageMaker*",
     "arn:aws:s3:::amazon-datazone*"
    ]
   },
   {
    "Sid": "AmazonSageMakerS3Permission",
    "Effect": "Allow",
    "Action": [
     "s3:GetObject",
     "s3:ListBucket"
    ],
    "Resource": [
     "arn:aws:s3:::sagemaker-datazone*",
     "arn:aws:s3:::SageMaker-DataZone*",
     "arn:aws:s3:::datazone-sagemaker*",
     "arn:aws:s3:::DataZone-SageMaker*",
     "arn:aws:s3:::amazon-datazone*"
```

```
    ]
   },
   {
    "Sid": "AmazonSageMakerECRPermission",
    "Effect": "Allow",
    "Action": [
     "ecr:GetRepositoryPolicy",
     "ecr:SetRepositoryPolicy",
     "ecr:DeleteRepositoryPolicy"
    ],
    "Resource": "*",
    "Condition": {
     "Null": {
      "aws:ResourceTag/AmazonDataZoneEnvironment": "false"
     }
    }
   },
   {
    "Sid": "AmazonSageMakerKMSReadPermission",
    "Effect": "Allow",
    "Action": [
     "kms:DescribeKey"
    ],
    "Resource": "*",
    "Condition": {
     "ForAnyValue:StringEquals": {
      "aws:TagKeys": [
       "AmazonDataZoneEnvironment"
      ]
     }
    }
   },
   {
    "Sid": "AmazonSageMakerKMSGrantPermission",
    "Effect": "Allow",
    "Action": [
     "kms:CreateGrant"
    ],
    "Resource": "*",
    "Condition": {
     "ForAnyValue:StringEquals": {
      "aws:TagKeys": [
       "AmazonDataZoneEnvironment"
      ]
```

```
    },
    "ForAllValues:StringEquals": {
     "kms:GrantOperations": [
      "Decrypt"
     ]
    }
   }
  }
 ]
}
```

AWS verwaltete Richtlinie: AmazonDataZoneSageMakerEnvironmentRolePermissionsBoundary

> **Note**
>
> Bei dieser Richtlinie handelt es sich um eine Berechtigungsgrenze. Eine Berechtigungsgrenze legt die maximalen Berechtigungen fest, die eine identitätsbasierte Richtlinie einer IAM-Entität gewähren kann. Sie sollten die Richtlinien für die Begrenzung von DataZone Berechtigungen von Amazon nicht eigenständig verwenden und anhängen. Grenzrichtlinien für DataZone Amazon-Berechtigungen sollten nur an von Amazon DataZone verwaltete Rollen angehängt werden. Weitere Informationen zu Berechtigungsgrenzen finden Sie unter Berechtigungsgrenzen für IAM-Entitäten im IAM-Benutzerhandbuch.

Wenn Sie eine SageMaker Amazon-Umgebung über das DataZone Amazon-Datenportal erstellen, DataZone wendet Amazon diese Berechtigungsgrenze auf die IAM-Rollen an, die bei der Umgebungserstellung erstellt werden. Die Berechtigungsgrenze begrenzt den Umfang der Rollen, die Amazon DataZone erstellt, und aller Rollen, die Sie hinzufügen.

Amazon DataZone verwendet die `AmazonDataZoneSageMakerEnvironmentRolePermissionsBoundary` verwaltete Richtlinie, um den bereitgestellten IAM-Prinzipal einzuschränken, an den sie angehängt ist. Die Principals könnten die Form der Benutzerrollen annehmen, die Amazon im Namen interaktiver Unternehmensbenutzer oder Analysedienste (zum Beispiel) übernehmen DataZone kann AWS SageMaker, und dann Aktionen zur Verarbeitung von Daten durchführen, wie das Lesen und Schreiben von Amazon S3 oder Amazon Redshift oder das Ausführen AWS von Glue Crawler.

Die `AmazonDataZoneSageMakerEnvironmentRolePermissionsBoundary` Richtlinie gewährt Amazon Lese- und Schreibzugriff DataZone auf Dienste wie Amazon SageMaker, AWS Glue, Amazon S3, AWS Lake Formation, Amazon Redshift und Amazon Athena. Die Richtlinie gewährt auch Lese- und Schreibberechtigungen für einige Infrastrukturressourcen, die für die Nutzung dieser Dienste erforderlich sind, wie Netzwerkschnittstellen, Amazon ECR-Repositorys und AWS KMS-Schlüssel. Es ermöglicht auch den Zugriff auf SageMaker Amazon-Anwendungen wie Amazon SageMaker Canvas.

Amazon DataZone wendet die `AmazonDataZoneSageMakerEnvironmentRolePermissionsBoundary` verwaltete Richtlinie als Berechtigungsgrenze für alle Rollen in der DataZone Amazon-Umgebung (Eigentümer und Mitwirkender) an. Diese Berechtigungsgrenze schränkt diese Rollen so ein, dass sie nur Zugriff auf die erforderlichen Ressourcen und Aktionen gewähren, die für eine Umgebung erforderlich sind.

```
       {
"Version": "2012-10-17",
"Statement": [
 {
  "Sid": "AllowAllNonAdminSageMakerActions",
  "Effect": "Allow",
  "Action": [
   "sagemaker:*",
   "sagemaker-geospatial:*"
  ],
  "NotResource": [
   "arn:aws:sagemaker:*:*:domain/*",
   "arn:aws:sagemaker:*:*:user-profile/*",
   "arn:aws:sagemaker:*:*:app/*",
   "arn:aws:sagemaker:*:*:space/*",
   "arn:aws:sagemaker:*:*:flow-definition/*"
  ]
 },
 {
  "Sid": "AllowSageMakerProfileManagement",
  "Effect": "Allow",
  "Action": [
   "sagemaker:CreateUserProfile",
   "sagemaker:DescribeUserProfile",
   "sagemaker:UpdateUserProfile",
   "sagemaker:CreatePresignedDomainUrl"
  ],
```

```
    "Resource": "arn:aws:sagemaker:*:*:*/*"
   },
   {
    "Sid": "AllowLakeFormation",
    "Effect": "Allow",
    "Action": [
     "lakeformation:GetDataAccess"
    ],
    "Resource": "*"
   },
   {
    "Sid": "AllowAddTagsForAppAndSpace",
    "Effect": "Allow",
    "Action": [
     "sagemaker:AddTags"
    ],
    "Resource": [
     "arn:aws:sagemaker:*:*:app/*",
     "arn:aws:sagemaker:*:*:space/*"
    ],
    "Condition": {
     "StringEquals": {
      "sagemaker:TaggingAction": [
       "CreateApp",
       "CreateSpace"
      ]
     }
    }
   },
   {
    "Sid": "AllowStudioActions",
    "Effect": "Allow",
    "Action": [
     "sagemaker:CreatePresignedDomainUrl",
     "sagemaker:DescribeApp",
     "sagemaker:DescribeDomain",
     "sagemaker:DescribeSpace",
     "sagemaker:DescribeUserProfile",
     "sagemaker:ListApps",
     "sagemaker:ListDomains",
     "sagemaker:ListSpaces",
     "sagemaker:ListUserProfiles"
    ],
    "Resource": "*"
```

```
  },
  {
   "Sid": "AllowAppActionsForUserProfile",
   "Effect": "Allow",
   "Action": [
    "sagemaker:CreateApp",
    "sagemaker:DeleteApp"
   ],
   "Resource": "arn:aws:sagemaker:*:*:app/*/*/*/*",
   "Condition": {
    "Null": {
     "sagemaker:OwnerUserProfileArn": "true"
    }
   }
  },
  {
   "Sid": "AllowAppActionsForSharedSpaces",
   "Effect": "Allow",
   "Action": [
    "sagemaker:CreateApp",
    "sagemaker:DeleteApp"
   ],
   "Resource": "arn:aws:sagemaker:*:*:app/${sagemaker:DomainId}/*/*/*",
   "Condition": {
    "StringEquals": {
     "sagemaker:SpaceSharingType": [
      "Shared"
     ]
    }
   }
  },
  {
   "Sid": "AllowMutatingActionsOnSharedSpacesWithoutOwner",
   "Effect": "Allow",
   "Action": [
    "sagemaker:CreateSpace",
    "sagemaker:DeleteSpace",
    "sagemaker:UpdateSpace"
   ],
   "Resource": "arn:aws:sagemaker:*:*:space/${sagemaker:DomainId}/*",
   "Condition": {
    "Null": {
     "sagemaker:OwnerUserProfileArn": "true"
    }
```

```
    }
   },
   {
    "Sid": "RestrictMutatingActionsOnSpacesToOwnerUserProfile",
    "Effect": "Allow",
    "Action": [
     "sagemaker:CreateSpace",
     "sagemaker:DeleteSpace",
     "sagemaker:UpdateSpace"
    ],
    "Resource": "arn:aws:sagemaker:*:*:space/${sagemaker:DomainId}/*",
    "Condition": {
     "ArnLike": {
      "sagemaker:OwnerUserProfileArn": "arn:aws:sagemaker:*:*:user-profile/
${sagemaker:DomainId}/${sagemaker:UserProfileName}"
     },
     "StringEquals": {
      "sagemaker:SpaceSharingType": [
       "Private",
       "Shared"
      ]
     }
    }
   },
   {
    "Sid": "RestrictMutatingActionsOnPrivateSpaceAppsToOwnerUserProfile",
    "Effect": "Allow",
    "Action": [
     "sagemaker:CreateApp",
     "sagemaker:DeleteApp"
    ],
    "Resource": "arn:aws:sagemaker:*:*:app/${sagemaker:DomainId}/*/*/*",
    "Condition": {
     "ArnLike": {
      "sagemaker:OwnerUserProfileArn": "arn:aws:sagemaker:*:*:user-profile/
${sagemaker:DomainId}/${sagemaker:UserProfileName}"
     },
     "StringEquals": {
      "sagemaker:SpaceSharingType": [
       "Private"
      ]
     }
    }
   },
```

```
{
 "Sid": "AllowFlowDefinitionActions",
 "Effect": "Allow",
 "Action": "sagemaker:*",
 "Resource": [
  "arn:aws:sagemaker:*:*:flow-definition/*"
 ],
 "Condition": {
  "StringEqualsIfExists": {
   "sagemaker:WorkteamType": [
    "private-crowd",
    "vendor-crowd"
   ]
  }
 }
},
{
 "Sid": "AllowAWSServiceActions",
 "Effect": "Allow",
 "Action": [
  "sqlworkbench:*",
  "datazone:*",
  "application-autoscaling:DeleteScalingPolicy",
  "application-autoscaling:DeleteScheduledAction",
  "application-autoscaling:DeregisterScalableTarget",
  "application-autoscaling:DescribeScalableTargets",
  "application-autoscaling:DescribeScalingActivities",
  "application-autoscaling:DescribeScalingPolicies",
  "application-autoscaling:DescribeScheduledActions",
  "application-autoscaling:PutScalingPolicy",
  "application-autoscaling:PutScheduledAction",
  "application-autoscaling:RegisterScalableTarget",
  "aws-marketplace:ViewSubscriptions",
  "cloudformation:GetTemplateSummary",
  "cloudwatch:DeleteAlarms",
  "cloudwatch:DescribeAlarms",
  "cloudwatch:GetMetricData",
  "cloudwatch:GetMetricStatistics",
  "cloudwatch:ListMetrics",
  "cloudwatch:PutMetricAlarm",
  "cloudwatch:PutMetricData",
  "codecommit:BatchGetRepositories",
  "codecommit:CreateRepository",
  "codecommit:GetRepository",
```

```
    "codecommit:List*",
    "ec2:CreateNetworkInterface",
    "ec2:CreateNetworkInterfacePermission",
    "ec2:DeleteNetworkInterface",
    "ec2:DeleteNetworkInterfacePermission",
    "ec2:DescribeDhcpOptions",
    "ec2:DescribeNetworkInterfaces",
    "ec2:DescribeRouteTables",
    "ec2:DescribeSecurityGroups",
    "ec2:DescribeSubnets",
    "ec2:DescribeVpcEndpoints",
    "ec2:DescribeVpcEndpointServices",
    "ec2:DescribeVpcs",
    "ecr:BatchCheckLayerAvailability",
    "ecr:BatchGetImage",
    "ecr:Describe*",
    "ecr:GetAuthorizationToken",
    "ecr:GetDownloadUrlForLayer",
    "ecr:StartImageScan",
    "elastic-inference:Connect",
    "elasticfilesystem:DescribeFileSystems",
    "elasticfilesystem:DescribeMountTargets",
    "fsx:DescribeFileSystems",
    "groundtruthlabeling:*",
    "iam:GetRole",
    "iam:ListRoles",
    "kms:DescribeKey",
    "kms:ListAliases",
    "lambda:ListFunctions",
    "logs:CreateLogDelivery",
    "logs:CreateLogGroup",
    "logs:CreateLogStream",
    "logs:DeleteLogDelivery",
    "logs:DescribeLogGroups",
    "logs:DescribeLogStreams",
    "logs:GetLogDelivery",
    "logs:GetLogEvents",
    "logs:ListLogDeliveries",
    "logs:PutLogEvents",
    "logs:UpdateLogDelivery",
    "redshift-data:BatchExecuteStatement",
    "redshift-data:CancelStatement",
    "redshift-data:DescribeStatement",
    "redshift-data:DescribeTable",
```

```
    "redshift-data:ExecuteStatement",
    "redshift-data:GetStatementResult",
    "redshift-data:ListSchemas",
    "redshift-data:ListTables",
    "redshift-serverless:GetCredentials",
    "redshift-serverless:GetNamespace",
    "redshift-serverless:GetWorkgroup",
    "redshift-serverless:ListNamespaces",
    "redshift-serverless:ListWorkgroups",
    "secretsmanager:ListSecrets",
    "servicecatalog:Describe*",
    "servicecatalog:List*",
    "servicecatalog:ScanProvisionedProducts",
    "servicecatalog:SearchProducts",
    "servicecatalog:SearchProvisionedProducts",
    "sns:ListTopics",
    "tag:GetResources"
   ],
   "Resource": "*"
  },
  {
   "Sid": "AllowRAMInvitation",
   "Effect": "Allow",
   "Action": "ram:AcceptResourceShareInvitation",
   "Resource": "*",
   "Condition": {
    "StringLike": {
     "ram:ResourceShareName": "dzd_*"
    }
   }
  },
  {
   "Sid": "AllowECRActions",
   "Effect": "Allow",
   "Action": [
    "ecr:SetRepositoryPolicy",
    "ecr:CompleteLayerUpload",
    "ecr:CreateRepository",
    "ecr:BatchDeleteImage",
    "ecr:UploadLayerPart",
    "ecr:DeleteRepositoryPolicy",
    "ecr:InitiateLayerUpload",
    "ecr:DeleteRepository",
    "ecr:PutImage",
```

```
    "ecr:TagResource",
    "ecr:UntagResource"
   ],
   "Resource": [
    "arn:aws:ecr:*:*:repository/sagemaker*",
    "arn:aws:ecr:*:*:repository/datazone*"
   ]
  },
  {
   "Sid": "AllowCodeCommitActions",
   "Effect": "Allow",
   "Action": [
    "codecommit:GitPull",
    "codecommit:GitPush"
   ],
   "Resource": [
    "arn:aws:codecommit:*:*:*sagemaker*",
    "arn:aws:codecommit:*:*:*SageMaker*",
    "arn:aws:codecommit:*:*:*Sagemaker*"
   ]
  },
  {
   "Sid": "AllowCodeBuildActions",
   "Action": [
    "codebuild:BatchGetBuilds",
    "codebuild:StartBuild"
   ],
   "Resource": [
    "arn:aws:codebuild:*:*:project/sagemaker*",
    "arn:aws:codebuild:*:*:build/*"
   ],
   "Effect": "Allow"
  },
  {
   "Sid": "AllowStepFunctionsActions",
   "Action": [
    "states:DescribeExecution",
    "states:GetExecutionHistory",
    "states:StartExecution",
    "states:StopExecution",
    "states:UpdateStateMachine"
   ],
   "Resource": [
    "arn:aws:states:*:*:statemachine:*sagemaker*",
```

```
    "arn:aws:states:*:*:execution:*sagemaker*:*"
   ],
   "Effect": "Allow"
  },
  {
   "Sid": "AllowSecretManagerActions",
   "Effect": "Allow",
   "Action": [
    "secretsmanager:DescribeSecret",
    "secretsmanager:GetSecretValue",
    "secretsmanager:CreateSecret",
    "secretsmanager:PutResourcePolicy"
   ],
   "Resource": [
    "arn:aws:secretsmanager:*:*:secret:AmazonSageMaker-*"
   ]
  },
  {
   "Sid": "AllowServiceCatalogProvisionProduct",
   "Effect": "Allow",
   "Action": [
    "servicecatalog:ProvisionProduct"
   ],
   "Resource": "*"
  },
  {
   "Sid": "AllowServiceCatalogTerminateUpdateProvisionProduct",
   "Effect": "Allow",
   "Action": [
    "servicecatalog:TerminateProvisionedProduct",
    "servicecatalog:UpdateProvisionedProduct"
   ],
   "Resource": "*",
   "Condition": {
    "StringEquals": {
     "servicecatalog:userLevel": "self"
    }
   }
  },
  {
   "Sid": "AllowS3ObjectActions",
   "Effect": "Allow",
   "Action": [
    "s3:AbortMultipartUpload",
```

