aws

Panduan Pengguna

Amazon DataZone

Amazon DataZone: Panduan Pengguna

Table of Contents

Apa itu Amazon DataZone?

Amazon DataZone adalah layanan manajemen data yang membuatnya lebih cepat dan mudah bagi Anda untuk membuat katalog, menemukan, berbagi, dan mengatur data yang disimpan di seluruh sumber lokal AWS, dan pihak ketiga. Dengan Amazon DataZone, administrator yang mengawasi aset data organisasi dapat mengelola dan mengatur akses ke data menggunakan kontrol halus. Kontrol ini membantu memastikan akses dengan tingkat hak istimewa dan konteks yang tepat. Amazon DataZone memudahkan para insinyur, ilmuwan data, manajer produk, analis, dan pengguna bisnis untuk berbagi dan mengakses data di seluruh organisasi sehingga mereka dapat menemukan, menggunakan, dan berkolaborasi untuk memperoleh wawasan berbasis data.

Amazon DataZone membantu Anda mengirimkan data ke pengguna akhir secara langsung dan menyederhanakan arsitektur Anda dengan mengintegrasikan layanan manajemen data, termasuk Amazon Redshift, Amazon Athena, Amazon, QuickSight Glue, Lake AWS Formation AWS , sumber lokal, sumber pihak ketiga, dan banyak lagi.

Topik

Apa yang bisa saya lakukan dengan Amazon DataZone?

Dengan Amazon DataZone, Anda dapat melakukan hal berikut:

- Mengatur akses data melintasi batas-batas organisasi. Dengan Amazon DataZone, Anda dapat membantu memastikan bahwa data yang tepat diakses oleh pengguna yang tepat untuk tujuan yang benar, sesuai dengan peraturan keamanan organisasi Anda, tanpa bergantung pada kredensi individu. Anda juga dapat memberikan transparansi tentang penggunaan aset data dan menyetujui langganan data dengan alur kerja yang diatur. Anda juga dapat memantau aset data di seluruh proyek melalui kemampuan audit penggunaan.
- Hubungkan pekerja data melalui data bersama dan alat untuk mendorong wawasan bisnis. Dengan Amazon DataZone, Anda dapat meningkatkan efisiensi tim bisnis dengan berkolaborasi secara mulus di seluruh tim dan menyediakan akses layanan mandiri ke alat data dan analitik. Anda dapat menggunakan istilah bisnis untuk mencari, berbagi, dan mengakses data katalog yang disimpan di

AWS, lokal, atau dengan penyedia pihak ketiga. Dan Anda dapat mempelajari lebih lanjut tentang data yang ingin Anda gunakan dengan menggunakan glosarium DataZone bisnis Amazon.

- Otomatiskan penemuan dan katalogisasi data dengan pembelajaran mesin. Dengan Amazon DataZone, Anda dapat mengurangi waktu yang dihabiskan untuk entri manual atribut data ke dalam katalog data bisnis. Data yang lebih kaya dalam katalog data juga meningkatkan pengalaman pencarian.

Bagaimana Amazon DataZone mendukung dan mengintegrasikan dengan AWS layanan lain?

Amazon DataZone mendukung tiga jenis integrasi dengan AWS layanan lain:

- Sumber data produsen - Anda dapat mempublikasikan aset data ke DataZone katalog Amazon dari data yang disimpan dalam Katalog Data AWS Glue dan tabel dan tampilan Amazon Redshift. Anda juga dapat mempublikasikan objek secara manual dari Amazon Simple Storage Service (S3) ke katalog Amazon. DataZone
- Alat konsumen - Anda dapat menggunakan editor kueri Amazon Athena atau Amazon Redshift untuk mengakses dan menganalisis aset data Anda.
- Kontrol dan pemenuhan akses - Amazon DataZone mendukung pemberian akses ke tabel AWS Glue yang dikelola AWS Lake Formation serta tabel dan tampilan Amazon Redshift. Untuk semua aset data lainnya, Amazon DataZone menerbitkan peristiwa standar yang terkait dengan tindakan Anda (misalnya, persetujuan yang diberikan untuk permintaan berlangganan) ke Amazon EventBridge. Anda dapat menggunakan acara standar ini untuk berintegrasi dengan AWS layanan lain atau solusi pihak ketiga untuk integrasi khusus.

Bagaimana saya bisa mengakses Amazon DataZone?

Anda dapat mengakses Amazon DataZone dengan salah satu cara berikut:

- DataZone Konsol Amazon

  Anda dapat menggunakan konsol DataZone manajemen Amazon untuk mengakses dan mengonfigurasi DataZone domain, cetak biru, dan pengguna Amazon Anda. Untuk informasi lebih lanjut, lihat https://console.aws.amazon.com/datazone. Konsol DataZone manajemen Amazon juga digunakan untuk membuat portal DataZone data Amazon.

- Portal DataZone data Amazon

  Portal DataZone data Amazon adalah aplikasi web berbasis browser tempat Anda dapat membuat katalog, menemukan, mengatur, berbagi, dan menganalisis data dengan cara swalayan. Portal data dapat mengautentikasi Anda dengan kredensi dari penyedia identitas Anda melalui AWS IAM Identity Center (penerus AWS SSO), atau dengan kredensi IAM Anda. Anda dapat memperoleh URL portal data dengan mengakses DataZone konsol Amazon di https://console.aws.amazon.com/datazone.

- API DataZone HTTPS Amazon

  Anda dapat mengakses Amazon DataZone secara terprogram menggunakan Amazon DataZone HTTPS API, yang memungkinkan Anda mengeluarkan permintaan HTTPS langsung ke layanan. Untuk informasi selengkapnya, lihat Referensi Amazon DataZone API.

DataZone Terminologi dan konsep Amazon

Saat Anda memulai dengan Amazon DataZone, penting bagi Anda untuk memahami konsep, terminologi, dan komponennya.

Topik

DataZone Komponen Amazon

Amazon DataZone mencakup empat komponen utama berikut:

- Katalog data bisnis - Anda dapat menggunakan komponen ini untuk membuat katalog data di seluruh organisasi Anda dengan konteks bisnis dan dengan demikian memungkinkan semua orang di organisasi Anda untuk menemukan dan memahami data dengan cepat.
- Publikasikan dan berlangganan alur kerja - Anda dapat menggunakan alur kerja otomatis ini untuk mengamankan data antara produsen dan konsumen dengan cara layanan mandiri dan untuk memastikan bahwa setiap orang di organisasi Anda memiliki akses ke data yang tepat untuk tujuan yang tepat.
- Proyek dan lingkungan
  - Di Amazon, DataZone proyek terdapat pengelompokan orang, aset (data), dan alat berbasis kasus penggunaan bisnis yang digunakan untuk menyederhanakan akses ke analitik. AWS Proyek menyediakan area di mana anggota proyek dapat berkolaborasi, bertukar data, dan berbagi aset. Secara default, proyek dikonfigurasikan sehingga hanya mereka yang secara eksplisit ditambahkan ke proyek yang dapat mengakses data dan alat analitik di dalamnya. Proyek mengelola kepemilikan aset yang dihasilkan sesuai dengan kebijakan proyek untuk diakses konsumen data.

  - Dalam DataZone proyek Amazon, lingkungan adalah kumpulan dari nol atau lebih sumber daya yang dikonfigurasi (misalnya, bucket Amazon S3, AWS Glue database, atau workgroup Amazon Athena) tempat kumpulan prinsipal IAM tertentu (misalnya, pengguna dengan izin kontributor) dapat beroperasi.
- Portal data (di luar AWS Management Console) - ini adalah aplikasi web berbasis browser di mana pengguna yang berbeda dapat pergi ke katalog, menemukan, mengatur, berbagi, dan menganalisis data dengan cara swalayan. Portal data mengautentikasi pengguna dengan kredensi IAM atau kredensil yang ada dari penyedia identitas Anda melalui. AWS IAM Identity Center

Apa itu DataZone domain Amazon?

Anda dapat menggunakan DataZone domain Amazon untuk mengatur aset, pengguna, dan proyek mereka. Dengan mengaitkan AWS akun tambahan dengan DataZone domain Amazon Anda, Anda dapat mengumpulkan sumber data Anda. Anda kemudian dapat mempublikasikan aset dari sumber data ini ke katalog domain Anda, dengan formulir metadata dan glosarium yang meningkatkan kelengkapan dan kualitas metadata. Anda juga dapat mencari dan menelusuri aset ini untuk melihat data apa yang dipublikasikan di domain. Selain itu, Anda dapat bergabung dengan proyek untuk berkolaborasi dengan pengguna lain, berlangganan aset, dan menggunakan lingkungan proyek untuk mengakses alat analitik, termasuk Amazon Athena dan Amazon Redshift. DataZone Domain Amazon memungkinkan Anda dengan fleksibilitas untuk mencerminkan kebutuhan data dan analitik struktur organisasi Anda, baik itu membuat satu DataZone domain Amazon untuk perusahaan Anda atau beberapa DataZone domain Amazon untuk unit bisnis yang berbeda.

Apa itu DataZone proyek dan lingkungan Amazon?

Amazon DataZone memungkinkan tim dan pengguna analitik untuk berkolaborasi dalam proyek dengan membuat pengelompokan tim, alat, dan data berbasis kasus penggunaan.

- Di Amazon DataZone, proyek memungkinkan sekelompok pengguna untuk berkolaborasi dalam berbagai kasus penggunaan bisnis yang melibatkan penerbitan, penemuan, berlangganan, dan konsumsi data dalam katalog Amazon. DataZone Anggota proyek menggunakan aset dari DataZone katalog Amazon dan menghasilkan aset baru menggunakan satu atau lebih alur kerja analitis. Proyek mendukung kegiatan berikut dalam portal data:
  - Pemilik proyek dapat menambahkan anggota dengan izin pemilik dan kontributor
  - Anggota proyek dapat berupa pengguna SSO, grup SSO, dan pengguna IAM
  - Anggota proyek dapat meminta berlangganan aset dalam katalog data

Persetujuan berlangganan diberikan untuk proyek

- Dalam DataZone proyek Amazon, lingkungan adalah kumpulan sumber daya nol atau lebih yang dikonfigurasi (misalnya, Amazon S3, AWS Glue database, atau kelompok kerja Amazon Athena), dengan seperangkat prinsip IAM tertentu yang dapat beroperasi pada sumber daya tersebut. Lingkungan dibuat dengan menggunakan profil lingkungan yang merupakan kumpulan sumber daya dan cetak biru yang telah dikonfigurasi sebelumnya yang menyediakan templat yang dapat digunakan kembali untuk menciptakan lingkungan. Profil lingkungan menentukan pengaturan seperti Akun AWS atau wilayah di mana lingkungan digunakan.

Apa itu DataZone cetak biru Amazon?

Cetak biru yang dengannya lingkungan dibuat mendefinisikan AWS alat dan layanan apa (misalnya, atau Amazon AWS Glue Redshift) anggota proyek tempat lingkungan berada dapat digunakan saat mereka bekerja dengan aset dalam katalog Amazon. DataZone

Dalam rilis Amazon saat ini DataZone, cetak biru default berikut didukung:

Nama cetak biru	Deskripsi	Sumber daya dibuat
Cetak biru Data Lake	Memungkinkan anggota DataZone proyek Amazon untuk meluncurkan produsen Data Lake dan layanan konsumen di lingkungan. Sebagai konsumen, ini memungkinkan anggota DataZone proyek Amazon untuk mengakses salinan 'hanya baca' dari aset yang dikelola Lake Formation langsung di Amazon Athena dan di mesin kueri lain yang didukung Lake Formation. Sebagai produser, ini memungkinkan anggota	Memberikan pengguna kemampuan untuk membuat dan menanyakan tabel Lake Formation menggunakan Amazon Athena. Grup kerja Amazon Athena, AWS Glue database dengan izin Formasi Danau 'hanya baca', izin IAM 'baca saja', dan akses ke Amazon S3 yang dikelola oleh proyek. AWS Glue database dengan 'buat' dan 'berikan' izin Lake Formation, izin IAM 'baca' dan 'tulis', AWS Glue ETL (ekstrak, transformasi, dan muat) dengan penandaan.

Nama cetak biru	Deskripsi	Sumber daya dibuat
	DataZone proyek Amazon untuk membuat tabel LakeFormation terkelola baru menggunakan Amazon Athena dan mempublik asikannya ke katalog Amazon DataZone.	
Cetak biru Gudang Data	Sebagai konsumen, cetak biru ini memungkinkan anggota DataZone proyek Amazon untuk terhubung ke cluster Amazon Redshift mereka sendiri untuk menanyaka n penyimpanan data jarak jauh dan untuk membuat dan menyimpan kumpulan data baru. Sebagai produser, cetak biru ini memungkinkan anggota DataZone proyek Amazon untuk terhubung ke cluster Amazon Redshift mereka sendiri untuk menanyakan penyimpanan data jarak jauh, untuk membuat kumpulan data baru, dan mempublik asikannya ke katalog Amazon. DataZone	Akses ke editor kueri Amazon Redshift, akses 'baca' ke sumber data berlangga nan dari DataZone katalog Amazon, kemampuan untuk membuat aset lokal di cluster Amazon Redshift yang dikonfigurasi. Akses ke editor kueri Amazon Redshift, akses 'baca' ke sumber data berlangganan dari DataZone katalog Amazon, kemampuan untuk membuat dan mempublikasikan aset dari cluster Amazon Redshift yang dikonfigurasi.

Nama cetak biru	Deskripsi	Sumber daya dibuat
Cetak biru Amazon Sagemaker	Cetak biru ini membantu produsen data dan konsumen untuk beralih ke Amazon dengan mulus SageMaker untuk berkolaborasi dalam proyek pembelajaran mesin (ML) sambil menegakkan tata kelola akses ke data dan aset ML. Dengan integrasi bawaan baru antara Amazon DataZone dan Amazon SageMaker, konsumen dan produsen data dapat merampingkan tata kelola ML di seluruh penyiapan infrastru ktur, berkolaborasi dalam inisiatif bisnis, dan mengatur data dan aset ML dengan mudah.	Anda dapat membuat SageMaker domain Amazon yang dapat mencari, berlangganan, dan mempublik asikan data dan aset ML di Amazon DataZone. Juga dapat berlangganan dan mempublikasikan ke database AWS Glue dan pembentukan danau seperti yang dikonfigu rasi.

Apa itu DataZone inventaris Amazon dan alur kerja penerbitan?

Membuat aset inventaris proyek

Untuk menggunakan Amazon DataZone untuk membuat katalog data Anda, Anda harus terlebih dahulu membawa data (aset) Anda sebagai inventaris proyek Anda di Amazon DataZone. Membuat inventaris untuk sebuah proyek, membuat aset hanya dapat ditemukan oleh anggota proyek itu. Aset inventaris proyek tidak tersedia untuk semua pengguna domain dalam pencarian/penelusuran kecuali dipublikasikan secara eksplisit. Dalam rilis Amazon saat ini DataZone, Anda dapat menambahkan aset ke inventaris proyek dengan cara berikut:

- Membuat dan menjalankan sumber data melalui portal data atau dengan menggunakan Amazon DataZone API. Dalam rilis Amazon saat ini DataZone, Anda dapat membuat dan menjalankan sumber data untuk AWS Glue dan Amazon Redshift. Dengan membuat dan menjalankan sumber

data AWS Glue atau Amazon Redshift, Anda membuat aset dalam inventaris proyek yang dipilih dan mengimpor metadata teknisnya dari tabel database sumber atau gudang data sebagai inventaris ke Amazon. DataZone

- Menggunakan API, Anda dapat membuat aset dari jenis aset sistem yang tersedia (AWS Glue, Amazon Redshift, objek Amazon S3) atau dari jenis aset kustom Anda.
  - Buat jenis aset kustom dalam inventaris proyek dengan menggunakan Amazon DataZone API. Jenis aset kustom dapat mencakup model ML, dasbor, tabel lokal, dll.
  - Buat aset dari jenis aset kustom ini menggunakan Amazon DataZone API.
- Buat aset untuk objek S3 secara manual menggunakan portal DataZone data Amazon.

Kurasi aset inventaris proyek Anda - setelah membuat inventaris proyek, pemilik data dapat mengkurasi aset inventaris mereka dengan metadata bisnis yang diperlukan dengan menambahkan atau memperbarui nama bisnis (aset dan skema), deskripsi (aset dan skema), baca saya, istilah glosarium (aset dan skema), dan formulir metadata. Anda dapat melakukan ini melalui portal data atau dengan menggunakan DataZone API Amazon. Setiap pengeditan aset Anda akan membuat versi inventaris baru.

Menerbitkan aset inventaris proyek ke DataZone katalog Amazon

Langkah selanjutnya menggunakan Amazon DataZone untuk membuat katalog data Anda, adalah membuat aset inventaris proyek Anda dapat ditemukan oleh pengguna domain. Anda dapat melakukan ini dengan menerbitkan aset inventaris ke DataZone katalog Amazon. Hanya versi terbaru dari aset inventaris yang dapat dipublikasikan ke katalog dan hanya versi terbaru yang diterbitkan yang aktif dalam katalog penemuan. Jika aset inventaris diperbarui setelah dipublikasikan ke DataZone katalog Amazon, Anda harus menerbitkannya lagi secara eksplisit agar versi terbaru berada di katalog penemuan. Dalam rilis Amazon saat ini DataZone, Anda dapat mempublikasikan aset inventaris proyek Anda ke DataZone katalog Amazon dengan cara berikut:

- Publikasikan aset inventaris proyek Anda secara manual ke DataZone katalog Amazon baik melalui portal data atau dengan menggunakan DataZone API Amazon.
- Sebagai bagian dari pembuatan atau pengeditan sumber data, aktifkan opsional Publikasikan aset AWS Glue Anda ke katalog atau Publikasikan aset Amazon Redshift Anda ke pengaturan katalog yang akan digunakan selama sumber data terjadwal atau otomatis berjalan. Saat pengaturan ini diaktifkan, sumber data yang dijalankan akan menambahkan aset ke inventaris proyek Anda dan kemudian juga menerbitkan aset inventaris ke DataZone katalog Amazon. Perhatikan bahwa jika Anda mempublikasikan secara langsung, aset mungkin tidak memiliki metadata bisnis apa pun dan

akan dibuat langsung dapat ditemukan oleh semua pengguna domain. Anda dapat menggunakan pengaturan ini pada sumber data Anda baik melalui portal data atau dengan menggunakan Amazon DataZone API.

Apa itu alur kerja DataZone langganan dan pemenuhan Amazon?

Setelah aset Anda dipublikasikan ke DataZone katalog Amazon, pengguna domain Anda dapat menemukan aset ini, meminta dan mendapatkan akses ke aset tersebut, dan terus menggunakan Amazon DataZone untuk mengatur, berbagi, dan menganalisis aset tersebut.

Pengguna meminta akses ke aset dengan berlangganan aset tersebut atas nama proyek. Setelah permintaan berlangganan dibuat, pemilik aset mendapatkan pemberitahuan dan dapat meninjau permintaan berlangganan dan memutuskan apakah mereka ingin menyetujui atau menolaknya. Jika permintaan berlangganan disetujui oleh pemilik data, proyek berlangganan diberikan akses ke aset tersebut.

Setelah permintaan berlangganan disetujui, Amazon DataZone memulai alur kerja pemenuhan langganan yang secara otomatis menambahkan aset ke semua lingkungan yang berlaku dalam proyek dengan membuat hibah yang diperlukan di AWS Lake Formation atau Amazon Redshift. Ini memungkinkan anggota proyek berlangganan untuk menanyakan aset menggunakan salah satu alat kueri (Amazon Athena atau editor kueri Amazon Redshift) di lingkungan mereka.

Amazon DataZone dapat memicu logika pemenuhan otomatis ini hanya untuk aset terkelola (ini termasuk tabel AWS Glue dan tabel dan tampilan Amazon Redshift). Untuk semua jenis aset lainnya (aset tidak terkelola), Amazon tidak DataZone dapat secara otomatis memicu pemenuhan melainkan menerbitkan acara di Amazon Eventbridge dengan semua detail yang diperlukan dalam muatan acara sehingga Anda dapat membuat hibah yang diperlukan di luar Amazon. DataZone Amazon DataZone juga menyediakan `updateSubscriptionStatus` API yang memungkinkan Anda memperbarui status langganan setelah terpenuhi di luar Amazon DataZone sehingga Amazon DataZone dapat memberi tahu anggota proyek bahwa mereka dapat mulai mengkonsumsi aset tersebut.

Persona pengguna Amazon DataZone

Berikut ini adalah persona DataZone pengguna Amazon utama:

- Administrator domain yang memiliki pengaturan Amazon DataZone sebagai platform analitik untuk organisasi mereka.

Dalam konteks Amazon DataZone, administrator domain menginstal Amazon DataZone di AWS akun, membuat DataZone domain Amazon, dan mengonfigurasi asosiasi AWS akun dan asosiasi penyedia identitas dengan domain Amazon DataZone . Administrator domain juga menggunakan konsol AWS layanan lain seperti AWS Organization and Service Catalog untuk mengonfigurasi Amazon. DataZone

- Pengguna data yang merupakan pengguna utama Amazon DataZone (penerbit aset dan pelanggan) untuk tugas analitik dan pembelajaran mesin mereka.

  Pengguna data termasuk pekerja analitik data, ilmuwan data, dan pengguna sistem yang memproduksi dan mengkonsumsi aset data. Dalam konteks Amazon DataZone, pengguna data membuat dan bergabung dengan proyek dan lingkungan, berlangganan dan menggunakan aset data dengan analitik atau alat pembelajaran mesin yang telah dikonfigurasi sebelumnya, dan mempublikasikan aset data keluaran kembali ke katalog DataZone domain Amazon untuk dibagikan kepada orang lain.

- Pengembang sistem yang membuat templat infrastruktur khusus dan mengintegrasikan Amazon DataZone dengan katalog internal atau sistem produksi.

  Dalam konteks Amazon DataZone, pengembang sistem membangun cetak biru lingkungan (templat infrastruktur) atau pipa CI/CD Infrastruktur-As-Kode sebagai penyedia Lingkungan, jalur data untuk mempromosikan aset data di seluruh lingkungan, sinkronisasi katalog, dan adaptor pemenuhan hibah berlangganan untuk diintegrasikan dengan katalog internal, atau integrasi antara API Amazon dan antarmuka pengguna internal atau sistem produksi jika diperlukan. DataZone

- Petugas tata kelola data yang memiliki definisi dan risiko keamanan organisasi, privasi, dan kebijakan kepatuhan lainnya dan yang memastikan bahwa penggunaan Amazon DataZone di organisasi mereka sesuai dengan definisi ini.

DataZone Terminologi Amazon

Domain

DataZone Domain Amazon adalah entitas pengorganisasian untuk menghubungkan aset, pengguna, dan proyek Anda. Dengan DataZone domain Amazon, Anda memiliki fleksibilitas untuk mencerminkan kebutuhan data dan analitik struktur organisasi Anda, baik itu membuat satu DataZone domain Amazon untuk perusahaan Anda atau beberapa datazone; domain untuk unit bisnis atau tim yang berbeda.

Akun terkait

Mengaitkan AWS akun Anda dengan DataZone domain Amazon memungkinkan Anda mempublikasikan data dari AWS akun ini ke dalam DataZone katalog Amazon dan membuat DataZone proyek Amazon agar berfungsi dengan data Anda di beberapa AWS akun. Permintaan asosiasi akun hanya dapat dimulai di AWS akun yang memiliki DataZone domain Amazon. Permintaan asosiasi akun hanya dapat diterima oleh pengguna administratif AWS akun yang diundang. Setelah AWS akun dikaitkan dengan DataZone domain Amazon, Anda dapat mendaftarkan sumber data Anda seperti katalog AWS Glue dan Amazon Redshift di akun ini ke domain ini. Terkait juga memungkinkan AWS akun untuk membuat DataZone proyek dan lingkungan Amazon.

An Akun AWS dapat dikaitkan dengan satu atau lebih DataZone domain Amazon.

Sumber data

Di Amazon DataZone, Anda dapat menggunakan sumber data untuk mengimpor metadata teknis aset (data) dari database sumber atau gudang data ke Amazon. DataZone Dalam rilis Amazon saat ini DataZone, Anda dapat membuat dan menjalankan sumber data untuk AWS Glue dan Amazon Redshift. Dengan membuat sumber data, Anda membuat sambungan antara Amazon DataZone dan sumber (AWS Glue Data Catalog atau Amazon Redshift Warehouse) yang memungkinkan Anda membaca metadata teknis, termasuk nama tabel, nama kolom, dan tipe data. Dengan membuat sumber data, Anda juga memulai proses sumber data awal yang membuat aset baru atau memperbarui aset yang ada di Amazon DataZone. Saat membuat sumber data atau setelah sumber data berhasil dibuat, Anda juga memiliki opsi untuk menentukan jadwal untuk menjalankan sumber data Anda.

Jalankan sumber data

Di Amazon DataZone, menjalankan sumber data adalah tugas yang DataZone dilakukan Amazon untuk membuat aset dalam inventaris proyek dan juga secara opsional untuk mempublikasikan aset inventaris proyek ke katalog Amazon DataZone . Sumber data berjalan dapat otomatis (dimulai ketika sumber data awalnya dibuat) atau dijadwalkan atau manual. Kriteria pemilihan data memungkinkan Anda menyempurnakan kumpulan data yang ada dan yang akan datang untuk dimasukkan ke dalam inventaris proyek atau DataZone katalog Amazon dan frekuensi pembaruan metadata ke inventaris atau aset katalog tersebut.

Target berlangganan

Di Amazon DataZone, target langganan memungkinkan Anda mengakses data yang telah Anda langgani dalam proyek Anda. Target langganan menentukan lokasi (misalnya, database

atau skema) dan izin yang diperlukan (misalnya, peran IAM) yang DataZone dapat digunakan Amazon untuk membuat koneksi dengan data sumber dan untuk membuat hibah yang diperlukan sehingga anggota DataZone proyek Amazon dapat mulai menanyakan data yang telah mereka langgani.

Permintaan berlangganan

Di Amazon DataZone, permintaan berlangganan adalah proses yang harus diikuti oleh DataZone proyek Amazon agar dapat diberikan akses ke aset tertentu. Permintaan berlangganan dapat disetujui, ditolak, dicabut, atau dikabulkan.

Aset

Di Amazon DataZone, aset adalah entitas yang menyajikan objek data fisik tunggal (misalnya, tabel, dasbor, file) atau objek data virtual (misalnya, tampilan).

Jenis aset

Jenis aset menentukan bagaimana aset direpresentasikan dalam DataZone katalog Amazon. Jenis aset mendefinisikan skema untuk jenis aset tertentu. Ketika aset dibuat, mereka divalidasi terhadap skema yang ditentukan oleh jenis aset mereka (secara default, versi terbaru). Saat pembaruan aset terjadi, Amazon DataZone membuat versi aset baru dan memungkinkan DataZone pengguna Amazon beroperasi di semua versi aset.

Glosarium bisnis

Di Amazon DataZone, glosarium bisnis adalah kumpulan istilah bisnis yang mungkin terkait dengan aset. Glosarium bisnis membantu memastikan bahwa istilah dan definisi yang sama digunakan di seluruh organisasi di berbagai tugas analisis datanya.

Istilah dalam glosarium bisnis dapat ditambahkan ke aset dan kolom untuk mengklasifikasikan atau meningkatkan identifikasi atribut tersebut selama pencarian. Glosarium dapat dipilih sebagai tipe nilai untuk bidang dalam bentuk metadata yang terkait dengan aset. Ketika istilah tertentu dipilih sebagai nilai untuk bidang formulir metadata aset, pengguna dapat mencari istilah glosarium bisnis dan menemukan aset terkait.

Jenis bentuk metadata

Jenis formulir metadata adalah templat yang mendefinisikan metadata yang dikumpulkan dan disimpan saat aset dibuat sebagai inventaris atau diterbitkan dalam domain Amazon. DataZone Jenis bentuk metadata dapat dikaitkan dengan aset data. Jenis formulir metadata membantu administrator domain untuk menentukan formulir metadata yang diperlukan untuk domain tersebut seperti informasi kepatuhan, informasi peraturan, atau klasifikasi. Ini memungkinkan

administrator domain untuk menyesuaikan metadata tambahan untuk aset mereka. Amazon DataZone memiliki tipe bentuk metadata sistem seperti asset-common-details-form -type, column-business-metadata-form -type,,,, glue-table-form-type glue-view-form-type, s3- redshift-table-form-type redshift-view-form-type, dan. object-collection-form-type subscription-terms-form-type suggestion-form-type

Bentuk metadata

Di Amazon DataZone, formulir metadata menentukan metadata yang dikumpulkan dan disimpan saat aset dibuat sebagai inventaris atau diterbitkan dalam domain Amazon. DataZone Definisi bentuk metadata dibuat dalam domain katalog oleh administrator domain. Definisi bentuk metadata terdiri dari satu atau lebih definisi bidang, dengan dukungan untuk tipe data nilai bidang boolean, date, desimal, integer, string, dan glosarium bisnis.

Administrator domain menerapkan formulir metadata ke aset di domain mereka dengan menambahkan formulir metadata ke domain mereka. Penerbit aset kemudian memberikan nilai bidang opsional dan wajib dalam bentuk metadata.

Proyek

Di Amazon DataZone, proyek memungkinkan sekelompok pengguna untuk berkolaborasi dalam berbagai kasus penggunaan bisnis yang melibatkan pembuatan aset dalam inventaris proyek dan dengan demikian membuatnya dapat ditemukan oleh semua anggota proyek, dan kemudian menerbitkan, menemukan, berlangganan, dan mengkonsumsi aset di katalog Amazon. DataZone Anggota proyek menggunakan aset dari DataZone katalog Amazon dan menghasilkan aset baru menggunakan satu atau lebih alur kerja analitis. Anggota proyek dapat menjadi pemilik atau kontributor. Pemilik proyek dapat menambah atau menghapus pengguna lain sebagai pemilik atau kontributor dan mereka dapat memodifikasi atau menghapus proyek. Pembatasan lain pada kontributor dapat didefinisikan dengan kebijakan. Ketika pengguna membuat proyek, mereka menjadi pemilik pertama proyek itu.

Environment

Lingkungan adalah kumpulan sumber daya yang dikonfigurasi (misalnya, bucket Amazon S3, AWS Glue database, atau grup kerja Amazon Athena), dengan sekumpulan prinsipal IAM tertentu (dengan izin kontributor yang ditetapkan) yang dapat beroperasi pada sumber daya tersebut. Setiap lingkungan mungkin juga memiliki kepala sekolah pengguna yang berwenang untuk mengakses sumber daya dan mendapatkan akses ke data melalui langganan dan pemenuhan. Lingkungan dirancang untuk menyimpan tautan yang dapat ditindaklanjuti ke dalam AWS layanan dan IDE dan konsol eksternal. Anggota proyek dapat mengakses layanan seperti konsol Amazon Athena dan lainnya melalui tautan dalam yang dikonfigurasi dalam suatu lingkungan. Pengguna

SSO dan pengguna IAM dari proyek dapat dicakup lebih lanjut untuk menggunakan/mengakses lingkungan tertentu.

Profil lingkungan

Di Amazon DataZone, profil lingkungan adalah template yang dapat Anda gunakan untuk membuat lingkungan. Profil lingkungan dibuat dengan menggunakan cetak biru.

Dengan profil lingkungan, administrator domain dapat membungkus cetak biru dengan parameter yang telah dikonfigurasi sebelumnya, dan kemudian pekerja data dapat dengan cepat membuat sejumlah lingkungan baru dengan memilih profil lingkungan yang ada dan menentukan nama untuk lingkungan baru. Hal ini memungkinkan pekerja data untuk mengelola proyek dan lingkungan mereka secara efisien sambil memastikan bahwa mereka memenuhi kebijakan tata kelola data yang diberlakukan oleh administrator domain mereka.

Cetak biru

Cetak biru yang dengannya lingkungan dibuat mendefinisikan AWS alat dan layanan apa (misalnya, atau Amazon AWS Glue Redshift) anggota proyek tempat lingkungan berada dapat digunakan saat mereka bekerja dengan aset dalam katalog Amazon. DataZone

Dalam rilis Amazon saat ini DataZone , cetak biru default berikut didukung:

- Cetak biru danau data
- Cetak biru gudang data
- Cetak biru Amazon Sagemaker

Profil pengguna

Profil pengguna mewakili DataZone pengguna Amazon. Amazon DataZone mendukung peran IAM dan identitas SSO untuk berinteraksi dengan Konsol DataZone Manajemen Amazon dan portal data untuk tujuan yang berbeda. Administrator domain menggunakan peran IAM untuk melakukan pekerjaan terkait domain administratif awal di Amazon DataZone Management Console, termasuk membuat DataZone domain Amazon baru, mengonfigurasi jenis formulir metadata, dan menerapkan kebijakan. Pekerja data menggunakan identitas perusahaan SSO mereka melalui Pusat Identitas untuk masuk ke Portal DataZone Data Amazon dan mengakses proyek di mana mereka memiliki keanggotaan.

Profil grup

Profil grup mewakili kelompok DataZone pengguna Amazon. Grup dapat dibuat secara manual, atau dipetakan ke grup Active Directory pelanggan perusahaan. Di Amazon DataZone, grup

melayani dua tujuan. Pertama, grup dapat memetakan ke tim pengguna di bagan organisasi, dan dengan demikian mengurangi pekerjaan administratif pemilik DataZone proyek Amazon ketika ada karyawan baru yang bergabung atau meninggalkan tim. Kedua, administrator perusahaan menggunakan grup Active Directory untuk mengelola dan memperbarui status pengguna sehingga administrator DataZone domain Amazon dapat menggunakan keanggotaan grup ini untuk menerapkan kebijakan domain Amazon. DataZone

Administrator domain

Di Amazon DataZone, prinsipal IAM yang membuat DataZone domain Amazon adalah administrator domain default dari domain tersebut. Administrator domain di Amazon DataZone menjalankan fungsionalitas utama untuk domain, termasuk membuat domain, menetapkan administrator domain lain, menambahkan sumber data dan target langganan, membuat proyek dan lingkungan, dan menetapkan pemilik proyek.

Penerbit

Di Amazon DataZone, penerbit mempublikasikan aset ke dalam DataZone katalog Amazon dan dapat mengedit metadata aset yang mereka terbitkan. Jika diberikan otoritas ini, penerbit dapat menyetujui atau menolak permintaan berlangganan ke aset yang mereka terbitkan di katalog Amazon. DataZone

Pelanggan

Di Amazon DataZone, pelanggan adalah DataZone proyek Amazon yang ingin menemukan, mengakses, dan mengkonsumsi aset dalam katalog Amazon DataZone .

Akun AWS pemilik

Di Amazon DataZone, Akun AWS pemilik membuat peran, kebijakan, dan izin di dalamnya Akun AWS yang memungkinkannya dikaitkan dengan DataZone domain Amazon. Akun AWS

Apa yang baru di Amazon DataZone?

Bagian ini menjelaskan fitur dan peningkatan baru di Amazon DataZone berdasarkan tanggal rilis.

Topik

2024

Amazon DataZone meluncurkan integrasi dengan Amazon SageMaker

Dirilis pada 05/06/2024

Amazon DataZone meluncurkan integrasi dengan Amazon SageMaker untuk membantu produsen data dan konsumen beralih ke Amazon dengan mulus SageMaker untuk berkolaborasi dalam proyek pembelajaran mesin (ML) sambil menegakkan tata kelola akses ke data dan aset ML. Dengan integrasi bawaan baru antara Amazon DataZone dan Amazon SageMaker, konsumen dan produsen data dapat merampingkan tata kelola ML di seluruh penyiapan infrastruktur, berkolaborasi dalam inisiatif bisnis, dan mengatur data dan aset ML dengan mudah. Untuk informasi selengkapnya, lihat Bekerja dengan cetak biru DataZone bawaan Amazon dan Bekerja dengan akun terkait untuk mempublikasikan dan mengkonsumsi data.

Amazon DataZone meluncurkan integrasi dengan mode akses hybrid AWS Lake Formation

Dirilis pada 04/03/2024

Amazon DataZone telah memperkenalkan integrasi dengan mode akses hybrid AWS Lake Formation. Integrasi ini memungkinkan Anda untuk dengan mudah mempublikasikan dan membagikan tabel AWS Glue Anda melalui Amazon DataZone, tanpa perlu mendaftarkannya di AWS Lake Formation terlebih dahulu. Untuk memulai, administrator mengaktifkan setelan pendaftaran lokasi data di bawah `DefaultDataLake` cetak biru di konsol Amazon. DataZone Kemudian, ketika konsumen data berlangganan tabel AWS Glue yang dikelola melalui izin IAM, Amazon DataZone pertama-tama mendaftarkan lokasi Amazon S3 dari tabel ini dalam mode hibrida, dan kemudian memberikan akses ke konsumen data dengan mengelola izin pada tabel melalui Lake Formation.

AWS Ini memastikan bahwa izin IAM pada tabel terus ada dengan izin Lake AWS Formation yang baru diberikan, tanpa mengganggu alur kerja yang ada. Untuk informasi selengkapnya, lihat DataZone Integrasi Amazon dengan mode hybrid AWS Lake Formation .

Amazon DataZone meluncurkan integrasi dengan AWS Glue Data Quality

Dirilis pada 04/03/2024

Amazon DataZone meluncurkan integrasi dengan AWS Glue Data Quality dan menawarkan API untuk mengintegrasikan metrik kualitas data dari solusi kualitas data pihak ketiga. Integrasi baru ini memungkinkan Anda mempublikasikan skor Kualitas Data AWS Glue secara otomatis ke dalam katalog data DataZone bisnis Amazon. Amazon DataZone API dapat digunakan untuk menyerap metrik kualitas dari sumber pihak ketiga. Setelah dipublikasikan, konsumen data dapat dengan mudah mencari aset data, melihat metrik kualitas terperinci, dan mengidentifikasi pemeriksaan dan aturan yang gagal - memberdayakan keputusan bisnis. Untuk informasi selengkapnya, lihat Kualitas data di Amazon DataZone.

Rilis ketersediaan umum rekomendasi AI untuk deskripsi di Amazon DataZone

Dirilis pada 03/27/2024

Amazon DataZone mengumumkan rilis ketersediaan umum dari kemampuan berbasis AI generatif baru untuk meningkatkan penemuan data, pemahaman data, dan penggunaan data dengan memperkaya katalog data bisnis. Dengan satu klik, produsen data dapat menghasilkan deskripsi dan konteks data bisnis yang komprehensif, menyoroti kolom yang berdampak, dan menyertakan rekomendasi tentang kasus penggunaan analitis. Peluncuran ini menambahkan dukungan untuk API yang dapat digunakan produsen data untuk menghasilkan deskripsi aset secara terprogram. Untuk informasi selengkapnya, lihat Menggunakan pembelajaran mesin dan AI generatif.

Amazon DataZone meluncurkan perangkat tambahan untuk integrasi Amazon Redshift

Dirilis pada 03/21/2024

Amazon DataZone telah memperkenalkan beberapa peningkatan pada integrasi Amazon Redshift, menyederhanakan proses penerbitan dan berlangganan tabel dan tampilan Amazon Redshift. Pembaruan ini merampingkan pengalaman bagi produsen data dan konsumen, memungkinkan mereka untuk dengan cepat membuat lingkungan gudang data menggunakan kredensional yang

telah dikonfigurasi sebelumnya dan parameter koneksi yang disediakan oleh administrator Amazon mereka. DataZone Selain itu, penyempurnaan ini memberikan administrator kontrol yang lebih besar atas siapa yang dapat menggunakan sumber daya dalam AWS akun mereka dan kluster Amazon Redshift, dan untuk tujuan apa.

- Konfigurasi cetak biru: setelah Anda mengaktifkan `DefaultDataWarehouseBlueprint` cetak biru, Anda dapat mengontrol proyek mana yang dapat menggunakan cetak `DefaultDataWarehouseBlueprint` biru di akun Anda untuk membuat profil lingkungan dengan menetapkan mengelola proyek ke cetak biru yang diaktifkan. Anda juga dapat membuat set parameter di atas `DefaultDataWarehouseBlueprint` dengan menyediakan parameter seperti cluster, database, dan AWS Secret. Anda juga dapat membuat AWS Rahasia dari dalam DataZone konsol Amazon.
- Profil lingkungan: saat membuat profil lingkungan, Anda dapat memilih untuk memberikan parameter Amazon Redshift Anda sendiri atau menggunakan salah satu set parameter dari konfigurasi cetak biru. Jika Anda memilih untuk menggunakan set parameter yang dibuat dalam konfigurasi cetak biru, AWS rahasia hanya memerlukan `AmazonDataZoneDomain` tag (`AmazonDataZoneProject`tag hanya diperlukan jika Anda memilih untuk menyediakan set parameter Anda sendiri di profil lingkungan). Di profil lingkungan, Anda dapat menentukan daftar proyek resmi. Hanya proyek resmi yang dapat menggunakan profil lingkungan ini untuk membuat lingkungan gudang data. Anda juga dapat menentukan data proyek resmi apa yang diizinkan untuk dipublikasikan. Saat ini Anda dapat memilih salah satu opsi berikut: 1) Publikasikan dari skema apa pun, 2) Publikasikan dari skema lingkungan default, 3) Jangan izinkan penerbitan.
- Lingkungan: Produsen data atau konsumen sekarang dapat memilih profil lingkungan untuk membuat lingkungan, tanpa perlu menyediakan parameter Amazon Redshift mereka sendiri termasuk AWS Secret, cluster, workgroup, dan database. Parameter ini di-porting ke lingkungan dari profil lingkungan. Seiring dengan pembuatan lingkungan, Amazon DataZone sekarang juga membuat skema default untuk lingkungan. Anggota proyek telah membaca dan menulis akses ke skema ini dan dapat dengan mudah mempublikasikan tabel apa pun yang dibuat dalam skema ini ke katalog dengan menjalankan sumber data default yang dibuat sebagai bagian dari pembuatan lingkungan. Parameter Amazon Redshift yang digunakan untuk membuat lingkungan juga dapat digunakan untuk membuat sumber data baru (bukan produsen data untuk menyediakan parameter mereka sendiri dalam pembuatan sumber data).

AWS Dukungan Cloud Formation untuk Amazon DataZone

Dirilis pada 01/18/2024

Pengguna Amazon sekarang DataZone dapat memanfaatkan AWS CloudFormation untuk memodelkan dan mengelola serangkaian DataZone sumber daya Amazon secara efektif. Pendekatan ini memfasilitasi penyediaan sumber daya yang konsisten, sementara juga memungkinkan manajemen siklus hidup melalui infrastruktur sebagai praktik kode. Dengan template khusus, Anda dapat dengan tepat menentukan sumber daya yang diperlukan dan saling ketergantungannya. Untuk informasi selengkapnya, lihat referensi jenis DataZone sumber daya Amazon.

Tambahkan prinsipal IAM secara langsung sebagai anggota proyek Amazon DataZone

Dirilis pada 01/05/2024

Anda sekarang dapat menambahkan prinsipal IAM sebagai anggota proyek, bahkan jika prinsipal IAM tersebut belum masuk ke Amazon (persyaratan sebelumnya). DataZone Setelah administrator domain atau administrator TI menambahkan `iam:GetUser` dan `iam:GetRole` ke peran eksekusi domain domain, pemilik proyek dapat menambahkan prinsip IAM sebagai anggota hanya dengan memberikan Nama Resouce Amazon (ARN) dari peran IAM atau pengguna IAM. Prinsipal IAM masih harus memiliki izin IAM yang diperlukan untuk mengakses Amazon DataZone dan yang dapat dikonfigurasi di konsol IAM. Untuk informasi selengkapnya, lihat Menambahkan anggota ke proyek.

Support untuk jenis aset kustom dari Portal Data

Dirilis pada 01/05/2024

Dukungan untuk aset kustom memungkinkan Amazon DataZone untuk membuat katalog aset melalui Portal Data untuk data tidak terstruktur, termasuk dasbor, kueri, dan model, sehingga memudahkan Anda untuk menambahkan aset kustom secara langsung di portal data bersama dengan dukungan API yang tersedia sebelumnya. Kemampuan untuk membuat, memperbarui, dan mempublikasikan aset khusus di Amazon DataZone, memungkinkan Anda berbagi, menemukan, berlangganan semua jenis aset, dan membangun alur kerja bisnis yang menyediakan tata kelola aset tersebut. Untuk informasi selengkapnya, lihat Buat jenis aset khusus.

2023

Hapus domain

Dirilis pada 12/27/2023

Ini adalah fitur yang memungkinkan Anda untuk lebih mudah menghapus domain Anda. Sekarang, Anda dapat melanjutkan dengan penghapusan domain meskipun tidak kosong (seperti dalam berisi proyek, lingkungan, aset, sumber data, dll.). Untuk informasi selengkapnya, lihat Hapus domain.

Mode hibrida

Dirilis pada 12/22/2023

Amazon DataZone telah menambahkan dukungan untuk mode hibrida AWS Lake Formation. Dengan dukungan ini, jika Anda mempublikasikan tabel AWS Glue ke Amazon DataZone dengan lokasi AWS S3-nya yang terdaftar di Lake Formation dalam mode hybrid, Amazon DataZone memperlakukan tabel ini sebagai aset terkelola dan dapat mengelola hibah berlangganan ke tabel ini. Sebelum rilis fitur ini, Amazon DataZone akan memperlakukan tabel ini sebagai aset yang tidak dikelola yaitu, Amazon tidak DataZone akan dapat memberikan langganan ke tabel ini. Untuk informasi selengkapnya, lihat Konfigurasikan izin Lake Formation untuk Amazon DataZone.

Kelayakan HIPAA

Dirilis pada 12/14/2023

Amazon sekarang DataZone mematuhi Undang-Undang Portabilitas dan Akuntabilitas Asuransi Kesehatan AS tahun 1996 (HIPAA). Untuk melihat daftar AWS layanan dengan kepatuhan HIPAA lihat https://aws.amazon.com/compliance/hipaa-eligible-services-reference/.

Rekomendasi AI untuk deskripsi di Amazon DataZone (Pratinjau)

Dirilis pada 11/28/2023

AWS mengumumkan pratinjau kemampuan berbasis AI generatif baru di Amazon DataZone untuk meningkatkan penemuan data, pemahaman data, dan penggunaan data dengan memperkaya katalog data bisnis. Dengan satu klik, produsen data dapat menghasilkan deskripsi dan konteks data bisnis yang komprehensif, menyoroti kolom yang berdampak, dan menyertakan rekomendasi tentang kasus penggunaan analitis. Dengan rekomendasi AI untuk deskripsi di Amazon DataZone, konsumen data dapat mengidentifikasi tabel dan kolom data yang diperlukan untuk analisis, yang meningkatkan kemampuan ditemukan data dan mengurangi back-and-forth komunikasi dengan produsen data. Pratinjau tersedia di DataZone domain Amazon yang disediakan di AWS Wilayah berikut: US East (Virginia N.), US West (Oregon). Untuk informasi selengkapnya, lihat Menggunakan pembelajaran mesin dan AI generatif.

DefaultDataLake peningkatan cetak biru

Dirilis pada 11/20/2023

Amazon DataZone telah menambahkan peningkatan pada DefaultDataLake cetak biru yang memberi Anda kontrol yang lebih baik atas siapa yang dapat mempublikasikan data apa dari akun Anda. AWS Ada dua perubahan utama yang diperkenalkan dengan peluncuran fitur ini.

- Di konsol, setelah Anda mengaktifkan DefaultDataLake cetak biru, Anda dapat mengontrol proyek mana yang dapat menggunakan DefaultDataLake cetak biru di akun Anda untuk membuat profil lingkungan dengan menetapkan mengelola proyek ke cetak biru yang diaktifkan.
- Perubahan kedua ada di portal. Jika Anda membuat profil lingkungan menggunakan DefaultDataLake cetak biru, Anda juga dapat memilih proyek resmi yang diizinkan untuk menggunakan profil lingkungan untuk membuat lingkungan. Secara default, semua proyek diizinkan untuk menggunakan profil lingkungan danau data, tetapi Anda dapat membatasi profil lingkungan untuk proyek tertentu dan juga mengontrol data apa yang dapat dipublikasikan menggunakan lingkungan yang dibuat dengan profil.

Untuk informasi selengkapnya, lihat Buat profil lingkungan.

Mengatur

Untuk menyiapkan Amazon DataZone, Anda harus memiliki AWS akun dan menyiapkan kebijakan dan izin IAM yang diperlukan untuk Amazon. DataZone

Setelah Anda mengatur DataZone izin Amazon, Anda disarankan untuk menyelesaikan langkah-langkah di bagian Memulai yang membawa Anda melalui pembuatan DataZone domain Amazon, mendapatkan URL portal data, dan DataZone alur kerja Amazon dasar untuk produsen data dan konsumen data.

Topik

Mendaftar untuk AWS akun

Jika Anda tidak memiliki AWS akun, selesaikan langkah-langkah berikut untuk membuatnya.

Jika Anda memiliki AWS organisasi, buat akun:

1. Masuk ke AWS Management Console dan buka konsol Organizations di https://console.aws.amazon.com/organizations/.
2. Di panel navigasi, pilih AWS akun.
3. Pilih Tambahkan AWS akun.
4. Pilih Buat AWS akun dan berikan detail yang diminta. Pilih Buat AWS akun.

Untuk mendaftar AWS akun

1. Buka https://portal.aws.amazon.com/billing/signup
2. Ikuti petunjuk online.

   Bagian dari prosedur pendaftaran melibatkan tindakan menerima panggilan telepon dan memasukkan kode verifikasi di keypad telepon.

Saat Anda mendaftar untuk AWS akun, pengguna root AWS akun dibuat. Pengguna root memiliki akses ke semua AWS layanan dan sumber daya di akun. Sebagai praktik terbaik keamanan, tetapkan akses administratif ke pengguna administratif, dan hanya gunakan pengguna root untuk melakukan tugas-tugas yang memerlukan akses pengguna root.

Konfigurasikan izin IAM yang diperlukan untuk menggunakan konsol manajemen Amazon DataZone

Setiap pengguna, grup, atau peran yang ingin menggunakan konsol DataZone manajemen Amazon, harus memiliki izin yang diperlukan.

Topik

- Lampirkan kebijakan wajib dan opsional ke pengguna, grup, atau peran untuk akses DataZone konsol Amazon
- Membuat kebijakan khusus untuk izin IAM untuk mengaktifkan pembuatan peran yang disederhanakan konsol DataZone layanan Amazon
- Membuat kebijakan khusus untuk izin mengelola akun yang terkait dengan domain Amazon DataZone
- (Opsional) Buat kebijakan khusus untuk izin Pusat AWS Identitas untuk mengaktifkan sistem masuk tunggal (SSO) untuk domain Anda
- (Opsional) Buat kebijakan khusus untuk izin Pusat AWS Identitas untuk menambah dan menghapus akses pengguna SSO dan grup SSO ke domain Amazon Anda. DataZone
- (Opsional) Tambahkan prinsipal IAM Anda sebagai pengguna utama untuk membuat DataZone domain Amazon Anda dengan kunci yang dikelola pelanggan dari Key Management Service (AWS KMS)

Lampirkan kebijakan wajib dan opsional ke pengguna, grup, atau peran untuk akses DataZone konsol Amazon

Selesaikan prosedur berikut untuk melampirkan kebijakan kustom yang diperlukan dan opsional ke pengguna, grup, atau peran. Untuk informasi selengkapnya, lihat AWS kebijakan terkelola untuk Amazon DataZone.

1. Masuk ke AWS Management Console dan buka konsol IAM di https://console.aws.amazon.com/iam/.
2. Di panel navigasi, pilih Kebijakan.
3. Pilih kebijakan berikut untuk dilampirkan ke pengguna, grup, atau peran Anda.

