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 lebih mudah bagi Anda untuk membuat katalog, menemukan, berbagi, dan mengatur data yang disimpan AWS, sumber lokal, 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 AWS Glue AWS Lake Formation, 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 yang lain AWS layanan?

Amazon DataZone mendukung tiga jenis integrasi dengan yang lain AWS layanan:

- Sumber data produsen - Anda dapat mempublikasikan aset data ke DataZone katalog Amazon dari data yang disimpan AWS Glue Data Catalog 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 AWS Lake Formation dikelola AWS Glue tabel dan 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 yang lain AWS layanan 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 IAMPusat Identitas (penerus AWS SSO), atau dengan IAM kredensil Anda. Anda dapat memperoleh portal data URL dengan mengakses DataZone konsol Amazon di https://console.aws.amazon.com/datazone.

- Amazon DataZone HTTPS API

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

DataZone Terminologi dan konsep Amazon

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

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 adalah pengelompokan orang, aset (data), dan alat berbasis kasus penggunaan bisnis yang digunakan untuk menyederhanakan akses ke AWS analitik. 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 sumber daya nol atau lebih yang dikonfigurasi (misalnya, bucket Amazon S3, dan AWS Glue database, atau grup kerja Amazon Athena) di mana sekumpulan IAM prinsipal 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 IAM kredensi atau kredensi 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 mengasosiasikan tambahan AWS akun 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 SSO pengguna, SSO grup, dan IAM pengguna
  - 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, dan AWS Glue database, atau kelompok kerja Amazon Athena), dengan seperangkat IAM prinsip 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 dikerahkan.

Apa itu DataZone cetak biru Amazon?

Cetak biru yang dengannya lingkungan dibuat mendefinisikan apa AWS alat dan layanan (misalnya, AWS Glue atau Amazon Redshift) anggota proyek tempat lingkungan berada dapat digunakan saat mereka bekerja dengan aset di 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	Memberikan pengguna kemampuan untuk membuat dan menanyakan tabel Lake

Nama cetak biru	Deskripsi	Sumber daya dibuat
	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 DataZone proyek Amazon untuk membuat tabel LakeFormation terkelola baru menggunakan Amazon Athena dan mempublik asikannya ke katalog Amazon DataZone.	Formation menggunakan Amazon Athena. Kelompok kerja Amazon Athena, AWS Glue database dengan izin Formasi Danau 'hanya terbaca', izin 'hanya baca'IAM, dan akses ke Amazon S3 yang dikelola oleh proyek. AWS Glue database dengan 'buat' dan 'berikan' izin Lake Formation, izin 'baca' dan 'tulis'IAM, AWS Glue ETL(ekstrak, ubah, dan muat) dengan penandaan.

Nama cetak biru	Deskripsi	Sumber daya dibuat
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 AWS Glue database 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:

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

data 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

- Dengan menggunakanAPIs, 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 APIs. Jenis aset kustom dapat mencakup model ML, dasbor, tabel lokal, dll.
  - Buat aset dari jenis aset kustom ini menggunakan Amazon DataZone APIs.
- 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 Amazon DataZone APIs. 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 Amazon DataZone APIs.
- Sebagai bagian dari pembuatan atau pengeditan sumber data, aktifkan opsional Publikasikan AWS Glue aset 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 APIs.

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 langganan 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 yang dikelola (ini termasuk AWS Glue tabel 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 di DataZone AWS akun, buat DataZone domain Amazon, dan konfigurasikan AWS asosiasi akun dan asosiasi penyedia identitas dengan DataZone domain Amazon. Administrator domain juga menggunakan AWS Konsol layanan seperti AWS Organisasi dan 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 Infrastructure-As-Code 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 Amazon dan antarmuka pengguna internal atau sistem produksi jika diperlukan. DataZone APIs
- 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.

Satuan domain

Unit domain memungkinkan Anda untuk dengan mudah mengatur aset dan entitas domain lainnya di bawah unit bisnis dan tim tertentu. Untuk menyiapkan berbagi data yang aman dan efisien di dalam dan di seluruh unit bisnis organisasi Anda, Anda dapat membuat unit domain di Amazon DataZone dan memungkinkan pengguna terpilih dalam setiap unit bisnis untuk masuk dan membagikan aset mereka ke katalog. Unit domain juga dapat digunakan untuk mengaktifkan pemilik sumber daya, seperti AWS pemilik akun, untuk mengatur DataZone izin otorisasi Amazon pada sumber daya mereka. Unit domain memberikan wewenang yang didelegasikan dari pemilik akun ke pemilik unit domain dan mereka dapat mengatur izin otorisasi pada profil lingkungan (dibuat menggunakan konfigurasi cetak biru), atas nama pemilik akun. Untuk informasi selengkapnya, lihat Unit domain dan kebijakan otorisasi di Amazon DataZone.

Kebijakan otorisasi

Kebijakan DataZone otorisasi Amazon adalah seperangkat kontrol dalam Amazon yang DataZone diterapkan pada entitas seperti proyek, cetak biru, lingkungan, glosarium, dan formulir metadata. Kebijakan ini menentukan siapa yang dapat membuat entitas ini dan mengelola siklus hidupnya di portal Amazon DataZone.

Dalam unit DataZone domain Amazon, Anda dapat menetapkan kebijakan otorisasi berikut kepada pengguna dan grup untuk memberi mereka izin khusus:

- Kebijakan pembuatan unit domain
- Kebijakan pembuatan proyek
- Kebijakan keanggotaan proyek
- Kebijakan asumsi kepemilikan unit domain
- Kebijakan asumsi kepemilikan proyek

Untuk informasi selengkapnya, lihat Menetapkan kebijakan otorisasi untuk pengguna dan grup dalam unit domain Amazon DataZone .

Dalam unit DataZone domain Amazon, Anda dapat menetapkan kebijakan otorisasi berikut ke proyek Anda untuk memberikan izin khusus kepada mereka:

- Kebijakan pembuatan glosarium
- Kebijakan pembuatan formulir metadata
- Kebijakan pembuatan jenis aset khusus

Untuk informasi selengkapnya, lihat Menetapkan kebijakan otorisasi untuk proyek dalam unit domain Amazon DataZone .

Dalam konfigurasi cetak biru tertentu, Anda dapat menetapkan kebijakan otorisasi berikut untuk proyek dan pemilik unit domain:

- Buat profil lingkungan menggunakan cetak biru ini - kebijakan ini dapat ditetapkan ke DataZone proyek Amazon dan mengizinkan mereka untuk membuat profil lingkungan menggunakan cetak biru ini.
- Berikan izin untuk membuat profil lingkungan menggunakan cetak biru ini - kebijakan ini dapat ditetapkan ke pemilik unit domain dan memberi wewenang kepada mereka untuk memberikan izin kepada proyek untuk membuat profil lingkungan menggunakan cetak biru ini.

Untuk informasi selengkapnya, lihat Tetapkan kebijakan otorisasi dalam konfigurasi cetak biru Amazon DataZone .

Akun terkait

Mengasosiasikan Anda AWS akun dengan DataZone domain Amazon memungkinkan Anda mempublikasikan data dari ini AWS akun ke dalam DataZone katalog Amazon dan buat DataZone proyek Amazon untuk bekerja 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 yang diundang AWS akun. Sekali AWS akun dikaitkan dengan DataZone domain Amazon, Anda dapat mendaftarkan sumber data Anda seperti AWS Glue katalog dan Amazon Redshift di akun ini ke domain ini. Terkait juga memungkinkan AWS akun untuk membuat DataZone proyek dan lingkungan Amazon.

Sesi 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 AWS Glue dan Amazon Redshift. Dengan membuat sumber data, Anda membuat koneksi antara Amazon DataZone dan sumbernya (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, IAM peran) 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. Tipe 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, dan AWS Glue database, atau grup kerja Amazon Athena), dengan sekumpulan IAM prinsipal 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 AWS layanan dan eksternal IDEs dan konsol. Anggota proyek dapat mengakses layanan seperti konsol Amazon Athena dan lainnya melalui tautan dalam yang dikonfigurasi dalam suatu lingkungan. SSOpengguna dan IAM pengguna 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 apa AWS alat dan layanan (misalnya, AWS Glue atau Amazon Redshift) anggota proyek tempat lingkungan berada dapat digunakan saat mereka bekerja dengan aset di 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 IAM peran dan SSO identitas untuk berinteraksi dengan Konsol DataZone Manajemen Amazon dan portal data untuk tujuan yang berbeda. Administrator domain menggunakan IAM peran 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 SSO perusahaan 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, IAM prinsipal 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 publikasikan 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 owner

Di Amazon DataZone, Akun AWS pemilik membuat peran, kebijakan, dan izin di Akun AWS yang memungkinkan ini Akun AWS untuk dikaitkan dengan DataZone domain Amazon.

Apa yang baru di Amazon DataZone?

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

Topik

2024

Amazon DataZone meluncurkan unit domain dan kebijakan otorisasi

Dirilis pada 08/12/2024

Amazon DataZone memperkenalkan serangkaian kemampuan tata kelola data baru yang disebut unit domain dan kebijakan otorisasi yang memungkinkan pelanggan membuat organisasi unit bisnis/tingkat tim dan mengelola kebijakan sesuai kebutuhan bisnis mereka. Dengan penambahan unit domain, pengguna dapat mengatur, membuat, mencari, dan menemukan aset data dan proyek yang terkait dengan unit bisnis atau tim. Dengan kebijakan otorisasi, pengguna unit domain tersebut dapat menetapkan kebijakan akses untuk membuat proyek, glosarium, dan menggunakan sumber daya komputasi di Amazon. DataZone Untuk informasi selengkapnya, lihat Unit domain dan kebijakan otorisasi di Amazon DataZone.

Amazon DataZone meluncurkan produk data

Dirilis pada 08/05/2024

Amazon DataZone memperkenalkan produk data, yang memungkinkan pengelompokan aset data ke dalam paket mandiri yang terdefinisi dengan baik yang disesuaikan untuk kasus penggunaan bisnis tertentu. Misalnya, produk data analisis pemasaran dapat menggabungkan berbagai aset data, seperti data kampanye pemasaran, data pipa, dan data pelanggan. Dengan produk data, pelanggan dapat menyederhanakan proses penemuan dan berlangganan, menyelaraskannya dengan tujuan bisnis dan mengurangi redundansi dalam menangani aset individu. Untuk informasi lebih lanjut, lihatProduk DataZone data Amazon .

Amazon DataZone meluncurkan fungsionalitas kontrol akses berbutir halus

Dirilis pada 07/02/2024

Amazon DataZone telah memperkenalkan kontrol akses berbutir halus, memberi Anda kontrol terperinci atas aset data Anda di katalog data bisnis Amazon DataZone di seluruh danau data dan gudang data. Dengan kemampuan baru, pemilik data sekarang dapat membatasi akses ke catatan data tertentu pada tingkat baris dan kolom, alih-alih memberikan akses ke seluruh aset data. Misalnya, jika data Anda berisi kolom dengan informasi sensitif seperti Informasi Identifikasi Pribadi (PII), Anda dapat membatasi akses hanya ke kolom yang diperlukan, memastikan bahwa informasi sensitif dilindungi sambil tetap mengizinkan akses ke data yang tidak sensitif. Demikian pula, Anda dapat mengontrol akses di tingkat baris, memungkinkan pengguna untuk hanya melihat catatan yang relevan dengan peran atau tugas mereka. Untuk informasi selengkapnya, silakan lihat Kontrol akses berbutir halus ke data di Amazon DataZone

Amazon DataZone meluncurkan fungsionalitas garis keturunan data

Dirilis pada 06/27/2024

Amazon DataZone meluncurkan garis keturunan data dalam pratinjau, membantu pelanggan memvisualisasikan peristiwa garis keturunan dari sistem yang OpenLineage diaktifkan atau melalui API dan melacak pergerakan data dari sumber ke konsumsi. Menggunakan DataZone Amazon OpenLineage -compatibleAPIs, administrator domain dan produsen data dapat menangkap dan menyimpan peristiwa silsilah di luar apa yang tersedia di Amazon, termasuk transformasi di Amazon DataZone S3, AWS Glue, dan layanan lainnya. Selain itu, DataZone Amazon membuat garis keturunan dengan setiap peristiwa, memungkinkan pengguna untuk memvisualisasikan garis keturunan kapan saja atau membandingkan transformasi di seluruh aset atau riwayat pekerjaan. Garis keturunan historis ini memberikan pemahaman yang lebih dalam tentang bagaimana data telah berevolusi, penting untuk pemecahan masalah, audit, dan memvalidasi integritas aset data. Untuk informasi selengkapnya, silakan lihat Garis keturunan data di Amazon DataZone (Pratinjau)

Amazon DataZone meluncurkan kustom AWS cetak biru layanan

Dirilis pada 06/17/2024

Dengan kustom AWS cetak biru layanan, jika Anda sudah ada AWS sumber daya termasuk IAM peran, data lake, jerat data, bucket Amazon S3, dan kluster Amazon Redshift, Anda sekarang dapat menentukan izin ke sumber daya yang ada ini menggunakan IAM peran kustom Anda sendiri, sehingga pengguna DataZone Amazon Anda dapat memanfaatkan publikasi dan langganan untuk berbagi dan mengatur sumber daya ini. Dengan kustom AWS cetak biru layanan, administrator Amazon DataZone dapat mengonfigurasi AWS lingkungan layanan menggunakan peran kustom mereka sendiri. Mereka dapat mengonfigurasi tautan tindakan untuk ini AWS lingkungan layanan dan

dengan demikian menyediakan akses federasi ke salah satu yang ada AWS sumber daya. Mereka juga dapat mengonfigurasi target langganan dan sumber data dalam kustom ini AWS lingkungan layanan. Administrator dapat mengatur AWS lingkungan layanan di akun DataZone domain Amazon mereka sendiri atau di akun terkait tempat mereka ingin mempublikasikan, berlangganan, menemukan, atau mengatur data. Untuk informasi selengkapnya, lihat DataZone Kustom Amazon AWS cetak biru layanan .

Penyempurnaan aliran pembuatan sumber data

Dirilis pada 06/10/2024

Amazon DataZone telah menambahkan penyempurnaan pada alur pembuatan sumber data untuk menyederhanakan manajemen akses bagi produsen data. Dengan pembaruan ini, ketika produsen data membuat sumber data untuk mempublikasikannya AWS Glue dan aset Amazon Redshift, Amazon memberikan izin DataZone hanya-baca kepada anggota proyek. Saat membuat AWS Glue sumber data, Amazon DataZone secara otomatis memberikan izin 'hanya-baca' untuk IAM peran lingkungan yang digunakan untuk membuat sumber data, memungkinkan akses ke semua tabel di terkait AWS Basis data Glue. Demikian pula, untuk sumber data Amazon Redshift, Amazon DataZone memberikan akses 'hanya-baca' ke semua tabel dalam skema Amazon Redshift yang digunakan dalam sumber data. Untuk informasi selengkapnya, silakan lihat Membuat dan menjalankan sumber DataZone data Amazon untuk AWS Glue Data Catalog dan Membuat dan menjalankan sumber DataZone data Amazon untuk Amazon Redshift.

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, silakan lihat Cetak biru DataZone bawaan Amazon dan Akun terkait di Amazon DataZone.

Amazon DataZone meluncurkan integrasi dengan AWS Mode akses hibrida Lake Formation

Dirilis pada 04/03/2024

Amazon DataZone telah memperkenalkan integrasi dengan AWS Mode akses hibrida Lake Formation. Integrasi ini memungkinkan Anda untuk dengan mudah mempublikasikan dan berbagi AWS Glue tabel melalui Amazon DataZone, tanpa perlu mendaftarkannya AWS Lake Formation terlebih dahulu. Untuk memulai, administrator mengaktifkan pengaturan pendaftaran lokasi data di bawah `DefaultDataLake` cetak biru di konsol Amazon. DataZone Kemudian, ketika konsumen data berlangganan AWS Glue table dikelola melalui IAM izin, Amazon DataZone pertama-tama mendaftarkan lokasi Amazon S3 dari tabel ini dalam mode hybrid, dan kemudian memberikan akses ke konsumen data dengan mengelola izin pada tabel melalui AWS Formasi Danau. Ini memastikan bahwa IAM izin pada tabel terus ada dengan yang baru diberikan AWS Izin Lake Formation, tanpa mengganggu alur kerja yang ada. Untuk informasi selengkapnya, lihat DataZone Integrasi Amazon dengan AWS Mode hibrida Lake Formation .