```
    "s3:DeleteObject",
    "s3:DeleteObjectVersion",
    "s3:GetObject",
    "s3:PutObject",
    "s3:PutObjectRetention",
    "s3:ReplicateObject",
    "s3:RestoreObject",
    "s3:GetBucketAcl",
    "s3:PutObjectAcl"
   ],
   "Resource": [
    "arn:aws:s3:::SageMaker-DataZone*",
    "arn:aws:s3:::DataZone-SageMaker*",
    "arn:aws:s3:::Sagemaker-DataZone*",
    "arn:aws:s3:::DataZone-Sagemaker*",
    "arn:aws:s3:::sagemaker-datazone*",
    "arn:aws:s3:::datazone-sagemaker*",
    "arn:aws:s3:::amazon-datazone*"
   ]
  },
  {
   "Sid": "AllowS3GetObjectWithSageMakerExistingObjectTag",
   "Effect": "Allow",
   "Action": [
    "s3:GetObject"
   ],
   "Resource": [
    "arn:aws:s3:::*"
   ],
   "Condition": {
    "StringEqualsIgnoreCase": {
     "s3:ExistingObjectTag/SageMaker": "true"
    }
   }
  },
  {
   "Sid": "AllowS3GetObjectWithServiceCatalogProvisioningExistingObjectTag",
   "Effect": "Allow",
   "Action": [
    "s3:GetObject"
   ],
   "Resource": [
    "arn:aws:s3:::*"
   ],
```

```
    "Condition": {
     "StringEquals": {
      "s3:ExistingObjectTag/servicecatalog:provisioning": "true"
     }
    }
   },
   {
    "Sid": "AllowS3BucketActions",
    "Effect": "Allow",
    "Action": [
     "s3:GetBucketLocation",
     "s3:ListBucket",
     "s3:ListAllMyBuckets",
     "s3:GetBucketCors",
     "s3:PutBucketCors"
    ],
    "Resource": [
     "arn:aws:s3:::SageMaker-DataZone*",
     "arn:aws:s3:::DataZone-SageMaker*",
     "arn:aws:s3:::Sagemaker-DataZone*",
     "arn:aws:s3:::DataZone-Sagemaker*",
     "arn:aws:s3:::sagemaker-datazone*",
     "arn:aws:s3:::datazone-sagemaker*",
     "arn:aws:s3:::amazon-datazone*"
    ]
   },
   {
    "Sid": "ReadSageMakerJumpstartArtifacts",
    "Effect": "Allow",
    "Action": "s3:GetObject",
    "Resource": [
     "arn:aws:s3:::jumpstart-cache-prod-us-west-2/*",
     "arn:aws:s3:::jumpstart-cache-prod-us-east-1/*",
     "arn:aws:s3:::jumpstart-cache-prod-us-east-2/*",
     "arn:aws:s3:::jumpstart-cache-prod-eu-west-1/*",
     "arn:aws:s3:::jumpstart-cache-prod-eu-central-1/*",
     "arn:aws:s3:::jumpstart-cache-prod-ap-south-1/*",
     "arn:aws:s3:::jumpstart-cache-prod-ap-northeast-2/*",
     "arn:aws:s3:::jumpstart-cache-prod-ap-northeast-1/*",
     "arn:aws:s3:::jumpstart-cache-prod-ap-southeast-1/*",
     "arn:aws:s3:::jumpstart-cache-prod-ap-southeast-2/*"
    ]
   },
   {
```

```
    "Sid": "AllowLambdaInvokeFunction",
    "Effect": "Allow",
    "Action": [
     "lambda:InvokeFunction"
    ],
    "Resource": [
     "arn:aws:lambda:*:*:function:*SageMaker*",
     "arn:aws:lambda:*:*:function:*sagemaker*",
     "arn:aws:lambda:*:*:function:*Sagemaker*",
     "arn:aws:lambda:*:*:function:*LabelingFunction*"
    ]
   },
   {
    "Sid": "AllowCreateServiceLinkedRoleForSageMakerApplicationAutoscaling",
    "Action": "iam:CreateServiceLinkedRole",
    "Effect": "Allow",
    "Resource": "arn:aws:iam::*:role/aws-service-role/sagemaker.application-
autoscaling.amazonaws.com/AWSServiceRoleForApplicationAutoScaling_SageMakerEndpoint",
    "Condition": {
     "StringLike": {
      "iam:AWSServiceName": "sagemaker.application-autoscaling.amazonaws.com"
     }
    }
   },
   {
    "Sid": "AllowSNSActions",
    "Effect": "Allow",
    "Action": [
     "sns:Subscribe",
     "sns:CreateTopic",
     "sns:Publish"
    ],
    "Resource": [
     "arn:aws:sns:*:*:*SageMaker*",
     "arn:aws:sns:*:*:*Sagemaker*",
     "arn:aws:sns:*:*:*sagemaker*"
    ]
   },
   {
    "Sid": "AllowPassRoleForSageMakerRoles",
    "Effect": "Allow",
    "Action": [
     "iam:PassRole"
    ],
```

```
    "Resource": [
     "arn:aws:iam::*:role/sm-provisioning/datazone_usr_sagemaker_execution_role_*"
    ],
    "Condition": {
     "StringEquals": {
      "iam:PassedToService": [
       "glue.amazonaws.com",
       "bedrock.amazonaws.com",
       "states.amazonaws.com",
       "lakeformation.amazonaws.com",
       "events.amazonaws.com",
       "sagemaker.amazonaws.com",
       "forecast.amazonaws.com"
      ]
     }
    }
   },
   {
    "Sid": "CrossAccountKmsOperations",
    "Effect": "Allow",
    "Action": [
     "kms:DescribeKey",
     "kms:Decrypt",
     "kms:ListKeys"
    ],
    "Resource": "*",
    "Condition": {
     "StringNotEquals": {
      "aws:ResourceAccount": "${aws:PrincipalAccount}"
     }
    }
   },
   {
    "Sid": "KmsOperationsWithResourceTag",
    "Effect": "Allow",
    "Action": [
     "kms:DescribeKey",
     "kms:Decrypt",
     "kms:ListKeys",
     "kms:Encrypt",
     "kms:GenerateDataKey",
     "kms:RetireGrant"
    ],
    "Resource": "*",
```

```
    "Condition": {
     "Null": {
      "aws:ResourceTag/AmazonDataZoneEnvironment": "false"
     }
    }
   },
   {
    "Sid": "AllowAthenaActions",
    "Effect": "Allow",
    "Action": [
     "athena:BatchGetNamedQuery",
     "athena:BatchGetPreparedStatement",
     "athena:BatchGetQueryExecution",
     "athena:CreateNamedQuery",
     "athena:CreateNotebook",
     "athena:CreatePreparedStatement",
     "athena:CreatePresignedNotebookUrl",
     "athena:DeleteNamedQuery",
     "athena:DeleteNotebook",
     "athena:DeletePreparedStatement",
     "athena:ExportNotebook",
     "athena:GetDatabase",
     "athena:GetDataCatalog",
     "athena:GetNamedQuery",
     "athena:GetPreparedStatement",
     "athena:GetQueryExecution",
     "athena:GetQueryResults",
     "athena:GetQueryResultsStream",
     "athena:GetQueryRuntimeStatistics",
     "athena:GetTableMetadata",
     "athena:GetWorkGroup",
     "athena:ImportNotebook",
     "athena:ListDatabases",
     "athena:ListDataCatalogs",
     "athena:ListEngineVersions",
     "athena:ListNamedQueries",
     "athena:ListPreparedStatements",
     "athena:ListQueryExecutions",
     "athena:ListTableMetadata",
     "athena:ListTagsForResource",
     "athena:ListWorkGroups",
     "athena:StartCalculationExecution",
     "athena:StartQueryExecution",
     "athena:StartSession",
```

```
    "athena:StopCalculationExecution",
    "athena:StopQueryExecution",
    "athena:TerminateSession",
    "athena:UpdateNamedQuery",
    "athena:UpdateNotebook",
    "athena:UpdateNotebookMetadata",
    "athena:UpdatePreparedStatement"
   ],
   "Resource": [
    "*"
   ]
  },
  {
   "Sid": "AllowGlueCreateDatabase",
   "Effect": "Allow",
   "Action": [
    "glue:CreateDatabase"
   ],
   "Resource": [
    "arn:aws:glue:*:*:catalog",
    "arn:aws:glue:*:*:database/default"
   ]
  },
  {
   "Sid": "AllowRedshiftGetClusterCredentials",
   "Effect": "Allow",
   "Action": [
    "redshift:GetClusterCredentials"
   ],
   "Resource": [
    "arn:aws:redshift:*:*:dbuser:*/sagemaker_access*",
    "arn:aws:redshift:*:*:dbname:*"
   ]
  },
  {
   "Sid": "AllowListTags",
   "Effect": "Allow",
   "Action": [
    "sagemaker:ListTags"
   ],
   "Resource": [
    "arn:aws:sagemaker:*:*:user-profile/*",
    "arn:aws:sagemaker:*:*:domain/*"
   ]
```

```
  },
  {
   "Sid": "AllowCloudformationListStackResources",
   "Effect": "Allow",
   "Action": [
    "cloudformation:ListStackResources"
   ],
   "Resource": "arn:aws:cloudformation:*:*:stack/SC-*"
  },
  {
   "Sid": "AllowGlueActions",
   "Effect": "Allow",
   "Action": [
    "glue:GetColumnStatisticsForPartition",
    "glue:GetColumnStatisticsForTable",
    "glue:ListJobs",
    "glue:CreateSession",
    "glue:RunStatement",
    "glue:BatchCreatePartition",
    "glue:CreatePartitionIndex",
    "glue:CreateTable",
    "glue:BatchGetWorkflows",
    "glue:BatchUpdatePartition",
    "glue:BatchDeletePartition",
    "glue:GetPartition",
    "glue:GetPartitions",
    "glue:UpdateTable",
    "glue:DeleteTableVersion",
    "glue:DeleteTable",
    "glue:DeleteColumnStatisticsForPartition",
    "glue:DeleteColumnStatisticsForTable",
    "glue:DeletePartitionIndex",
    "glue:UpdateColumnStatisticsForPartition",
    "glue:UpdateColumnStatisticsForTable",
    "glue:BatchDeleteTableVersion",
    "glue:BatchDeleteTable",
    "glue:CreatePartition",
    "glue:DeletePartition",
    "glue:UpdatePartition",
    "glue:CreateBlueprint",
    "glue:CreateJob",
    "glue:CreateConnection",
    "glue:CreateCrawler",
    "glue:CreateDataQualityRuleset",
```

```
    "glue:CreateWorkflow",
    "glue:GetDatabases",
    "glue:GetTables",
    "glue:GetTable",
    "glue:SearchTables",
    "glue:NotifyEvent",
    "glue:ListSchemas",
    "glue:BatchGetJobs",
    "glue:GetConnection",
    "glue:GetDatabase"
   ],
   "Resource": [
    "*"
   ]
  },
  {
   "Sid": "AllowGlueActionsWithEnvironmentTag",
   "Effect": "Allow",
   "Action": [
    "glue:SearchTables",
    "glue:NotifyEvent",
    "glue:StartBlueprintRun",
    "glue:PutWorkflowRunProperties",
    "glue:StopCrawler",
    "glue:DeleteJob",
    "glue:DeleteWorkflow",
    "glue:UpdateCrawler",
    "glue:DeleteBlueprint",
    "glue:UpdateWorkflow",
    "glue:StartCrawler",
    "glue:ResetJobBookmark",
    "glue:UpdateJob",
    "glue:StartWorkflowRun",
    "glue:StopCrawlerSchedule",
    "glue:ResumeWorkflowRun",
    "glue:ListSchemas",
    "glue:DeleteCrawler",
    "glue:UpdateBlueprint",
    "glue:BatchStopJobRun",
    "glue:StopWorkflowRun",
    "glue:BatchGetJobs",
    "glue:BatchGetWorkflows",
    "glue:UpdateCrawlerSchedule",
    "glue:DeleteConnection",
```

```
    "glue:UpdateConnection",
    "glue:GetConnection",
    "glue:GetDatabase",
    "glue:GetTable",
    "glue:GetPartition",
    "glue:GetPartitions",
    "glue:BatchDeleteConnection",
    "glue:StartCrawlerSchedule",
    "glue:StartJobRun",
    "glue:CreateWorkflow",
    "glue:*DataQuality*"
   ],
   "Resource": "*",
   "Condition": {
    "Null": {
     "aws:ResourceTag/AmazonDataZoneEnvironment": "false"
    }
   }
  },
  {
   "Sid": "AllowGlueDefaultAccess",
   "Effect": "Allow",
   "Action": [
    "glue:BatchGet*",
    "glue:Get*",
    "glue:SearchTables",
    "glue:List*",
    "glue:RunStatement"
   ],
   "Resource": [
    "arn:aws:glue:*:*:catalog",
    "arn:aws:glue:*:*:database/default",
    "arn:aws:glue:*:*:connection/dz-sm-*",
    "arn:aws:glue:*:*:session/*"
   ]
  },
  {
   "Sid": "AllowRedshiftClusterActions",
   "Effect": "Allow",
   "Action": [
    "redshift:GetClusterCredentialsWithIAM",
    "redshift:DescribeClusters"
   ],
   "Resource": [
```

```
    "arn:aws:redshift:*:*:cluster:*",
    "arn:aws:redshift:*:*:dbname:*"
   ]
  },
  {
   "Sid": "AllowCreateClusterUser",
   "Effect": "Allow",
   "Action": [
    "redshift:CreateClusterUser"
   ],
   "Resource": [
    "arn:aws:redshift:*:*:dbuser:*"
   ]
  },
  {
   "Sid": "AllowCreateSecretActions",
   "Effect": "Allow",
   "Action": [
    "secretsmanager:CreateSecret",
    "secretsmanager:TagResource"
   ],
   "Resource": "arn:aws:secretsmanager:*:*:secret:AmazonDataZone-*",
   "Condition": {
    "StringLike": {
     "aws:ResourceTag/AmazonDataZoneDomain": "dzd_*",
     "aws:RequestTag/AmazonDataZoneDomain": "dzd_*"
    },
    "Null": {
     "aws:TagKeys": "false",
     "aws:ResourceTag/AmazonDataZoneProject": "false",
     "aws:ResourceTag/AmazonDataZoneDomain": "false",
     "aws:RequestTag/AmazonDataZoneDomain": "false",
     "aws:RequestTag/AmazonDataZoneProject": "false"
    },
    "ForAllValues:StringEquals": {
     "aws:TagKeys": [
      "AmazonDataZoneDomain",
      "AmazonDataZoneProject"
     ]
    }
   }
  },
  {
   "Sid": "ForecastOperations",
```

```
    "Effect": "Allow",
    "Action": [
     "forecast:CreateExplainabilityExport",
     "forecast:CreateExplainability",
     "forecast:CreateForecastEndpoint",
     "forecast:CreateAutoPredictor",
     "forecast:CreateDatasetImportJob",
     "forecast:CreateDatasetGroup",
     "forecast:CreateDataset",
     "forecast:CreateForecast",
     "forecast:CreateForecastExportJob",
     "forecast:CreatePredictorBacktestExportJob",
     "forecast:CreatePredictor",
     "forecast:DescribeExplainabilityExport",
     "forecast:DescribeExplainability",
     "forecast:DescribeAutoPredictor",
     "forecast:DescribeForecastEndpoint",
     "forecast:DescribeDatasetImportJob",
     "forecast:DescribeDataset",
     "forecast:DescribeForecast",
     "forecast:DescribeForecastExportJob",
     "forecast:DescribePredictorBacktestExportJob",
     "forecast:GetAccuracyMetrics",
     "forecast:InvokeForecastEndpoint",
     "forecast:GetRecentForecastContext",
     "forecast:DescribePredictor",
     "forecast:TagResource",
     "forecast:DeleteResourceTree"
    ],
    "Resource": [
     "arn:aws:forecast:*:*:*Canvas*"
    ]
   },
   {
    "Sid": "RDSOperation",
    "Effect": "Allow",
    "Action": "rds:DescribeDBInstances",
    "Resource": "*"
   },
   {
    "Sid": "AllowEventBridgeRule",
    "Effect": "Allow",
    "Action": [
     "events:PutRule"
```

```
    ],
    "Resource": "arn:aws:events:*:*:rule/*",
    "Condition": {
     "StringEquals": {
      "aws:RequestTag/sagemaker:is-canvas-data-prep-job": "true"
     }
    }
   },
   {
    "Sid": "EventBridgeOperations",
    "Effect": "Allow",
    "Action": [
     "events:DescribeRule",
     "events:PutTargets"
    ],
    "Resource": "arn:aws:events:*:*:rule/*",
    "Condition": {
     "StringEquals": {
      "aws:ResourceTag/sagemaker:is-canvas-data-prep-job": "true"
     }
    }
   },
   {
    "Sid": "EventBridgeTagBasedOperations",
    "Effect": "Allow",
    "Action": [
     "events:TagResource"
    ],
    "Resource": "arn:aws:events:*:*:rule/*",
    "Condition": {
     "StringEquals": {
      "aws:RequestTag/sagemaker:is-canvas-data-prep-job": "true",
      "aws:ResourceTag/sagemaker:is-canvas-data-prep-job": "true"
     }
    }
   },
   {
    "Sid": "EventBridgeListTagOperation",
    "Effect": "Allow",
    "Action": "events:ListTagsForResource",
    "Resource": "*"
   },
   {
    "Sid": "AllowEMR",
```