   - Dalam daftar kebijakan, pilih kotak centang di sebelah AmazonDataZoneFullAccess. Anda bisa memakai menu Filter dan kotak pencarian untuk mem-filter daftar kebijakan. Untuk informasi selengkapnya, lihat AWS kebijakan terkelola: AmazonDataZoneFullAccess.
   - (Opsional) Buat kebijakan khusus untuk izin IAM untuk mengaktifkan pembuatan peran yang disederhanakan konsol DataZone layanan Amazon.
   - (Opsional) Buat kebijakan khusus untuk izin Pusat AWS Identitas untuk mengaktifkan sistem masuk tunggal (SSO) untuk domain Anda.
   - (Opsional) Buat kebijakan khusus untuk izin Pusat AWS Identitas untuk menambah dan menghapus akses pengguna SSO dan grup SSO ke domain Amazon Anda. DataZone
4. Pilih Tindakan, lalu pilih Lampirkan.
5. Pilih pengguna, grup, atau peran yang ingin Anda lampirkan kebijakan. Anda bisa menggunakan menu Filter dan kotak pencarian untuk mem-filter daftar entitas utama. Setelah memilih pengguna, grup, atau peran, pilih Lampirkan kebijakan.

Membuat kebijakan khusus untuk izin IAM untuk mengaktifkan pembuatan peran yang disederhanakan konsol DataZone layanan Amazon

Selesaikan prosedur berikut untuk membuat kebijakan sebaris khusus agar memiliki izin yang diperlukan DataZone agar Amazon dapat membuat peran yang diperlukan di konsol AWS manajemen atas nama Anda.

1. Masuk ke AWS Management Console dan buka konsol IAM di https://console.aws.amazon.com/iam/.
2. Di panel navigasi, pilih Pengguna atau Grup pengguna.
3. Dalam daftar, pilih nama pengguna atau grup untuk menyematkan kebijakan.
4. Pilih tab Izin dan, jika diperlukan, perluas bagian Kebijakan izin.
5. Pilih Tambahkan izin dan Buat tautan kebijakan sebaris.
6. Di layar Buat Kebijakan, di bagian Editor kebijakan, pilih JSON.

   Buat dokumen kebijakan dengan pernyataan JSON berikut, lalu pilih Berikutnya.

```
{
    "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. Pada layar Kebijakan peninjauan, masukkan nama untuk kebijakan tersebut. Jika Anda puas dengan kebijakan ini, pilih Buat kebijakan. Pastikan bahwa tidak ada kesalahan yang muncul di kotak merah yang ada di bagian atas layar. Perbaiki apapun yang dilaporkan.

Membuat kebijakan khusus untuk izin mengelola akun yang terkait dengan domain Amazon DataZone

Selesaikan prosedur berikut untuk membuat kebijakan sebaris khusus agar memiliki izin yang diperlukan di AWS akun terkait untuk membuat daftar, menerima, dan menolak pembagian sumber daya domain, lalu mengaktifkan, mengonfigurasi, dan menonaktifkan cetak biru lingkungan di akun terkait. Untuk mengaktifkan pembuatan peran disederhanakan konsol DataZone layanan Amazon opsional yang tersedia selama konfigurasi cetak biru, Anda juga harus melakukannya. Membuat kebijakan khusus untuk izin IAM untuk mengaktifkan pembuatan peran yang disederhanakan konsol DataZone layanan Amazon

1. Masuk ke AWS Management Console dan buka konsol IAM di https://console.aws.amazon.com/iam/.
2. Di panel navigasi, pilih Pengguna atau Grup pengguna.
3. Dalam daftar, pilih nama pengguna atau grup untuk menyematkan kebijakan.
4. Pilih tab Izin dan, jika diperlukan, perluas bagian Kebijakan izin.
5. Pilih Tambahkan izin dan Buat tautan kebijakan sebaris.
6. Di layar Buat Kebijakan, di bagian Editor kebijakan, pilih JSON. Buat dokumen kebijakan dengan pernyataan JSON berikut, lalu pilih Berikutnya.

```
{
    "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. Pada layar Kebijakan peninjauan, masukkan nama untuk kebijakan tersebut. Jika Anda puas dengan kebijakan ini, pilih Buat kebijakan. Pastikan bahwa tidak ada kesalahan yang muncul di kotak merah yang ada di bagian atas layar. Perbaiki apapun yang dilaporkan.

(Opsional) Buat kebijakan khusus untuk izin Pusat AWS Identitas untuk mengaktifkan sistem masuk tunggal (SSO) untuk domain Anda

Selesaikan prosedur berikut untuk membuat kebijakan sebaris khusus agar memiliki izin yang diperlukan untuk mengaktifkan sistem masuk tunggal (SSO) menggunakan Pusat Identitas AWS IAM di Amazon. DataZone

1. Masuk ke AWS Management Console dan buka konsol IAM di https://console.aws.amazon.com/iam/.
2. Di panel navigasi, pilih Pengguna atau Grup pengguna.
3. Dalam daftar, pilih nama pengguna atau grup untuk menyematkan kebijakan.

4. Pilih tab Izin dan, jika diperlukan, perluas bagian Kebijakan izin.
5. Pilih Tambahkan izin dan Buat kebijakan sebaris.
6. Di layar Buat Kebijakan, di bagian Editor kebijakan, pilih JSON.

   Buat dokumen kebijakan dengan pernyataan JSON berikut, lalu pilih Berikutnya.

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

7. Pada layar Kebijakan peninjauan, masukkan nama untuk kebijakan tersebut. Jika Anda puas dengan kebijakan ini, pilih Buat kebijakan. Pastikan bahwa tidak ada kesalahan yang muncul di kotak merah yang ada di bagian atas layar. Perbaiki apapun yang dilaporkan.

(Opsional) Buat kebijakan khusus untuk izin Pusat AWS Identitas untuk menambah dan menghapus akses pengguna SSO dan grup SSO ke domain Amazon Anda. DataZone

Selesaikan prosedur berikut untuk membuat kebijakan sebaris khusus agar memiliki izin yang diperlukan untuk menambah dan menghapus akses pengguna SSO dan grup SSO ke domain Amazon Anda. DataZone

1. Masuk ke AWS Management Console dan buka konsol IAM di https://console.aws.amazon.com/iam/.
2. Di panel navigasi, pilih Pengguna atau Grup pengguna.

3. Dalam daftar, pilih nama pengguna atau grup untuk menyematkan kebijakan.
4. Pilih tab Izin dan, jika diperlukan, perluas bagian Kebijakan izin.
5. Pilih Tambahkan izin dan Buat kebijakan sebaris.
6. Di layar Buat Kebijakan, di bagian Editor kebijakan, pilih JSON.

   Buat dokumen kebijakan dengan pernyataan JSON berikut, lalu pilih Berikutnya.

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

7. Pada layar Kebijakan peninjauan, masukkan nama untuk kebijakan tersebut. Jika Anda puas dengan kebijakan ini, pilih Buat kebijakan. Pastikan bahwa tidak ada kesalahan yang muncul di kotak merah yang ada di bagian atas layar. Perbaiki apapun yang dilaporkan.

(Opsional) Tambahkan prinsipal IAM Anda sebagai pengguna utama untuk membuat DataZone domain Amazon Anda dengan kunci yang dikelola pelanggan dari Key Management Service (AWS KMS)

Sebelum Anda dapat membuat DataZone domain Amazon secara opsional dengan kunci yang dikelola pelanggan (CMK) dari Layanan Manajemen AWS Kunci (KMS), selesaikan prosedur berikut untuk menjadikan prinsipal IAM Anda sebagai pengguna kunci KMS Anda.

1. Masuk ke Konsol AWS Manajemen dan buka konsol KMS di https://console.aws.amazon.com/kms/.
2. Untuk melihat tombol di akun yang Anda buat dan kelola, di panel navigasi pilih CMK.
3. Dalam daftar kunci KMS, pilih alias atau ID kunci dari kunci KMS yang ingin Anda periksa.
4. Untuk menambah atau menghapus pengguna kunci, dan untuk mengizinkan atau melarang AWS akun eksternal menggunakan kunci KMS, gunakan kontrol di bagian Pengguna kunci halaman. Pengguna kunci dapat menggunakan kunci KMS dalam operasi kriptografi, seperti mengenkripsi, mendekripsi, mengenkripsi ulang, dan menghasilkan kunci data.

Konfigurasikan izin IAM yang diperlukan untuk menggunakan portal data Amazon DataZone

Setiap pengguna, grup, atau peran yang ingin menggunakan portal atau katalog DataZone data Amazon harus memiliki izin yang diperlukan.

Topik

- Lampirkan kebijakan yang diperlukan ke pengguna, grup, atau peran untuk akses portal DataZone data Amazon
- Lampirkan kebijakan yang diperlukan ke pengguna, grup, atau peran untuk akses DataZone katalog Amazon
- Lampirkan kebijakan opsional ke pengguna, grup, atau peran untuk portal DataZone data Amazon atau akses katalog jika domain Anda dienkripsi dengan kunci yang dikelola pelanggan dari Layanan Manajemen AWS Kunci (KMS)

Lampirkan kebijakan yang diperlukan ke pengguna, grup, atau peran untuk akses portal DataZone data Amazon

Anda dapat mengakses portal DataZone data Amazon dengan menggunakan kredensil atau AWS kredensial masuk tunggal (SSO) Anda. Ikuti petunjuk di bagian di bawah ini untuk mengatur izin yang diperlukan untuk mengakses portal data dengan AWS kredensil Anda. Untuk informasi selengkapnya tentang menggunakan Amazon DataZone dengan SSO, lihatMenyiapkan Pusat AWS Identitas IAM untuk Amazon DataZone.

> **Note**
>
> Hanya prinsipal IAM di AWS akun domain Anda yang dapat mengakses portal data domain. Prinsipal IAM dari AWS akun lain tidak dapat mengakses portal data domain.

Selesaikan prosedur berikut untuk melampirkan kebijakan yang diperlukan ke pengguna, grup, atau peran. Untuk informasi selengkapnya, lihat AWS kebijakan terkelola untuk Amazon DataZone.

1. Masuk ke AWS Management Console dan buka konsol IAM di https://console.aws.amazon.com/iam/.
2. Di panel navigasi, pilih Pengguna, Grup pengguna, atau Peran.
3. Dalam daftar, pilih nama pengguna, grup, atau peran untuk menyematkan kebijakan.
4. Pilih tab Izin dan, jika diperlukan, perluas bagian Kebijakan izin.
5. Pilih Tambahkan izin dan Buat tautan kebijakan sebaris.
6. Di layar Buat Kebijakan, di bagian Editor kebijakan, pilih JSON. Buat dokumen kebijakan dengan pernyataan JSON berikut, lalu pilih Berikutnya.

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

7. Pada layar Kebijakan peninjauan, masukkan nama untuk kebijakan tersebut. Jika Anda puas dengan kebijakan ini, pilih Buat kebijakan. Pastikan bahwa tidak ada kesalahan yang muncul di kotak merah yang ada di bagian atas layar. Perbaiki apapun yang dilaporkan.

Lampirkan kebijakan yang diperlukan ke pengguna, grup, atau peran untuk akses DataZone katalog Amazon

> **Note**
>
> Hanya prinsipal IAM di AWS akun domain Anda yang dapat mengakses katalog domain. Prinsipal IAM dari AWS akun lain tidak dapat mengakses katalog domain.

Anda dapat memberikan akses identitas IAM ke katalog DataZone domain Amazon Anda melalui API dan SDK dengan prosedur berikut. Jika Anda ingin identitas IAM ini juga memiliki akses ke portal DataZone data Amazon, ikuti juga prosedur di atas untuk. Lampirkan kebijakan yang diperlukan ke pengguna, grup, atau peran untuk akses portal DataZone data Amazon Untuk informasi selengkapnya, lihat AWS kebijakan terkelola untuk Amazon DataZone.

1. Masuk ke AWS Management Console dan buka konsol IAM di https://console.aws.amazon.com/iam/.
2. Di panel navigasi, pilih Kebijakan.
3. Dalam daftar kebijakan, pilih tombol radio di sebelah AmazonDataZoneFullUserAccesskebijakan. Anda bisa memakai menu Filter dan kotak pencarian untuk mem-filter daftar kebijakan. Untuk informasi selengkapnya, lihat AWS kebijakan terkelola: AmazonDataZoneFullUserAccess
4. Pilih Tindakan, lalu pilih Lampirkan.
5. Pilih pengguna, grup, atau peran yang ingin Anda lampirkan kebijakan dengan memilih kotak centang di samping setiap prinsipal. Anda bisa menggunakan menu Filter dan kotak pencarian untuk mem-filter daftar entitas utama. Setelah memilih pengguna, grup, atau peran, pilih Lampirkan kebijakan.

Lampirkan kebijakan opsional ke pengguna, grup, atau peran untuk portal DataZone data Amazon atau akses katalog jika domain Anda dienkripsi dengan kunci yang dikelola pelanggan dari Layanan Manajemen AWS Kunci (KMS)

Jika Anda membuat DataZone domain Amazon dengan kunci KMS Anda sendiri untuk enkripsi data, Anda juga harus membuat kebijakan sebaris dengan izin berikut dan melampirkannya ke prinsipal IAM Anda sehingga mereka dapat mengakses portal atau katalog data Amazon. DataZone

1. Masuk ke AWS Management Console dan buka konsol IAM di https://console.aws.amazon.com/iam/.
2. Di panel navigasi, pilih Pengguna, Grup pengguna, atau Peran.
3. Dalam daftar, pilih nama pengguna, grup, atau peran untuk menyematkan kebijakan.
4. Pilih tab Izin dan, jika diperlukan, perluas bagian Kebijakan izin.
5. Pilih Tambahkan izin dan Buat tautan kebijakan sebaris.
6. Di layar Buat Kebijakan, di bagian Editor kebijakan, pilih JSON. Buat dokumen kebijakan dengan pernyataan JSON berikut, lalu pilih Berikutnya.

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

7. Pada layar Kebijakan peninjauan, masukkan nama untuk kebijakan tersebut. Jika Anda puas dengan kebijakan ini, pilih Buat kebijakan. Pastikan bahwa tidak ada kesalahan yang muncul di kotak merah yang ada di bagian atas layar. Perbaiki apapun yang dilaporkan.

Menyiapkan Pusat AWS Identitas IAM untuk Amazon DataZone

> **Note**
>
> AWS Pusat Identitas harus diaktifkan di AWS Wilayah yang sama dengan DataZone domain Amazon Anda. Saat ini, Pusat AWS Identitas hanya dapat diaktifkan di satu AWS Wilayah.

Anda dapat mengakses portal DataZone data Amazon dengan menggunakan kredenal atau kredensial masuk tunggal (SSO) Anda. AWS Ikuti petunjuk di bagian ini untuk menyiapkan Pusat Identitas AWS IAM untuk Amazon DataZone. Untuk informasi selengkapnya tentang menggunakan Amazon DataZone dengan AWS kredensialnya, lihat. Konfigurasikan izin IAM yang diperlukan untuk menggunakan konsol manajemen Amazon DataZone

Anda dapat melewati prosedur di bagian ini jika Anda sudah mengaktifkan Pusat Identitas AWS IAM (penerus AWS Single Sign-On) dan dikonfigurasi di AWS wilayah yang sama di mana Anda ingin membuat domain Amazon Anda. DataZone

Selesaikan prosedur berikut untuk mengaktifkan AWS IAM Identity Center (penerus AWS Single Sign-On).

1. Untuk mengaktifkan Pusat AWS Identitas IAM, Anda harus masuk ke Konsol AWS Manajemen menggunakan kredensil akun manajemen AWS Organisasi Anda. Anda tidak dapat mengaktifkan Pusat Identitas IAM saat masuk dengan kredensil dari akun anggota AWS Organizations. Untuk informasi selengkapnya, lihat Membuat dan mengelola AWS organisasi di Panduan Pengguna Organizations.
2. Buka konsol AWS IAM Identity Center (penerus AWS Single Sign-On) dan gunakan pemilih wilayah di bilah navigasi atas untuk memilih AWS wilayah yang Anda inginkan buat domain Amazon Anda. DataZone
3. Pilih Aktifkan.
4. Pilih sumber identitas Anda.

   Secara default, Anda mendapatkan toko IAM Identity Center untuk manajemen pengguna yang cepat dan mudah. Secara opsional, Anda dapat menghubungkan penyedia identitas eksternal sebagai gantinya. Dalam prosedur ini, kami menggunakan toko IAM Identity Center default.

   Untuk informasi selengkapnya, lihat Memilih sumber identitas Anda.
5. Di panel navigasi Pusat Identitas IAM, pilih Grup, dan pilih Buat grup. Masukkan nama grup dan pilih Buat.
6. Di panel navigasi Pusat Identitas IAM, pilih Pengguna.
7. Pada layar Tambahkan pengguna, masukkan informasi yang diperlukan dan pilih Kirim email ke pengguna dengan instruksi pengaturan kata sandi. Pengguna harus mendapatkan email tentang langkah-langkah pengaturan berikutnya.

8. Pilih Berikutnya: Grup, pilih grup yang Anda inginkan, dan pilih Tambah pengguna. Pengguna harus menerima email yang mengundang mereka untuk menggunakan SSO. Dalam email ini, mereka harus memilih Terima undangan dan mengatur kata sandi.

Setelah membuat DataZone domain Amazon, Anda dapat mengaktifkan Pusat AWS Identitas untuk Amazon DataZone dan memberikan akses ke pengguna SSO dan grup SSO Anda. Untuk informasi selengkapnya, lihat Aktifkan Pusat Identitas IAM untuk Amazon DataZone.

Memulai

Informasi di bagian ini membantu Anda mulai menggunakan Amazon DataZone. Jika Anda baru mengenal Amazon DataZone, mulailah dengan menjadi akrab dengan konsep dan terminologi yang disajikan. DataZone Terminologi dan konsep Amazon

Bagian memulai ini akan membawa Anda melalui alur kerja DataZone quickstart Amazon berikut:

Topik

- Amazon DataZone mulai cepat dengan data AWS Glue
- DataZone Mulai cepat Amazon dengan data Amazon Redshift
- Amazon DataZone mulai cepat dengan skrip contoh

> **Important**
>
> Sebelum Anda memulai langkah-langkah di salah satu alur kerja quickstart ini, Anda harus menyelesaikan prosedur yang dijelaskan di bagian Pengaturan panduan ini. Jika Anda menggunakan AWS akun baru, Anda harus mengonfigurasi izin yang diperlukan untuk menggunakan konsol DataZone manajemen Amazon. Jika Anda menggunakan AWS akun yang memiliki objek Katalog Data AWS Glue yang ada, Anda juga harus mengonfigurasi izin Lake Formation ke Amazon DataZone.

Amazon DataZone mulai cepat dengan data AWS Glue

Topik

- Langkah 1 - Buat DataZone domain Amazon dan portal data
- Langkah 2 - Buat proyek penerbitan
- Langkah 3 - Ciptakan lingkungan
- Langkah 4 - Menghasilkan data untuk penerbitan
- Langkah 5 - Kumpulkan metadata dari Glue AWS
- Langkah 6 - Kurasi dan publikasikan aset data
- Langkah 7 - Buat proyek untuk analisis data
- Langkah 8 - Buat lingkungan untuk analisis data

- Langkah 9 - Cari katalog data dan berlangganan data
- Langkah 10 - Menyetujui permintaan berlangganan
- Langkah 11 - Buat kueri dan analisis data di Amazon Athena

Langkah 1 - Buat DataZone domain Amazon dan portal data

Bagian ini menjelaskan langkah-langkah membuat DataZone domain Amazon dan portal data untuk alur kerja ini.

Selesaikan prosedur berikut untuk membuat DataZone domain Amazon. Untuk informasi selengkapnya tentang DataZone domain Amazon, lihat DataZone Terminologi dan konsep Amazon.

1. Arahkan ke DataZone konsol Amazon di https://console.aws.amazon.com/datazone, masuk, lalu pilih Buat domain.

   > **Note**
   >
   > Jika Anda ingin menggunakan DataZone domain Amazon yang ada untuk alur kerja ini, pilih Lihat domain, lalu pilih domain yang ingin Anda gunakan, lalu lanjutkan ke Langkah 2 membuat proyek penerbitan.

2. Pada halaman Buat domain, berikan nilai untuk bidang berikut:

   - Nama - tentukan nama untuk domain Anda. Untuk keperluan alur kerja ini, Anda dapat menghubungi pemasaran domain ini.
   - Deskripsi - tentukan deskripsi domain opsional.
   - Enkripsi data - data Anda dienkripsi secara default dengan kunci yang AWS memiliki dan mengelola untuk Anda. Untuk kasus penggunaan ini, Anda dapat meninggalkan pengaturan enkripsi data default.

     Untuk informasi selengkapnya tentang menggunakan kunci yang dikelola pelanggan, lihatEnkripsi data saat istirahat untuk Amazon DataZone. Jika Anda menggunakan kunci KMS Anda sendiri untuk enkripsi data, Anda harus menyertakan pernyataan berikut dalam default AmazonDataZoneDomainExecutionRole Anda.

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

```
  "Statement": [
    {
      "Effect": "Allow",
      "Action": [
        "kms:Decrypt",
        "kms:GenerateDataKey"
      ],
      "Resource": "*"
    }
  ]
}
```

- Akses layanan - biarkan yang dipilih secara default Gunakan opsi peran default tidak berubah.

> **Note**
>
> Jika Anda menggunakan DataZone domain Amazon yang ada untuk alur kerja ini, Anda dapat memilih opsi Gunakan peran layanan yang ada, lalu pilih peran yang ada dari menu tarik-turun.

- Di bawah Pengaturan cepat, pilih Siapkan akun ini untuk konsumsi dan penerbitan data. Opsi ini memungkinkan DataZone cetak biru Amazon bawaan dari Data lake dan gudang Data, dan mengonfigurasi izin yang diperlukan, sumber daya, proyek default, dan data lake default dan profil lingkungan gudang data untuk akun ini. Untuk informasi selengkapnya tentang DataZone cetak biru Amazon, lihat. DataZone Terminologi dan konsep Amazon
- Simpan kolom yang tersisa di bawah Detail izin tidak berubah.

> **Note**
>
> Jika Anda memiliki DataZone domain Amazon yang sudah ada, Anda dapat memilih opsi Gunakan peran layanan yang ada dan kemudian memilih peran yang ada dari menu tarik-turun untuk peran Glue Manage Access, peran Redshift Manage Access, dan peran Penyediaan.

- Jaga agar bidang di bawah Tag tidak berubah.
- Pilih Create domain (Buat domain).

3. Setelah domain berhasil dibuat, pilih domain ini, dan pada halaman ringkasan domain, catat URL portal data untuk domain ini. Anda dapat menggunakan URL ini untuk mengakses portal

DataZone data Amazon Anda untuk menyelesaikan langkah-langkah lainnya dalam alur kerja ini. Anda juga dapat menavigasi ke portal data dengan memilih Buka portal data.

> **Note**
>
> Dalam rilis Amazon saat ini DataZone, setelah domain dibuat, URL yang dihasilkan untuk portal data tidak dapat dimodifikasi.

Pembuatan domain dapat memakan waktu beberapa menit untuk menyelesaikannya. Tunggu domain memiliki status Tersedia sebelum melanjutkan ke langkah berikutnya.

Langkah 2 - Buat proyek penerbitan

Bagian ini menjelaskan langkah-langkah yang diperlukan untuk membuat proyek penerbitan untuk alur kerja ini.

1. Setelah Anda menyelesaikan Langkah 1 di atas dan membuat domain, Anda akan melihat Selamat Datang di Amazon DataZone! jendela. Di jendela ini, pilih Buat proyek.
2. Tentukan nama proyek, misalnya, untuk alur kerja ini, Anda dapat menamainya SalesDataPublishingProject, lalu biarkan bidang lainnya tidak berubah, lalu pilih Buat.

Langkah 3 - Ciptakan lingkungan

Bagian ini menjelaskan langkah-langkah yang diperlukan untuk membuat lingkungan untuk alur kerja ini.

1. Setelah Anda menyelesaikan Langkah 2 di atas dan membuat proyek Anda, Anda akan melihat jendela Proyek Anda siap digunakan. Di jendela ini, pilih Buat lingkungan.
2. Pada halaman Buat lingkungan, tentukan yang berikut ini dan kemudian pilih Buat lingkungan.
3. Tentukan nilai untuk yang berikut:

   - Nama - tentukan nama untuk lingkungan. Untuk panduan ini, Anda bisa menyebutnya. `Default data lake environment`
   - Deskripsi - tentukan deskripsi untuk lingkungan.

- Profil lingkungan - pilih profil DataLakeProfilelingkungan. Ini memungkinkan Anda menggunakan Amazon DataZone dalam alur kerja ini untuk bekerja dengan data di Amazon S3, AWS Glue Catalog, dan Amazon Athena.
- Untuk panduan ini, jaga agar bidang lainnya tidak berubah.

4. Pilih Buat lingkungan.

Langkah 4 - Menghasilkan data untuk penerbitan

Bagian ini menjelaskan langkah-langkah yang diperlukan untuk menghasilkan data untuk penerbitan dalam alur kerja ini.

1. Setelah Anda menyelesaikan langkah 3 di atas, dalam `SalesDataPublishingProject` proyek Anda, di panel sebelah kanan, di bawah alat Analytics, pilih Amazon Athena. Ini membuka editor kueri Athena menggunakan kredensi proyek Anda untuk otentikasi. Pastikan bahwa lingkungan penerbitan Anda dipilih di dropdown DataZone lingkungan Amazon dan `<environment_name>%_pub_db` database dipilih seperti pada editor kueri.
2. Untuk panduan ini, Anda menggunakan skrip kueri Create Table as Select (CTAS) untuk membuat tabel baru yang ingin Anda publikasikan ke Amazon. DataZone Di editor kueri Anda, jalankan skrip CTAS ini untuk membuat `mkt_sls_table` tabel yang dapat Anda publikasikan dan sediakan untuk pencarian dan berlangganan.

```
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
```

Pastikan tabel mkt_sls_table berhasil dibuat di bagian Tabel dan tampilan di sisi kiri. Sekarang Anda memiliki aset data yang dapat dipublikasikan ke dalam DataZone katalog Amazon.

Langkah 5 - Kumpulkan metadata dari Glue AWS

Bagian ini menjelaskan langkah pengumpulan metadata dari AWS Glue untuk alur kerja ini.

1. Setelah Anda menyelesaikan langkah 4 di atas, di portal DataZone data Amazon, pilih `SalesDataPublishingProject` proyek, lalu pilih tab Data, lalu pilih Sumber data di panel sebelah kiri.
2. Pilih sumber yang dibuat sebagai bagian dari proses pembuatan lingkungan.
3. Pilih Run di sebelah menu dropdown Action dan kemudian pilih tombol refresh. Setelah sumber data berjalan selesai, aset ditambahkan ke DataZone inventaris Amazon.

Langkah 6 - Kurasi dan publikasikan aset data

Bagian ini menjelaskan langkah-langkah kurasi dan penerbitan aset data dalam alur kerja ini.

1. Setelah Anda menyelesaikan langkah 5 di atas, di portal DataZone data Amazon, pilih `SalesDataPublishingProject` proyek yang Anda buat pada langkah sebelumnya, pilih tab Data, pilih Data inventaris di panel sebelah kiri, dan temukan tabel. `mkt_sls_table`
2. Buka halaman detail `mkt_sls_table` aset untuk melihat nama bisnis yang dibuat secara otomatis. Pilih ikon metadata yang dihasilkan secara otomatis untuk melihat nama aset dan kolom yang dibuat secara otomatis. Anda dapat menerima atau menolak setiap nama satu per satu atau memilih Terima semua untuk menerapkan nama yang dihasilkan. Secara opsional, Anda juga dapat menambahkan formulir metadata yang tersedia ke aset Anda dan memilih istilah glosarium untuk mengklasifikasikan data Anda.
3. Pilih Publikasikan aset untuk mempublikasikan `mkt_sls_table` aset.

Langkah 7 - Buat proyek untuk analisis data

Bagian ini menjelaskan langkah-langkah pembuatan proyek untuk analisis data. Ini adalah awal dari langkah-langkah konsumen data dari alur kerja ini.

1. Setelah Anda menyelesaikan langkah 6 di atas, di portal DataZone data Amazon, pilih Buat proyek dari menu drop-down Project.
2. Pada halaman Buat proyek, tentukan nama proyek, misalnya, untuk alur kerja ini, Anda dapat menamainya MarketingDataAnalysisProject, lalu biarkan bidang lainnya tidak berubah, lalu pilih Buat.

Langkah 8 - Buat lingkungan untuk analisis data

Bagian ini menjelaskan langkah-langkah menciptakan lingkungan untuk analisis data.

1. Setelah Anda menyelesaikan langkah 7 di atas, di portal DataZone data Amazon, pilih `MarketingDataAnalysisProject` proyek, lalu pilih tab Lingkungan, lalu pilih Buat lingkungan.
2. Pada halaman Buat lingkungan, tentukan yang berikut ini dan kemudian pilih Buat lingkungan.
   - Nama - tentukan nama untuk lingkungan. Untuk panduan ini, Anda bisa menyebutnya. `Default data lake environment`
   - Deskripsi - tentukan deskripsi untuk lingkungan.
   - Profil lingkungan - pilih profil DataLakeProfilelingkungan bawaan.
   - Untuk panduan ini, jaga agar bidang lainnya tidak berubah.

Langkah 9 - Cari katalog data dan berlangganan data

Bagian ini menjelaskan langkah-langkah mencari katalog data dan berlangganan data.

1. Setelah Anda menyelesaikan langkah 8 di atas, di portal DataZone data Amazon, pilih DataZone ikon Amazon, dan di bidang DataZone Pencarian Amazon, cari aset data menggunakan kata kunci (misalnya, 'katalog' atau 'penjualan') di bilah Pencarian portal data.

   Jika perlu, terapkan filter atau penyortiran, dan setelah Anda menemukan aset Data Penjualan Produk, Anda dapat memilihnya untuk membuka halaman detail aset.
2. Pada halaman detail aset Data Penjualan Katalog, pilih Berlangganan.
3. Dalam dialog Subscribe, pilih project MarketingDataAnalysisProjectkonsumen Anda dari dropdown, lalu tentukan alasan permintaan berlangganan Anda, lalu pilih Subscribe.

Langkah 10 - Menyetujui permintaan berlangganan

Bagian ini menjelaskan langkah-langkah menyetujui permintaan berlangganan.

1. Setelah Anda menyelesaikan langkah 9 di atas, di portal DataZone data Amazon, pilih SalesDataPublishingProjectproyek yang Anda gunakan untuk menerbitkan aset Anda.
2. Pilih tab Data, lalu Data yang dipublikasikan, lalu pilih Permintaan masuk.
3. Sekarang Anda dapat melihat baris untuk permintaan baru yang membutuhkan persetujuan. Pilih Lihat permintaan. Berikan alasan untuk persetujuan dan pilih Menyetujui.

Langkah 11 - Buat kueri dan analisis data di Amazon Athena

Sekarang setelah Anda berhasil menerbitkan aset ke DataZone katalog Amazon dan berlangganan, Anda dapat menganalisisnya.

1. Di portal DataZone data Amazon, pilih proyek MarketingDataAnalysisProjectkonsumen Anda dan kemudian, dari panel sebelah kanan, di bawah alat Analytics, pilih tautan Data kueri dengan Amazon Athena. Ini membuka editor kueri Amazon Athena menggunakan kredensi proyek Anda untuk otentikasi. Pilih lingkungan MarketingDataAnalysisProjectkonsumen dari dropdown Amazon DataZone Environment di editor kueri dan kemudian pilih proyek Anda `<environment_name>%sub_db` dari dropdown database.
2. Anda sekarang dapat menjalankan kueri pada tabel berlangganan. Anda dapat memilih tabel dari Tabel dan Tampilan, dan kemudian memilih Pratinjau untuk memiliki pernyataan pilih di editor layar. Jalankan kueri untuk melihat hasilnya.

DataZone Mulai cepat Amazon dengan data Amazon Redshift

Topik

- Langkah 8 - Buat lingkungan untuk analisis data
- Langkah 9 - Cari katalog data dan berlangganan data
- Langkah 10 - Menyetujui permintaan berlangganan
- Langkah 11 - Buat kueri dan analisis data di Amazon Redshift

Langkah 1 - Buat DataZone domain Amazon dan portal data

Selesaikan prosedur berikut untuk membuat DataZone domain Amazon. Untuk informasi selengkapnya tentang DataZone domain Amazon, lihat DataZone Terminologi dan konsep Amazon.

1. Arahkan ke DataZone konsol Amazon di https://console.aws.amazon.com/datazone, masuk, lalu pilih Buat domain.

   > **Note**
   >
   > Jika Anda ingin menggunakan DataZone domain Amazon yang ada untuk alur kerja ini, pilih Lihat domain, lalu pilih domain yang ingin Anda gunakan, lalu lanjutkan ke Langkah 2 membuat proyek penerbitan.

2. Pada halaman Buat domain, berikan nilai untuk bidang berikut:

   - Nama - tentukan nama untuk domain Anda. Untuk keperluan alur kerja ini, Anda dapat memanggil domain `Marketing` ini.
   - Deskripsi - tentukan deskripsi domain opsional.
   - Enkripsi data - data Anda dienkripsi secara default dengan kunci yang AWS memiliki dan mengelola untuk Anda. Untuk panduan ini, Anda dapat meninggalkan pengaturan enkripsi data default.

     Untuk informasi selengkapnya tentang menggunakan kunci yang dikelola pelanggan, lihatEnkripsi data saat istirahat untuk Amazon DataZone. Jika Anda menggunakan kunci KMS Anda sendiri untuk enkripsi data, Anda harus menyertakan pernyataan berikut dalam default AmazonDataZoneDomainExecutionRole Anda.

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

```
      "Effect": "Allow",
      "Action": [
        "kms:Decrypt",
        "kms:GenerateDataKey"
      ],
      "Resource": "*"
    }
  ]
}
```

- Akses layanan - pilih opsi Gunakan peran layanan khusus dan kemudian pilih AmazonDataZoneDomainExecutionRoledari menu tarik-turun.
- Di bawah Pengaturan cepat, pilih Siapkan akun ini untuk konsumsi dan penerbitan data. Opsi ini memungkinkan DataZone cetak biru Amazon bawaan dari Data lake dan gudang Data, dan mengonfigurasi izin dan sumber daya yang diperlukan untuk menyelesaikan langkah-langkah lainnya dalam alur kerja ini. Untuk informasi selengkapnya tentang DataZone cetak biru Amazon, lihat. DataZone Terminologi dan konsep Amazon
- Simpan kolom yang tersisa di bawah Detail izin dan Tag tidak berubah, lalu pilih Buat domain.

3. Setelah domain berhasil dibuat, pilih domain ini, dan pada halaman ringkasan domain, catat URL portal data untuk domain ini. Anda dapat menggunakan URL ini untuk mengakses portal DataZone data Amazon Anda untuk menyelesaikan langkah-langkah lainnya dalam alur kerja ini.

> **Note**
>
> Dalam rilis Amazon saat ini DataZone, setelah domain dibuat, URL yang dihasilkan untuk portal data tidak dapat dimodifikasi.

Pembuatan domain dapat memakan waktu beberapa menit untuk menyelesaikannya. Tunggu domain memiliki status Tersedia sebelum melanjutkan ke langkah berikutnya.

Langkah 2 - Buat proyek penerbitan

Bagian berikut menjelaskan langkah-langkah pembuatan proyek penerbitan dalam alur kerja ini.

1. Setelah Anda menyelesaikan Langkah 1, navigasikan ke portal DataZone data Amazon menggunakan URL portal data dan masuk menggunakan kredenal masuk tunggal (SSO) atau AWS IAM Anda.

2. Pilih Buat proyek, tentukan nama proyek, misalnya, untuk alur kerja ini, Anda dapat menamainya SalesDataPublishingProject, lalu biarkan bidang lainnya tidak berubah, lalu pilih Buat.

Langkah 3 - Ciptakan lingkungan

Bagian berikut menjelaskan langkah-langkah menciptakan lingkungan dalam alur kerja ini.

1. Setelah Anda menyelesaikan Langkah 2, di portal DataZone data Amazon, pilih `SalesDataPublishingProject` proyek yang Anda buat pada langkah sebelumnya, lalu pilih tab Lingkungan, lalu pilih Buat lingkungan.
2. Pada halaman Buat lingkungan, tentukan yang berikut ini dan kemudian pilih Buat lingkungan.

   - Nama - tentukan nama untuk lingkungan. Untuk panduan ini, Anda bisa menyebutnya. `Default data warehouse environment`
   - Deskripsi - tentukan deskripsi untuk lingkungan.
   - Profil lingkungan - pilih profil DataWarehouseProfilelingkungan.
   - Berikan nama cluster Amazon Redshift Anda, nama database, dan ARN rahasia untuk cluster Amazon Redshift tempat data Anda disimpan.

   > **Note**
   >
   > Pastikan rahasia Anda di AWS Secrets Manager menyertakan tag berikut (kunci/nilai):
   >
   > - Untuk cluster Amazon Redshift - datazone.rs.cluster: <cluster_name:database name>
   >
   >   Untuk grup kerja Amazon Redshift Tanpa Server - datazone.rs.workgroup: <workgroup_name:database_name>
   > - AmazonDataZoneProject: <projectID>
   > - AmazonDataZoneDomain: <domainID>
   >
   > Untuk informasi selengkapnya, lihat Menyimpan kredensi database di AWS Secrets Manager.
   >
   > Pengguna database yang Anda berikan di AWS Secrets Manager harus memiliki izin pengguna super.

Langkah 4 - Menghasilkan data untuk penerbitan

Bagian berikut menjelaskan langkah-langkah memproduksi data untuk penerbitan dalam alur kerja ini.

1. Setelah Anda menyelesaikan Langkah 3, di portal DataZone data Amazon, pilih `SalesDataPublishingProject` proyek, dan kemudian, di panel sebelah kanan, di bawah alat Analytics, pilih Amazon Redshift. Ini membuka editor kueri Amazon Redshift menggunakan kredensi proyek Anda untuk autentikasi.
2. Untuk panduan ini, Anda menggunakan skrip kueri Create Table as Select (CTAS) untuk membuat tabel baru yang ingin Anda publikasikan ke Amazon. DataZone Di editor kueri Anda, jalankan skrip CTAS ini untuk membuat `mkt_sls_table` tabel yang dapat Anda publikasikan dan sediakan untuk pencarian dan berlangganan.

```
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
```

   Pastikan tabel mkt_sls_table berhasil dibuat. Sekarang Anda memiliki aset data yang dapat dipublikasikan ke dalam DataZone katalog Amazon.

Langkah 5 - Kumpulkan metadata dari Amazon Redshift

Bagian berikut menjelaskan langkah-langkah pengumpulan metadata dari Amazon Redshift.

1. Setelah Anda menyelesaikan Langkah 4, di portal DataZone data Amazon, pilih `SalesDataPublishingProject` proyek, lalu pilih tab Data, lalu pilih Sumber data.
2. Pilih sumber yang dibuat sebagai bagian dari proses pembuatan lingkungan.
3. Pilih Run di sebelah menu dropdown Action dan kemudian pilih tombol refresh. Setelah sumber data berjalan selesai, aset ditambahkan ke DataZone inventaris Amazon.

Langkah 6 - Kurasi dan publikasikan aset data

Bagian berikut menjelaskan langkah-langkah kurasi dan penerbitan aset data dalam alur kerja ini.

1. Setelah Anda menyelesaikan langkah 5, di portal DataZone data Amazon, pilih `SalesDataPublishingProject` proyek, lalu pilih tab Data, pilih Data inventaris, dan temukan `mkt_sls_table` tabel.
2. Buka halaman detail `mkt_sls_table` aset untuk melihat nama bisnis yang dibuat secara otomatis. Pilih ikon metadata yang dihasilkan secara otomatis untuk melihat nama aset dan kolom yang dibuat secara otomatis. Anda dapat menerima atau menolak setiap nama satu per satu atau memilih Terima semua untuk menerapkan nama yang dihasilkan. Secara opsional, Anda juga dapat menambahkan formulir metadata yang tersedia ke aset Anda dan memilih istilah glosarium untuk mengklasifikasikan data Anda.
3. Pilih Publikasikan untuk mempublikasikan `mkt_sls_table` aset.

Langkah 7 - Buat proyek untuk analisis data

Bagian berikut menjelaskan langkah-langkah membuat proyek untuk analisis data dalam alur kerja ini.

1. Setelah Anda menyelesaikan Langkah 6, di portal DataZone data Amazon, pilih Buat proyek.
2. Di halaman Buat proyek, tentukan nama proyek, misalnya, untuk alur kerja ini, Anda dapat menamainya MarketingDataAnalysisProject, lalu biarkan bidang lainnya tidak berubah, lalu pilih Buat.

Langkah 8 - Buat lingkungan untuk analisis data

Bagian berikut menjelaskan langkah-langkah menciptakan lingkungan untuk analisis data dalam alur kerja ini.

1. Setelah Anda menyelesaikan Langkah 7, di portal DataZone data Amazon, pilih `MarketingDataAnalysisProject` proyek yang Anda buat pada langkah sebelumnya, lalu pilih tab Lingkungan, lalu pilih Tambahkan lingkungan.
2. Pada halaman Buat lingkungan, tentukan yang berikut ini dan kemudian pilih Buat lingkungan.
   - Nama - tentukan nama untuk lingkungan. Untuk panduan ini, Anda bisa menyebutnya. `Default data warehouse environment`
   - Deskripsi - tentukan deskripsi untuk lingkungan.
   - Profil lingkungan - pilih profil DataWarehouseProfilelingkungan.
   - Berikan nama cluster Amazon Redshift Anda, nama database, dan ARN rahasia untuk cluster Amazon Redshift tempat data Anda disimpan.

     > **Note**
     >
     > Pastikan rahasia Anda di AWS Secrets Manager menyertakan tag berikut (kunci/nilai):
     >
     > - Untuk cluster Amazon Redshift - datazone.rs.cluster: <cluster_name:database name>
     >
     >   Untuk grup kerja Amazon Redshift Tanpa Server - datazone.rs.workgroup: <workgroup_name:database_name>
     > - AmazonDataZoneProject: <projectID>
     > - AmazonDataZoneDomain: <domainID>
     >
     > Untuk informasi selengkapnya, lihat Menyimpan kredensi database di AWS Secrets Manager.
     > Pengguna database yang Anda berikan di AWS Secrets Manager harus memiliki izin pengguna super.

   - Untuk panduan ini, jaga agar bidang lainnya tidak berubah.

Langkah 9 - Cari katalog data dan berlangganan data

Bagian berikut menjelaskan langkah-langkah mencari katalog data dan berlangganan data.

1. Setelah Anda menyelesaikan Langkah 8, di portal DataZone data Amazon, cari aset data menggunakan kata kunci (misalnya, 'katalog' atau 'penjualan') di bilah Pencarian portal data.

Jika perlu, terapkan filter atau penyortiran, dan setelah Anda menemukan aset Data Penjualan Produk, Anda dapat memilihnya untuk membuka halaman detail aset.

2. Pada halaman detail aset Data Penjualan Produk, pilih Berlangganan.
3. Dalam dialog, pilih proyek konsumen Anda dari dropdown, berikan alasan permintaan akses, lalu pilih Berlangganan.

Langkah 10 - Menyetujui permintaan berlangganan

Bagian berikut menjelaskan langkah-langkah menyetujui permintaan berlangganan dalam alur kerja ini.

1. Setelah Anda menyelesaikan Langkah 9, di portal DataZone data Amazon, pilih SalesDataPublishingProjectproyek yang Anda gunakan untuk menerbitkan aset Anda.
2. Pilih tab Data, lalu Data yang dipublikasikan, lalu Permintaan masuk.
3. Pilih tautan permintaan tampilan dan kemudian pilih Menyetujui.

Langkah 11 - Buat kueri dan analisis data di Amazon Redshift

Sekarang setelah Anda berhasil menerbitkan aset ke DataZone katalog Amazon dan berlangganan, Anda dapat menganalisisnya.

1. Di portal DataZone data Amazon, di panel sebelah kanan, klik tautan Amazon Redshift. Ini membuka editor kueri Amazon Redshift menggunakan kredensi proyek untuk otentikasi.
2. Anda sekarang dapat menjalankan kueri (pilih pernyataan) pada tabel berlangganan. Anda dapat mengklik tabel (three-vertical-dots opsi) dan memilih pratinjau untuk memilih pernyataan di layar editor. Jalankan kueri untuk melihat hasilnya.

Amazon DataZone mulai cepat dengan skrip contoh

Bagian berikut menjelaskan contoh skrip yang memanggil berbagai DataZone API Amazon yang dapat Anda gunakan untuk menyelesaikan tugas-tugas berikut:

Topik

- Buat DataZone domain Amazon dan portal data
- Buat proyek penerbitan

- Buat profil lingkungan
- Buat lingkungan
- Kumpulkan metadata dari Glue AWS
- Kurasi dan publikasikan aset data
- Cari katalog data dan berlangganan data
- Contoh skrip berguna lainnya

Buat DataZone domain Amazon dan portal data

Anda dapat menggunakan skrip contoh berikut untuk membuat DataZone domain Amazon. Untuk informasi selengkapnya tentang DataZone domain Amazon, lihat DataZone Terminologi dan konsep Amazon.

```
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",
    )
```

Buat proyek penerbitan

Anda dapat menggunakan contoh skrip berikut untuk membuat proyek penerbitan di Amazon DataZone.

```
// Create Project
def create_project(domainId):
```

```
    return dzclient.create_project(
        domainIdentifier = domainId,
        name = "sample-project"
    )
```

Buat profil lingkungan

Anda dapat menggunakan contoh skrip berikut untuk membuat profil lingkungan di Amazon DataZone.

Contoh payload ini digunakan saat `CreateEnvironmentProfile` API dipanggil:

```
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"]
            }
        ]
    }
}
```

Contoh skrip ini memanggil `CreateEnvironmentProfile` API:

```
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
```

Ini adalah payload keluaran sampel setelah `CreateEnvironmentProfile` API dipanggil:

```
{
    "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": ""
                    }
                ]
            }
        ]
    }
}
```

Buat lingkungan

Anda dapat menggunakan skrip contoh berikut untuk membuat lingkungan di Amazon 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
```

Kumpulkan metadata dari Glue AWS

Anda dapat menggunakan skrip contoh ini untuk mengumpulkan metadata dari Glue AWS . Skrip ini berjalan pada jadwal standar. Anda dapat mengambil parameter dari skrip sampel dan membuatnya global. Ambil proyek, lingkungan, dan ID domain menggunakan fungsi standar. Sumber data AWS Glue dibuat dan dijalankan pada waktu standar yang dapat diperbarui di bagian cron skrip.

```
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"
    }
}
```

Kurasi dan publikasikan aset data

Anda dapat menggunakan contoh skrip berikut untuk mengkurasi dan mempublikasikan aset data di Amazon. DataZone

Anda dapat menggunakan skrip berikut untuk membuat jenis formulir kustom:

```
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"
    )
```

Anda dapat menggunakan contoh skrip berikut untuk membuat jenis aset kustom:

```
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,
    )
```

Anda dapat menggunakan contoh skrip berikut untuk membuat aset kustom:

```
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\"}"
            }
        ]
    )
```

Anda dapat menggunakan contoh skrip berikut untuk membuat glosarium:

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

Anda dapat menggunakan contoh skrip berikut untuk membuat istilah glosarium:

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

Anda dapat menggunakan skrip contoh berikut untuk membuat aset menggunakan tipe aset yang ditentukan sistem:

```
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\"}"
            }
        ]
    )
```

Anda dapat menggunakan contoh skrip berikut untuk membuat revisi aset dan melampirkan istilah glosarium:

```
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:>"]
    )
```

Anda dapat menggunakan contoh skrip berikut untuk mempublikasikan aset:

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

Cari katalog data dan berlangganan data

Anda dapat menggunakan contoh skrip berikut untuk mencari katalog data dan berlangganan data:

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

Anda dapat menggunakan contoh script berikut untuk mendapatkan ID listing untuk aset:

```
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']
```

Anda dapat menggunakan contoh skrip berikut untuk membuat permintaan berlangganan menggunakan ID daftar:

```
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."
    )
```

Dengan menggunakan `create_subscription_response` hal di atas, dapatkan `subscription_request_id`, lalu terima/setujui langganan menggunakan contoh skrip berikut:

```
subscription_request_id = create_subscription_response["id"]

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

Contoh skrip berguna lainnya

Anda dapat menggunakan contoh skrip berikut untuk menyelesaikan berbagai tugas saat Anda bekerja dengan data Anda di Amazon DataZone.

Gunakan contoh skrip berikut untuk mencantumkan DataZone domain Amazon yang ada:

```
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
```

Gunakan contoh skrip berikut untuk mencantumkan DataZone proyek Amazon yang ada:

```
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
```

Gunakan contoh skrip berikut untuk mencantumkan formulir DataZone metadata Amazon yang ada:

```
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
```

Mengelola DataZone domain Amazon dan akses pengguna

Topik

Buat domain

> **Note**
>
> Jika Anda menggunakan Amazon DataZone dengan Pusat AWS Identitas untuk menyediakan akses ke pengguna dan grup SSO, maka saat ini DataZone domain Amazon Anda harus berada di AWS Wilayah yang sama dengan instans Pusat AWS Identitas Anda.

Amazon DataZone, domain adalah entitas pengorganisasian untuk menghubungkan aset, pengguna, dan proyek Anda. Untuk informasi selengkapnya, lihat DataZone Terminologi dan konsep Amazon.

Untuk membuat DataZone domain Amazon, Anda harus mengambil peran IAM di akun dengan izin administratif. Konfigurasikan izin IAM yang diperlukan untuk menggunakan konsol manajemen Amazon DataZone untuk mendapatkan izin minimum yang diperlukan untuk membuat domain.

Peran IAM tambahan diperlukan oleh Amazon DataZone untuk melakukan tindakan atas nama pengguna domain dengan konfigurasi default. Anda dapat membuat peran IAM ini terlebih dahulu, atau meminta Amazon DataZone membuatnya untuk Anda. Jika Anda DataZone ingin Amazon membuat peran IAM ini untuk Anda selama proses pembuatan domain, maka untuk pembuatan domain Anda harus mengambil peran IAM dengan izin pembuatan peran. Lihat Membuat kebijakan khusus untuk izin IAM untuk mengaktifkan pembuatan peran yang disederhanakan konsol DataZone layanan Amazon . Bergantung pada pilihan pembuatan domain Anda, Amazon DataZone akan

membuat hingga empat peran IAM baru untuk Anda: AmazonDataZoneDomainExecutionRole,, AmazonDataZoneGlueManageAccessRoleAmazonDataZoneRedshiftManageAccessRole, dan AmazonDataZoneProvisioningRole.

Selesaikan prosedur berikut untuk membuat DataZone domain Amazon.

1. Arahkan ke DataZone konsol Amazon di https://console.aws.amazon.com/datazone dan gunakan pemilih wilayah di bilah navigasi atas untuk memilih AWS Wilayah yang sesuai.
2. Pilih Buat domain dan berikan nilai untuk bidang berikut:

   - Nama - tentukan nama ramah untuk domain. Setelah domain dibuat nama ini tidak dapat diubah.
   - Deskripsi - (opsional) tentukan deskripsi domain.
   - Enkripsi data - DataZone Domain Amazon, metadata, dan data pelaporan Anda dienkripsi oleh Layanan Manajemen AWS Kunci (KMS) menggunakan kunci khusus untuk Amazon Anda. DataZone Gunakan bidang ini untuk menentukan apakah Anda ingin menggunakan kunci yang AWS dimiliki atau memilih kunci AWS KMS yang berbeda.