Amazon DataZone meluncurkan integrasi dengan AWS Kualitas Data Glue

Dirilis pada 04/03/2024

Amazon DataZone meluncurkan integrasi dengan AWS Glue Data Quality dan menawarkan APIs untuk mengintegrasikan metrik kualitas data dari solusi kualitas data pihak ketiga. Integrasi baru memungkinkan Anda untuk mempublikasikan secara otomatis AWS Glue Data Quality skor ke dalam katalog data DataZone bisnis Amazon. Amazon DataZone APIs dapat digunakan untuk menelan 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 produsen data APIs yang dapat digunakan 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, perangkat tambahan ini memberikan administrator kontrol yang lebih besar atas siapa yang dapat menggunakan sumber daya di dalamnya AWS akun dan cluster 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 Rahasia. 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 secret hanya membutuhkan `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 Rahasia, 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 secara efektif memodelkan dan mengelola serangkaian DataZone sumber daya Amazon. 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 IAM prinsipal secara langsung sebagai anggota proyek Amazon DataZone

Dirilis pada 01/05/2024

Anda sekarang dapat menambahkan IAM prinsipal sebagai anggota proyek, bahkan jika IAM prinsipal 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 IAM prinsipal sebagai anggota hanya dengan memberikan Amazon Resouce Name (ARN) peran atau pengguna. IAM IAM IAMKepala sekolah masih harus memiliki IAM izin yang diperlukan untuk mengakses Amazon DataZone dan yang dapat dikonfigurasi di IAM konsol. 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 yang tersedia sebelumnya. API 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 DataZone domain Amazon.

Mode hibrida

Dirilis pada 12/22/2023

Amazon DataZone telah menambahkan dukungan untuk AWS Mode hibrida Lake Formation. Dengan dukungan ini, jika Anda mempublikasikan AWS Glue tabel ke Amazon DataZone dengan miliknya AWS Lokasi S3 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.

HIPAAkelayakan

Dirilis pada 12/14/2023

Amazon DataZone sekarang mematuhi Undang-Undang Portabilitas dan Akuntabilitas Asuransi Kesehatan AS tahun 1996 ()HIPAA. Untuk melihat daftar AWS layanan dengan HIPAA kepatuhan 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 sebagai berikut AWS Wilayah: AS Timur (Virginia N.), AS Barat (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 Anda AWS akun. 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.

Menyiapkan Amazon DataZone

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

Setelah Anda mengatur DataZone izin Amazon Anda, Anda disarankan untuk menyelesaikan langkah-langkah di bagian Memulai yang membawa Anda melalui pembuatan DataZone domain Amazon, mendapatkan portal dataURL, 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 untuk AWS akun

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

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

Ketika Anda mendaftar untuk AWS akun, sebuah AWS pengguna root 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 IAM izin yang diperlukan untuk menggunakan konsol DataZone manajemen Amazon

Untuk mengakses dan mengonfigurasi DataZone domain, cetak biru, dan pengguna Amazon Anda, serta untuk membuat portal DataZone data Amazon, Anda harus menggunakan konsol manajemen Amazon. DataZone

Anda harus menyelesaikan prosedur berikut untuk mengonfigurasi izin yang diperlukan dan/atau opsional untuk pengguna, grup, atau peran apa pun yang ingin menggunakan konsol DataZone manajemen Amazon.

Prosedur untuk mengatur IAM izin untuk menggunakan konsol manajemen

- Lampirkan kebijakan wajib dan opsional ke pengguna, grup, atau peran untuk akses DataZone konsol Amazon
- Membuat kebijakan khusus untuk IAM izin 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 AWS Izin Pusat Identitas untuk menambah dan menghapus akses SSO pengguna dan SSO grup ke domain Amazon DataZone
- (Opsional) Tambahkan IAM prinsipal Anda sebagai pengguna utama untuk membuat DataZone domain Amazon Anda dengan kunci yang dikelola pelanggan dari AWS Layanan Manajemen Kunci (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 IAM konsol 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 IAM izin guna mengaktifkan pembuatan peran disederhanakan konsol DataZone layanan Amazon.
   - (Opsional) Buat kebijakan khusus untuk AWS Izin Pusat Identitas untuk menambah dan menghapus akses SSO pengguna dan SSO grup ke DataZone domain Amazon Anda.
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 IAM izin untuk mengaktifkan pembuatan peran yang disederhanakan konsol DataZone layanan Amazon

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

1. Masuk ke AWS Management Console dan buka IAM konsol 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 JSON pernyataan 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 inline kustom agar memiliki izin yang diperlukan di terkait AWS akun 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 IAM izin untuk mengaktifkan pembuatan peran yang disederhanakan konsol DataZone layanan Amazon

1. Masuk ke AWS Management Console dan buka IAM konsol 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 JSON pernyataan 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 AWS Izin Pusat Identitas untuk menambah dan menghapus akses SSO pengguna dan SSO grup ke domain Amazon DataZone

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

1. Masuk ke AWS Management Console dan buka IAM konsol 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 JSON pernyataan 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 IAM prinsipal Anda sebagai pengguna utama untuk membuat DataZone domain Amazon Anda dengan kunci yang dikelola pelanggan dari AWS Layanan Manajemen Kunci (KMS)

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

1. Masuk ke AWS Management Console dan buka KMS konsol 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 KMS kunci, pilih alias atau ID kunci dari KMS kunci yang ingin Anda periksa.
4. Untuk menambah atau menghapus pengguna kunci, dan untuk mengizinkan atau melarang eksternal AWS akun untuk menggunakan KMS kunci, gunakan kontrol di bagian Pengguna kunci halaman. Pengguna kunci dapat menggunakan KMS kunci dalam operasi kriptografi, seperti mengenkripsi, mendekripsi, mengenkripsi ulang, dan menghasilkan kunci data.

Konfigurasikan IAM izin yang diperlukan untuk menggunakan portal DataZone data Amazon

Portal DataZone data Amazon (di luar AWS Management Console) adalah aplikasi web berbasis browser tempat pengguna dapat membuka katalog, menemukan, mengatur, berbagi, dan menganalisis data dengan cara swalayan. Portal data mengautentikasi pengguna dengan IAM kredensi atau kredensi yang ada dari penyedia identitas Anda melalui AWS IAMPusat Identitas.

Anda harus menyelesaikan prosedur berikut untuk mengonfigurasi izin yang diperlukan untuk pengguna, grup, atau peran apa pun yang ingin menggunakan portal atau katalog DataZone data Amazon:

Prosedur untuk mengkonfigurasi IAM izin untuk menggunakan portal data

- 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 AWS Layanan Manajemen 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 salah satu AWS kredensial atau kredensial sign-on () tunggal Anda. SSO Ikuti petunjuk di bagian di bawah ini untuk

mengatur izin yang diperlukan untuk mengakses portal data dengan Anda AWS kredensialnya. Untuk informasi selengkapnya tentang menggunakan Amazon DataZone denganSSO, lihatPengaturan AWS IAMPusat Identitas untuk Amazon DataZone.

> **Note**
>
> Hanya IAM prinsipal di domain Anda AWS akun dapat mengakses portal data domain. IAMprinsipal dari yang lain AWS akun 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 IAM konsol 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 JSON pernyataan 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 IAM prinsipal di domain Anda AWS akun dapat mengakses katalog domain. IAMprinsipal dari yang lain AWS akun tidak dapat mengakses katalog domain.

Anda dapat memberikan IAM identitas Anda akses ke katalog DataZone domain Amazon Anda melalui API dan SDK dengan prosedur berikut. Jika Anda ingin IAM identitas ini juga memiliki akses ke portal DataZone data Amazon, ikuti juga prosedur di atas untukLampirkan 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 IAM konsol 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, silakan 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 AWS Layanan Manajemen Kunci (KMS)

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

1. Masuk ke AWS Management Console dan buka IAM konsol 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 JSON pernyataan 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.

Pengaturan AWS IAMPusat Identitas untuk Amazon DataZone

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

Anda dapat mengakses portal DataZone data Amazon dengan menggunakan kredensi single sign-on (SSO) atau AWS kredensialnya. Ikuti petunjuk di bagian ini untuk mengatur AWS IAMPusat Identitas untuk Amazon DataZone. Untuk informasi lebih lanjut tentang menggunakan Amazon DataZone dengan AWS kredensialnya, lihat. Konfigurasikan IAM izin yang diperlukan untuk menggunakan konsol DataZone manajemen Amazon

Anda dapat melewati prosedur di bagian ini jika Anda sudah memiliki AWS IAMPusat Identitas (penerus AWS Single Sign-On) diaktifkan dan dikonfigurasi dalam hal yang sama AWS wilayah tempat Anda ingin membuat DataZone domain Amazon Anda.

Selesaikan prosedur berikut untuk mengaktifkan AWS IAMPusat Identitas (penerus AWS Masuk Tunggal).

1. Untuk mengaktifkan AWS IAMPusat Identitas, Anda harus masuk ke AWS Management Console dengan menggunakan kredensi AWS Akun manajemen organisasi. Anda tidak dapat mengaktifkan Pusat IAM Identitas saat masuk dengan kredensi dari AWS Akun anggota Organizations. Untuk informasi selengkapnya, lihat Membuat dan mengelola organisasi di AWS Panduan Pengguna Organizations.
2. Buka AWS IAMPusat Identitas (penerus AWS Konsol Single Sign-On) dan gunakan pemilih wilayah di bilah navigasi atas untuk memilih AWS wilayah di mana Anda ingin membuat DataZone domain Amazon Anda.
3. Pilih Aktifkan.
4. Pilih sumber identitas Anda.

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

   Untuk informasi selengkapnya, lihat Memilih sumber identitas Anda.

5. Di panel navigasi Pusat IAM Identitas, pilih Grup, dan pilih Buat grup. Masukkan nama grup dan pilih Buat.
6. Di panel navigasi Pusat IAM Identitas, 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 menggunakannyaSSO. Dalam email ini, mereka harus memilih Terima undangan dan mengatur kata sandi.

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

Memulai dengan Amazon DataZone

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

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 merek baru AWS akun, Anda harus mengonfigurasi izin yang diperlukan untuk menggunakan konsol DataZone manajemen Amazon. Jika Anda menggunakan sebuah AWS Akun yang sudah ada AWS Glue Data Catalog objek, Anda juga harus mengkonfigurasi izin Lake Formation ke Amazon DataZone.

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

Topik

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

Amazon DataZone mulai cepat dengan AWS Glue data

Selesaikan langkah-langkah mulai cepat berikut untuk menjalankan alur kerja produsen data dan konsumen data lengkap di Amazon DataZone dengan sampel AWS Glue data.

Langkah mulai cepat

- Langkah 1 - Buat DataZone domain Amazon dan portal data
- Langkah 2 - Buat proyek penerbitan
- Langkah 3 - Buat lingkungan
- Langkah 4 - Menghasilkan data untuk penerbitan
- Langkah 5 - Kumpulkan metadata dari AWS Glue
- 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 terkelola pelanggan, lihatEnkripsi data saat istirahat untuk Amazon DataZone. Jika Anda menggunakan KMS kunci Anda sendiri untuk enkripsi data, Anda harus menyertakan pernyataan berikut dalam default AndaAmazonDataZoneDomainExecutionRole.

```
{
  "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 portal Data URL untuk domain ini. Anda dapat menggunakan ini URL 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, yang URL 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 - Buat 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 Katalog Glue, 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 CTAS skrip 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 AWS Glue

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

Selesaikan langkah-langkah mulai cepat berikut untuk menjalankan alur kerja produsen data dan konsumen data lengkap di Amazon DataZone dengan contoh data Amazon Redshift.

Langkah mulai cepat

- Langkah 1 - Buat DataZone domain Amazon dan portal data
- Langkah 2 - Buat proyek penerbitan
- Langkah 3 - Buat lingkungan
- Langkah 4 - Menghasilkan data untuk penerbitan

- Langkah 5 - Kumpulkan metadata dari Amazon Redshift
- 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 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 terkelola pelanggan, lihatEnkripsi data saat istirahat untuk Amazon DataZone. Jika Anda menggunakan KMS kunci Anda sendiri untuk enkripsi data, Anda harus menyertakan pernyataan berikut dalam default AndaAmazonDataZoneDomainExecutionRole.

```
{
  "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 portal Data URL untuk domain ini. Anda dapat menggunakan ini URL 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, yang URL 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 portal data URL dan masuk menggunakan single sign-on () SSO atau AWS IAMkredensi.
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 - Buat 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 rahasia ARN 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 CTAS skrip 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 rahasia ARN 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

Anda dapat mengakses Amazon DataZone melalui portal manajemen atau portal DataZone data Amazon, atau secara terprogram dengan menggunakan Amazon DataZone HTTPSAPI, yang memungkinkan Anda mengeluarkan HTTPS permintaan langsung ke layanan. Bagian ini berisi contoh skrip yang memanggil Amazon DataZone APIs yang dapat Anda gunakan untuk menyelesaikan tugas-tugas umum berikut:

Contoh skrip

- Buat DataZone domain Amazon dan portal data
- Buat proyek penerbitan
- Buat profil lingkungan
- Buat lingkungan
- Kumpulkan metadata dari AWS Glue
- 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.

Muatan sampel 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"]
            }
        ]
    }
}
```

Skrip contoh 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 AWS Glue

Anda dapat menggunakan skrip contoh ini untuk mengumpulkan metadata AWS Glue. Script ini berjalan pada jadwal standar. Anda dapat mengambil parameter dari skrip sampel dan membuatnya global. Ambil proyek, lingkungan, dan ID domain menggunakan fungsi standar. Bagian AWS Sumber data 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
```

Domain dan akses pengguna di Amazon DataZone

Bagian ini menjelaskan bagaimana Anda dapat membuat dan mengelola domain dan akses pengguna di Amazon DataZone.

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.

Bagian ini juga menjelaskan pengelolaan akses pengguna ke DataZone konsol Amazon dan portal Amazon DataZone.

Untuk informasi selengkapnya, lihat DataZone Terminologi dan konsep Amazon.

Topik

Buat DataZone domain Amazon

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

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 IAM berperan dalam akun dengan izin administratif. Konfigurasikan IAM izin yang diperlukan untuk menggunakan konsol DataZone manajemen Amazonuntuk mendapatkan izin minimum yang diperlukan untuk membuat domain.

IAMPeran tambahan diperlukan oleh Amazon DataZone untuk melakukan tindakan atas nama pengguna domain dengan konfigurasi default. Anda dapat membuat IAM peran ini sebelumnya, atau meminta Amazon DataZone membuatnya untuk Anda. Jika Anda DataZone ingin Amazon membuat IAM peran ini untuk Anda selama proses pembuatan domain, maka untuk pembuatan domain Anda harus mengambil IAM peran dengan izin pembuatan peran. Lihat Membuat kebijakan khusus untuk IAM izin untuk mengaktifkan pembuatan peran yang disederhanakan konsol DataZone layanan Amazon . Bergantung pada pilihan pembuatan domain Anda, Amazon DataZone akan membuat hingga empat IAM peran baru untuk Anda: AmazonDataZoneDomainExecutionRole, AmazonDataZoneGlueManageAccessRole, AmazonDataZoneRedshiftManageAccessRole, 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 yang sesuai AWS Wilayah.
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 AWS Layanan Manajemen Kunci (KMS) menggunakan kunci khusus untuk Amazon Anda DataZone. Gunakan bidang ini untuk menentukan apakah Anda ingin menggunakan AWS memiliki kunci atau memilih yang berbeda AWS KMSkunci.