```
    "Effect": "Allow",
    "Action": [
     "elasticmapreduce:DescribeCluster",
     "elasticmapreduce:ListInstanceGroups",
     "elasticmapreduce:ListClusters"
    ],
    "Resource": "*"
   },
   {
    "Sid": "AllowSSOAction",
    "Effect": "Allow",
    "Action": [
     "sso:CreateApplicationAssignment",
     "sso:AssociateProfile"
    ],
    "Resource": "*"
   },
   {
    "Sid": "DenyNotAction",
    "Effect": "Deny",
    "NotAction": [
     "sagemaker:*",
     "sagemaker-geospatial:*",
     "sqlworkbench:*",
     "datazone:*",
     "forecast:*",
     "application-autoscaling:DeleteScalingPolicy",
     "application-autoscaling:DeleteScheduledAction",
     "application-autoscaling:DeregisterScalableTarget",
     "application-autoscaling:DescribeScalableTargets",
     "application-autoscaling:DescribeScalingActivities",
     "application-autoscaling:DescribeScalingPolicies",
     "application-autoscaling:DescribeScheduledActions",
     "application-autoscaling:PutScalingPolicy",
     "application-autoscaling:PutScheduledAction",
     "application-autoscaling:RegisterScalableTarget",
     "athena:BatchGetNamedQuery",
     "athena:BatchGetPreparedStatement",
     "athena:BatchGetQueryExecution",
     "athena:CreateNamedQuery",
     "athena:CreateNotebook",
     "athena:CreatePreparedStatement",
     "athena:CreatePresignedNotebookUrl",
     "athena:DeleteNamedQuery",
```

```
    "athena:DeleteNotebook",
    "athena:DeletePreparedStatement",
    "athena:ExportNotebook",
    "athena:GetDatabase",
    "athena:GetDataCatalog",
    "athena:GetNamedQuery",
    "athena:GetPreparedStatement",
    "athena:GetQueryExecution",
    "athena:GetQueryResults",
    "athena:GetQueryResultsStream",
    "athena:GetQueryRuntimeStatistics",
    "athena:GetTableMetadata",
    "athena:GetWorkGroup",
    "athena:ImportNotebook",
    "athena:ListDatabases",
    "athena:ListDataCatalogs",
    "athena:ListEngineVersions",
    "athena:ListNamedQueries",
    "athena:ListPreparedStatements",
    "athena:ListQueryExecutions",
    "athena:ListTableMetadata",
    "athena:ListTagsForResource",
    "athena:ListWorkGroups",
    "athena:StartCalculationExecution",
    "athena:StartQueryExecution",
    "athena:StartSession",
    "athena:StopCalculationExecution",
    "athena:StopQueryExecution",
    "athena:TerminateSession",
    "athena:UpdateNamedQuery",
    "athena:UpdateNotebook",
    "athena:UpdateNotebookMetadata",
    "athena:UpdatePreparedStatement",
    "aws-marketplace:ViewSubscriptions",
    "cloudformation:GetTemplateSummary",
    "cloudformation:ListStackResources",
    "cloudwatch:DeleteAlarms",
    "cloudwatch:DescribeAlarms",
    "cloudwatch:GetMetricData",
    "cloudwatch:GetMetricStatistics",
    "cloudwatch:ListMetrics",
    "cloudwatch:PutMetricAlarm",
    "cloudwatch:PutMetricData",
    "codebuild:BatchGetBuilds",
```

```
    "codebuild:StartBuild",
    "codecommit:BatchGetRepositories",
    "codecommit:CreateRepository",
    "codecommit:GetRepository",
    "codecommit:List*",
    "codecommit:GitPull",
    "codecommit:GitPush",
    "ec2:CreateNetworkInterface",
    "ec2:CreateNetworkInterfacePermission",
    "ec2:DeleteNetworkInterface",
    "ec2:DeleteNetworkInterfacePermission",
    "ec2:DescribeDhcpOptions",
    "ec2:DescribeNetworkInterfaces",
    "ec2:DescribeRouteTables",
    "ec2:DescribeSecurityGroups",
    "ec2:DescribeSubnets",
    "ec2:DescribeVpcEndpoints",
    "ec2:DescribeVpcEndpointServices",
    "ec2:DescribeVpcs",
    "ecr:BatchCheckLayerAvailability",
    "ecr:BatchGetImage",
    "ecr:CreateRepository",
    "ecr:Describe*",
    "ecr:GetAuthorizationToken",
    "ecr:GetDownloadUrlForLayer",
    "ecr:SetRepositoryPolicy",
    "ecr:CompleteLayerUpload",
    "ecr:BatchDeleteImage",
    "ecr:UploadLayerPart",
    "ecr:DeleteRepositoryPolicy",
    "ecr:InitiateLayerUpload",
    "ecr:DeleteRepository",
    "ecr:PutImage",
    "ecr:StartImageScan",
    "ecr:TagResource",
    "ecr:UntagResource",
    "elastic-inference:Connect",
    "elasticfilesystem:DescribeFileSystems",
    "elasticfilesystem:DescribeMountTargets",
    "elasticmapreduce:DescribeCluster",
    "elasticmapreduce:ListInstanceGroups",
    "elasticmapreduce:ListClusters",
    "events:PutRule",
    "events:DescribeRule",
```

```
    "events:PutTargets",
    "events:TagResource",
    "events:ListTagsForResource",
    "fsx:DescribeFileSystems",
    "glue:SearchTables",
    "glue:NotifyEvent",
    "glue:StartBlueprintRun",
    "glue:PutWorkflowRunProperties",
    "glue:StopCrawler",
    "glue:DeleteJob",
    "glue:DeleteWorkflow",
    "glue:UpdateCrawler",
    "glue:DeleteBlueprint",
    "glue:UpdateWorkflow",
    "glue:StartCrawler",
    "glue:ResetJobBookmark",
    "glue:UpdateJob",
    "glue:StartWorkflowRun",
    "glue:StopCrawlerSchedule",
    "glue:ResumeWorkflowRun",
    "glue:DeleteCrawler",
    "glue:UpdateBlueprint",
    "glue:BatchStopJobRun",
    "glue:StopWorkflowRun",
    "glue:BatchGet*",
    "glue:UpdateCrawlerSchedule",
    "glue:DeleteConnection",
    "glue:UpdateConnection",
    "glue:Get*",
    "glue:BatchDeleteConnection",
    "glue:StartCrawlerSchedule",
    "glue:StartJobRun",
    "glue:CreateWorkflow",
    "glue:*DataQuality*",
    "glue:List*",
    "glue:CreateSession",
    "glue:RunStatement",
    "glue:BatchCreatePartition",
    "glue:CreateDatabase",
    "glue:CreatePartitionIndex",
    "glue:CreateTable",
    "glue:BatchUpdatePartition",
    "glue:BatchDeletePartition",
    "glue:UpdateTable",
```

```
    "glue:DeleteTableVersion",
    "glue:DeleteTable",
    "glue:DeleteColumnStatisticsForPartition",
    "glue:DeleteColumnStatisticsForTable",
    "glue:DeletePartitionIndex",
    "glue:UpdateColumnStatisticsForPartition",
    "glue:UpdateColumnStatisticsForTable",
    "glue:BatchDeleteTableVersion",
    "glue:BatchDeleteTable",
    "glue:CreatePartition",
    "glue:DeletePartition",
    "glue:UpdatePartition",
    "glue:CreateBlueprint",
    "glue:CreateJob",
    "glue:CreateConnection",
    "glue:CreateCrawler",
    "groundtruthlabeling:*",
    "iam:CreateServiceLinkedRole",
    "iam:GetRole",
    "iam:ListRoles",
    "iam:PassRole",
    "kms:DescribeKey",
    "kms:ListAliases",
    "kms:Decrypt",
    "kms:ListKeys",
    "kms:Encrypt",
    "kms:GenerateDataKey",
    "kms:RetireGrant",
    "lakeformation:GetDataAccess",
    "lambda:ListFunctions",
    "lambda:InvokeFunction",
    "logs:CreateLogDelivery",
    "logs:CreateLogGroup",
    "logs:CreateLogStream",
    "logs:DeleteLogDelivery",
    "logs:Describe*",
    "logs:GetLogDelivery",
    "logs:GetLogEvents",
    "logs:ListLogDeliveries",
    "logs:PutLogEvents",
    "logs:UpdateLogDelivery",
    "ram:AcceptResourceShareInvitation",
    "rds:DescribeDBInstances",
    "redshift:CreateClusterUser",
```

```
    "redshift:GetClusterCredentials",
    "redshift:GetClusterCredentialsWithIAM",
    "redshift:DescribeClusters",
    "redshift-data:BatchExecuteStatement",
    "redshift-data:CancelStatement",
    "redshift-data:DescribeStatement",
    "redshift-data:DescribeTable",
    "redshift-data:ExecuteStatement",
    "redshift-data:GetStatementResult",
    "redshift-data:ListSchemas",
    "redshift-data:ListTables",
    "redshift-serverless:ListNamespaces",
    "redshift-serverless:ListWorkgroups",
    "redshift-serverless:GetNamespace",
    "redshift-serverless:GetWorkgroup",
    "redshift-serverless:GetCredentials",
    "s3:GetBucketAcl",
    "s3:PutObjectAcl",
    "s3:GetObject",
    "s3:PutObject",
    "s3:DeleteObject",
    "s3:AbortMultipartUpload",
    "s3:CreateBucket",
    "s3:GetBucketLocation",
    "s3:ListBucket",
    "s3:ListAllMyBuckets",
    "s3:GetBucketCors",
    "s3:PutBucketCors",
    "s3:DeleteObjectVersion",
    "s3:PutObjectRetention",
    "s3:ReplicateObject",
    "s3:RestoreObject",
    "secretsmanager:ListSecrets",
    "secretsmanager:DescribeSecret",
    "secretsmanager:GetSecretValue",
    "secretsmanager:CreateSecret",
    "secretsmanager:PutResourcePolicy",
    "secretsmanager:TagResource",
    "servicecatalog:Describe*",
    "servicecatalog:List*",
    "servicecatalog:ScanProvisionedProducts",
    "servicecatalog:SearchProducts",
    "servicecatalog:SearchProvisionedProducts",
    "servicecatalog:ProvisionProduct",
```

```
    "servicecatalog:TerminateProvisionedProduct",
    "servicecatalog:UpdateProvisionedProduct",
    "sns:ListTopics",
    "sns:Subscribe",
    "sns:CreateTopic",
    "sns:Publish",
    "states:DescribeExecution",
    "states:GetExecutionHistory",
    "states:StartExecution",
    "states:StopExecution",
    "states:UpdateStateMachine",
    "tag:GetResources",
    "sso:CreateApplicationAssignment",
    "sso:AssociateProfile"
   ],
   "Resource": "*"
  }
 ]
}
```

DataZone Aktualisierungen der AWS verwalteten Richtlinien durch Amazon

Sehen Sie sich Details zu Aktualisierungen der AWS verwalteten Richtlinien für Amazon an, DataZone seit dieser Service begonnen hat, diese Änderungen zu verfolgen. Abonnieren Sie den RSS-Feed auf der Amazon DataZone Document-Verlaufsseite, um automatische Benachrichtigungen über Änderungen an dieser Seite zu erhalten.

Änderung	Beschreibung	Datum
AmazonDataZoneSageMakerEnvironmentRolePermissionsBoundary - neue Grenze für Berechtigungen	Neue Berechtigungsgrenze aufgerufen AmazonDataZoneSageMakerEnvironmentRolePermissionsBoundary. Wenn Sie eine SageMaker Amazon-Umgebung über das DataZone Amazon-Datenportal erstellen, DataZone wendet Amazon diese Berechtigungsgrenz	30. April 2024

Änderung	Beschreibung	Datum
	e auf die IAM-Rollen an, die bei der Umgebungs erstellung erstellt werden. Die Berechtigungsgrenze begrenzt den Umfang der Rollen, die Amazon DataZone erstellt, und aller Rollen, die Sie hinzufügen.	
AmazonDataZoneSage MakerAccess - neue Richtlinie	Eine neue Richtlinie namens AmazonDataZoneSage MakerAccessgibt Amazon die DataZone Erlaubnis , SageMaker Amazon-Re ssourcen im Katalog zu veröffentlichen. Es gibt Amazon auch die DataZone Erlaubnis, Zugriff auf die von Amazon SageMaker veröffent lichten Assets im Katalog zu gewähren oder den Zugriff zu widerrufen.	30. April 2024

Änderung	Beschreibung	Datum
AmazonDataZoneFullAccess - Aktualisierung der Richtlinien	Eine Aktualisierung der AmazonDataZoneFull AccessRichtlinie, die Zugriff auf `DescribeSecurityGroups` Aktionen erweitert, um die Benutzerfreundlichkeit für Kontoadministratoren zu verbessern, indem sie Blueprints in der Konsole konfigurieren und `GetPolicy` Aktionen zum Abrufen von Informationen über die angegebene verwaltete Richtlinie durchführen.	30. April 2024
AmazonDataZoneSageMakerProvisioning - neue Richtlinie	Eine neue Richtlinie namens AmazonDataZoneSageMakerProvisioninggewährt Amazon DataZone die für die Zusammenarbeit mit Amazon SageMaker erforderlichen Berechtigungen.	30. April 2024
AmazonDataZoneS3Manage-<region>- <domainId>- neue Rolle	Neue Rolle namens AmazonDataZoneS3Manage- — <region><domainId> die verwendet wird, wenn Amazon AWS Lake Formation DataZone aufruft, um einen Amazon Simple Storage Service (Amazon S3) - Standort zu registrieren. AWS Lake Formation übernimmt diese Rolle beim Zugriff auf die Daten an diesem Standort.	1. April 2024

Änderung	Beschreibung	Datum
AmazonDataZoneGlue ManageAccessRolePolicy - Aktualisierung der Richtlinie	Das wurde aktualisiert AmazonDataZoneGlue ManageAccessRolePolicy, um die Unterstützung für Berechtigungen zu aktiviere n, die es Amazon ermöglichen DataZone , Veröffentlichungen und Zugriffserlaubnisse für Daten zu ermöglichen.	1. April 2024
AmazonDataZoneDoma inExecutionRolePolicy und AmazonDataZoneFull UserAccess — Aktualisierung der Richtlinien	Das AmazonDataZoneDoma inExecutionRolePolicyund wurde aktualisiert AmazonDat aZoneFullUserAccess, um die Unterstützung für die `CancelMetadataGene rationRun` API zu aktivieren.	29. März 2024
AmazonDataZoneFullAccess - Aktualisierung der Richtlinie	Das wurde aktualisi ert`AmazonDataZoneFull Access` , sodass Benutzer ihre Geheimnisse, Cluster, VPCs und Subnetze in der DataZone Amazon-Ma nagementkonsole auswählen können, anstatt sie in ein Textfeld einzugeben.	13. März 2024

Änderung	Beschreibung	Datum
AmazonDataZoneDomainExecutionRolePolicy - Aktualisierung der Richtlinie	Das wurde aktualisiert AmazonDataZoneDomainExecutionRolePolicy, um die Unterstützung für die `ListEnvironmentBlueprintConfigurationSummaries` API zu aktivieren, die für die Erstellung von Umgebungsprofilen erforderlich ist, indem identifiziert wird, welche Blueprints in welchem Konto und welcher Region aktiviert sind.	01. Februar 2024
AmazonDataZoneGlueManageAccessRolePolicy - Aktualisierung der Richtlinie	Das wurde aktualisiert AmazonDataZoneGlueManageAccessRolePolicy, um die Unterstützung für den AWS Lake Formation Formation-Hybridmodus zu aktivieren.	14. Dezember 2023
AmazonDataZoneFullUserAccess und AmazonDataZoneDomainExecutionRolePolicy — Aktualisierungen der Richtlinien	Die AmazonDataZoneFullUserAccessund die AmazonDataZoneDomainExecutionRolePolicyRichtlinien wurden aktualisiert, um die generativen KI-gestützten Datenbeschreibungsfunktionen in Amazon DataZone zu unterstützen.	28. November 2023

Änderung	Beschreibung	Datum
AmazonDataZoneEnvironmentRolePermissionsBoundary - Aktualisierung der Richtlinien	Amazon DataZone hat eine Aktualisierung der AmazonDataZoneEnvironmentRolePermissionsBoundaryverwalteten Richtlinie vorgenommen, die aus einer zusätzlichen `athena:GetQueryResultsStream` Genehmigung besteht, die auf die `ResourceTag` Bedingung zugeschnitten ist.	17. November 2023
AmazonDataZoneRedshiftManageAccessRolePolicy - Aktualisierung der Richtlinie	Amazon hat das DataZone aktualisiert, AmazonDataZoneRedshiftManageAccessRolePolicyindem es das Häkchen bei der Organisations-ID für die `redshift:AssociateDataShareConsumer` Aktion entfernt hat. Auf diese Weise können Sie Ressourcen organisationsübergreifend AWS gemeinsam nutzen.	16. November 2023
AmazonDataZoneFullUserAccess - Aktualisierung der Richtlinie	Amazon hat die AmazonDataZoneFullUserAccessRichtlinie DataZone aktualisiert, die Amazon vollen Zugriff gewährt DataZone, aber sie erlaubt nicht die Verwaltung von Domains, Benutzern oder zugehörigen Konten.	02. Oktober 2023

Änderung	Beschreibung	Datum
AmazonDataZonePortalFullAccessPolicy - Richtlinie veraltet	Amazon DataZone hat das abgelehnt. AmazonDataZonePortalFullAccessPolicy	29. September 2023
AmazonDataZonePreviewConsoleFullAccess - Richtlinie veraltet	Amazon DataZone hat das abgelehnt. AmazonDataZonePreviewConsoleFullAccess	29. September 2023
AmazonDataZoneDomainExecutionRolePolicy - Neue Richtlinie	Amazon DataZone hat eine neue Richtlinie namens hinzugefügt AmazonDataZoneDomainExecutionRolePolicy. Dies ist die Standardrichtlinie für die DataZone `AmazonDataZoneDomainExecutionRole` Amazon-Serverolle. Diese Rolle wird von Amazon verwendet, DataZone um Daten in der DataZone Amazon-Domain zu katalogisieren, zu entdecken, zu verwalten, zu teilen und zu analysieren. Sie können die `AmazonDataZoneDomainExecutionRolePolicy` Richtlinie an Ihre anhängen`AmazonDataZoneDomainExecutionRole` .	25. September 2023

Änderung	Beschreibung	Datum
AmazonDataZoneCrossAccountAdmin - Neue Richtlinie	Amazon DataZone hat eine neue Richtlinie hinzugefügt, AmazonDataZoneCrossAccountAdmindie es Benutzern ermöglicht, mit Amazon DataZone und den zugehörigen Konten zu arbeiten.	19. September 2023
AmazonDataZoneFullUserAccess - Neue Richtlinie	Amazon DataZone hat eine neue Richtlinie hinzugefügt AmazonDataZoneFullUserAccess, die Amazon vollen Zugriff gewährt DataZone, aber nicht die Verwaltung von Domains, Benutzern oder zugehörigen Konten erlaubt.	12. September 2023
AmazonDataZoneRedshiftManageAccessRolePolicy - Neue Richtlinie	Amazon DataZone hat eine neue Richtlinie hinzugefügt, AmazonDataZoneRedshiftManageAccessRolePolicydie Berechtigungen gewährt, damit Amazon DataZone die Veröffentlichung und den Zugriff auf Daten ermöglichen kann.	12. September 2023

Änderung	Beschreibung	Datum
AmazonDataZoneGlue ManageAccessRolePolicy - Neue Richtlinie	Amazon DataZone hat eine neue Richtlinie hinzugefügt, AmazonDataZoneGlue ManageAccessRolePolicydie Amazon DataZone Erlaubnis erteilt, AWS Glue-Daten im Katalog zu veröffentlichen. Es gibt Amazon auch die DataZone Erlaubnis, Zugriff auf veröffentlichte AWS Glue-Assets im Katalog zu gewähren oder den Zugriff zu widerrufen.	12. September 2023
AmazonDataZoneRedshiftGlueProvisioningPolicy - Neue Richtlinie	Amazon DataZone hat eine neue Richtlinie hinzugefügt, AmazonDataZoneRedshiftGlueProvisioningPolicydie Amazon DataZone die für die Zusammenarbeit mit den unterstützten Datenquellen erforderlichen Berechtigungen gewährt.	12. September 2023
AmazonDataZoneEnvironmentRolePermissionsBoundary - Neue Richtlinie	Amazon DataZone hat eine neue Richtlinie hinzugefügt AmazonDataZoneEnvironmentRolePermissionsBoundary, die den bereitgestellten IAM-Prinzipal einschränkt, an den sie angehängt ist.	12. September 2023

Änderung	Beschreibung	Datum
AmazonDataZoneFullAccess - Neue Richtlinie	Amazon DataZone hat eine neue Richtlinie hinzugefügt, AmazonDataZoneFullAccessdie vollen Zugriff auf Amazon DataZone über die AWS Management Console bietet.	12. September 2023
Aktualisierung der verwalteten Richtlinien	Aktualisierungen der AmazonDataZonePreviewConsoleFullAccessverwalteten Richtlinie, die aus zusätzlichen `iam:GetPolicy` Berechtigungen besteht.	13. Juni 2023
Amazon DataZone hat begonnen, Änderungen zu verfolgen	Amazon DataZone hat damit begonnen, Änderungen an seinen AWS verwalteten Richtlinien nachzuverfolgen.	20. März 2023

IAM-Rollen für Amazon DataZone

Themen

- AmazonDataZoneProvisioningRole-<domainAccountId>
- AmazonDataZoneDomainExecutionRole
- AmazonDataZoneGlueAccess- <region>- <domainId>
- AmazonDataZoneRedshiftAccess- <region>- <domainId>
- AmazonDataZone<region>S3 Manage- - <domainId>
- AmazonDataZoneSageMakerManageAccessRole<region>- - <domainId>
- AmazonDataZoneSageMakerProvisioningRole-<domainAccountId>

AmazonDataZoneProvisioningRole-<domainAccountId>

Das `AmazonDataZoneProvisioningRole-<domainAccountId>` hat das `AmazonDataZoneRedshiftGlueProvisioningPolicy` angehängt. Diese Rolle gewährt Amazon DataZone die für die Zusammenarbeit mit AWS Glue und Amazon Redshift erforderlichen Berechtigungen.

In der Standardeinstellung `AmazonDataZoneProvisioningRole-<domainAccountId>` ist die folgende Vertrauensrichtlinie angehängt:

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Principal": {
        "Service": "datazone.amazonaws.com"
      },
      "Action": "sts:AssumeRole",
      "Condition": {
        "StringEquals": {
            "aws:SourceAccount": "{{domain_account}}"
        }
      }
    }
  ]
}
```