     Untuk informasi selengkapnya tentang menggunakan kunci yang dikelola pelanggan, lihatEnkripsi data saat istirahat untuk Amazon DataZone. Jika Anda menggunakan kunci KMS Anda sendiri untuk enkripsi data, Anda harus menyertakan pernyataan berikut dalam default AmazonDataZoneDomainExecutionRole Anda.

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Sid": "Statement1",
      "Effect": "Allow",
      "Action": [
        "kms:Decrypt",
        "kms:DescribeKey",
        "kms:GenerateDataKey"
      ],
      "Resource": [
        "*"
      ]
    }
  ]
```

```
}
```

- Akses layanan - pilih apakah Amazon DataZone membuat dan menggunakan yang baru DomainExecutionRoleuntuk Anda, atau pilih peran IAM yang ada.
- Penyiapan cepat - (opsional) centang kotak ini untuk memulai lebih cepat dengan meminta Amazon DataZone menyiapkan akun Anda untuk konsumsi dan penerbitan data. Amazon DataZone akan membuat tiga peran IAM untuk menyediakan, menelan, dan mengelola akses ke sumber daya Glue dan AWS Amazon Redshift, membuat bucket Amazon S3 baru, membuat proyek DataZone Amazon administratif, dan membuat profil lingkungan untuk data lake dan data warehouse default cetak biru.
- Tag - (opsional) tentukan AWS tag (pasangan kunci dan nilai) untuk domain.
- Setelah domain berhasil dibuat, browser Anda harus disegarkan untuk menampilkan halaman detail DataZone domain Amazon baru Anda.

Edit domain

Di Amazon DataZone, domain adalah entitas pengorganisasian untuk menghubungkan aset, pengguna, dan proyek Anda. Untuk informasi selengkapnya, lihat DataZone Terminologi dan konsep Amazon.

Setelah membuat DataZone domain Amazon, Anda nantinya dapat mengedit domain menjadi: mengubah deskripsi, mengaktifkan Pusat Identitas IAM, dan menambahkan, mengedit, atau menghapus kunci tag dan nilainya. Untuk mengedit DataZone domain Amazon, Anda harus mengambil peran IAM di akun dengan izin administratif. Konfigurasikan izin IAM yang diperlukan untuk menggunakan konsol manajemen Amazon DataZone untuk mendapatkan izin minimum yang diperlukan untuk mengedit domain.

Untuk mengedit domain, selesaikan langkah-langkah berikut:

1. Masuk ke Konsol AWS Manajemen dan buka DataZone konsol Amazon di https://console.aws.amazon.com/datazone.
2. Pilih Lihat domain dan pilih nama domain dari daftar. Namanya hyperlink.
3. Pada halaman detail untuk domain, pilih Edit.
4.
   - Edit Deskripsi.
   - Atur pengaturan Pusat Identitas IAM. Pelajari lebih lanjut tentang pengaturan ini diMenyiapkan Pusat AWS Identitas IAM untuk Amazon DataZone.

- Tambahkan, edit, atau hapus kunci Tag dan nilainya.

5. Setelah Anda melakukan pengeditan, pilih Perbarui domain.

Hapus domain

Di Amazon DataZone, domain adalah entitas pengorganisasian untuk menghubungkan aset, pengguna, dan proyek Anda. Untuk informasi selengkapnya, lihat DataZone Terminologi dan konsep Amazon.

Tindakan menghapus domain adalah final. Penghapusan secara permanen menghapus setiap entitas DataZone Amazon, termasuk sumber data, proyek, lingkungan, aset, glosarium, dan formulir metadata. Penghapusan tidak menghapus sumber daya non-Amazon DataZone AWS yang DataZone mungkin telah dibantu Amazon Anda buat, seperti peran IAM, bucket S3, database AWS Glue, dan hibah langganan melalui atau Redshift. LakeFormation Jika Anda tidak lagi membutuhkan sumber daya ini, hapus di AWS layanan masing-masing.

Untuk mencegah seseorang menghapus domain secara jahat, menghapus domain memerlukan izin IAM administratif untuk DataZone Amazon, yang dapat Anda konfigurasikan dengan IAM. Untuk mencegah seseorang menghapus domain secara tidak sengaja, menghapus domain memerlukan kata konfirmasi (di DataZone konsol Amazon).

Untuk menghapus domain, selesaikan langkah-langkah berikut:

1. Masuk ke Konsol AWS Manajemen dan buka DataZone konsol Amazon di https://console.aws.amazon.com/datazone.
2. Pilih Lihat domain dan pilih nama domain dari daftar. Namanya hyperlink.
3. Pilih Hapus dan tinjau peringatan informasi.
4. Ketik teks yang diminta untuk mengonfirmasi bahwa Anda memahami peringatan ini. Pilih Hapus.

> **Important**
>
> Menghapus domain Anda adalah tindakan yang tidak dapat dibatalkan yang tidak dapat dibatalkan oleh Anda atau oleh. AWS

> **Note**
>
> Saat Anda atau pengguna domain membuat lingkungan dalam proyek, Amazon DataZone membuat AWS sumber daya di domain atau akun terkait untuk memberi Anda dan pengguna domain fungsionalitas. Di bawah ini adalah daftar AWS sumber daya yang DataZone dapat dibuat Amazon untuk proyek di domain Anda, bersama dengan nama default. Menghapus domain tidak menghapus AWS sumber daya ini di AWS akun Anda.
>
> - <environmentId>Peran IAM: datazone_usr_.
> - <environmentName>Basis data Glue: (1) <environmentName>_pub_db-*, (2) _sub_db-*. Jika sudah ada database nama ini, Amazon DataZone akan menambahkan ID lingkungan.
> - <environmentName>Kelompok kerja Athena: -*. Jika sudah ada workgroup nama ini, Amazon DataZone akan menambahkan ID lingkungan.
> - CloudWatch grup log: datazone_ <environmentId>

Aktifkan Pusat Identitas IAM untuk Amazon DataZone

> **Note**
>
> Untuk menyelesaikan prosedur ini, Anda harus mengaktifkan Pusat AWS Identitas IAM di AWS Wilayah yang sama dengan DataZone domain Amazon Anda.

Anda dapat memberi pengguna dan grup SSO akses ke portal DataZone data Amazon Anda menggunakan AWS IAM Identity Center. Setelah selesaiMenyiapkan Pusat AWS Identitas IAM untuk Amazon DataZone, Anda dapat mengaktifkan pengguna dan grup SSO untuk mengakses portal data DataZone domain Amazon Anda.

Untuk mengaktifkan Pusat AWS Identitas IAM untuk digunakan dengan DataZone domain Amazon Anda, Anda harus mengambil peran IAM di akun dengan izin administratif. Konfigurasikan izin IAM yang diperlukan untuk menggunakan konsol manajemen Amazon DataZone dan Membuat kebijakan khusus untuk izin IAM untuk mengaktifkan pembuatan peran yang disederhanakan konsol DataZone layanan Amazon untuk mendapatkan izin minimum yang diperlukan untuk mengaktifkan Pusat Identitas IAM untuk digunakan dengan Amazon. DataZone

Selesaikan prosedur berikut untuk mengaktifkan Pusat AWS Identitas IAM untuk Amazon DataZone.

1. Masuk ke AWS Management Console dan buka DataZone konsol di https://console.aws.amazon.com/datazone.
2. Pilih Lihat domain dan pilih nama domain dari daftar. Namanya hyperlink.
3. Pada halaman detail untuk domain, pilih Edit.
   - Pilih kotak centang untuk Aktifkan pengguna di Pusat Identitas IAM.
   - Pilih di antara dua mode penugasan pengguna. Setelah domain Anda diperbarui dengan pilihan Anda, itu tidak dapat diubah nanti.
     - Dengan penetapan pengguna Implisit, setiap pengguna yang ditambahkan ke direktori Pusat Identitas IAM Anda dapat mengakses domain Amazon Anda. DataZone
     - Dengan penetapan pengguna eksplisit, Anda akan menambahkan pengguna atau grup tertentu dari direktori Pusat Identitas IAM Anda untuk memberi mereka akses ke domain Amazon Anda. DataZone Anda akan menambah dan menghapus pengguna dan grup ini nanti di DataZone Konsol Amazon.
4. Setelah Anda puas dengan pilihan Anda, pilih Perbarui domain.

Nonaktifkan Pusat Identitas IAM untuk Amazon DataZone

Menonaktifkan Pusat AWS Identitas IAM untuk DataZone domain Amazon akan menghapus akses untuk semua pengguna SSO.

> **Note**
>
> Menonaktifkan IAM Identity Center tidak akan menghentikan penagihan untuk pengguna SSO. Untuk menghentikan penagihan untuk pengguna SSO, Anda harus menonaktifkannya di domain Anda. Penagihan berlanjut hingga akhir bulan di mana pengguna dinonaktifkan. Untuk menonaktifkan pengguna, lihatKelola pengguna di DataZone konsol Amazon.

Anda dapat memberi pengguna dan grup SSO akses ke portal DataZone data Amazon Anda menggunakan AWS IAM Identity Center. Jika Anda telah mengaktifkan Pusat AWS Identitas IAM untuk Amazon DataZone, Anda nantinya dapat menonaktifkan akses untuk semua pengguna.

Untuk menonaktifkan Pusat AWS Identitas IAM untuk digunakan dengan DataZone domain Amazon Anda, Anda harus mengambil peran IAM di akun dengan izin administratif. Konfigurasikan izin IAM yang diperlukan untuk menggunakan konsol manajemen Amazon DataZone dan Membuat kebijakan

khusus untuk izin IAM untuk mengaktifkan pembuatan peran yang disederhanakan konsol DataZone layanan Amazon untuk mendapatkan izin minimum yang diperlukan untuk menonaktifkan Pusat Identitas IAM dari penggunaan dengan Amazon. DataZone

Selesaikan prosedur berikut untuk menonaktifkan Pusat AWS Identitas IAM untuk Amazon DataZone.

1. Masuk ke AWS Management Console dan buka DataZone konsol di https://console.aws.amazon.com/datazone.
2. Pilih Lihat domain dan pilih nama domain dari daftar. Namanya hyperlink.
3. <regionName><accountId><domainName>Salin Nama Sumber Daya Amazon (ARN) untuk domain Anda, yang dimulai dengan arn:aws:datazone: ::domain/.
4. Buka konsol Pusat Identitas IAM di https://console.aws.amazon.com/singlesignon/.
5. Pilih Aplikasi.
6. Pilih domain yang ingin Anda nonaktifkan AWS IAM Identity Center, yang akibatnya akan menghapus akses ke portal data domain untuk semua pengguna SSO. Anda dapat menggunakan menu Filter dan kotak pencarian untuk memfilter daftar aplikasi.
7. Dari menu Tindakan, pilih Nonaktifkan.
8. Pengguna SSO akan kehilangan akses ke DataZone domain Amazon.
9. Untuk mengaktifkan kembali Pusat AWS Identitas IAM untuk DataZone domain Amazon, pilih domain yang ingin Anda aktifkan kembali Pusat Identitas AWS IAM, dan dari menu Tindakan, pilih Aktifkan.

Kelola pengguna di DataZone konsol Amazon

Pengguna Anda dapat mengakses portal DataZone data Amazon dengan menggunakan AWS kredensialnya atau kredensyal masuk tunggal (SSO) mereka. Untuk mengelola pengguna di DataZone konsol Amazon untuk DataZone domain Amazon, Anda harus mengambil peran IAM di akun dengan izin administratif. Konfigurasikan izin IAM yang diperlukan untuk menggunakan konsol manajemen Amazon DataZone untuk mendapatkan izin minimum yang diperlukan untuk mengelola pengguna di DataZone konsol Amazon.

Topik

- Kelola peran dan pengguna IAM
- Kelola pengguna SSO
- Kelola grup SSO

Kelola peran dan pengguna IAM

Peran dan pengguna IAM dibuat menggunakan AWS Identity and Access Management (IAM) and Access Management (IAM) dan mendapatkan akses ke DataZone domain Amazon Anda melalui izin yang dilampirkan padanya melalui kebijakan. Untuk informasi selengkapnya, lihat Konfigurasikan izin IAM yang diperlukan untuk menggunakan portal data Amazon DataZone . Anda dapat melihat daftar peran IAM dan pengguna yang telah mengaktifkan langganan DataZone domain Amazon mereka, menonaktifkan akses mereka, dan mengaktifkan akses mereka jika sebelumnya dinonaktifkan.

1. Masuk ke AWS Management Console dan buka DataZone konsol di https://console.aws.amazon.com/datazone.
2. Pilih Lihat domain dan pilih nama domain dari daftar. Namanya hyperlink.
3. Pada halaman detail untuk domain, pilih Manajemen pengguna.
4. Untuk jenis pengguna, pilih Pengguna IAM untuk melihat daftar pengguna dan peran IAM yang diaktifkan dan dinonaktifkan saat ini.

    - Kolom Nama menunjukkan arn pengguna atau peran IAM.
    - Kolom Status menunjukkan status pengguna IAM saat ini atau peran dalam domain.
        - Aktif berarti bahwa pengguna atau peran IAM telah memanggil API, mengeluarkan perintah (melalui Antarmuka Baris Perintah), atau mengakses DataZone portal Amazon untuk domain Anda, dan Anda ditagih untuk langganan pengguna.
        - Dinonaktifkan berarti bahwa pengguna atau peran IAM memiliki akses mereka diblokir ke domain Amazon DataZone Anda.
5. Untuk menonaktifkan pengguna IAM atau peran yang saat ini diaktifkan, centang kotak di sebelah pengguna dan pilih Nonaktifkan dari menu Tindakan. Pengguna akan kehilangan akses ke DataZone domain Amazon. Penagihan untuk pengguna akan berakhir pada akhir bulan kalender saat ini.
6. Untuk mengaktifkan pengguna IAM atau peran yang saat ini dinonaktifkan, centang kotak di sebelah pengguna dan pilih Aktifkan dari menu Tindakan. Pengguna akan mendapatkan akses ke DataZone domain Amazon jika pengguna atau peran IAM memiliki izin yang sesuai. Penagihan untuk pengguna akan dimulai lagi.

Kelola pengguna SSO

Pengguna SSO dibuat atau disinkronkan dengan penyedia identitas Anda di AWS IAM Identity Center. Untuk informasi selengkapnya, lihat Menyiapkan Pusat AWS Identitas IAM untuk Amazon DataZone dan Aktifkan Pusat Identitas IAM untuk Amazon DataZone untuk mengaktifkan dan mengonfigurasi Pusat AWS Identitas IAM untuk Amazon DataZone. Anda dapat melihat daftar pengguna SSO yang ditetapkan ke domain, menambahkan pengguna SSO, dan menghapus pengguna SSO.

1. Masuk ke AWS Management Console dan buka DataZone konsol di https://console.aws.amazon.com/datazone.
2. Pilih Lihat domain dan pilih nama domain dari daftar. Namanya hyperlink.
3. Pada halaman detail untuk domain, gulir ke bawah dan pilih Manajemen pengguna.
4. Untuk jenis pengguna, pilih Pengguna SSO untuk melihat daftar pengguna SSO saat ini.
   - Kolom Nama menunjukkan nama pengguna SSO.
   - Kolom Status menunjukkan status pengguna SSO saat ini di domain.
     - Ditugaskan berarti bahwa pengguna SSO telah secara eksplisit ditugaskan ke domain. Akibatnya, pengguna memiliki akses ke Amazon DataZone. Status ini hanya digunakan ketika mode penyedia identitas domain Anda disetel ke penetapan eksplisit.
     - Diaktifkan berarti bahwa pengguna SSO telah mengakses DataZone portal Amazon untuk domain dan Anda ditagih untuk langganan pengguna. Aktivasi terjadi secara otomatis.
     - Dinonaktifkan berarti akses pengguna SSO diblokir ke portal data domain. Penagihan untuk pengguna berakhir pada akhir bulan di mana akses mereka dinonaktifkan.
     - Dihapus berarti bahwa pengguna SSO sebelumnya ditetapkan ke domain, tetapi dihapus sebelum diakses.
5. Tambahkan pengguna SSO dengan memilih Tambah dan Tambah pengguna. Opsi ini tidak tersedia jika domain disetel ke penetapan pengguna implisit, yang berarti bahwa semua pengguna di kumpulan identitas memiliki akses ke domain Amazon. DataZone
   - Pada halaman Tambah pengguna, cari alias pengguna yang ingin Anda tambahkan. Daftar akan muncul di bawah kotak pencarian dengan potensi kecocokan.
   - Pilih pengguna yang ingin Anda tambahkan. Alias mereka akan muncul sebagai chip di bawah kotak pencarian.

- Bila Anda puas dengan daftar pengguna yang ingin Anda tambahkan, pilih Tambahkan pengguna.
- Pengguna ditetapkan ke DataZone domain Amazon dengan status Ditugaskan.
- Ketika pengguna pertama kali mengakses portal data domain, status akan berubah secara otomatis menjadi Aktif, dan Anda akan mulai ditagih untuk langganan pengguna.

6. Hapus pengguna SSO yang Ditugaskan dengan memilih pengguna dan memilih Nonaktifkan dari menu Tindakan. Akibatnya, pengguna akan kehilangan akses ke DataZone domain Amazon. Status pengguna akan ditampilkan sebagai Dihapus. Opsi ini tidak tersedia jika domain disetel ke penetapan pengguna implisit.
7. Nonaktifkan pengguna SSO yang Diaktifkan dengan memilih pengguna dan memilih Nonaktifkan dari menu Tindakan. Akibatnya, akses pengguna ke DataZone domain Amazon akan hilang dan diblokir. Penagihan akan berlanjut untuk langganan pengguna hingga akhir bulan. Status pengguna akan ditampilkan sebagai Dinonaktifkan.
8. Aktifkan pengguna SSO Dinonaktifkan dengan memilih pengguna dan memilih Aktifkan dari menu Tindakan. Akibatnya, pengguna akan mendapatkan kembali akses ke DataZone domain Amazon. Penagihan akan segera dimulai. Pengguna akan ditampilkan sebagai Diaktifkan.

Kelola grup SSO

Grup SSO dibuat atau disinkronkan dengan penyedia identitas Anda di Pusat Identitas AWS IAM. Untuk informasi selengkapnya, lihat Menyiapkan Pusat AWS Identitas IAM untuk Amazon DataZone dan Aktifkan Pusat Identitas IAM untuk Amazon DataZone untuk mengaktifkan dan mengonfigurasi Pusat AWS Identitas IAM untuk Amazon DataZone. Anda dapat melihat daftar grup SSO yang ditetapkan ke domain, menambahkan grup SSO, dan menghapus grup SSO.

1. Masuk ke AWS Management Console dan buka DataZone konsol di https://console.aws.amazon.com/datazone.
2. Pilih Lihat domain dan pilih nama domain dari daftar. Namanya hyperlink.
3. Pada halaman detail untuk domain, gulir ke bawah dan pilih Manajemen pengguna.
4. Untuk jenis pengguna, pilih Grup SSO untuk melihat daftar grup SSO saat ini.
   - Kolom Nama menunjukkan nama grup SSO.
   - Kolom Status menunjukkan status grup SSO saat ini di domain.

- Ditugaskan berarti bahwa grup SSO telah secara eksplisit ditetapkan ke domain. Akibatnya, semua pengguna dalam grup memiliki akses ke portal data domain (kecuali pengguna dinonaktifkan).
- Tidak Ditugaskan berarti bahwa grup SSO telah dihapus dari domain. Pengguna dalam grup tidak memiliki akses ke portal data domain melalui keanggotaan mereka di grup ini.

5. Tambahkan grup SSO dengan memilih Tambah dan Tambah grup. Opsi ini tidak tersedia jika domain disetel ke penetapan pengguna implisit, yang berarti bahwa semua pengguna di kumpulan identitas memiliki akses ke DataZone domain Amazon terlepas dari keanggotaan grup.

   - Pada halaman Tambah grup, cari alias grup yang ingin Anda tambahkan. Daftar akan muncul di bawah kotak pencarian dengan potensi kecocokan.
   - Pilih grup yang ingin Anda tambahkan. Alias mereka akan muncul sebagai chip di bawah kotak pencarian.
   - Jika Anda puas dengan daftar grup yang ingin Anda tambahkan, pilih Tambahkan grup.
   - Grup ditetapkan ke DataZone domain Amazon dengan status Ditugaskan.
   - Ketika anggota grup mengakses portal data domain, status akan berubah secara otomatis menjadi Aktif, dan Anda akan mulai ditagih untuk langganan pengguna.

6. Hapus grup SSO yang Ditugaskan dengan memilih grup dan memilih Unassign dari menu Tindakan. Akibatnya, grup akan kehilangan akses ke DataZone domain Amazon. Status grup akan ditampilkan sebagai Tidak Ditugaskan. Pengguna yang mendapatkan akses ke Amazon DataZone melalui keanggotaan mereka di grup ini akan kehilangan akses. Opsi ini tidak tersedia jika domain disetel ke penetapan pengguna implisit. Untuk menghentikan penagihan bagi pengguna yang aksesnya dihapus dengan membatalkan penugasan grup mereka, Anda harus memilih secara manual dan Nonaktifkan profil pengguna mereka.

Mengelola izin pengguna di portal DataZone data Amazon

Dalam rilis Amazon saat ini DataZone, mekanisme otorisasi default memungkinkan semua pengguna yang diautentikasi (IAM dan SSO) dari DataZone domain Amazon untuk membuat proyek, membuat entitas dalam proyek, dan melakukan pencarian. Anggota proyek harus tetap mematuhi izin yang diberikan kepada mereka per pemilik proyek yang ditunjuk atau peran kontributor proyek.

Bekerja dengan cetak biru DataZone bawaan Amazon

Cetak biru yang dengannya lingkungan dibuat mendefinisikan alat dan layanan apa yang anggota proyek yang dapat digunakan oleh lingkungan saat mereka bekerja dengan aset dalam katalog Amazon. DataZone Dalam rilis Amazon saat ini DataZone, ada cetak biru bawaan berikut:

- Cetak biru danau data
- Cetak biru gudang data
- SageMaker Cetak biru Amazon

Topik

Aktifkan cetak biru bawaan di AWS akun yang memiliki domain Amazon DataZone

Cetak biru yang dengannya lingkungan dibuat mendefinisikan alat dan layanan apa yang anggota proyek yang dapat digunakan oleh lingkungan saat mereka bekerja dengan aset dalam katalog Amazon. DataZone

Dalam rilis Amazon saat ini DataZone, ada beberapa cetak biru bawaan: cetak biru danau data, cetak biru gudang data, dan cetak biru Amazon. SageMaker

- Cetak biru data lake berisi definisi untuk meluncurkan dan mengonfigurasi serangkaian layanan (Glue,AWS AWS Lake Formation, Amazon Athena) untuk mempublikasikan dan menggunakan aset data lake di katalog Amazon. DataZone
- Cetak biru gudang data berisi definisi untuk meluncurkan dan mengonfigurasi serangkaian layanan (Amazon Redshift) untuk mempublikasikan dan menggunakan aset Amazon Redshift di katalog Amazon. DataZone
- SageMaker Cetak biru Amazon berisi definisi untuk meluncurkan dan mengonfigurasi serangkaian layanan (Amazon SageMaker Studio) untuk mempublikasikan dan menggunakan aset Amazon SageMaker di katalog Amazon. DataZone

Untuk informasi selengkapnya, lihat DataZone Terminologi dan konsep Amazon.

Saat membuat DataZone domain Amazon, Anda memiliki opsi untuk memilih Pengaturan cepat yang secara otomatis mengaktifkan data lake default dan cetak biru bawaan gudang data default sebagai bagian dari proses pembuatan domain. Pengaturan cepat juga membuat profil lingkungan default dan lingkungan default untuk Anda menggunakan cetak biru bawaan ini.

Jika Anda tidak memilih Penyiapan cepat sebagai bagian dari pembuatan DataZone domain Amazon, Anda dapat menggunakan prosedur di bawah ini untuk mengaktifkan cetak biru bawaan yang tersedia di AWS akun yang menampung domain Amazon ini. DataZone Anda harus mengaktifkan cetak biru bawaan ini sebelum dapat menggunakannya untuk membuat profil lingkungan dan lingkungan di domain ini.

Untuk mengaktifkan cetak biru bawaan di DataZone domain Amazon melalui konsol DataZone manajemen Amazon, Anda harus mengambil peran IAM di akun dengan izin administratif. Konfigurasikan izin IAM yang diperlukan untuk menggunakan konsol manajemen Amazon DataZone untuk mendapatkan izin minimum.

Aktifkan cetak biru bawaan di domain Amazon DataZone

1. Arahkan ke DataZone konsol Amazon di https://console.aws.amazon.com/datazone dan masuk dengan kredensi akun Anda.
2. Pilih Lihat domain dan pilih domain tempat Anda ingin mengaktifkan satu atau beberapa cetak biru bawaan.
3. Pada halaman detail domain, navigasikan ke tab Blueprints.
4. Dari daftar Blueprints, pilih salah satu atau DefaultDataWarehouse, DefaultDataLakeatau cetak biru Amazon. SageMaker
5. Pada halaman detail cetak biru yang dipilih, pilih Aktifkan di akun ini.
6. Pada halaman Izin dan sumber daya, tentukan yang berikut ini:

    - Jika Anda mengaktifkan DefaultDataLakecetak biru, untuk peran Glue Manage Access, tentukan peran layanan baru atau yang sudah ada yang memberikan DataZone otorisasi Amazon untuk menelan dan mengelola akses ke tabel di Glue dan Lake Formation. AWS AWS
    - Jika Anda mengaktifkan DefaultDataWarehousecetak biru, untuk peran Kelola Akses Redshift, tentukan peran layanan baru atau yang sudah ada yang memberikan DataZone otorisasi Amazon untuk menelan dan mengelola akses ke rangkaian data, tabel, dan tampilan di Amazon Redshift.

- Jika Anda mengaktifkan SageMaker cetak biru Amazon, untuk peran SageMaker Kelola Akses, tentukan peran layanan baru atau yang sudah ada yang memberikan izin Amazon DataZone untuk mempublikasikan data Amazon ke katalog. SageMaker Ini juga memberikan DataZone izin Amazon untuk memberikan akses atau mencabut akses ke aset yang SageMaker diterbitkan Amazon dalam katalog.

  > **Important**
  >
  > Saat Anda mengaktifkan SageMaker cetak biru Amazon, Amazon memeriksa apakah peran IAM berikut untuk DataZone DataZone Amazon ada di akun dan wilayah saat ini. Jika peran ini tidak ada, Amazon DataZone secara otomatis membuatnya.
  >
  > - AmazonDataZoneGlueAccess- <region>- <domainId>
  > - AmazonDataZoneRedshiftAccess- <region>- <domainId>

- Untuk peran Penyediaan, tentukan peran layanan baru atau yang sudah ada yang memberikan otorisasi DataZone Amazon untuk membuat dan mengonfigurasi sumber daya lingkungan yang AWS CloudFormation digunakan di akun dan wilayah lingkungan.
- Jika Anda mengaktifkan SageMaker cetak biru Amazon, untuk bucket Amazon S3 untuk sumber data SageMaker -Glue, tentukan bucket Amazon S3 yang akan digunakan oleh semua lingkungan di akun. SageMaker AWS Awalan bucket yang Anda tentukan harus salah satu dari berikut ini:
  - datazon amazon*
  - pembuat sagemaker datazon*
  - pembuat data sagemaker*
  - DataZone-Pembuat sagem*
  - Sagemaker- * DataZone
  - DataZone-SageMaker*
  - SageMaker-DataZone*

7. Pilih Aktifkan cetak biru.

Setelah Anda mengaktifkan cetak biru yang dipilih, Anda dapat mengontrol proyek mana yang dapat menggunakan cetak biru di akun Anda untuk membuat profil lingkungan. Anda dapat melakukan ini dengan menetapkan mengelola proyek ke konfigurasi cetak biru.

Tentukan pengelolaan proyek pada cetak biru yang diaktifkan

1. Arahkan ke DataZone konsol Amazon di https://console.aws.amazon.com/datazone dan masuk dengan kredensi akun Anda.
2. Pilih Lihat Domain dan kemudian pilih domain tempat Anda ingin menambahkan proyek pengelola untuk cetak biru yang dipilih.
3. Pilih tab Blueprints dan kemudian pilih cetak biru yang ingin Anda kerjakan.
4. Secara default, semua proyek dalam domain dapat menggunakan DefaultDataLake atau DefaultDataWareshouse, atau SageMaker cetak biru Amazon di akun untuk membuat profil lingkungan. Namun, Anda dapat membatasi ini dengan menetapkan mengelola proyek ke cetak biru. Untuk menambahkan proyek pengelolaan, pilih Pilih mengelola proyek, lalu pilih proyek yang ingin Anda tambahkan sebagai mengelola proyek dari menu tarik-turun, lalu pilih Pilih mengelola proyek.

Setelah Anda mengaktifkan DefaultDataWarehouse cetak biru di AWS akun Anda, Anda dapat menambahkan set parameter ke konfigurasi cetak biru. Kumpulan parameter adalah sekelompok kunci dan nilai, yang diperlukan Amazon untuk membuat koneksi DataZone ke klaster Amazon Redshift Anda dan digunakan untuk membuat lingkungan gudang data. Parameter ini mencakup nama cluster Amazon Redshift Anda, database, dan AWS rahasia yang menyimpan kredensi ke cluster.

Menambahkan set parameter ke DefaultDataWarehouse cetak biru

1. Arahkan ke DataZone konsol Amazon di https://console.aws.amazon.com/datazone dan masuk dengan kredensi akun Anda.
2. Pilih Lihat domain dan kemudian pilih domain tempat Anda ingin menambahkan set parameter.
3. Pilih tab Blueprints dan kemudian pilih DefaultDataWareshouse cetak biru untuk membuka halaman detail cetak biru.
4. Di bawah tab Set parameter pada halaman detail cetak biru, pilih Buat set parameter.
    - Berikan Nama untuk set parameter.
    - Secara opsional, berikan deskripsi untuk set parameter.
    - Pilihan wilayah
    - Pilih cluster Amazon Redshift atau Amazon Redshift Tanpa Server.

- Pilih ARN AWS rahasia yang menyimpan kredensional ke cluster Amazon Redshift yang dipilih atau workgroup Amazon Redshift Tanpa Server. AWS Rahasia harus ditandai dengan `AmazonDataZoneDomain : [Domain_ID]` tag agar memenuhi syarat untuk digunakan dalam set parameter.
  - Jika Anda tidak memiliki AWS rahasia yang ada, Anda juga dapat membuat rahasia baru dengan memilih Buat AWS Rahasia Baru. Ini membuka kotak dialog di mana Anda dapat memberikan nama rahasia, nama pengguna, dan kata sandi. Setelah Anda memilih Buat AWS Rahasia Baru, Amazon DataZone membuat rahasia baru di layanan AWS Secrets Manager dan memastikan bahwa rahasia tersebut ditandai dengan domain tempat Anda mencoba membuat set parameter.
- Jika Anda memilih klaster Amazon Redshift pada langkah di atas, sekarang pilih cluster dari dropdown. Jika Anda memilih workgroup Amazon Redshift pada langkah di atas, sekarang pilih workgroup dari drop-down.
- Masukkan nama database dalam klaster Amazon Redshift atau grup kerja Amazon Redshift Serverless yang dipilih.
- Pilih Buat set parameter.

Setelah Anda mengaktifkan SageMaker cetak biru Amazon di AWS akun Anda, Anda dapat menambahkan set parameter ke konfigurasi cetak biru. Set parameter adalah sekelompok kunci dan nilai, yang diperlukan Amazon untuk membuat koneksi DataZone ke Amazon Anda SageMaker dan digunakan untuk membuat lingkungan pembuat sagemaker.

Menambahkan set parameter ke SageMaker cetak biru Amazon

1. Arahkan ke DataZone konsol Amazon di https://console.aws.amazon.com/datazone dan masuk dengan kredensi akun Anda.
2. Pilih Lihat domain dan kemudian pilih domain yang berisi cetak biru yang diaktifkan di mana Anda ingin menambahkan set parameter.
3. Pilih tab Blueprints dan kemudian pilih SageMaker cetak biru Amazon untuk membuka halaman detail cetak biru.
4. Di bawah tab Set parameter pada halaman detail cetak biru, pilih Buat set parameter, lalu tentukan yang berikut ini:
   - Berikan Nama untuk set parameter.
   - Secara opsional, berikan Deskripsi untuk set parameter.

- Tentukan jenis otentikasi SageMaker domain Amazon. Anda dapat memilih IAM atau IAM Identity Center (SSO).
- Tentukan suatu AWS wilayah.
- Tentukan kunci AWS KMS untuk enkripsi data. Anda dapat memilih kunci yang ada atau membuat kunci baru.
- Di bawah parameter Lingkungan, tentukan yang berikut ini:
  - ID VPC - ID yang Anda gunakan untuk VPC lingkungan Amazon. SageMaker Anda dapat menentukan yang sudah ada atau membuat VPC baru.
  - Subnet - satu atau lebih ID untuk berbagai alamat IP untuk sumber daya tertentu dalam VPC Anda.
  - Akses jaringan - pilih VPC saja atau Internet publik saja.
  - Grup keamanan - grup keamanan untuk digunakan saat mengkonfigurasi VPC dan subnet.
- Di bawah Parameter sumber data, pilih salah satu dari berikut ini:
  - AWS Glue saja
  - AWS Glu+Amazon Redshift Tanpa Server. Jika Anda memilih opsi ini, tentukan yang berikut ini:
    - Tentukan ARN AWS rahasia yang menyimpan kredensional ke cluster Amazon Redshift yang dipilih. AWS Rahasia harus ditandai dengan `AmazonDataZoneDomain : [Domain_ID]` tag agar memenuhi syarat untuk digunakan dalam set parameter.

      Jika Anda tidak memiliki AWS rahasia yang ada, Anda juga dapat membuat rahasia baru dengan memilih Buat AWS Rahasia Baru. Ini membuka kotak dialog di mana Anda dapat memberikan nama rahasia, nama pengguna, dan kata sandi. Setelah Anda memilih Buat AWS Rahasia Baru, Amazon DataZone membuat rahasia baru di layanan AWS Secrets Manager dan memastikan bahwa rahasia tersebut ditandai dengan domain tempat Anda mencoba membuat set parameter.
    - Tentukan workgroup Amazon Redshift yang ingin Anda gunakan saat membuat lingkungan.
    - Tentukan nama database (dalam workgroup yang Anda pilih) yang ingin Anda gunakan saat membuat lingkungan.
  - AWS Hanya lem + Amazon Redshift Cluster
    - Tentukan ARN AWS rahasia yang menyimpan kredensional ke cluster Amazon Redshift yang dipilih. AWS Rahasia harus ditandai dengan `AmazonDataZoneDomain : [Domain_ID]` tag agar memenuhi syarat untuk digunakan dalam set parameter.

Jika Anda tidak memiliki AWS rahasia yang ada, Anda juga dapat membuat rahasia baru dengan memilih Buat AWS Rahasia Baru. Ini membuka kotak dialog di mana Anda dapat memberikan nama rahasia, nama pengguna, dan kata sandi. Setelah Anda memilih Buat AWS Rahasia Baru, Amazon DataZone membuat rahasia baru di layanan AWS Secrets Manager dan memastikan bahwa rahasia tersebut ditandai dengan domain tempat Anda mencoba membuat set parameter.

- Tentukan cluster Amazon Redshift yang ingin Anda gunakan saat membuat lingkungan.
- Tentukan nama database (dalam cluster yang Anda pilih) yang ingin Anda gunakan saat membuat lingkungan.

5. Pilih Buat set parameter.

Tambahkan Amazon SageMaker sebagai layanan tepercaya di AWS akun yang memiliki domain Amazon DataZone

Jika Anda telah mengaktifkan SageMaker cetak biru Amazon, Anda juga harus menambahkan SageMaker sebagai salah satu layanan tepercaya di Amazon. DataZone Untuk melakukan ini, selesaikan prosedur berikut:

1. Arahkan ke DataZone konsol Amazon di https://console.aws.amazon.com/datazone dan masuk dengan kredensi akun Anda.
2. Pilih Lihat domain, lalu pilih domain yang berisi SageMaker cetak biru yang diaktifkan.
3. Pilih layanan Tepercaya, lalu pilih Amazon SageMaker, lalu pilih Aktifkan.

Bekerja dengan akun terkait untuk mempublikasikan dan mengkonsumsi data

Mengaitkan AWS akun Anda dengan DataZone domain Amazon Anda memungkinkan pengguna domain mempublikasikan dan menggunakan data dari AWS akun ini. Ada tiga langkah untuk mengatur asosiasi akun.

- Pertama, bagikan domain dengan AWS akun yang diinginkan dengan meminta asosiasi. Amazon DataZone menggunakan AWS Resource Access Manager (RAM) jika AWS akun berbeda dari AWS akun domain. Asosiasi akun hanya dapat dimulai oleh DataZone domain Amazon.
- Kedua, minta pemilik akun menerima permintaan asosiasi.
- Ketiga, minta pemilik akun mengaktifkan cetak biru lingkungan yang diinginkan. Dengan mengaktifkan cetak biru, pemilik akun menyediakan peran IAM dan konfigurasi sumber daya kepada pengguna di domain yang diperlukan untuk membuat dan mengakses sumber daya di akun mereka, seperti database AWS Glue dan cluster Amazon Redshift.

Topik

Minta asosiasi dengan AWS akun lain

> **Note**
>
> Dengan mengirimkan permintaan asosiasi ke AWS akun lain, Anda membagikan domain Anda dengan AWS akun lain dengan AWS Resource Access Manager (RAM). Pastikan untuk memeriksa keakuratan ID akun yang Anda masukkan.

Untuk meminta asosiasi dengan AWS akun lain di DataZone konsol Amazon untuk DataZone domain Amazon, Anda harus mengambil peran IAM di akun dengan izin administratif. Konfigurasikan izin IAM yang diperlukan untuk menggunakan konsol manajemen Amazon DataZone untuk mendapatkan izin minimum yang diperlukan untuk meminta asosiasi akun.

Lengkapi prosedur berikut untuk meminta asosiasi dengan AWS akun lain.

1. Masuk ke Konsol AWS Manajemen dan buka konsol DataZone manajemen Amazon di https://console.aws.amazon.com/datazone.
2. Pilih Lihat domain dan pilih nama domain dari daftar. Namanya hyperlink.
3. Gulir ke bawah ke tab Akun terkait dan pilih Minta asosiasi.
4. Masukkan ID akun yang ingin Anda minta asosiasi. Jika Anda puas dengan daftar ID akun, pilih Permintaan asosiasi.
5. Amazon DataZone membuat pembagian sumber daya di AWS Resource Access Manager atas nama akun Anda, dengan ID akun yang dimasukkan sebagai prinsipal.
6. Anda harus memberi tahu pemilik AWS akun lain untuk menerima permintaan Anda. Undangan berakhir setelah tujuh (7) hari.

Berikan akses akun ke kunci KMS yang dikelola pelanggan Anda

DataZone Domain Amazon dan metadatanya dienkripsi, baik (secara default) menggunakan kunci yang dipegang oleh AWS, atau (opsional) kunci yang dikelola pelanggan dari Layanan Manajemen AWS Kunci (KMS) yang Anda miliki dan berikan selama pembuatan domain. Jika domain Anda dienkripsi dengan kunci yang dikelola pelanggan, ikuti prosedur di bawah ini untuk memberikan izin akun terkait untuk menggunakan kunci KMS.

1. Masuk ke Konsol AWS Manajemen dan buka konsol KMS di https://console.aws.amazon.com/kms/.
2. Untuk melihat tombol di akun yang Anda buat dan kelola, di panel navigasi pilih CMK.
3. Untuk melihat tombol di akun yang Anda buat dan kelola, di panel navigasi pilih CMK.
4. Dalam daftar kunci KMS, pilih alias atau ID kunci dari kunci KMS yang ingin Anda periksa.
5. Untuk mengizinkan atau melarang AWS akun eksternal menggunakan kunci KMS, gunakan kontrol di bagian AWS Akun lain di halaman. Prinsipal IAM di akun ini (dengan izin KMS yang tepat sendiri) dapat menggunakan kunci KMS dalam operasi kriptografi, seperti mengenkripsi, mendekripsi, mengenkripsi ulang, dan menghasilkan kunci data.

Terima permintaan asosiasi akun dari DataZone domain Amazon dan aktifkan cetak biru lingkungan

Untuk menerima asosiasi di konsol DataZone manajemen Amazon dengan DataZone domain Amazon, Anda harus mengambil peran IAM di akun dengan izin administratif. Konfigurasikan izin IAM yang diperlukan untuk menggunakan konsol manajemen Amazon DataZone untuk mendapatkan izin minimum.

Lengkapi yang berikut ini untuk menerima asosiasi dengan DataZone domain Amazon.

1. Masuk ke Konsol AWS Manajemen dan buka konsol DataZone manajemen Amazon di https://console.aws.amazon.com/datazone.
2. Pilih Lihat permintaan dan pilih domain yang mengundang dari daftar. Status undangan harus Diminta. Pilih Permintaan tinjau.
3. Pilih apakah akan mengaktifkan cetak biru lingkungan data lake dan/atau data warehouse default dengan memilih tidak satu pun, keduanya, atau salah satu kotak. Anda bisa melakukannya nanti.

    - Cetak biru lingkungan data lake memungkinkan pengguna domain untuk membuat dan mengelola sumber daya AWS Glue, Amazon S3, dan Amazon Athena untuk dipublikasikan dan dikonsumsi dari data lake.
    - Cetak biru lingkungan gudang data memungkinkan pengguna domain membuat dan mengelola sumber daya Amazon Redshift untuk dipublikasikan dan dikonsumsi dari gudang data.
4. Jika Anda memilih untuk memilih salah satu atau kedua cetak biru lingkungan default, maka konfigurasikan izin dan sumber daya berikut.

    - Peran Kelola akses IAM memberikan izin DataZone ke Amazon untuk memungkinkan pengguna domain menyerap dan mengelola akses ke tabel, seperti AWS Glue dan Amazon Redshift. Anda dapat memilih untuk DataZone membuat Amazon dan menggunakan peran IAM baru, atau Anda dapat memilih dari daftar peran IAM yang ada.
    - Peran IAM Penyediaan memberikan izin ke DataZone Amazon untuk memungkinkan pengguna domain membuat dan mengonfigurasi sumber daya lingkungan, seperti AWS database Glue. Anda dapat memilih untuk DataZone membuat Amazon dan menggunakan peran IAM baru, atau Anda dapat memilih dari daftar peran IAM yang ada.

- Bucket Amazon S3 untuk Data Lake adalah bucket atau path yang DataZone akan digunakan Amazon saat pengguna domain menyimpan data lake data. Anda dapat menggunakan bucket default yang dipilih oleh Amazon DataZone atau memilih jalur Amazon S3 Anda sendiri dengan memasukkan string jalurnya. Jika Anda memilih jalur Amazon S3 Anda sendiri, Anda perlu memperbarui kebijakan IAM untuk DataZone memberi Amazon izin untuk menggunakannya.

5. Bila Anda puas dengan konfigurasi Anda, pilih Terima dan konfigurasikan asosiasi.

Tolak permintaan asosiasi akun dari domain Amazon DataZone

Untuk menolak permintaan asosiasi di konsol DataZone manajemen Amazon dari DataZone domain Amazon, Anda harus mengambil peran IAM di akun dengan izin administratif. Konfigurasikan izin IAM yang diperlukan untuk menggunakan konsol manajemen Amazon DataZone untuk mendapatkan izin minimum.

Lengkapi yang berikut ini untuk menolak permintaan asosiasi dari DataZone domain Amazon.

1. Masuk ke Konsol AWS Manajemen dan buka konsol DataZone manajemen Amazon di https://console.aws.amazon.com/datazone.
2. Pilih Lihat permintaan dan pilih domain yang mengundang dari daftar. Status undangan harus Diminta. Pilih Tolak asosiasi. Konfirmasikan pilihan Anda dengan memilih Tolak asosiasi.

Mengaktifkan cetak biru lingkungan di akun terkait AWS

Untuk mengaktifkan cetak biru lingkungan di konsol DataZone manajemen Amazon, Anda harus mengambil peran IAM di akun dengan izin administratif. Konfigurasikan izin IAM yang diperlukan untuk menggunakan konsol manajemen Amazon DataZone untuk mendapatkan izin minimum.

Selesaikan berikut ini untuk mengaktifkan cetak biru di domain terkait.

1. Masuk ke Konsol AWS Manajemen dan buka konsol DataZone manajemen Amazon di https://console.aws.amazon.com/datazone.
2. Buka panel navigasi kiri dan pilih Domain terkait.
3. Pilih domain yang ingin Anda aktifkan cetak biru lingkungan.
4. Dari daftar Blueprints, pilih salah satu atau DefaultDataWarehouse, DefaultDataLakeatau cetak biru Amazon. SageMaker

5. Pada halaman detail cetak biru yang dipilih, pilih Aktifkan di akun ini.
6. Pada halaman Izin dan sumber daya, tentukan yang berikut ini:

   - Jika Anda mengaktifkan DefaultDataLakecetak biru, untuk peran Glue Manage Access, tentukan peran layanan baru atau yang sudah ada yang memberikan DataZone otorisasi Amazon untuk menyerap dan mengelola akses ke tabel di Glue dan Lake Formation. AWS AWS
   - Jika Anda mengaktifkan DefaultDataWarehousecetak biru, untuk peran Kelola Akses Redshift, tentukan peran layanan baru atau yang sudah ada yang memberikan DataZone otorisasi Amazon untuk menyerap dan mengelola akses ke rangkaian data, tabel, dan tampilan di Amazon Redshift.
   - Jika Anda mengaktifkan SageMaker cetak biru Amazon, untuk peran SageMaker Kelola Akses, tentukan peran layanan baru atau yang sudah ada yang memberikan izin Amazon DataZone untuk mempublikasikan data Amazon ke katalog. SageMaker Ini juga memberikan DataZone izin Amazon untuk memberikan akses atau mencabut akses ke aset yang SageMaker diterbitkan Amazon dalam katalog.

     > **Important**
     >
     > Saat Anda mengaktifkan SageMaker cetak biru Amazon, Amazon memeriksa apakah peran IAM berikut untuk DataZone DataZone Amazon ada di akun dan wilayah saat ini. Jika peran ini tidak ada, Amazon DataZone secara otomatis membuatnya.
     >
     > - AmazonDataZoneGlueAccess- <region>- <domainId>
     > - AmazonDataZoneRedshiftAccess- <region>- <domainId>

   - Untuk peran Penyediaan, tentukan peran layanan baru atau yang sudah ada yang memberikan otorisasi DataZone Amazon untuk membuat dan mengonfigurasi sumber daya lingkungan yang AWS CloudFormation digunakan di akun dan wilayah lingkungan.
   - Jika Anda mengaktifkan SageMaker cetak biru Amazon, untuk bucket Amazon S3 untuk sumber data SageMaker -Glue, tentukan bucket Amazon S3 yang akan digunakan oleh semua lingkungan di akun. SageMaker AWS Awalan bucket yang Anda tentukan harus salah satu dari berikut ini:
     - datazon amazon*
     - pembuat sagemaker datazon*
     - pembuat data sagemaker*

- DataZone-Pembuat sagem*
- Sagemaker- * DataZone
- DataZone-SageMaker*
- SageMaker-DataZone*

7. Pilih Aktifkan cetak biru.

Setelah Anda mengaktifkan cetak biru yang dipilih, Anda dapat mengontrol proyek mana yang dapat menggunakan cetak biru di akun Anda untuk membuat profil lingkungan. Anda dapat melakukan ini dengan menetapkan mengelola proyek ke konfigurasi cetak biru.

Tentukan pengelolaan proyek pada diaktifkan DefaultDataLake atau DefaultDataWarehouse cetak biru

1. Arahkan ke DataZone konsol Amazon di https://console.aws.amazon.com/datazone dan masuk dengan kredensil akun Anda.
2. Buka panel navigasi kiri dan pilih Domain terkait dan kemudian pilih domain tempat Anda ingin menambahkan proyek pengelolaan.
3. Pilih tab Blueprints dan kemudian pilih DefaultDataLake atau cetak biru. DefaultDataWareshouse
4. Secara default, semua proyek dalam domain dapat menggunakan DefaultDataLake atau DefaultDataWareshouse cetak biru di akun untuk membuat profil lingkungan. Namun, Anda dapat membatasi ini dengan menetapkan mengelola proyek ke cetak biru. Untuk menambahkan proyek pengelolaan, pilih Pilih mengelola proyek, lalu pilih proyek yang ingin Anda tambahkan sebagai mengelola proyek dari menu tarik-turun, lalu pilih Pilih mengelola proyek.

Setelah Anda mengaktifkan DefaultDataWarehouse cetak biru di AWS akun Anda, Anda dapat menambahkan set parameter ke konfigurasi cetak biru. Kumpulan parameter adalah sekelompok kunci dan nilai, yang diperlukan Amazon untuk membuat koneksi DataZone ke klaster Amazon Redshift Anda dan digunakan untuk membuat lingkungan gudang data. Parameter ini mencakup nama cluster Amazon Redshift Anda, database, dan AWS rahasia yang menyimpan kredensi ke cluster.

Menambahkan set parameter ke DefaultDataWarehouse cetak biru

1. Arahkan ke DataZone konsol Amazon di https://console.aws.amazon.com/datazone dan masuk dengan kredensil akun Anda.

2. Buka panel navigasi kiri dan pilih Domain terkait dan kemudian pilih domain tempat Anda ingin menambahkan set parameter.
3. Pilih tab Blueprints dan kemudian pilih DefaultDataWareshouse cetak biru untuk membuka halaman detail cetak biru.
4. Di bawah tab Set parameter pada halaman detail cetak biru, pilih Buat set parameter.

    - Berikan Nama untuk set parameter.
    - Secara opsional, berikan deskripsi untuk set parameter.
    - Pilihan wilayah
    - Pilih cluster Amazon Redshift atau Amazon Redshift Tanpa Server.
    - Pilih ARN AWS rahasia yang menyimpan kredensil ke cluster Amazon Redshift yang dipilih atau workgroup Amazon Redshift Tanpa Server. AWS Rahasia harus ditandai dengan `AmazonDataZoneDomain : [Domain_ID]` tag agar memenuhi syarat untuk digunakan dalam set parameter.
        - Jika Anda tidak memiliki AWS rahasia yang ada, Anda juga dapat membuat rahasia baru dengan memilih Buat AWS Rahasia Baru. Ini membuka kotak dialog di mana Anda dapat memberikan nama rahasia, nama pengguna, dan kata sandi. Setelah Anda memilih Buat AWS Rahasia Baru, Amazon DataZone membuat rahasia baru di layanan AWS Secrets Manager dan memastikan bahwa rahasia tersebut ditandai dengan domain tempat Anda mencoba membuat set parameter.
    - Pilih cluster Amazon Redshift atau grup kerja Amazon Redshift Serverless.
    - Masukkan nama database dalam klaster Amazon Redshift atau grup kerja Amazon Redshift Serverless yang dipilih.
    - Pilih Buat set parameter.

Setelah Anda mengaktifkan SageMaker cetak biru Amazon di AWS akun Anda, Anda dapat menambahkan set parameter ke konfigurasi cetak biru. Set parameter adalah sekelompok kunci dan nilai, yang diperlukan Amazon untuk membuat koneksi DataZone ke Amazon Anda SageMaker dan digunakan untuk membuat lingkungan pembuat sagemaker.

Menambahkan set parameter ke SageMaker cetak biru Amazon

1. Arahkan ke DataZone konsol Amazon di https://console.aws.amazon.com/datazone dan masuk dengan kredensil akun Anda.

2. Pilih Lihat domain dan kemudian pilih domain yang berisi cetak biru yang diaktifkan di mana Anda ingin menambahkan set parameter.
3. Pilih tab Blueprints dan kemudian pilih SageMaker cetak biru Amazon untuk membuka halaman detail cetak biru.
4. Di bawah tab Set parameter pada halaman detail cetak biru, pilih Buat set parameter, lalu tentukan yang berikut ini:

   - Berikan Nama untuk set parameter.
   - Secara opsional, berikan Deskripsi untuk set parameter.
   - Tentukan jenis otentikasi SageMaker domain Amazon. Anda dapat memilih IAM atau IAM Identity Center (SSO).
   - Tentukan suatu AWS wilayah.
   - Tentukan kunci AWS KMS untuk enkripsi data. Anda dapat memilih kunci yang ada atau membuat kunci baru.
   - Di bawah parameter Lingkungan, tentukan yang berikut ini:
     - ID VPC - ID yang Anda gunakan untuk VPC lingkungan Amazon. SageMaker Anda dapat menentukan yang sudah ada atau membuat VPC baru.
     - Subnet - satu atau lebih ID untuk berbagai alamat IP untuk sumber daya tertentu dalam VPC Anda.
     - Akses jaringan - pilih VPC saja atau Internet publik saja.
     - Grup keamanan - grup keamanan untuk digunakan saat mengkonfigurasi VPC dan subnet.
   - Di bawah Parameter sumber data, pilih salah satu dari berikut ini:
     - AWS Glue saja
     - AWS Glu+Amazon Redshift Tanpa Server. Jika Anda memilih opsi ini, tentukan yang berikut:
       - Tentukan ARN AWS rahasia yang menyimpan kredensional ke cluster Amazon Redshift yang dipilih. AWS Rahasia harus ditandai dengan `AmazonDataZoneDomain : [Domain_ID]` tag agar memenuhi syarat untuk digunakan dalam set parameter.

         Jika Anda tidak memiliki AWS rahasia yang ada, Anda juga dapat membuat rahasia baru dengan memilih Buat AWS Rahasia Baru. Ini membuka kotak dialog di mana Anda dapat memberikan nama rahasia, nama pengguna, dan kata sandi. Setelah Anda memilih Buat AWS Rahasia Baru, Amazon DataZone membuat rahasia baru di layanan AWS Secrets

Manager dan memastikan bahwa rahasia tersebut ditandai dengan domain tempat Anda mencoba membuat set parameter.

- Tentukan workgroup Amazon Redshift yang ingin Anda gunakan saat membuat lingkungan.
- Tentukan nama database (dalam workgroup yang Anda pilih) yang ingin Anda gunakan saat membuat lingkungan.

- AWS Hanya Iem + Amazon Redshift Cluster
  - Tentukan ARN AWS rahasia yang menyimpan kredensional ke cluster Amazon Redshift yang dipilih. AWS Rahasia harus ditandai dengan `AmazonDataZoneDomain : [Domain_ID]` tag agar memenuhi syarat untuk digunakan dalam set parameter.

    Jika Anda tidak memiliki AWS rahasia yang ada, Anda juga dapat membuat rahasia baru dengan memilih Buat AWS Rahasia Baru. Ini membuka kotak dialog di mana Anda dapat memberikan nama rahasia, nama pengguna, dan kata sandi. Setelah Anda memilih Buat AWS Rahasia Baru, Amazon DataZone membuat rahasia baru di layanan AWS Secrets Manager dan memastikan bahwa rahasia tersebut ditandai dengan domain tempat Anda mencoba membuat set parameter.
  - Tentukan cluster Amazon Redshift yang ingin Anda gunakan saat membuat lingkungan.
  - Tentukan nama database (dalam cluster yang Anda pilih) yang ingin Anda gunakan saat membuat lingkungan.

5. Pilih Buat set parameter.

Tambahkan Amazon SageMaker sebagai layanan tepercaya di AWS akun terkait

Jika Anda telah mengaktifkan SageMaker cetak biru Amazon, Anda juga harus menambahkan SageMaker sebagai salah satu layanan tepercaya di Amazon. DataZone Untuk melakukan ini, selesaikan prosedur berikut:

1. Arahkan ke DataZone konsol Amazon di https://console.aws.amazon.com/datazone dan masuk dengan kredensil akun Anda.
2. Pilih Lihat domain, lalu pilih domain yang berisi SageMaker cetak biru yang diaktifkan.
3. Pilih layanan Tepercaya, lalu pilih Amazon SageMaker, lalu pilih Aktifkan.

Hapus akun terkait

Untuk menghapus AWS akun terkait di konsol DataZone manajemen Amazon, Anda harus mengambil peran IAM di akun dengan izin administratif. Konfigurasikan izin IAM yang diperlukan untuk menggunakan konsol manajemen Amazon DataZone untuk mendapatkan izin minimum.

Selesaikan prosedur berikut untuk menghapus akun terkait dari domain Anda.

1. Masuk ke Konsol AWS Manajemen dan buka konsol DataZone manajemen Amazon di https://console.aws.amazon.com/datazone.
2. Pilih Lihat Domain dan pilih nama domain dari daftar. Namanya hyperlink.
3. Gulir ke bawah ke tab Akun terkait. Pilih ID akun untuk AWS akun yang ingin Anda hapus.
4. Pilih Pisahkan. Konfirmasikan pilihan Anda dengan memasukkan disassociate di bidang dan memilih Disassociate.
5. Akun sekarang dihapus dari domain Anda dan tidak dapat digunakan oleh pengguna domain untuk mempublikasikan dan mengkonsumsi data.

Bekerja dengan katalog DataZone data Amazon

Anda dapat menggunakan katalog data DataZone bisnis Amazon untuk membuat katalog data di seluruh organisasi Anda dengan konteks bisnis dan dengan demikian memungkinkan semua orang di organisasi Anda untuk menemukan dan memahami data dengan cepat. Untuk informasi selengkapnya, lihat DataZone Terminologi dan konsep Amazon.

Topik

Membuat, mengedit, atau menghapus glosarium bisnis

Di Amazon DataZone, glosarium bisnis adalah kumpulan istilah bisnis (kata-kata) yang mungkin terkait dengan aset (data). Ini memberikan kosakata yang sesuai dengan daftar istilah bisnis dan definisi mereka untuk pengguna bisnis untuk memastikan definisi yang sama digunakan di seluruh organisasi saat menganalisis data. Glosarium bisnis dibuat dalam domain katalog dan dapat diterapkan pada aset dan kolom untuk membantu memahami karakteristik utama dari aset atau kolom tersebut. Satu atau lebih istilah glosarium dapat diterapkan. Glosarium bisnis dapat berupa daftar istilah datar di mana istilah apa pun dalam glosarium bisnis dapat dikaitkan dengan sublis istilah lain. Untuk informasi selengkapnya, lihat DataZone Terminologi dan konsep Amazon. Untuk membuat, mengedit, atau menghapus glosarium di DataZone domain Amazon Anda, Anda harus menjadi anggota proyek pemilik dengan izin yang tepat untuk domain tersebut.