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

```
{
  "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 IAM peran 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 IAM peran untuk penyediaan, menelan, dan mengelola akses ke AWS Glue dan sumber daya Amazon Redshift, buat bucket Amazon S3 baru, buat proyek DataZone Amazon administratif, dan buat profil lingkungan untuk cetak biru default data lake dan gudang data.
- 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 DataZone domain Amazon

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 IAM Identitas, dan menambahkan, mengedit, atau menghapus kunci tag dan nilainya. Untuk mengedit DataZone domain Amazon, Anda harus IAM berperan dalam akun dengan izin administratif. Konfigurasikan IAM izin yang diperlukan untuk menggunakan konsol DataZone manajemen Amazonuntuk mendapatkan izin minimum yang diperlukan untuk mengedit domain.

Untuk mengedit domain, selesaikan langkah-langkah berikut:

1. Masuk ke AWS Management Console dan buka DataZone konsol Amazon di https://console.aws.amazon.com/datazone.
2. Pilih Lihat domain dan pilih nama domain dari daftar. Namanya adalah hyperlink.
3. Pada halaman detail untuk domain, pilih Edit.
4.
   - Edit Deskripsi.
   - Atur pengaturan Pusat IAM Identitas. Pelajari lebih lanjut tentang pengaturan ini diPengaturan AWS IAMPusat Identitas untuk Amazon DataZone.
   - Tambahkan, edit, atau hapus kunci Tag dan nilainya.
5. Setelah Anda melakukan pengeditan, pilih Perbarui domain.

Hapus DataZone domain Amazon

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 non-Amazon DataZone AWS sumber daya yang DataZone mungkin telah dibantu Amazon Anda buat, seperti IAM peran, bucket S3, AWS Glue database, dan hibah berlangganan melalui atau LakeFormation Redshift. Jika Anda tidak lagi membutuhkan sumber daya ini, hapus di masing-masing AWS layanan.

Untuk mencegah seseorang menghapus domain secara jahat, menghapus domain memerlukan izin administratif IAM untuk Amazon DataZone, yang dapat Anda konfigurasikan. 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 AWS Management Console dan buka DataZone konsol Amazon di https://console.aws.amazon.com/datazone.
2. Pilih Lihat domain dan pilih nama domain dari daftar. Namanya adalah 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 Anda membuat lingkungan dalam sebuah proyek, Amazon DataZone membuat AWS sumber daya di domain Anda atau akun terkait untuk memberi Anda dan pengguna domain Anda fungsionalitas. Di bawah ini adalah daftar AWS sumber daya yang DataZone dapat dibuat Amazon untuk proyek di domain Anda, bersama dengan nama defaultnya. Menghapus domain tidak menghapus semua ini AWS sumber daya di Anda AWS akun.
>
> - IAMperan: environmentId datazone_usr_< >.
> - Basis data Glue: (1) < environmentName >_pub_db-*, (2) < >_sub_db-*. environmentName Jika sudah ada database nama ini, Amazon DataZone akan menambahkan ID lingkungan.
> - Kelompok kerja Athena: < >-*. environmentName Jika sudah ada workgroup nama ini, Amazon DataZone akan menambahkan ID lingkungan.
> - CloudWatch grup log: environmentId datazone_< >

Aktifkan Pusat IAM Identitas untuk Amazon DataZone

> **Note**
>
> Untuk menyelesaikan prosedur ini, Anda harus memiliki AWS IAMPusat Identitas diaktifkan dalam hal yang sama AWS Wilayah sebagai DataZone domain Amazon Anda.

Anda dapat memberi SSO pengguna dan grup akses ke portal DataZone data Amazon Anda menggunakan AWS IAMPusat Identitas. Setelah selesaiPengaturan AWS IAMPusat Identitas untuk

Amazon DataZone, Anda dapat mengaktifkan SSO pengguna dan grup untuk mengakses portal data DataZone domain Amazon Anda.

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

Selesaikan prosedur berikut untuk mengaktifkan AWS IAMPusat Identitas 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 adalah hyperlink.
3. Pada halaman detail untuk domain, pilih Edit.
   - Pilih kotak centang untuk Aktifkan pengguna di Pusat IAM Identitas.
   - 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 IAM Identitas Anda dapat mengakses domain Amazon DataZone Anda.
     - Dengan penetapan pengguna eksplisit, Anda akan menambahkan pengguna atau grup tertentu dari direktori Pusat IAM Identitas Anda untuk memberi mereka akses ke domain Amazon DataZone Anda. 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 IAM Identitas untuk Amazon DataZone

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

> **Note**
>
> Menonaktifkan Pusat IAM Identitas tidak akan menghentikan penagihan untuk pengguna. SSO Untuk menghentikan penagihan SSO pengguna, 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 SSO pengguna dan grup akses ke portal DataZone data Amazon Anda menggunakan AWS IAMPusat Identitas. Jika Anda telah mengaktifkan AWS IAMPusat Identitas untuk Amazon DataZone, Anda nantinya dapat menonaktifkan akses untuk semua pengguna.

Untuk menonaktifkan AWS IAMPusat Identitas untuk digunakan dengan DataZone domain Amazon Anda, Anda harus IAM berperan dalam akun dengan izin administratif. Konfigurasikan IAM izin yang diperlukan untuk menggunakan konsol DataZone manajemen Amazondan Membuat kebijakan khusus untuk IAM izin untuk mengaktifkan pembuatan peran yang disederhanakan konsol DataZone layanan Amazon untuk mendapatkan izin minimum yang diperlukan untuk menonaktifkan Pusat IAM Identitas dari penggunaan dengan Amazon DataZone.

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

Kelola pengguna di DataZone konsol Amazon

Pengguna Anda dapat mengakses portal DataZone data Amazon dengan menggunakan salah satu AWS kredensial atau kredensial sign-on () tunggal. SSO Untuk mengelola pengguna di DataZone konsol Amazon untuk DataZone domain Amazon, Anda harus IAM berperan dalam akun dengan izin administratif. Konfigurasikan IAM izin yang diperlukan untuk menggunakan konsol DataZone manajemen Amazonuntuk mendapatkan izin minimum yang diperlukan untuk mengelola pengguna di DataZone konsol Amazon.

Topik

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

Kelola IAM peran dan pengguna

IAMperan dan pengguna dibuat menggunakan AWS Identity and Access Management (IAM) dan dapatkan akses ke DataZone domain Amazon Anda melalui izin yang dilampirkan padanya melalui kebijakan. Untuk informasi selengkapnya, lihat Konfigurasikan IAM izin yang diperlukan untuk menggunakan portal DataZone data Amazon. Dalam rilis Amazon saat ini DataZone, administrator dari akun pemilik DataZone domain Amazon, dapat membuat profil IAM pengguna untuk pengguna di akun mereka sendiri atau untuk pengguna di akun terkait. Administrator dari akun pemilik DataZone domain Amazon juga dapat menyetel status pengguna yang ada ke Ditugaskan atau Tidak Ditugaskan (seperti yang ditetapkan atau tidak ditetapkan untuk menggunakan Amazon DataZone) atau mengaktifkan atau menonaktifkan pengguna yang ada.

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 adalah hyperlink.
3. Pada halaman detail untuk domain, pilih Manajemen pengguna.
4. Untuk menambahkan pengguna IAM pengguna di akun pemilik DataZone domain Amazon atau di akun terkait, pilih Tambah, lalu pilih Tambah IAM pengguna.
5. Pada halaman Tambah pengguna, pilih Akun saat ini atau Akun Terkait, gunakan bidang Temukan dan tambahkan pengguna atau peran untuk menemukan pengguna yang ingin Anda tambahkan, lalu pilih Tambah pengguna.

6. Untuk melihat status IAM pengguna yang ada, pada halaman Manajemen pengguna, pilih IAMPengguna di menu tarik-turun tipe pengguna.

   - Kolom Nama ARN menunjukkan IAM pengguna atau peran.
   - Kolom Status menunjukkan status IAM pengguna atau peran saat ini di domain.
     - Ditugaskan berarti bahwa IAM pengguna telah ditugaskan untuk menggunakan Amazon DataZone.
     - Tidak ditetapkan berarti bahwa IAM pengguna telah tidak ditetapkan untuk menggunakan Amazon. DataZone
     - Aktif berarti bahwa IAM pengguna atau peran telah memanggilAPI, mengeluarkan perintah (melalui Antarmuka Baris Perintah), atau mengakses DataZone portal Amazon untuk domain Anda, dan Anda ditagih untuk langganan pengguna.
     - Dinonaktifkan berarti bahwa IAM pengguna atau peran memiliki akses mereka diblokir ke DataZone domain Amazon Anda.
7. Untuk menonaktifkan IAM pengguna 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.
8. Untuk mengaktifkan IAM pengguna 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 IAM pengguna atau peran memiliki izin yang sesuai. Penagihan untuk pengguna akan dimulai lagi.

Kelola SSO pengguna

SSOpengguna dibuat atau disinkronkan dengan penyedia identitas Anda di AWS IAMPusat Identitas. Untuk informasi selengkapnya, lihat Pengaturan AWS IAMPusat Identitas untuk Amazon DataZone dan Aktifkan Pusat IAM Identitas untuk Amazon DataZone untuk mengaktifkan dan mengkonfigurasi AWS IAMPusat Identitas untuk Amazon DataZone. Anda dapat melihat daftar SSO pengguna yang ditetapkan ke domain, menambahkan SSO pengguna, dan menghapus SSO pengguna.

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 adalah hyperlink.
3. Pada halaman detail untuk domain, gulir ke bawah dan pilih Manajemen pengguna.

4. Untuk jenis pengguna, pilih SSOPengguna untuk melihat daftar SSO pengguna saat ini.

   - Kolom Nama menunjukkan nama SSO pengguna.
   - Kolom Status menunjukkan status SSO pengguna saat ini di domain.
     - Ditugaskan berarti bahwa SSO pengguna 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 SSO pengguna telah mengakses DataZone portal Amazon untuk domain dan Anda ditagih untuk langganan pengguna. Aktivasi terjadi secara otomatis.
     - Dinonaktifkan berarti bahwa akses SSO pengguna diblokir ke portal data domain. Penagihan untuk pengguna berakhir pada akhir bulan di mana akses mereka dinonaktifkan.
     - Dihapus berarti bahwa SSO pengguna sebelumnya ditugaskan ke domain, tetapi dihapus sebelum diakses.
5. Tambahkan SSO pengguna 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 SSO pengguna 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 SSO pengguna 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 SSO pengguna yang 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 SSO grup

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

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 adalah hyperlink.
3. Pada halaman detail untuk domain, gulir ke bawah dan pilih Manajemen pengguna.
4. Untuk jenis pengguna, pilih SSOGrup untuk melihat daftar SSO grup saat ini.
   - Kolom Nama menunjukkan nama SSO grup.
   - Kolom Status menunjukkan status SSO grup saat ini di domain.
     - Ditugaskan berarti bahwa SSO grup telah secara eksplisit ditugaskan ke domain. Akibatnya, semua pengguna dalam grup memiliki akses ke portal data domain (kecuali pengguna dinonaktifkan).
     - Tidak Ditugaskan berarti bahwa SSO grup telah dihapus dari domain. Pengguna dalam grup tidak memiliki akses ke portal data domain melalui keanggotaan mereka di grup ini.
5. Tambahkan SSO grup 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 SSOgrup 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.

Kelola izin pengguna di portal DataZone data Amazon

Dalam rilis Amazon saat ini DataZone, mekanisme otorisasi default memungkinkan semua pengguna (IAMdanSSO) DataZone domain Amazon yang diautentikasi 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.

Unit domain dan kebijakan otorisasi di Amazon DataZone

Unit domain memungkinkan Anda untuk dengan mudah mengatur aset dan entitas domain lainnya di bawah unit bisnis dan tim tertentu. Untuk menyiapkan berbagi data yang aman dan efisien di dalam dan di seluruh unit bisnis organisasi Anda, Anda dapat membuat unit domain di Amazon DataZone dan memungkinkan pengguna terpilih dalam setiap unit bisnis untuk masuk dan membagikan aset mereka ke katalog. Pengguna dari mana saja di perusahaan dapat dengan mudah mencari aset di bawah unit bisnis tersebut dan meminta akses ke aset tersebut. Unit domain juga dapat digunakan untuk mengaktifkan pemilik sumber daya, seperti AWS pemilik akun, untuk mengatur DataZone izin otorisasi Amazon pada sumber daya mereka. Unit domain memberikan wewenang yang didelegasikan dari pemilik akun ke pemilik unit domain dan mereka dapat mengatur izin otorisasi pada profil lingkungan (dibuat menggunakan konfigurasi cetak biru), atas nama pemilik akun. Ini memungkinkan Anda untuk dengan mudah membatasi siapa yang dapat membuat dan menggunakan profil lingkungan mana tergantung pada unit bisnis tempat mereka berada. Izin DataZone otorisasi Amazon juga dapat digunakan untuk menegakkan standar metadata dan hanya mengaktifkan proyek yang dipilih untuk membuat formulir dan glosarium metadata. Ini dapat membantu mempertahankan metadata yang konsisten dan berkualitas. Untuk informasi selengkapnya, lihat DataZone Terminologi dan konsep Amazon.

Dalam unit DataZone domain Amazon, Anda dapat menetapkan kebijakan otorisasi berikut kepada pengguna dan grup untuk memberi mereka izin khusus:

- Kebijakan pembuatan unit domain
- Kebijakan pembuatan proyek
- Kebijakan keanggotaan proyek
- Kebijakan asumsi kepemilikan unit domain
- Kebijakan asumsi kepemilikan proyek

Untuk informasi selengkapnya, lihat Menetapkan kebijakan otorisasi untuk pengguna dan grup dalam unit domain Amazon DataZone .

Dalam unit DataZone domain Amazon, Anda dapat menetapkan kebijakan otorisasi berikut ke proyek Anda untuk memberikan izin khusus kepada mereka:

- Kebijakan pembuatan glosarium
- Kebijakan pembuatan formulir metadata

- Kebijakan pembuatan jenis aset khusus

Untuk informasi selengkapnya, lihat Menetapkan kebijakan otorisasi untuk proyek dalam unit domain Amazon DataZone .

Cara lain untuk menggunakan mekanisme otorisasi di Amazon DataZone adalah dengan menerapkan kebijakan otorisasi untuk proyek dan pemilik unit domain dalam konfigurasi DataZone cetak biru Amazon.

Konfigurasi DataZone cetak biru Amazon adalah entitas yang merangkum informasi yang diperlukan untuk membuat dan mengonfigurasi sumber daya yang digunakan dalam menerbitkan dan berlangganan alur kerja pengguna. Informasi ini termasuk AWS nomor akun dan wilayah, CFN template, parameter tingkat akun seperti VPCs dan subnet, dan juga dapat berisi informasi koneksi database dan kredensil. Untuk mengontrol biaya dan meningkatkan keamanan, pengguna platform data memerlukan kemampuan untuk mengontrol siapa yang dapat menggunakan cetak biru ini dan menciptakan lingkungan.

Dalam konfigurasi cetak biru tertentu, Anda dapat menetapkan kebijakan otorisasi berikut untuk proyek dan pemilik unit domain:

- Buat profil lingkungan menggunakan cetak biru ini - kebijakan ini dapat ditetapkan ke DataZone proyek Amazon dan mengizinkan mereka untuk membuat profil lingkungan menggunakan cetak biru ini.
- Berikan izin untuk membuat profil lingkungan menggunakan cetak biru ini - kebijakan ini dapat ditetapkan ke pemilik unit domain dan memberi wewenang kepada mereka untuk memberikan izin kepada proyek untuk membuat profil lingkungan menggunakan cetak biru ini.

Untuk informasi selengkapnya, lihat Tetapkan kebijakan otorisasi dalam konfigurasi cetak biru Amazon DataZone .

Topik

- Buat unit domain di Amazon DataZone
- Edit unit domain di Amazon DataZone
- Hapus unit domain di Amazon DataZone
- Kelola pemilik unit domain di Amazon DataZone
- Menetapkan kebijakan otorisasi untuk pengguna dan grup dalam unit domain Amazon DataZone

- Menetapkan kebijakan otorisasi untuk proyek dalam unit domain Amazon DataZone
- Tetapkan kebijakan otorisasi dalam konfigurasi cetak biru Amazon DataZone

Buat unit domain di Amazon DataZone

Di Amazon DataZone, unit domain memungkinkan Anda mengatur aset dan entitas domain lainnya di bawah unit bisnis dan tim tertentu. Untuk informasi selengkapnya, lihat DataZone Terminologi dan konsep Amazon.

Untuk membuat unit domain

1. Arahkan ke portal DataZone data Amazon menggunakan portal data URL dan masuk menggunakan SSO atau AWS kredensil. Jika Anda DataZone administrator Amazon, Anda dapat memperoleh portal data URL dengan mengakses DataZone konsol Amazon di https://console.aws.amazon.com/datazone di AWS akun tempat DataZone domain Amazon dibuat.
2. Pilih Lihat domain dan pilih domain tempat Anda ingin membuat unit domain.
3. Pada halaman detail domain, navigasikan ke tab Unit domain.
4. Pilih Buat unit domain.
5. Tentukan yang berikut dan kemudian pilih Buat unit domain:
   - Di bawah Rincian unit domain, untuk Nama, tentukan nama unit domain.
   - Di bawah Rincian unit domain, untuk Deskripsi, tentukan deskripsi unit domain.
   - Induk unit domain - pilih unit domain induk di mana Anda ingin menambahkan unit domain baru.
   - Pemilik unit domain - tentukan pemilik unit domain yang dapat mengedit unit domain ini.

Edit unit domain di Amazon DataZone

Di Amazon DataZone, unit domain memungkinkan Anda mengatur aset dan entitas domain lainnya di bawah unit bisnis dan tim tertentu. Untuk informasi selengkapnya, lihat DataZone Terminologi dan konsep Amazon.

Untuk mengedit unit domain

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

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

2. Pilih Lihat domain dan pilih domain tempat Anda ingin mengedit unit domain.
3. Pada halaman detail domain, navigasikan ke tab Unit domain dan pilih unit domain yang ingin Anda edit.
4. Perluas Tindakan dan pilih Edit unit domain.
5. Buat perubahan pada nama dan deskripsi unit domain, lalu pilih Simpan perubahan.

Hapus unit domain di Amazon DataZone

Di Amazon DataZone, unit domain memungkinkan Anda mengatur aset dan entitas domain lainnya di bawah unit bisnis dan tim tertentu. Untuk informasi selengkapnya, lihat DataZone Terminologi dan konsep Amazon.

Untuk mengedit unit domain

1. Arahkan ke portal DataZone data Amazon menggunakan portal data URL dan masuk menggunakan SSO atau AWS kredensil. Jika Anda DataZone administrator Amazon, Anda dapat memperoleh portal data URL dengan mengakses DataZone konsol Amazon di https://console.aws.amazon.com/datazone di AWS akun tempat DataZone domain Amazon dibuat.
2. Pilih Lihat domain dan pilih domain tempat Anda ingin menghapus unit domain.
3. Pada halaman detail domain, navigasikan ke tab Unit domain dan pilih unit domain yang ingin Anda hapus.
4. Perluas Tindakan dan pilih Hapus unit domain.
5. Di jendela pop up Hapus unit domain, konfirmasikan penghapusan dengan memilih Hapus unit domain.

Kelola pemilik unit domain di Amazon DataZone

Di Amazon DataZone, unit domain memungkinkan Anda mengatur aset dan entitas domain lainnya di bawah unit bisnis dan tim tertentu. Untuk informasi selengkapnya, lihat DataZone Terminologi dan konsep Amazon.

Untuk menambahkan pemilik ke unit domain tingkat atas melalui konsol DataZone manajemen Amazon, selesaikan langkah-langkah berikut.

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 DataZone domain Amazon tempat Anda ingin menambahkan pemilik unit domain.
3. Pada halaman detail domain, navigasikan ke tab Pemilik root domain.
4. Pilih Tambah, lalu di jendela pop up Tambahkan pemilik unit domain, tentukan pengguna yang ingin Anda jadikan pemilik unit domain. Pilih Tambah pemilik.

Untuk menambahkan pemilik unit domain melalui Portal DataZone Data Amazon, selesaikan prosedur berikut:

1. Arahkan ke portal DataZone data Amazon menggunakan portal data URL dan masuk menggunakan SSO atau AWS kredensil. Jika Anda DataZone administrator Amazon, Anda dapat memperoleh portal data URL dengan mengakses DataZone konsol Amazon di https://console.aws.amazon.com/datazone di AWS akun tempat DataZone domain Amazon dibuat.
2. Pilih Lihat domain dan pilih domain dan unit domain tempat Anda ingin menambahkan pemilik unit domain.
3. Pada halaman detail unit domain, pilih tab Pemilik dan kemudian pilih Tambah pemilik.
4. Di jendela pop up Tambahkan pemilik unit domain, tentukan pengguna yang ingin Anda jadikan pemilik unit domain, lalu pilih Tambah pemilik.

Menetapkan kebijakan otorisasi untuk pengguna dan grup dalam unit domain Amazon DataZone

Di Amazon DataZone, unit domain memungkinkan Anda mengatur aset dan entitas domain lainnya di bawah unit bisnis dan tim tertentu. Untuk informasi selengkapnya, lihat DataZone Terminologi dan konsep Amazon.

Di unit DataZone domain Amazon, Anda dapat menetapkan kebijakan otorisasi berikut kepada pengguna dan grup untuk memberi mereka berbagai izin otorisasi dalam unit domain ini:

- Kebijakan pembuatan unit domain
- Kebijakan pembuatan proyek
- Kebijakan keanggotaan proyek
- Kebijakan asumsi kepemilikan unit domain

- Kebijakan asumsi kepemilikan proyek

Untuk menetapkan kebijakan otorisasi kepada pengguna dan grup dalam unit domain, selesaikan prosedur berikut:

1. Arahkan ke portal DataZone data Amazon URL dan masuk menggunakan single sign-on (SSO) atau AWS kredensil. 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 Lihat domain dan pilih domain dan unit domain tempat Anda ingin menetapkan kebijakan otorisasi.
3. Pada halaman detail unit domain, pilih kebijakan otorisasi yang ingin Anda tetapkan ke pengguna/grup, lalu pilih Tambah pengguna.
4. Di jendela pop up Tambah pengguna, lakukan salah satu hal berikut:
   - Pilih Pengguna dan grup yang dipilih, tentukan pengguna dan grup yang ingin Anda tetapkan kebijakan otorisasi yang dipilih, lalu pilih Tambahkan pengguna.
   - Pilih Semua pengguna dan kemudian pilih Tambah pengguna.
   - Pilih Semua grup lalu pilih Tambah pengguna.
5. Anda juga dapat mengaktifkan atau menonaktifkan izin kaskade dari kebijakan otorisasi yang dipilih untuk pengguna yang dipilih. Untuk melakukannya, pilih pengguna yang ingin Anda aktifkan izin kaskade, lalu perluas Tindakan, lalu pilih Setel izin kaskade ke true. Pengguna yang dipilih akan memiliki izin yang diberikan oleh kebijakan ini di semua unit domain anak di bawah unit domain ini. Atau Anda dapat memilih pengguna yang ingin Anda nonaktifkan izin kaskade, lalu memperluas Tindakan, dan mengatur Setel izin kaskade ke false.

Kebijakan keanggotaan proyek dalam hierarki unit domain

Kebijakan keanggotaan proyek mendefinisikan individu atau grup yang memenuhi syarat untuk ditambahkan sebagai anggota ke proyek dalam unit domain. Topik ini menjelaskan skenario dampak kebijakan dalam kaitannya dengan unit domain individu dan unit domain dalam struktur hierarki.

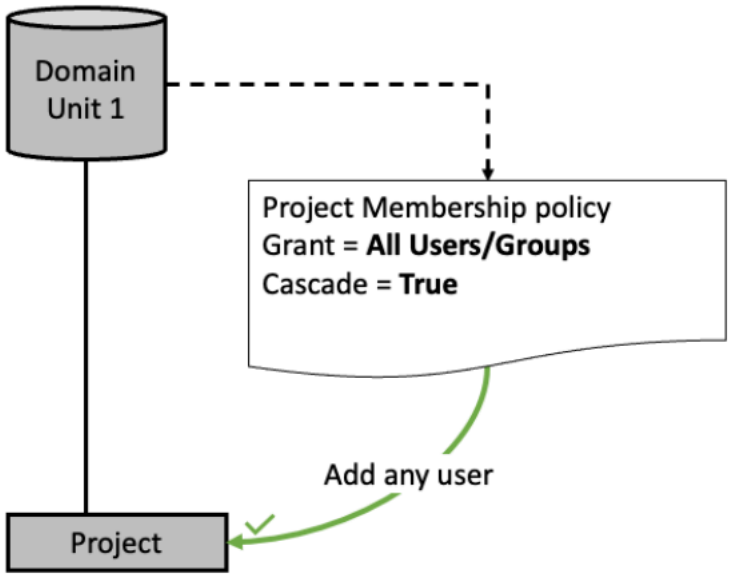
Penting untuk dicatat beberapa konsep yang digunakan dalam topik ini:

- Kumpulan keanggotaan - kepala sekolah (pengguna atau grup) yang diberikan akses melalui kebijakan keanggotaan proyek dianggap sebagai bagian dari kumpulan keanggotaan proyek.

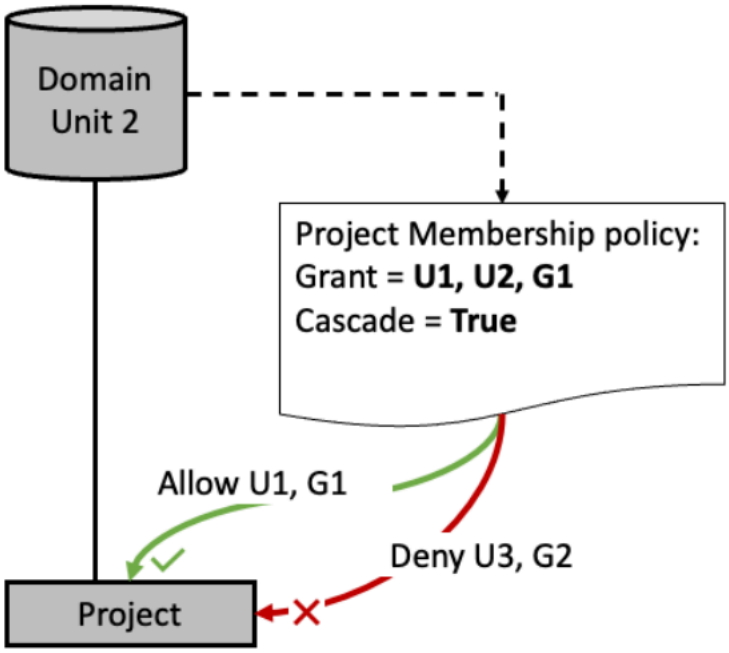
Misalnya, jika kebijakan untuk unit domain DU1 diberikan kepada pengguna U1 dan U2, serta grup Single Sign-On (SSO) G1, kumpulan keanggotaan proyek untuk DU1 akan terdiri dari {U1, U2, G1}.

- Cascade - kemampuan untuk meneruskan hibah ke semua unit domain anak yang terhubung melalui hierarki unit domain.
- Hibah - izin bagi pengguna atau grup untuk melakukan suatu tindakan.

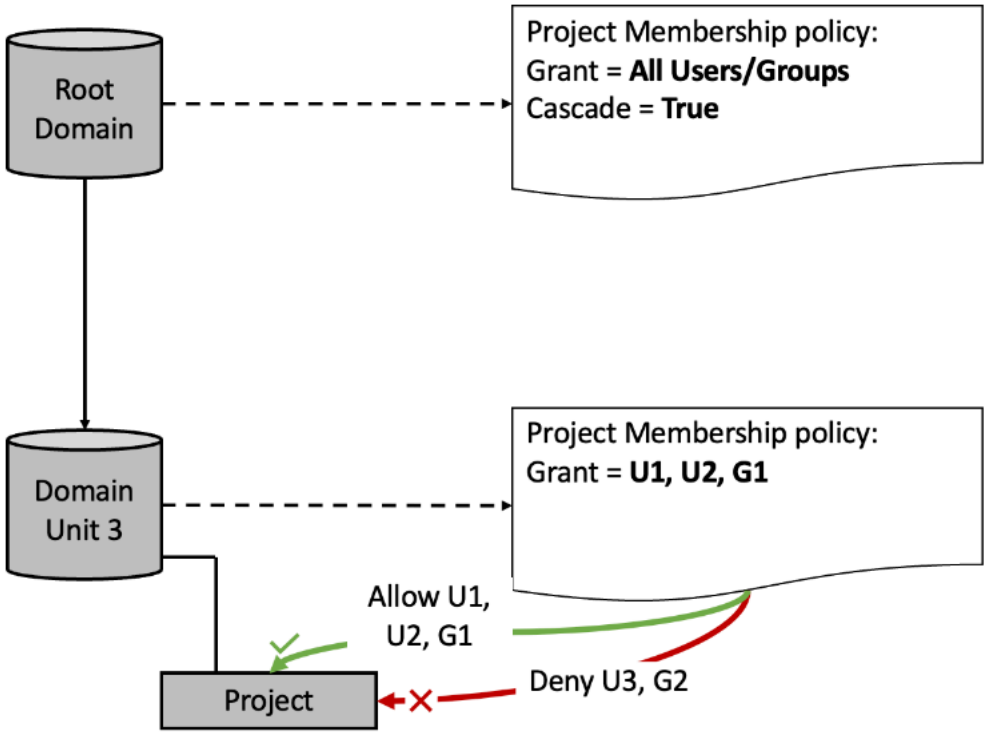
Skenario 1 - setiap pengguna atau grup dapat ditambahkan ke proyek di bawah Domain Unit 1 karena kumpulan keanggotaan terdiri dari {Semua Pengguna/Grup}.



Skenario 2 - Pengguna {U1, G1} dapat ditambahkan ke proyek di bawah Domain Unit 2 karena mereka adalah bagian dari kumpulan keanggotaan di bawah Domain Unit 2. Pengguna {U3, G2} tidak dapat ditambahkan ke proyek apa pun karena mereka bukan bagian dari kumpulan keanggotaan.

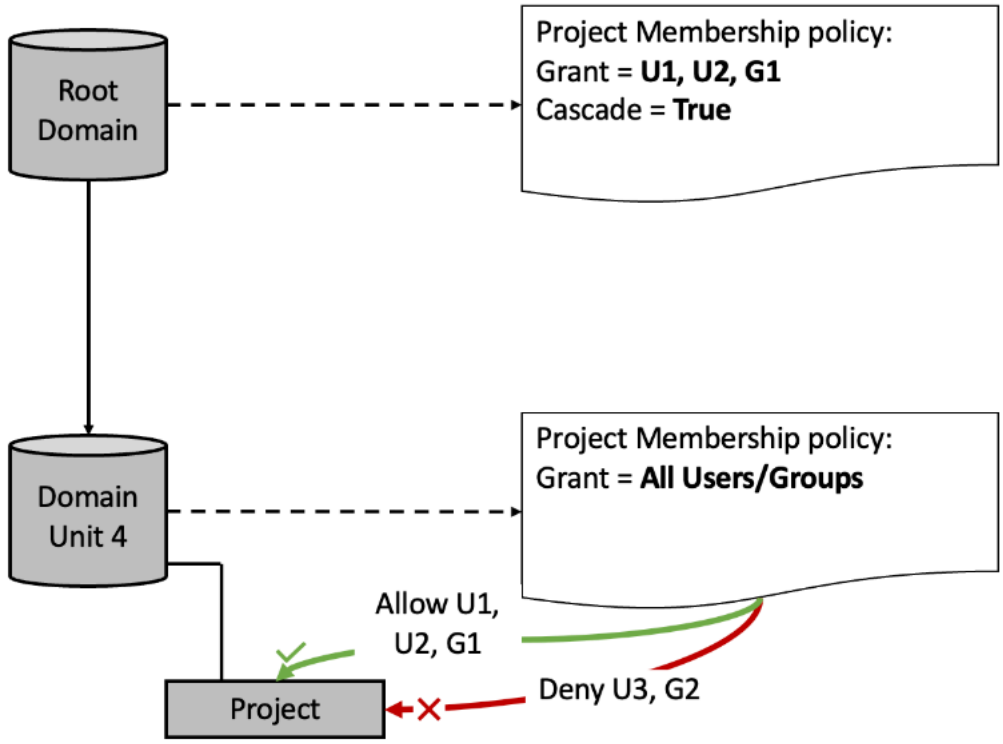


Skenario 3 - Persimpangan kumpulan keanggotaan: ketika ada kumpulan keanggotaan pada tingkat hierarki unit domain yang berbeda, hanya pengguna dan grup yang ada di semua kumpulan keanggotaan yang dapat ditambahkan ke proyek.



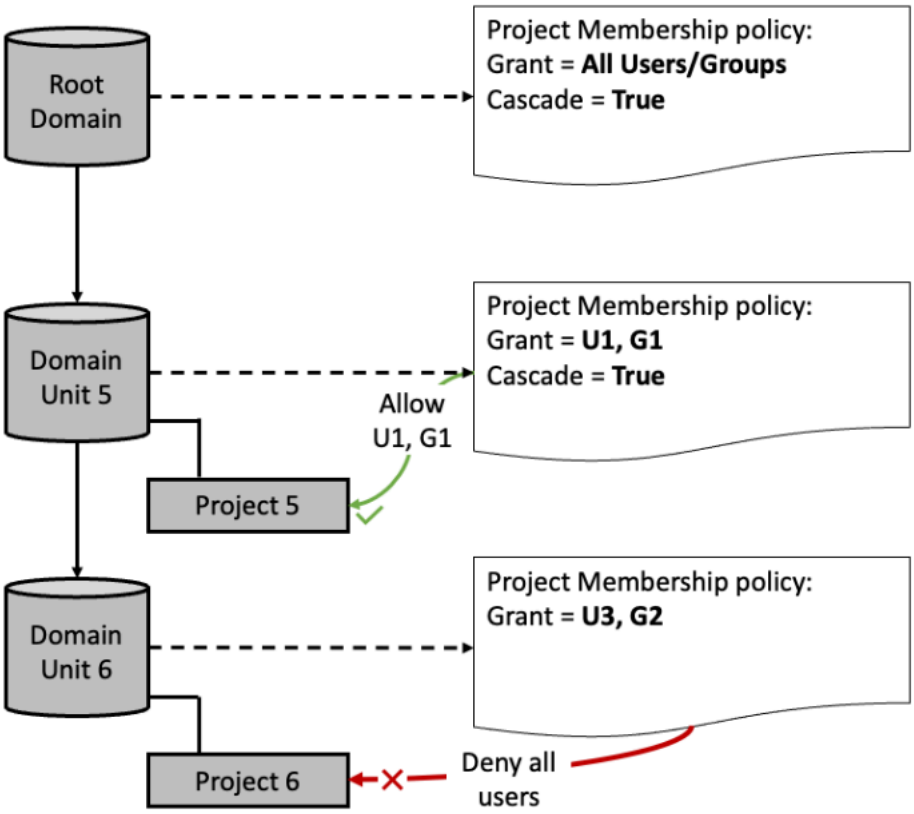
- Persimpangan pengguna di kedua kumpulan keanggotaan adalah {U1, U2, G1}.
- Pengguna {U1, U2, G1} dapat ditambahkan ke proyek di bawah Domain Unit 3.
- Pengguna {U3, G2} tidak dapat ditambahkan ke proyek di bawah Domain Unit 3 bahkan dengan Semua Pengguna dan Semua Grup berada di kolam keanggotaan di tingkat unit Domain Root.

Skenario 4 - Persimpangan kumpulan keanggotaan: ketika ada kumpulan keanggotaan pada tingkat hierarki unit domain yang berbeda, hanya pengguna dan grup yang ada di semua kumpulan keanggotaan yang dapat ditambahkan ke proyek.

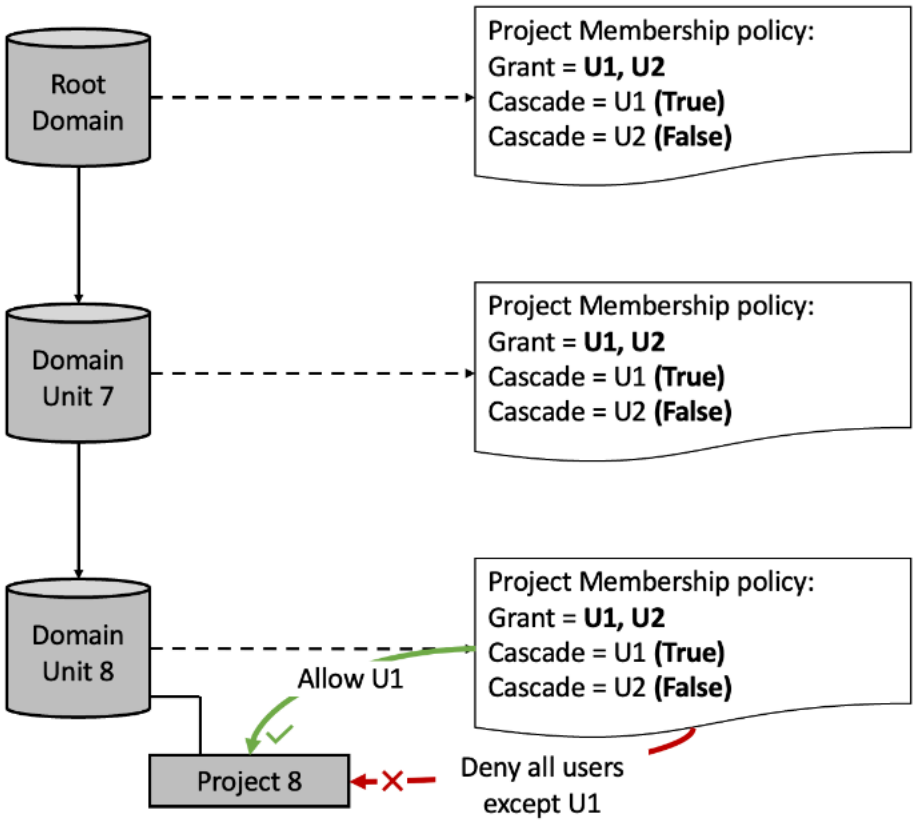


- Persimpangan pengguna di kedua kumpulan keanggotaan adalah {U1, U2, G1}.
- Kumpulan keanggotaan di Domain Unit 4 adalah {Semua Pengguna/Grup} tetapi kumpulan keanggotaan tidak dapat diperluas melampaui kumpulan keanggotaan di Root Domain {U1, U2, G1}.
- Pengguna {U3, G2} tidak dapat ditambahkan ke proyek di bawah Domain Unit 4 bahkan dengan Semua Pengguna dan Semua Grup berada di kolam keanggotaan di Unit Domain 4.

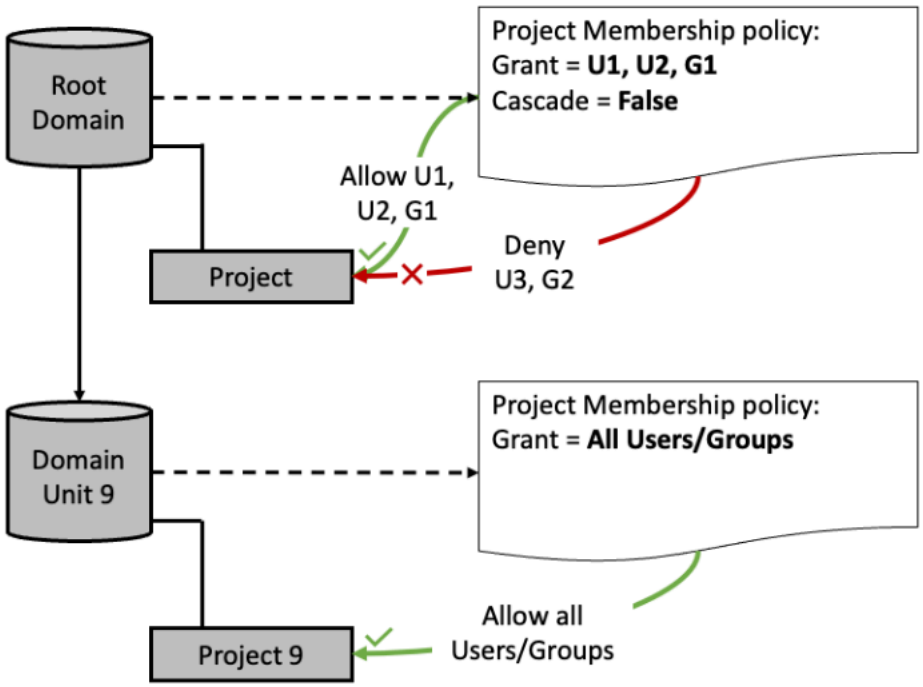
Skenario 5 - Pengguna {U1, G1} dapat ditambahkan ke Project 5 sebagai bagian dari persimpangan pool keanggotaan antara Root Domain dan Domain Unit 5. Tidak ada pengguna/grup yang dapat ditambahkan ke Proyek 6 karena persimpangan dari tiga kumpulan keanggotaan kosong.



Skenario 6 - Persimpangan di ketiga kumpulan keanggotaan berarti hanya pengguna {U1} yang dapat ditambahkan ke Project 8. Kumpulan persimpangan di untuk Domain Unit 8 adalah {U1}, {U1}, {U1, U2} - dengan hanya {U1} yang umum di ketiganya.



Skenario 7 - Pengguna {U1, U2, G1} dapat ditambahkan ke proyek Domain Root sebagai bagian dari kumpulan keanggotaan dari Domain Root. Setiap pengguna atau grup dapat ditambahkan ke proyek di bawah Domain Unit 9 karena kumpulan keanggotaan terdiri dari {Semua Pengguna/Grup} karena kaskade disetel ke false di Domain Root di atasnya.



Menetapkan kebijakan otorisasi untuk proyek dalam unit domain Amazon DataZone

Di Amazon DataZone, unit domain memungkinkan Anda mengatur aset dan entitas domain lainnya di bawah unit bisnis dan tim tertentu. Untuk informasi selengkapnya, lihat DataZone Terminologi dan konsep Amazon.

Di unit DataZone domain Amazon, Anda dapat menetapkan kebijakan otorisasi berikut ke proyek Anda untuk memberikan entitas ini berbagai izin otorisasi dalam unit domain ini:

- Kebijakan pembuatan glosarium
- Kebijakan pembuatan formulir metadata
- Kebijakan pembuatan jenis aset khusus

Untuk menetapkan kebijakan otorisasi ke proyek dalam unit domain, selesaikan prosedur berikut:

1. Arahkan ke portal DataZone data Amazon URL dan masuk menggunakan single sign-on (SSO) atau AWS kredensil. 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 Lihat domain dan pilih domain dan unit domain tempat Anda ingin menetapkan kebijakan otorisasi.
3. Pada halaman detail unit domain, pilih kebijakan otorisasi yang ingin Anda tetapkan ke proyek, lalu pilih Tambah proyek.
4. Di jendela pop up Add projects, lakukan salah satu hal berikut:
   - Pilih Proyek yang dipilih dalam unit domain, tentukan proyek yang ingin Anda tetapkan kebijakan otorisasi yang dipilih, lalu pilih Tambahkan proyek.
   - Pilih Semua proyek dalam unit domain dan kemudian pilih Tambah proyek.

Tetapkan kebijakan otorisasi dalam konfigurasi cetak biru Amazon DataZone

Cara lain untuk menggunakan mekanisme otorisasi di Amazon DataZone adalah dengan menerapkan kebijakan otorisasi untuk proyek dan pemilik unit domain dalam konfigurasi DataZone cetak biru Amazon.

Konfigurasi DataZone cetak biru Amazon adalah entitas yang merangkum informasi yang diperlukan untuk membuat dan mengonfigurasi sumber daya yang digunakan dalam menerbitkan dan berlangganan alur kerja pengguna. Informasi ini termasuk AWS nomor akun dan wilayah, CFN template, parameter tingkat akun seperti VPCs dan subnet, dan juga dapat berisi informasi koneksi database dan kredensil. Untuk mengontrol biaya dan meningkatkan keamanan, pengguna platform data memerlukan kemampuan untuk mengontrol siapa yang dapat menggunakan cetak biru ini dan menciptakan lingkungan.

Dalam konfigurasi cetak biru tertentu, Anda dapat menetapkan kebijakan otorisasi berikut untuk proyek dan pemilik unit domain:

- Buat profil lingkungan menggunakan cetak biru ini - kebijakan ini dapat ditetapkan ke DataZone proyek Amazon dan mengizinkan mereka untuk membuat profil lingkungan menggunakan cetak biru ini.
- Berikan izin untuk membuat profil lingkungan menggunakan cetak biru ini - kebijakan ini dapat ditetapkan ke pemilik unit domain dan memberi wewenang kepada mereka untuk memberikan izin kepada proyek untuk membuat profil lingkungan menggunakan cetak biru ini.

Tetapkan profil lingkungan Buat menggunakan kebijakan otorisasi cetak biru ini ke proyek dari konfigurasi cetak biru melalui portal data Amazon DataZone

1. Arahkan ke portal DataZone data Amazon URL dan masuk menggunakan single sign-on (SSO) atau AWS kredensil. 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 domain yang memiliki cetak biru aktif yang ingin Anda gunakan, lalu arahkan ke tab Konfigurasi cetak biru.
3. Di tab Konfigurasi cetak biru, pilih cetak biru yang diaktifkan yang ingin Anda gunakan, lalu di halaman detail cetak biru ini, arahkan ke tab Kebijakan otorisasi, lalu pilih Buat profil lingkungan menggunakan kebijakan otorisasi cetak biru ini.
4. Di halaman Buat profil lingkungan menggunakan detail kebijakan otorisasi cetak biru ini, perluas Tindakan dan pilih Tambahkan proyek.
5. Di jendela pop up Add projects, Anda dapat melakukan salah satu hal berikut:

   - Pilih opsi Semua proyek dalam unit domain, lalu cari dan tentukan unit domain yang berisi proyek yang ingin Anda otorisasi untuk membuat profil lingkungan dengan cetak biru ini, lalu pilih Tambahkan proyek.
   - Pilih opsi Proyek yang dipilih dalam unit domain, lalu cari dan tentukan unit domain yang berisi proyek yang ingin Anda tetapkan kebijakan ini, lalu pilih dan pilih proyek yang ingin Anda tetapkan kebijakan ini, lalu pilih Tambahkan proyek.

Tetapkan izin Hibah untuk membuat profil lingkungan menggunakan kebijakan otorisasi cetak biru ini kepada pemilik unit domain dari konfigurasi cetak biru melalui konsol manajemen Amazon DataZone

1. Arahkan ke DataZone konsol Amazon di https://console.aws.amazon.com/datazone dan masuk dengan kredensi akun Anda.
2. Di DataZone konsol Amazon, pilih domain yang memiliki cetak biru aktif yang ingin Anda gunakan, lalu arahkan ke tab Blueprints.
3. Di tab Blueprints, pilih cetak biru yang diaktifkan yang ingin Anda kerjakan, lalu di halaman detail cetak biru, arahkan ke tab Izin yang didelegasikan.
4. Di tab Izin yang didelegasikan, cari dan pilih unit domain untuk pemilik yang ingin Anda tetapkan izin Hibah untuk membuat profil lingkungan menggunakan kebijakan cetak biru ini, lalu pilih Tambahkan izin yang didelegasikan.

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

Anda dapat menjalankan langkah-langkah prosedur berikut untuk mengaktifkan cetak biru default di Amazon: DataZone

- Aktifkan cetak biru bawaan di AWS akun yang memiliki domain Amazon DataZone
- Tambahkan Amazon SageMaker sebagai layanan tepercaya di AWS akun yang memiliki domain Amazon DataZone

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 danau data berisi definisi untuk meluncurkan dan mengonfigurasi serangkaian layanan (AWS Glue 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. Penyiapan 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 DataZone domain Amazon ini. 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 IAM berperan dalam akun dengan izin administratif. Konfigurasikan IAM izin yang diperlukan untuk menggunakan konsol DataZone manajemen Amazonuntuk 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 AWS Glue dan AWS Formasi Danau.

- 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 IAM peran 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 menggunakan AWS CloudFormation di akun lingkungan dan wilayah.
- 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 SageMaker AWS akun. 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.

> **Important**
>
> Secara default, tidak ada proyek pengelolaan yang ditentukan untuk cetak biru lingkungan, yang berarti bahwa setiap DataZone pengguna Amazon dapat membuat profil untuk cetak biru lingkungan. Oleh karena itu, sangat disarankan agar Anda selalu menentukan pengelolaan proyek untuk cetak biru lingkungan Anda untuk memastikan tata kelola yang lebih kuat.

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 dapat menambahkan set parameter ke konfigurasi cetak biru. Set 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 AWS rahasia ARN yang menyimpan kredensional ke cluster Amazon Redshift yang dipilih atau grup kerja Amazon Redshift Serverless. Bagian AWS secret harus ditandai dengan `AmazonDataZoneDomain : [Domain_ID]` tag agar memenuhi syarat untuk digunakan dalam set parameter.
     - Jika Anda tidak memiliki yang ada AWS rahasia, Anda juga dapat membuat rahasia baru dengan memilih Buat Baru AWS Rahasia. Ini membuka kotak dialog di mana Anda dapat memberikan nama rahasia, nama pengguna, dan kata sandi. Setelah Anda memilih Create New AWS Rahasia, Amazon DataZone menciptakan rahasia baru di AWS Secrets Manager layanan dan memastikan bahwa rahasia ditandai dengan domain di mana Anda mencoba untuk 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.

> **Note**
>
> Anda hanya dapat menambahkan hingga 10 set parameter ke DefaultDataWarehouse cetak biru.

Setelah Anda mengaktifkan SageMaker cetak biru Amazon di AWS akun, 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 salah satu IAM atau IAM Identity Center (SSO).
    - Tentukan AWS region.
    - Tentukan AWS KMSkunci untuk enkripsi data. Anda dapat memilih kunci yang ada atau membuat kunci baru.
    - Di bawah parameter Lingkungan, tentukan yang berikut ini:
        - VPCID - ID yang Anda gunakan untuk SageMaker lingkungan Amazon. VPC Anda dapat menentukan yang sudah ada atau membuat yang baruVPC.
        - Subnet - satu atau lebih IDs untuk berbagai alamat IP untuk sumber daya tertentu dalam AndaVPC.
        - Akses jaringan - pilih VPChanya 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 AWS rahasia ARN yang menyimpan kredensional ke cluster Amazon Redshift yang dipilih. Bagian AWS secret harus ditandai dengan `AmazonDataZoneDomain : [Domain_ID]` tag agar memenuhi syarat untuk digunakan dalam set parameter.

  Jika Anda tidak memiliki yang ada AWS rahasia, Anda juga dapat membuat rahasia baru dengan memilih Buat Baru AWS Rahasia. Ini membuka kotak dialog di mana Anda dapat memberikan nama rahasia, nama pengguna, dan kata sandi. Setelah Anda memilih Create New AWS Rahasia, Amazon DataZone menciptakan rahasia baru di AWS Secrets Manager layanan dan memastikan bahwa rahasia ditandai dengan domain di mana Anda mencoba untuk 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 Glue saja+Amazon Redshift Cluster
  - Tentukan AWS rahasia ARN yang menyimpan kredensional ke cluster Amazon Redshift yang dipilih. Bagian AWS secret harus ditandai dengan `AmazonDataZoneDomain : [Domain_ID]` tag agar memenuhi syarat untuk digunakan dalam set parameter.

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

DataZone Kustom Amazon AWS cetak biru layanan

Di Amazon DataZone, kustom AWS cetak biru layanan memungkinkan Anda mengoptimalkan penggunaan dan biaya sumber daya dengan mengonfigurasi Amazon DataZone untuk menggunakan milik Anda yang sudah ada AWS Peran Identity and Access Management (IAM) dan AWS layanan yang sudah Anda siapkan di organisasi Anda.

Cetak biru yang dengannya DataZone lingkungan Amazon dibuat mendefinisikan alat dan layanan apa yang dapat digunakan anggota proyek tempat lingkungan tersebut dapat digunakan 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

Dengan DataZone kustom Amazon AWS cetak biru layanan, Anda dapat membuat lingkungan dan proyek yang disesuaikan dengan apa pun AWS layanan yang saat ini Anda gunakan di organisasi Anda. Dengan cetak biru khusus, Anda dapat menyertakan Amazon DataZone di jalur data yang ada dengan mengonfigurasinya untuk menggunakan IAM peran yang ada guna meningkatkan tata kelola di seluruh penyiapan infrastruktur dan berkolaborasi dalam inisiatif bisnis.

Topik

Aktifkan kustom AWS cetak biru layanan

Selesaikan prosedur berikut untuk mengaktifkan kustom AWS cetak biru layanan di domain Anda.

1. Masuk ke AWS Management Console dan buka konsol DataZone manajemen Amazon di https://console.aws.amazon.com/datazone.
2. Pilih Lihat domain dan pilih domain tempat Anda ingin mengaktifkan kustom AWS cetak biru layanan.
3. Pilih tab Blueprints, lalu pilih AWS service bluepint dari daftar cetak biru yang tersedia, lalu pilih Aktifkan.

Buat lingkungan menggunakan kustom AWS cetak biru layanan

Selesaikan prosedur berikut untuk membuat lingkungan menggunakan kustom AWS cetak biru layanan.

1. Masuk ke AWS Management Console dan buka konsol DataZone manajemen Amazon di https://console.aws.amazon.com/datazone.
2. Pilih Lihat domain dan pilih domain tempat kustom Anda AWS cetak biru layanan diaktifkan.
3. Pilih tab Blueprints, lalu pilih yang diaktifkan AWS layanan bluepint, dan kemudian pilih Buat lingkungan.
4. Pada halaman Buat lingkungan, tentukan yang berikut ini dan kemudian pilih Buat lingkungan:

   - Nama - tentukan nama untuk lingkungan.
   - Deskripsi - tentukan deskripsi untuk lingkungan.
   - Proyek - tentukan proyek pemilik baru atau yang sudah ada untuk lingkungan. Proyek memungkinkan grup pengguna untuk menemukan, menerbitkan, berlangganan, dan menggunakan aset di Amazon DataZone. Lingkungan ini akan tersedia untuk semua anggota proyek yang ditentukan. Semua lingkungan dimiliki oleh proyek yang penggunanya memiliki akses ke lingkungan.
   - Peran lingkungan - tentukan IAM peran yang ada yang akan memberikan Amazon DataZone akses ke yang sudah ada AWS layanan dan sumber daya, seperti Amazon S3 dan AWS Glue, di lingkungan ini.

     > **Note**
     >
     > Amazon DataZone tidak menyediakan peran ini untuk Anda. Anda harus memiliki IAM peran yang ada dengan izin untuk yang ada AWS layanan dan sumber daya yang ingin Anda aktifkan di lingkungan ini.

Pastikan bahwa IAM peran ini memiliki izin minimum yang diperlukan, dengan kata lain, dicakup untuk memberikan akses hanya ke AWS layanan dan sumber daya yang ingin Anda aktifkan di lingkungan ini.