AmazonDataZoneDomainExecutionRole

Dem AmazonDataZoneDomainExecutionRoleist die AWS verwaltete Richtlinie AmazonDataZoneDomainExecutionRolePolicyangehängt. Amazon DataZone erstellt diese Rolle für Sie in Ihrem Namen. Für bestimmte Aktionen im Datenportal DataZone übernimmt Amazon diese Rolle in dem Konto, in dem die Rolle erstellt wurde, und überprüft, ob diese Rolle berechtigt ist, die Aktion auszuführen.

Die AmazonDataZoneDomainExecutionRoleRolle ist in der erforderlich AWS-Konto , die Ihre DataZone Amazon-Domain hostet. Diese Rolle wird automatisch für Sie erstellt, wenn Sie Ihre DataZone Amazon-Domain erstellen.

Die AmazonDataZoneDomainExecutionRoleStandardrolle hat die folgende Vertrauensrichtlinie.

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Principal": {
                "Service": "datazone.amazonaws.com"
            },
            "Action": [
                "sts:AssumeRole",
                "sts:TagSession"
            ],
            "Condition": {
                "StringEquals": {
                    "aws:SourceAccount": "{{source_account_id}}"
                },
                "ForAllValues:StringLike": {
                    "aws:TagKeys": [
                        "datazone*"
                    ]
                }
            }
        }
    ]
}
```

AmazonDataZoneGlueAccess- <region>- <domainId>

Die `AmazonDataZoneGlueAccess-<region>-<domainId>` Rolle ist `AmazonDataZoneGlueManageAccessRolePolicy` angehängt. Diese Rolle erteilt Amazon die DataZone Erlaubnis, AWS Glue-Daten im Katalog zu veröffentlichen. Es gibt Amazon auch die DataZone Erlaubnis, Zugriff auf veröffentlichte AWS Glue-Assets im Katalog zu gewähren oder den Zugriff zu widerrufen.

Mit der `AmazonDataZoneGlueAccess-<region>-<domainId>` Standardrolle ist die folgende Vertrauensrichtlinie verknüpft:

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Principal": {
        "Service": "datazone.amazonaws.com"
      },
      "Action": "sts:AssumeRole",
      "Condition": {
            "StringEquals": {
                "aws:SourceAccount": "{{domain_account}}"
            },
            "ArnEquals": {
                "aws:SourceArn": "arn:aws:datazone:{{region}}:
{{domain_account}}:domain/{{root_domain_id}}"
            }
        }
    }
  ]
}
```

AmazonDataZoneRedshiftAccess- <region>- <domainId>

Die `AmazonDataZoneRedshiftAccess-<region>-<domainId>` Rolle ist `AmazonDataZoneRedshiftManageAccessRolePolicy` angehängt. Diese Rolle gewährt Amazon die DataZone Erlaubnis, Amazon Redshift Redshift-Daten im Katalog zu veröffentlichen. Es gibt Amazon auch die DataZone Erlaubnis, Zugriff auf veröffentlichte Amazon Redshift- oder Amazon Redshift Serverless-Assets im Katalog zu gewähren oder den Zugriff zu widerrufen.

An die `AmazonDataZoneRedshiftAccess-<region>-<domainId>` Standardrolle ist die folgende Inline-Berechtigungsrichtlinie angehängt:

```
{
   "Version":"2012-10-17",
   "Statement":[
      {
         "Sid": "RedshiftSecretStatement",
         "Effect":"Allow",
```

```
         "Action":"secretsmanager:GetSecretValue",
         "Resource":"*",
         "Condition":{
            "StringEquals":{
               "secretsmanager:ResourceTag/AmazonDataZoneDomain":"{{domainId}}"
            }
         }
      }
   ]
}
```

Der Standardeinstellung `AmazonDataZoneRedshiftManageAccessRole<timestamp>` ist die folgende Vertrauensrichtlinie angehängt:

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Principal": {
        "Service": "datazone.amazonaws.com"
      },
      "Action": "sts:AssumeRole",
      "Condition": {
            "StringEquals": {
                "aws:SourceAccount": "{{domain_account}}"
            },
            "ArnEquals": {
                "aws:SourceArn": "arn:aws:datazone:{{region}}:
{{domain_account}}:domain/{{root_domain_id}}"
            }
        }
    }
  ]
}
```

AmazonDataZone<region>S3 Manage- - <domainId>

AmazonDataZoneS3Manage- <region>- <domainId>wird verwendet, wenn Amazon AWS Lake Formation DataZone anruft, um einen Amazon Simple Storage Service (Amazon S3) -Standort zu

registrieren. AWS Lake Formation übernimmt diese Rolle beim Zugriff auf die Daten an diesem Standort. Weitere Informationen finden Sie unter Anforderungen für Rollen, die zur Registrierung von Standorten verwendet werden.

Dieser Rolle ist die folgende Inline-Berechtigungsrichtlinie beigefügt.

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Sid": "LakeFormationDataAccessPermissionsForS3",
            "Effect": "Allow",
            "Action": [
                "s3:PutObject",
                "s3:GetObject",
                "s3:DeleteObject"
            ],
            "Resource": "*",
            "Condition": {
                "StringEquals": {
                    "aws:ResourceAccount": "{{accountId}}"
                }
            }
        },
        {
            "Sid": "LakeFormationDataAccessPermissionsForS3ListBucket",
            "Effect": "Allow",
            "Action": [
                "s3:ListBucket"
            ],
            "Resource": "*",
            "Condition": {
                "StringEquals": {
                    "aws:ResourceAccount": "{{accountId}}"
                }
            }
        },
        {
            "Sid": "LakeFormationDataAccessPermissionsForS3ListAllMyBuckets",
            "Effect": "Allow",
            "Action": [
                "s3:ListAllMyBuckets"
```

```
            ],
            "Resource": "arn:aws:s3:::*",
            "Condition": {
                "StringEquals": {
                    "aws:ResourceAccount": "{{accountId}}"
                }
            }
        },
        {
            "Sid": "LakeFormationExplicitDenyPermissionsForS3",
            "Effect": "Deny",
            "Action": [
                "s3:PutObject",
                "s3:GetObject",
                "s3:DeleteObject"
            ],
            "Resource": [
                "arn:aws:s3:::[[BucketNames]]/*"
            ],
            "Condition": {
                "StringEquals": {
                    "aws:ResourceAccount": "{{accountId}}"
                }
            }
        },
        {
            "Sid": "LakeFormationExplicitDenyPermissionsForS3ListBucket",
            "Effect": "Deny",
            "Action": [
                "s3:ListBucket"
            ],
            "Resource": [
                "arn:aws:s3:::[[BucketNames]]"
            ],
            "Condition": {
                "StringEquals": {
                    "aws:ResourceAccount": "{{accountId}}"
                }
            }
        }
    ]
}
```

An AmazonDataZone S3Manage- <region>- <domainId>ist die folgende Vertrauensrichtlinie angehängt:

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Sid": "TrustLakeFormationForDataLocationRegistration",
            "Effect": "Allow",
            "Principal": {
                "Service": "lakeformation.amazonaws.com"
            },
            "Action": "sts:AssumeRole",
            "Condition": {
                "StringEquals": {
                    "aws:SourceAccount": "{{source_account_id}}"
                }
            }
        }
    ]
}
```

AmazonDataZoneSageMakerManageAccessRole<region>- - <domainId>

Der `AmazonDataZoneSageMakerManageAccessRole` Rolle sind das `AmazonDataZoneSageMakerAccessAmazonDataZoneRedshiftManageAccessRolePolicy`, das und das `AmazonDataZoneGlueManageAccessRolePolicy` angehängte. Diese Rolle gewährt Amazon die DataZone Erlaubnis, Abonnements für Data Lake-, Data Warehouse- und Amazon Sagemaker-Assets zu veröffentlichen und zu verwalten.

Der `AmazonDataZoneSageMakerManageAccessRole` Rolle ist die folgende Inline-Richtlinie beigefügt:

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

```
         "Effect":"Allow",
         "Action":"secretsmanager:GetSecretValue",
         "Resource":"*",
         "Condition":{
            "StringEquals":{
               "secretsmanager:ResourceTag/AmazonDataZoneDomain":"{{domainId}}"
            }
         }
      }
   ]
}
```

Der `AmazonDataZoneSageMakerManageAccessRole` Rolle ist die folgende Vertrauensrichtlinie angehängt:

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Sid": "DatazoneTrustPolicyStatement",
      "Effect": "Allow",
      "Principal": {
        "Service":  ["datazone.amazonaws.com",
                    "sagemaker.amazonaws.com"]
      },
      "Action": "sts:AssumeRole",
      "Condition": {
            "StringEquals": {
                "aws:SourceAccount": "{{domain_account}}"
            },
            "ArnEquals": {
                "aws:SourceArn": "arn:aws:datazone:{{region}}:
{{domain_account}}:domain/{{root_domain_id}}"
            }
        }
    }
]
}
```

AmazonDataZoneSageMakerProvisioningRole-<domainAccountId>

Der `AmazonDataZoneSageMakerProvisioningRole` Rolle ist das `AmazonDataZoneSageMakerProvisioning` und das `AmazonDataZoneRedshiftGlueProvisioningPolicy` angehängt. Diese Rolle gewährt Amazon die für die Zusammenarbeit mit AWS Glue, Amazon Redshift und Amazon Sagemaker erforderlichen DataZone Berechtigungen.

Der `AmazonDataZoneSageMakerProvisioningRole` Rolle ist die folgende Inline-Richtlinie beigefügt:

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Sid": "SageMakerStudioTagOnCreate",
            "Effect": "Allow",
            "Action": [
                "sagemaker:AddTags"
            ],
            "Resource": "arn:aws:sagemaker:*:{{AccountId}}:*/*",
            "Condition": {
                "Null": {
                    "sagemaker:TaggingAction": "false"
                }
            }
        }
    ]
}
```

Der `AmazonDataZoneSageMakerProvisioningRole` Rolle ist die folgende Vertrauensrichtlinie angehängt:

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Sid": "DataZoneTrustPolicyStatement",
      "Effect": "Allow",
```

```
      "Principal": {
        "Service": "datazone.amazonaws.com"
      },
      "Action": "sts:AssumeRole",
      "Condition": {
        "StringEquals": {
            "aws:SourceAccount": "{{domain_account}}"
        }
      }
    }
  ]
}
```

Identitätsbasierte Rollen

Identitätsbasierte Richtlinien sind JSON-Berechtigungsrichtliniendokumente, die Sie einer Identität anfügen können, wie z. B. IAM-Benutzern, -Benutzergruppen oder -Rollen. Diese Richtlinien steuern, welche Aktionen die Benutzer und Rollen für welche Ressourcen und unter welchen Bedingungen ausführen können. Informationen zum Erstellen identitätsbasierter Richtlinien finden Sie unter Erstellen von IAM-Richtlinien im IAM-Benutzerhandbuch.

Mit identitätsbasierten IAM-Richtlinien können Sie angeben, welche Aktionen und Ressourcen zugelassen oder abgelehnt werden. Darüber hinaus können Sie die Bedingungen festlegen, unter denen Aktionen zugelassen oder abgelehnt werden. Sie können den Prinzipal nicht in einer identitätsbasierten Richtlinie angeben, da er für den Benutzer oder die Rolle gilt, dem er zugeordnet ist. Informationen zu sämtlichen Elementen, die Sie in einer JSON-Richtlinie verwenden, finden Sie in der IAM-Referenz für JSON-Richtlinienelemente im IAM-Benutzerhandbuch.

Wenn Sie ein DataZone Amazon-Projekt erstellen, werden im Portal drei IAM-Rollen für dieses Projekt erstellt, eine für jeden Rollentyp des Projektmitglieds: Eigentümer und Mitwirkender. Die jeder Rolle zugewiesenen Berechtigungen hängen von der Projektrolle ab, und die zugehörigen Berechtigungsrichtlinien hängen von den Funktionen ab, mit denen das Projekt bereitgestellt wird.

Damit Amazon DataZone Berechtigungen verwalten und Ressourcen mit Abonnentenprojekten teilen kann, werden die Benutzerrollen für Abonnentenprojekte automatisch als Data Lake-Administrator AWS Lake Formation in dem Bereich hinzugefügt AWS-Konto , der Assets veröffentlicht.

Sie können die meisten up-to-date Versionen der Rolle in der AWS IAM-Managementkonsole einsehen oder sich die verschiedenen Rollenberechtigungen in der folgenden Tabelle ansehen.