Untuk membuat glosarium, selesaikan langkah-langkah berikut:

1. Arahkan ke portal DataZone data Amazon menggunakan URL portal data dan masuk menggunakan SSO atau AWS kredensil Anda. Jika Anda seorang DataZone administrator Amazon, Anda dapat memperoleh URL portal data dengan mengakses DataZone konsol Amazon di https://console.aws.amazon.com/datazone di AWS akun tempat DataZone domain Amazon dibuat.
2. Arahkan ke menu Katalog di bilah navigasi atas di sebelah Cari.
3. Di Portal DataZone Data Amazon, pilih Glosarium, lalu pilih Buat glosarium.

4. Tentukan nama, deskripsi, pemilik untuk glosarium dan kemudian pilih Buat glosarium.
5. Aktifkan glosarium baru dengan memilih sakelar Diaktifkan.
6. Pada halaman detail glosarium, Anda dapat memilih Buat readme untuk menambahkan beberapa informasi tambahan tentang glosarium ini.

Untuk menonaktifkan atau mengaktifkan glosarium bisnis, selesaikan langkah-langkah berikut:

1. Arahkan ke portal DataZone data Amazon menggunakan URL portal data dan masuk menggunakan SSO atau AWS kredensil Anda. Jika Anda seorang DataZone administrator Amazon, Anda dapat memperoleh URL portal data dengan mengakses DataZone konsol Amazon di https://console.aws.amazon.com/datazone di AWS akun tempat DataZone domain Amazon dibuat.
2. Arahkan ke menu Katalog di bilah navigasi atas di sebelah Cari.
3. Di Portal DataZone Data Amazon, pilih Glosarium, dan temukan glosarium bisnis yang ingin Anda nonaktifkan/aktifkan.
4. Pada halaman detail glosarium, cari sakelar Aktifkan/Nonaktifkan dan gunakan untuk mengaktifkan atau menonaktifkan glosarium yang Anda pilih.

> **Note**
>
> Menonaktifkan glosarium juga menonaktifkan semua istilah yang dikandungnya.

Untuk mengedit glosarium bisnis, selesaikan langkah-langkah berikut:

1. Arahkan ke portal DataZone data Amazon menggunakan URL portal data dan masuk menggunakan SSO atau AWS kredensil Anda. Jika Anda seorang DataZone administrator Amazon, Anda dapat memperoleh URL portal data dengan mengakses DataZone konsol Amazon di https://console.aws.amazon.com/datazone di AWS akun tempat DataZone domain Amazon dibuat.
2. Arahkan ke menu Katalog di bilah navigasi atas di sebelah Cari.
3. Di Portal DataZone Data Amazon, pilih Glosarium, dan temukan glosarium bisnis yang ingin Anda edit.
4. Pada halaman rincian glosarium, perluas Tindakan dan kemudian pilih Edit untuk mengedit glosarium.

5. Buat pembaruan Anda pada nama, deskripsi, lalu pilih Simpan.

Untuk menghapus glosarium bisnis, selesaikan langkah-langkah berikut:

1. Arahkan ke portal DataZone data Amazon menggunakan URL portal data dan masuk menggunakan SSO atau AWS kredensil Anda. Jika Anda seorang DataZone administrator Amazon, Anda dapat memperoleh URL portal data dengan mengakses DataZone konsol Amazon di https://console.aws.amazon.com/datazone di AWS akun tempat DataZone domain Amazon dibuat.
2. Arahkan ke menu Katalog di bilah navigasi atas di sebelah Cari.
3. Di Portal DataZone Data Amazon, pilih Glosarium, dan cari glosarium bisnis yang ingin Anda hapus.
4. Pada halaman rincian glosarium, perluas Tindakan dan kemudian pilih Hapus untuk menghapus glosarium.

> **Note**
>
> Anda harus menghapus semua istilah yang ada dalam glosarium sebelum Anda dapat menghapus glosarium.

5. Konfirmasikan penghapusan glosarium dengan memilih Hapus.

Membuat, mengedit, atau menghapus istilah dalam glosarium

Di Amazon DataZone, glosarium bisnis adalah kumpulan istilah bisnis yang mungkin terkait dengan aset (data). Untuk informasi selengkapnya, lihat DataZone Terminologi dan konsep Amazon. Untuk membuat, mengedit, atau menghapus istilah dalam glosarium di DataZone domain Amazon Anda, Anda harus menjadi anggota proyek pemilik dengan izin yang tepat untuk domain tersebut.

Di Amazon DataZone, istilah glosarium bisnis dapat memiliki deskripsi yang dekat. Untuk mengatur konteks istilah tertentu, Anda dapat menentukan hubungan antar istilah. Ketika Anda mendefinisikan hubungan untuk suatu istilah, itu secara otomatis ditambahkan ke definisi istilah terkait. Istilah glosarium hubungan yang tersedia di Amazon DataZone meliputi yang berikut:

- Adalah Jenis - menunjukkan bahwa istilah saat ini adalah jenis istilah yang diidentifikasi. Menunjukkan bahwa istilah yang diidentifikasi adalah induk dari istilah saat ini.

- Memiliki Jenis - menunjukkan bahwa istilah saat ini adalah istilah umum untuk istilah atau istilah tertentu yang ditunjukkan. Hubungan ini dapat menunjukkan istilah anak untuk istilah generik.

Untuk membuat istilah baru, selesaikan langkah-langkah berikut:

1. Arahkan ke portal DataZone data Amazon menggunakan URL portal data dan masuk menggunakan SSO atau AWS kredensil Anda. Jika Anda seorang DataZone administrator Amazon, Anda dapat memperoleh URL portal data dengan mengakses DataZone konsol Amazon di https://console.aws.amazon.com/datazone di AWS akun tempat DataZone domain Amazon dibuat.
2. Arahkan ke menu Katalog di bilah navigasi atas di sebelah Cari.
3. Di Portal DataZone Data Amazon, pilih Glosarium, lalu pilih glosarium tempat Anda ingin membuat istilah baru.
4. Tentukan nama, deskripsi, pemilik untuk istilah tersebut, lalu pilih Buat istilah.
5. Aktifkan istilah baru dengan memilih sakelar Diaktifkan.
6. Untuk menambahkan Readme, navigasikan ke halaman detail istilah, dan kemudian Anda dapat memilih Buat readme untuk menambahkan beberapa informasi tambahan tentang glosarium ini.
7. Untuk menambahkan hubungan, buka halaman detail istilah, pilih bagian Hubungan Istilah, lalu pilih Tambahkan Istilah Glosarium. Dalam dialog, pilih hubungan dan istilah yang ingin Anda kaitkan, lalu pilih Tutup untuk menambahkan istilah ke jenis hubungan yang sesuai. Hubungan ini juga ditambahkan ke semua istilah yang Anda buat terkait.

Untuk mengedit istilah dalam glosarium, selesaikan langkah-langkah berikut:

1. Arahkan ke portal DataZone data Amazon menggunakan URL portal data dan masuk menggunakan SSO atau AWS kredensil Anda. Jika Anda seorang DataZone administrator Amazon, Anda dapat memperoleh URL portal data dengan mengakses DataZone konsol Amazon di https://console.aws.amazon.com/datazone di AWS akun tempat DataZone domain Amazon dibuat.
2. Arahkan ke menu Katalog di bilah navigasi atas di sebelah Cari.
3. Di Portal DataZone Data Amazon, pilih Glosarium, cari glosarium yang berisi istilah yang ingin Anda edit, lalu pilih istilah itu.
4. Pada halaman detail istilah, perluas Tindakan, lalu pilih Edit untuk mengedit istilah.
5. Buat pembaruan Anda pada nama, deskripsi, lalu pilih Simpan.

Untuk menghapus istilah dalam glosarium, selesaikan langkah-langkah berikut:

1. Arahkan ke portal DataZone data Amazon menggunakan URL portal data dan masuk menggunakan SSO atau AWS kredensil Anda. Jika Anda seorang DataZone administrator Amazon, Anda dapat memperoleh URL portal data dengan mengakses DataZone konsol Amazon di https://console.aws.amazon.com/datazone di AWS akun tempat DataZone domain Amazon dibuat.
2. Arahkan ke menu Katalog di bilah navigasi atas di sebelah Cari.
3. Di Portal DataZone Data Amazon, pilih Glosarium, cari glosarium yang berisi istilah yang ingin Anda hapus, lalu pilih istilah itu.
4. Pada halaman rincian glosarium, perluas Tindakan dan kemudian pilih Hapus untuk menghapus istilah.
5. Konfirmasikan penghapusan istilah dengan memilih Hapus.

Membuat, mengedit, atau menghapus formulir metadata

Di Amazon DataZone, formulir metadata adalah bentuk sederhana untuk menambah konteks bisnis tambahan ke metadata aset dalam katalog. Ini berfungsi sebagai mekanisme yang dapat diperluas bagi pemilik data untuk memperkaya aset dengan informasi yang dapat membantu pengguna data ketika mereka mencari dan menemukan data tersebut. Formulir metadata juga dapat berfungsi sebagai mekanisme untuk menegakkan konsistensi terhadap semua aset yang dipublikasikan ke katalog Amazon. DataZone

Definisi bentuk metadata terdiri dari satu atau lebih definisi bidang, dengan dukungan untuk tipe data nilai bidang boolean, date, desimal, integer, string, dan glosarium bisnis. Untuk informasi selengkapnya, lihat DataZone Terminologi dan konsep Amazon. Untuk membuat, mengedit, atau menghapus formulir metadata di DataZone domain Amazon Anda, Anda harus menjadi anggota proyek pemilik yang memiliki kredensi yang tepat.

Untuk membuat formulir metadata, lengkapi langkah-langkah berikut:

1. Arahkan ke portal DataZone data Amazon menggunakan URL portal data dan masuk menggunakan SSO atau AWS kredensil Anda. Jika Anda seorang DataZone administrator Amazon, Anda dapat memperoleh URL portal data dengan mengakses DataZone konsol Amazon di https://console.aws.amazon.com/datazone di AWS akun tempat DataZone domain Amazon dibuat.
2. Arahkan ke menu Katalog di bilah navigasi atas di sebelah Cari.

3. Di Portal DataZone Data Amazon, pilih Formulir metadata lalu pilih Buat formulir.
4. Tentukan nama formulir metadata, deskripsi, pemilik, lalu pilih Buat formulir.

Untuk mengedit formulir metadata, lengkapi langkah-langkah berikut:

1. Arahkan ke portal DataZone data Amazon menggunakan URL portal data dan masuk menggunakan SSO atau AWS kredensil Anda. Jika Anda seorang DataZone administrator Amazon, Anda dapat memperoleh URL portal data dengan mengakses DataZone konsol Amazon di https://console.aws.amazon.com/datazone di AWS akun tempat DataZone domain Amazon dibuat.
2. Arahkan ke menu Katalog di bilah navigasi atas di sebelah Cari.
3. Di Portal DataZone Data Amazon, pilih Formulir metadata, lalu cari formulir metadata yang ingin Anda edit.
4. Pada halaman detail formulir metadata, perluas Tindakan, lalu pilih Edit.
5. Lakukan pembaruan Anda pada nama, deskripsi, bidang pemilik, lalu pilih Perbarui formulir.

Untuk menghapus formulir metadata, lengkapi langkah-langkah berikut:

> **Note**
>
> Sebelum Anda dapat menghapus formulir metadata, Anda harus menghapusnya dari semua jenis aset atau aset yang diterapkan.

1. Arahkan ke portal DataZone data Amazon menggunakan URL portal data dan masuk menggunakan SSO atau AWS kredensil Anda. Jika Anda seorang DataZone administrator Amazon, Anda dapat memperoleh URL portal data dengan mengakses DataZone konsol Amazon di https://console.aws.amazon.com/datazone di AWS akun tempat DataZone domain Amazon dibuat.
2. Arahkan ke menu Katalog di bilah navigasi atas di sebelah Cari.
3. Di Portal DataZone Data Amazon, pilih Formulir metadata, lalu cari formulir metadata yang ingin Anda hapus.
4. Jika formulir metadata yang ingin Anda hapus diaktifkan, nonaktifkan formulir metadata dengan memilih sakelar Diaktifkan.
5. Pada halaman detail formulir metadata, perluas Tindakan, lalu pilih Hapus.

6. Konfirmasikan penghapusan dengan memilih Hapus.

Membuat, mengedit, atau menghapus bidang dalam bentuk metadata

Di Amazon DataZone, formulir metadata adalah bentuk sederhana untuk menambah konteks bisnis tambahan ke metadata aset dalam katalog. Ini berfungsi sebagai mekanisme yang dapat diperluas bagi pemilik data untuk memperkaya aset dengan informasi yang dapat membantu pengguna data ketika mereka mencari dan menemukan data tersebut. Formulir metadata juga dapat berfungsi sebagai mekanisme untuk menegakkan konsistensi terhadap semua aset yang dipublikasikan ke katalog Amazon. DataZone

Definisi bentuk metadata terdiri dari satu atau lebih definisi bidang, dengan dukungan untuk tipe data nilai bidang boolean, date, desimal, integer, string, dan glosarium bisnis. Untuk informasi selengkapnya, lihat DataZone Terminologi dan konsep Amazon. Untuk membuat, mengedit, atau menghapus bidang dalam formulir metadata di DataZone domain Amazon Anda, Anda harus menjadi anggota proyek pemilik yang memiliki kredensil yang tepat.

Untuk membuat bidang dalam bentuk metadata, lengkapi langkah-langkah berikut:

1. Arahkan ke portal DataZone data Amazon menggunakan URL portal data dan masuk menggunakan SSO atau AWS kredensil Anda. Jika Anda seorang DataZone administrator Amazon, Anda dapat memperoleh URL portal data dengan mengakses DataZone konsol Amazon di https://console.aws.amazon.com/datazone di AWS akun tempat DataZone domain Amazon dibuat.
2. Arahkan ke menu Katalog di bilah navigasi atas di sebelah Cari.
3. Di Portal DataZone Data Amazon, pilih Formulir metadata lalu pilih formulir metadata tempat Anda ingin membuat bidang.
4. Pada halaman detail formulir, pilih Buat bidang.
5. Tentukan nama bidang, deskripsi, jenis, dan apakah ini adalah bidang wajib, lalu pilih Buat bidang.

Untuk mengedit bidang dalam bentuk metadata, lengkapi langkah-langkah berikut:

1. Arahkan ke portal DataZone data Amazon menggunakan URL portal data dan masuk menggunakan SSO atau AWS kredensil Anda. Jika Anda seorang DataZone administrator

Amazon, Anda dapat memperoleh URL portal data dengan mengakses DataZone konsol Amazon di https://console.aws.amazon.com/datazone di AWS akun tempat DataZone domain Amazon dibuat.

2. Arahkan ke menu Katalog di bilah navigasi atas di sebelah Cari.
3. Di Portal DataZone Data Amazon, pilih Formulir metadata lalu pilih formulir metadata tempat Anda ingin mengedit bidang.
4. Pada halaman detail formulir, pilih bidang yang ingin Anda edit, lalu perluas Tindakan, dan pilih Edit.
5. Buat pembaruan Anda ke nama bidang, deskripsi, jenis, dan apakah ini adalah bidang wajib, lalu pilih bidang Perbarui.

Untuk menghapus bidang dalam formulir metadata, lengkapi langkah-langkah berikut:

1. Arahkan ke portal DataZone data Amazon menggunakan URL portal data dan masuk menggunakan SSO atau AWS kredensil Anda. Jika Anda seorang DataZone administrator Amazon, Anda dapat memperoleh URL portal data dengan mengakses DataZone konsol Amazon di https://console.aws.amazon.com/datazone di AWS akun tempat DataZone domain Amazon dibuat.
2. Arahkan ke menu Katalog di bilah navigasi atas di sebelah Cari.
3. Di Portal DataZone Data Amazon, pilih Formulir metadata lalu pilih formulir metadata tempat Anda ingin menghapus bidang.
4. Pada halaman detail formulir, pilih bidang yang ingin Anda hapus, lalu perluas Tindakan, dan pilih Hapus.
5. Konfirmasikan penghapusan dengan memilih Hapus.

Bekerja dengan proyek dan lingkungan di Amazon DataZone

Di Amazon DataZone, proyek memungkinkan sekelompok pengguna untuk berkolaborasi dalam berbagai kasus penggunaan bisnis yang melibatkan penerbitan, penemuan, berlangganan, dan konsumsi aset data dalam katalog Amazon. DataZone Setiap DataZone proyek Amazon memiliki serangkaian kontrol akses yang diterapkan padanya sehingga hanya individu, grup, dan peran yang berwenang yang dapat mengakses proyek dan aset data tempat proyek ini berlangganan, dan hanya dapat menggunakan alat yang ditentukan oleh izin proyek. Proyek bertindak sebagai prinsipal identitas yang menerima hibah akses ke sumber daya yang mendasarinya, DataZone memungkinkan Amazon beroperasi dalam infrastruktur organisasi tanpa bergantung pada kredensi pengguna individu. Untuk informasi selengkapnya, lihat DataZone Terminologi dan konsep Amazon

Topik

Buat profil lingkungan

Di Amazon DataZone, profil lingkungan adalah template yang dapat Anda gunakan untuk membuat lingkungan. Tujuan dari profil lingkungan adalah untuk menyederhanakan pembuatan lingkungan dengan menyematkan informasi penempatan seperti AWS akun dan wilayah dalam profil. Untuk informasi selengkapnya, lihat DataZone Terminologi dan konsep Amazon. Untuk membuat profil

lingkungan di DataZone domain Amazon, Anda harus menjadi bagian dari DataZone proyek Amazon. Semua profil lingkungan dimiliki oleh proyek dan dapat digunakan oleh semua pengguna yang berwenang, dari proyek apa pun, untuk menciptakan lingkungan baru.

Untuk membuat profil lingkungan

1. Arahkan ke portal DataZone data Amazon menggunakan URL portal data dan masuk menggunakan SSO atau AWS kredensil Anda. Jika Anda DataZone administrator Amazon, Anda dapat memperoleh URL portal data dengan mengakses DataZone konsol Amazon di https://console.aws.amazon.com/datazone di AWS akun tempat DataZone domain Amazon dibuat.
2. Di dalam portal data, pilih Jelajahi proyek dan pilih proyek tempat Anda ingin membuat profil lingkungan.
3. Arahkan ke tab Lingkungan dalam proyek, lalu pilih Buat profil lingkungan.
4. Konfigurasi bidang berikut:

   - Nama — Nama untuk profil lingkungan Anda.
   - Deskripsi - (Opsional) Deskripsi untuk profil lingkungan Anda.
   - Proyek Pemilik - Proyek tempat profil dibuat dipilih secara default di bidang ini.
   - Blueprint — Cetak biru yang membuat profil ini. Anda dapat memilih salah satu DataZone cetak biru Amazon default (Data Lake atau Data Warehouse).

     Jika Anda menentukan cetak biru Data Warehouse, lakukan hal berikut:

     - Berikan set parameter. Untuk memilih set parameter yang ada pilih opsi Pilih set parameter. Jika Anda ingin memasukkan parameter Anda sendiri, pilih Enter my own.
     - Jika Anda memilih untuk memilih parameter yang ada, maka lakukan hal berikut:
       - Pilih AWS akun dari drop-down.
       - Pilih set parameter dari dropdown.
     - Jika Anda memilih untuk memasukkan parameter Anda sendiri, lakukan hal berikut:
       - Berikan AWS parameter dengan memilih AWS Akun dan Wilayah dari dropdown.
       - Berikan parameter Redshift Data Wareshoue:
         - Pilih cluster Amazon Redshift atau Amazon Redshift Tanpa Server
         - Masukkan ARN AWS Rahasia yang menyimpan kredensil ke cluster Amazon Redshift atau grup kerja Amazon Redshift Serverless yang dipilih. AWS Rahasianya harus ditandai dengan Id domain dan Project Id tempat Anda membuat profil lingkungan.
           - `AmazonDataZoneDomain: [Domain_ID]`

    - `AmazonDataZoneProject: [Project_ID]`
  - Masukkan nama cluster Amazon Redshift atau workgroup Amazon Redshift Serverless.
  - Masukkan nama database dalam klaster Amazon Redshift atau grup kerja Amazon Redshift Serverless yang dipilih.
- Di bagian Proyek resmi, tentukan proyek yang dapat menggunakan profil lingkungan untuk membuat lingkungan. Secara default, semua proyek dalam domain dapat menggunakan profil lingkungan di akun untuk membuat lingkungan. Untuk mempertahankan pengaturan default ini, pilih Semua proyek. Namun, Anda dapat membatasi ini dengan menetapkan proyek resmi ke lingkungan. Untuk melakukannya, pilih Proyek resmi saja dan kemudian tentukan proyek yang dapat menggunakan profil proyek ini untuk membuat lingkungan.
- Di bagian Penerbitan, pilih salah satu opsi berikut:
  - Publikasikan dari skema apa pun: Jika Anda memilih opsi ini, lingkungan yang dibuat menggunakan profil lingkungan ini dapat digunakan untuk mempublikasikan dari skema apa pun dalam database yang dipilih dalam parameter Redshift yang disediakan di atas. Pengguna lingkungan yang dibuat menggunakan profil lingkungan ini juga dapat memberikan parameter Amazon Redshift mereka sendiri untuk dipublikasikan dari skema apa pun dalam AWS akun dan wilayah yang dipilih di profil lingkungan.
  - Publikasikan hanya dari skema lingkungan default: Jika Anda memilih opsi ini, lingkungan yang dibuat menggunakan ini dapat digunakan untuk mempublikasikan hanya dari skema default yang dibuat oleh Amazon DataZone untuk lingkungan tersebut. Pengguna lingkungan yang dibuat menggunakan profil lingkungan ini tidak dapat memberikan parameter Amazon Redshift mereka sendiri.
  - Jangan izinkan penerbitan: Jika Anda memilih opsi ini, lingkungan yang dibuat menggunakan profil lingkungan ini hanya dapat digunakan untuk berlangganan dan konsumsi data. Lingkungan tidak dapat digunakan untuk mempublikasikan data apa pun sama sekali.

Jika Anda menentukan cetak biru Data Lake, lakukan hal berikut:

- Di bagian parameter AWS akun, tentukan nomor AWS akun dan wilayah AWS akun tempat lingkungan potensial akan dibuat.
- Di bagian Proyek resmi, tentukan proyek yang dapat menggunakan profil lingkungan dengan profil lingkungan Data Lake bawaan untuk membuat lingkungan. Secara default, semua proyek dalam domain dapat menggunakan cetak biru data lake di akun untuk membuat profil lingkungan. Untuk mempertahankan pengaturan default ini, pilih Semua

proyek. Namun, Anda dapat membatasi ini dengan menetapkan proyek ke cetak biru. Untuk melakukannya, pilih Proyek resmi saja dan kemudian tentukan proyek yang dapat menggunakan profil proyek ini untuk membuat lingkungan.

- Di bagian Database, pilih database apa saja untuk mengaktifkan penerbitan dari database apa pun di dalam AWS akun dan wilayah tempat lingkungan dibuat atau pilih Hanya database default untuk mengaktifkan penerbitan hanya dari database penerbitan default yang dibuat dengan lingkungan.

5. Pilih Buat profil lingkungan.

Mengedit profil lingkungan

Di Amazon DataZone, profil lingkungan adalah template yang dapat Anda gunakan untuk membuat lingkungan. Untuk informasi selengkapnya, lihat DataZone Terminologi dan konsep Amazon. Untuk mengedit profil lingkungan yang ada di DataZone domain Amazon, Anda harus menjadi bagian dari DataZone proyek Amazon.

Untuk mengedit profil lingkungan

1. Arahkan ke URL portal DataZone data Amazon dan masuk menggunakan sistem masuk tunggal (SSO) atau kredensional Anda. AWS Jika Anda DataZone administrator Amazon, Anda dapat menavigasi ke DataZone konsol Amazon di https://console.aws.amazon.com/datazone dan masuk dengan Akun AWS tempat domain dibuat, lalu pilih Buka portal data.
2. Di dalam portal data, pilih Jelajahi proyek dan pilih proyek tempat Anda ingin mengedit profil lingkungan.
3. Arahkan ke tab Lingkungan dalam proyek, lalu pilih Profil lingkungan, lalu pilih profil lingkungan yang ingin Anda edit.

   Jika Anda mengedit profil lingkungan Data Warehouse, Anda hanya dapat mengedit nama dan deskripsi profil lingkungan yang ada.

   Jika Anda mengedit profil lingkungan Data Lake, Anda dapat mengedit nama dan deskripsi profil dan Anda juga dapat mengedit proyek yang diizinkan untuk menggunakan profil ini untuk membuat lingkungan dan Anda dapat mengedit database. Untuk mengedit pengaturan ini, lakukan hal berikut:

   - Di bagian Proyek resmi, tentukan proyek yang dapat menggunakan profil lingkungan dengan profil lingkungan Data Lake bawaan untuk membuat lingkungan. Secara default, semua

proyek dalam domain dapat menggunakan cetak biru data lake di akun untuk membuat profil lingkungan. Untuk mempertahankan pengaturan default ini, pilih Semua proyek. Namun, Anda dapat membatasi ini dengan menetapkan proyek ke cetak biru. Untuk melakukannya, pilih Proyek resmi saja dan kemudian tentukan proyek yang dapat menggunakan profil proyek ini untuk membuat lingkungan.

- Di bagian Database, pilih database apa saja untuk mengaktifkan penerbitan dari database apa pun di dalam AWS akun dan wilayah tempat lingkungan dibuat atau pilih Hanya database default untuk mengaktifkan penerbitan hanya dari database penerbitan default yang dibuat dengan lingkungan.

Saat Anda menyelesaikan pengeditan, pilih Edit profil lingkungan.

Menghapus profil lingkungan

Di Amazon DataZone, profil lingkungan adalah template yang dapat Anda gunakan untuk membuat lingkungan. Tujuan dari profil lingkungan adalah untuk menyederhanakan pembuatan lingkungan dengan menyematkan informasi penempatan seperti AWS akun dan wilayah dalam profil. Untuk informasi selengkapnya, lihat DataZone Terminologi dan konsep Amazon. Untuk menghapus profil lingkungan di DataZone domain Amazon, Anda harus menjadi bagian dari DataZone proyek Amazon.

> **Note**
>
> Saat menghapus profil lingkungan, Anda tidak dapat membuat lingkungan lagi menggunakan profil ini.

Untuk menghapus profil lingkungan

1. Arahkan ke URL portal DataZone data Amazon dan masuk menggunakan sistem masuk tunggal (SSO) atau kredensional Anda. AWS Jika Anda DataZone administrator Amazon, Anda dapat menavigasi ke DataZone konsol Amazon di https://console.aws.amazon.com/datazone dan masuk dengan Akun AWS tempat domain dibuat, lalu pilih Buka portal data.
2. Di dalam portal data, pilih Jelajahi proyek dan pilih proyek tempat Anda ingin menghapus profil lingkungan.
3. Arahkan ke tab Lingkungan dalam proyek, lalu pilih Profil lingkungan, lalu pilih profil lingkungan yang ingin Anda hapus.

4. Pilih profil lingkungan yang ingin Anda hapus, lalu pilih Tindakan, Hapus, dan konfirmasi penghapusan.

Ciptakan lingkungan baru

Dalam DataZone proyek Amazon, lingkungan adalah kumpulan sumber daya yang dikonfigurasi (misalnya, bucket Amazon S3, database AWS Glue, atau grup kerja Amazon Athena), dengan kumpulan prinsip IAM tertentu (peran pengguna lingkungan) dengan izin pemilik atau kontributor yang ditetapkan yang dapat beroperasi pada sumber daya tersebut. Untuk informasi selengkapnya, lihat DataZone Terminologi dan konsep Amazon.

Setiap DataZone pengguna Amazon dengan izin yang diperlukan untuk mengakses portal data dapat membuat DataZone lingkungan Amazon dalam sebuah proyek.

Untuk membuat lingkungan baru, selesaikan langkah-langkah berikut.

1. Arahkan ke URL portal DataZone data Amazon dan masuk menggunakan sistem masuk tunggal (SSO) atau kredensional Anda. AWS Jika Anda DataZone administrator Amazon, Anda dapat menavigasi ke DataZone konsol Amazon di https://console.aws.amazon.com/datazone dan masuk dengan Akun AWS tempat domain dibuat, lalu pilih Buka portal data.
2. Pilih Jelajahi semua proyek dan pilih proyek tempat Anda ingin membuat lingkungan baru.
3. Pilih Buat lingkungan, tentukan nilai untuk bidang berikut, lalu pilih Buat lingkungan:

   - Nama — nama lingkungan
   - Deskripsi — deskripsi lingkungan
   - Profil lingkungan — pilih profil lingkungan yang ada atau buat yang baru. Profil lingkungan adalah template yang dapat Anda gunakan untuk membuat lingkungan. Untuk informasi selengkapnya, lihat DataZone Terminologi dan konsep Amazon.

     Setelah Anda memilih profil lingkungan, di bawah bagian Parameter, tentukan nilai untuk bidang yang merupakan bagian dari profil lingkungan ini.

Mengedit lingkungan

Dalam DataZone proyek Amazon, lingkungan adalah kumpulan sumber daya yang dikonfigurasi (misalnya, bucket Amazon S3, database AWS Glue, atau workgroup Amazon Athena), dengan kumpulan prinsipal IAM tertentu (dengan izin kontributor yang ditetapkan) yang dapat beroperasi

pada sumber daya tersebut. Untuk informasi selengkapnya, lihat DataZone Terminologi dan konsep Amazon.

Setiap DataZone pengguna Amazon dengan izin yang diperlukan untuk mengakses portal data dapat mengedit DataZone lingkungan Amazon dalam sebuah proyek.

Untuk mengedit lingkungan yang ada, selesaikan langkah-langkah berikut.

1. Arahkan ke URL portal DataZone data Amazon dan masuk menggunakan sistem masuk tunggal (SSO) atau kredensional Anda. AWS Jika Anda DataZone administrator Amazon, Anda dapat menavigasi ke DataZone konsol Amazon di https://console.aws.amazon.com/datazone dan masuk dengan Akun AWS tempat domain dibuat, lalu pilih Buka portal data.
2. Pilih Jelajahi proyek dari panel navigasi atas dan pilih proyek yang berisi lingkungan yang ingin Anda edit.
3. Temukan dan pilih lingkungan untuk membuka halaman detailnya. Kemudian perluas Tindakan dan pilih Edit lingkungan.
4. Lakukan pengeditan nama dan deskripsi lingkungan, lalu pilih Simpan perubahan.

Hapus lingkungan

Dalam DataZone proyek Amazon, lingkungan adalah kumpulan sumber daya yang dikonfigurasi (misalnya, bucket Amazon S3, database AWS Glue, atau workgroup Amazon Athena), dengan kumpulan prinsipal IAM tertentu (dengan izin kontributor yang ditetapkan) yang dapat beroperasi pada sumber daya tersebut. Untuk informasi selengkapnya, lihat DataZone Terminologi dan konsep Amazon.

Setiap DataZone pengguna Amazon dengan izin yang diperlukan untuk mengakses portal data dapat menghapus DataZone lingkungan Amazon dalam sebuah proyek.

Untuk menghapus lingkungan yang ada, selesaikan langkah-langkah berikut.

1. Arahkan ke URL portal DataZone data Amazon dan masuk menggunakan sistem masuk tunggal (SSO) atau kredensional Anda. AWS Jika Anda DataZone administrator Amazon, Anda dapat menavigasi ke DataZone konsol Amazon di https://console.aws.amazon.com/datazone dan masuk dengan Akun AWS tempat domain dibuat, lalu pilih Buka portal data.
2. Pilih Jelajahi proyek dari panel navigasi atas dan pilih proyek yang berisi lingkungan yang ingin Anda hapus.

3. Cari dan pilih lingkungan untuk membuka halaman detailnya, lalu perluas Tindakan dan pilih Hapus lingkungan.
4. Di jendela pop up Hapus lingkungan, konfirmasikan penghapusan dengan mengetik `Delete` di bidang dan kemudian pilih Hapus lingkungan.

   Anda dapat berhasil menghapus lingkungan hanya setelah semua entitas dengan ketergantungan ke lingkungan ini telah dihapus. Untuk menghapus lingkungan, Anda harus terlebih dahulu menghapus semua sumber data terkait dan target berlangganan.

Membuat sebuah proyek baru

Di Amazon DataZone, proyek memungkinkan sekelompok pengguna untuk berkolaborasi dalam berbagai kasus penggunaan bisnis yang melibatkan penerbitan, penemuan, berlangganan, dan konsumsi aset data dalam katalog Amazon. DataZone Untuk informasi selengkapnya, lihat DataZone Terminologi dan konsep Amazon.

Setiap DataZone pengguna Amazon dengan izin yang diperlukan untuk mengakses portal data dapat membuat DataZone proyek Amazon.

Untuk membuat proyek baru, selesaikan langkah-langkah berikut.

1. Arahkan ke URL portal DataZone data Amazon dan masuk menggunakan sistem masuk tunggal (SSO) atau kredensional Anda. AWS Jika Anda DataZone administrator Amazon, Anda dapat menavigasi ke DataZone konsol Amazon di https://console.aws.amazon.com/datazone dan masuk dengan Akun AWS tempat domain dibuat, lalu pilih Buka portal data.
2. Di portal DataZone data Amazon, pilih Buat Proyek.
3. Tentukan nilai untuk bidang berikut, lalu pilih Buat proyek:

   - Nama - Nama proyek.
   - Deskripsi — Deskripsi proyek.

Edit proyek

Di Amazon DataZone, proyek memungkinkan sekelompok pengguna untuk berkolaborasi dalam berbagai kasus penggunaan bisnis yang melibatkan penerbitan, penemuan, berlangganan, dan konsumsi aset data dalam katalog Amazon. DataZone Untuk informasi selengkapnya, lihat DataZone

Terminologi dan konsep Amazon. Untuk mengedit DataZone proyek Amazon, Anda harus menjadi pemilik proyek itu atau administrator domain domain yang berisi proyek ini.

Untuk mengedit proyek yang ada, selesaikan langkah-langkah berikut.

1. Arahkan ke URL portal DataZone data Amazon dan masuk menggunakan sistem masuk tunggal (SSO) atau kredensional Anda. AWS Jika Anda DataZone administrator Amazon, Anda dapat menavigasi ke DataZone konsol Amazon di https://console.aws.amazon.com/datazone dan masuk dengan Akun AWS tempat domain dibuat, lalu pilih Buka portal data.
2. Pilih Jelajahi proyek.
3. Pilih proyek yang ingin Anda edit. Jika Anda tidak mudah melihatnya dalam daftar proyek, Anda dapat mencarinya dengan menentukan nama proyek di bidang Temukan proyek.
4. Perluas Tindakan dan pilih Edit proyek.
5. Lakukan pembaruan Anda pada nama dan deskripsi proyek, lalu pilih Simpan.

Hapus proyek

Di Amazon DataZone, proyek memungkinkan sekelompok pengguna untuk berkolaborasi dalam berbagai kasus penggunaan bisnis yang melibatkan penerbitan, penemuan, berlangganan, dan/atau mengkonsumsi aset data dalam katalog Amazon. DataZone Untuk informasi selengkapnya, lihat DataZone Terminologi dan konsep Amazon.

Tindakan menghapus proyek adalah final. Penghapusan menghapus konten proyek secara permanen, termasuk sumber data, lingkungan, aset, glosarium, dan formulir metadata. Amazon DataZone mencabut hibah yang DataZone telah diberikan Amazon pada aset yang dikelola melalui Lake Formation dan Amazon Redshift. Menghapus proyek tidak menghapus DataZone AWS sumber daya non-Amazon yang DataZone mungkin telah dibantu Amazon Anda buat. Jika Anda tidak lagi membutuhkan AWS sumber daya ini, hapus di AWS layanan dan akun masing-masing.

Untuk menghapus DataZone proyek Amazon, Anda harus menjadi pemilik proyek.

Untuk menghapus proyek yang ada, selesaikan langkah-langkah berikut.

1. Arahkan ke URL portal DataZone data Amazon dan masuk menggunakan sistem masuk tunggal (SSO) atau kredensional Anda. AWS Prinsipal IAM dapat menavigasi ke DataZone konsol Amazon di https://console.aws.amazon.com/datazone dan masuk dengan Akun AWS tempat domain dibuat, lalu pilih Buka portal data.
2. Pilih Jelajahi proyek dari panel navigasi atas.

3. Pilih proyek yang ingin Anda hapus. Jika Anda tidak melihatnya dalam daftar proyek, Anda dapat mencarinya dengan menentukan nama proyek di bidang Temukan proyek.
4. Perluas Tindakan dan pilih Hapus proyek.

   Tinjau peringatan informasi tentang dampak potensial dari penghapusan proyek.
5. Jika Anda menerima peringatan, ketikkan teks konfirmasi, dan pilih Hapus.

> **Important**
>
> Menghapus proyek adalah tindakan yang tidak dapat dibatalkan yang tidak dapat dibatalkan oleh Anda atau oleh. AWS

> **Note**
>
> Saat Anda atau pengguna domain membuat lingkungan dalam proyek, Amazon DataZone membuat AWS sumber daya di domain atau akun terkait untuk memberi Anda dan pengguna domain fungsionalitas. Di bawah ini adalah daftar sumber AWS daya yang DataZone dapat dibuat Amazon untuk sebuah proyek, bersama dengan nama defaultnya. Menghapus proyek tidak menghapus AWS sumber daya ini di AWS akun Anda.
>
> - <environmentId>Peran IAM: datazone_usr_.
> - <environmentName>Basis data Glue: (1) <environmentName>_pub_db-*, (2) _sub_db-*. Jika sudah ada database nama ini, Amazon DataZone akan menambahkan ID lingkungan.
> - <environmentName>Kelompok kerja Athena: -*. Jika sudah ada workgroup nama ini, Amazon DataZone akan menambahkan ID lingkungan.
> - CloudWatch grup log: datazone_ <environmentId>

Tinggalkan proyek

Di Amazon DataZone, proyek memungkinkan sekelompok pengguna untuk berkolaborasi dalam berbagai kasus penggunaan bisnis yang melibatkan penerbitan, penemuan, berlangganan, dan konsumsi aset data dalam katalog Amazon. DataZone Untuk informasi selengkapnya, lihat DataZone Terminologi dan konsep Amazon.

Untuk meninggalkan proyek yang ada, selesaikan langkah-langkah berikut.

1. Arahkan ke URL portal DataZone data Amazon dan masuk menggunakan sistem masuk tunggal (SSO) atau kredensional Anda. AWS Jika Anda DataZone administrator Amazon, Anda dapat menavigasi ke DataZone konsol Amazon di https://console.aws.amazon.com/datazone dan masuk dengan Akun AWS tempat domain dibuat, lalu pilih Buka portal data.
2. Pilih Pilih proyek dari panel navigasi atas dan pilih proyek.
3. Pilih proyek yang ingin Anda tinggalkan. Jika Anda tidak mudah melihatnya dalam daftar proyek, Anda dapat mencarinya dengan menentukan nama proyek di bidang Temukan proyek.
4. Perluas Tindakan dan pilih Tinggalkan proyek.

Menambahkan anggota ke proyek

Di Amazon DataZone, proyek memungkinkan sekelompok pengguna untuk berkolaborasi dalam berbagai kasus penggunaan bisnis yang melibatkan penerbitan, penemuan, berlangganan, dan konsumsi aset data dalam katalog Amazon. DataZone Untuk informasi selengkapnya, lihat DataZone Terminologi dan konsep Amazon.

Anda harus menjadi pemilik proyek atau kontributor untuk menambahkan anggota ke proyek. Anda dapat menambahkan grup SSO, pengguna SSO, atau kepala sekolah IAM (peran atau pengguna) sebagai anggota proyek.

Untuk menambahkan anggota ke proyek yang keluar, selesaikan langkah-langkah berikut.

1. Arahkan ke URL portal DataZone data Amazon dan masuk menggunakan sistem masuk tunggal (SSO) atau kredensional Anda. AWS Jika Anda DataZone administrator Amazon, Anda dapat menavigasi ke DataZone konsol Amazon di https://console.aws.amazon.com/datazone dan masuk dengan Akun AWS tempat domain dibuat, lalu pilih Buka portal data.
2. Pilih Pilih proyek dari panel navigasi atas dan pilih proyek.
3. Pilih proyek yang ingin Anda tambahkan memebrs. Jika Anda tidak mudah melihatnya dalam daftar proyek, Anda dapat mencarinya dengan menentukan nama proyek di bidang Temukan proyek.
4. Pada halaman detail proyek, pilih tab Anggota dan simpul pilih Semua anggota.
5. Di tab Anggota proyek, pilih Tambahkan anggota.
6. Di jendela pop up Tambahkan anggota ke proyek, tentukan pengguna yang ingin Anda tambahkan dan tentukan perannya dalam proyek (pemilik atau kontributor) lalu pilih Tambahkan anggota.

> **Note**
>
> Anda dapat menambahkan prinsipal IAM sebagai anggota proyek jika prinsipal tersebut sudah memiliki profil DataZone pengguna Amazon di domain. Amazon DataZone secara otomatis membuat profil pengguna untuk prinsipal IAM ketika berhasil berinteraksi dengan domain melalui portal, API, atau CLI. Anda tidak dapat membuat profil pengguna untuk kepala sekolah IAM. Untuk menambahkan prinsipal IAM sebagai anggota proyek jika prinsipal IAM tidak memiliki profil DataZone pengguna Amazon yang ada di domain, minta administrator Anda untuk menambahkan dua izin IAM berikut ke domain Anda di konsol IAM: dan. AmazonDataZoneDomainExecutionRole`iam:GetUser` `iam:GetRole` Secara terpisah, untuk melakukan tindakan dalam domain, kepala IAM harus memiliki izin IAM yang sesuai untuk tindakan tersebut.

Menghapus anggota dari proyek

Di Amazon DataZone, proyek memungkinkan sekelompok pengguna untuk berkolaborasi dalam berbagai kasus penggunaan bisnis yang melibatkan penerbitan, penemuan, berlangganan, dan konsumsi aset data dalam katalog Amazon. DataZone Untuk informasi selengkapnya, lihat DataZone Terminologi dan konsep Amazon. Anda harus menjadi pemilik proyek untuk menghapus anggota dari proyek.

Untuk menghapus anggota dari proyek yang keluar, selesaikan langkah-langkah berikut.

1. Arahkan ke portal DataZone data Amazon menggunakan URL portal data dan masuk menggunakan SSO atau AWS kredensil Anda. Jika Anda DataZone administrator Amazon, Anda dapat memperoleh URL portal data dengan mengakses DataZone konsol Amazon di https://console.aws.amazon.com/datazone di AWS akun tempat DataZone domain Amazon dibuat.
2. Pilih Pilih proyek dari panel navigasi atas dan pilih proyek.
3. Pilih proyek tempat Anda ingin menghapus memebrs. Jika Anda tidak mudah melihatnya dalam daftar proyek, Anda dapat mencarinya dengan menentukan nama proyek di bidang Temukan proyek.
4. Pada halaman detail proyek, pilih tab Anggota dan simpul pilih Semua anggota.
5. Di tab Anggota proyek, pilih anggota yang ingin Anda hapus dari proyek dan kemudian pilih Hapus.
6. Di jendela pop up Hapus anggota, konfirmasikan penghapusan dengan memilih Hapus anggota.

Membuat inventaris dan menerbitkan data di Amazon DataZone

Bagian ini menjelaskan tugas dan prosedur yang ingin Anda lakukan untuk membuat inventaris data Anda di Amazon DataZone dan mempublikasikan data Anda di Amazon DataZone.

Untuk menggunakan Amazon DataZone untuk membuat katalog data Anda, Anda harus terlebih dahulu membawa data (aset) Anda sebagai inventaris proyek Anda di Amazon DataZone. Membuat inventaris untuk proyek tertentu, membuat aset hanya dapat ditemukan oleh anggota proyek itu. Aset inventaris proyek tidak tersedia untuk semua pengguna domain dalam pencarian/penelusuran kecuali dipublikasikan secara eksplisit. Setelah membuat inventaris proyek, pemilik data dapat mengkurasi aset inventaris mereka dengan metadata bisnis yang diperlukan dengan menambahkan atau memperbarui nama bisnis (aset dan skema), deskripsi (aset dan skema), baca saya, istilah glosarium (aset dan skema), dan bentuk metadata.

Langkah selanjutnya menggunakan Amazon DataZone untuk membuat katalog data Anda, adalah membuat aset inventaris proyek Anda dapat ditemukan oleh pengguna domain. Anda dapat melakukan ini dengan menerbitkan aset inventaris ke DataZone katalog Amazon. Hanya versi terbaru dari aset inventaris yang dapat dipublikasikan ke katalog dan hanya versi terbaru yang diterbitkan yang aktif dalam katalog penemuan. Jika aset inventaris diperbarui setelah dipublikasikan ke DataZone katalog Amazon, Anda harus menerbitkannya lagi secara eksplisit agar versi terbaru berada di katalog penemuan.

Topik

- Hapus DataZone aset Amazon
- Memulai sumber data secara manual yang dijalankan di Amazon DataZone
- Revisi aset di Amazon DataZone
- Kualitas data di Amazon DataZone
- Menggunakan pembelajaran mesin dan AI generatif

Konfigurasikan izin Lake Formation untuk Amazon DataZone

Saat Anda membuat lingkungan menggunakan blueprint data lake (DefaultDataLake) bawaan, database AWS Glue ditambahkan di Amazon DataZone sebagai bagian dari proses pembuatan lingkungan ini. Jika Anda ingin mempublikasikan aset dari database AWS Glue ini, tidak diperlukan izin tambahan.

Namun, jika Anda ingin mempublikasikan aset dan berlangganan aset dari database AWS Glue yang ada di luar DataZone lingkungan Amazon Anda, Anda harus secara eksplisit memberikan Amazon DataZone izin untuk mengakses tabel di database Glue AWS eksternal ini. Untuk melakukan ini, Anda harus menyelesaikan pengaturan berikut di AWS Lake Formation dan melampirkan izin Lake Formation yang diperlukan keAmazonDataZoneGlueAccess- <region>- <domainId>.

- Konfigurasikan lokasi Amazon S3 untuk data lake Anda di AWS Lake Formation dengan mode izin Lake Formation atau mode akses Hybrid. Untuk informasi lebih lanjut, lihat https://docs.aws.amazon.com/lake-formation/latest/dg/ register-data-lake .html.
- Hapus `IAMAllowedPrincipals` izin dari tabel Amazon Lake Formation tempat Amazon DataZone menangani izin. Untuk informasi lebih lanjut, lihat https://docs.aws.amazon.com/lake-formation/latest/dg/ upgrade-glue-lake-formation -background.html.
- Lampirkan izin AWS Lake Formation berikut keAmazonDataZoneGlueAccess- <region>- <domainId>:
  - `Describe`dan `Describe grantable` izin pada database tempat tabel ada
  - `Describe`,`Select`,`Describe Grantable`, `Select Grantable` izin pada semua tabel dalam database di atas yang ingin Anda kelola DataZone akses atas nama Anda.

> **Note**
>
> Amazon DataZone mendukung mode AWS Lake Formation Hybrid. Mode hibrida Lake Formation memungkinkan Anda untuk mulai mengelola izin pada database dan tabel AWS

Glue Anda melalui Lake Formation, sambil terus mempertahankan izin IAM yang ada pada tabel dan database ini. Untuk informasi selengkapnya, lihat DataZone Integrasi Amazon dengan mode hybrid AWS Lake Formation

Untuk informasi selengkapnya, lihat Memecahkan masalah izin AWS Lake Formation untuk Amazon DataZone.

DataZone Integrasi Amazon dengan mode hybrid AWS Lake Formation

Amazon DataZone terintegrasi dengan mode hybrid AWS Lake Formation. Integrasi ini memungkinkan Anda untuk dengan mudah mempublikasikan dan membagikan tabel AWS Glue Anda melalui Amazon DataZone tanpa perlu mendaftarkannya di AWS Lake Formation terlebih dahulu. Mode hibrida memungkinkan Anda untuk mulai mengelola izin pada tabel AWS Glue Anda melalui AWS Lake Formation sambil terus mempertahankan izin IAM yang ada pada tabel ini.

Untuk memulai, Anda dapat mengaktifkan pengaturan pendaftaran lokasi data di bawah DefaultDataLakecetak biru di konsol manajemen Amazon DataZone.

Aktifkan integrasi dengan mode hybrid AWS Lake Formation

1. Arahkan ke DataZone konsol Amazon di https://console.aws.amazon.com/datazone dan masuk dengan kredensil akun Anda.
2. Pilih Lihat domain dan pilih domain tempat Anda ingin mengaktifkan integrasi dengan mode hibrida AWS Lake Formation.
3. Pada halaman detail domain, navigasikan ke tab Blueprints.
4. Dari daftar Blueprints, pilih cetak biru. DefaultDataLake
5. Pastikan DefaultDataLake cetak biru diaktifkan. Jika tidak diaktifkan, ikuti langkah-langkah Aktifkan cetak biru bawaan di AWS akun yang memiliki domain Amazon DataZone untuk mengaktifkannya di AWS Akun Anda.
6. Pada halaman DefaultDataLake detail, buka tab Penyediaan dan pilih tombol Edit di sudut kanan atas halaman.
7. Di bawah Pendaftaran lokasi data, centang kotak untuk mengaktifkan pendaftaran lokasi data.
8. Untuk peran manajemen lokasi data, Anda dapat membuat peran IAM baru atau memilih peran IAM yang ada. Amazon DataZone menggunakan peran ini untuk mengelola akses baca/tulis ke bucket Amazon S3 yang dipilih untuk Data Lake menggunakan mode akses hybrid Lake

AWS Formation. Untuk informasi selengkapnya, lihat AmazonDataZone<region>S3Kelola- -<domainId>.

9. Secara opsional, Anda dapat memilih untuk mengecualikan lokasi Amazon S3 tertentu jika Anda tidak ingin DataZone Amazon mendaftarkannya secara otomatis dalam mode hybrid. Untuk ini, selesaikan langkah-langkah berikut:

   - Pilih tombol sakelar untuk mengecualikan lokasi Amazon S3 yang ditentukan.
   - Berikan URI bucket Amazon S3 yang ingin Anda kecualikan.
   - Untuk menambahkan bucket tambahan, pilih Tambahkan lokasi S3.

   > **Note**
   >
   > Amazon DataZone hanya mengizinkan mengecualikan lokasi root S3. Setiap lokasi S3 dalam jalur lokasi root S3 akan secara otomatis dikecualikan dari pendaftaran.

   - Pilih Simpan perubahan.

Setelah Anda mengaktifkan pengaturan pendaftaran lokasi data di AWS akun Anda, ketika konsumen data berlangganan tabel AWS Glue yang dikelola melalui izin IAM, Amazon pertama-tama DataZone akan mendaftarkan lokasi Amazon S3 dari tabel ini dalam mode hibrida, dan kemudian memberikan akses ke konsumen data dengan mengelola izin di atas tabel melalui Lake Formation. AWS Ini memastikan bahwa izin IAM pada tabel terus ada dengan izin AWS Lake Formation yang baru diberikan, tanpa mengganggu alur kerja yang ada.

Cara menangani lokasi Amazon S3 terenkripsi saat mengaktifkan integrasi mode hybrid AWS Lake Formation di Amazon DataZone

Jika Anda menggunakan lokasi Amazon S3 yang dienkripsi dengan kunci KMS yang AWS dikelola atau Dikelola Pelanggan, peran AmazonDataZoneS3Manage harus memiliki izin untuk mengenkripsi dan mendekripsi data dengan kunci KMS, atau kebijakan kunci KMS harus memberikan izin pada kunci peran tersebut.

Jika lokasi Amazon S3 Anda dienkripsi dengan kunci AWS terkelola, tambahkan kebijakan sebaris berikut ke peran: AmazonDataZoneDataLocationManagement

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

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

Jika lokasi Amazon S3 Anda dienkripsi dengan kunci yang dikelola pelanggan, lakukan hal berikut:

1. Buka konsol AWS KMS di https://console.aws.amazon.com/kms dan masuk sebagai pengguna administratif AWS Identity and Access Management (IAM) and Access Management (IAM) atau sebagai pengguna yang dapat memodifikasi kebijakan kunci kunci KMS yang digunakan untuk mengenkripsi lokasi.
2. Di panel navigasi, pilih Kunci yang dikelola pelanggan, lalu pilih nama kunci KMS yang diinginkan.
3. Pada halaman detail kunci KMS, pilih tab Kebijakan kunci, lalu lakukan salah satu hal berikut untuk menambahkan peran kustom Anda atau peran terkait layanan Lake Formation sebagai pengguna kunci KMS:

   - Jika tampilan default ditampilkan (dengan Administrator kunci, Penghapusan kunci, Pengguna kunci, dan bagian AWS Akun lainnya) — di bawah bagian Pengguna kunci, tambahkan peran. AmazonDataZoneDataLocationManagement
   - Jika kebijakan kunci (JSON) ditampilkan — edit kebijakan untuk menambahkan AmazonDataZoneDataLocationManagementperan ke objek “Izinkan penggunaan kunci,” seperti yang ditunjukkan pada contoh berikut

     ```
     ...
            {
                "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**
>
> Jika kunci KMS atau lokasi Amazon S3 tidak berada di akun AWS yang sama dengan katalog data, ikuti petunjuk di Mendaftarkan lokasi Amazon S3 terenkripsi di seluruh akun. AWS

Buat jenis aset khusus

Di Amazon DataZone, aset mewakili jenis sumber daya data tertentu seperti tabel database, dasbor, atau model pembelajaran mesin. Untuk memberikan konsistensi dan standardisasi saat mendeskripsikan aset katalog, DataZone domain Amazon harus memiliki sekumpulan jenis aset yang menentukan bagaimana aset direpresentasikan dalam katalog. Jenis aset mendefinisikan skema untuk jenis aset tertentu. Tipe aset memiliki sekumpulan tipe formulir metadata yang diperlukan dan dapat diberi nama opsional (misalnya, GovForm atau). GovernanceFormType Jenis aset di Amazon DataZone berversi. Ketika aset dibuat, mereka divalidasi terhadap skema yang ditentukan oleh jenis aset mereka (biasanya versi terbaru), dan jika struktur yang tidak valid ditentukan, pembuatan aset gagal.

Jenis aset sistem - Amazon DataZone menyediakan jenis aset sistem milik layanan (termasuk GlueTableAssetType,,,, GlueViewAssetType RedshiftTableAssetType RedshiftViewAssetType, dan S3ObjectCollectionAssetType) dan jenis formulir sistem (termasuk DataSourceReferenceFormType,

AssetCommonDetailsFormType, dan). SubscriptionTermsFormType Jenis aset sistem tidak dapat diedit.

Jenis aset kustom - untuk membuat jenis aset kustom, Anda mulai dengan membuat jenis formulir metadata yang diperlukan dan glosarium untuk digunakan dalam jenis formulir. Anda kemudian dapat membuat jenis aset kustom dengan menentukan nama, deskripsi, dan formulir metadata terkait yang dapat diperlukan atau opsional.

Untuk tipe aset dengan data terstruktur, untuk mewakili skema kolom di portal data, Anda dapat menggunakan `RelationalTableFormType` untuk menambahkan metadata teknis ke kolom Anda, termasuk nama kolom, deskripsi, dan tipe data) dan `ColumnBusinessMetadataForm` untuk menambahkan deskripsi bisnis kolom, termasuk nama bisnis, istilah glosarium, dan pasangan nilai kunci kustom.

Untuk membuat jenis aset kustom melalui portal Data, selesaikan langkah-langkah berikut:

1. Arahkan ke URL portal DataZone data Amazon dan masuk menggunakan sistem masuk tunggal (SSO) atau kredensil Anda. AWS Jika Anda DataZone administrator Amazon, Anda dapat menavigasi ke DataZone konsol Amazon di https://console.aws.amazon.com/datazone dan masuk dengan Akun AWS tempat domain dibuat, lalu pilih Buka portal data.
2. Pilih Pilih proyek dari panel navigasi atas dan pilih proyek tempat Anda ingin membuat jenis aset kustom.
3. Arahkan ke tab Data untuk proyek.
4. Pilih Jenis aset dari panel navigasi kiri, lalu pilih Buat jenis aset.
5. Tentukan yang berikut dan kemudian pilih Buat.
   - Nama - nama jenis aset kustom
   - Deskripsi - deskripsi jenis aset kustom.
   - Pilih Tambahkan formulir metadata untuk menambahkan formulir metadata ke jenis aset kustom ini.
6. Setelah jenis aset kustom dibuat, Anda dapat menggunakannya untuk membuat aset.

Untuk membuat jenis aset kustom melalui API, selesaikan langkah-langkah berikut:

1. Buat tipe formulir metadata dengan menjalankan tindakan API. `CreateFormType`

   Berikut ini adalah SageMaker contoh Amazon:

```
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. Selanjutnya, Anda dapat membuat tipe aset dengan menjalankan tindakan `CreateAssetType` API. Anda dapat membuat jenis aset hanya melalui Amazon DataZone API menggunakan jenis formulir sistem yang tersedia (`SubscriptionTermsFormType`dalam contoh di bawah ini) atau jenis formulir kustom Anda. Untuk tipe formulir sistem, nama tipe harus dimulai dengan`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,
        },
    },
)
```

Berikut ini adalah contoh untuk membuat tipe aset untuk data terstruktur:

```
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. Dan sekarang, Anda dapat membuat aset menggunakan jenis aset khusus yang Anda buat pada langkah-langkah di atas.

```
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}"
        }
        ]
)
```

Dan dalam contoh ini Anda membuat aset data terstruktur:

```
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": ".."
        },
        .....
        ]
)
```

Membuat dan menjalankan sumber DataZone data Amazon untuk AWS Glue Data Catalog

Di Amazon DataZone, Anda dapat membuat sumber AWS Glue Data Catalog data untuk mengimpor metadata teknis tabel database. AWS Glue Untuk menambahkan sumber data untuk AWS Glue Data Catalog, database sumber harus sudah ada di AWS Glue.

Saat membuat dan menjalankan sumber AWS Glue data, Anda menambahkan aset dari AWS Glue database sumber ke inventaris DataZone proyek Amazon Anda. Anda dapat menjalankan sumber AWS Glue data Anda pada jadwal yang ditetapkan atau sesuai permintaan untuk membuat atau memperbarui metadata teknis aset Anda. Selama sumber data berjalan, Anda dapat memilih untuk mempublikasikan aset Anda ke DataZone katalog Amazon dan dengan demikian membuatnya dapat ditemukan oleh semua pengguna domain. Anda juga dapat mempublikasikan aset inventaris proyek Anda setelah mengedit metadata bisnis mereka. Pengguna domain dapat mencari dan menemukan aset Anda yang dipublikasikan, dan meminta langganan ke aset tersebut.

Untuk menambahkan sumber AWS Glue data

1. Arahkan ke URL portal DataZone data Amazon dan masuk menggunakan sistem masuk tunggal (SSO) atau kredensil Anda. AWS Jika Anda DataZone administrator Amazon, Anda dapat menavigasi ke DataZone konsol Amazon di https://console.aws.amazon.com/datazone dan masuk dengan Akun AWS tempat domain dibuat, lalu pilih Buka portal data.
2. Pilih Pilih proyek dari panel navigasi atas dan pilih proyek yang ingin Anda tambahkan sumber data.
3. Arahkan ke tab Data untuk proyek.
4. Pilih Sumber data dari panel navigasi kiri, lalu pilih Buat sumber data.
5. Konfigurasi bidang berikut:

- Nama — Nama sumber data.
- Deskripsi — Deskripsi sumber data.

6. Di bawah Jenis sumber data, pilih AWS Glue.
7. Di bawah Pilih lingkungan, tentukan lingkungan untuk mempublikasikan AWS Glue tabel.
8. Di bawah Pemilihan data, berikan AWS Glue database dan masukkan kriteria pemilihan tabel Anda. Misalnya, jika Anda memilih Sertakan dan masukkan`*corporate`, database akan menyertakan semua tabel sumber yang diakhiri dengan kata`corporate`.

   Anda dapat memilih AWS Glue database dari dropdown atau mengetik nama database. Dropdown mencakup dua database: database penerbitan dan database langganan lingkungan. Jika Anda ingin membawa aset membentuk database yang tidak dibuat oleh lingkungan, maka Anda harus mengetikkan nama database alih-alih memilihnya dari dropdown.

   Anda dapat menambahkan beberapa aturan include dan exclude untuk tabel dalam satu database. Anda juga dapat menambahkan beberapa database menggunakan tombol Add another database.

9. Di bawah Kualitas data, Anda dapat memilih untuk Mengaktifkan kualitas data untuk sumber data ini. Jika Anda melakukan ini, Amazon DataZone mengimpor output kualitas data AWS Glue yang ada ke dalam DataZone katalog Amazon Anda. Secara default, Amazon DataZone mengimpor 100 laporan kualitas terbaru yang ada tanpa tanggal kedaluwarsa dari Glue. AWS

   Metrik kualitas data di Amazon DataZone membantu Anda memahami kelengkapan dan keakuratan sumber data Anda. Amazon DataZone menarik metrik kualitas data ini dari AWS Glue untuk memberikan konteks selama suatu titik waktu, misalnya, selama pencarian katalog data bisnis. Pengguna data dapat melihat bagaimana metrik kualitas data berubah dari waktu ke waktu untuk aset berlangganan mereka. Produsen data dapat menelan skor kualitas data AWS Glue sesuai jadwal. Katalog data DataZone bisnis Amazon juga dapat menampilkan metrik kualitas data dari sistem pihak ketiga melalui API kualitas data. Untuk informasi selengkapnya, lihat Kualitas data di Amazon DataZone
10. Pilih Selanjutnya.
11. Untuk pengaturan Penerbitan, pilih apakah aset segera dapat ditemukan di katalog data bisnis. Jika Anda hanya menambahkannya ke inventaris, Anda dapat memilih persyaratan berlangganan nanti dan mempublikasikannya ke katalog data bisnis. Untuk informasi selengkapnya, lihat the section called “Mengelola sumber data yang ada”.

12. Untuk pembuatan nama bisnis otomatis, pilih apakah akan secara otomatis menghasilkan metadata untuk aset saat diimpor dari sumbernya.
13. (Opsional) Untuk formulir Metadata, tambahkan formulir untuk menentukan metadata yang dikumpulkan dan disimpan saat aset diimpor ke Amazon. DataZone Untuk informasi selengkapnya, lihat the section called “Membuat, mengedit, atau menghapus formulir metadata”.
14. Untuk preferensi Jalankan, pilih kapan menjalankan sumber data.
    - Jalankan sesuai jadwal - Tentukan tanggal dan waktu untuk menjalankan sumber data.
    - Jalankan sesuai permintaan - Anda dapat memulai proses sumber data secara manual.
15. Pilih Selanjutnya.
16. Tinjau konfigurasi sumber data Anda dan pilih Buat.

Membuat dan menjalankan sumber DataZone data Amazon untuk Amazon Redshift

Di Amazon DataZone, Anda dapat membuat sumber data Amazon Redshift untuk mengimpor metadata teknis tabel database dan tampilan dari gudang data Amazon Redshift. Untuk menambahkan sumber DataZone data Amazon untuk Amazon Redshift, gudang data sumber harus sudah ada di Amazon Redshift.

Saat membuat dan menjalankan sumber data Amazon Redshift, Anda menambahkan aset dari gudang data Amazon Redshift sumber ke inventaris proyek DataZone Amazon Anda. Anda dapat menjalankan sumber data Amazon Redshift pada jadwal yang ditetapkan atau sesuai permintaan untuk membuat atau memperbarui metadata teknis aset Anda. Selama sumber data berjalan, Anda dapat memilih untuk mempublikasikan aset inventaris proyek Anda ke DataZone katalog Amazon dan dengan demikian membuatnya dapat ditemukan oleh semua pengguna domain. Anda juga dapat mempublikasikan aset inventaris Anda setelah mengedit metadata bisnis mereka. Pengguna domain dapat mencari dan menemukan aset Anda yang dipublikasikan dan meminta langganan ke aset ini.

Untuk menambahkan sumber data Amazon Redshift

1. Arahkan ke URL portal DataZone data Amazon dan masuk menggunakan sistem masuk tunggal (SSO) atau kredensil Anda. AWS Jika Anda DataZone administrator Amazon, Anda dapat menavigasi ke DataZone konsol Amazon di https://console.aws.amazon.com/datazone dan masuk dengan Akun AWS tempat domain dibuat, lalu pilih Buka portal data.

2. Pilih Pilih proyek dari panel navigasi atas dan pilih proyek yang ingin Anda tambahkan sumber data.
3. Arahkan ke tab Data untuk proyek.
4. Pilih Sumber data dari panel navigasi kiri, lalu pilih Buat sumber data.
5. Konfigurasi bidang berikut:
   - Nama — Nama sumber data.
   - Deskripsi — Deskripsi sumber data.
6. Di bawah Jenis sumber data, pilih Amazon Redshift.
7. Di bawah Pilih lingkungan, tentukan lingkungan untuk mempublikasikan tabel Amazon Redshift.
8. Bergantung pada lingkungan yang Anda pilih, Amazon DataZone akan secara otomatis menerapkan kredensil Amazon Redshift dan parameter lain langsung dari lingkungan atau memberi Anda opsi untuk memilih sendiri.
   - Jika Anda telah memilih lingkungan yang hanya memungkinkan penerbitan dari skema Amazon Redshift default lingkungan, Amazon DataZone akan secara otomatis menerapkan kredenal Amazon Redshift dan parameter lainnya termasuk klaster Amazon Redshift atau nama grup kerja, rahasia, nama database, dan nama skema. AWS Anda tidak dapat mengedit parameter yang diisi otomatis ini.
   - Jika Anda memilih lingkungan yang tidak memungkinkan untuk mempublikasikan data apa pun, Anda tidak akan dapat melanjutkan pembuatan sumber data.
   - Jika Anda memilih lingkungan yang memungkinkan penerbitan data dari skema apa pun, Anda akan melihat opsi untuk menggunakan kredensil dan parameter Amazon Redshift lainnya dari lingkungan atau memasukkan kredensial/parameter Anda sendiri.
9. Jika Anda memilih untuk menggunakan kredensil Anda sendiri untuk membuat sumber data, berikan detail berikut:
   - Di bawah Menyediakan kredensyal Amazon Redshift, pilih apakah akan menggunakan klaster Amazon Redshift yang disediakan atau ruang kerja Amazon Redshift Tanpa Server sebagai sumber data Anda.
   - Bergantung pada pilihan Anda pada langkah di atas, pilih klaster Amazon Redshift atau ruang kerja Anda dari menu tarik-turun, lalu pilih rahasia di Secrets Manager AWS yang akan digunakan untuk otentikasi. Anda dapat memilih rahasia yang ada atau membuat yang baru.
   - Agar rahasia yang ada muncul di drop-down, pastikan rahasia Anda di AWS Secrets Manager menyertakan tag berikut (kunci/nilai):

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

Jika Anda memilih untuk membuat rahasia baru, maka rahasia secara otomatis ditandai dengan tag yang direferensikan di atas dan tidak ada langkah tambahan yang diperlukan. Untuk informasi selengkapnya, lihat Menyimpan kredensi database di. AWS Secrets Manager

Pengguna Amazon Redshift dalam AWS rahasia yang disediakan untuk membuat sumber data harus memiliki `SELECT` izin pada tabel yang akan dipublikasikan. Jika Anda DataZone ingin Amazon juga mengelola langganan (akses) atas nama Anda, pengguna database dalam AWS rahasia juga harus memiliki izin berikut:

- `CREATE DATASHARE`
- `ALTER DATASHARE`
- `DROP DATASHARE`

10. Di bawah Pemilihan data, berikan database Amazon Redshift, skema, dan masukkan tabel atau kriteria pemilihan tampilan Anda. Misalnya, jika Anda memilih Sertakan dan masukkan`*corporate`, aset akan menyertakan semua tabel sumber yang diakhiri dengan kata`corporate`.

    Anda dapat menambahkan beberapa aturan include untuk tabel dalam satu database. Anda juga dapat menambahkan beberapa database menggunakan tombol Add another database.

11. Pilih Selanjutnya.
12. Untuk pengaturan Penerbitan, pilih apakah aset segera dapat ditemukan di katalog data. Jika Anda hanya menambahkannya ke inventaris, Anda dapat memilih persyaratan berlangganan nanti dan mempublikasikannya ke katalog data bisnis. Untuk informasi selengkapnya, lihat the section called “Mengelola sumber data yang ada”.
13. Untuk pembuatan nama bisnis otomatis, pilih apakah akan secara otomatis menghasilkan metadata untuk aset saat dipublikasikan dan diperbarui dari sumbernya.
14. (Opsional) Untuk formulir Metadata, tambahkan formulir untuk menentukan metadata yang dikumpulkan dan disimpan saat aset diimpor ke Amazon. DataZone Untuk informasi selengkapnya, lihat the section called “Membuat, mengedit, atau menghapus formulir metadata”.
15. Untuk preferensi Jalankan, pilih kapan menjalankan sumber data.

    - Jalankan sesuai jadwal - Tentukan tanggal dan waktu untuk menjalankan sumber data.
    - Jalankan sesuai permintaan - Anda dapat memulai proses sumber data secara manual.

16. Pilih Selanjutnya.
17. Tinjau konfigurasi sumber data Anda dan pilih Buat.

Mengelola sumber DataZone data Amazon yang ada

Setelah membuat sumber DataZone data Amazon, Anda dapat memodifikasinya kapan saja untuk mengubah detail sumber atau kriteria pemilihan data. Ketika Anda tidak lagi membutuhkan sumber data, Anda dapat menghapusnya.

Untuk menyelesaikan langkah-langkah ini, Anda harus memiliki kebijakan AmazonDataZoneFullAccess AWS terkelola yang dilampirkan. Untuk informasi selengkapnya, lihat the section called “AWS kebijakan terkelola”.

Topik

Mengedit sumber data

Anda dapat mengedit sumber DataZone data Amazon untuk mengubah setelan pemilihan datanya, termasuk menambahkan, menghapus, atau mengubah kriteria pemilihan tabel. Anda juga dapat menambah dan menghapus database. Anda tidak dapat mengubah tipe sumber data atau lingkungan tempat sumber data dipublikasikan.

Untuk mengedit sumber data

1. Arahkan ke URL portal DataZone data Amazon dan masuk menggunakan sistem masuk tunggal (SSO) atau kredensil Anda. AWS Jika Anda DataZone administrator Amazon, Anda dapat menavigasi ke DataZone konsol Amazon di https://console.aws.amazon.com/datazone dan masuk dengan Akun AWS tempat domain dibuat, lalu pilih Buka portal data.
2. Pilih Pilih proyek dari panel navigasi atas dan pilih proyek yang menjadi sumber datanya.
3. Arahkan ke tab Data untuk proyek.
4. Pilih Sumber data dari panel navigasi kiri, lalu pilih sumber data yang ingin Anda ubah.
5. Arahkan ke tab Definisi sumber data dan pilih Edit.
6. Buat perubahan Anda pada definisi sumber data. Anda dapat memperbarui detail sumber data dan membuat perubahan pada kriteria pemilihan data.

7. Setelah selesai membuat perubahan, pilih Simpan.

Hapus sumber data

Jika Anda tidak lagi membutuhkan sumber DataZone data Amazon, Anda dapat menghapusnya secara terus-menerus. Setelah Anda menghapus sumber data, semua aset yang berasal dari sumber data tersebut masih tersedia di katalog, dan pengguna masih dapat berlangganan. Namun, aset akan berhenti menerima pembaruan dari sumbernya. Kami menyarankan Anda terlebih dahulu memindahkan aset dependen ke sumber data yang berbeda sebelum Anda menghapusnya.

> **Note**
>
> Anda harus menghapus semua pemenuhan pada sumber data sebelum Anda dapat menghapusnya. Untuk informasi selengkapnya, lihat Menemukan, berlangganan, dan mengkonsumsi data di Amazon DataZone.

Untuk menghapus sumber data

1. Pada tab Data untuk proyek, pilih Sumber data dari panel navigasi kiri.
2. Pilih sumber data yang ingin Anda hapus.
3. Pilih Tindakan, Hapus sumber data, dan konfirmasi penghapusan.

Publikasikan aset ke DataZone katalog Amazon dari inventaris proyek

Anda dapat mempublikasikan DataZone aset Amazon dan metadatanya dari inventaris proyek ke dalam katalog Amazon. DataZone Anda hanya dapat mempublikasikan versi terbaru dari aset ke katalog.

Pertimbangkan hal berikut saat menerbitkan aset ke katalog:

- Untuk mempublikasikan aset ke katalog, Anda harus menjadi pemilik atau kontributor proyek tersebut.
- Untuk aset Amazon Redshift, pastikan bahwa klaster Amazon Redshift yang terkait dengan klaster penerbit dan pelanggan memenuhi semua persyaratan untuk berbagi data Amazon Redshift agar

Amazon dapat mengelola akses untuk tabel dan tampilan Redshift. DataZone Lihat Konsep berbagi data untuk Amazon Redshift.

- Amazon DataZone hanya mendukung manajemen akses untuk aset yang diterbitkan dari AWS Glue Data Catalog dan Amazon Redshift. Untuk semua aset lainnya, seperti objek Amazon S3, Amazon DataZone tidak mengelola akses untuk pelanggan yang disetujui. Jika berlangganan aset yang tidak dikelola ini, Anda akan diberi tahu dengan pesan berikut:

  ```
  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.
  ```

Publikasikan aset

Jika Anda tidak memilih untuk membuat aset segera dapat ditemukan di katalog data saat membuat sumber data, lakukan langkah-langkah berikut untuk mempublikasikannya nanti.

Untuk mempublikasikan aset

1. Arahkan ke URL portal DataZone data Amazon dan masuk menggunakan sistem masuk tunggal (SSO) atau kredensil Anda. AWS Jika Anda DataZone administrator Amazon, Anda dapat menavigasi ke DataZone konsol Amazon di https://console.aws.amazon.com/datazone dan masuk dengan Akun AWS tempat domain dibuat, lalu pilih Buka portal data.
2. Pilih Pilih proyek dari panel navigasi atas dan pilih proyek tempat aset tersebut berada.
3. Arahkan ke tab Data untuk proyek.
4. Pilih Data inventaris dari panel navigasi kiri, lalu pilih aset yang ingin Anda publikasikan.

   > **Note**
   >
   > Secara default, semua aset memerlukan persetujuan berlangganan, yang berarti pemilik data harus menyetujui semua permintaan langganan ke aset tersebut. Jika Anda ingin mengubah setelan ini sebelum memublikasikan aset, buka detail aset dan pilih Edit di samping Persetujuan langganan. Anda dapat mengubah setelan ini nanti dengan memodifikasi dan menerbitkan ulang aset.

5. Pilih Publikasikan aset. Aset tersebut langsung dipublikasikan ke katalog.

Jika Anda membuat perubahan pada aset, seperti memodifikasi persyaratan persetujuannya, Anda dapat memilih Publikasikan ulang untuk mempublikasikan pembaruan ke katalog.

Kelola inventaris dan kurasi aset

Untuk menggunakan Amazon DataZone untuk membuat katalog data Anda, Anda harus terlebih dahulu membawa data (aset) Anda sebagai inventaris proyek Anda di Amazon DataZone. Membuat inventaris untuk proyek tertentu, membuat aset hanya dapat ditemukan oleh anggota proyek itu.

Setelah aset dibuat dalam inventaris proyek, metadatanya dapat dikuratori. Misalnya, Anda dapat mengedit nama aset, deskripsi, atau membaca saya. Setiap pengeditan aset membuat versi baru aset. Anda dapat menggunakan tab Riwayat di halaman detail aset untuk melihat semua versi aset.

Anda dapat mengedit bagian Baca Saya dan menambahkan deskripsi kaya untuk aset. Bagian Read Me mendukung penurunan harga, sehingga memungkinkan Anda untuk memformat deskripsi Anda sesuai kebutuhan dan menjelaskan informasi penting tentang aset kepada konsumen.

Istilah glosarium dapat ditambahkan di tingkat aset dengan mengisi formulir yang tersedia.

Untuk mengkurasi skema, Anda dapat meninjau kolom, menambahkan nama bisnis, deskripsi, dan menambahkan istilah glosarium di tingkat kolom.

Jika pembuatan metadata otomatis diaktifkan saat sumber data dibuat, nama bisnis untuk aset dan kolom tersedia untuk ditinjau dan diterima atau ditolak secara individual atau sekaligus.

Anda juga dapat mengedit persyaratan berlangganan untuk menentukan apakah persetujuan untuk aset diperlukan atau tidak.

Formulir metadata di Amazon DataZone memungkinkan Anda memperluas model metadata aset data dengan menambahkan atribut yang ditentukan khusus (misalnya, wilayah penjualan, tahun penjualan, dan kuartal penjualan). Formulir metadata yang dilampirkan ke jenis aset diterapkan ke semua aset yang dibuat dari jenis aset tersebut. Anda juga dapat menambahkan formulir metadata tambahan ke aset individual sebagai bagian dari sumber data yang dijalankan atau setelah dibuat. Untuk membuat formulir baru, lihatthe section called “Membuat, mengedit, atau menghapus formulir metadata”.

Untuk memperbarui metadata aset, Anda harus menjadi pemilik atau kontributor proyek tempat aset tersebut berada.

Untuk memperbarui metadata aset

1. Arahkan ke URL portal DataZone data Amazon dan masuk menggunakan sistem masuk tunggal (SSO) atau kredensil Anda. AWS Jika Anda DataZone administrator Amazon, Anda dapat menavigasi ke DataZone konsol Amazon di https://console.aws.amazon.com/datazone dan masuk dengan Akun AWS tempat domain dibuat, lalu pilih Buka portal data.
2. Pilih Pilih proyek dari panel navigasi atas dan pilih proyek yang berisi aset yang metadatanya ingin Anda perbarui.
3. Arahkan ke tab Data untuk proyek.
4. Pilih Data inventaris dari panel navigasi kiri, lalu pilih nama aset yang metadatanya ingin Anda perbarui.
5. Pada halaman detail aset, di bawah Formulir metadata, pilih Edit dan edit formulir yang ada sesuai kebutuhan. Anda juga dapat melampirkan formulir metadata tambahan ke aset. Untuk informasi selengkapnya, lihat the section called “Lampirkan formulir metadata tambahan ke aset”.
6. Setelah selesai melakukan pembaruan, pilih Simpan formulir.

   Saat Anda menyimpan formulir, Amazon DataZone menghasilkan versi inventaris baru dari aset tersebut. Untuk mempublikasikan versi terbaru ke katalog, pilih Publikasikan ulang aset.

Lampirkan formulir metadata tambahan ke aset

Secara default, formulir metadata yang dilampirkan ke domain dilampirkan ke semua aset yang dipublikasikan ke domain tersebut. Penerbit data dapat mengaitkan formulir metadata tambahan ke aset individu untuk memberikan konteks tambahan.

Untuk melampirkan formulir metadata tambahan ke aset

1. Arahkan ke URL portal DataZone data Amazon dan masuk menggunakan sistem masuk tunggal (SSO) atau kredensil Anda. AWS Jika Anda DataZone administrator Amazon, Anda dapat menavigasi ke DataZone konsol Amazon di https://console.aws.amazon.com/datazone dan masuk dengan Akun AWS tempat domain dibuat, lalu pilih Buka portal data.
2. Pilih Pilih proyek dari panel navigasi atas dan pilih proyek yang berisi aset yang metadatanya ingin Anda tambahkan.
3. Arahkan ke tab Data untuk proyek.

4. Pilih Data inventaris dari panel navigasi kiri, lalu pilih nama aset yang metadatanya ingin Anda tambahkan.
5. Pada halaman detail aset, di bawah Formulir metadata, pilih Tambahkan formulir.
6. Pilih formulir yang akan ditambahkan ke aset, lalu pilih Tambahkan formulir.
7. Masukkan nilai untuk setiap bidang metadata, lalu pilih Simpan formulir.

   Saat Anda menyimpan formulir, Amazon DataZone menghasilkan versi inventaris baru dari aset tersebut. Untuk mempublikasikan versi terbaru ke katalog, pilih Publikasikan ulang aset.

Publikasikan aset ke katalog setelah kurasi

Setelah puas dengan kurasi aset, pemilik data dapat mempublikasikan versi aset ke DataZone katalog Amazon dan dengan demikian membuatnya dapat ditemukan oleh semua pengguna domain. Aset menunjukkan versi inventaris dan versi yang diterbitkan. Dalam katalog penemuan, hanya versi terbitan terbaru yang muncul. Jika metadata diperbarui setelah diterbitkan, maka versi inventaris baru akan tersedia untuk diterbitkan ke katalog.

Buat aset secara manual

Di Amazon DataZone, aset adalah entitas yang menyajikan objek data fisik tunggal (misalnya, tabel, dasbor, file) atau objek data virtual (misalnya, tampilan). Untuk informasi selengkapnya, lihat DataZone Terminologi dan konsep Amazon. Menerbitkan aset secara manual adalah operasi satu kali. Anda tidak menentukan jadwal berjalan untuk aset, sehingga tidak diperbarui secara otomatis jika sumbernya berubah.

Untuk membuat aset secara manual melalui proyek, Anda harus menjadi pemilik atau kontributor proyek itu.

Untuk membuat aset secara manual

1. Arahkan ke URL portal DataZone data Amazon dan masuk menggunakan sistem masuk tunggal (SSO) atau kredensil Anda. AWS Jika Anda DataZone administrator Amazon, Anda dapat menavigasi ke DataZone konsol Amazon di https://console.aws.amazon.com/datazone dan masuk dengan Akun AWS tempat domain dibuat, lalu pilih Buka portal data.
2. Pilih Pilih proyek dari panel navigasi atas dan pilih proyek untuk membuat aset.
3. Arahkan ke tab Data untuk proyek.

4. Pilih Sumber data dari panel navigasi kiri, lalu pilih Buat aset data.
5. Untuk detail Aset, konfigurasikan pengaturan berikut:
   - Jenis aset — Jenis aset.
   - Nama — Nama aset.
   - Deskripsi — Deskripsi aset.
6. Untuk lokasi S3, masukkan Nama Sumber Daya Amazon (ARN) dari bucket S3 sumber.

   Secara opsional, masukkan titik akses S3. Untuk informasi selengkapnya, lihat Mengelola akses data dengan titik akses Amazon S3.
7. Untuk pengaturan Penerbitan, pilih apakah aset segera dapat ditemukan di katalog. Jika Anda hanya menambahkannya ke inventaris, Anda dapat memilih persyaratan berlangganan nanti untuk mempublikasikannya ke katalog.
8. Pilih Buat.

   Setelah aset dibuat, itu akan langsung diterbitkan sebagai aset aktif dalam katalog, atau akan disimpan dalam inventaris sampai Anda memutuskan untuk menerbitkannya.

Batalkan publikasi aset dari katalog Amazon DataZone

Saat Anda membatalkan publikasi aset Amazon dari katalog, DataZone aset tersebut tidak lagi muncul di hasil penelusuran global. Pengguna baru tidak akan dapat menemukan atau berlangganan daftar aset di katalog, tetapi semua langganan yang ada tetap sama.

Untuk membatalkan penerbitan aset, Anda harus menjadi pemilik atau kontributor proyek tempat aset tersebut berada:

Untuk membatalkan publikasi aset

1. Arahkan ke URL portal DataZone data Amazon dan masuk menggunakan sistem masuk tunggal (SSO) atau kredensil Anda. AWS Jika Anda DataZone administrator Amazon, Anda dapat menavigasi ke DataZone konsol Amazon di https://console.aws.amazon.com/datazone dan masuk dengan Akun AWS tempat domain dibuat, lalu pilih Buka portal data.
2. Pilih Pilih proyek dari panel navigasi atas dan pilih proyek tempat aset tersebut berada.
3. Arahkan ke tab Data untuk proyek.
4. Pilih Data yang dipublikasikan dari panel navigasi kiri.

5. Temukan aset dari daftar aset yang dipublikasikan, lalu pilih Batalkan publikasi.

   Aset dihapus dari katalog. Anda dapat mempublikasikan ulang aset kapan saja dengan memilih Publikasikan.

Hapus DataZone aset Amazon

Ketika Anda tidak lagi membutuhkan aset di Amazon DataZone, Anda dapat menghapusnya secara permanen. Menghapus aset berbeda dengan membatalkan penerbitan aset dari katalog. Anda dapat menghapus aset dan daftar terkaitnya di katalog sehingga tidak terlihat di hasil penelusuran apa pun. Untuk menghapus daftar aset, Anda harus mencabut semua langganannya terlebih dahulu.

Untuk menghapus aset, Anda harus menjadi pemilik atau kontributor proyek tempat aset tersebut berada:

> **Note**
>
> Untuk menghapus daftar aset, Anda harus terlebih dahulu mencabut semua langganan aset yang ada. Anda tidak dapat menghapus daftar aset yang memiliki pelanggan yang sudah ada.

Untuk menghapus dan aset

1. Arahkan ke URL portal DataZone data Amazon dan masuk menggunakan sistem masuk tunggal (SSO) atau kredensil Anda. AWS Jika Anda DataZone administrator Amazon, Anda dapat menavigasi ke DataZone konsol Amazon di https://console.aws.amazon.com/datazone dan masuk dengan Akun AWS tempat domain dibuat, lalu pilih Buka portal data.
2. Pilih Pilih proyek dari panel navigasi atas dan pilih proyek yang berisi aset yang ingin Anda hapus.
3. Arahkan ke tab Data untuk proyek.
4. Pilih Data yang dipublikasikan dari panel navigasi kiri, lalu cari dan pilih aset yang ingin Anda hapus. Ini membuka halaman detail aset.
5. Pilih Tindakan, Hapus, dan konfirmasi penghapusan.

   Setelah aset dihapus, aset tidak lagi tersedia untuk dilihat dan pengguna tidak dapat berlangganan.

Memulai sumber data secara manual yang dijalankan di Amazon DataZone

Saat Anda menjalankan sumber data, Amazon DataZone menarik semua metadata baru atau yang dimodifikasi dari sumber dan memperbarui aset terkait dalam inventaris. Saat menambahkan sumber data ke Amazon DataZone, Anda menentukan preferensi jalankan sumber, yang menentukan apakah sumber berjalan sesuai jadwal atau sesuai permintaan. Jika sumber Anda berjalan sesuai permintaan, Anda harus memulai sumber data yang dijalankan secara manual.

Bahkan jika sumber Anda berjalan sesuai jadwal, Anda masih dapat menjalankannya secara manual kapan saja. Setelah menambahkan metadata bisnis ke aset, Anda dapat memilih aset dan mempublikasikannya ke DataZone katalog Amazon agar aset ini dapat ditemukan oleh semua pengguna domain. Hanya aset yang dipublikasikan yang dapat dicari oleh pengguna domain lain.

Untuk menjalankan sumber data secara manual

1. Arahkan ke URL portal DataZone data Amazon dan masuk menggunakan sistem masuk tunggal (SSO) atau kredensil Anda. AWS Jika Anda DataZone administrator Amazon, Anda dapat menavigasi ke DataZone konsol Amazon di https://console.aws.amazon.com/datazone dan masuk dengan Akun AWS tempat domain dibuat, lalu pilih Buka portal data.
2. Pilih Pilih proyek dari panel navigasi atas dan pilih proyek yang menjadi sumber datanya.
3. Arahkan ke tab Data untuk proyek.
4. Pilih Sumber data dari panel navigasi kiri, lalu cari dan pilih sumber data yang ingin Anda jalankan. Ini membuka halaman detail sumber data.
5. Pilih Jalankan sesuai permintaan.

   Status sumber data berubah menjadi `Running` saat Amazon DataZone memperbarui metadata aset dengan data terbaru dari sumbernya. Anda dapat memantau status proses pada tab Sumber data berjalan.

Revisi aset di Amazon DataZone

Amazon DataZone meningkatkan revisi aset saat Anda mengedit metadata bisnis atau teknisnya. Pengeditan ini termasuk memodifikasi nama aset, deskripsi, istilah glosarium, nama kolom, formulir metadata, dan nilai bidang formulir metadata. Perubahan ini dapat dihasilkan dari pengeditan

manual, menjalankan pekerjaan sumber data, atau operasi API. Amazon DataZone secara otomatis menghasilkan revisi aset baru setiap kali Anda mengedit aset tersebut.

Setelah Anda memperbarui aset dan revisi baru dibuat, Anda harus mempublikasikan revisi baru ke katalog agar dapat diperbarui dan tersedia untuk pelanggan. Untuk informasi selengkapnya, lihat the section called “Publikasikan aset ke katalog dari inventaris proyek”. Anda hanya dapat mempublikasikan versi terbaru dari aset ke katalog.

Untuk melihat revisi aset sebelumnya

1. Arahkan ke URL portal DataZone data Amazon dan masuk menggunakan sistem masuk tunggal (SSO) atau kredensil Anda. AWS Jika Anda DataZone administrator Amazon, Anda dapat menavigasi ke DataZone konsol Amazon di https://console.aws.amazon.com/datazone dan masuk dengan Akun AWS tempat domain dibuat, lalu pilih Buka portal data.
2. Pilih Pilih proyek dari panel navigasi atas dan pilih proyek yang berisi aset.
3. Arahkan ke tab Data untuk proyek, lalu cari dan pilih aset. Ini membuka halaman detail aset.
4. Arahkan ke tab Riwayat, yang menampilkan daftar revisi aset sebelumnya.

Kualitas data di Amazon DataZone

Metrik kualitas data di Amazon DataZone membantu Anda memahami berbagai metrik kualitas seperti kelengkapan, ketepatan waktu, dan keakuratan sumber data Anda. Amazon DataZone terintegrasi dengan AWS Glue Data Quality dan menawarkan API untuk mengintegrasikan metrik kualitas data dari solusi kualitas data pihak ketiga. Pengguna data dapat melihat bagaimana metrik kualitas data berubah dari waktu ke waktu untuk aset berlangganan mereka. Untuk membuat dan menjalankan aturan kualitas data, Anda dapat menggunakan alat kualitas data pilihan Anda seperti kualitas data AWS Glue. Dengan metrik kualitas data di Amazon DataZone, konsumen data dapat memvisualisasikan skor kualitas data untuk aset dan kolom, membantu membangun kepercayaan pada data yang mereka gunakan untuk keputusan.

Prasyarat dan perubahan peran IAM

Jika Anda menggunakan kebijakan DataZone AWS terkelola Amazon, tidak ada langkah konfigurasi tambahan dan kebijakan terkelola ini diperbarui secara otomatis untuk mendukung kualitas data. Jika Anda menggunakan kebijakan Anda sendiri untuk peran yang memberikan Amazon DataZone izin yang diperlukan untuk beroperasi dengan layanan yang didukung, Anda harus memperbarui kebijakan yang dilampirkan pada peran ini untuk mengaktifkan dukungan untuk membaca informasi kualitas data AWS Glue di AWS kebijakan terkelola:

AmazonDataZoneGlueManageAccessRolePolicy dan mengaktifkan dukungan untuk API deret waktu di AWS kebijakan terkelola: AmazonDataZoneDomainExecutionRolePolicy dan. AWS kebijakan terkelola: AmazonDataZoneFullUserAccess

Mengaktifkan kualitas data untuk aset AWS Glue

Amazon DataZone menarik metrik kualitas data dari AWS Glue untuk memberikan konteks selama suatu titik waktu, misalnya, selama pencarian katalog data bisnis. Pengguna data dapat melihat bagaimana metrik kualitas data berubah dari waktu ke waktu untuk aset berlangganan mereka. Produsen data dapat menelan skor kualitas data AWS Glue sesuai jadwal. Katalog data DataZone bisnis Amazon juga dapat menampilkan metrik kualitas data dari sistem pihak ketiga melalui API kualitas data. Untuk informasi selengkapnya, lihat AWS Glue Data Quality dan Memulai AWS Glue Data Quality untuk Katalog Data.

Anda dapat mengaktifkan metrik kualitas data untuk DataZone aset Amazon Anda dengan cara berikut:

- Gunakan Portal Data atau Amazon DataZone API untuk mengaktifkan kualitas data untuk sumber data AWS Glue Anda melalui portal DataZone data Amazon baik saat membuat sumber data AWS Glue baru atau mengedit yang ada.

  Untuk informasi selengkapnya tentang mengaktifkan kualitas data untuk sumber data melalui portal, lihat Membuat dan menjalankan sumber DataZone data Amazon untuk AWS Glue Data Catalog danMengelola sumber DataZone data Amazon yang ada.

  > **Note**
  >
  > Anda dapat menggunakan Portal Data untuk mengaktifkan kualitas data hanya untuk aset inventaris AWS Glue Anda. Dalam rilis Amazon ini, DataZone mengaktifkan kualitas data untuk Amazon Redshift atau jenis kustom aset melalui portal data tidak didukung.

  Anda juga dapat menggunakan API untuk mengaktifkan kualitas data untuk sumber data baru atau yang sudah ada. Anda dapat melakukan ini dengan memanggil CreateDataSourceatau UpdateDataSourcedan mengatur `autoImportDataQualityResult` parameter ke 'Benar'.

  Setelah kualitas data diaktifkan, Anda dapat menjalankan sumber data sesuai permintaan atau sesuai jadwal. Setiap proses dapat menghasilkan hingga 100 metrik per aset. Tidak perlu membuat formulir atau menambahkan metrik secara manual saat menggunakan sumber data untuk kualitas

data. Ketika aset dipublikasikan, pembaruan yang dibuat pada formulir kualitas data (hingga 30 titik data per aturan sejarah) tercermin dalam daftar untuk konsumen. Selanjutnya, setiap penambahan metrik baru ke aset, secara otomatis ditambahkan ke daftar. Tidak perlu mempublikasikan ulang aset untuk membuat skor terbaru tersedia bagi konsumen.