Anda dapat menggunakan AWS Policy Generator untuk membuat kebijakan yang sesuai dengan kebutuhan Anda dan melampirkannya ke IAM peran kustom yang ingin Anda gunakan.
Pastikan peran dimulai dengan `AmazonDataZone` mengikuti konvensi. Ini tidak wajib, tetapi direkomendasikan. Jika IAM administrator menggunakan `AmazonDataZoneFullAccess` kebijakan, Anda harus mengikuti konvensi ini karena ada validasi pemeriksaan peran lulus.
Saat Anda membuat peran kustom Anda, pastikan bahwa itu mempercayai kebijakan `datazone.amazonaws.com` kepercayaannya:

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

- AWS wilayah - tentukan AWS wilayah di mana Anda ingin menciptakan lingkungan ini.

Buat tindakan dalam kustom AWS lingkungan layanan

Selesaikan prosedur berikut untuk membuat tindakan dalam kustom AWS lingkungan layanan. Dengan membuat tindakan dalam kustom AWS lingkungan layanan, Anda menambahkan tautan dalam ke portal DataZone data Amazon ke alat analitik yang tersedia di lingkungan ini.

1. Masuk ke AWS Management Console dan buka konsol DataZone manajemen Amazon di https://console.aws.amazon.com/datazone.
2. Pilih Lihat domain dan pilih domain tempat kustom Anda AWS cetak biru layanan diaktifkan.
3. Pilih tab Blueprints, lalu pilih yang diaktifkan AWS layanan bluepint, dan kemudian pilih AWS lingkungan layanan tempat Anda ingin menambahkan tindakan.
4. Pada AWS halaman tautan konsol, pilih tautan (tindakan) dari Populer AWS link atau Custom AWS bagian tautan untuk mengaktifkan tautan dalam ke bucket Amazon S3 Anda, grup kerja Amazon Athena, AWS Pekerjaan Glue, atau ke kustom lainnya AWS sumber daya konsol dari lingkungan ini melalui portal DataZone data Amazon.
5. Jika Anda menavigasi ke lingkungan ini di portal data dengan menggunakan tautan portal data dari bagian Ringkasan lingkungan ini, Anda dapat melihat tautan dalam yang telah Anda tambahkan di bagian alat Analytics.

Tambahkan anggota proyek ke kustom AWS lingkungan layanan

Selesaikan prosedur berikut untuk menambahkan anggota proyek ke AWS lingkungan layanan.

1. Masuk ke AWS Management Console dan buka konsol DataZone manajemen Amazon di https://console.aws.amazon.com/datazone.
2. Pilih tab Projects dan kemudian pilih proyek dalam AWS lingkungan layanan yang ingin Anda tambahkan anggota.
3. Pilih Tambah dan kemudian, pada halaman Tambah anggota, temukan dan tambahkan anggota dari IAMpengguna, SSOpengguna, atau SSOgrup. Tentukan peran proyek yang ditetapkan dari Pemilik atau Kontributor. Setelah selesai menemukan dan menambahkan anggota, pilih Tambahkan anggota.

Konfigurasikan sumber data dalam AWS lingkungan layanan

Selesaikan prosedur berikut untuk mengonfigurasi sumber data dalam AWS lingkungan layanan.

1. Masuk ke AWS Management Console dan buka konsol DataZone manajemen Amazon di https://console.aws.amazon.com/datazone.
2. Pilih tab Blueprints dan kemudian pilih kustom AWS cetak biru layanan.
3. Di bawah Lingkungan yang dibuat, pilih AWS lingkungan layanan tempat Anda ingin mengonfigurasi sumber data.
4. Pilih tab Sumber data, pilih Tambah, tentukan yang berikut ini, lalu pilih Tambah.

   - Nama - nama sumber data.
   - Sumber daya - pilih salah satu AWS Glue atau Amazon Redshift.
     - Untuk AWS Glue, tentukan database sumber daya.
     - Untuk Amazon Redshift, pilih Cluster atau Tanpa Server, lalu tentukan Kredenal Redshift, termasuk yang baru atau yang sudah ada AWS secret, cluster atau grup kerja tanpa server yang ingin Anda gunakan saat membuat lingkungan, database yang ingin Anda gunakan saat membuat lingkungan, dan skema dalam database yang ditentukan.
   - Izin - tentukan peran kelola akses yang akan DataZone memberi Amazon otorisasi untuk menyerap dan mengelola akses ke tabel di AWS Lake Formation (untuk AWS Glue) atau yang akan DataZone memberi Amazon otorisasi untuk menelan dan mengelola akses ke tabel di Amazon Redshift.
   - Gunakan untuk konsumsi data - di Amazon DataZone, anggota proyek dapat DataZone menggunakan data melalui target langganan yang digunakan Amazon untuk mengaktifkan akses ke data yang telah Anda langgani dalam proyek Anda. Tentukan apakah akan menambahkan sumber data ini sebagai target langganan.

Konfigurasikan target langganan di AWS lingkungan layanan

Selesaikan prosedur berikut untuk mengonfigurasi target langganan di AWS lingkungan layanan.

1. Masuk ke AWS Management Console dan buka konsol DataZone manajemen Amazon di https://console.aws.amazon.com/datazone.
2. Pilih tab Blueprints dan kemudian pilih AWS cetak biru layanan.
3. Di bawah Lingkungan yang dibuat, pilih AWS lingkungan layanan tempat Anda ingin mengonfigurasi target langganan.
4. Pilih tab Target langganan, pilih Tambah, tentukan yang berikut, lalu pilih Tambah.

   - Nama - nama target berlangganan.

- Sumber daya - pilih salah satu AWS Glue atau Amazon Redshift.
  - Untuk AWS Glue, tentukan database sumber daya.
  - Untuk Amazon Redshift, pilih Cluster atau Tanpa Server, lalu tentukan Kredenal Redshift, termasuk yang baru atau yang sudah ada AWS secret, cluster atau grup kerja tanpa server yang ingin Anda gunakan saat membuat lingkungan, database yang ingin Anda gunakan saat membuat lingkungan, dan skema dalam database yang ditentukan.
- Izin - tentukan peran kelola akses yang akan DataZone memberi Amazon otorisasi untuk menyerap dan mengelola akses ke tabel di AWS Lake Formation (untuk AWS Glue) atau yang akan DataZone memberi Amazon otorisasi untuk menelan dan mengelola akses ke tabel di Amazon Redshift.
- Gunakan untuk konsumsi data - di Amazon DataZone, Anda dapat mempublikasikan data ke katalog data melalui sumber data yang memungkinkan untuk konsumsi metadata. Tentukan apakah akan menambahkan target langganan ini sebagai sumber data.

Akun terkait di Amazon DataZone

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

- Pertama, bagikan domain dengan yang diinginkan AWS akun dengan meminta asosiasi. Amazon DataZone menggunakan AWS Resource Access Manager (RAM) jika AWS Akun berbeda dari domain AWS akun. 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 pengguna di domain IAM peran dan konfigurasi sumber daya yang diperlukan untuk membuat dan mengakses sumber daya di akun mereka, seperti AWS Basis data Glue dan cluster Amazon Redshift.

Selesaikan langkah berikut untuk mengaitkan akun dengan Amazon DataZone:

- Langkah 1 - Minta asosiasi dengan yang lain AWS rekening
- Langkah 2 - Terima permintaan asosiasi akun dari DataZone domain Amazon dan aktifkan cetak biru lingkungan
- Langkah 3 - Aktifkan cetak biru lingkungan yang terkait AWS akun

Minta asosiasi dengan yang lain AWS rekening

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

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

Lengkapi prosedur berikut untuk meminta asosiasi dengan yang lain AWS akun.

1. Masuk ke AWS Management Console dan buka konsol DataZone manajemen Amazon di https://console.aws.amazon.com/datazone.
2. Pilih Lihat domain dan pilih nama domain dari daftar. Namanya adalah hyperlink.
3. Gulir ke bawah ke tab Akun terkait dan pilih Minta asosiasi.
4. Masukkan akun IDs yang ingin Anda minta asosiasi. Bila Anda puas dengan daftar akunIDs, pilih Minta asosiasi.
5. Di bawah RAM Kebijakan, tentukan RAM kebijakan untuk asosiasi akun. Anda dapat memilih `AWSRAMPermissionDataZonePortalReadWrite` mana yang akan mengaktifkan akun terkait untuk mengeksekusi Amazon DataZone APIs dan mengakses portal data atau Anda dapat memilih`AWSRAMPermissionDataZoneDefault`, yang akan memungkinkan akun terkait untuk hanya mengeksekusi Amazon DataZone APIs dan tidak akan memberikan akses portal data. Amazon DataZone kemudian 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 yang lain AWS akun untuk menerima permintaan Anda. Undangan berakhir setelah tujuh (7) hari.

Berikan akses akun ke kunci yang dikelola pelanggan KMS Anda

DataZone Domain Amazon dan metadatanya dienkripsi, baik (secara default) menggunakan kunci yang dipegang oleh AWS, atau (opsional) kunci yang dikelola pelanggan dari AWS Layanan Manajemen Kunci (KMS) yang Anda miliki dan sediakan 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 tersebut. KMS

1. Masuk ke AWS Management Console dan buka KMS konsol 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 KMS kunci, pilih alias atau ID kunci dari KMS kunci yang ingin Anda periksa.
5. Untuk mengizinkan atau melarang eksternal AWS akun untuk menggunakan KMS kunci, gunakan kontrol di Lainnya AWS bagian akun dari halaman. IAMprinsipal dalam akun ini (dengan KMS izin yang tepat sendiri) dapat menggunakan KMS kunci 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 IAM berperan dalam akun dengan izin administratif. Konfigurasikan IAM izin yang diperlukan untuk menggunakan konsol DataZone manajemen Amazonuntuk mendapatkan izin minimum.

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

1. Masuk ke AWS Management Console 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 dapat melakukan ini nanti.
   - Cetak biru lingkungan data lake memungkinkan pengguna domain untuk membuat dan mengelola AWS Glue, Amazon S3, dan Amazon Athena sumber daya untuk mempublikasikan dan mengkonsumsi dari danau data.
   - 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.
   - IAMPeran Kelola akses memberikan izin ke Amazon DataZone 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 IAM peran baru, atau Anda dapat memilih dari daftar IAM peran yang ada.
   - IAMPeran Penyediaan memberikan izin ke Amazon DataZone untuk memungkinkan pengguna domain membuat dan mengonfigurasi sumber daya lingkungan, seperti AWS Basis data Glue. Anda dapat memilih untuk DataZone membuat Amazon dan menggunakan IAM peran baru, atau Anda dapat memilih dari daftar IAM peran 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 IAM kebijakan untuk DataZone memberi Amazon izin untuk menggunakannya.

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

Aktifkan cetak biru lingkungan yang terkait AWS akun

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

Selesaikan berikut ini untuk mengaktifkan cetak biru di domain terkait.

1. Masuk ke AWS Management Console 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 Cetak Biru, pilih salah satu atau, DefaultDataLakeatau Amazon DefaultDataWarehouse SageMaker, atau Kustom AWS Cetak biru layanan.

> **Note**
>
> Jika Anda mengaktifkan Custom AWS cetak biru layanan, Anda tidak perlu menentukan peran mengelola akses. Izin dan mekanisme otorisasi untuk Kustom AWS service bluerpint ditangani saat Anda membuat lingkungan menggunakan cetak biru ini. Untuk informasi selengkapnya, lihat Buat lingkungan menggunakan kustom AWS cetak biru layanan.

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 AWS Glue dan AWS Formasi Danau.

- 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 IAM peran 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 menggunakan AWS CloudFormation di akun lingkungan dan wilayah.
- 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 SageMaker AWS akun. 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 kredensi 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 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.

> **Important**
>
> Secara default, tidak ada proyek pengelolaan yang ditentukan untuk cetak biru lingkungan, yang berarti bahwa setiap DataZone pengguna Amazon dapat membuat profil untuk cetak biru lingkungan. Oleh karena itu, sangat disarankan agar Anda selalu menentukan pengelolaan proyek untuk cetak biru lingkungan Anda untuk memastikan tata kelola yang lebih kuat.

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. Buka panel navigasi kiri dan pilih Domain terkait lalu 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 AWS rahasia ARN yang menyimpan kredensil ke cluster Amazon Redshift yang dipilih atau grup kerja Amazon Redshift Serverless. Bagian AWS secret harus ditandai dengan `AmazonDataZoneDomain : [Domain_ID]` tag agar memenuhi syarat untuk digunakan dalam set parameter.
     - Jika Anda tidak memiliki yang ada AWS rahasia, Anda juga dapat membuat rahasia baru dengan memilih Buat Baru AWS Rahasia. Ini membuka kotak dialog di mana Anda dapat memberikan nama rahasia, nama pengguna, dan kata sandi. Setelah Anda memilih Create New AWS Rahasia, Amazon DataZone menciptakan rahasia baru di AWS Secrets Manager layanan dan memastikan bahwa rahasia ditandai dengan domain di mana Anda mencoba untuk 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.

> **Note**
>
> Anda hanya dapat menambahkan hingga 10 set parameter ke DefaultDataWarehouse cetak biru.

Setelah Anda mengaktifkan SageMaker cetak biru Amazon di AWS akun, 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 salah satu IAM atau IAM Identity Center (SSO).
    - Tentukan AWS region.
    - Tentukan AWS KMSkunci untuk enkripsi data. Anda dapat memilih kunci yang ada atau membuat kunci baru.
    - Di bawah parameter Lingkungan, tentukan yang berikut ini:
        - VPCID - ID yang Anda gunakan untuk SageMaker lingkungan Amazon. VPC Anda dapat menentukan yang sudah ada atau membuat yang baruVPC.
        - Subnet - satu atau lebih IDs untuk berbagai alamat IP untuk sumber daya tertentu dalam AndaVPC.
        - Akses jaringan - pilih VPChanya 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 AWS rahasia ARN yang menyimpan kredensil ke cluster Amazon Redshift yang dipilih. Bagian AWS secret harus ditandai dengan `AmazonDataZoneDomain : [Domain_ID]` tag agar memenuhi syarat untuk digunakan dalam set parameter.

  Jika Anda tidak memiliki yang ada AWS rahasia, Anda juga dapat membuat rahasia baru dengan memilih Buat Baru AWS Rahasia. Ini membuka kotak dialog di mana Anda dapat memberikan nama rahasia, nama pengguna, dan kata sandi. Setelah Anda memilih Create New AWS Rahasia, Amazon DataZone menciptakan rahasia baru di AWS Secrets Manager layanan dan memastikan bahwa rahasia ditandai dengan domain di mana Anda mencoba untuk 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 Glue saja+Amazon Redshift Cluster
  - Tentukan AWS rahasia ARN yang menyimpan kredensil ke cluster Amazon Redshift yang dipilih. Bagian AWS secret harus ditandai dengan `AmazonDataZoneDomain : [Domain_ID]` tag agar memenuhi syarat untuk digunakan dalam set parameter.

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

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.

Tolak permintaan asosiasi akun dari domain Amazon DataZone

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

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

1. Masuk ke AWS Management Console 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.

Hapus akun terkait

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

Selesaikan prosedur berikut untuk menghapus akun terkait dari domain Anda.

1. Masuk ke AWS Management Console dan buka konsol DataZone manajemen Amazon di https://console.aws.amazon.com/datazone.

2. Pilih Lihat Domain dan pilih nama domain dari daftar. Namanya adalah 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.

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 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.

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.

Untuk informasi selengkapnya, lihat DataZone Terminologi dan konsep Amazon.

Topik

- Hapus formulir metadata
- Buat bidang dalam bentuk metadata
- Mengedit bidang dalam bentuk metadata
- Menghapus bidang dalam bentuk metadata

Buat 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 portal data URL dan masuk menggunakan SSO atau AWS kredensil. Jika Anda DataZone administrator Amazon, Anda dapat memperoleh portal data URL 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 portal data URL dan masuk menggunakan SSO atau AWS kredensil. Jika Anda DataZone administrator Amazon, Anda

dapat memperoleh portal data URL 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.

Edit 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 mengedit glosarium di DataZone domain Amazon Anda, Anda harus menjadi anggota proyek pemilik dengan izin yang tepat untuk domain tersebut.

Untuk mengedit glosarium bisnis, selesaikan langkah-langkah berikut:

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

Hapus 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 menghapus glosarium di DataZone domain Amazon Anda, Anda harus menjadi anggota proyek pemilik dengan izin yang tepat untuk domain tersebut.

Untuk menghapus glosarium bisnis, selesaikan langkah-langkah berikut:

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

Buat 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 portal data URL dan masuk menggunakan SSO atau AWS kredensil. Jika Anda DataZone administrator Amazon, Anda dapat memperoleh portal data URL 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.

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

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

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

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

Buat 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 portal data URL dan masuk menggunakan SSO atau AWS kredensil. Jika Anda DataZone administrator Amazon, Anda dapat memperoleh portal data URL 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.

Mengedit 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 mengedit formulir metadata, lengkapi langkah-langkah berikut:

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

Hapus 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 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 portal data URL dan masuk menggunakan SSO atau AWS kredensil. Jika Anda DataZone administrator Amazon, Anda dapat memperoleh portal data URL 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.

Buat 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 portal data URL dan masuk menggunakan SSO atau AWS kredensil. Jika Anda DataZone administrator Amazon, Anda dapat memperoleh portal data URL 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.

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

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

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

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

DataZone Proyek dan lingkungan Amazon

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 kredensyal pengguna individu.

Di Amazon DataZone, lingkungan adalah kumpulan sumber daya yang dikonfigurasi (misalnya, bucket Amazon S3, dan AWS Glue database, atau grup kerja Amazon Athena), dengan sekumpulan IAM prinsipal 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 AWS layanan dan eksternal IDEs dan konsol. Anggota proyek dapat mengakses layanan seperti konsol Amazon Athena dan lainnya melalui tautan dalam yang dikonfigurasi dalam suatu lingkungan. SSOpengguna dan IAM pengguna dari proyek dapat dicakup lebih lanjut untuk menggunakan/mengakses lingkungan tertentu.

Di Amazon DataZone, Anda membuat lingkungan dengan menggunakan templat yang disebut profil lingkungan. Profil lingkungan, pada gilirannya, dibuat dengan menggunakan built-in dan custom AWS cetak biru layanan. 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.