Berechtigungen des Projektinhabers

Umgebungstyp	IAM-Berechtigungen
Standard-Data Lake	Dies ist die Kombination der Funktionen Essential, Data Lake Producer und Data Lake Consumer.
Essenziell	{ "Version": "2012-10-17", "Statement": [{ "Effect": "Allow", "Action": ["s3:List*", "s3:Get*", "s3:Describe*", "s3:DeleteObjectVersion", "s3:RestoreObject", "s3:ReplicateObject", "s3:PutObject", "s3:AbortMultipartUpload", "s3:PutObjectRetention", "s3:DeleteObject"], "Resource": ["s3BucketArn", "s3BucketArn/*"] }, { "Action": ["s3:List*"], "Resource": "*", "Effect": "Allow" }, {

Umgebungstyp	IAM-Berechtigungen	

```
      "Action": [
        "kms:List*",
        "kms:Get*",
        "kms:Desc
ribe*",
        "kms:Decrypt",
        "kms:Encrypt",
        "kms:ReEn
crypt*",
        "kms:Verify",
        "kms:Sign",
        "kms:Gene
rateDataKey"
      ],
      "Resource":
 "keyArn",
      "Effect": "Allow"
    },
    {
      "Action":
 ["kms:ListKeys",
 "kms:ListAliases"],
      "Resource": "*",
      "Effect": "Allow"
    },
    {
      "Action": [
        "ec2:Desc
ribeSecurityGroups",
        "ec2:Desc
ribeSecurityGroupR
ules",
        "ec2:Desc
ribeTags"
      ],
      "Resource": "*",
      "Effect": "Allow"
    },
    {
      "Action": [
        "logs:Des
cribe*",
```

Umgebungstyp	IAM-Berechtigungen	

```
        "logs:Sta
rtQuery",
        "logs:Sto
pQuery",
        "logs:Get*",
        "logs:List*",
        "logs:Put
LogEvents",
        "logs:Cre
ateLogStream",
        "logs:Fil
terLogEvents"
      ],
      "Resource":
 "arn:aws:logs:regi
on:account-id:log-
group:log-group-na
me:*",
      "Effect": "Allow"
    },
    {
      "Effect": "Allow",
      "Action": [
        "s3:Get*",
        "s3:List*",
        "kms:List*",
        "kms:Get*",
        "kms:Desc
ribe*",
        "kms:Decrypt"
      ],
      "Resource": "*",
      "Condition": {
        "StringNo
tEquals": {
          "aws:Reso
urceAccount":
 "project-account-id"
        }
      }
    }
  ]
```

Umgebungstyp	IAM-Berechtigungen	
	}]	

Umgebungstyp	IAM-Berechtigungen
Data Lake-Produzent	{ "Version": "2012-10-17", "Statement": [{ "Effect": "Allow", "Action": ["glue:BatchGet*", "glue:Get*", "glue:SearchTables", "glue:List*", "glue:BatchCreatePartition", "glue:CreatePartitionIndex", "glue:CreateTable", "glue:BatchUpdatePartition", "glue:BatchDeletePartition", "glue:UpdateTable", "glue:DeleteTableVersion", "glue:DeleteTable", "glue:DeleteColumn

Umgebungstyp	IAM-Berechtigungen	

```
StatisticsForParti
tion",

 "glue:DeleteColumn
StatisticsForTable",

 "glue:DeletePartit
ionIndex",

 "glue:UpdateColumn
StatisticsForParti
tion",

 "glue:UpdateColumn
StatisticsForTable",

 "glue:BatchDeleteT
ableVersion",

 "glue:BatchDeleteT
able",

 "glue:CreatePartit
ion",

 "glue:DeletePartit
ion",

 "glue:UpdatePartit
ion"
            ],
            "Resource":
 [

 "arn:aws:glue:regi
on:account:database/
dbName",

 "arn:aws:glue:regi
on:account:catalog",

 "arn:aws:glue:regi
```

Umgebungstyp	IAM-Berechtigungen	

```
on:account:table/d
bName/*"
            ]
        },
        {
            "Sid":
 "VisualEditor0",
            "Effect":
 "Allow",
            "Action": [

 "glue:SearchTables",

 "glue:NotifyEvent",

 "glue:StartBluepri
ntRun",

 "glue:PutWorkflowR
unProperties",

 "glue:StopCrawler",

 "glue:DeleteJob",

 "glue:DeleteWorkfl
ow",

 "glue:UpdateCrawler",

 "glue:DeleteBluepr
int",

 "glue:UpdateWorkfl
ow",

 "glue:StartCrawler",

 "glue:ResetJobBook
mark",

 "glue:UpdateJob",
```

Umgebungstyp	IAM-Berechtigungen	

```
 "glue:StartWorkflo
wRun",

 "glue:StopCrawlerS
chedule",

 "glue:ResumeWorkfl
owRun",

 "glue:List*",

 "glue:DeleteCrawler",

 "glue:UpdateBluepr
int",

 "glue:BatchStopJob
Run",

 "glue:StopWorkflow
Run",

 "glue:BatchGet*",

 "glue:UpdateCrawle
rSchedule",

 "glue:DeleteConnec
tion",

 "glue:UpdateConnec
tion",

 "glue:Get*",

 "glue:BatchDeleteC
onnection",

 "glue:StartCrawler
Schedule",
```

Umgebungstyp	IAM-Berechtigungen	

```
 "glue:StartJobRun",

 "glue:CreateWorkfl
ow",

 "glue:PublishDataQ
uality",

 "glue:*DataQuality*"
            ],
            "Resource":
 "*",
            "Conditio
n": {

 "ForAnyValue:Strin
gEquals": {

 "aws:ResourceTag/n
oah-analytics:proj
ectId": "projectId"
                }
            }
        },
        {
            "Sid":
 "CreateGlueResourc
es",
            "Effect":
 "Allow",
            "Action": [

 "glue:CreateBluepr
int",

 "glue:CreateJob",

 "glue:CreateConnec
tion",

 "glue:CreateCrawler",
```

Umgebungstyp	IAM-Berechtigungen	

```
 "glue:CreateDataQu
alityRuleset"
            ],
            "Resource":
 "*"
        },
        {
            "Sid":
 "VisualEditor0",
            "Effect":
 "Allow",
            "Action": [

 "iam:ListRoles",

 "iam:ListUsers",

 "iam:ListGroups",

 "iam:ListRolePolic
ies",

 "iam:GetRole",

 "iam:GetRolePolicy"
            ],
            "Resource":
 "*"
        }
    ]
}
```

Umgebungstyp	IAM-Berechtigungen	
Data Lake-Verbraucher	{ "Version": "2012-10-17", "Statement": [{ "Effect": "Allow", "Action": ["athena:TerminateSession", "athena:CreatePreparedStatement", "athena:StopCalculationExecution", "athena:StartQueryExecution", "athena:UpdatePreparedStatement", "athena:BatchGet*", "athena:UpdateNotebook", "athena:DeleteNotebook", "athena:DeletePreparedStatement", "athena:UpdateNotebookMetadata", "athena:DeleteNamedQuery", "athena:Get*", "athena:UpdateNamedQuery", "athena:CreateNamedQuery",	

Umgebungstyp	IAM-Berechtigungen	

```
        "athena:E
xportNotebook",
        "athena:S
topQueryExecution",
        "athena:S
tartCalculationExe
cution",
        "athena:S
tartSession",
        "athena:C
reatePresignedNote
bookUrl",
        "athena:C
reateNotebook",
        "athena:I
mportNotebook"
      ],
      "Resource": [
        "arn:aws:
athena:region:acco
unt-id:workgroup/w
orkGroupName",
        "arn:aws:
athena:region:acco
unt-id:datacatalog/
AwsDataCatalog"
      ]
    },
    {
      "Effect": "Allow",
      "Action": [
        "athena:L
istWorkGroups",
        "athena:L
istDataCatalogs",
        "athena:List*"
      ],
      "Resource": ["*"]
    },
    {
      "Effect": "Allow",
      "Action": [
```

Umgebungstyp	IAM-Berechtigungen	

```
        "glue:Bat
chGet*",
        "glue:Get*",
        "glue:Sea
rchTables",
        "glue:List*"
      ],
      "Resource": [
        "arn:aws:
glue:region:account-
id:database/dbName",
        "arn:aws:
glue:region:account-
id:catalog",
        "arn:aws:
glue:region:account-
id:table/dbName/*"
      ]
    }
  ]
}
```

Umgebungstyp	IAM-Berechtigungen

Data Warehouse-Hersteller	{
	  "Version": "2012-10-17",
	  "Statement": [
	    {
	      "Effect": "Allow",
	      "Action": [
	        "redshift:GetClusterCredentials",
	        "redshift:JoinGroup",
	        "redshift:CreateClusterUser",
	        "redshift:DescribeClusters"
	      ],
	      "Resource": "arn:aws:redshift:region:account:cluster:producerRedshiftCluster"
	    },
	    {
	      "Effect": "Allow",
	      "Action": [
	        "redshift-data:DescribeStatement",
	        "redshift-data:ExecuteStatement"
	      ],
	      "Resource": "arn:aws:redshift:region:account:cluster:producerRedshiftCluster"
	    }
	  ]
	}

Umgebungstyp	IAM-Berechtigungen	

Umgebungstyp	IAM-Berechtigungen

Data Warehouse-Nutzer	{
	  "Version": "2012-10-17",
	  "Statement": [
	  {
	  "Effect": "Allow",
	  "Action": [
	  "redshift:GetClusterCredentials",
	  "redshift:JoinGroup",
	  "redshift:CreateClusterUser",
	  "redshift:DescribeClusters"
	  ],
	  "Resource": [
	  "arn:aws:redshift:region:account:dbuser:cluster-identifier/dbUser",
	  "arn:aws:redshift:region:account:dbgroup:cluster-identifier/project_owner@projectName",
	  "arn:aws:redshift:region:account:dbname:cluster-identifier/*"
	  ],
	  "Condition": {
	  "ForAnyValue:StringEquals": {
	  "aws:PrincipalTag/RedshiftDbUser": "dbUser"
	  }

Umgebungstyp	IAM-Berechtigungen	

```
      }
    },
    {
      "Sid": "VisualEd
itor2",
      "Effect": "Allow",
      "Action": [
        "redshift-
data:DescribeStat
ement",
        "redshift-
data:ExecuteStatement"
      ],
      "Resource":
 "arn:aws:redshift:
region:account-id:
cluster:cluster-id
entifier"
    }
  ]
}
```

Umgebungstyp	IAM-Berechtigungen

Amazon-Redshift-Abfrage-Editor v2	{
	  "Version": "2012-10-17",
	  "Statement": [
	    {
	      "Action": "redshift:DescribeClusters",
	      "Effect": "Allow",
	      "Resource": "arn:aws:redshift:region:account-id:cluster:*",
	      "Sid": "RedshiftPermissions"
	    },
	    {
	      "Action": "tag:GetResources",
	      "Condition": {
	        "StringEquals": { "aws:CalledViaLast": "sqlworkbench.amazonaws.com" }
	      },
	      "Effect": "Allow",
	      "Resource": "*",
	      "Sid": "ResourceGroupsTaggingPermissions"
	    },
	    {
	      "Action": [
	        "sqlworkbench:DriverExecute",
	        "sqlworkbench:GenerateSession",

Umgebungstyp	IAM-Berechtigungen	

```
        "sqlworkb
ench:ListConnectio
ns",
        "sqlworkb
ench:ListDatabases",
        "sqlworkb
ench:ListFiles",
        "sqlworkb
ench:ListNotebooks",
        "sqlworkb
ench:ListQueryExec
utionHistory",
        "sqlworkb
ench:ListRedshiftC
lusters",
        "sqlworkb
ench:ListSampleDat
abases",
        "sqlworkb
ench:ListTabs",
        "sqlworkb
ench:ListTaggedRes
ources"
      ],
      "Effect": "Allow",
      "Resource": "*",
      "Sid": "AmazonRe
dshiftQueryEditorV
2PermissionsPart1"
    },
    {
      "Action":
 "sqlworkbench:*",
      "Effect": "Allow",
      "Resource": [
        "arn:aws:
sqlworkbench:regio
n:account-id:query/
*",
        "arn:aws:
sqlworkbench:regio
```

Umgebungstyp	IAM-Berechtigungen
	n:account-id:notebook/*", "arn:aws:sqlworkbench:region:account-id:connection/*", "arn:aws:sqlworkbench:region:account-id:chart/*", "arn:aws:sqlworkbench:region:account-id:/*"], "Sid": "AmazonRedshiftQueryEditorV2PermissionsPart2" }] }

Berechtigungen für Projektmitwirkende

Umgebungstyp	IAM-Berechtigungen
Standard-Data Lake	Dies ist die Kombination der Funktionen Essential, Data Lake Producer und Data Lake Consumer.
Essenziell	{ "Version": "2012-10-17", "Statement": [{ "Effect": "Allow",

Umgebungstyp	IAM-Berechtigungen	

```
      "Action": [
        "s3:List*",
        "s3:Get*",
        "s3:Describe*",
        "s3:Delet
eObjectVersion",
        "s3:Resto
reObject",
        "s3:Repli
cateObject",
        "s3:PutObject",
        "s3:Abort
MultipartUpload",
        "s3:PutOb
jectRetention",
        "s3:Delet
eObject"
      ],
      "Resource":
 ["s3BucketArn",
 "s3BucketArn/*"]
    },
    { "Action":
 ["s3:List*"],
 "Resource": "*",
 "Effect": "Allow" },
    {
      "Action": [
        "kms:List*",
        "kms:Get*",
        "kms:Desc
ribe*",
        "kms:Decrypt",
        "kms:Encrypt",
        "kms:ReEn
crypt*",
        "kms:Verify",
        "kms:Sign",
        "kms:Gene
rateDataKey"
      ],
```

Umgebungstyp	IAM-Berechtigungen	

```
      "Resource":
 "keyArn",
      "Effect": "Allow"
    },
    {
      "Action":
 ["kms:ListKeys",
 "kms:ListAliases"],
      "Resource": "*",
      "Effect": "Allow"
    },
    {
      "Action": [
        "ec2:Desc
ribeSecurityGroups",
        "ec2:Desc
ribeSecurityGroupR
ules",
        "ec2:Desc
ribeTags"
      ],
      "Resource": "*",
      "Effect": "Allow"
    },
    {
      "Action": [
        "logs:Des
cribe*",
        "logs:Sta
rtQuery",
        "logs:Sto
pQuery",
        "logs:Get*",
        "logs:List*",
        "logs:Put
LogEvents",
        "logs:Cre
ateLogStream",
        "logs:Fil
terLogEvents"
      ],
```

Umgebungstyp	IAM-Berechtigungen	

```
      "Resource":
 "arn:aws:logs:regi
on:account-id:log-
group:log-group-na
me:*",
      "Effect": "Allow"
    },
    {
      "Effect": "Allow",
      "Action": [
        "s3:Get*",
        "s3:List*",
        "kms:List*",
        "kms:Get*",
        "kms:Desc
ribe*",
        "kms:Decrypt"
      ],
      "Resource": "*",
      "Condition": {
        "StringNo
tEquals": {
          "aws:Reso
urceAccount":
 "project-account-id"
        }
      }
    }
  ]
}
```

Umgebungstyp	IAM-Berechtigungen
Data Lake-Produzent	{ "Version": "2012-10-17", "Statement": [{ "Effect": "Allow", "Action": ["glue:BatchGet*", "glue:Get*", "glue:SearchTables", "glue:List*", "glue:BatchCreatePartition", "glue:CreatePartitionIndex", "glue:CreateTable", "glue:BatchUpdatePartition", "glue:BatchDeletePartition", "glue:UpdateTable", "glue:DeleteTableVersion", "glue:DeleteTable", "glue:DeleteColumnStatisticsForPartition", "glue:DeleteColumnStatisticsForTable", "glue:DeletePartitionIndex", "glue:UpdateColumnStatisticsForPartition",

Umgebungstyp	IAM-Berechtigungen	

```
        "glue:Upd
ateColumnStatistic
sForTable",
        "glue:Bat
chDeleteTableVersi
on",
        "glue:Bat
chDeleteTable",
        "glue:Cre
atePartition",
        "glue:Del
etePartition",
        "glue:Upd
atePartition"
      ],
      "Resource": [
        "arn:aws:
glue:region:accoun
t:database/dbName",
        "arn:aws:
glue:region:accoun
t:catalog",
        "arn:aws:
glue:region:accoun
t:table/dbName/*"
      ]
    },
    {
      "Sid": "VisualEd
itor0",
      "Effect": "Allow",
      "Action": [
        "glue:Sea
rchTables",
        "glue:Not
ifyEvent",
        "glue:Sta
rtBlueprintRun",
        "glue:Put
WorkflowRunPropert
ies",
```

Umgebungstyp	IAM-Berechtigungen	

```
        "glue:Sto
pCrawler",
        "glue:Del
eteJob",
        "glue:Del
eteWorkflow",
        "glue:Upd
ateCrawler",
        "glue:Del
eteBlueprint",
        "glue:Upd
ateWorkflow",
        "glue:Sta
rtCrawler",
        "glue:Res
etJobBookmark",
        "glue:Upd
ateJob",
        "glue:Sta
rtWorkflowRun",
        "glue:Sto
pCrawlerSchedule",
        "glue:Res
umeWorkflowRun",
        "glue:List*",
        "glue:Del
eteCrawler",
        "glue:Upd
ateBlueprint",
        "glue:Bat
chStopJobRun",
        "glue:Sto
pWorkflowRun",
        "glue:Bat
chGet*",
        "glue:Upd
ateCrawlerSchedule",
        "glue:Del
eteConnection",
        "glue:Upd
ateConnection",
        "glue:Get*",
```

Umgebungstyp	IAM-Berechtigungen	

```
        "glue:Bat
chDeleteConnection",
        "glue:Sta
rtCrawlerSchedule",
        "glue:Sta
rtJobRun",
        "glue:Cre
ateWorkflow",
        "glue:Pub
lishDataQuality",
        "glue:*Da
taQuality*"
      ],
      "Resource": "*",
      "Condition": {
        "ForAnyVa
lue:StringEquals": {
          "aws:Reso
urceTag/noah-analy
tics:projectId":
 "projectId"
        }
      }
    },
    {
      "Sid": "CreateGl
ueResources",
      "Effect": "Allow",
      "Action": [
        "glue:Cre
ateBlueprint",
        "glue:Cre
ateJob",
        "glue:Cre
ateConnection",
        "glue:Cre
ateCrawler",
        "glue:Cre
ateDataQualityRule
set"
      ],
      "Resource": "*"
```