Mengaktifkan kualitas data untuk jenis aset kustom

Anda dapat menggunakan DataZone API Amazon untuk mengaktifkan kualitas data untuk semua jenis aset kustom Anda. Untuk informasi selengkapnya, lihat berikut ini:

- PostTimeSeriesDataPoints
- ListTimeSeriesDataPoints
- GetTimeSeriesDataPoint
- DeleteTimeSeriesDataPoints

Langkah-langkah berikut memberikan contoh penggunaan API atau CLI untuk mengimpor metrik pihak ketiga untuk aset Anda di Amazon: DataZone

1. Panggil `PostTimeSeriesDataPoints` API sebagai berikut:

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

dengan muatan berikut:

```
{
"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. Panggil `DeleteTimeSeriesDataPoints` API sebagai berikut:

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

Menggunakan pembelajaran mesin dan AI generatif

> **Note**
>
> Didukung oleh Amazon Bedrock: AWS mengimplementasikan deteksi penyalahgunaan otomatis. Karena rekomendasi AI untuk fungsionalitas deskripsi di Amazon DataZone dibangun di Amazon Bedrock, pengguna mewarisi kontrol yang diterapkan di Amazon Bedrock untuk menegakkan keselamatan, keamanan, dan penggunaan AI yang bertanggung jawab.

Dalam rilis Amazon saat ini DataZone, Anda dapat menggunakan rekomendasi AI untuk fungsionalitas deskripsi untuk mengotomatiskan penemuan dan katalogisasi data. Support untuk AI generatif dan pembelajaran mesin di Amazon DataZone membuat deskripsi untuk aset dan kolom. Anda dapat menggunakan deskripsi ini untuk menambahkan konteks bisnis untuk data Anda dan merekomendasikan analisis untuk kumpulan data, yang dapat membantu meningkatkan hasil penemuan data.

Didukung oleh model bahasa Amazon Bedrock yang besar, rekomendasi AI untuk deskripsi aset data di Amazon DataZone membantu Anda memastikan bahwa data Anda dapat dipahami dan mudah ditemukan. Rekomendasi AI juga menyarankan aplikasi analitis yang paling relevan untuk kumpulan data. Dengan mengurangi tugas dokumentasi manual dan memberi saran tentang penggunaan data yang tepat, deskripsi yang dibuat secara otomatis dapat membantu Anda meningkatkan kepercayaan data Anda dan meminimalkan pengabaian data berharga untuk mempercepat pengambilan keputusan berdasarkan informasi.

> **Important**
>
> Dalam DataZone rilis Amazon saat ini, rekomendasi AI untuk fitur deskripsi hanya didukung di wilayah berikut:
>
> - AS Timur (Virginia Utara)
> - AS Barat (Oregon)
> - Eropa (Frankfurt)
> - Asia Pasifik (Tokyo)

Prosedur berikut menjelaskan cara menghasilkan rekomendasi AI untuk deskripsi di Amazon DataZone:

1. Arahkan ke URL portal DataZone data Amazon, lalu masuk menggunakan sistem masuk tunggal (SSO) atau kredensil Anda. AWS Jika Anda DataZone administrator Amazon, navigasikan ke DataZone konsol Amazon di https://console.aws.amazon.com/datazone dan masuk dengan Akun AWS tempat domain dibuat, lalu pilih Buka portal data.
2. Di panel navigasi atas, pilih Pilih proyek, lalu pilih proyek yang berisi aset yang ingin Anda hasilkan rekomendasi AI untuk deskripsi.
3. Arahkan ke tab Data untuk proyek.
4. Di panel navigasi kiri, pilih Data inventaris, lalu pilih nama aset yang ingin Anda hasilkan rekomendasi AI untuk deskripsi aset tersebut.
5. Pada halaman detail aset, di tab Metadata bisnis, pilih Hasilkan deskripsi.
6. Setelah deskripsi dibuat, Anda dapat mengedit, menerima, atau menolaknya. Ikon hijau ditampilkan di samping setiap deskripsi metadata yang dihasilkan secara otomatis untuk aset data. Di tab Metadata bisnis, Anda dapat memilih ikon hijau di samping Ringkasan yang dibuat secara otomatis, lalu pilih Edit, Terima, atau Tolak untuk mengatasi deskripsi yang dihasilkan. Anda juga dapat memilih Terima semua atau Tolak semua opsi yang ditampilkan di bagian atas halaman saat tab Metadata Bisnis dipilih, dan dengan demikian melakukan tindakan yang dipilih pada semua deskripsi yang dihasilkan secara otomatis.

   Atau Anda dapat memilih tab Skema, dan kemudian alamat deskripsi yang dihasilkan secara otomatis satu per satu dengan memilih ikon hijau untuk satu deskripsi kolom pada satu waktu dan kemudian memilih Terima atau Tolak. Di tab Skema, Anda juga dapat memilih Terima semua atau Tolak semua dan dengan demikian melakukan tindakan yang dipilih pada semua deskripsi yang dibuat secara otomatis.
7. Untuk memublikasikan aset ke katalog dengan deskripsi yang dihasilkan, pilih Publikasikan aset, lalu konfirmasikan tindakan ini dengan memilih Publikasikan aset lagi di jendela pop up Publikasikan aset.

> **Note**
>
> Jika Anda tidak menerima atau menolak deskripsi yang dihasilkan untuk suatu aset, lalu Anda memublikasikan aset ini, metadata yang dihasilkan secara otomatis yang tidak ditinjau ini tidak disertakan dalam aset data yang dipublikasikan.

Menemukan, berlangganan, dan mengkonsumsi data di Amazon DataZone

Di Amazon DataZone, setelah aset dipublikasikan ke domain, pelanggan dapat menemukan dan meminta langganan aset ini. Proses berlangganan dimulai dengan pelanggan yang mencari dan menelusuri katalog untuk menemukan aset yang mereka inginkan. Dari DataZone portal Amazon, mereka memilih untuk berlangganan aset dengan mengirimkan permintaan berlangganan yang mencakup pembenaran dan alasan permintaan tersebut. Penyetuju langganan, sebagaimana didefinisikan dalam perjanjian penerbitan, kemudian meninjau permintaan akses. Mereka dapat menyetujui atau menolak permintaan tersebut.

Setelah berlangganan diberikan, proses pemenuhan mulai memfasilitasi akses ke aset untuk pelanggan. Ada dua mode utama kontrol dan pemenuhan akses aset: untuk aset yang DataZone dikelola Amazon dan untuk aset yang tidak dikelola oleh Amazon. DataZone

- Aset terkelola — Amazon DataZone dapat mengelola pemenuhan dan izin untuk aset terkelola, seperti AWS Glue tabel dan tabel serta tampilan Amazon Redshift.
- Aset yang tidak dikelola — Amazon DataZone menerbitkan peristiwa standar yang terkait dengan tindakan Anda (misalnya, persetujuan yang diberikan untuk permintaan berlangganan) ke Amazon. EventBridge Anda dapat menggunakan acara standar ini untuk berintegrasi dengan AWS layanan lain atau solusi pihak ketiga untuk integrasi khusus.

Topik

Menemukan data

Tugas-tugas berikut menjelaskan berbagai cara untuk menemukan data di Amazon DataZone.

Topik

Cari dan lihat aset di katalog

Amazon DataZone menyediakan cara yang efisien untuk mencari data. Setiap DataZone pengguna Amazon dengan izin untuk mengakses portal data dapat mencari aset di DataZone katalog Amazon dan melihat nama aset dan metadata yang ditetapkan untuk mereka. Anda dapat melihat lebih dekat aset dengan memeriksa halaman detailnya.

> **Note**
>
> Untuk melihat data aktual yang terkandung dalam aset, Anda harus terlebih dahulu berlangganan aset tersebut dan meminta permintaan langganan Anda disetujui dan akses diberikan. Untuk informasi selengkapnya, lihat Berlangganan data.

Untuk mencari aset di katalog

1. Arahkan ke URL portal DataZone data Amazon dan masuk menggunakan sistem masuk tunggal (SSO) atau kredensil Anda. AWS Jika Anda DataZone administrator Amazon, Anda dapat menavigasi ke DataZone konsol Amazon di https://console.aws.amazon.com/datazone dan masuk dengan Akun AWS tempat domain dibuat, lalu pilih Buka portal data.
2. Anda dapat mengetikkan nama aset yang Anda cari di bilah pencarian di halaman beranda portal data.
3. Untuk menelusuri ruang nama, pilih Katalog dari kanan atas halaman untuk membuka katalog. Katalog menyediakan pengalaman penelusuran segi bagi Anda untuk menemukan aset dengan mencari pada kriteria seperti, pemilik data, dan istilah glosarium.
4. Masukkan istilah pencarian Anda di salah satu kotak pencarian. Setelah Anda menjalankan pencarian, Anda dapat menerapkan berbagai filter untuk mempersempit hasil. Filter termasuk jenis aset, akun sumber, dan tempat Wilayah AWS aset tersebut berada.
5. Untuk melihat detail tentang aset tertentu, pilih aset untuk membuka halaman detailnya. Halaman detail mencakup informasi berikut:

   - Nama aset, sumber data (AWS Glue, Amazon Redshift, atau Amazon S3), jenis (tabel, tampilan, atau objek S3), jumlah kolom, dan ukuran.
   - Deskripsi aset.
   - Revisi aset yang diterbitkan saat ini, pemilik, apakah persetujuan diperlukan untuk langganan, namepace, dan riwayat pembaruan.

- Tab Ikhtisar yang mencakup istilah glosarium dan formulir metadata.
- Tab Skema yang menampilkan skema aset, termasuk nama kolom bisnis dan teknis, tipe data, dan deskripsi bisnis kolom. Tab skema hanya terlihat untuk tabel dan tampilan (bukan untuk objek Amazon S3).
- Tab Langganan yang mencakup daftar pelanggan ke domain.
- Tab Riwayat yang mencakup daftar revisi aset sebelumnya.

Berlangganan data

Tugas-tugas berikut memberikan detail tentang berlangganan aset di Amazon DataZone.

Topik

Minta berlangganan aset

Amazon DataZone memungkinkan Anda menemukan, mengakses, dan mengkonsumsi aset di DataZone katalog Amazon. Ketika Anda menemukan aset dalam katalog yang ingin Anda akses, Anda harus berlangganan aset, yang membuat permintaan berlangganan. Penyetuju kemudian dapat menyetujui atau meminta permintaan Anda.

Anda harus menjadi anggota proyek untuk meminta berlangganan aset dalam proyek itu.

Untuk berlangganan aset

1. Arahkan ke URL portal DataZone data Amazon dan masuk menggunakan sistem masuk tunggal (SSO) atau kredensil Anda. AWS Jika Anda DataZone administrator Amazon, Anda dapat menavigasi ke DataZone konsol Amazon di https://console.aws.amazon.com/datazone dan masuk dengan Akun AWS tempat domain dibuat, lalu pilih Buka portal data.

2. Gunakan bilah pencarian untuk mencari dan memilih aset yang ingin Anda berlangganan, lalu pilih Berlangganan.
3. Di jendela pop up Berlangganan, berikan informasi berikut:
   - Proyek yang ingin Anda berlangganan aset.
   - Pembenaran singkat untuk permintaan berlangganan Anda.
4. Pilih Langganan.

   Anda menerima pemberitahuan di portal data saat penerbit menyetujui permintaan Anda.

Untuk melihat status permintaan berlangganan, cari dan pilih proyek yang Anda gunakan untuk berlangganan aset tersebut. Arahkan ke tab Data untuk proyek, lalu pilih Data yang diminta dari panel navigasi kiri. Halaman ini mencantumkan aset yang diminta akses proyek. Anda dapat memfilter daftar berdasarkan status permintaan.

Menyetujui atau menolak permintaan berlangganan

Amazon DataZone memungkinkan Anda menemukan, mengakses, dan mengkonsumsi aset di DataZone katalog Amazon. Ketika Anda menemukan aset dalam katalog yang ingin Anda akses, Anda harus berlangganan aset, yang membuat permintaan berlangganan. Penyetuju kemudian dapat menyetujui atau menolak permintaan Anda.

Anda harus menjadi anggota proyek pemilik (proyek yang menerbitkan aset) untuk menyetujui atau menolak permintaan berlangganan.

Untuk menyetujui atau menolak permintaan berlangganan

1. Arahkan ke URL portal DataZone data Amazon dan masuk menggunakan sistem masuk tunggal (SSO) atau kredensil Anda. AWS Jika Anda DataZone administrator Amazon, Anda dapat menavigasi ke DataZone konsol Amazon di https://console.aws.amazon.com/datazone dan masuk dengan Akun AWS tempat domain dibuat, lalu pilih Buka portal data.
2. Di portal data, pilih Jelajahi daftar proyek dan pilih proyek yang berisi aset dengan permintaan berlangganan.
3. Arahkan ke tab Data, lalu pilih Permintaan masuk dari panel navigasi kiri.
4. Temukan permintaan dan pilih Lihat permintaan. Anda dapat memfilter berdasarkan Pending untuk melihat hanya permintaan yang masih terbuka.

5. Tinjau permintaan berlangganan dan alasan akses, dan putuskan apakah akan menyetujui atau menolaknya.
6. (Opsional) Masukkan respons yang menjelaskan alasan Anda menerima atau menolak permintaan.
7. Pilih Setujui atau Tolak.

Sebagai pemilik proyek, Anda dapat mencabut langganan kapan saja. Untuk informasi selengkapnya, lihat the section called “Cabut langganan yang sudah ada”.

Untuk melihat semua permintaan langganan, lihatBekerja dengan DataZone acara dan notifikasi Amazon.

Cabut langganan yang sudah ada

Amazon DataZone memungkinkan Anda menemukan, mengakses, dan mengkonsumsi aset di DataZone katalog Amazon. Ketika Anda menemukan aset dalam katalog yang ingin Anda akses, Anda harus berlangganan aset, yang membuat permintaan berlangganan. Penyetuju kemudian dapat menyetujui atau meminta permintaan Anda. Anda mungkin perlu mencabut langganan setelah Anda menyetujuinya, baik karena persetujuan itu adalah kesalahan, atau karena pelanggan tidak lagi memerlukan akses ke aset tersebut.

Anda harus menjadi anggota proyek pemilik (proyek yang menerbitkan aset) untuk mencabut langganan.

Untuk mencabut langganan

1. Arahkan ke URL portal DataZone data Amazon dan masuk menggunakan sistem masuk tunggal (SSO) atau kredensil Anda. AWS Jika Anda DataZone administrator Amazon, Anda dapat menavigasi ke DataZone konsol Amazon di https://console.aws.amazon.com/datazone dan masuk dengan Akun AWS tempat domain dibuat, lalu pilih Buka portal data.
2. Pilih Pilih proyek dari panel navigasi atas dan pilih proyek yang berisi langganan yang ingin Anda cabut.
3. Arahkan ke tab Data, lalu pilih Permintaan masuk dari panel navigasi kiri.
4. Temukan langganan yang ingin dicabut dan pilih Lihat langganan.
5. (Opsional) Aktifkan kotak centang untuk memungkinkan pelanggan menyimpan aset dalam target langganan proyek. Target langganan adalah referensi ke sekumpulan sumber daya di mana data berlangganan dapat tersedia dalam suatu lingkungan.

Jika Anda ingin mencabut akses ke aset dari target langganan di lain waktu, Anda harus melakukannya di. AWS Lake Formation

6. Pilih Cabut langganan.

Anda tidak dapat menyetujui kembali langganan setelah mencabutnya. Pelanggan harus berlangganan aset lagi agar Anda dapat menyetujuinya.

Membatalkan permintaan berlangganan

Amazon DataZone memungkinkan Anda menemukan, mengakses, dan mengkonsumsi aset di DataZone katalog Amazon. Ketika Anda menemukan aset dalam katalog yang ingin Anda akses, Anda harus berlangganan aset, yang membuat permintaan berlangganan. Penyetuju kemudian dapat menyetujui atau meminta permintaan Anda. Anda mungkin perlu membatalkan permintaan langganan yang tertunda, baik karena Anda mengirimkannya secara tidak sengaja, atau karena Anda tidak lagi memerlukan akses baca ke aset tersebut.

Untuk membatalkan permintaan berlangganan, Anda harus menjadi pemilik proyek atau kontributor.

Untuk membatalkan permintaan berlangganan

1. Arahkan ke URL portal DataZone data Amazon dan masuk menggunakan sistem masuk tunggal (SSO) atau kredensil Anda. AWS Jika Anda DataZone administrator Amazon, Anda dapat menavigasi ke DataZone konsol Amazon di https://console.aws.amazon.com/datazone dan masuk dengan Akun AWS tempat domain dibuat, lalu pilih Buka portal data.
2. Pilih Pilih proyek dari panel navigasi atas dan pilih proyek yang berisi permintaan berlangganan.
3. Arahkan ke tab Data untuk proyek, lalu pilih Data yang diminta dari panel navigasi kiri. Halaman ini mencantumkan aset yang diminta akses proyek.
4. Filter menurut Diminta untuk melihat hanya permintaan yang masih tertunda. Temukan permintaan dan pilih Lihat permintaan.
5. Tinjau permintaan berlangganan dan pilih Batalkan permintaan.

Jika Anda ingin berlangganan kembali aset (atau aset lain), lihatthe section called “Minta berlangganan aset”.

Berhenti berlangganan dari aset

Amazon DataZone memungkinkan Anda menemukan, mengakses, dan mengkonsumsi aset di DataZone katalog Amazon. Ketika Anda menemukan aset dalam katalog yang ingin Anda akses, Anda harus berlangganan aset, yang membuat permintaan berlangganan. Penyetuju kemudian dapat menyetujui atau meminta permintaan Anda. Anda mungkin perlu berhenti berlangganan dari aset, baik karena Anda berlangganan secara tidak sengaja dan disetujui, atau karena Anda tidak lagi memerlukan akses baca ke aset tersebut.

Anda harus menjadi anggota proyek untuk berhenti berlangganan dari salah satu asetnya.

Untuk berhenti berlangganan dari aset

1. Arahkan ke URL portal DataZone data Amazon dan masuk menggunakan sistem masuk tunggal (SSO) atau kredensil Anda. AWS Jika Anda DataZone administrator Amazon, Anda dapat menavigasi ke DataZone konsol Amazon di https://console.aws.amazon.com/datazone dan masuk dengan Akun AWS tempat domain dibuat, lalu pilih Buka portal data.
2. Pilih Pilih proyek dari panel navigasi atas dan pilih proyek yang berisi aset yang ingin Anda hentikan berlangganan.
3. Arahkan ke tab Data untuk proyek, lalu pilih Data yang diminta dari panel navigasi kiri. Halaman ini mencantumkan aset yang diminta akses proyek.
4. Filter menurut Disetujui untuk melihat hanya permintaan yang telah disetujui. Temukan permintaan dan pilih Lihat langganan.
5. Tinjau langganan dan pilih Berhenti Berlangganan.

Jika Anda ingin berlangganan kembali aset (atau aset lain), lihatthe section called “Minta berlangganan aset”.

Menggunakan peran IAM yang ada untuk memenuhi langganan Amazon DataZone

Dalam rilis saat ini, Amazon DataZone mendukung Anda menggunakan peran IAM yang ada untuk mendapatkan akses ke data. Untuk mencapai hal ini, Anda dapat membuat target berlangganan di DataZone lingkungan Amazon yang Anda gunakan untuk memenuhi langganan Anda. Untuk membuat target langganan untuk lingkungan di salah satu AWS akun terkait, Anda dapat menggunakan langkah-langkah berikut:

Langkah 1: Pastikan DataZone domain Amazon Anda menggunakan kebijakan RAM versi 2 atau lebih tinggi

1. Arahkan ke halaman Shared by me: Resource share di konsol AWS RAM.
2. Karena pembagian sumber daya AWS RAM ada di AWS Wilayah tertentu, pilih AWS Wilayah yang sesuai dari daftar tarik-turun di sudut kanan atas konsol.
3. Pilih pembagian sumber daya yang sesuai dengan DataZone domain Amazon Anda, lalu pilih Ubah. Anda dapat mengidentifikasi pembagian RAM untuk DataZone domain Amazon menggunakan nama atau ID domain saat pembagian RAM dibuat dengan nama:`DataZone-<domain-name>-<domain-id>`.
4. Pilih Berikutnya untuk melanjutkan ke langkah berikutnya di mana Anda dapat memeriksa versi kebijakan RAM dan memodifikasinya.
5. Pastikan bahwa versi kebijakan RAM adalah Versi 2 atau lebih tinggi. Jika tidak, gunakan dropdown untuk memilih Versi 2 atau lebih tinggi.
6. Pilih Lewati ke langkah 4: Tinjau dan perbarui.
7. Pilih Perbarui berbagi sumber daya.

Langkah 2: Buat target langganan dari akun terkait

- Dalam rilis saat ini, Amazon DataZone mendukung pembuatan target langganan hanya dengan menggunakan API. Di bawah ini adalah beberapa contoh payload yang dapat Anda gunakan untuk membuat target langganan untuk memenuhi langganan ke tabel AWS Glue dan tabel atau tampilan Amazon Redshift Anda. Untuk informasi lebih lanjut, lihat CreateSubscriptionTarget.

  Contoh target berlangganan untuk 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"
```

```
}
```

Contoh target berlangganan untuk 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

- EnvironmentIdentifier yang Anda gunakan dalam panggilan API di atas harus ada di akun terkait yang sama dari mana Anda melakukan panggilan API. Jika tidak, panggilan API tidak akan berhasil.
- ARN peran IAM yang Anda gunakan di “AuthorizedPrincipals” adalah peran yang akan diberikan DataZone Amazon akses setelah aset berlangganan ditambahkan ke target langganan. Prinsipal resmi ini harus memiliki akun yang sama dengan lingkungan tempat target berlangganan dibuat.
- Nilai untuk bidang penyedia harus “Amazon DataZone” DataZone agar Amazon dapat menyelesaikan pemenuhan langganan.
- Nama database yang disediakan subscriptionTargetConfig seharusnya sudah ada di akun tempat target dibuat. Amazon tidak DataZone akan membuat database ini. Pastikan juga bahwa peran kelola akses memiliki izin CREATE TABLE pada database ini.

- Pastikan juga bahwa peran (peran IAM untuk AWS Glue dan peran database untuk Amazon Redshift) disediakan sebagai prinsip resmi sudah ada di akun lingkungan. Untuk target langganan Amazon Redshift, pembaruan tambahan diperlukan untuk peran yang diasumsikan saat menghubungkan ke cluster. Peran ini harus memiliki RedshiftDbRoles tag yang melekat pada peran. Nilai tag dapat berupa daftar yang dipisahkan koma. Nilai harus menjadi peran database yang disediakan sebagai prinsipal resmi saat membuat target berlangganan.

Langkah 3: Berlangganan tabel baru dan memenuhi langganan ke target baru

- Setelah Anda membuat target berlangganan, Anda dapat berlangganan tabel baru dan Amazon DataZone akan memenuhinya ke target di atas. Untuk informasi selengkapnya, lihat Berlangganan data.

Memberikan akses ke data

Tugas-tugas berikut memberikan rincian pemberian akses ke langganan yang disetujui ke aset di Amazon. DataZone

Di Amazon DataZone, permintaan berlangganan dan langganan yang disetujui atau diberikan untuk akses baca ke aset dikelola oleh pemberi persetujuan langganan. Penyetuju berlangganan untuk suatu aset ditentukan oleh perjanjian penerbitan yang dengannya aset ini diterbitkan ke dalam DataZone katalog Amazon.

Topik

- Berikan akses ke AWS Glue Data Catalog aset terkelola
- Berikan akses ke aset Amazon Redshift yang dikelola
- Berikan akses untuk langganan yang disetujui ke aset yang tidak dikelola

Berikan akses ke AWS Glue Data Catalog aset terkelola

> **Note**
>
> Manajemen akses untuk AWS Glue Data Catalog aset yang menggunakan metode AWS Lake Formation LF-TBAC tidak didukung.

Support untuk berbagi aset lintas wilayah AWS Glue Data Catalog tidak didukung.

Setelah permintaan berlangganan ke AWS Glue Data Catalog aset terkelola disetujui, Amazon DataZone secara otomatis menambahkan aset ini ke semua lingkungan data lake yang ada dalam proyek. Amazon DataZone kemudian memberikan dan mengelola akses ke AWS Glue Data Catalog tabel yang disetujui atas nama Anda melalui AWS Lake Formation. Untuk proyek pelanggan, aset yang diberikan muncul di sumber daya AWS Glue Data Catalog as di akun Anda. Anda kemudian dapat menggunakan Amazon Athena untuk menanyakan tabel.

Note

Jika lingkungan data lake baru ditambahkan ke proyek setelah AWS Glue Data Catalog aset berlangganan ditambahkan secara otomatis ke lingkungan data lake yang ada, Anda harus menambahkan AWS Glue Data Catalog aset berlangganan ini secara manual ke lingkungan danau data baru ini. Anda dapat melakukan ini dengan memilih opsi Tambahkan hibah di tab Data halaman ikhtisar proyek di portal DataZone data Amazon.

Agar Amazon DataZone dapat memberikan akses ke tabel Katalog Data AWS Glue, ketentuan berikut harus dipenuhi.

- Tabel AWS Glue harus dikelola oleh Lake Formation karena Amazon DataZone memberikan akses dengan mengelola izin Lake Formation.
- Peran Kelola akses untuk lingkungan data lake yang digunakan untuk mempublikasikan tabel Katalog Data AWS Glue harus memiliki izin Lake Formation berikut:
  - `DESCRIBE`dan `DESCRIBE GRANTABLE` izin pada database AWS Glue yang berisi tabel yang diterbitkan.
  - `DESCRIBE`,`SELECT`,`DESCRIBE GRANTABLE`, `SELECT GRANTABLE` izin di Lake Formation pada tabel yang diterbitkan itu sendiri.

Untuk informasi selengkapnya, lihat Memberikan dan mencabut izin pada sumber daya katalog di Panduan Pengembang.AWS Lake Formation

Berikan akses ke aset Amazon Redshift yang dikelola

Saat berlangganan tabel atau tampilan Amazon Redshift disetujui, Amazon DataZone dapat secara otomatis menambahkan aset berlangganan ke semua lingkungan gudang data dalam proyek, sehingga anggota proyek dapat menanyakan data menggunakan tautan editor kueri Amazon Redshift di lingkungan mereka. Di bawah tenda, Amazon DataZone, menciptakan hibah dan datashares yang diperlukan antara sumber dan target berlangganan.

Proses pemberian akses bervariasi tergantung di mana basis data sumber (penerbit) dan basis data target (pelanggan) berada.

- Cluster yang sama, database yang sama - jika data harus dibagikan dalam database yang sama, Amazon DataZone memberikan izin langsung pada tabel sumber.
- Cluster yang sama, database yang berbeda - jika data harus dibagikan di dua database dalam cluster yang sama, Amazon DataZone membuat tampilan di database target dan izin diberikan pada tampilan yang dibuat.
- Akun yang sama cluster berbeda - Amazon DataZone membuat datashare antara sumber dan kluster target dan membuat tampilan di atas tabel bersama. Izin diberikan pada tampilan.
- Cross-account - sama seperti di atas tetapi langkah tambahan diperlukan untuk mengotorisasi datashare lintas akun di sisi cluster produsen dan langkah lain untuk mengaitkan pembagian data di sisi cluster konsumen.

> **Note**
>
> Jika lingkungan gudang data baru ditambahkan ke proyek setelah aset Amazon Redshift berlangganan ditambahkan secara otomatis ke lingkungan gudang data yang ada, Anda harus menambahkan aset Amazon Redshift berlangganan ini secara manual ke lingkungan gudang data baru ini. Anda dapat melakukan ini dengan memilih opsi Tambahkan hibah di tab Data halaman ikhtisar proyek di portal DataZone data Amazon.

Pastikan bahwa klaster Amazon Redshift yang menerbitkan dan berlangganan memenuhi semua persyaratan untuk rangkaian data Amazon Redshift. Untuk informasi selengkapnya, lihat Panduan Pengembang Amazon Redshift.

> **Note**
>
> Amazon DataZone mendukung pemberian langganan secara otomatis ke aset Amazon Redshift Cluster dan Amazon Redshift Tanpa Server.
> Berbagi data lintas wilayah menggunakan Amazon Redshift tidak didukung.

> **Note**
>
> Dalam rilis saat ini, Amazon DataZone dapat mengelola akses ke tabel dan tampilan Amazon Redshift hanya jika sumber dan target klaster Amazon Redshift atau grup kerja terletak di akun milik organisasi yang AWS sama. AWS

Berikan akses untuk langganan yang disetujui ke aset yang tidak dikelola

Amazon DataZone memungkinkan pengguna untuk mempublikasikan semua jenis aset dalam katalog data bisnis. Untuk beberapa aset ini, Amazon DataZone dapat secara otomatis mengelola hibah akses. Aset ini disebut aset terkelola dan termasuk tabel Katalog Data AWS Glue yang dikelola Lake Formation serta tabel dan tampilan Amazon Redshift. Semua aset lain yang Amazon tidak DataZone dapat secara otomatis memberikan langganan disebut tidak dikelola.

Amazon DataZone menyediakan jalur bagi Anda untuk mengelola hibah akses untuk aset Anda yang tidak dikelola. Ketika langganan aset dalam katalog data bisnis disetujui oleh pemilik data, Amazon DataZone menerbitkan acara di Amazon EventBridge di akun Anda bersama dengan semua informasi yang diperlukan dalam muatan yang memungkinkan Anda membuat hibah akses antara sumber dan target. Ketika Anda menerima acara ini, Anda dapat memicu penangan khusus yang dapat menggunakan informasi dalam acara tersebut untuk membuat hibah atau izin yang diperlukan. Setelah Anda memberikan akses, Anda dapat melaporkan kembali dan memperbarui status langganan di Amazon DataZone sehingga dapat memberi tahu pengguna yang berlangganan aset bahwa mereka dapat mulai mengkonsumsi aset tersebut. Untuk informasi selengkapnya, lihat Bekerja dengan DataZone acara dan notifikasi Amazon.

Mengkonsumsi data

Tugas-tugas berikut memberikan rincian konsumsi data yang telah Anda berlangganan di Amazon DataZone.

Topik

Kueri data di Amazon Athena atau Amazon Redshift

Di Amazon DataZone, setelah pelanggan memiliki akses ke aset dalam katalog, mereka dapat menggunakannya (kueri dan analisis) menggunakan Amazon Athena atau editor kueri Amazon Redshift v2. Anda harus menjadi pemilik proyek atau kontributor untuk menyelesaikan tugas ini. Bergantung pada cetak biru yang diaktifkan dalam proyek, Amazon DataZone menyediakan tautan ke Amazon Athena dan/atau editor kueri Amazon Redshift v2 di panel sisi kanan halaman proyek di portal data.

1. Arahkan ke URL portal DataZone data Amazon dan masuk menggunakan sistem masuk tunggal (SSO) atau kredensil Anda. AWS Jika Anda DataZone administrator Amazon, Anda dapat menavigasi ke DataZone konsol Amazon di https://console.aws.amazon.com/datazone dan masuk dengan Akun AWS tempat domain dibuat, lalu pilih Buka portal data.
2. Di portal DataZone data Amazon, pilih Jelajahi Daftar Proyek dan kemudian temukan dan pilih proyek tempat Anda memiliki data yang ingin Anda analisis.
3. Jika cetak biru Data Lake diaktifkan pada proyek ini, tautan ke Amazon Athena ditampilkan di panel sisi kanan di halaman beranda proyek.

   Jika cetak biru Data Warehouse diaktifkan pada proyek ini, tautan ke editor kueri ditampilkan di panel sisi kanan pada halaman beranda proyek.

   > **Note**
   >
   > Cetak biru didefinisikan dalam profil lingkungan yang dengannya proyek dibuat.

Topik

Kueri data menggunakan Amazon Athena

Pilih tautan Amazon Athena untuk membuka editor kueri Amazon Athena di tab baru di browser menggunakan kredensi proyek untuk otentikasi. DataZoneProyek Amazon yang Anda kerjakan secara otomatis dipilih sebagai workgroup saat ini di editor kueri.

Di editor kueri Amazon Athena, tulis dan jalankan kueri Anda. Beberapa tugas umum meliputi:

- Kueri dan analisis aset berlangganan Anda
- Buat tabel baru
- Buat tabel dari hasil kueri (CTAS) dari bucket S3 eksternal

Kueri dan analisis aset berlangganan Anda

Jika akses ke aset yang dilanggani project Anda tidak diberikan secara otomatis oleh Amazon DataZone, Anda harus diberi wewenang untuk mengakses data yang mendasarinya. Untuk informasi selengkapnya tentang cara memberikan akses ke aset ini, lihatBerikan akses untuk langganan yang disetujui ke aset yang tidak dikelola.

Jika akses ke aset yang dilanggani project Anda diberikan secara otomatis oleh Amazon DataZone, Anda dapat menjalankan kueri SQL pada tabel dan melihat hasilnya di Amazon Athena. Untuk informasi selengkapnya tentang penggunaan SQL di Amazon Athena, lihat referensi SQL untuk Athena.

Saat Anda menavigasi ke editor kueri Amazon Athena setelah memilih tautan Amazon Athena di panel sisi kanan di halaman beranda proyek, tarik-turun Proyek ditampilkan di sudut kanan atas editor kueri Amazon Athena dan konteks proyek Anda dipilih secara otomatis.

Anda dapat melihat database berikut di dropdown Database:

- Database penerbitan (*{environmentname}*_pub_db). Tujuan dari database ini adalah untuk memberi Anda lingkungan di mana Anda dapat menghasilkan data baru dalam konteks proyek Anda dan kemudian dapat mempublikasikan data ini ke dalam DataZone katalog Amazon. Pemilik proyek dan kontributor telah membaca dan menulis akses ke database ini. Pemirsa proyek hanya memiliki akses baca ke database ini.
- Database berlangganan (*{environmentname}*_sub_db). Tujuan dari database ini adalah untuk berbagi dengan Anda data yang telah Anda berlangganan sebagai anggota proyek di DataZone katalog Amazon, dan untuk memungkinkan Anda untuk menanyakan data tersebut.

Buat tabel baru

Jika Anda telah terhubung ke bucket S3 eksternal, Anda dapat menggunakan Amazon Athena untuk menanyakan dan menganalisis aset dari bucket Amazon S3 eksternal. Dalam skenario ini, Amazon DataZone tidak memiliki izin untuk memberikan akses langsung ke data yang mendasarinya di bucket Amazon S3 eksternal, dan data Amazon S3 eksternal yang dibuat di luar proyek tidak dikelola secara otomatis di Lake Formation, dan tidak dapat dikelola oleh Amazon. DataZone Alternatifnya adalah menyalin data dari bucket Amazon S3 eksternal ke tabel baru di dalam bucket Amazon S3 proyek menggunakan pernyataan di Amazon `CREATE TABLE` Athena. Saat Anda menjalankan `CREATE TABLE` kueri di Amazon Athena, Anda mendaftarkan tabel Anda dengan file. AWS Glue Data Catalog

Untuk menentukan jalur ke data Anda di Amazon S3, gunakan `LOCATION` properti, seperti yang ditunjukkan pada contoh berikut:

```
CREATE EXTERNAL TABLE 'test_table'(
...
)
ROW FORMAT ...
STORED AS INPUTFORMAT ...
OUTPUTFORMAT ...
LOCATION 's3://bucketname/folder/'
```

Untuk informasi selengkapnya, lihat Lokasi tabel di Amazon S3.

Buat tabel dari hasil kueri (CTAS) dari bucket S3 eksternal

Saat Anda berlangganan aset, akses ke data yang mendasarinya hanya baca. Anda dapat menggunakan Amazon Athena untuk membuat salinan tabel. Di Amazon Athena, `A CREATE TABLE AS SELECT (CTAS)` kueri membuat tabel baru di Amazon Athena dari hasil pernyataan dari kueri `SELECT` lain. Untuk informasi tentang sintaks CTAS, lihat MEMBUAT TABEL AS.

Contoh berikut membuat tabel dengan menyalin semua kolom dari tabel:

```
CREATE TABLE new_table AS
SELECT *
FROM old_table;
```

Dalam variasi berikut dari contoh yang sama, AndaSELECTpernyataan juga mencakupWHEREKlausul. Dalam kasus ini, kueri memilih hanya baris dari tabel yang memenuhiWHEREKlausul:

```
CREATE TABLE new_table AS
SELECT *
FROM old_table WHERE condition;
```

Contoh berikut membuat kueri baru yang berjalan pada satu set kolom dari tabel lain:

```
CREATE TABLE new_table AS
SELECT column_1, column_2, ... column_n
FROM old_table;
```

Variasi ini dari contoh yang sama menciptakan tabel baru dari kolom tertentu dari beberapa tabel:

```
CREATE TABLE new_table AS
SELECT column_1, column_2, ... column_n
FROM old_table_1, old_table_2, ... old_table_n;
```

Tabel yang baru dibuat ini sekarang menjadi bagian dari AWS Glue database proyek Anda, dan dapat ditemukan oleh orang lain dan dibagikan dengan DataZone proyek Amazon lainnya dengan menerbitkan data sebagai aset ke katalog Amazon. DataZone

Kueri data menggunakan Amazon Redshift

Di portal DataZone data Amazon, buka lingkungan yang menggunakan cetak biru gudang data. Pilih tautan Amazon Redshift di panel sebelah kanan pada halaman lingkungan. Ini membuka dialog konfirmasi dengan detail penting yang membantu Anda membuat koneksi ke klaster Amazon Redshift lingkungan atau grup kerja Amazon Redshift Serverless di editor kueri Amazon Redshift v2.0. Setelah Anda mengidentifikasi detail yang diperlukan untuk membuat koneksi, pilih tombol Buka Amazon Redshift. Ini membuka editor kueri Amazon Redshift v2.0 di tab baru di browser menggunakan kredensil sementara dari lingkungan Amazon. DataZone

Di editor kueri, ikuti langkah-langkah di bawah ini tergantung pada apakah lingkungan Anda menggunakan workgroup Amazon Redshift Tanpa Server atau cluster Amazon Redshift.

Untuk grup kerja Amazon Redshift Tanpa Server

1. Di editor kueri, identifikasi grup kerja Amazon Redshift Serverless DataZone lingkungan Amazon Anda, klik kanan dan pilih Buat koneksi.
2. Pilih Pengguna Federasi untuk otentikasi.
3. Berikan nama database DataZone lingkungan Amazon.
4. Pilih Buat koneksi.

Untuk cluster Amazon Redshift:

1. Di editor kueri, identifikasi klaster Amazon Redshift DataZone lingkungan Amazon Anda, klik kanan dan pilih Buat koneksi.
2. Pilih Kredensyal sementara menggunakan identitas IAM Anda untuk otentikasi.
3. Jika metode otentikasi di atas tidak tersedia, buka Pengaturan akun dengan memilih tombol roda gigi di sudut kiri bawah, pilih Otentikasi dengan kredensi IAM dan simpan. Ini adalah one-time-only pengaturan.
4. Berikan nama database DataZone lingkungan Amazon untuk membuat koneksi.
5. Pilih Buat koneksi.

Sekarang Anda dapat mulai melakukan kueri terhadap tabel dan tampilan dalam klaster Amazon Redshift atau grup kerja Amazon Redshift Tanpa Server yang dikonfigurasi untuk lingkungan Amazon Anda. DataZone

Tabel atau tampilan Amazon Redshift apa pun yang Anda berlangganan ditautkan ke cluster Amazon Redshift atau grup kerja Amazon Redshift Tanpa Server yang dikonfigurasi untuk lingkungan. Anda dapat berlangganan tabel dan tampilan serta mempublikasikan tabel dan tampilan baru apa pun yang Anda buat di cluster atau database lingkungan Anda.

Sebagai contoh, mari kita ambil skenario di mana lingkungan ditautkan ke cluster Amazon Redshift yang dipanggil `redshift-cluster-1` dan database yang dipanggil `dev` dalam cluster itu. Menggunakan portal DataZone data Amazon, Anda dapat menanyakan tabel dan tampilan yang ditambahkan ke lingkungan Anda. Di bawah `Analytics tools` bagian di panel sisi kanan portal data, Anda dapat memilih tautan Amazon Redshift untuk lingkungan ini, yang membuka editor kueri. Anda kemudian dapat mengklik kanan pada `redshift-cluster-1` cluster dan membuat koneksi menggunakan kredensi Sementara menggunakan identitas IAM Anda. Setelah koneksi dibuat, Anda

dapat melihat semua tabel dan tampilan yang dapat diakses lingkungan Anda di bawah database dev.

Bekerja dengan DataZone acara dan notifikasi Amazon

Amazon DataZone memberi Anda informasi tentang aktivitas penting dalam portal data Anda, seperti permintaan berlangganan, pembaruan, komentar, dan peristiwa sistem. Amazon DataZone memberi Anda informasi ini dengan mengirimkan pesan di kotak masuk khusus di portal data atau melalui bus EventBridge default Amazon.

Topik

Bekerja dengan acara melalui kotak masuk khusus di portal DataZone data Amazon

Amazon DataZone menyediakan kotak masuk khusus di portal data tempat Anda dapat melihat dan mengambil tindakan atas pesan Anda. Pesan terbaru juga muncul di halaman rumah, halaman proyek, dan halaman katalog. Misalnya, jika pengguna meminta akses ke aset data, pemilik proyek penerbitan dan kontributor aset tersebut melihat permintaan di portal data dan setelah tindakan diambil, anggota proyek proyek berlangganan yang terkait dengan permintaan ini melihat pemberitahuan di portal data. Ada dua jenis pesan:

- Tugas - pesan-pesan ini menginformasikan penerima bahwa ada tindakan yang diperlukan di suatu tempat. Mereka memiliki bidang status opsional yang dapat Anda gunakan untuk melacak.
- Acara - pesan-pesan ini bersifat informasi dan tidak memiliki status yang ditetapkan. Acara menyediakan jejak audit pembaruan terbaru.

Di Amazon DataZone, pesan dibuat untuk jenis acara berikut:

Kategori acara	Nama peristiwa	Deskripsi acara	Jenis peristiwa
Langganan	Permintaan berlangganan dibuat	Acara dihasilkan saat permintaan berlangganan dibuat	Tugas

Kategori acara	Nama peristiwa	Deskripsi acara	Jenis peristiwa
Langganan	Permintaan berlangganan diterima	Acara dihasilkan saat permintaan berlangganan diterima	Peristiwa
Langganan	Permintaan berlangganan ditolak	Peristiwa dihasilkan saat permintaan berlangganan ditolak	Peristiwa
Langganan	Permintaan langganan dihapus	Peristiwa dihasilkan saat permintaan langganan dihapus	Peristiwa
Proyek	Pembuatan proyek berhasil	Acara dihasilkan saat pembuatan proyek berhasil	Peristiwa
Keanggotaan proyek	Penambahan anggota proyek berhasil	Acara dihasilkan ketika anggota baru ditambahkan ke proyek	Peristiwa
Keanggotaan proyek	Penghapusan anggota proyek berhasil	Peristiwa dihasilkan ketika anggota dihapus ke proyek	Peristiwa
Keanggotaan proyek	Perubahan peran anggota proyek berhasil	Peristiwa dihasilkan peran anggota dalam proyek diubah	Peristiwa
Environment	Penyebaran lingkungan dimulai	Peristiwa dihasilkan saat penerapan lingkungan dimulai	Peristiwa
Environment	Penyebaran lingkungan selesai	Peristiwa dihasilkan ketika penerapan lingkungan berhasil diselesaikan	Peristiwa

Kategori acara	Nama peristiwa	Deskripsi acara	Jenis peristiwa
Environment	Penerapan lingkungan gagal	Peristiwa dihasilkan saat penerapan lingkungan gagal	Peristiwa
Environment	Alur kerja kustom penerapan lingkungan dimulai	Peristiwa dihasilkan ketika lingkungan dengan alur kerja khusus dimulai	Peristiwa
Aset data	Aset ditambahkan ke inventaris	Peristiwa dihasilkan ketika aset data baru ditambahkan ke inventaris yaitu ditambahkan ke katalog dalam keadaan draf	Peristiwa
Aset data	Aset diterbitkan	Peristiwa dihasilkan ketika aset data baru diterbitkan yaitu tersedia untuk berlangganan	Peristiwa
Aset data	Skema aset berubah	Peristiwa dihasilkan ketika skema aset telah berubah sejak pekerjaan konsumsi sebelumnya	Peristiwa
Berlangganan	Langganan dibuat	Peristiwa dihasilkan ketika seseorang meminta untuk berlangganan aset data	Tugas

Kategori acara	Nama peristiwa	Deskripsi acara	Jenis peristiwa
Berlangganan	Langganan disetujui	Acara dihasilkan ketika langganan disetujui oleh pemilik proyek atau kontributor penerbitan	Peristiwa
Berlangganan	Langganan ditolak	Peristiwa dihasilkan ketika langganan ditolak oleh pemilik proyek atau kontributor penerbitan	Peristiwa
Berlangganan	Langganan dihapus	Acara dihasilkan saat langganan dibatalkan oleh pelanggan	Peristiwa
Berlangganan	Hibah berlangganan diminta	Peristiwa dihasilkan ketika seseorang meminta akses ke aset	Peristiwa
Berlangganan	Hibah berlangganan selesai	Peristiwa dihasilkan ketika langganan diberikan akses ke aset oleh pemilik proyek atau kontributor penerbitan	Peristiwa
Berlangganan	Pemberian langganan gagal	Peristiwa dihasilkan saat hibah langganan gagal	Peristiwa

Kategori acara	Nama peristiwa	Deskripsi acara	Jenis peristiwa
Berlangganan	Pencabutan hibah langganan diminta	Peristiwa dihasilkan ketika hibah langganan yang dicabut dimulai oleh pemilik proyek atau kontributor penerbitan	Peristiwa
Berlangganan	Pencabutan hibah langganan selesai	Acara dihasilkan saat pencabutan hibah langganan selesai	Peristiwa
Berlangganan	Pencabutan hibah langganan gagal	Peristiwa dihasilkan saat pencabutan hibah langganan gagal	Peristiwa
Pembuatan nama bisnis otomatis	Nama bisnis yang dihasilkan berhasil	Acara dihasilkan ketika pekerjaan yang dihasilkan nama bisnis otomatis selesai dengan sukses	Peristiwa
Pembuatan nama bisnis otomatis	Nama bisnis yang dihasilkan gagal	Peristiwa dihasilkan ketika pekerjaan yang dihasilkan nama bisnis otomatis gagal	Peristiwa
Sumber data dijalankan	Sumber data dibuat	Peristiwa dihasilkan saat sumber data baru dibuat	Peristiwa
Sumber data dijalankan	Sumber data diperbarui	Peristiwa dihasilkan ketika sumber data yang ada diperbarui	Peristiwa

Kategori acara	Nama peristiwa	Deskripsi acara	Jenis peristiwa
Sumber data dijalankan	Sumber data berjalan dipicu	Peristiwa dihasilkan saat menjalankan sumber data dimulai	Peristiwa
Sumber data dijalankan	Sumber data berjalan berhasil	Peristiwa dihasilkan ketika sumber data berjalan berhasil	Peristiwa
Sumber data dijalankan	Sumber data berjalan gagal	Peristiwa dihasilkan ketika sumber data berjalan gagal	Peristiwa

Untuk melihat tugas di kotak masuk portal data Anda, selesaikan langkah-langkah berikut:

1. Arahkan ke portal DataZone data Amazon menggunakan URL portal data dan masuk menggunakan SSO atau AWS kredenal Anda. Jika Anda DataZone administrator Amazon, Anda dapat memperoleh URL portal data dengan mengakses DataZone konsol Amazon di https://console.aws.amazon.com/datazone di AWS akun tempat DataZone domain Amazon dibuat.
2. Di portal data, untuk melihat pop up dengan serangkaian tugas terbaru, pilih ikon lonceng di sebelah bilah Pencarian.
3. Pilih Lihat semua untuk melihat semua tugas. Anda dapat mengubah tampilan dan melihat semua acara dengan memilih tab Acara.
4. Anda dapat memfilter pencarian berdasarkan subjek acara, status aktif atau tidak aktif, atau rentang tanggal.
5. Pilih tugas individual apa pun untuk menavigasi ke lokasi di mana Anda dapat menanggapi tugas tersebut.

Untuk melihat peristiwa di kotak masuk portal data Anda, selesaikan langkah-langkah berikut:

1. Arahkan ke portal DataZone data Amazon menggunakan URL portal data dan masuk menggunakan SSO atau AWS kredenal Anda. Jika Anda seorang DataZone administrator Amazon, Anda dapat memperoleh URL portal data dengan mengakses DataZone konsol Amazon di https://console.aws.amazon.com/datazone di AWS akun tempat domain DataZone root Amazon dibuat.

2. Di portal data, untuk melihat pop up untuk rangkaian acara terbaru, pilih ikon lonceng di sebelah bilah Pencarian.
3. Pilih Lihat semua untuk melihat semua acara. Anda dapat mengubah tampilan dan melihat semua tugas dengan memilih tab Tugas.
4. Filter pencarian berdasarkan subjek acara atau rentang tanggal.
5. Pilih acara individual apa pun untuk menavigasi ke lokasi tempat Anda dapat melihat detail tentang acara tersebut.

Bekerja dengan acara melalui bus EventBridge default Amazon

Selain mengirim pesan ke kotak masuk khusus Anda di portal data, kirim DataZone juga pesan-pesan ini ke bus acara EventBridge default Amazon Anda di AWS akun yang sama tempat domain DataZone root Amazon Anda di-host. Ini memungkinkan otomatisasi berbasis peristiwa, seperti pemenuhan langganan atau integrasi khusus dengan alat lain. Anda dapat membuat aturan yang cocok dengan EventBridge peristiwa Amazon yang masuk dan mengirimkannya ke EventBridge target Amazon untuk diproses. Aturan tunggal dapat mengirim acara ke beberapa target, yang kemudian dapat berjalan secara paralel.

Berikut contoh acara:


```
{
  "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"
        }
      ]
    }
  }
}
```

Daftar lengkap tipe detail yang didukung oleh Amazon meliputi: DataZone

- Permintaan Langganan Dibuat
- Permintaan Berlangganan Diterima
- Permintaan Langganan Ditolak
- Permintaan Langganan Dihapus
- Hibah Berlangganan Diminta
- Hibah Berlangganan Selesai
- Hibah Berlangganan Gagal
- Pencabutan Hibah Berlangganan Diminta
- Pencabutan Hibah Berlangganan Selesai
- Pencabutan Hibah Berlangganan Gagal
- Aset Ditambahkan Ke Inventaris
- Aset Ditambahkan Ke Katalog

- Skema Aset Berubah
- Perubahan Status Sumber Data
- Sumber Data Dibuat
- Sumber Data Diperbarui
- Jalankan Sumber Data Dipicu
- Jalankan Sumber Data Berhasil
- Jalankan Sumber Data Gagal
- Pembuatan Domain Berhasil
- Pembuatan Domain Gagal
- Penghapusan Domain Berhasil
- Penghapusan Domain Gagal
- Penyebaran Lingkungan Dimulai
- Penyebaran Lingkungan Selesai
- Penerapan Lingkungan Gagal
- Penghapusan Lingkungan Dimulai
- Penghapusan Lingkungan Selesai
- Penghapusan Lingkungan Gagal
- Pembuatan Proyek Berhasil
- Penambahan Anggota Proyek Berhasil
- Penghapusan Anggota Proyek Berhasil
- Perubahan Peran Anggota Proyek Berhasil
- Penyebaran Lingkungan Alur Kerja Pelanggan Dimulai
- Generasi Nama Bisnis Berhasil
- Generasi Nama Bisnis Gagal

Untuk informasi selengkapnya, lihat Amazon EventBridge.

Keamanan di Amazon DataZone

Keamanan cloud di AWS adalah prioritas tertinggi. Sebagai AWS pelanggan, Anda mendapat manfaat dari pusat data dan arsitektur jaringan yang dibangun untuk memenuhi persyaratan organisasi yang paling sensitif terhadap keamanan.

Keamanan adalah tanggung jawab bersama antara Anda AWS dan Anda. Model tanggung jawab bersama menjelaskan hal ini sebagai keamanan cloud dan keamanan dalam cloud:

- Keamanan cloud — AWS bertanggung jawab untuk melindungi infrastruktur yang menjalankan AWS layanan di AWS Cloud. AWS juga memberi Anda layanan yang dapat Anda gunakan dengan aman. Auditor pihak ketiga secara teratur menguji dan memverifikasi efektivitas keamanan kami sebagai bagian dari Program AWS Kepatuhan Program AWS Kepatuhan . Untuk mempelajari tentang program kepatuhan yang berlaku untuk Amazon DataZone, lihat AWS Layanan dalam Lingkup berdasarkan AWS Layanan Program Kepatuhan .
- Keamanan di cloud — Tanggung jawab Anda ditentukan oleh AWS layanan yang Anda gunakan. Anda juga bertanggung jawab atas faktor lain, yang mencakup sensitivitas data Anda, persyaratan perusahaan Anda, serta undang-undang dan peraturan yang berlaku.

Dokumentasi ini membantu Anda memahami cara menerapkan model tanggung jawab bersama saat menggunakan Amazon DataZone. Topik berikut menunjukkan cara mengonfigurasi Amazon DataZone untuk memenuhi tujuan keamanan dan kepatuhan Anda. Anda juga mempelajari cara menggunakan AWS layanan lain yang membantu Anda memantau dan mengamankan DataZone sumber daya Amazon Anda.