Untuk informasi selengkapnya, silakan lihat DataZone Terminologi dan konsep Amazon

Topik

- Buat profil lingkungan
- Mengedit profil lingkungan

- Menghapus profil lingkungan
- Ciptakan lingkungan baru
- Mengedit lingkungan
- Hapus lingkungan
- Membuat sebuah proyek baru
- Edit proyek
- Hapus proyek
- Tinggalkan proyek
- Menambahkan anggota ke proyek
- Menghapus anggota dari proyek

Buat profil lingkungan

Di Amazon DataZone, profil lingkungan adalah template yang dapat Anda gunakan untuk membuat lingkungan. Tujuan dari profil lingkungan adalah untuk menyederhanakan penciptaan 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 portal data URL dan masuk menggunakan SSO atau AWS kredensialnya. Jika Anda DataZone administrator Amazon, Anda dapat memperoleh portal data URL 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 sebuah 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 AWS Rahasia ARN yang menyimpan kredensil ke cluster Amazon Redshift atau grup kerja Amazon Redshift Serverless yang dipilih. Bagian AWS secret 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 di 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 AWS bagian parameter akun, tentukan AWS nomor rekening dan AWS wilayah 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 portal DataZone data Amazon URL dan masuk menggunakan single sign-on (SSO) atau AWS kredensialnya. 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 penciptaan 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 portal DataZone data Amazon URL dan masuk menggunakan single sign-on (SSO) atau AWS kredensialnya. 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, dan AWS Glue database, atau workgroup Amazon Athena), dengan sekumpulan IAM prinsipal 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 portal DataZone data Amazon URL dan masuk menggunakan single sign-on (SSO) atau AWS kredensialnya. 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, dan AWS Glue database, atau workgroup Amazon Athena), dengan sekumpulan IAM prinsipal 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 portal DataZone data Amazon URL dan masuk menggunakan single sign-on (SSO) atau AWS kredensialnya. 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, dan AWS Glue database, atau workgroup Amazon Athena), dengan sekumpulan IAM prinsipal 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 portal DataZone data Amazon URL dan masuk menggunakan single sign-on (SSO) atau AWS kredensialnya. 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 portal DataZone data Amazon URL dan masuk menggunakan single sign-on (SSO) atau AWS kredensialnya. 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.
   - Unit domain — Unit domain di mana Anda ingin membuat proyek ini.

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 portal DataZone data Amazon URL dan masuk menggunakan single sign-on (SSO) atau AWS kredensialnya. 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 tidak dapat dibatalkan, 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 non-Amazon DataZone AWS sumber daya yang Amazon DataZone mungkin telah membantu Anda membuat. Jika Anda tidak lagi membutuhkannya AWS sumber daya, hapus mereka di masing-masing AWS layanan dan akun.

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

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

1. Arahkan ke portal DataZone data Amazon URL dan masuk menggunakan single sign-on (SSO) atau AWS kredensialnya. IAMPrincipal 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 Anda membuat lingkungan dalam sebuah proyek, Amazon DataZone membuat AWS sumber daya di domain Anda atau akun terkait untuk memberi Anda dan pengguna domain Anda fungsionalitas. Di bawah ini adalah daftar AWS sumber daya yang DataZone dapat dibuat Amazon untuk proyek, bersama dengan nama default. Menghapus proyek tidak menghapus semua ini AWS sumber daya di Anda AWS akun.
>
> - IAMperan: environmentId datazone_usr_< >.
> - Basis data Glue: (1) < environmentName >_pub_db-*, (2) < >_sub_db-*. environmentName Jika sudah ada database nama ini, Amazon DataZone akan menambahkan ID lingkungan.
> - Kelompok kerja Athena: < >-*. environmentName Jika sudah ada workgroup nama ini, Amazon DataZone akan menambahkan ID lingkungan.
> - CloudWatch grup log: environmentId datazone_< >

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 portal DataZone data Amazon URL dan masuk menggunakan single sign-on (SSO) atau AWS kredensialnya. 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 SSO grup, SSO pengguna, atau IAM kepala sekolah (peran atau pengguna) sebagai anggota proyek.

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

1. Arahkan ke portal DataZone data Amazon URL dan masuk menggunakan single sign-on (SSO) atau AWS kredensialnya. 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.

> **Important**
>
> Anda hanya dapat menambahkan pengguna tersebut sebagai anggota proyek yang diberi wewenang untuk menjadi anggota proyek ini dengan kebijakan otorisasi keanggotaan proyek yang dikonfigurasi untuk unit domain tempat proyek ini tinggal. Untuk informasi selengkapnya, lihat Menetapkan kebijakan otorisasi untuk pengguna dan grup dalam unit domain Amazon DataZone .

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

Inventaris data dan penerbitan 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.

Untuk informasi selengkapnya, silakan lihat DataZone Terminologi dan konsep Amazon

Topik

- Konfigurasikan izin Lake Formation untuk Amazon DataZone
- Buat jenis aset khusus
- Membuat dan menjalankan sumber DataZone data Amazon untuk AWS Glue Data Catalog
- Membuat dan menjalankan sumber DataZone data Amazon untuk Amazon Redshift
- Mengedit sumber data
- Hapus sumber data
- Publikasikan aset ke DataZone katalog Amazon dari inventaris proyek
- Kelola inventaris dan kurasi aset
- Buat aset secara manual
- Batalkan publikasi aset dari katalog Amazon DataZone

- 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
- Garis keturunan data di Amazon DataZone (Pratinjau)

Konfigurasikan izin Lake Formation untuk Amazon DataZone

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

Namun, jika Anda ingin mempublikasikan aset dan berlangganan aset dari AWS Glue database yang ada di luar DataZone lingkungan Amazon Anda, Anda harus secara eksplisit memberikan Amazon DataZone dengan izin untuk mengakses tabel di eksternal ini AWS Basis data Glue. Untuk melakukan ini, Anda harus menyelesaikan pengaturan berikut di AWS Lake Formation dan lampirkan izin Lake Formation yang diperlukan ke. AmazonDataZoneGlueAccess- <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/register-data-laketerbaru/dg/ .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/upgrade-glue-lake-formationterbaru/dg/ -background.html.
- Lampirkan yang berikut AWS Izin Lake Formation untuk: AmazonDataZoneGlueAccess- <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 AWS Mode Hibrida Lake Formation. Mode hibrida Lake Formation memungkinkan Anda untuk mulai mengelola izin pada Anda AWS Glue database dan tabel melalui Lake Formation, sambil terus mempertahankan IAM izin yang ada pada tabel dan database ini. Untuk informasi selengkapnya, silakan lihat DataZone Integrasi Amazon dengan AWS Mode hibrida Lake Formation

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

DataZone Integrasi Amazon dengan AWS Mode hibrida Lake Formation

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

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

Aktifkan integrasi dengan AWS Mode hibrida Lake Formation

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 integrasi AWS Mode hibrida 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.
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 IAM peran baru atau memilih IAM peran yang ada. Amazon DataZone menggunakan peran ini untuk mengelola akses baca/tulis ke bucket Amazon S3 yang dipilih untuk Data Lake menggunakan AWS Mode akses hibrida Lake 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 bucket Amazon S3 yang ingin Anda kecualikan. URI
    - 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, ketika konsumen data berlangganan AWS Glue table yang dikelola melalui IAM izin, Amazon pertama-tama DataZone akan mendaftarkan lokasi Amazon S3 dari tabel ini dalam mode hybrid, dan kemudian memberikan akses ke konsumen data dengan mengelola izin di atas tabel melalui AWS Formasi Danau. Ini memastikan bahwa IAM izin pada tabel terus ada dengan yang baru diberikan AWS Izin Lake Formation, tanpa mengganggu alur kerja yang ada.

Cara menangani lokasi Amazon S3 terenkripsi saat mengaktifkan AWS Integrasi mode hibrida Lake Formation di Amazon DataZone

Jika Anda menggunakan lokasi Amazon S3 yang dienkripsi dengan Pelanggan yang dikelola atau AWS KMSKunci AmazonDataZoneterkelola, peran S3Manage harus memiliki izin untuk mengenkripsi dan mendekripsi data dengan KMS kunci, atau kebijakan KMS kunci harus memberikan izin pada kunci peran.

Jika lokasi Amazon S3 Anda dienkripsi dengan AWS kunci terkelola, tambahkan kebijakan inline berikut ke AmazonDataZoneDataLocationManagementperan:

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

   - Jika tampilan default ditampilkan (dengan administrator Kunci, Penghapusan kunci, Pengguna kunci, dan Lainnya AWS bagian akun) — di bawah bagian Pengguna kunci, tambahkan AmazonDataZoneDataLocationManagementperan.
   - 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 KMS kunci atau lokasi Amazon S3 tidak sama AWS akun sebagai katalog data, ikuti petunjuk di Mendaftarkan lokasi Amazon S3 terenkripsi di seluruh AWS akun.

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 standarisasi saat mendeskripsikan aset katalog, DataZone domain Amazon harus memiliki sekumpulan jenis aset yang menentukan bagaimana aset direpresentasikan dalam katalog. Tipe aset mendefinisikan skema untuk jenis aset tertentu. Tipe aset memiliki satu set tipe formulir metadata yang dapat diberi nama wajib dan 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 portal DataZone data Amazon URL dan masuk menggunakan single sign-on (SSO) atau AWS kredensialnya. 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 khusus.
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 melaluiAPIs, selesaikan langkah-langkah berikut:

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

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 jenis aset dengan menjalankan `CreateAssetType` API tindakan. Anda dapat membuat jenis aset hanya melalui Amazon DataZone APIs 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 AWS Glue Data Catalog sumber data untuk mengimpor metadata teknis tabel database dari AWS Glue. Untuk menambahkan sumber data untuk AWS Glue Data Catalog Database sumber harus sudah ada di AWS Glue.

Saat Anda membuat dan menjalankan AWS Glue sumber data, Anda menambahkan aset dari sumbernya AWS Glue database ke inventaris DataZone proyek Amazon Anda. Anda dapat menjalankan AWS Glue sumber data 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 AWS Glue sumber data

1. Arahkan ke portal DataZone data Amazon URL dan masuk menggunakan single sign-on (SSO) atau AWS kredensialnya. 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 membentuk dropdown atau ketik 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 yang sudah ada AWS Glue output kualitas data ke dalam DataZone katalog Amazon Anda. Secara default, Amazon DataZone mengimpor 100 laporan kualitas terbaru yang ada tanpa tanggal kedaluwarsa AWS Glue.

   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 AWS Glue skor kualitas data pada jadwal. Katalog data DataZone bisnis Amazon juga dapat menampilkan metrik kualitas data dari sistem pihak ketiga melalui kualitas APIs data. Untuk informasi selengkapnya, silakan lihat Kualitas data di Amazon DataZone

10. Pilih Berikutnya.
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.

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 “Buat 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 Berikutnya.
16. Tinjau konfigurasi sumber data Anda dan pilih Buat.

> **Note**
>
> Ketika sebuah AWS Glue sumber data dibuat, Amazon DataZone membuat izin 'baca hanya' Lake Formation untuk IAM peran lingkungan yang digunakan untuk membuat sumber data untuk mengakses semua tabel di AWS Glue database yang digunakan dalam sumber data. Anda dapat memantau status hibah ini di bawah sumber data di halaman detail lingkungan Anda. Amazon DataZone menambahkan yang berikut AWS tag ke AWS Glue database saat memberikan akses ke IAM peran lingkungan penerbitan: `DataZoneDiscoverable_${domainId}: true`
> Untuk lingkungan yang dibuat sebelum rilis Amazon saat ini DataZone, anggota proyek tidak akan dapat melihat tabel yang diberikan di Amazon Athena.

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 portal DataZone data Amazon URL dan masuk menggunakan single sign-on (SSO) atau AWS kredensialnya. 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, AWS rahasia, nama database, dan nama skema. 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 kredensyal Anda sendiri untuk membuat sumber data, berikan detail berikut:

   - Di bawah Menyediakan kredensil 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 cluster Amazon Redshift atau ruang kerja Anda dari menu tarik-turun, lalu pilih rahasianya di AWS Secrets Manager 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 masuk 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 di 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 di 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 Berikutnya.
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.

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 “Buat 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 Berikutnya.
17. Tinjau konfigurasi sumber data Anda dan pilih Buat.

> **Note**
>
> Saat sumber data Amazon Redshift dibuat, Amazon hanya DataZone memberikan akses baca ke lingkungan yang digunakan untuk membuat sumber data untuk mengakses semua tabel dalam skema Amazon Redshift yang digunakan dalam sumber data. Anda dapat memantau status hibah ini di bawah sumber data di halaman detail lingkungan Anda.
> Saat menggunakan klaster Amazon Redshift atau grup kerja Tanpa Server yang berbeda dari yang digunakan untuk membuat lingkungan, Anda harus memastikan bahwa yang berikut AWS tag ditambahkan ke cluster atau workgroup. Hal ini diperlukan agar pengguna lingkungan dapat melihat database yang diberikan di Amazon Redshift Query Editor V2:
> `DataZoneDiscoverable_${domainId}: true`
> Untuk lingkungan yang dibuat sebelum rilis Amazon saat ini DataZone, anggota proyek tidak akan dapat melihat tabel yang diberikan di Amazon Redshift.

Mengedit sumber data

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 AmazonDataZoneFullAccess AWS kebijakan terkelola terlampir. Untuk informasi selengkapnya, lihat the section called “AWS kebijakan terkelola ”.

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 portal DataZone data Amazon URL dan masuk menggunakan single sign-on (SSO) atau AWS kredensialnya. 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 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

Setelah membuat sumber DataZone data Amazon, Anda dapat memodifikasinya kapan saja untuk mengubah detail sumber atau kriteria pemilihan data.

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

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 Penemuan data, berlangganan, dan konsumsi.

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 portal DataZone data Amazon URL dan masuk menggunakan single sign-on (SSO) atau AWS kredensialnya. 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 mengatur 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 “Buat formulir metadata”.

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

Untuk memperbarui metadata aset

1. Arahkan ke portal DataZone data Amazon URL dan masuk menggunakan single sign-on (SSO) atau AWS kredensialnya. 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 aset baru. 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 portal DataZone data Amazon URL dan masuk menggunakan single sign-on (SSO) atau AWS kredensialnya. 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 aset baru. 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 portal DataZone data Amazon URL dan masuk menggunakan single sign-on (SSO) atau AWS kredensialnya. 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 setelan berikut:
   - Jenis aset — Jenis aset.
   - Nama — Nama aset.
   - Deskripsi — Deskripsi aset.
6. Untuk lokasi S3, masukkan Amazon Resource Name (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 portal DataZone data Amazon URL dan masuk menggunakan single sign-on (SSO) atau AWS kredensialnya. 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 portal DataZone data Amazon URL dan masuk menggunakan single sign-on (SSO) atau AWS kredensialnya. 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 portal DataZone data Amazon URL dan masuk menggunakan single sign-on (SSO) atau AWS kredensialnya. 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 API operasi. 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 portal DataZone data Amazon URL dan masuk menggunakan single sign-on (SSO) atau AWS kredensialnya. 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 APIs 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 AWS Kualitas data 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 DataZone Amazon AWS kebijakan terkelola, 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 AWS Glue informasi kualitas data dalam AWS kebijakan terkelola: AmazonDataZoneGlueManageAccessRolePolicy dan memungkinkan dukungan untuk deret waktu APIs dalam AWS kebijakan terkelola: AmazonDataZoneDomainExecutionRolePolicy danAWS kebijakan terkelola: AmazonDataZoneFullUserAccess.

Mengaktifkan kualitas data untuk AWS Aset 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 AWS Glue skor kualitas data pada jadwal. Katalog data DataZone bisnis Amazon juga dapat menampilkan metrik kualitas data dari sistem pihak ketiga melalui kualitas APIs data. Untuk informasi selengkapnya, silakan lihat AWS Glue Data Quality dan Memulai AWS Kualitas Data Glue untuk Katalog Data.

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

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

  Untuk informasi selengkapnya tentang mengaktifkan kualitas data untuk sumber data melalui portal, lihatMembuat dan menjalankan sumber DataZone data Amazon untuk AWS Glue Data Catalog.

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

  Anda juga dapat menggunakan APIs 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 Amazon DataZone APIs 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 APIs atau CLI mengimpor metrik pihak ketiga untuk aset Anda di Amazon DataZone:

1. Memanggil `PostTimeSeriesDataPoints` API sebagai berikut:

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

dengan muatan berikut:

```
"domainId": "dzd_5oo7xzoqltu8mf",
    "entityId": "4wyh64k2n8czaf",
    "entityType": "ASSET",
    "form": {
        "content": "{\n  \"evaluations\" : [ {\n    \"types\" : [ \"MaximumLength
\" ],\n    \"description\" : \"ColumnLength \\\"ShippingCountry\\\" <= 6\",\n
   \"details\" : { },\n    \"applicableFields\" : [ \"ShippingCountry\" ],\n
   \"status\" : \"PASS\"\n  }, {\n    \"types\" : [ \"MaximumLength\" ],\n
 \"description\" : \"ColumnLength \\\"ShippingState\\\" <= 2\",\n    \"details
\" : { },\n    \"applicableFields\" : [ \"ShippingState\" ],\n    \"status\" :
 \"PASS\"\n  }, {\n    \"types\" : [ \"MaximumLength\" ],\n    \"description
\" : \"ColumnLength \\\"ShippingCity\\\" <= 8\",\n    \"details\" : { },\n
 \"applicableFields\" : [ \"ShippingCity\" ],\n    \"status\" : \"PASS\"\n  },
 {\n    \"types\" : [ \"Completeness\" ],\n    \"description\" : \"Completeness \
\\"ShippingStreet\\\" >= 0.59\",\n    \"details\" : { },\n    \"applicableFields
\" : [ \"ShippingStreet\" ],\n    \"status\" : \"PASS\"\n  }, {\n    \"types\" :
 [ \"MaximumLength\" ],\n    \"description\" : \"ColumnLength \\\"ShippingStreet\\
\" <= 101\",\n    \"details\" : { },\n    \"applicableFields\" : [ \"ShippingStreet
\" ],\n    \"status\" : \"PASS\"\n  }, {\n    \"types\" : [ \"MaximumLength\" ],\n
    \"description\" : \"ColumnLength \\\"BillingCountry\\\" <= 6\",\n    \"details
\" : { },\n    \"applicableFields\" : [ \"BillingCountry\" ],\n    \"status\" :
 \"PASS\"\n  }, {\n    \"types\" : [ \"Completeness\" ],\n    \"description\" :
 \"Completeness \\\"biLlingcountry\\\" >= 0.5\",\n    \"details\" : {\n
 \"EVALUATION_MESSAGE\" : \"Value: 0.26666666666666666 does not meet the constraint
 requirement!\"\n    },\n    \"applicableFields\" : [ \"biLlingcountry\" ],\n
   \"status\" : \"FAIL\"\n  }, {\n    \"types\" : [ \"Completeness\" ],\n
 \"description\" : \"Completeness \\\"Billingstreet\\\" >= 0.5\",\n    \"details
\" : { },\n    \"applicableFields\" : [ \"Billingstreet\" ],\n    \"status\" :
 \"PASS\"\n  } ],\n  \"passingPercentage\" : 88.0,\n  \"evaluationsCount\" : 8\n}",
```