Umgebungstyp	IAM-Berechtigungen	

```
    },
    {
      "Sid": "VisualEd
itor0",
      "Effect": "Allow",
      "Action": [
        "iam:List
Roles",
        "iam:List
Users",
        "iam:List
Groups",
        "iam:List
RolePolicies",
        "iam:GetRole",
        "iam:GetR
olePolicy"
      ],
      "Resource": "*"
    }
  ]
}
```

Umgebungstyp	IAM-Berechtigungen

Data Lake-Verbraucher	{
	  "Version": "2012-10-17",
	  "Statement": [
	  {
	  "Effect": "Allow",
	  "Action": [
	  "athena:TerminateSession",
	  "athena:CreatePreparedStatement",
	  "athena:StopCalculationExecution",
	  "athena:StartQueryExecution",
	  "athena:UpdatePreparedStatement",
	  "athena:BatchGet*",
	  "athena:UpdateNotebook",
	  "athena:DeleteNotebook",
	  "athena:DeletePreparedStatement",
	  "athena:UpdateNotebookMetadata",
	  "athena:DeleteNamedQuery",
	  "athena:Get*",
	  "athena:UpdateNamedQuery",
	  "athena:CreateNamedQuery",

Umgebungstyp	IAM-Berechtigungen	

```
        "athena:E
xportNotebook",
        "athena:S
topQueryExecution",
        "athena:S
tartCalculationExe
cution",
        "athena:S
tartSession",
        "athena:C
reatePresignedNote
bookUrl",
        "athena:C
reateNotebook",
        "athena:I
mportNotebook"
      ],
      "Resource": [
        "arn:aws:
athena:region:acco
unt-id:workgroup/w
orkGroupName",
        "arn:aws:
athena:region:acco
unt-id:datacatalog/
AwsDataCatalog"
      ]
    },
    {
      "Effect": "Allow",
      "Action": [
        "athena:L
istWorkGroups",
        "athena:L
istDataCatalogs",
        "athena:List*"
      ],
      "Resource": ["*"]
    },
    {
      "Effect": "Allow",
      "Action": [
```

Umgebungstyp	IAM-Berechtigungen	

```
        "glue:Bat
chGet*",
        "glue:Get*",
        "glue:Sea
rchTables",
        "glue:List*"
      ],
      "Resource": [
        "arn:aws:
glue:region:account-
id:database/dbName",
        "arn:aws:
glue:region:account-
id:catalog",
        "arn:aws:
glue:region:account-
id:table/dbName/*"
      ]
    }
  ]
}
```

Umgebungstyp	IAM-Berechtigungen

Data Warehouse-Hersteller	{
	  "Version": "2012-10-17",
	  "Statement": [
	    {
	      "Effect": "Allow",
	      "Action": [
	        "redshift:GetClusterCredentials",
	        "redshift:JoinGroup",
	        "redshift:CreateClusterUser",
	        "redshift:DescribeClusters"
	      ],
	      "Resource": "arn:aws:redshift:region:account:cluster:producerRedshiftCluster"
	    },
	    {
	      "Effect": "Allow",
	      "Action": [
	        "redshift-data:DescribeStatement",
	        "redshift-data:ExecuteStatement"
	      ],
	      "Resource": "arn:aws:redshift:region:account:cluster:producerRedshiftCluster"
	    }
	  ]
	}

Umgebungstyp	IAM-Berechtigungen	

Umgebungstyp	IAM-Berechtigungen

Data Warehouse-Nutzer	{
	"Version": "2012-10-17",
	"Statement": [
	{
	"Effect": "Allow",
	"Action": [
	"redshift:GetClusterCredentials",
	"redshift:JoinGroup",
	"redshift:CreateClusterUser",
	"redshift:DescribeClusters"
	],
	"Resource": [
	"arn:aws:redshift:region:account:dbuser:cluster-identifier/dbUser",
	"arn:aws:redshift:region:account:dbgroup:cluster-identifier/project_owner@projectName",
	"arn:aws:redshift:region:account:dbname:cluster-identifier/*"
	],
	"Condition": {
	"ForAnyValue:StringEquals": {
	"aws:PrincipalTag/RedshiftDbUser": "dbUser"
	}

Umgebungstyp	IAM-Berechtigungen	

```
      }
    },
    {
      "Sid": "VisualEd
itor2",
      "Effect": "Allow",
      "Action": [
        "redshift-
data:DescribeStat
ement",
        "redshift-
data:ExecuteStatement"
      ],
      "Resource":
 "arn:aws:redshift:
region:account-id:
cluster:cluster-id
entifier"
    }
  ]
}
```

Umgebungstyp	IAM-Berechtigungen

Amazon-Redshift-Abfrage-Editor v2	{
	  "Version": "2012-10-17",
	  "Statement": [
	    {
	      "Action": "redshift:DescribeClusters",
	      "Effect": "Allow",
	      "Resource": "arn:aws:redshift:region:account-id:cluster:*",
	      "Sid": "RedshiftPermissions"
	    },
	    {
	      "Action": "tag:GetResources",
	      "Condition": {
	        "StringEquals": { "aws:CalledViaLast": "sqlworkbench.amazonaws.com" }
	      },
	      "Effect": "Allow",
	      "Resource": "*",
	      "Sid": "ResourceGroupsTaggingPermissions"
	    },
	    {
	      "Action": [
	        "sqlworkbench:DriverExecute",
	        "sqlworkbench:GenerateSession",

Umgebungstyp	IAM-Berechtigungen	

```
        "sqlworkb
ench:ListConnectio
ns",
        "sqlworkb
ench:ListDatabases",
        "sqlworkb
ench:ListFiles",
        "sqlworkb
ench:ListNotebooks",
        "sqlworkb
ench:ListQueryExec
utionHistory",
        "sqlworkb
ench:ListRedshiftC
lusters",
        "sqlworkb
ench:ListSampleDat
abases",
        "sqlworkb
ench:ListTabs",
        "sqlworkb
ench:ListTaggedRes
ources"
      ],
      "Effect": "Allow",
      "Resource": "*",
      "Sid": "AmazonRe
dshiftQueryEditorV
2PermissionsPart1"
    },
    {
      "Action":
 "sqlworkbench:*",
      "Effect": "Allow",
      "Resource": [
        "arn:aws:
sqlworkbench:regio
n:account-id:query/
*",
        "arn:aws:
sqlworkbench:regio
```

Umgebungstyp	IAM-Berechtigungen	

```
n:account-id:noteb
ook/*",
        "arn:aws:
sqlworkbench:regio
n:account-id:conne
ction/*",
        "arn:aws:
sqlworkbench:regio
n:account-id:chart/
*",
        "arn:aws:
sqlworkbench:regio
n:account-id:/*"
      ],
      "Sid": "AmazonRe
dshiftQueryEditorV
2PermissionsPart2"
    }
  ]
}
```

Temporäre Anmeldeinformationen

Einige AWS Dienste funktionieren nicht, wenn Sie sich mit temporären Anmeldeinformationen anmelden. Weitere Informationen, einschließlich der AWS Dienste, die mit temporären Anmeldeinformationen funktionieren, finden Sie im IAM-Benutzerhandbuch unter AWS Dienste, die mit IAM funktionieren.

Sie verwenden temporäre Anmeldeinformationen, wenn Sie sich mit einer anderen AWS Management Console Methode als einem Benutzernamen und einem Passwort bei der Anmeldung anmelden. Wenn Sie beispielsweise AWS über den Single Sign-On-Link (SSO) Ihres Unternehmens darauf zugreifen, werden bei diesem Vorgang automatisch temporäre Anmeldeinformationen erstellt. Sie erstellen auch automatisch temporäre Anmeldeinformationen, wenn Sie sich als Benutzer bei der Konsole anmelden und dann die Rollen wechseln. Weitere Informationen zum Wechseln von Rollen finden Sie unter Wechseln zu einer Rolle (Konsole) im IAM-Benutzerhandbuch.

Mithilfe der AWS API AWS CLI oder können Sie temporäre Anmeldeinformationen manuell erstellen. Sie können diese temporären Anmeldeinformationen dann für den Zugriff verwenden AWS. AWS empfiehlt, temporäre Anmeldeinformationen dynamisch zu generieren, anstatt langfristige Zugriffsschlüssel zu verwenden. Weitere Informationen finden Sie unter Temporäre Sicherheitsanmeldeinformationen in IAM.

Prinzipal-Berechtigungen

Wenn Sie einen IAM-Benutzer oder eine IAM-Rolle verwenden, um Aktionen auszuführen AWS, gelten Sie als Principal. Richtlinien erteilen einem Prinzipal-Berechtigungen. Bei einigen Services könnte es Aktionen geben, die dann eine andere Aktion in einem anderen Service auslösen. In diesem Fall müssen Sie über Berechtigungen zum Ausführen beider Aktionen verfügen. Informationen darüber, ob für eine Aktion zusätzliche abhängige Aktionen in einer Richtlinie erforderlich sind, finden Sie unter Aktionen, Ressourcen und Bedingungsschlüssel für AWS Documentation Essentials in der Serviceautorisierungsreferenz.

Konformitätsvalidierung für Amazon DataZone

Informationen darüber, ob AWS-Service ein AWS-Services in den Geltungsbereich bestimmter Compliance-Programme fällt, finden Sie unter Umfang nach Compliance-Programm AWS-Services unter . Wählen Sie dort das Compliance-Programm aus, an dem Sie interessiert sind. Allgemeine Informationen finden Sie unter AWS Compliance-Programme AWS .

Sie können Prüfberichte von Drittanbietern unter herunterladen AWS Artifact. Weitere Informationen finden Sie unter Berichte herunterladen unter .

Ihre Verantwortung für die Einhaltung der Vorschriften bei der Nutzung AWS-Services hängt von der Vertraulichkeit Ihrer Daten, den Compliance-Zielen Ihres Unternehmens und den geltenden Gesetzen und Vorschriften ab. AWS stellt die folgenden Ressourcen zur Verfügung, die Sie bei der Einhaltung der Vorschriften unterstützen:

- Schnellstartanleitungen zu Sicherheit und Compliance — In diesen Bereitstellungsleitfäden werden architektonische Überlegungen erörtert und Schritte für die Implementierung von Basisumgebungen beschrieben AWS , bei denen Sicherheit und Compliance im Mittelpunkt stehen.
- Architecting for HIPAA Security and Compliance on Amazon Web Services — In diesem Whitepaper wird beschrieben, wie Unternehmen HIPAA-fähige Anwendungen erstellen AWS können.

> **Note**
>
> AWS-Services Nicht alle sind HIPAA-fähig. Weitere Informationen finden Sie in der Referenz für HIPAA-berechtigte Services.

- AWS Compliance-Ressourcen — Diese Sammlung von Arbeitsmappen und Leitfäden gilt möglicherweise für Ihre Branche und Ihren Standort.
- AWS Leitfäden zur Einhaltung von Vorschriften für Kunden — Verstehen Sie das Modell der gemeinsamen Verantwortung aus dem Blickwinkel der Einhaltung von Vorschriften. In den Leitfäden werden die bewährten Verfahren zur Sicherung zusammengefasst AWS-Services und die Leitlinien den Sicherheitskontrollen in verschiedenen Frameworks (einschließlich des National Institute of Standards and Technology (NIST), des Payment Card Industry Security Standards Council (PCI) und der International Organization for Standardization (ISO)) zugeordnet.
- Evaluierung von Ressourcen anhand von Regeln im AWS Config Entwicklerhandbuch — Der AWS Config Service bewertet, wie gut Ihre Ressourcenkonfigurationen den internen Praktiken, Branchenrichtlinien und Vorschriften entsprechen.
- AWS Security Hub— Auf diese AWS-Service Weise erhalten Sie einen umfassenden Überblick über Ihren internen Sicherheitsstatus. AWS Security Hub verwendet Sicherheitskontrollen, um Ihre AWS -Ressourcen zu bewerten und Ihre Einhaltung von Sicherheitsstandards und bewährten Methoden zu überprüfen. Eine Liste der unterstützten Services und Kontrollen finden Sie in der Security-Hub-Steuerungsreferenz.
- Amazon GuardDuty — Dies AWS-Service erkennt potenzielle Bedrohungen für Ihre Workloads AWS-Konten, Container und Daten, indem es Ihre Umgebung auf verdächtige und böswillige Aktivitäten überwacht. GuardDuty kann Ihnen helfen, verschiedene Compliance-Anforderungen wie PCI DSS zu erfüllen, indem es die in bestimmten Compliance-Frameworks vorgeschriebenen Anforderungen zur Erkennung von Eindringlingen erfüllt.
- AWS Audit Manager— Auf diese AWS-Service Weise können Sie Ihre AWS Nutzung kontinuierlich überprüfen, um das Risikomanagement und die Einhaltung von Vorschriften und Industriestandards zu vereinfachen.

Bewährte Sicherheitsmethoden für Amazon DataZone

Amazon DataZone bietet eine Reihe von Sicherheitsfunktionen, die Sie bei der Entwicklung und Implementierung Ihrer eigenen Sicherheitsrichtlinien berücksichtigen sollten. Die folgenden bewährten Methoden sind allgemeine Richtlinien und keine vollständige Sicherheitslösung. Da diese

bewährten Methoden für Ihre Umgebung möglicherweise nicht angemessen oder ausreichend sind, sollten Sie sie als hilfreiche Überlegungen und nicht als bindend ansehen.

Implementieren des Zugriffs mit geringsten Berechtigungen

Bei der Erteilung von Berechtigungen entscheiden Sie, wer welche Berechtigungen für welche DataZone Amazon-Ressourcen erhält. Sie aktivieren die spezifischen Aktionen, die daraufhin für die betreffenden Ressourcen erlaubt sein sollen. Aus diesem Grund sollten Sie nur Berechtigungen gewähren, die zum Ausführen einer Aufgabe erforderlich sind. Die Implementierung der geringstmöglichen Zugriffsrechte ist eine grundlegende Voraussetzung zum Reduzieren des Sicherheitsrisikos und der Auswirkungen, die aufgrund von Fehlern oder böswilligen Absichten entstehen könnten.

Verwenden von IAM-Rollen

Hersteller- und Kundenanwendungen müssen über gültige Anmeldeinformationen verfügen, um auf DataZone Amazon-Ressourcen zugreifen zu können. Sie sollten AWS Anmeldeinformationen nicht direkt in einer Client-Anwendung oder in einem Amazon S3 S3-Bucket speichern. Dabei handelt es sich um langfristige Anmeldeinformationen, die nicht automatisch rotiert werden und bedeutende geschäftliche Auswirkungen haben könnten, wenn sie kompromittiert werden.

Stattdessen sollten Sie eine IAM-Rolle verwenden, um temporäre Anmeldeinformationen für Ihre Produzenten- und Kundenanwendungen für den Zugriff auf DataZone Amazon-Ressourcen zu verwalten. Wenn Sie eine Rolle verwenden, müssen Sie keine langfristigen Anmeldeinformationen (z. B. Benutzername und Passwort oder Zugriffsschlüssel) für den Zugriff auf andere Ressourcen verwenden.

Weitere Informationen finden Sie unter folgenden Themen im IAM-Benutzerhandbuch:

- IAM-Rollen
- Gängige Szenarien für Rollen: Benutzer, Anwendungen und Services

Implementieren einer serverseitigen Verschlüsselung in abhängigen Ressourcen

Daten im Ruhezustand und Daten während der Übertragung können in Amazon verschlüsselt werden DataZone.

Wird CloudTrail zur Überwachung von API-Aufrufen verwendet

Amazon DataZone ist in einen Service integriert AWS CloudTrail, der eine Aufzeichnung der Aktionen bereitstellt, die von einem Benutzer, einer Rolle oder einem AWS Service bei Amazon ausgeführt wurden DataZone.

Anhand der von gesammelten Informationen können Sie die Anfrage CloudTrail, die an Amazon gestellt wurde DataZone, die IP-Adresse, von der aus die Anfrage gestellt wurde, wer die Anfrage gestellt hat, wann sie gestellt wurde, und weitere Details ermitteln.

Resilienz bei Amazon DataZone

Die AWS globale Infrastruktur basiert auf Availability AWS-Regionen Zones. AWS-Regionen bieten mehrere physisch getrennte und isolierte Availability Zones, die über Netzwerke mit niedriger Latenz, hohem Durchsatz und hoher Redundanz miteinander verbunden sind. Mithilfe von Availability Zones können Sie Anwendungen und Datenbanken erstellen und ausführen, die automatisch Failover zwischen Zonen ausführen, ohne dass es zu Unterbrechungen kommt. Availability Zones sind besser verfügbar, fehlertoleranter und skalierbarer als herkömmliche Infrastrukturen mit einem oder mehreren Rechenzentren.

Weitere Informationen zu Availability Zones AWS-Regionen und Availability Zones finden Sie unter AWS Globale Infrastruktur.

Zusätzlich zur AWS globalen Infrastruktur DataZone bietet Amazon mehrere Funktionen, um Ihre Datenstabilität und Backup-Anforderungen zu erfüllen.

Themen

- Resilienz von Datenquellen
- Resilienz von Anlagen
- Asset-Typ und Metadaten sorgen für Resilienz
- Glossar: Resilienz
- Resilienz bei der globalen Suche
- Resilienz von Abonnements
- Widerstandsfähigkeit der Umwelt
- Umwelt, Blaupause, Resilienz

- Resilienz des Projekts
- RAM-Resilienz
- Resilienz der Benutzerprofilverwaltung
- Ausfallsicherheit von Domänen

Resilienz von Datenquellen

Während eines DataZone Verfügbarkeitsereignisses bei Amazon werden `DataSource` Jobs in regelmäßigen Abständen bis zu 24 Stunden lang wiederholt. Wenn ein Job aufgrund einer Fehlkonfiguration fehlschlägt, wird ein `DataSourceRunFailed` Ereignis ausgelöst. Wenn die DataZone Amazon-Domain mit einem KMS-Schlüssel konfiguriert ist und sie während einer Jobausführung den Zugriff auf diesen Schlüssel AmazonDataZoneDomainExecutionRole verliert, endet die Ausführung im `INACCESSIBLE` Status. Sobald der KMS-Zugriff wiederhergestellt ist, sollte der Job manuell aktualisiert werden, um den Übergang zurück in einen verwendbaren Zustand auszulösen.