Topik

- Analisis konfigurasi dan kerentanan untuk Amazon DataZone

Perlindungan data di Amazon DataZone

Model tanggung jawab AWS bersama model berlaku untuk perlindungan data di Amazon DataZone. Seperti yang dijelaskan dalam model AWS ini, bertanggung jawab untuk melindungi infrastruktur global yang menjalankan semua AWS Cloud. Anda bertanggung jawab untuk mempertahankan kendali atas konten yang di-host pada infrastruktur ini. Anda juga bertanggung jawab atas tugas-tugas konfigurasi dan manajemen keamanan untuk Layanan AWS yang Anda gunakan. Lihat informasi yang lebih lengkap tentang privasi data dalam Pertanyaan Umum Privasi Data. Lihat informasi tentang perlindungan data di Eropa di pos blog Model Tanggung Jawab Bersama dan GDPR AWS di Blog Keamanan AWS .

Untuk tujuan perlindungan data, kami menyarankan Anda melindungi Akun AWS kredensil dan mengatur pengguna individu dengan AWS IAM Identity Center atau AWS Identity and Access Management (IAM). Dengan cara itu, setiap pengguna hanya diberi izin yang diperlukan untuk memenuhi tanggung jawab tugasnya. Kami juga menyarankan supaya Anda mengamankan data dengan cara-cara berikut:

- Gunakan autentikasi multi-faktor (MFA) pada setiap akun.
- Gunakan SSL/TLS untuk berkomunikasi dengan sumber daya. AWS Kami mensyaratkan TLS 1.2 dan menganjurkan TLS 1.3.
- Siapkan API dan pencatatan aktivitas pengguna dengan AWS CloudTrail.
- Gunakan solusi AWS enkripsi, bersama dengan semua kontrol keamanan default di dalamnya Layanan AWS.
- Gunakan layanan keamanan terkelola lanjut seperti Amazon Macie, yang membantu menemukan dan mengamankan data sensitif yang disimpan di Amazon S3.
- Jika Anda memerlukan modul kriptografi tervalidasi FIPS 140-2 saat mengakses AWS melalui antarmuka baris perintah atau API, gunakan titik akhir FIPS. Lihat informasi yang lebih lengkap tentang titik akhir FIPS yang tersedia di Standar Pemrosesan Informasi Federal (FIPS) 140-2.

Kami sangat merekomendasikan agar Anda tidak pernah memasukkan informasi identifikasi yang sensitif, seperti nomor rekening pelanggan Anda, ke dalam tanda atau bidang isian bebas seperti bidang Nama. Ini termasuk saat Anda bekerja dengan Amazon DataZone atau lainnya Layanan AWS menggunakan konsol, API AWS CLI, atau AWS SDK. Data apa pun yang Anda masukkan ke dalam tanda atau bidang isian bebas yang digunakan untuk nama dapat digunakan untuk log penagihan

atau log diagnostik. Saat Anda memberikan URL ke server eksternal, kami sangat menganjurkan supaya Anda tidak menyertakan informasi kredensial di dalam URL untuk memvalidasi permintaan Anda ke server itu.

Enkripsi data

Saat memberikan izin, Anda memutuskan siapa yang mendapatkan izin apa untuk sumber daya Amazon mana. DataZone Anda mengaktifkan tindakan tertentu yang ingin Anda izinkan pada sumber daya tersebut. Oleh karena itu, Anda harus memberikan hanya izin yang diperlukan untuk melakukan tugas. Menerapkan akses hak akses paling rendah adalah hal mendasar dalam mengurangi risiko keamanan dan dampak yang dapat diakibatkan oleh kesalahan atau niat jahat.

Enkripsi diam

Amazon DataZone mengenkripsi semua data Anda secara default dengan kunci Layanan Manajemen AWS Kunci (AWS KMS) yang AWS memiliki dan mengelola untuk Anda. Anda juga dapat mengenkripsi data yang disimpan dalam DataZone katalog Amazon menggunakan kunci yang Anda kelola dengan AWS KMS.

Saat membuat domain di Amazon DataZone, Anda dapat menyediakan pengaturan enkripsi dengan memilih kotak centang di samping Sesuaikan pengaturan enkripsi (lanjutan) di bawah Enkripsi Data, dan menyediakan kunci KMS.

Enkripsi bergerak

Amazon DataZone menggunakan Transport Layer Security (TLS) dan enkripsi sisi klien untuk enkripsi dalam perjalanan. Komunikasi dengan Amazon selalu DataZone dilakukan melalui HTTPS sehingga data Anda selalu dienkripsi saat transit.

Privasi lalu lintas antar jaringan

Untuk mengamankan koneksi antar akun, Amazon DataZone menggunakan peran layanan dan peran IAM untuk terhubung dengan aman ke akun pelanggan dan menjalankan operasi atas nama pelanggan.

Topik

- Enkripsi data saat istirahat untuk Amazon DataZone
- Menggunakan Endpoint VPC Antarmuka untuk Amazon DataZone

Enkripsi data saat istirahat untuk Amazon DataZone

Enkripsi data saat istirahat secara default membantu mengurangi overhead operasional dan kompleksitas yang terlibat dalam melindungi data sensitif. Pada saat yang sama, ini memungkinkan Anda untuk membangun aplikasi aman yang memenuhi kepatuhan enkripsi yang ketat dan persyaratan peraturan.

Amazon DataZone menggunakan kunci yang AWS dimiliki default untuk mengenkripsi data Anda secara otomatis saat istirahat. Anda tidak dapat melihat, mengelola, atau mengaudit penggunaan kunci yang AWS dimiliki. Untuk informasi selengkapnya, lihat kunci AWS yang dimiliki.

Meskipun Anda tidak dapat menonaktifkan lapisan enkripsi ini atau memilih jenis enkripsi alternatif, Anda dapat menambahkan lapisan enkripsi kedua di atas kunci enkripsi yang ada AWS dengan memilih kunci yang dikelola pelanggan saat Anda membuat domain Amazon DataZone . Amazon DataZone mendukung penggunaan kunci terkelola pelanggan simetris yang dapat Anda buat, miliki, dan kelola untuk menambahkan lapisan enkripsi kedua di atas enkripsi yang AWS dimiliki yang ada. Karena Anda memiliki kendali penuh atas lapisan enkripsi ini, di dalamnya Anda dapat melakukan tugas-tugas berikut:

- Menetapkan dan memelihara kebijakan utama
- Menetapkan dan memelihara kebijakan dan hibah IAM
- Mengaktifkan dan menonaktifkan kebijakan utama
- Putar bahan kriptografi kunci
- Tambahkan tag
- Buat alias kunci
- Kunci jadwal untuk penghapusan

Untuk informasi selengkapnya, lihat Kunci terkelola pelanggan.

> **Note**
>
> Amazon DataZone secara otomatis mengaktifkan enkripsi saat istirahat menggunakan kunci yang AWS dimiliki untuk melindungi data pelanggan tanpa biaya.
> AWS Biaya KMS berlaku untuk menggunakan kunci yang dikelola pelanggan. Untuk informasi selengkapnya tentang harga, lihat Harga Layanan Manajemen AWS Utama.

Bagaimana Amazon DataZone menggunakan hibah di KMS AWS

Amazon DataZone membutuhkan tiga hibah untuk menggunakan kunci yang dikelola pelanggan Anda. Saat Anda membuat DataZone domain Amazon yang dienkripsi dengan kunci yang dikelola pelanggan, Amazon DataZone membuat hibah dan sub-hibah atas nama Anda dengan mengirimkan permintaan ke KMS. CreateGrant AWS Hibah di AWS KMS digunakan untuk memberi Amazon DataZone akses ke kunci KMS di akun Anda. Amazon DataZone membuat hibah berikut untuk menggunakan kunci terkelola pelanggan Anda untuk operasi internal berikut:

Satu hibah untuk mengenkripsi data Anda saat istirahat untuk operasi berikut:

- Kirim DescribeKeypermintaan ke AWS KMS untuk memverifikasi bahwa ID kunci KMS yang dikelola pelanggan simetris yang dimasukkan saat membuat koleksi DataZone domain Amazon valid.
- Kirim GenerateDataKeyrequestske AWS KMS untuk menghasilkan kunci data yang dienkripsi oleh kunci yang dikelola pelanggan Anda.
- Kirim permintaan Dekripsi ke AWS KMS untuk mendekripsi kunci data terenkripsi sehingga mereka dapat digunakan untuk mengenkripsi data Anda.
- RetireGrantuntuk menghentikan hibah saat domain dihapus.

Dua hibah untuk pencarian dan penemuan data Anda:

- Hibah 2:
  - DescribeKey
  - GenerateDataKey
  - Enkripsi, Dekripsi, ReEncrypt
  - CreateGrantuntuk membuat hibah anak untuk AWS layanan yang digunakan secara internal oleh. DataZone
  - RetireGrant
- Hibah 3:
  - GenerateDataKey
  - Dekripsi
  - RetireGrant

Anda dapat mencabut akses ke hibah, atau menghapus akses layanan ke kunci yang dikelola pelanggan kapan saja. Jika Anda melakukannya, Amazon DataZone tidak akan dapat mengakses data apa pun yang dienkripsi oleh kunci yang dikelola pelanggan, yang memengaruhi operasi yang bergantung pada data tersebut. Misalnya, jika Anda mencoba mendapatkan detail Aset Data yang tidak DataZone dapat diakses Amazon, maka operasi akan mengembalikan `AccessDeniedException` kesalahan.

Buat kunci terkelola pelanggan

Anda dapat membuat kunci terkelola pelanggan simetris dengan menggunakan AWS Management Console, atau AWS KMS API.

Untuk membuat kunci terkelola pelanggan simetris, ikuti langkah-langkah untuk Membuat kunci terkelola pelanggan simetris di Panduan Pengembang Layanan Manajemen AWS Kunci.

Kebijakan utama - kebijakan utama mengontrol akses ke kunci yang dikelola pelanggan Anda. Setiap kunci yang dikelola pelanggan harus memiliki persis satu kebijakan utama, yang berisi pernyataan yang menentukan siapa yang dapat menggunakan kunci dan bagaimana mereka dapat menggunakannya. Saat membuat kunci terkelola pelanggan, Anda dapat menentukan kebijakan kunci. Untuk informasi selengkapnya, lihat Mengelola akses ke kunci yang dikelola pelanggan di Panduan Pengembang Layanan Manajemen AWS Kunci.

Untuk menggunakan kunci terkelola pelanggan dengan DataZone sumber daya Amazon Anda, operasi API berikut harus diizinkan dalam kebijakan kunci:

- kms: CreateGrant — menambahkan hibah ke kunci yang dikelola pelanggan. Memberikan akses kontrol ke kunci KMS tertentu, yang memungkinkan akses ke operasi hibah yang dibutuhkan Amazon DataZone . Untuk informasi selengkapnya tentang Menggunakan Hibah, lihat Panduan Pengembang Layanan Manajemen AWS Utama.
- kms: DescribeKey — menyediakan detail kunci yang dikelola pelanggan untuk memungkinkan Amazon DataZone memvalidasi kunci.
- kms: GenerateDataKey — mengembalikan kunci data simetris yang unik untuk digunakan di luar KMS. AWS
- KMS: Decrypt — mendekripsi ciphertext yang dienkripsi oleh kunci KMS.

Berikut ini adalah contoh pernyataan kebijakan yang dapat Anda tambahkan untuk Amazon 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**
>
> Tolak kebijakan KMS tidak diterapkan untuk sumber daya yang diakses melalui portal DataZone data Amazon.

Untuk informasi selengkapnya tentang menentukan izin dalam kebijakan, lihat Panduan Pengembang Layanan Manajemen AWS Kunci.

Untuk informasi selengkapnya tentang akses kunci pemecahan masalah, lihat Panduan Pengembang Layanan Manajemen AWS Kunci.

Menentukan kunci yang dikelola pelanggan untuk Amazon DataZone

Konteks DataZone enkripsi Amazon

Konteks enkripsi adalah kumpulan opsional pasangan kunci-nilai yang berisi informasi kontekstual tambahan tentang data.

AWS KMS menggunakan konteks enkripsi sebagai data otentikasi tambahan untuk mendukung enkripsi yang diautentikasi. Saat Anda menyertakan konteks enkripsi dalam permintaan untuk

mengenkripsi data, AWS KMS mengikat konteks enkripsi ke data terenkripsi. Untuk mendekripsi data, Anda menyertakan konteks enkripsi yang sama dalam permintaan.

Amazon DataZone menggunakan konteks enkripsi berikut:

```
"encryptionContextSubset": {
    "aws:datazone:domainId": "{root-domain-uuid}"
}
```

Menggunakan konteks enkripsi untuk pemantauan - saat Anda menggunakan kunci terkelola pelanggan simetris untuk mengenkripsi Amazon DataZone, Anda juga dapat menggunakan konteks enkripsi dalam catatan audit dan log untuk mengidentifikasi bagaimana kunci yang dikelola pelanggan digunakan. Konteks enkripsi juga muncul di log yang dihasilkan oleh AWS CloudTrail atau Amazon CloudWatch Logs.

Menggunakan konteks enkripsi untuk mengontrol akses ke kunci terkelola pelanggan Anda - Anda dapat menggunakan konteks enkripsi dalam kebijakan utama dan kebijakan IAM sebagai kondisi untuk mengontrol akses ke kunci terkelola pelanggan simetris Anda. Anda juga dapat menggunakan kendala konteks enkripsi dalam hibah.

Amazon DataZone menggunakan batasan konteks enkripsi dalam hibah untuk mengontrol akses ke kunci yang dikelola pelanggan di akun atau wilayah Anda. Batasan hibah mengharuskan operasi yang diizinkan oleh hibah menggunakan konteks enkripsi yang ditentukan.

Berikut ini adalah contoh pernyataan kebijakan kunci untuk memberikan akses ke kunci yang dikelola pelanggan untuk konteks enkripsi tertentu. Kondisi dalam pernyataan kebijakan ini mengharuskan hibah memiliki batasan konteks enkripsi yang menentukan konteks enkripsi.

```
{
    "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}"
        }
    }
}
```

Memantau kunci enkripsi Anda untuk Amazon DataZone

Saat Anda menggunakan kunci terkelola pelanggan AWS KMS dengan DataZone sumber daya Amazon Anda, Anda dapat menggunakannya AWS CloudTrailuntuk melacak permintaan yang DataZone dikirimkan Amazon ke AWS KMS. Contoh berikut adalah AWS CloudTrail peristiwa untuk`CreateGrant`,, `GenerateDataKeyDecrypt`, dan `DescribeKey` untuk memantau operasi KMS yang dipanggil oleh Amazon DataZone untuk mengakses data yang dienkripsi oleh kunci yang dikelola pelanggan Anda. Saat Anda menggunakan kunci yang dikelola pelanggan AWS KMS untuk mengenkripsi DataZone domain Amazon Anda, Amazon DataZone mengirimkan `CreateGrant` permintaan atas nama Anda untuk mengakses kunci KMS di akun Anda. AWS Hibah yang DataZone dibuat Amazon khusus untuk sumber daya yang terkait dengan kunci yang dikelola pelanggan AWS KMS. Selain itu, Amazon DataZone menggunakan `RetireGrant` operasi untuk menghapus hibah saat Anda menghapus domain. Contoh peristiwa berikut mencatat `CreateGrant` operasi:

```
{
    "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"
}
```

Membuat lingkungan Data Lake yang melibatkan katalog Glue terenkripsi AWS

Dalam kasus penggunaan lanjutan, saat Anda bekerja dengan katalog AWS Glue yang dienkripsi, Anda harus memberikan akses ke DataZone layanan Amazon untuk menggunakan kunci KMS yang dikelola pelanggan Anda. Anda dapat melakukan ini dengan memperbarui kebijakan KMS kustom Anda dan menambahkan tag ke kunci. Untuk memberikan akses ke DataZone layanan Amazon agar bekerja dengan data dalam katalog AWS Glue terenkripsi, lengkapi yang berikut ini:

- Tambahkan kebijakan berikut ke kunci KMS kustom Anda. Untuk informasi selengkapnya, lihat Mengubah kebijakan utama.

```
{
  "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*"
    }
  }
}
```

- Tambahkan tag berikut ke kunci KMS kustom Anda. Untuk informasi selengkapnya, lihat Menggunakan tag untuk mengontrol akses ke kunci KMS.

```
key: AmazonDataZoneEnvironment
value: all
```

Menggunakan Endpoint VPC Antarmuka untuk Amazon DataZone

Jika Anda menggunakan Amazon Virtual Private Cloud (Amazon VPC) untuk meng-host AWS sumber daya Anda, Anda dapat membuat koneksi antara Amazon VPC dan Amazon. DataZone Anda dapat menggunakan koneksi ini dengan Amazon DataZone tanpa melintasi internet publik.

Amazon VPC memungkinkan Anda meluncurkan AWS sumber daya di jaringan virtual khusus. Anda dapat menggunakan VPC untuk mengendalikan pengaturan jaringan, seperti rentang alamat IP, subnet, tabel rute, dan gateway jaringan. Untuk informasi lebih lanjut tentang Amazon VPC, lihat Panduan Pengguna Amazon VPC.

Untuk menghubungkan VPC Amazon Anda ke Amazon DataZone, Anda harus terlebih dahulu menentukan titik akhir VPC antarmuka, yang memungkinkan Anda menghubungkan VPC Anda ke layanan lain. AWS Titik akhir memberikan konektivitas yang dapat andal, dapat diskalakan, tanpa memerlukan gateway internet, instans terjemahan alamat jaringan (NAT), atau koneksi VPN. Untuk informasi selengkapnya dan langkah-langkah mendetail tentang cara membuat titik akhir VPC, lihat Titik Akhir VPC Antarmuka () di AWS PrivateLink Panduan Pengguna Amazon VPC.

> **Important**
>
> Di VPC, kebijakan endpoint adalah kebijakan berbasis sumber daya yang dapat Anda lampirkan ke titik akhir VPC untuk mengontrol prinsip mana AWS yang dapat menggunakan titik akhir untuk mengakses layanan. AWS

Dalam rilis Amazon saat ini DataZone, penggunaan kebijakan endpoint tidak didukung untuk membuat dan menggunakan koneksi antara Amazon VPC dan Amazon Anda. DataZone Manajemen DataZone akses Amazon bergantung pada konfigurasi RAM dan kebijakan utama IAM yang ditentukan pada tingkat layanan.

Otorisasi di Amazon DataZone

Antarmuka DataZone Amazon terdiri dari konsol manajemen di dalam AWS dan aplikasi web off-console (portal data).

Konsol DataZone manajemen Amazon dapat digunakan oleh AWS administrator untuk top-level-resource API, termasuk membuat dan mengelola domain, asosiasi AWS akun untuk domain ini, dan sumber data yang ingin Anda delegasikan manajemen aksesnya ke Amazon. DataZone Anda dapat menggunakan konsol DataZone manajemen Amazon untuk mengelola semua peran dan konfigurasi IAM yang diperlukan untuk mendelegasikan kontrol manajemen akses ke DataZone layanan Amazon untuk akun yang dikonfigurasi secara eksplisit. AWS Portal DataZone data Amazon adalah aplikasi Pusat AWS Identitas pihak pertama untuk pengguna SSO. Jika diaktifkan, konsol juga dapat digunakan oleh prinsipal IAM resmi untuk bergabung ke portal data alih-alih menggunakan identitas SSO.

Portal data DataZone Amazon dirancang untuk digunakan terutama oleh pengguna yang diautentikasi AWS IAM Identity Center untuk mengelola akses ke data dan melakukan tugas penerbitan data, penemuan, berlangganan, dan analitik.

Otorisasi di konsol Amazon DataZone

Model otorisasi DataZone konsol Amazon menggunakan otorisasi IAM. Konsol digunakan oleh administrator terutama untuk pengaturan. Amazon DataZone menggunakan konsep AWS akun administrator domain, dan AWS akun anggota, dan konsol digunakan dari semua akun ini untuk membangun hubungan kepercayaan sambil menghormati batasan AWS Organisasi.

Otorisasi di portal Amazon DataZone

Model otorisasi portal DataZone data Amazon adalah ACL hierarkis dengan arketipe peran statis (profil) yang mencakup administrator dan pemirsa. Misalnya, pengguna dapat memiliki profil administrator atau pengguna. Pada tingkat domain, mereka mungkin memiliki penunjukan pengguna domain pemilik data. Pada tingkat proyek, pengguna dapat menjadi pemilik atau kontributor. Profil

ini dapat dikonfigurasi sebagai salah satu dari dua jenis: pengguna dan grup. Profil ini kemudian dikaitkan dengan domain dan proyek, dan status untuk izin ini disimpan dalam tabel asosiasi.

Dalam model otorisasi ini, Amazon DataZone memungkinkan pengguna untuk mengelola izin pengguna dan grup. Pengguna mengelola keanggotaan proyek, meminta keanggotaan proyek, dan menyetujui keanggotaan. Pengguna mempublikasikan data, menentukan persetujuan langganan data, berlangganan data, dan menyetujui langganan.

Pengguna melakukan analisis data dalam proyek tertentu ketika klien portal data mereka meminta kredensional sesi IAM yang DataZone dihasilkan Amazon berdasarkan profil efektif pengguna dalam konteks proyek tertentu. Sesi ini mencakup izin pengguna dan juga sumber daya proyek tertentu. Pengguna kemudian mampir ke Athena atau Redshift untuk menanyakan data yang relevan, dan semua pekerjaan IAM yang mendasarinya sepenuhnya diabstraksikan.

DataZone Profil dan peran Amazon

Setelah pengguna diautentikasi, konteks yang diautentikasi akan dipetakan ke ID profil pengguna. Profil pengguna ini dapat memiliki beberapa asosiasi yang berbeda (pemilik proyek, administrator domain, dll.) Yang digunakan untuk mengotorisasi pengguna. Setiap asosiasi (misalnya, pemilik proyek, administrator domain, dll.) memiliki izin untuk aktivitas tertentu berdasarkan konteksnya. Misalnya, pengguna yang memiliki asosiasi admin domain dapat membuat domain tambahan, dapat menetapkan administrator domain lain ke domain, dan dapat membuat templat proyek dalam domain mereka. Pemilik proyek dapat menambah atau menghapus anggota proyek untuk proyek mereka, mereka dapat membuat perjanjian penerbitan dengan domain, dan mempublikasikan aset ke domain.

Mengontrol akses ke DataZone sumber daya Amazon menggunakan IAM

Anda perlu AWS Identity and Access Management (IAM) untuk menyelesaikan tugas-tugas terkait keamanan berikut:

- Buat pengguna dan grup di bawah Anda Akun AWS.
- Tetapkan kredensi keamanan unik untuk setiap pengguna di bawah Anda. Akun AWS
- Kontrol izin setiap pengguna untuk melakukan tugas dengan AWS sumber daya.
- Izinkan pengguna di tempat lain Akun AWS untuk berbagi AWS sumber daya Anda.
- Buat peran untuk Anda Akun AWS dan tentukan pengguna atau layanan yang dapat mengasumsikan mereka.

- Gunakan identitas yang ada untuk perusahaan Anda untuk memberikan izin untuk melakukan tugas menggunakan sumber daya AWS

Untuk informasi selengkapnya tentang IAM, lihat berikut ini:

- AWS Identity and Access Management (IAM)
- Memulai
- Panduan Pengguna IAM

Bagian berikut menjelaskan kebijakan dan izin yang diperlukan untuk menyiapkan Amazon DataZone dan komponennya, seperti domain (termasuk domain), akun terkait, proyek, dan sumber data. Untuk informasi selengkapnya, lihat DataZone Terminologi dan konsep Amazon.

Daftar Isi

AWS kebijakan terkelola untuk Amazon DataZone

Kebijakan AWS terkelola adalah kebijakan mandiri yang dibuat dan dikelola oleh AWS. AWS Kebijakan terkelola dirancang untuk memberikan izin bagi banyak kasus penggunaan umum sehingga Anda dapat mulai menetapkan izin kepada pengguna, grup, dan peran.

Perlu diingat bahwa kebijakan AWS terkelola mungkin tidak memberikan izin hak istimewa paling sedikit untuk kasus penggunaan spesifik Anda karena tersedia untuk digunakan semua pelanggan. AWS Kami menyarankan Anda untuk mengurangi izin lebih lanjut dengan menentukan kebijakan yang dikelola pelanggan yang khusus untuk kasus penggunaan Anda.

Anda tidak dapat mengubah izin yang ditentukan dalam kebijakan AWS terkelola. Jika AWS memperbarui izin yang ditentukan dalam kebijakan AWS terkelola, pemutakhiran akan memengaruhi semua identitas utama (pengguna, grup, dan peran) yang dilampirkan kebijakan tersebut. AWS kemungkinan besar akan memperbarui kebijakan AWS terkelola saat baru Layanan AWS diluncurkan atau operasi API baru tersedia untuk layanan yang ada.

Untuk informasi selengkapnya, lihat AWS kebijakan yang dikelola dalam Panduan Pengguna IAM.

Daftar Isi

AWS kebijakan terkelola: AmazonDataZoneFullAccess

Anda dapat melampirkan kebijakan `AmazonDataZoneFullAccess` ke identitas IAM Anda.

Kebijakan ini menyediakan akses penuh ke Amazon DataZone melalui AWS Management Console.

Detail izin

Kebijakan ini mencakup izin berikut:

- `datazone`— memberikan kepala sekolah akses penuh ke Amazon melalui. DataZone AWS Management Console
- `kms`— Memungkinkan kepala sekolah untuk membuat daftar alias dan mendeskripsikan kunci.
- `s3`— Memungkinkan kepala sekolah untuk memilih yang ada atau membuat bucket S3 baru untuk menyimpan data Amazon. DataZone
- `ram`— Memungkinkan kepala sekolah untuk berbagi domain Amazon DataZone di seluruh. Akun AWS

- `iam`— Memungkinkan kepala sekolah untuk membuat daftar dan meneruskan peran dan mendapatkan kebijakan.
- `sso`— Memungkinkan kepala sekolah untuk mendapatkan wilayah di mana AWS IAM Identity Center diaktifkan.

```
{
  "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_*"
        }
      }
    }
  ]
}
```

Pertimbangan dan batasan kebijakan

Ada fungsionalitas tertentu yang tidak dicakup oleh `AmazonDataZoneFullAccess` kebijakan tersebut.

- Jika Anda membuat DataZone domain Amazon dengan AWS KMS kunci Anda sendiri, Anda harus memiliki izin agar `kms:CreateGrant` pembuatan domain berhasil, dan `kms:Decrypt` untuk`kms:GenerateDataKey`, agar kunci tersebut memanggil DataZone API Amazon lainnya seperti `listDataSources` dan. `createDataSource` Dan Anda juga harus memiliki izin untuk`kms:CreateGrant`,, `kms:Decrypt``kms:GenerateDataKey`, dan `kms:DescribeKey` dalam kebijakan sumber daya kunci itu.

  Jika Anda menggunakan kunci KMS milik layanan default, maka ini tidak diperlukan.

  Untuk informasi selengkapnya, lihat AWS Key Management Service.
- Jika Anda ingin menggunakan fungsi peran buat dan perbarui dalam DataZone konsol Amazon, Anda harus memiliki hak administrator atau memiliki izin IAM yang diperlukan

untuk membuat peran IAM dan membuat/memperbarui kebijakan. Izin yang diperlukan termasuk`iam:CreateRole`,`iam:CreatePolicy`,`iam:CreatePolicyVersion`,`iam:DeletePolicyV` dan `iam:AttachRolePolicy` izin.

- Jika Anda membuat domain baru di Amazon DataZone dengan login AWS IAM Identity Center pengguna diaktifkan, atau jika Anda mengaktifkannya untuk domain yang ada di Amazon DataZone, Anda harus memiliki izin untuk hal berikut:`sso:CreateManagedApplicationInstance`,`sso:DeleteManagedApplicationInstance`, dan`sso:PutApplicationAssignmentConfiguration`.
- Untuk menerima permintaan asosiasi AWS akun di Amazon DataZone, Anda harus memiliki `ram:AcceptResourceShareInvitation` izin.

AWS kebijakan terkelola: AmazonDataZoneFullUserAccess

Kebijakan ini memberikan akses penuh ke Amazon DataZone, tetapi kebijakan ini tidak mengizinkan pengelolaan domain, pengguna, atau akun terkait.

Detail izin

```
{
  "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 kebijakan terkelola: AmazonDataZoneCustomEnvironmentDeploymentPolicy

Anda dapat menggunakan kebijakan ini untuk memperbarui konfigurasi lingkungan yang dibuat menggunakan cetak biru kustom. Kebijakan ini juga dapat digunakan untuk membuat target DataZone langganan Amazon dan sumber data.

Detail izin

```
{
 "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 kebijakan terkelola: AmazonDataZoneEnvironmentRolePermissionsBoundary

> **Note**
>
> Kebijakan ini adalah batas izin. Batas izin menetapkan izin maksimum yang dapat diberikan oleh kebijakan berbasis identitas kepada entitas IAM. Anda tidak boleh menggunakan dan melampirkan kebijakan batas DataZone izin Amazon sendiri. Kebijakan batas DataZone izin Amazon hanya boleh dilampirkan ke peran yang dikelola Amazon DataZone . Untuk informasi selengkapnya tentang batas izin, lihat Batas izin untuk entitas IAM di Panduan Pengguna IAM.

Saat Anda membuat lingkungan melalui portal DataZone data Amazon, Amazon DataZone menerapkan batas izin ini ke peran IAM yang dihasilkan selama pembuatan lingkungan. Batas izin membatasi cakupan peran yang DataZone dibuat Amazon dan peran apa pun yang Anda tambahkan.

Amazon DataZone menggunakan kebijakan `AmazonDataZoneEnvironmentRolePermissionsBoundary` terkelola untuk membatasi prinsipal IAM yang disediakan yang dilampirkan. Prinsipal mungkin mengambil bentuk peran pengguna yang DataZone dapat diasumsikan Amazon atas nama pengguna perusahaan interaktif atau layanan analitik (misalnya)AWS Glue, dan kemudian melakukan tindakan untuk memproses data seperti membaca dan menulis dari Amazon S3 atau menjalankan. Perayap AWS Glue

`AmazonDataZoneEnvironmentRolePermissionsBoundary`Kebijakan tersebut memberikan akses baca dan tulis untuk Amazon DataZone ke layanan seperti AWS Glue, Amazon S3, Amazon Redshift AWS Lake Formation, dan Amazon Athena. Kebijakan ini juga memberikan izin baca dan tulis ke beberapa sumber daya infrastruktur yang diperlukan untuk menggunakan layanan ini seperti antarmuka jaringan dan AWS KMS kunci.

Amazon DataZone menerapkan kebijakan `AmazonDataZoneEnvironmentRolePermissionsBoundary` AWS terkelola sebagai batas izin untuk semua peran DataZone lingkungan Amazon (pemilik dan kontributor). Batas izin ini membatasi peran ini untuk hanya mengizinkan akses ke sumber daya yang diperlukan dan tindakan yang diperlukan untuk lingkungan.

Batas mencakup pernyataan JSON berikut:

```
{
  "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 kebijakan terkelola: AmazonDataZoneRedshiftGlueProvisioningPolicy

AmazonDataZoneRedshiftGlueProvisioningPolicyKebijakan ini memberi Amazon izin DataZone yang diperlukan untuk berinteraksi dengan AWS Glue dan Amazon Redshift.

```
{
 "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 kebijakan terkelola: AmazonDataZoneGlueManageAccessRolePolicy

Kebijakan ini memberikan DataZone izin Amazon untuk mempublikasikan data AWS Glue ke katalog. Ini juga memberikan DataZone izin Amazon untuk memberikan akses atau mencabut akses ke aset yang diterbitkan AWS Glue di katalog.

```
{
 "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 kebijakan terkelola: AmazonDataZoneRedshiftManageAccessRolePolicy

Kebijakan ini memberikan DataZone izin Amazon untuk mempublikasikan data Amazon Redshift ke katalog. Ini juga memberikan DataZone izin Amazon untuk memberikan akses atau mencabut akses ke Amazon Redshift atau Amazon Redshift Serverless aset yang diterbitkan dalam katalog.

```
{
 "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*"
   }
  ]
}
```

Kebijakan terkelola AWS : AmazonDataZoneCrossAccountAdmin

Anda dapat melampirkan AmazonDataZoneCrossAccountAdmin kebijakan ke identitas IAM Anda.

Kebijakan ini memungkinkan pengguna untuk bekerja dengan akun DataZone terkait Amazon.

```
{
    "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 kebijakan terkelola: AmazonDataZoneDomainExecutionRolePolicy

Ini adalah kebijakan default untuk peran DataZone `DomainExecutionRole` layanan Amazon. Peran ini digunakan oleh Amazon DataZone untuk membuat katalog, menemukan, mengatur, berbagi, dan menganalisis data dalam DataZone domain Amazon.

Anda dapat melampirkan AmazonDataZoneDomainExecutionRolePolicy kebijakan ke Anda`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 kebijakan terkelola: AmazonDataZoneSageMakerProvisioning

AmazonDataZoneSageMakerProvisioning Kebijakan ini memberi Amazon izin DataZone yang diperlukan untuk berinteraksi dengan Amazon. SageMaker

```
{
 "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 kebijakan terkelola: AmazonDataZoneSageMakerAccess

Kebijakan ini memberikan DataZone izin Amazon untuk memublikasikan SageMaker aset Amazon ke katalog. Ini juga memberikan DataZone izin Amazon untuk memberikan akses atau mencabut akses ke aset yang SageMaker diterbitkan Amazon dalam katalog.

Kebijakan ini mencakup izin untuk melakukan hal berikut:

- cloudtrail — mengambil informasi tentang jalur. CloudTrail
- cloudwatch — mengambil alarm saat ini. CloudWatch
- log — mengambil filter metrik untuk CloudWatch log.
- sns - mengambil daftar langganan ke topik SNS.
- config — mengambil informasi tentang perekam konfigurasi, sumber daya, dan aturan Config AWS . Juga memungkinkan peran terkait layanan untuk membuat dan menghapus aturan AWS Config, dan menjalankan evaluasi terhadap aturan.
- iam — dapatkan dan buat laporan kredensi untuk akun.
- organisasi — mengambil informasi akun dan unit organisasi (OU) untuk suatu organisasi.
- securityhub — mengambil informasi tentang bagaimana layanan, standar, dan kontrol Security Hub dikonfigurasi.
- tag — mengambil informasi tentang tag sumber daya.

```
{
 "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 kebijakan terkelola: AmazonDataZoneSageMakerEnvironmentRolePermissionsBoundary

> **Note**
>
> Kebijakan ini adalah batas izin. Batas izin menetapkan izin maksimum yang dapat diberikan oleh kebijakan berbasis identitas kepada entitas IAM. Anda tidak boleh menggunakan dan melampirkan kebijakan batas DataZone izin Amazon sendiri. Kebijakan batas DataZone izin Amazon hanya boleh dilampirkan ke peran yang dikelola Amazon DataZone . Untuk informasi selengkapnya tentang batas izin, lihat Batas izin untuk entitas IAM di Panduan Pengguna IAM.

Saat Anda membuat SageMaker lingkungan Amazon melalui portal DataZone data Amazon, Amazon DataZone menerapkan batas izin ini ke peran IAM yang dihasilkan selama pembuatan lingkungan. Batas izin membatasi cakupan peran yang DataZone dibuat Amazon dan peran apa pun yang Anda tambahkan.

Amazon DataZone menggunakan kebijakan `AmazonDataZoneSageMakerEnvironmentRolePermissionsBoundary` terkelola untuk membatasi prinsipal IAM yang disediakan yang dilampirkan. Prinsipal mungkin mengambil bentuk peran pengguna yang DataZone dapat diambil Amazon atas nama pengguna perusahaan interaktif atau layanan analitik (misalnya)AWS SageMaker, dan kemudian melakukan tindakan untuk

memproses data seperti membaca dan menulis dari Amazon S3 atau Amazon Redshift atau menjalankan Glue crawler. AWS

`AmazonDataZoneSageMakerEnvironmentRolePermissionsBoundary`Kebijakan tersebut memberikan akses baca dan tulis untuk Amazon DataZone ke layanan seperti Amazon SageMaker, AWS Glue, Amazon S3, Lake AWS Formation, Amazon Redshift, dan Amazon Athena. Kebijakan ini juga memberikan izin baca dan tulis ke beberapa sumber daya infrastruktur yang diperlukan untuk menggunakan layanan ini seperti antarmuka jaringan, repositori Amazon ECR, dan kunci KMS. AWS Ini juga memberikan akses ke SageMaker aplikasi Amazon seperti Amazon SageMaker Canvas.

Amazon DataZone menerapkan kebijakan `AmazonDataZoneSageMakerEnvironmentRolePermissionsBoundary` terkelola sebagai batas izin untuk semua peran DataZone lingkungan Amazon (pemilik dan kontributor). Batas izin ini membatasi peran ini untuk hanya mengizinkan akses ke sumber daya yang diperlukan dan tindakan yang diperlukan untuk lingkungan.

```
       {
"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": "*"
  }
 ]
}
```

Amazon DataZone memperbarui kebijakan AWS terkelola

Lihat detail tentang pembaruan kebijakan AWS terkelola untuk Amazon DataZone sejak layanan ini mulai melacak perubahan ini. Untuk peringatan otomatis tentang perubahan pada halaman ini, berlangganan umpan RSS di halaman riwayat DataZone Dokumen Amazon.

Perubahan	Deskripsi	Tanggal
AmazonDataZoneSageMakerEnvironmentRolePermissionsBoundary - batas izin baru	Batas izin baru disebut. AmazonDataZoneSageMakerEnvironmentRolePermissionsBoundary Saat Anda membuat SageMaker lingkungan Amazon melalui portal DataZone data Amazon, Amazon DataZone menerapkan batas izin ini ke peran	30 April 2024

Perubahan	Deskripsi	Tanggal
	IAM yang dihasilkan selama pembuatan lingkungan. Batas izin membatasi cakupan peran yang DataZone dibuat Amazon dan peran apa pun yang Anda tambahkan.	
AmazonDataZoneSage MakerAccess - kebijakan baru	Kebijakan baru yang disebut AmazonDataZoneSage MakerAccessmemberikan DataZone izin Amazon untuk mempublikasikan SageMaker aset Amazon ke katalog. Ini juga memberikan DataZone izin Amazon untuk memberika n akses atau mencabut akses ke aset yang SageMaker diterbitkan Amazon dalam katalog.	30 April 2024
AmazonDataZoneFullAccess - pembaruan kebijakan	Pembaruan AmazonDat aZoneFullAccesskebijakan yang menambahkan akses ke `DescribeSecurityGr oups` tindakan guna meningkatkan kegunaan administrator akun yang mengonfigurasi cetak biru di konsol dan `GetPolicy` tindakan untuk membantu mengambil informasi tentang kebijakan terkelola yang ditentukan.	30 April 2024

Perubahan	Deskripsi	Tanggal
AmazonDataZoneSage MakerProvisioning - kebijakan baru	Kebijakan baru yang disebut AmazonDataZoneSage MakerProvisioningmemberikan Amazon izin DataZone yang diperlukan untuk berinteraksi dengan Amazon. SageMaker	30 April 2024
AmazonDataZoneS3Manage-<region>- <domainId>- peran baru	Peran baru yang disebut AmazonDataZoneS3Manage--<region><domainId>yang digunakan saat Amazon DataZone memanggil AWS Lake Formation untuk mendaftarkan lokasi Amazon Simple Storage Service (Amazon S3). AWS Lake Formation mengambil peran ini ketika mengakses data di lokasi itu.	1 April 2024
AmazonDataZoneGlue ManageAccessRolePolicy - Pembaruan kebijakan	Memperbarui AmazonDataZoneGlueManageAccessRolePolicyuntuk mengaktifkan dukungan untuk izin yang memungkinkan Amazon DataZone mengaktifkan penerbitan dan akses hibah ke data.	1 April 2024

Perubahan	Deskripsi	Tanggal
AmazonDataZoneDomainExecutionRolePolicy dan AmazonDataZoneFullUserAccess - Pembaruan kebijakan	Memperbarui AmazonDataZoneDomainExecutionRolePolicydan AmazonDataZoneFullUserAccesmengaktifkan dukungan untuk `CancelMetadataGenerationRun` API.	Maret 29, 2024
AmazonDataZoneFullAccess - Pembaruan kebijakan	Memperbarui `AmazonDataZoneFullAccess` untuk memungkinkan pengguna memilih rahasia, cluster, vpc, dan subnet mereka di konsol DataZone manajemen Amazon daripada mengetikn ya di kotak teks.	Maret 13, 2024
AmazonDataZoneDomainExecutionRolePolicy - Pembaruan kebijakan	Memperbarui AmazonDataZoneDomainExecutionRolePolicyuntuk mengaktifkan dukungan untuk `ListEnvironmentBlueprintConfigurationSummaries` API yang diperlukan untuk membuat profil lingkungan dengan mengidentifikasi cetak biru mana yang diaktifkan di akun dan wilayah mana.	Februari 01, 2024

Perubahan	Deskripsi	Tanggal
AmazonDataZoneGlue ManageAccessRolePolicy - Pembaruan kebijakan	Memperbarui AmazonDat aZoneGlueManageAcc essRolePolicyuntuk mengaktif kan dukungan untuk mode hibrida AWS Lake Formation.	14 Desember 2023
AmazonDataZoneFull UserAccess dan AmazonDat aZoneDomainExecuti onRolePolicy - Pembaruan kebijakan	Memperbarui AmazonDat aZoneFullUserAccessdan AmazonDataZoneDoma inExecutionRolePol icykebijakan untuk mendukung fungsionalitas deskripsi data bertenaga AI generatif di Amazon. DataZone	28 November 2023
AmazonDataZoneEnvi ronmentRolePermiss ionsBoundary - Pembaruan kebijakan	Amazon DataZone membuat pembaruan pada kebijakan AmazonDataZoneEnvi ronmentRolePermiss ionsBoundaryterkelola yang terdiri dari `athena:Ge tQueryResultsStrea m` izin tambahan yang tercakup dengan kondisi tersebut`ResourceTag` .	17 November 2023

Perubahan	Deskripsi	Tanggal
AmazonDataZoneReds hiftManageAccessRolePolicy - Pembaruan kebijakan	Amazon DataZone memperbarui AmazonDat aZoneRedshiftManag eAccessRolePolicydengan menghapus cek pada ID organisasi untuk `redshift: AssociateDataShare Consumer` tindakan tersebut. Ini memungkinkan Anda untuk berbagi sumber daya di seluruh AWS organisasi.	16 November 2023
AmazonDataZoneFull UserAccess - Pembaruan kebijakan	Amazon DataZone memperbarui AmazonDat aZoneFullUserAcces skebijakan yang memberika n akses penuh ke Amazon DataZone, tetapi tidak mengizinkan pengelolaan domain, pengguna, atau akun terkait.	Oktober 02, 2023
AmazonDataZonePort alFullAccessPolicy - kebijakan usang	Amazon DataZone menghenti kan. AmazonDataZonePort alFullAccessPolicy	September 29, 2023
AmazonDataZonePrev iewConsoleFullAccess - kebijakan usang	Amazon DataZone menghenti kan. AmazonDataZonePrev iewConsoleFullAccess	September 29, 2023

Perubahan	Deskripsi	Tanggal
AmazonDataZoneDomainExecutionRolePolicy - Kebijakan baru	Amazon DataZone menambahkan kebijakan baru yang disebut AmazonDataZoneDomainExecutionRolePolicy. Ini adalah kebijakan default untuk peran DataZone `AmazonDataZoneDomainExecutionRole` layanan Amazon. Peran ini digunakan oleh Amazon DataZone untuk membuat katalog, menemukan, mengatur, berbagi, dan menganalisis data dalam DataZone domain Amazon. Anda dapat melampirkan `AmazonDataZoneDomainExecutionRolePolicy` kebijakan ke Anda`AmazonDataZoneDomainExecutionRole` .	25 September 2023
AmazonDataZoneCrossAccountAdmin - Kebijakan baru	Amazon DataZone menambahkan kebijakan baru yang disebut AmazonDataZoneCrossAccountAdminyang memungkinkan pengguna untuk bekerja dengan Amazon DataZone dan akun terkaitnya.	September 19, 2023

Perubahan	Deskripsi	Tanggal
AmazonDataZoneFull UserAccess - Kebijakan baru	Amazon DataZone menambahkan kebijakan baru yang disebut AmazonDat aZoneFullUserAccessyang memberikan akses penuh ke Amazon DataZone, tetapi tidak mengizinkan pengelola an domain, pengguna, atau akun terkait.	12 September 2023
AmazonDataZoneReds hiftManageAccessRolePolicy - Kebijakan baru	Amazon DataZone menambahkan kebijakan baru yang disebut AmazonDat aZoneRedshiftManag eAccessRolePolicyyang memberikan izin untuk memungkinkan Amazon mengaktifkan penerbitan dan akses hibah DataZone ke data.	12 September 2023
AmazonDataZoneGlue ManageAccessRolePolicy - Kebijakan baru	Amazon DataZone menambahkan kebijakan baru yang disebut AmazonDat aZoneGlueManageAcc essRolePolicyyang memberika n DataZone izin Amazon untuk mempublikasikan data AWS Glue ke katalog. Ini juga memberikan DataZone izin Amazon untuk memberikan akses atau mencabut akses ke aset yang diterbitkan AWS Glue di katalog.	12 September 2023

Perubahan	Deskripsi	Tanggal
AmazonDataZoneRedshiftGlueProvisioningPolicy - Kebijakan baru	Amazon DataZone menambahkan kebijakan baru yang disebut AmazonDataZoneRedshiftGlueProvisioningPolicyyang memberikan Amazon izin DataZone yang diperlukan untuk berinteraksi dengan sumber data yang didukung.	12 September 2023
AmazonDataZoneEnvironmentRolePermissionsBoundary - Kebijakan baru	Amazon DataZone menambahkan kebijakan baru yang disebut AmazonDataZoneEnvironmentRolePermissionsBoundaryyang membatasi prinsipal IAM yang disediakan yang dilampirkan.	12 September 2023
AmazonDataZoneFullAccess - Kebijakan baru	Amazon DataZone menambahkan kebijakan baru yang disebut AmazonDataZoneFullAccessyang menyediakan akses penuh ke Amazon DataZone melalui Konsol AWS Manajemen.	12 September 2023
Pembaruan kebijakan terkelola	Pembaruan kebijakan AmazonDataZonePreviewConsoleFullAccessterkelola yang terdiri dari `iam:GetPolicy` izin tambahan.	13 Juni 2023

Perubahan	Deskripsi	Tanggal
Amazon DataZone mulai melacak perubahan	Amazon DataZone mulai melacak perubahan untuk kebijakan yang AWS dikelola.	20 Maret 2023

Peran IAM untuk Amazon DataZone

Topik

AmazonDataZoneProvisioningRole-<domainAccountId>

`AmazonDataZoneProvisioningRole-<domainAccountId>`Memiliki yang `AmazonDataZoneRedshiftGlueProvisioningPolicy` terlampir. Peran ini memberi Amazon izin DataZone yang diperlukan untuk berinteraksi dengan AWS Glue dan Amazon Redshift.

Default `AmazonDataZoneProvisioningRole-<domainAccountId>` memiliki kebijakan kepercayaan berikut terlampir:

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

```
        "StringEquals": {
            "aws:SourceAccount": "{{domain_account}}"
        }
      }
    }
  ]
}
```

AmazonDataZoneDomainExecutionRole

AmazonDataZoneDomainExecutionRoleMemiliki kebijakan AWS terkelola AmazonDataZoneDomainExecutionRolePolicyterlampir. Amazon DataZone menciptakan peran ini untuk Anda atas nama Anda. Untuk tindakan tertentu di portal data, Amazon DataZone mengasumsikan peran ini dalam akun tempat peran dibuat dan memeriksa apakah peran ini diizinkan untuk melakukan tindakan.

AmazonDataZoneDomainExecutionRolePeran diperlukan dalam Akun AWS yang meng-host DataZone domain Amazon Anda. Peran ini secara otomatis dibuat untuk Anda saat Anda membuat DataZone domain Amazon Anda.

AmazonDataZoneDomainExecutionRolePeran default memiliki kebijakan kepercayaan berikut.

```
{
    "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>

`AmazonDataZoneGlueAccess-<region>-<domainId>`Peran memiliki `AmazonDataZoneGlueManageAccessRolePolicy` terlampir. Peran ini memberikan DataZone izin Amazon untuk mempublikasikan data AWS Glue ke katalog. Ini juga memberikan DataZone izin Amazon untuk memberikan akses atau mencabut akses ke aset yang diterbitkan AWS Glue di katalog.

`AmazonDataZoneGlueAccess-<region>-<domainId>`Peran default memiliki kebijakan kepercayaan berikut terlampir:

```
{
  "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>

`AmazonDataZoneRedshiftAccess-<region>-<domainId>`Peran memiliki `AmazonDataZoneRedshiftManageAccessRolePolicy` terlampir. Peran ini memberikan DataZone izin Amazon untuk mempublikasikan data Amazon Redshift ke katalog. Ini juga memberikan DataZone izin Amazon untuk memberikan akses atau mencabut akses ke Amazon Redshift atau Amazon Redshift Serverless aset yang diterbitkan dalam katalog.

`AmazonDataZoneRedshiftAccess-<region>-<domainId>`Peran default memiliki kebijakan izin inline berikut dilampirkan:

```
{
   "Version":"2012-10-17",
   "Statement":[
      {
         "Sid": "RedshiftSecretStatement",
         "Effect":"Allow",
         "Action":"secretsmanager:GetSecretValue",
         "Resource":"*",
         "Condition":{
            "StringEquals":{
               "secretsmanager:ResourceTag/AmazonDataZoneDomain":"{{domainId}}"
            }
         }
      }
   ]
}
```

Default `AmazonDataZoneRedshiftManageAccessRole<timestamp>` memiliki kebijakan kepercayaan berikut terlampir:

```
{
  "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>S3Kelola- - <domainId>

AmazonDataZoneS3Manage- <region>- <domainId>digunakan saat Amazon DataZone memanggil AWS Lake Formation untuk mendaftarkan lokasi Amazon Simple Storage Service (Amazon S3). AWS Lake Formation mengambil peran ini ketika mengakses data di lokasi itu. Untuk informasi selengkapnya, lihat Persyaratan untuk peran yang digunakan untuk mendaftarkan lokasi.

Peran ini memiliki kebijakan izin sebaris berikut yang dilampirkan.

```
{
    "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}}"
                }
            }
        }
    ]
}
```

AmazonDataZoneS3Manage- <region>- <domainId>memiliki kebijakan kepercayaan berikut terlampir:

```
{
    "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>

`AmazonDataZoneSageMakerManageAccessRole`Peran memiliki`AmazonDataZoneSageMakerAccess`, yang`AmazonDataZoneRedshiftManageAccessRolePolicy`, dan `AmazonDataZoneGlueManageAccessRolePolicy` terlampir. Peran ini memberikan DataZone izin Amazon untuk menerbitkan dan mengelola langganan untuk data lake, gudang data, dan aset Amazon Sagemaker.