Resilienz von Anlagen

In Amazon DataZone werden Assets versioniert. Wenn eine Version eines Assets zurückgesetzt werden muss, können Sie eine neue Version mit dem Inhalt der letzten stabilen Version erstellen. Eine Asset-Version kann veröffentlicht werden. Eine veröffentlichte Version eines Assets kann nicht bearbeitet werden, es sei denn, es wird eine neue Version veröffentlicht. Ein veröffentlichtes Asset (auch Listing genannt) kann abonniert werden. Um neue Abonnements für ein Asset zu verhindern, kann dessen Veröffentlichung rückgängig gemacht werden. Das Rückgängigmachen der Veröffentlichung eines Assets hat keine Auswirkungen auf die bestehenden Abonnements. Durch das Löschen eines Assets werden alle unveröffentlichten Versionen des Assets gelöscht. Veröffentlichte Versionen des Assets müssen separat gelöscht werden. Eine veröffentlichte Version eines Assets kann nur gelöscht werden, wenn es keine Abonnements gibt.

Asset-Typ und Metadaten sorgen für Resilienz

In Amazon DataZone werden Asset-Typen und Metadaten-Formulartypen versioniert. Ein Asset-Typ kann nicht gelöscht werden, wenn er von einem Asset verwendet wird. Ein Metadaten-Formulartyp kann nicht gelöscht werden, wenn er von einem Asset-Typ oder einem Asset verwendet wird. Wenn Sie nicht möchten, dass bestimmte Elemente metadata-form-type für die Kuration verwendet werden, können Sie sie deaktivieren, was sich nicht auf diejenigen auswirkt, an die sie bereits angehängt sind.

Glossar: Resilienz

In Amazon DataZone können Glossare und Glossarbegriffe nicht gelöscht werden, wenn sie verwendet werden. Wenn Sie nicht möchten, dass ein bestimmtes Glossar oder ein bestimmter Glossarbegriff für die Kuratierung verwendet wird, können Sie sie deaktivieren, was sich nicht auf diejenigen auswirkt, an die sie bereits angehängt sind.

Resilienz bei der globalen Suche

Bei Amazon DataZone können veröffentlichte Inhalte (auch Angebote genannt) über die globale Suche gefunden werden. Die Veröffentlichung eines Assets kann rückgängig gemacht werden, indem die Veröffentlichung des Assets rückgängig gemacht wird. Das Rückgängigmachen der Veröffentlichung eines Assets hat keine Auswirkungen auf bestehende Abonnements. Ein veröffentlichtes Asset kann auf eine bestimmte Version des Assets zurückgesetzt werden, indem diese Version erneut veröffentlicht wird. Dies hat keine Auswirkungen auf bestehende Abonnements.

Resilienz von Abonnements

Bei Amazon DataZone versucht der Versand mit SubscriptionGrant zweimal, bis der Versand fehlschlägt. Schlägt der Vorgang fehl, muss er manuell gelöscht werden, um es erneut zu versuchen. Wenn Amazon die Berechtigungen für ein Abonnement DataZone nicht widerrufen kann, schlägt das Löschen des Abonnements möglicherweise fehl. Der zugrunde liegende Fehler sollte behoben werden, oder das `retainPermissions` Flag kann im `DeleteSubscriptionGrant` API-Vorgang verwendet werden, um die Löschung des Zuschusses von Amazon zu erzwingen, DataZone ohne die Berechtigungen zu widerrufen.

Wenn die DataZone Amazon-Domain mit einem KMS-Schlüssel konfiguriert ist und sie während des `SubscriptionGrant` Workflows den Zugriff auf diesen Schlüssel `AmazonDataZoneDomainExecutionRole` verliert, wird die Gewährung markiert`INACCESSIBLE`. Sobald der KMS-Zugriff wiederhergestellt ist, müssen die `INACCESSIBLE` Grants gelöscht und neu erstellt werden.

Widerstandsfähigkeit der Umwelt

Wenn die DataZone Amazon-Domain mit einem KMS-Schlüssel konfiguriert ist und sie während des Umgebungsworkflows den Zugriff auf diesen Schlüssel `AmazonDataZoneDomainExecutionRole` verliert, wird die Umgebung markiert`INACCESSIBLE`. Sobald der KMS-Zugriff wiederhergestellt ist, muss die `INACCESSIBLE` Umgebung gelöscht und neu erstellt werden. Bei der Erstellung der

Umgebung werden zwei Versuche unternommen, bis der Vorgang fehlschlägt. Schlägt sie fehl, muss sie manuell gelöscht werden, um es erneut zu versuchen. Wenn der Umgebungsworkflow fehlschlägt, wechselt die Umgebung in den Status Fehlgeschlagen. Zu diesem Zeitpunkt kann sie nur gelöscht und neu erstellt werden.

Umwelt, Blaupause, Resilienz

In Amazon DataZone kann ein Umgebungs-Blueprint nicht gelöscht werden, wenn es irgendwelche zugrunde liegenden Umgebungsprofile gibt.

Resilienz des Projekts

In Amazon DataZone kann ein Projekt nicht gelöscht werden, wenn es eigene Umgebungen gibt.

RAM-Resilienz

Informationen zur RAM-Resilienz finden Sie unter https://docs.aws.amazon.com/ram/latest/userguide/security-disaster-recovery-resiliency .html.

Resilienz der Benutzerprofilverwaltung

Informationen zur Widerstandsfähigkeit von Benutzerprofilen finden Sie unter AWS Identity Center.

Ausfallsicherheit von Domänen

In Amazon kann eine Domain nicht gelöscht werden DataZone, wenn sie Projekte oder Datenquellen enthält.

Infrastruktursicherheit bei Amazon DataZone

Als verwalteter Service DataZone ist Amazon durch AWS globale Netzwerksicherheit geschützt. Informationen zu AWS Sicherheitsdiensten und zum AWS Schutz der Infrastruktur finden Sie unter AWS Cloud-Sicherheit. Informationen zum Entwerfen Ihrer AWS Umgebung unter Verwendung der bewährten Methoden für die Infrastruktursicherheit finden Sie unter Infrastructure Protection in Security Pillar AWS Well-Architected Framework.

Sie verwenden AWS veröffentlichte API-Aufrufe, um DataZone über das Netzwerk auf Amazon zuzugreifen. Kunden müssen Folgendes unterstützen:

- Transport Layer Security (TLS). Wir benötigen TLS 1.2 und empfehlen TLS 1.3.
- Verschlüsselungs-Suiten mit Perfect Forward Secrecy (PFS) wie DHE (Ephemeral Diffie-Hellman) oder ECDHE (Elliptic Curve Ephemeral Diffie-Hellman). Die meisten modernen Systeme wie Java 7 und höher unterstützen diese Modi.

Außerdem müssen Anforderungen mit einer Zugriffsschlüssel-ID und einem geheimen Zugriffsschlüssel signiert sein, der einem IAM-Prinzipal zugeordnet ist. Alternativ können Sie mit AWS Security Token Service (AWS STS) temporäre Sicherheitsanmeldeinformationen erstellen, um die Anforderungen zu signieren.

Dienstübergreifende Prävention verwirrter Stellvertreter bei Amazon DataZone

Das Problem des verwirrten Stellvertreters ist ein Sicherheitsproblem, bei dem eine Entität, die keine Berechtigung zur Durchführung einer Aktion hat, eine privilegiertere Entität zur Durchführung der Aktion zwingen kann. Bei AWS dienstübergreifendem Identitätswechsel kann es zu einem Problem mit verwirrtem Stellvertreter kommen. 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, den Kontextschlüssel aws: SourceAccount global condition in den Ressourcenrichtlinien zu verwenden, um die Berechtigungen einzuschränken, die Amazon einem anderen Service für die Ressource DataZone erteilt. Verwenden Sie aws:, SourceAccount wenn Sie zulassen möchten, dass jede Ressource in diesem Konto mit der dienstübergreifenden Nutzung verknüpft wird.

Konfiguration und Schwachstellenanalyse für Amazon DataZone

AWS kümmert sich um grundlegende Sicherheitsaufgaben wie das Patchen von Gastbetriebssystemen (OS) und Datenbanken, die Firewall-Konfiguration und die Notfallwiederherstellung. Diese Verfahren wurden von qualifizierten Dritten überprüft und zertifiziert. Weitere Informationen finden Sie im Modell der AWS gemeinsamen Verantwortung.

Domains, die Sie Ihrer Zulassungsliste hinzufügen möchten

Damit das DataZone Amazon-Datenportal auf den DataZone Amazon-Service zugreifen kann, müssen Sie die folgenden Domains zur Zulassungsliste in dem Netzwerk hinzufügen, von dem aus das Datenportal versucht, auf den Service zuzugreifen.

- `*.api.aws`
- `*.on.aws`

Überwachung von Amazon DataZone

Die Überwachung ist ein wichtiger Bestandteil der Aufrechterhaltung der Zuverlässigkeit, Verfügbarkeit und Leistung von Amazon DataZone und Ihren anderen AWS Lösungen. AWS bietet die folgenden Überwachungstools, um Amazon zu beobachten DataZone, zu melden, wenn etwas nicht stimmt, und gegebenenfalls automatische Maßnahmen zu ergreifen:

- Amazon CloudWatch überwacht Ihre AWS Ressourcen und die Anwendungen, auf denen Sie laufen, AWS in Echtzeit. Sie können Kennzahlen erfassen und verfolgen, benutzerdefinierte Dashboards erstellen und Alarme festlegen, die Sie benachrichtigen oder Maßnahmen ergreifen, wenn eine bestimmte Metrik einen von Ihnen festgelegten Schwellenwert erreicht. Sie können beispielsweise die CPU-Auslastung oder andere Kennzahlen Ihrer Amazon EC2 EC2-Instances CloudWatch verfolgen und bei Bedarf automatisch neue Instances starten. Weitere Informationen finden Sie im CloudWatch Amazon-Benutzerhandbuch.
- Mit Amazon CloudWatch Logs können Sie Ihre Protokolldateien von Amazon EC2 EC2-Instances und anderen Quellen überwachen CloudTrail, speichern und darauf zugreifen. CloudWatch Logs können Informationen in den Protokolldateien überwachen und Sie benachrichtigen, wenn bestimmte Schwellenwerte erreicht werden. Sie können Ihre Protokolldaten auch in einem sehr robusten Speicher archivieren. Weitere Informationen finden Sie im Amazon CloudWatch Logs-Benutzerhandbuch.
- Amazon EventBridge kann verwendet werden, um Ihre AWS Services zu automatisieren und automatisch auf Systemereignisse wie Probleme mit der Anwendungsverfügbarkeit oder Ressourcenänderungen zu reagieren. Ereignisse im AWS Rahmen von Services werden nahezu EventBridge in Echtzeit zugestellt. Sie können einfache Regeln schreiben, um anzugeben, welche Ereignisse für Sie interessant sind und welche automatisierten Aktionen ausgeführt werden sollen, wenn ein Ereignis mit einer Regel übereinstimmt. Weitere Informationen finden Sie im EventBridge Amazon-Benutzerhandbuch.
- AWS CloudTrailerfasst API-Aufrufe und zugehörige Ereignisse, die von oder im Namen Ihres AWS Kontos getätigt wurden, und übermittelt die Protokolldateien an einen von Ihnen angegebenen Amazon S3 S3-Bucket. Sie können feststellen, welche Benutzer und Konten angerufen wurden AWS, von welcher Quell-IP-Adresse aus die Anrufe getätigt wurden und wann die Aufrufe erfolgten. Weitere Informationen finden Sie im AWS CloudTrail -Benutzerhandbuch.

Amazon DataZone mit Amazon überwachen CloudWatch

Sie können Amazon DataZone mithilfe von Amazon überwachen CloudWatch, das Rohdaten sammelt und sie zu lesbaren, nahezu in Echtzeit verfügbaren Metriken verarbeitet. Diese Statistiken werden 15 Monate gespeichert, damit Sie auf Verlaufsinformationen zugreifen können und einen besseren Überblick darüber erhalten, wie Ihre Webanwendung oder der Service ausgeführt werden. Sie können auch Alarme einrichten, die auf bestimmte Grenzwerte achten und Benachrichtigungen senden oder Aktivitäten auslösen, wenn diese Grenzwerte erreicht werden. Weitere Informationen finden Sie im CloudWatch Amazon-Benutzerhandbuch.

Das DataZone Amazon-Datenportal verwendet Amazon DataZone Data Plane-APIs mit JWT-Authentifizierung und -Autorisierung. Amazon DataZone übernimmt die DataZone Standard-Servicerolle von Amazon und protokolliert alle DataZone Amazon-API-Aufrufe, die über das DataZone Amazon-Datenportal getätigt werden, in einer Protokollgruppe namens DataZoneDataPortalAPI CallLogs.

Überwachung von DataZone Amazon-Ereignissen in Amazon EventBridge

Sie können DataZone Amazon-Ereignisse überwachen EventBridge, wodurch ein Stream von Echtzeitdaten aus Ihren eigenen Anwendungen, software-as-a-service (SaaS-) Anwendungen und AWS Diensten bereitgestellt wird. EventBridgeleitet diese Daten an Ziele wie AWS Lambda Amazon Simple Notification Service weiter. Diese Ereignisse sind identisch mit denen, die in Amazon CloudWatch Events erscheinen. Amazon Events liefert einen Stream von Systemereignissen, die Änderungen an AWS Ressourcen beschreiben, nahezu in Echtzeit.

Weitere Informationen finden Sie unter Arbeiten mit Ereignissen über den EventBridge Amazon-Standardbus.

Protokollieren Amazon DataZone Amazon-API-Aufrufen mit AWS CloudTrail

Amazon DataZone ist in einen Service integriert AWS CloudTrail, der eine Aufzeichnung der Aktionen bereitstellt, die von einem Benutzer, einer Rolle oder einem AWS Service bei Amazon ausgeführt wurden DataZone. CloudTrail erfasst alle API-Aufrufe für Amazon DataZone als Ereignisse. Zu den erfassten Aufrufen gehören Aufrufe von der DataZone Amazon-Konsole und Code-Aufrufe der

DataZone Amazon-API-Operationen. Wenn Sie einen Trail erstellen, können Sie die kontinuierliche Übermittlung von CloudTrail Ereignissen an einen Amazon S3 S3-Bucket aktivieren, einschließlich Ereignissen für Amazon DataZone. 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 Amazon gestellt wurde DataZone, 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.

DataZone Amazon-Informationen in CloudTrail

CloudTrail ist auf Ihrem aktiviert AWS-Konto , wenn Sie das Konto erstellen. Wenn in der DataZone Amazon-Managementkonsole Aktivitäten auftreten, wird diese Aktivität zusammen mit anderen AWS Serviceereignissen in der CloudTrail Ereignishistorie in einem Ereignis aufgezeichnet. Sie können aktuelle Ereignisse in Ihrem ansehen, suchen und herunterladen AWS-Konto. Weitere Informationen finden Sie unter Ereignisse mit dem CloudTrail Ereignisverlauf anzeigen.

Für eine fortlaufende Aufzeichnung der Ereignisse in Ihrem AWS-Konto Konto, einschließlich Veranstaltungen für Amazon DataZone, erstellen Sie einen Trail. Ein Trail ermöglicht CloudTrail die Übermittlung von Protokolldateien an einen Amazon S3 S3-Bucket. Wenn Sie einen Trail in der Konsole anlegen, gilt dieser für alle AWS-Regionen-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 andere AWS Dienste konfigurieren, um die in den CloudTrail Protokollen gesammelten Ereignisdaten weiter zu analysieren und darauf zu reagieren. 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

Alle DataZone Amazon-Aktionen werden von protokolliert CloudTrail.

Problembehebung bei Amazon DataZone

Wenn Sie bei der Arbeit mit Amazon auf Probleme mit Zugriffsverweigerung oder ähnliche Probleme stoßen, DataZone lesen Sie die Themen in diesem Abschnitt.

Fehlerbehebung bei AWS Lake Formation Formation-Berechtigungen für Amazon DataZone

Dieser Abschnitt enthält Anweisungen zur Fehlerbehebung für Probleme, die bei Ihnen auftreten könnenLake Formation Formation-Berechtigungen für Amazon konfigurieren DataZone.

Fehlermeldung im Datenportal	Auflösung
Die Datenzugriffsrolle konnte nicht übernommen werden.	Dieser Fehler wird angezeigt, wenn Amazon DataZone nicht davon ausgehen kann AmazonDataZoneGlueDataAccessRole, dass Sie das DefaultDataLakeBlueprintin Ihrem Konto aktiviert haben. Um das Problem zu beheben, rufen Sie die AWS IAM-Konsole des Kontos auf, in dem sich Ihr Datenbestand befindet, und stellen Sie sicher, dass AmazonDataZoneGlueDataAccessRoledas richtige Vertrauensverhältnis mit dem Amazon DataZone Service Principal besteht. Weitere Informationen finden Sie unter AmazonDataZoneGlueAccess- <region>- <domainId>.
Die Datenzugriffsrolle verfügt nicht über die erforderlichen Berechtigungen, um die Metadaten der Ressource zu lesen, die Sie abonnieren möchten.	Dieser Fehler wird angezeigt, wenn Amazon die AmazonDataZoneGlueDataAccessRoleRolle DataZone erfolgreich annimmt, die Rolle jedoch nicht über die erforderlichen Berechtigungen verfügt. Um das Problem zu beheben, rufen Sie die AWS IAM-Konsole in dem Konto auf, in dem sich Ihr Datenbestand befindet, und vergewissern Sie sich, dass der Rolle die Datei AmazonDataZoneGlue

Fehlermeldung im Datenportal	Auflösung
	ManageAccessRolePolicyangehängt ist. Weitere Informationen finden Sie unter AmazonDataZoneGlueAccess- <region>-<domainId>.
Ein Asset ist ein Ressourcenlink. Amazon unterstützt DataZone keine Abonnements für Ressourcenlinks.	Dieser Fehler wird angezeigt, wenn es sich bei dem Asset, das Sie auf Amazon veröffentlichen möchten, um einen Ressourcenlink zu einer AWS Glue-Tabelle DataZone handelt.

Fehlermeldung im Datenportal	Auflösung
Das Asset wird nicht von AWS Lake Formation verwaltet.	Dieser Fehler weist darauf hin, dass die AWS Lake Formation Formation-Berechtigungen für das Asset, das Sie veröffentlichen möchten, nicht durchgesetzt wurden. Dies kann in den folgenden Fällen passieren. • Der Amazon S3 S3-Standort des Assets ist nicht in AWS Lake Formation registriert. Um das Problem zu beheben, melden Sie sich bei Ihrer AWS Lake Formation Formation-Konsole in dem Konto an, in dem die Tabelle vorhanden ist, und registrieren Sie den Amazon S3 S3-Standort entweder im AWS Lake Formation Formation-Modus oder im Hybrid-Modus. Weitere Informationen finden Sie unter Registrieren eines Amazon-S3-Speicherorts. Es gibt mehrere Szenarien, die weitere Änderungen erfordern. Dazu gehören verschlüsselte AmazonS3-Buckets oder ein kontoübergreifender S3-Bucket und ein AWS Glue-Katalog-Setup. In solchen Fällen können Änderungen der KMS- und/oder S3-Einstellungen erforderlich sein. Weitere Informationen finden Sie unter Registrieren eines verschlüsselten Amazon-S3-Speicherorts. • Der Amazon S3 S3-Standort ist im AWS Lake Formation Formation-Modus registriert, aber IAM AllowedPrincipal wird zu den Berechtigungen der Tabelle hinzugefügt. Um das Problem zu beheben, können Sie entweder das IAM AllowedPrincipal aus den Berechtigungen der Tabelle entfernen oder den S3-Standort im Hybridmodus registrieren. Weitere Informationen finden Sie unter

Fehlermeldung im Datenportal	Auflösung
	Informationen zum Upgrade auf das Lake Formation Formation-Berechtigungsmodell. Wenn Ihr S3-Standort verschlüsselt ist oder sich der S3-Standort in einem anderen Konto als Ihrer AWS Glue-Tabelle befindet, folgen Sie den Anweisungen unter Registrierung eines verschlüsselten Amazon S3 S3-Standorts.
Die Datenzugriffsrolle verfügt nicht über die erforderlichen Lake Formation Formation-Berechtigungen, um Zugriff auf dieses Asset zu gewähren.	Dieser Fehler weist darauf hin AmazonDataZoneGlueDataAccessRole, dass das, was Sie zur Aktivierung von DefaultDataLakeBlueprintin Ihrem Konto verwenden, nicht über die erforderlichen Berechtigungen verfügt, DataZone damit Amazon die Berechtigungen für das veröffentlichte Asset verwalten kann. Sie können das Problem lösen, indem Sie entweder den AmazonDataZoneGlueDataAccessRoleals AWS Lake Formation-Administrator hinzufügen oder indem Sie dem Asset, das AmazonDataZoneGlueDataAccessRoleSie veröffentlichen möchten, die folgenden Berechtigungen gewähren. • Beschreiben und beschreiben Sie die erteilbaren Berechtigungen für die Datenbank, in der sich das Asset befindet • Beschreibe, Select, Describe Grantable, Select Grantable Berechtigungen für alle Assets in der Datenbank, deren Zugriff Amazon in deinem Namen verwalten DataZone soll.

Kontingente für Amazon DataZone

Ihr AWS Konto hat Standardkontingente, früher als Limits bezeichnet, für jeden AWS Service. Sofern nicht anders angegeben, ist jedes Kontingent regionsspezifisch.

Amazon DataZone hat die folgenden Kontingente und Limits.

Ressource	Beschreibung	Wert
Typen von Datenbeständen	Die maximale Anzahl von Datenobjekttypen, die in einer DataZone Domäne erstellt werden können	1000
Datenbestände	Die maximale Anzahl von Datenbeständen, die in einer DataZone Amazon-Domain erstellt werden können	1 Mio.
Glossare	Die maximale Anzahl von Geschäftsglossaren, die Sie in einer Domain erstellen können	1000
Begriffe aus dem Geschäfts glossar	Die maximale Gesamtanz ahl von Begriffen aus dem Geschäftsglossar, die Sie in einer Domain erstellen können	10000
Umgebungen in einer Domäne	Die maximale Anzahl von Umgebungen in einer DataZone Amazon-Domain	500

Dokumentenverlauf für das DataZone Amazon-Benutzerhandbuch

In der folgenden Tabelle werden die Dokumentationsversionen für Amazon beschrieben DataZone.

Änderung	Beschreibung	Datum
AmazonDataZoneSageMakerProvisioning - neue Richtlinie	Eine neue Richtlinie namens AmazonDataZoneSageMakerProvisioninggewährt Amazon DataZone die für die Zusammenarbeit mit Amazon SageMaker erforderlichen Berechtigungen. Weitere Informationen finden Sie unter DataZone Amazon-Updates zu AWS verwalteten Richtlinien.	30. April 2024
AmazonDataZoneSageMakerEnvironmentRolePermissionsBoundary - neue Grenze für Berechtigungen	Neue Berechtigungsgrenze aufgerufen AmazonDataZoneSageMakerEnvironmentRolePermissionsBoundary. Wenn Sie eine SageMaker Amazon-Umgebung über das DataZone Amazon-Datenportal erstellen, DataZone wendet Amazon diese Berechtigungsgrenze auf die IAM-Rollen an, die bei der Umgebungserstellung erstellt werden. Die Berechtigungsgrenze begrenzt den Umfang der Rollen, die Amazon DataZone erstellt, und aller Rollen, die Sie hinzufügen. Weitere	30. April 2024

	Informationen finden Sie unter DataZone Amazon-Updates zu AWS verwalteten Richtlinien.	
AmazonDataZoneSageMakerAccess - neue Richtlinie	Eine neue Richtlinie namens AmazonDataZoneSageMakerAccessgewährt Amazon DataZone die erforderlichen Berechtigungen, um Benutzern Zugriff auf verschiedene Ressourcen in der SageMaker Amazon-Umgebung zu gewähren. Weitere Informationen finden Sie unter DataZone Amazon-Updates zu AWS verwalteten Richtlinien.	30. April 2024
AmazonDataZoneFullAccess - Aktualisierung der Richtlinien	Eine Aktualisierung der AmazonDataZoneFullAccessRichtlinie, die Zugriff auf `DescribeSecurityGroups` Aktionen erweitert, um die Benutzerfreundlichkeit für Kontoadministratoren zu verbessern, indem sie Blueprints in der Konsole konfigurieren und `GetPolicy` Aktionen zum Abrufen von Informationen über die angegebene verwaltete Richtlinie durchführen. Weitere Informationen finden Sie unter DataZone Amazon-Updates zu AWS verwalteten Richtlinien.	30. April 2024

AmazonDataZoneS3Manage- - neue Rolle <region>< domainId>	Neue Rolle namens AmazonDataZoneS3Ma nage- — <region><domainId> die verwendet wird, wenn Amazon AWS Lake Formation DataZone aufruft, um einen Amazon Simple Storage Service (Amazon S3) - Standort zu registrieren. AWS Lake Formation übernimmt diese Rolle beim Zugriff auf die Daten an diesem Standort. Weitere Informationen finden Sie unter DataZone Amazon-Updates zu AWS verwalteten Richtlinien.	1. April 2024
AmazonDataZoneGlue ManageAccessRolePolicy - Aktualisierung der Richtlinie	Das wurde aktualisiert AmazonDataZoneGlue ManageAccessRolePolicy, um die Unterstützung für Berechtigungen zu aktiviere n, die es Amazon ermöglichen DataZone , Veröffentlichungen und Zugriffserlaubnisse für Daten zu ermöglichen. Weitere Informationen finden Sie unter DataZone Amazon-Updates zu AWS verwalteten Richtlinien.	1. April 2024

AmazonDataZoneDomainExecutionRolePolicy und AmazonDataZoneFullUserAccess — Aktualisierung der Richtlinien	Das AmazonDataZoneDomainExecutionRolePolicyund wurde aktualisiert AmazonDataZoneFullUserAccess, um die Unterstützung für die `CancelMetadataGenerationRun` API zu aktivieren. Weitere Informationen finden Sie unter DataZone Amazon-Updates zu AWS verwalteten Richtlinien.	29. März 2024
AmazonDataZoneFullAccess - Aktualisierung der Richtlinie	Das wurde aktualisiertAmazonDataZoneFullAccess , sodass Benutzer ihre Geheimnisse, Cluster, VPCs und Subnetze in der DataZone Amazon-Managementkonsole auswählen können, anstatt sie in ein Textfeld einzugeben. Weitere Informationen finden Sie unter DataZone Amazon-Updates zu AWS verwalteten Richtlinien.	13. März 2024

AmazonDataZoneDomainExecutionRolePolicy - Aktualisierung der Richtlinie	Das wurde aktualisiert AmazonDataZoneDomainExecutionRolePolicy, um die Unterstützung für die ListEnvironmentBlueprintConfigurationSummaries API zu aktivieren, die für die Erstellung von Umgebungsprofilen erforderlich ist, indem identifiziert wird, welche Blueprints in welchem Konto und welcher Region aktiviert sind. Weitere Informationen finden Sie unter DataZone Amazon-Updates zu AWS verwalteten Richtlinien.	1. Februar 2024
AmazonDataZoneGlueManageAccessRolePolicy - Aktualisierung der Richtlinie	Das wurde aktualisiert AmazonDataZoneGlueManageAccessRolePolicy, um die Unterstützung für den AWS Lake Formation Formation-Hybridmodus zu aktivieren. Weitere Informationen finden Sie unter DataZone Amazon-Updates zu AWS verwalteten Richtlinien.	14. Dezember 2023

AmazonDataZoneFullUserAccess und AmazonDataZoneDomainExecutionRolePolicy — Aktualisierungen der Richtlinien	Amazon hat die AmazonDataZoneFullUserAccessAmazonDataZoneDomainExecutionRolePolicyRichtlinien DataZone aktualisiert, um die generative KI-gestützte Datenbeschreibungsfunktion in Amazon DataZone zu unterstützen. Weitere Informationen finden Sie unter DataZone Amazon-Updates zu AWS verwalteten Richtlinien.	28. November 2023
AmazonDataZoneEnvironmentRolePermissionsBoundary - Aktualisierung der Richtlinien	Amazon DataZone hat eine Aktualisierung der AmazonDataZoneEnvironmentRolePermissionsBoundaryverwalteten Richtlinie vorgenommen, die aus einer zusätzlichen `athena:GetQueryResultsStream` Genehmigung besteht, die auf die `ResourceTag` Bedingung zugeschnitten ist. Weitere Informationen finden Sie unter DataZone Amazon-Updates zu AWS verwalteten Richtlinien.	17. November 2023

AmazonDataZoneRedshiftManageAccessRolePolicy - Aktualisierung der Richtlinien	Amazon hat die AmazonDataZoneRedshiftManageAccessRolePolicyRichtlinie DataZone aktualisiert, indem das Häkchen auf die Organisations-ID für die `redshift:AssociateDataShareConsumer` Aktion entfernt wurde. Auf diese Weise können Sie Ressourcen organisationsübergreifend AWS gemeinsam nutzen. Weitere Informationen finden Sie unter DataZone Amazon-Updates zu AWS verwalteten Richtlinien.	16. November 2023
AmazonDataZoneFullUserAccess - Aktualisierung der Richtlinien	Amazon hat die AmazonDataZoneFullUserAccessRichtlinie DataZone aktualisiert, die vollen Zugriff auf Amazon gewährt DataZone, aber die Verwaltung von Domains, Benutzern oder zugehörigen Konten nicht erlaubt. Weitere Informationen finden Sie unter DataZone Amazon-Aktualisierungen zu AWS verwalteten Richtlinien.	2. Oktober 2023

AmazonDataZonePreviewConsoleFullAccess — Richtlinie ist veraltet	Amazon DataZone hat das als veraltet eingestuft AmazonDataZonePreviewConsoleFullAccess. Weitere Informationen finden Sie unter DataZone Amazon-Updates zu AWS verwalteten Richtlinien.	29. September 2023
AmazonDataZonePortalFullAccessPolicy - Richtlinie ist veraltet	Amazon DataZone hat das als veraltet eingestuft AmazonDataZonePortalFullAccessPolicy. Weitere Informationen finden Sie unter DataZone Amazon-Updates zu AWS verwalteten Richtlinien.	29. September 2023

AmazonDataZoneDomainExecutionRolePolicy - Neue Richtlinie	Amazon DataZone hat eine neue Richtlinie namens hinzugefügt AmazonDataZoneDomainExecutionRolePolicy. Dies ist die Standardrichtlinie für die DataZone `AmazonDataZoneDomainExecutionRole` Amazon-Servicerolle. Diese Rolle wird von Amazon verwendet , DataZone um Daten in der DataZone Amazon-Domain zu katalogisieren, zu entdecken, zu verwalten, zu teilen und zu analysieren. Sie können die `AmazonDataZoneDomainExecutionRolePolicy` Richtlinie an Ihre anhängen`AmazonDataZoneDomainExecutionRole` . Weitere Informationen finden Sie unter DataZone Amazon-Updates zu AWS verwalteten Richtlinien.	25. September 2023

AmazonDataZoneCrossAccountAdmin - Neue Richtlinie	Amazon DataZone hat eine neue Richtlinie hinzugefügt, AmazonDataZoneCrossAccountAdmindie es Benutzern ermöglicht, mit Amazon DataZone und den zugehörigen Konten zu arbeiten. Weitere Informationen finden Sie unter DataZone Amazon-Updates zu AWS verwalteten Richtlinien.	19. September 2023
AmazonDataZoneRedshiftManageAccessRolePolicy - Neue Richtlinie	Amazon DataZone hat eine neue Richtlinie hinzugefügt, AmazonDataZoneRedshiftManageAccessRolePolicydie Berechtigungen gewährt, damit Amazon DataZone die Veröffentlichung und den Zugriff auf Daten ermöglichen kann. Weitere Informationen finden Sie unter DataZone Amazon-Updates zu AWS verwalteten Richtlinien.	12. September 2023

AmazonDataZoneRedshiftGlueProvisioningPolicy - Neue Richtlinie	Amazon DataZone hat eine neue Richtlinie hinzugefügt, AmazonDataZoneRedshiftGlueProvisioningPolicydie Amazon DataZone die für die Zusammenarbeit mit den unterstützten Datenquellen erforderlichen Berechtigungen gewährt. Weitere Informationen finden Sie unter DataZone Amazon-Updates zu AWS verwalteten Richtlinien.	12. September 2023
AmazonDataZoneGlueManageAccessRolePolicy - Neue Richtlinie	Amazon DataZone hat eine neue Richtlinie hinzugefügt, die Amazon die DataZone Erlaubnis AmazonDataZoneGlueManageAccessRolePolicyerteilt, AWS Glue-Daten im Katalog zu veröffentlichen. Es gibt Amazon auch die DataZone Erlaubnis, Zugriff auf veröffentlichte AWS Glue-Assets im Katalog zu gewähren oder den Zugriff zu widerrufen. Weitere Informationen finden Sie unter DataZone Amazon-Updates zu AWS verwalteten Richtlinien.	12. September 2023

AmazonDataZoneFull UserAccess - Neue Richtlinie	Amazon DataZone hat eine neue Richtlinie hinzugefügt AmazonDataZoneFull UserAccess, die Amazon DataZone über das Datenportal vollen Zugriff gewährt. Weitere Informationen finden Sie unter DataZone Amazon-Updates zu AWS verwalteten Richtlinien.	12. September 2023
AmazonDataZoneFullAccess - Neue Richtlinie	Amazon DataZone hat eine neue Richtlinie hinzugefügt, AmazonDataZoneFull Accessdie vollen Zugriff auf Amazon DataZone über die AWS Management Console bietet. Weitere Informationen finden Sie unter DataZone Amazon-Updates zu AWS verwalteten Richtlinien.	12. September 2023
AmazonDataZoneEnvironmentRolePermissionsBoundary - Neue Richtlinie	Amazon DataZone hat eine neue Richtlinie hinzugefügt AmazonDataZoneEnvironmentRolePermissionsBoundary, die den bereitgestellten IAM-Prinzipal einschränkt, an den sie angehängt ist. Weitere Informationen finden Sie unter DataZone Amazon-Updates zu AWS verwalteten Richtlinien.	12. September 2023

Aktualisierung der verwalteten Richtlinien	Aktualisierungen der AmazonDataZonePreviewConsoleFullAccess verwalteten Richtlinie. Weitere Informationen finden Sie unter DataZone Amazon-Updates zu AWS verwalteten Richtlinien.	13. Juni 2023
Aktualisierung der verwalteten Richtlinien	Aktualisierungen der AmazonDataZoneProjectDeploymentPermissionsBoundary verwalteten Richtlinie. Weitere Informationen finden Sie unter DataZone Amazon-Updates zu AWS verwalteten Richtlinien.	03. April 2023
???	Erste Version des Amazon-Benutzerhandbuchs DataZone (Preview).	29. März 2023

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.