`AmazonDataZoneSageMakerManageAccessRole`Peran tersebut memiliki kebijakan inline berikut terlampir:

```
{
   "Version":"2012-10-17",
   "Statement":[
      {
         "Sid": "RedshiftSecretStatement",
         "Effect":"Allow",
         "Action":"secretsmanager:GetSecretValue",
         "Resource":"*",
         "Condition":{
            "StringEquals":{
               "secretsmanager:ResourceTag/AmazonDataZoneDomain":"{{domainId}}"
            }
         }
      }
   ]
}
```

`AmazonDataZoneSageMakerManageAccessRole`Peran tersebut memiliki kebijakan kepercayaan berikut terlampir:

```
{
  "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>

`AmazonDataZoneSageMakerProvisioningRole`Peran memiliki `AmazonDataZoneSageMakerProvisioning` dan `AmazonDataZoneRedshiftGlueProvisioningPolicy` terlampir. Peran ini memberikan DataZone izin Amazon yang diperlukan untuk berinteraksi dengan AWS Glue, Amazon Redshift, dan Amazon Sagemaker.

`AmazonDataZoneSageMakerProvisioningRole`Peran tersebut memiliki kebijakan inline berikut terlampir:

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Sid": "SageMakerStudioTagOnCreate",
            "Effect": "Allow",
            "Action": [
                "sagemaker:AddTags"
            ],
```

```
            "Resource": "arn:aws:sagemaker:*:{{AccountId}}:*/*",
            "Condition": {
                "Null": {
                    "sagemaker:TaggingAction": "false"
                }
            }
        }
    ]
}
```

`AmazonDataZoneSageMakerProvisioningRole`Peran tersebut memiliki kebijakan kepercayaan berikut terlampir:

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Sid": "DataZoneTrustPolicyStatement",
      "Effect": "Allow",
      "Principal": {
        "Service": "datazone.amazonaws.com"
      },
      "Action": "sts:AssumeRole",
      "Condition": {
        "StringEquals": {
            "aws:SourceAccount": "{{domain_account}}"
        }
      }
    }
  ]
}
```

Peran berbasis identitas

Kebijakan berbasis identitas adalah dokumen kebijakan izin JSON yang dapat Anda lampirkan ke sebuah identitas, seperti pengguna IAM, grup pengguna IAM, atau peran IAM. Kebijakan ini mengontrol jenis tindakan yang dapat dilakukan oleh pengguna dan peran, di sumber daya mana, dan berdasarkan kondisi seperti apa. Untuk mempelajari cara membuat kebijakan berbasis identitas, lihat Membuat kebijakan IAM dalam Panduan Pengguna IAM.

Dengan kebijakan berbasis identitas IAM, Anda dapat menentukan secara spesifik apakah tindakan dan sumber daya diizinkan atau ditolak, serta kondisi yang menjadi dasar dikabulkan atau ditolaknya tindakan tersebut. Anda tidak dapat menentukan secara spesifik prinsipal dalam sebuah kebijakan berbasis identitas karena prinsipal berlaku bagi pengguna atau peran yang melekat kepadanya. Untuk mempelajari semua elemen yang dapat Anda gunakan dalam kebijakan JSON, lihat Referensi elemen kebijakan JSON IAM dalam Panduan Pengguna IAM.

Saat Anda membuat DataZone proyek Amazon, di portal, tiga peran IAM dibuat untuk proyek ini, satu untuk setiap jenis peran anggota proyek: pemilik dan kontributor. Izin yang dilampirkan pada setiap peran dicakup ke peran proyek, dan kebijakan izin terlampir bergantung pada kemampuan yang digunakan proyek.

Agar Amazon dapat DataZone mengelola izin dan berbagi aset dengan proyek pelanggan, peran pengguna proyek pelanggan secara otomatis ditambahkan sebagai Administrator data lake di AWS Lake Formation dalam aset Akun AWS penerbitan.

Anda dapat melihat up-to-date versi peran terbanyak di konsol manajemen AWS IAM, atau meninjau izin peran yang berbeda dalam tabel di bawah ini.

Izin pemilik proyek

Tipe lingkungan	Izin IAM
Data Lake standar	Ini adalah kombinasi dari kemampuan Essential, Data Lake Producer, dan Data Lake Consumer.

Esensi	<pre>{
	  "Version": "2012-10-17",
	  "Statement": [
	  {
	  "Effect": "Allow",
	  "Action": [
	  "s3:List*",
	  "s3:Get*",
	  "s3:Describe*",
	  "s3:DeleteObjectVersion",</pre>

Tipe lingkungan	Izin IAM	

```
        "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"
      ],
      "Resource":
 "keyArn",
      "Effect": "Allow"
    },
    {
```

Tipe lingkungan	Izin IAM	

```
      "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"
      ],
      "Resource":
 "arn:aws:logs:regi
on:account-id:log-
group:log-group-na
me:*",
      "Effect": "Allow"
```

Tipe lingkungan	Izin IAM	

```
    },
    {
      "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"
        }
      }
    }
  ]
}
```

Tipe lingkungan	Izin IAM
Produsen Data Lake	{ "Version": "2012-10-17", "Statement": [{ "Effect": "Allow", "Action": ["glue:BatchGet*", "glue:Get*", "glue:SearchTables", "glue:List*", "glue:BatchCreateP artition", "glue:CreatePartit ionIndex", "glue:CreateTable", "glue:BatchUpdateP artition", "glue:BatchDeleteP artition", "glue:UpdateTable", "glue:DeleteTableV ersion", "glue:DeleteTable", "glue:DeleteColumn

Tipe lingkungan	Izin IAM	

```
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
```

Tipe lingkungan	Izin IAM	

```
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",
```

Tipe lingkungan	Izin IAM	
	"glue:StartWorkflowRun", "glue:StopCrawlerSchedule", "glue:ResumeWorkflowRun", "glue:List*", "glue:DeleteCrawler", "glue:UpdateBlueprint", "glue:BatchStopJobRun", "glue:StopWorkflowRun", "glue:BatchGet*", "glue:UpdateCrawlerSchedule", "glue:DeleteConnection", "glue:UpdateConnection", "glue:Get*", "glue:BatchDeleteConnection", "glue:StartCrawlerSchedule",	

Tipe lingkungan	Izin IAM	

```
 "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",
```

Tipe lingkungan	Izin IAM	

```
 "glue:CreateDataQu
alityRuleset"
            ],
            "Resource":
 "*"
        },
        {
            "Sid":
 "VisualEditor0",
            "Effect":
 "Allow",
            "Action": [

 "iam:ListRoles",

 "iam:ListUsers",

 "iam:ListGroups",

 "iam:ListRolePolic
ies",

 "iam:GetRole",

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

Tipe lingkungan	Izin IAM	

Konsumen Data Lake	{
	  "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",	

Tipe lingkungan	Izin IAM	

```
        "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": [
```

Tipe lingkungan	Izin IAM	
	"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/*"] }] }	

Tipe lingkungan	Izin IAM	

Produsen Data Warehouse	{
	  "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"
	  }
	  ]
	}	

Tipe lingkungan	Izin IAM	

Tipe lingkungan	Izin IAM	

Konsumen Data Warehouse	{
	"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"
	}	

Tipe lingkungan	Izin IAM	
	`} }, { "Sid": "VisualEd itor2", "Effect": "Allow", "Action": [ "redshift- data:DescribeStat ement", "redshift- data:ExecuteStatement" ], "Resource": "arn:aws:redshift: region:account-id: cluster:cluster-id entifier" } ] }`	

Tipe lingkungan	Izin IAM	

Editor kueri Amazon Redshift 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",	

Tipe lingkungan	Izin IAM	

```
        "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
```

Tipe lingkungan	Izin IAM
	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" }] }

Izin kontributor proyek

Tipe lingkungan	Izin IAM
Data Lake standar	Ini adalah kombinasi dari kemampuan Essential, Data Lake Producer, dan Data Lake Consumer.
Esensi	{ "Version": "2012-10-17", "Statement": [{ "Effect": "Allow",

Tipe lingkungan	Izin IAM	

```
      "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"
      ],
```

Tipe lingkungan	Izin IAM	

```
      "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"
      ],
```

Tipe lingkungan	Izin IAM	

```
      "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"
        }
      }
    }
  ]
}
```

Tipe lingkungan	Izin IAM	
Produsen Data Lake	{ "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",	

Tipe lingkungan	Izin IAM	

```
        "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",
```

Tipe lingkungan	Izin IAM	

```
        "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*",
```

Tipe lingkungan	Izin IAM	

```
        "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": "*"
```

Tipe lingkungan	Izin IAM	

```
    },
    {
      "Sid": "VisualEd
itor0",
      "Effect": "Allow",
      "Action": [
        "iam:List
Roles",
        "iam:List
Users",
        "iam:List
Groups",
        "iam:List
RolePolicies",
        "iam:GetRole",
        "iam:GetR
olePolicy"
      ],
      "Resource": "*"
    }
  ]
}
```

Tipe lingkungan	Izin IAM	
Konsumen Data Lake	{ "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",	

Tipe lingkungan	Izin IAM	

```
        "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": [
```

Tipe lingkungan	Izin IAM	

	<pre>"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/*"
	]
	}
	]
	}</pre>	

Tipe lingkungan	Izin IAM	

Produsen Data Warehouse	{
	  "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"
	  }
	  ]
	}	

Tipe lingkungan	Izin IAM	

Tipe lingkungan	Izin IAM

Konsumen Data Warehouse	{
	"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"
	}

Tipe lingkungan	Izin IAM	

	`}`
	`},`
	`{`
	`"Sid": "VisualEd itor2",`
	`"Effect": "Allow",`
	`"Action": [`
	`"redshift- data:DescribeStat ement",`
	`"redshift- data:ExecuteStatement"`
	`],`
	`"Resource": "arn:aws:redshift: region:account-id: cluster:cluster-id entifier"`
	`}`
	`]`
	`}`	

Tipe lingkungan	Izin IAM	

Editor kueri Amazon Redshift 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",	

Tipe lingkungan	Izin IAM	

```
        "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
```

Tipe lingkungan	Izin IAM	

```
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"
    }
  ]
}
```

Kredensial Sementara

Beberapa AWS layanan tidak berfungsi saat Anda masuk menggunakan kredensil sementara. Untuk informasi tambahan, termasuk AWS layanan mana yang bekerja dengan kredensi sementara, lihat AWS layanan yang bekerja dengan IAM di Panduan Pengguna IAM.

Anda menggunakan kredensi sementara jika Anda masuk AWS Management Console menggunakan metode apa pun kecuali nama pengguna dan kata sandi. Misalnya, ketika Anda mengakses AWS menggunakan tautan masuk tunggal (SSO) perusahaan Anda, proses tersebut secara otomatis membuat kredensil sementara. Anda juga akan secara otomatis membuat kredensial sementara ketika Anda masuk ke konsol sebagai seorang pengguna lalu beralih peran. Untuk informasi selengkapnya tentang peralihan peran, lihat Peralihan peran (konsol) dalam Panduan Pengguna IAM.

Anda dapat membuat kredensil sementara secara manual menggunakan API AWS CLI atau AWS . Anda kemudian dapat menggunakan kredensyal sementara tersebut untuk mengakses. AWS AWS merekomendasikan agar Anda secara dinamis menghasilkan kredensi sementara alih-alih menggunakan kunci akses jangka panjang. Untuk informasi selengkapnya, lihat Kredensial keamanan sementara di IAM.

Izin prinsipal

Saat Anda menggunakan pengguna atau peran IAM untuk melakukan tindakan AWS, Anda dianggap sebagai prinsipal. Kebijakan memberikan izin kepada principal. Saat Anda menggunakan beberapa layanan, Anda mungkin melakukan tindakan yang kemudian memicu tindakan lain di layanan yang berbeda. Dalam hal ini, Anda harus memiliki izin untuk melakukan kedua tindakan tersebut. Untuk melihat apakah suatu tindakan memerlukan tindakan dependen tambahan dalam kebijakan, lihat Tindakan, Sumber Daya, dan Kunci Kondisi untuk Essentials AWS Dokumentasi dalam Referensi Otorisasi Layanan.

Validasi kepatuhan untuk Amazon DataZone

Untuk mempelajari apakah an Layanan AWS berada dalam lingkup program kepatuhan tertentu, lihat Layanan AWS di Lingkup oleh Program Kepatuhan Layanan AWS dan pilih program kepatuhan yang Anda minati. Untuk informasi umum, lihat Program AWS Kepatuhan Program AWS .

Anda dapat mengunduh laporan audit pihak ketiga menggunakan AWS Artifact. Untuk informasi selengkapnya, lihat Mengunduh Laporan di AWS Artifact .

Tanggung jawab kepatuhan Anda saat menggunakan Layanan AWS ditentukan oleh sensitivitas data Anda, tujuan kepatuhan perusahaan Anda, dan hukum dan peraturan yang berlaku. AWS menyediakan sumber daya berikut untuk membantu kepatuhan:

- Panduan Memulai Cepat Keamanan dan Kepatuhan — Panduan penerapan ini membahas pertimbangan arsitektur dan memberikan langkah-langkah untuk menerapkan lingkungan dasar AWS yang berfokus pada keamanan dan kepatuhan.
- Arsitektur untuk Keamanan dan Kepatuhan HIPAA di Amazon Web Services — Whitepaper ini menjelaskan bagaimana perusahaan dapat menggunakan AWS untuk membuat aplikasi yang memenuhi syarat HIPAA.

> **Note**
>
> Tidak semua memenuhi Layanan AWS syarat HIPAA. Untuk informasi selengkapnya, lihat Referensi Layanan yang Memenuhi Syarat HIPAA.

- AWS Sumber Daya AWS — Kumpulan buku kerja dan panduan ini mungkin berlaku untuk industri dan lokasi Anda.
- AWS Panduan Kepatuhan Pelanggan - Memahami model tanggung jawab bersama melalui lensa kepatuhan. Panduan ini merangkum praktik terbaik untuk mengamankan Layanan AWS dan memetakan panduan untuk kontrol keamanan di berbagai kerangka kerja (termasuk Institut Standar dan Teknologi Nasional (NIST), Dewan Standar Keamanan Industri Kartu Pembayaran (PCI), dan Organisasi Internasional untuk Standardisasi (ISO)).
- Mengevaluasi Sumber Daya dengan Aturan dalam Panduan AWS Config Pengembang — AWS Config Layanan menilai seberapa baik konfigurasi sumber daya Anda mematuhi praktik internal, pedoman industri, dan peraturan.
- AWS Security Hub— Ini Layanan AWS memberikan pandangan komprehensif tentang keadaan keamanan Anda di dalamnya AWS. Security Hub menggunakan kontrol keamanan untuk sumber daya AWS Anda serta untuk memeriksa kepatuhan Anda terhadap standar industri keamanan dan praktik terbaik. Untuk daftar layanan dan kontrol yang didukung, lihat Referensi kontrol Security Hub.
- Amazon GuardDuty — Ini Layanan AWS mendeteksi potensi ancaman terhadap beban kerja Akun AWS, kontainer, dan data Anda dengan memantau lingkungan Anda untuk aktivitas yang mencurigakan dan berbahaya. GuardDuty dapat membantu Anda mengatasi berbagai persyaratan kepatuhan, seperti PCI DSS, dengan memenuhi persyaratan deteksi intrusi yang diamanatkan oleh kerangka kerja kepatuhan tertentu.
- AWS Audit ManagerIni Layanan AWS membantu Anda terus mengaudit AWS penggunaan Anda untuk menyederhanakan cara Anda mengelola risiko dan kepatuhan terhadap peraturan dan standar industri.

Praktik Terbaik Keamanan untuk Amazon DataZone

Amazon DataZone menyediakan sejumlah fitur keamanan untuk dipertimbangkan saat Anda mengembangkan dan menerapkan kebijakan keamanan Anda sendiri. Praktik terbaik berikut adalah pedoman umum dan tidak mewakili solusi keamanan yang lengkap. Karena praktik terbaik

ini mungkin tidak sesuai atau tidak memadai untuk lingkungan Anda, perlakukan itu sebagai pertimbangan yang bermanfaat, bukan sebagai resep.

Terapkan akses hak akses paling rendah

Saat memberikan izin, Anda memutuskan siapa yang mendapatkan izin apa untuk sumber daya Amazon mana. DataZone Anda memungkinkan tindakan tertentu yang ingin Anda lakukan di sumber daya tersebut. Oleh karena itu, Anda harus memberikan hanya izin yang diperlukan untuk melaksanakan tugas. Menerapkan akses hak istimewa yang terkecil adalah hal mendasar dalam mengurangi risiko keamanan dan dampak yang dapat diakibatkan oleh kesalahan atau niat jahat.

Gunakan IAM role

Aplikasi produsen dan klien harus memiliki kredensyal yang valid untuk mengakses sumber daya Amazon DataZone. Anda tidak boleh menyimpan AWS kredensyal secara langsung di aplikasi klien atau di bucket Amazon S3. Ini adalah kredensial jangka panjang yang tidak dirotasi secara otomatis dan dapat menimbulkan dampak bisnis yang signifikan jika dibobol.

Sebagai gantinya, Anda harus menggunakan peran IAM untuk mengelola kredensi sementara untuk aplikasi produsen dan klien Anda untuk mengakses sumber daya Amazon. DataZone Saat Anda menggunakan peran, Anda tidak perlu menggunakan kredensial jangka panjang (seperti nama pengguna dan kata sandi atau access key) untuk mengakses sumber daya lainnya.

Untuk informasi selengkapnya, lihat topik berikut di Panduan Pengguna IAM:

- Peran IAM
- Skenario Umum untuk Peran: Pengguna, Aplikasi, dan Layanan

Terapkan Enkripsi Sisi Server di Sumber Daya Dependen

Data saat istirahat dan data dalam perjalanan dapat dienkripsi di Amazon. DataZone

Gunakan CloudTrail untuk Memantau Panggilan API

Amazon DataZone terintegrasi dengan AWS CloudTrail, layanan yang menyediakan catatan tindakan yang diambil oleh pengguna, peran, atau AWS layanan di Amazon DataZone.

Dengan menggunakan informasi yang dikumpulkan oleh CloudTrail, Anda dapat menentukan permintaan yang dibuat ke Amazon DataZone, alamat IP dari mana permintaan itu dibuat, siapa yang membuat permintaan, kapan dibuat, dan detail tambahan.

Ketahanan di Amazon DataZone

Infrastruktur AWS global dibangun di sekitar Wilayah AWS dan Availability Zones. Wilayah AWS menyediakan beberapa Availability Zone yang terpisah secara fisik dan terisolasi, yang terhubung dengan latensi rendah, throughput tinggi, dan jaringan yang sangat redundan. Dengan Zona Ketersediaan, Anda dapat merancang serta mengoperasikan aplikasi dan basis data yang secara otomatis melakukan fail over di antara zona tanpa gangguan. Zona Ketersediaan memiliki ketersediaan dan toleransi kesalahan yang lebih baik, dan dapat diskalakan dibandingkan infrastruktur pusat data tunggal atau multi tradisional.

Untuk informasi selengkapnya tentang Wilayah AWS dan Availability Zone, lihat Infrastruktur AWS Global.

Selain infrastruktur AWS global, Amazon DataZone menawarkan beberapa fitur untuk membantu mendukung ketahanan data dan kebutuhan cadangan Anda.

Topik

Ketahanan sumber data

Selama acara DataZone ketersediaan Amazon, `DataSource` pekerjaan akan dicoba lagi secara berkala hingga 24 jam. Jika pekerjaan gagal karena kesalahan konfigurasi, sebuah `DataSourceRunFailed` peristiwa akan dipancarkan. Jika DataZone domain Amazon dikonfigurasi

dengan kunci KMS, dan AmazonDataZoneDomainExecutionRole kehilangan akses ke kunci ini selama menjalankan pekerjaan, proses akan berakhir di `INACCESSIBLE` status. Setelah akses KMS dipulihkan, pekerjaan harus diperbarui secara manual untuk memicu transisi kembali ke keadaan yang dapat digunakan.

Ketahanan aset

Di Amazon DataZone, aset diberi versi. Jika versi aset perlu diputar kembali, Anda dapat membuat versi baru menggunakan konten versi stabil terakhir. Versi aset dapat dipublikasikan. Versi aset yang diterbitkan tidak dapat diedit, kecuali dengan menerbitkan versi baru. Aset yang diterbitkan (alias listing) dapat berlangganan. Untuk mencegah langganan baru ke suatu aset, itu bisa tidak dipublikasikan. Tidak menerbitkan aset tidak berpengaruh pada langganan yang ada. Menghapus aset akan menghapus semua versi aset yang tidak dipublikasikan. Versi aset yang diterbitkan harus dihapus secara terpisah. Versi aset yang diterbitkan hanya dapat dihapus jika tidak ada langganan.

Jenis aset dan metadata membentuk ketahanan

Di Amazon DataZone, tipe aset dan tipe formulir metadata diberi versi. Jenis aset tidak dapat dihapus jika digunakan oleh aset. Jenis formulir metadata tidak dapat dihapus jika digunakan oleh jenis aset atau aset. Jika Anda tidak ingin spesifik digunakan metadata-form-type untuk kurasi, Anda dapat menonaktifkannya yang tidak memengaruhi yang sudah dilampirkan.

Ketahanan glosarium

Di Amazon DataZone, glosarium dan istilah glosarium tidak dapat dihapus jika sedang digunakan. Jika Anda tidak ingin glosarium atau istilah glosari tertentu digunakan untuk kurasi, Anda dapat menonaktifkannya yang tidak memengaruhi glosarium yang sudah dilampirkan.

Ketahanan pencarian global

Di Amazon DataZone, aset yang diterbitkan (alias daftar) dapat ditemukan melalui pencarian global. Penerbitan aset dapat dibatalkan dengan membatalkan penerbitan aset. Membatalkan penerbitan aset tidak memengaruhi langganan yang ada. Aset yang diterbitkan dapat dikembalikan ke versi aset tertentu dengan menerbitkan ulang versi tersebut. Ini tidak akan mempengaruhi langganan yang ada.

Ketahanan berlangganan

Di Amazon DataZone, pemenuhan SubscriptionGrant akan mencoba dua pensiunan sebelum gagal. Jika gagal, itu harus dihapus secara manual untuk mencoba lagi. Jika Amazon DataZone

tidak dapat mencabut izin untuk berlangganan, menghapus langganan mungkin gagal. Kesalahan mendasar harus diatasi, atau `retainPermissions` flag dapat digunakan dalam operasi `DeleteSubscriptionGrant` API untuk memaksa penghapusan hibah dari Amazon DataZone tanpa mencabut izin.

Jika DataZone domain Amazon dikonfigurasi dengan kunci KMS, dan `AmazonDataZoneDomainExecutionRole` kehilangan akses ke kunci ini selama `SubscriptionGrant` alur kerja, hibah akan ditandai. `INACCESSIBLE` Setelah akses KMS dipulihkan, `INACCESSIBLE` hibah harus dihapus dan dibuat ulang.

Ketahanan lingkungan

Jika DataZone domain Amazon dikonfigurasi dengan kunci KMS, dan `AmazonDataZoneDomainExecutionRole` kehilangan akses ke kunci ini selama alur kerja lingkungan, lingkungan akan ditandai. `INACCESSIBLE` Setelah akses KMS dipulihkan, `INACCESSIBLE` lingkungan harus dihapus dan dibuat ulang. Penciptaan lingkungan akan mencoba dua pensiunan sebelum gagal. Jika gagal, itu harus dihapus secara manual untuk mencoba lagi. Jika alur kerja lingkungan gagal, lingkungan akan memasuki status gagal. Pada titik ini, itu hanya dapat dihapus dan dibuat ulang.

Ketahanan cetak biru lingkungan

Di Amazon DataZone, cetak biru lingkungan tidak dapat dihapus jika ada profil lingkungan yang mendasarinya.

Ketahanan proyek

Di Amazon DataZone, proyek tidak dapat dihapus jika ada lingkungan yang terkandung.

Ketahanan RAM

Untuk informasi ketahanan RAM, lihat https://docs.aws.amazon.com/ram/latest/userguide/ security-disaster-recovery-resiliency .html.

Ketahanan manajemen profil pengguna

Untuk informasi ketahanan profil pengguna, lihat Pusat AWS Identitas.

Ketahanan domain

Di Amazon DataZone, domain tidak dapat dihapus jika berisi proyek atau sumber data.

Keamanan Infrastruktur di Amazon DataZone

Sebagai layanan terkelola, Amazon DataZone dilindungi oleh keamanan jaringan AWS global. Untuk informasi tentang layanan AWS keamanan dan cara AWS melindungi infrastruktur, lihat Keamanan AWS Cloud. Untuk mendesain AWS lingkungan Anda menggunakan praktik terbaik untuk keamanan infrastruktur, lihat Perlindungan Infrastruktur dalam Kerangka Kerja yang AWS Diarsiteksikan dengan Baik Pilar Keamanan.

Anda menggunakan panggilan API yang AWS dipublikasikan untuk mengakses Amazon DataZone melalui jaringan. Klien harus mendukung hal-hal berikut:

- Keamanan Lapisan Pengangkutan (TLS). Kami mensyaratkan TLS 1.2 dan menganjurkan TLS 1.3.
- Sandi cocok dengan sistem kerahasiaan maju sempurna (perfect forward secrecy, PFS) seperti DHE (Ephemeral Diffie-Hellman) atau ECDHE (Elliptic Curve Ephemeral Diffie-Hellman). Sebagian besar sistem modern seperti Java 7 dan versi lebih baru mendukung mode-mode ini.

Selain itu, permintaan harus ditandatangani menggunakan ID kunci akses dan kunci akses rahasia yang terkait dengan prinsipal IAM. Atau Anda dapat menggunakan AWS Security Token Service (AWS STS) untuk menghasilkan kredensial keamanan sementara untuk menandatangani permintaan.

Pencegahan deputi kebingungan lintas layanan di Amazon DataZone

Masalah deputi yang bingung adalah masalah keamanan di mana entitas yang tidak memiliki izin untuk melakukan tindakan dapat memaksa entitas yang lebih istimewa untuk melakukan tindakan. Pada tahun AWS, peniruan lintas layanan dapat mengakibatkan masalah wakil yang membingungkan. Peniruan identitas lintas layanan dapat terjadi ketika satu layanan (layanan yang dipanggil) memanggil layanan lain (layanan yang dipanggil). Layanan pemanggilan dapat dimanipulasi menggunakan izinnya untuk bertindak pada sumber daya pelanggan lain dengan cara yang seharusnya tidak dilakukannya kecuali bila memiliki izin untuk mengakses. Untuk mencegah hal ini, AWS sediakan alat yang membantu Anda melindungi data Anda untuk semua layanan dengan prinsip layanan yang telah diberikan akses ke sumber daya di akun Anda.

Sebaiknya gunakan kunci konteks kondisi SourceAccount global aws: dalam kebijakan sumber daya untuk membatasi izin yang DataZone diberikan Amazon layanan lain ke sumber daya. Gunakan aws: SourceAccount jika Anda ingin mengizinkan sumber daya apa pun di akun itu dikaitkan dengan penggunaan lintas layanan.

Analisis konfigurasi dan kerentanan untuk Amazon DataZone

AWS menangani tugas-tugas keamanan dasar seperti sistem operasi tamu (OS) dan patching database, konfigurasi firewall, dan pemulihan bencana. Prosedur ini telah ditinjau dan disertifikasi oleh pihak ketiga yang sesuai. Untuk informasi selengkapnya, lihat model tanggung jawab AWS bersama.

Domain untuk ditambahkan ke daftar izin Anda

Agar portal DataZone data Amazon dapat mengakses DataZone layanan Amazon, Anda harus menambahkan domain berikut ke daftar izinkan di jaringan tempat portal data mencoba mengakses layanan.

- `*.api.aws`
- `*.on.aws`

Memantau Amazon DataZone

Pemantauan adalah bagian penting dalam menjaga keandalan, ketersediaan, dan kinerja Amazon DataZone dan AWS solusi Anda yang lain. AWS menyediakan alat pemantauan berikut untuk menonton Amazon DataZone, melaporkan ketika ada sesuatu yang salah, dan mengambil tindakan otomatis bila perlu:

- Amazon CloudWatch memantau AWS sumber daya Anda dan dan aplikasi yang Anda jalankan AWS secara real time. Anda dapat mengumpulkan dan melacak metrik, membuat dasbor yang disesuaikan, dan mengatur alarm yang memberi tahu Anda atau mengambil tindakan saat metrik tertentu mencapai ambang batas yang ditentukan. Misalnya, Anda dapat CloudWatch melacak penggunaan CPU atau metrik lain dari instans Amazon EC2 Anda dan secara otomatis meluncurkan instans baru bila diperlukan. Untuk informasi selengkapnya, lihat Panduan CloudWatch Pengguna Amazon.
- Amazon CloudWatch Logs memungkinkan Anda memantau, menyimpan, dan mengakses file log Anda dari instans Amazon EC2, CloudTrail, dan sumber lainnya. CloudWatch Log dapat memantau informasi dalam file log dan memberi tahu Anda ketika ambang batas tertentu terpenuhi. Anda juga dapat mengarsipkan data log dalam penyimpanan yang sangat durabel. Untuk informasi selengkapnya, lihat Panduan Pengguna Amazon CloudWatch Logs.
- Amazon EventBridge dapat digunakan untuk mengotomatiskan AWS layanan Anda dan merespons secara otomatis peristiwa sistem, seperti masalah ketersediaan aplikasi atau perubahan sumber daya. Acara dari AWS layanan dikirimkan ke EventBridge dalam waktu dekat. Anda dapat menuliskan aturan sederhana untuk menunjukkan peristiwa mana yang sesuai kepentingan Anda, dan tindakan otomatis mana yang diambil ketika suatu peristiwa sesuai dengan suatu aturan. Untuk informasi selengkapnya, lihat Panduan EventBridge Pengguna Amazon.
- AWS CloudTrailmenangkap panggilan API dan peristiwa terkait yang dibuat oleh atau atas nama AWS akun Anda dan mengirimkan file log ke bucket Amazon S3 yang Anda tentukan. Anda dapat mengidentifikasi pengguna dan akun mana yang dipanggil AWS, alamat IP sumber dari mana panggilan dilakukan, dan kapan panggilan terjadi. Untuk informasi selengkapnya, silakan lihat Panduan Pengguna AWS CloudTrail.

Memantau Amazon DataZone dengan Amazon CloudWatch

Anda dapat memantau DataZone penggunaan Amazon CloudWatch, yang mengumpulkan data mentah dan memprosesnya menjadi metrik yang dapat dibaca, mendekati waktu nyata. Statistik

ini disimpan untuk jangka waktu 15 bulan, sehingga Anda dapat mengakses informasi historis dan mendapatkan perspektif yang lebih baik tentang performa aplikasi atau layanan web Anda. Anda juga dapat mengatur alarm yang memperhatikan ambang batas tertentu dan mengirim notifikasi atau mengambil tindakan saat ambang batas tersebut terpenuhi. Untuk informasi selengkapnya, lihat Panduan CloudWatch Pengguna Amazon.

Portal DataZone data Amazon menggunakan API pesawat DataZone data Amazon dengan otentikasi dan otorisasi JWT. Amazon DataZone mengasumsikan peran layanan DataZone default Amazon dan mencatat semua panggilan DataZone API Amazon yang dilakukan melalui portal DataZone data Amazon dalam grup log bernama DataZoneDataPortalAPI CallLogs.

Memantau DataZone peristiwa Amazon di Amazon EventBridge

Anda dapat memantau DataZone peristiwa Amazon di EventBridge, yang mengirimkan aliran data waktu nyata dari aplikasi, aplikasi software-as-a-service (SaaS), dan layanan Anda sendiri. AWS EventBridgemerutekan data tersebut ke target seperti AWS Lambda dan Amazon Simple Notification Service. Peristiwa ini sama dengan yang muncul di Amazon CloudWatch Events, yang memberikan aliran peristiwa sistem yang mendekati waktu nyata yang menggambarkan perubahan AWS sumber daya.

Untuk informasi selengkapnya, lihat Bekerja dengan acara melalui bus EventBridge default Amazon.

Pencatatan panggilan DataZone API Amazon menggunakan AWS CloudTrail

Amazon DataZone terintegrasi dengan AWS CloudTrail, layanan yang menyediakan catatan tindakan yang diambil oleh pengguna, peran, atau AWS layanan di Amazon DataZone. CloudTrail menangkap semua panggilan API untuk Amazon DataZone sebagai peristiwa. Panggilan yang diambil termasuk panggilan dari DataZone konsol Amazon dan panggilan kode ke operasi Amazon DataZone API. Jika Anda membuat jejak, Anda dapat mengaktifkan pengiriman CloudTrail acara secara berkelanjutan ke bucket Amazon S3, termasuk acara untuk Amazon. DataZone Jika Anda tidak mengonfigurasi jejak, Anda masih dapat melihat peristiwa terbaru di CloudTrail konsol dalam Riwayat acara. Dengan menggunakan informasi yang dikumpulkan oleh CloudTrail, Anda dapat menentukan permintaan yang dibuat ke Amazon DataZone, alamat IP dari mana permintaan itu dibuat, siapa yang membuat permintaan, kapan dibuat, dan detail tambahan.

Untuk mempelajari selengkapnya CloudTrail, lihat Panduan AWS CloudTrail Pengguna.

DataZone Informasi Amazon di CloudTrail

CloudTrail diaktifkan pada Akun AWS saat Anda membuat akun. Saat aktivitas terjadi di konsol DataZone manajemen Amazon, aktivitas tersebut direkam dalam suatu CloudTrail peristiwa bersama dengan peristiwa AWS layanan lainnya dalam riwayat Acara. Anda dapat melihat, mencari, dan mengunduh acara terbaru di situs Anda Akun AWS. Untuk informasi selengkapnya, lihat Melihat peristiwa dengan Riwayat CloudTrail acara.

Untuk catatan acara yang sedang berlangsung di Anda Akun AWS, termasuk acara untuk Amazon DataZone, buat jejak. Jejak memungkinkan CloudTrail untuk mengirimkan file log ke bucket Amazon S3. Secara default, saat Anda membuat jejak di konsol, jejak tersebut berlaku untuk semua Wilayah AWS. Jejak mencatat peristiwa dari semua Wilayah di AWS partisi dan mengirimkan file log ke bucket Amazon S3 yang Anda tentukan. Selain itu, Anda dapat mengonfigurasi AWS layanan lain untuk menganalisis lebih lanjut dan menindaklanjuti data peristiwa yang dikumpulkan dalam CloudTrail log. Untuk informasi selengkapnya, lihat berikut:

- Gambaran umum untuk membuat jejak
- CloudTrail layanan dan integrasi yang didukung
- Mengonfigurasi notifikasi Amazon SNS untuk CloudTrail
- Menerima file CloudTrail log dari beberapa wilayah dan Menerima file CloudTrail log dari beberapa akun

Semua DataZone tindakan Amazon dicatat oleh CloudTrail.

Memecahkan Masalah Amazon DataZone

Jika Anda mengalami masalah yang ditolak akses atau kesulitan serupa saat bekerja dengan Amazon, DataZone lihat topik di bagian ini.

Memecahkan masalah izin AWS Lake Formation untuk Amazon DataZone

Bagian ini berisi petunjuk pemecahan masalah untuk masalah yang mungkin Anda temui saat Anda. Konfigurasikan izin Lake Formation untuk Amazon DataZone

Pesan galat di Portal Data	Resolusi
Tidak dapat mengasumsikan Peran Akses Data.	Kesalahan ini ditampilkan ketika Amazon DataZone tidak dapat mengasumsikan AmazonDataZoneGlueDataAccessRolebahwa Anda digunakan untuk mengaktifkan DefaultDataLakeBlueprintdi akun Anda. Untuk memperbaiki masalah ini, buka konsol AWS IAM di akun tempat aset data Anda ada dan pastikan bahwa mereka AmazonDataZoneGlue DataAccessRolememiliki hubungan kepercaya an yang tepat dengan prinsipal DataZone layanan Amazon. Untuk informasi selengkap nya, lihat AmazonDataZoneGlueAccess- <region>- <domainId>
Peran Akses Data tidak memiliki izin yang diperlukan untuk membaca metadata aset yang Anda coba berlangganan.	Kesalahan ini ditampilkan ketika Amazon DataZone berhasil mengambil AmazonDat aZoneGlueDataAccessRoleperan, tetapi peran tersebut tidak memiliki izin yang diperluka n. Untuk memperbaiki masalah ini, buka konsol AWS IAM di akun tempat aset data Anda ada dan pastikan peran tersebut telah AmazonDataZoneGlueManageAccessRolePo licydilampirkan. Untuk informasi selengkapnya,

Pesan galat di Portal Data	Resolusi
	lihat AmazonDataZoneGlueAccess- <region>-<domainId>.
Aset adalah tautan sumber daya. Amazon DataZone tidak mendukung langganan ke tautan sumber daya.	Kesalahan ini ditampilkan ketika aset yang Anda coba publikasikan ke Amazon DataZone adalah tautan sumber daya ke tabel AWS Glue.

Pesan galat di Portal Data	Resolusi
Aset tidak dikelola oleh AWS Lake Formation.	Kesalahan ini menunjukkan bahwa izin AWS Lake Formation tidak diberlakukan pada aset yang ingin Anda publikasikan. Ini bisa terjadi dalam kasus-kasus berikut. • Lokasi aset Amazon S3 tidak terdaftar di AWS Lake Formation. Untuk memperbai ki masalah, masuk ke konsol AWS Lake Formation Anda di akun tempat tabel ada dan daftarkan lokasi Amazon S3 baik dalam mode AWS Lake Formation atau mode Hybrid. Untuk informasi selengkapnya, lihat Mendaftarkan lokasi Amazon S3. Ada beberapa skenario yang membutuhkan modifikasi lebih lanjut. Ini termasuk bucket AmazonS3 terenkripsi atau bucket S3 lintas akun dan pengaturan Glue Catalog. AWS Dalam kasus seperti itu, modifikasi dalam pengaturan KMS dan/atau S3 mungkin diperlukan. Untuk informasi selengkap nya, lihat Mendaftarkan lokasi Amazon S3 terenkripsi. • Lokasi Amazon S3 terdaftar dalam mode AWS Lake Formation tetapi IAM AllowedPr incipal ditambahkan ke izin tabel. Untuk memperbaiki masalah, Anda dapat menghapus IAM AllowedPrincipal dari izin tabel atau mendaftarkan lokasi S3 dalam mode Hybrid. Untuk informasi selengkap nya, lihat Tentang memutakhirkan ke model izin Lake Formation. Jika lokasi S3 Anda dienkripsi atau lokasi S3 berada di bagian yang berbeda dari tabel AWS Glue Anda,

Pesan galat di Portal Data	Resolusi
	ikuti petunjuk di Mendaftarkan lokasi Amazon S3 terenkripsi.
Peran Akses Data tidak memiliki izin Lake Formation yang diperlukan untuk memberikan akses ke aset ini.	Kesalahan ini menunjukkan AmazonDataZoneGlueDataAccessRolebahwa yang Anda gunakan untuk mengaktifkan DefaultDataLakeBlueprintdi akun Anda tidak memiliki izin yang diperlukan bagi Amazon DataZone untuk mengelola izin pada aset yang dipublikasikan. Anda dapat menyelesaikan masalah dengan menambahkan AmazonDataZoneGlueDataAccessRolesebagai administrator AWS Lake Formation atau dengan memberikan izin berikut ke AmazonDataZoneGlueDataAccessRoleaset yang ingin Anda publikasikan. • Jelaskan dan Jelaskan izin yang dapat diberikan pada database tempat aset itu ada • Jelaskan, Pilih, Jelaskan Dapat Diberikan, Pilih Izin yang Dapat Diberikan pada semua aset dalam database acecss yang ingin Anda kelola Amazon atas nama Anda. DataZone

Kuota untuk Amazon DataZone

AWS Akun Anda memiliki kuota default, sebelumnya disebut sebagai batas, untuk setiap layanan. AWS Kecuali dinyatakan lain, setiap kuota bersifat spesifik wilayah.

Amazon DataZone memiliki kuota dan batasan berikut.

Sumber Daya	Deskripsi	Nilai
Jenis Aset Data	Jumlah maksimum tipe aset data yang dapat dibuat dalam DataZone domain	1000
Aset data	Jumlah maksimum aset data yang dapat dibuat di DataZone domain Amazon	1 juta.
Glosarium	Jumlah maksimum glosarium bisnis yang dapat Anda buat di domain	1000
Istilah glosarium bisnis	Jumlah maksimum istilah glosarium bisnis total yang dapat Anda buat di domain	10000
Lingkungan dalam domain	Jumlah maksimum lingkungan dalam DataZone domain Amazon	500

Riwayat dokumen untuk Panduan DataZone Pengguna Amazon

Tabel berikut menjelaskan rilis dokumentasi untuk Amazon DataZone.

Perubahan	Deskripsi	Tanggal
AmazonDataZoneSageMakerProvisioning - kebijakan baru	Kebijakan baru yang disebut AmazonDataZoneSageMakerProvisioningmemberikan Amazon izin DataZone yang diperlukan untuk berinteraksi dengan Amazon. SageMaker Untuk informasi selengkapnya, lihat Amazon DataZone memperbarui kebijakan AWS terkelola.	April 30, 2024
AmazonDataZoneSageMakerEnvironmentRolePermissionsBoundary - batas izin baru	Batas izin baru disebut. AmazonDataZoneSageMakerEnvironmentRolePermissionsBoundary Saat Anda membuat SageMaker lingkungan Amazon melalui portal DataZone data Amazon, Amazon DataZone menerapkan batas izin ini ke peran IAM yang dihasilkan selama pembuatan lingkungan. Batas izin membatasi cakupan peran yang DataZone dibuat Amazon dan peran apa pun yang Anda tambahkan. Untuk informasi selengkapnya, lihat	April 30, 2024

	Amazon DataZone memperbarui kebijakan AWS terkelola.	
AmazonDataZoneSageMakerAccess - kebijakan baru	Kebijakan baru yang disebut AmazonDataZoneSageMakerAccessmemberi Amazon izin DataZone yang diperlukan untuk memberikan akses pengguna ke berbagai sumber daya di lingkungan Amazon SageMaker. Untuk informasi selengkapnya, lihat Amazon DataZone memperbarui kebijakan AWS terkelola.	April 30, 2024
AmazonDataZoneFullAccess - pembaruan kebijakan	Pembaruan AmazonDataZoneFullAccesskebijakan yang menambahkan akses ke `DescribeSecurityGroups` tindakan guna meningkatkan kegunaan administrator akun yang mengonfigurasi cetak biru di konsol dan `GetPolicy` tindakan untuk membantu mengambil informasi tentang kebijakan terkelola yang ditentukan. Untuk informasi selengkapnya, lihat Amazon DataZone memperbarui kebijakan AWS terkelola.	April 30, 2024

AmazonDataZoneS3Manage- - peran baru <region>< domainId>	Peran baru yang disebut AmazonDataZoneS3Manage- - <region><domainId>yang digunakan saat Amazon DataZone memanggil AWS Lake Formation untuk mendaftarkan lokasi Amazon Simple Storage Service (Amazon S3). AWS Lake Formation mengambil peran ini ketika mengakses data di lokasi itu. Untuk informasi selengkapnya, lihat Amazon DataZone memperbarui kebijakan AWS terkelola.	April 1, 2024
AmazonDataZoneGlue ManageAccessRolePolicy - Pembaruan kebijakan	Memperbarui AmazonDat aZoneGlueManageAcc essRolePolicyuntuk mengaktif kan dukungan untuk izin yang memungkinkan Amazon DataZone mengaktifkan penerbitan dan akses hibah ke data. Untuk informasi selengkapnya, lihat Amazon DataZone memperbarui kebijakan AWS terkelola.	April 1, 2024

AmazonDataZoneDomainExecutionRolePolicy dan AmazonDataZoneFullUserAccess - Pembaruan kebijakan	Memperbarui AmazonDataZoneDomainExecutionRolePolicydan AmazonDataZoneFullUserAccessuntuk mengaktifkan dukungan untuk `CancelMetadataGenerationRun` API. Untuk informasi selengkapnya, lihat Amazon DataZone memperbarui kebijakan AWS terkelola.	Maret 29, 2024
AmazonDataZoneFullAccess - Pembaruan kebijakan	Memperbarui `AmazonDataZoneFullAccess` untuk memungkinkan pengguna memilih rahasia, cluster, vpc, dan subnet mereka di konsol DataZone manajemen Amazon daripada mengetikn ya di kotak teks. Untuk informasi selengkapnya, lihat Amazon DataZone memperbarui kebijakan AWS terkelola.	Maret 13, 2024

AmazonDataZoneDomainExecutionRolePolicy - Pembaruan kebijakan	Memperbarui AmazonDataZoneDomainExecutionRolePolicyuntuk mengaktifkan dukungan untuk ListEnvironmentBlueprintConfigurationSummaries API yang diperlukan untuk membuat profil lingkungan dengan mengidentifikasi cetak biru mana yang diaktifkan di akun dan wilayah mana. Untuk informasi selengkapnya, lihat Amazon DataZone memperbarui kebijakan AWS terkelola.	Februari 1, 2024
AmazonDataZoneGlueManageAccessRolePolicy - Pembaruan kebijakan	Memperbarui AmazonDataZoneGlueManageAccessRolePolicyuntuk mengaktifkan dukungan untuk mode hibrida AWS Lake Formation. Untuk informasi selengkapnya, lihat Amazon DataZone memperbarui kebijakan AWS terkelola.	14 Desember 2023

AmazonDataZoneFullUserAccess dan AmazonDataZoneDomainExecutionRolePolicy - Pembaruan kebijakan	Amazon DataZone memperbarui kebijakan AmazonDataZoneFullUserAccessdan AmazonDataZoneDomainExecutionRolePolicykebijakan untuk mendukung fitur deskripsi data bertenaga AI generatif di Amazon. DataZone Untuk informasi selengkapnya, lihat Amazon DataZone memperbarui kebijakan AWS terkelola.	28 November 2023
AmazonDataZoneEnvironmentRolePermissionsBoundary - Pembaruan kebijakan	Amazon DataZone membuat pembaruan pada kebijakan AmazonDataZoneEnvironmentRolePermissionsBoundaryterkelola yang terdiri dari `athena:GetQueryResultsStream` izin tambahan yang tercakup dengan kondisi tersebut`ResourceTag` . Untuk informasi selengkapnya, lihat Amazon DataZone memperbarui kebijakan AWS terkelola.	17 November 2023

AmazonDataZoneRedshiftManageAccessRolePolicy - Pembaruan kebijakan	Amazon DataZone memperbarui AmazonDataZoneRedshiftManageAccessRolePolicykebijakan dengan menghapus cek pada ID organisasi untuk `redshift:AssociateDataShareConsumer` tindakan tersebut. Ini memungkinkan Anda untuk berbagi sumber daya di seluruh AWS organisasi. Untuk informasi selengkapnya, lihat Amazon DataZone memperbarui kebijakan AWS terkelola.	16 November 2023
AmazonDataZoneFullUserAccess - Pembaruan kebijakan	Amazon DataZone memperbarui AmazonDataZoneFullUserAccesskebijakan yang memberikan akses penuh ke Amazon DataZone, tetapi tidak mengizinkan pengelolaan domain, pengguna, atau akun terkait.Untuk informasi selengkapnya, lihat DataZone Pembaruan Amazon ke AWS kebijakan terkelola.	2 Oktober 2023
AmazonDataZonePreviewConsoleFullAccess - kebijakan usang	Amazon tidak DataZone menggunakan lagi AmazonDataZonePreviewConsoleFullAccess.Untuk informasi selengkapnya, lihat Amazon DataZone memperbarui kebijakan terkelola. AWS	September 29, 2023

AmazonDataZonePortalFullAccessPolicy - kebijakan usang	Amazon tidak DataZone menggunakan lagi AmazonDataZonePortalFullAccessPolicy .Untuk informasi selengkapnya, lihat Amazon DataZone memperbarui kebijakan terkelola. AWS	September 29, 2023
AmazonDataZoneDomainExecutionRolePolicy - Kebijakan baru	Amazon DataZone menambahkan kebijakan baru yang disebut AmazonDataZoneDomainExecutionRolePolicy. Ini adalah kebijakan default untuk peran DataZone `AmazonDataZoneDomainExecutionRole` layanan Amazon. Peran ini digunakan oleh Amazon DataZone untuk membuat katalog, menemukan, mengatur, berbagi, dan menganalisis data dalam DataZone domain Amazon. Anda dapat melampirkan `AmazonDataZoneDomainExecutionRolePolicy` kebijakan ke Anda`AmazonDataZoneDomainExecutionRole` . Untuk informasi selengkapnya, lihat Amazon DataZone memperbarui kebijakan AWS terkelola.	25 September 2023

AmazonDataZoneCrossAccountAdmin - Kebijakan baru	Amazon DataZone menambahkan kebijakan baru yang disebut AmazonDataZoneCrossAccountAdminyang memungkinkan pengguna untuk bekerja dengan Amazon DataZone dan akun terkaitnya. Untuk informasi selengkapnya, lihat Amazon DataZone memperbarui kebijakan AWS terkelola.	September 19, 2023
AmazonDataZoneRedshiftManageAccessRolePolicy - Kebijakan baru	Amazon DataZone menambahkan kebijakan baru yang disebut AmazonDataZoneRedshiftManageAccessRolePolicyyang memberikan izin untuk memungkinkan Amazon mengaktifkan penerbitan dan akses hibah DataZone ke data. Untuk informasi selengkapnya, lihat Amazon DataZone memperbarui kebijakan AWS terkelola.	12 September 2023

AmazonDataZoneRedshiftGlueProvisioningPolicy - Kebijakan baru	Amazon DataZone menambahkan kebijakan baru yang disebut AmazonDataZoneRedshiftGlueProvisioningPolicyyang memberikan Amazon izin DataZone yang diperlukan untuk berinteraksi dengan sumber data yang didukung. Untuk informasi selengkapnya, lihat Amazon DataZone memperbarui kebijakan AWS terkelola.	12 September 2023
AmazonDataZoneGlueManageAccessRolePolicy - Kebijakan baru	Amazon DataZone menambahkan kebijakan baru yang disebut AmazonDataZoneGlueManageAccessRolePolicymemberikan DataZone izin Amazon untuk mempublikasikan data AWS Glue ke katalog. Ini juga memberikan DataZone izin Amazon untuk memberikan akses atau mencabut akses ke aset yang diterbitkan AWS Glue di katalog. Untuk informasi selengkapnya, lihat Amazon DataZone memperbarui kebijakan AWS terkelola.	12 September 2023

AmazonDataZoneFull UserAccess - Kebijakan baru	Amazon DataZone menambahkan kebijakan baru yang disebut AmazonDat aZoneFullUserAccessyang memberikan akses penuh ke Amazon DataZone melalui portal data. Untuk informasi selengkapnya, lihat Amazon DataZone memperbarui kebijakan AWS terkelola.	12 September 2023
AmazonDataZoneFullAccess - Kebijakan baru	Amazon DataZone menambahkan kebijakan baru yang disebut AmazonDat aZoneFullAccessyang menyediakan akses penuh ke Amazon DataZone melalui Konsol AWS Manajemen. Untuk informasi selengkap nya, lihat Amazon DataZone memperbarui kebijakan AWS terkelola.	12 September 2023
AmazonDataZoneEnvi ronmentRolePermiss ionsBoundary - Kebijakan baru	Amazon DataZone menambahkan kebijakan baru yang disebut AmazonDat aZoneEnvironmentRo lePermissionsBoundaryyang membatasi prinsipal IAM yang disediakan yang dilampirkan. Untuk informasi selengkap nya, lihat Amazon DataZone memperbarui kebijakan AWS terkelola.	12 September 2023

Pembaruan kebijakan terkelola	Pembaruan kebijakan AmazonDataZonePrev iewConsoleFullAccess terkelola. Untuk informasi selengkapnya, lihat Amazon DataZone memperbarui kebijakan AWS terkelola.	13 Juni 2023
Pembaruan kebijakan terkelola	Pembaruan kebijakan AmazonDataZoneProj ectDeploymentPermi ssionsBoundary terkelola. Untuk informasi selengkap nya, lihat Amazon DataZone memperbarui kebijakan AWS terkelola.	3 April 2023
???	Rilis awal Panduan Pengguna Amazon DataZone (Pratinjau).	29 Maret 2023

Terjemahan disediakan oleh mesin penerjemah. Jika konten terjemahan yang diberikan bertentangan dengan versi bahasa Inggris aslinya, utamakan versi bahasa Inggris.