```
        "formName": "shortschemaruleset",
        "id": "athp9dyw75gzhj",
        "timestamp": 1.71700477757E9,
        "typeIdentifier": "amazon.datazone.DataQualityResultFormType",
        "typeRevision": "8"
    },
    "formName": "shortschemaruleset"
}
```

Anda dapat memperoleh muatan ini dengan menjalankan tindakan: `GetFormType`

```
aws datazone get-form-type --domain-identifier <your_domain_id> --form-type-
identifier amazon.datazone.DataQualityResultFormType --region <domain_region> --
output text --query 'model.smithy'
```

2. Memanggil `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 portal DataZone data AmazonURL, lalu masuk menggunakan single sign-on (SSO) atau AWS kredensialnya. Jika Anda DataZone administrator Amazon, navigasikan ke DataZone konsol Amazon di https://console.aws.amazon.com/datazone dan masuk dengan Akun AWS di mana domain dibuat, dan kemudian 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 Buat 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 memublikasikan aset ini, metadata yang dihasilkan secara otomatis yang tidak ditinjau ini tidak disertakan dalam aset data yang dipublikasikan.

Garis keturunan data di Amazon DataZone (Pratinjau)

> **Important**
>
> Saat ini, fungsionalitas garis keturunan data di Amazon DataZone ada dalam rilis Pratinjau.

Garis keturunan data di Amazon DataZone adalah fitur yang API digerakkan dan OpenLineage kompatibel yang dapat membantu Anda menangkap dan memvisualisasikan peristiwa garis keturunan, dari sistem yang OpenLineage diaktifkan atau melalui, untuk melacak asal data, melacak

transformasiAPIs, dan melihat konsumsi data lintas organisasi. Ini memberi Anda pandangan menyeluruh ke aset data Anda untuk melihat asal aset dan rantai koneksinya. Data garis keturunan mencakup informasi tentang aktivitas di dalam katalog data bisnis Amazon DataZone, termasuk informasi tentang aset yang dikatalogkan, pelanggan aset tersebut, dan aktivitas yang terjadi di luar katalog data bisnis yang diambil secara terprogram menggunakan. APIs

Menggunakan DataZone Amazon OpenLineage -compatibleAPIs, administrator domain dan produsen data dapat menangkap dan menyimpan peristiwa silsilah di luar apa yang tersedia di Amazon, termasuk transformasi di Amazon DataZone S3, AWS Glue, dan layanan lainnya. Ini memberikan pandangan komprehensif untuk konsumen data dan membantu mereka mendapatkan kepercayaan tentang asal aset, sementara produsen data dapat menilai dampak perubahan aset dengan memahami penggunaannya. Selain itu, DataZone Amazon membuat garis keturunan dengan setiap peristiwa, memungkinkan pengguna untuk memvisualisasikan garis keturunan kapan saja atau membandingkan transformasi di seluruh aset atau riwayat pekerjaan. Garis keturunan historis ini memberikan pemahaman yang lebih dalam tentang bagaimana data telah berevolusi, penting untuk pemecahan masalah, audit, dan memastikan integritas aset data.

Dengan garis keturunan data, Anda dapat mencapai hal berikut di Amazon: DataZone

- Memahami asal data: mengetahui dari mana data berasal menumbuhkan kepercayaan pada data dengan memberi Anda pemahaman yang jelas tentang asal-usul, ketergantungan, dan transformasinya. Transparansi ini membantu dalam membuat keputusan berbasis data yang percaya diri.
- Memahami dampak perubahan pada jaringan data: ketika perubahan dilakukan pada pipa data, garis keturunan dapat digunakan untuk mengidentifikasi semua konsumen hilir yang akan terpengaruh. Ini membantu memastikan bahwa perubahan dilakukan tanpa mengganggu aliran data penting.
- Identifikasi akar penyebab masalah kualitas data: jika masalah kualitas data terdeteksi dalam laporan hilir, garis keturunan, terutama garis keturunan tingkat kolom, dapat digunakan untuk melacak data kembali (pada tingkat kolom) untuk mengidentifikasi masalah kembali ke sumbernya. Ini dapat membantu insinyur data untuk mengidentifikasi dan memperbaiki masalah.
- Meningkatkan tata kelola dan kepatuhan data: garis keturunan tingkat kolom dapat digunakan untuk menunjukkan kepatuhan terhadap tata kelola data dan peraturan privasi. Misalnya, garis keturunan tingkat kolom dapat digunakan untuk menunjukkan di mana data sensitif (sepertiPII) disimpan dan bagaimana diproses dalam aktivitas hilir.

Jenis simpul garis keturunan di Amazon DataZone

di Amazon DataZone, informasi garis keturunan data disajikan dalam node yang mewakili tabel dan tampilan. Bergantung pada konteks proyek, misalnya, proyek yang dipilih di kiri atas di portal data, produsen dapat melihat keduanya, inventaris dan aset yang dipublikasikan, sedangkan konsumen hanya dapat melihat aset yang dipublikasikan. Saat pertama kali membuka tab silsilah di halaman detail aset, simpul kumpulan data yang dikatalogkan adalah titik awal untuk menavigasi hulu atau hilir melalui simpul garis keturunan grafik garis keturunan Anda.

Berikut ini adalah jenis node garis keturunan data yang didukung di Amazon: DataZone

- Dataset node - tipe node ini mencakup informasi garis keturunan data tentang aset data tertentu.
  - Node dataset yang menyertakan informasi tentang AWS Aset Glue atau Amazon Redshift yang diterbitkan dalam DataZone katalog Amazon dibuat secara otomatis dan menyertakan yang sesuai AWS Glue atau ikon Amazon Redshift di dalam node.
  - Node kumpulan data yang menyertakan informasi tentang aset yang tidak dipublikasikan di DataZone katalog Amazon, dibuat secara manual oleh administrator domain (produsen) dan diwakili oleh ikon aset kustom default di dalam node.
- Job (run) node - tipe node ini menampilkan rincian pekerjaan, termasuk run terbaru dari pekerjaan tertentu dan rincian run. Node ini juga menangkap beberapa proses pekerjaan dan dapat dilihat di tab History dari detail node. Anda dapat melihat detail node dengan memilih ikon node.

Atribut kunci dalam simpul garis keturunan

`sourceIdentifier`Atribut dalam simpul garis keturunan mewakili peristiwa yang terjadi pada kumpulan data. Simpul garis keturunan adalah pengidentifikasi kumpulan data (tabel/tampilan dll). `sourceIdentifier` Ini digunakan untuk penegakan keunikan pada node garis keturunan. Misalnya, tidak mungkin ada dua simpul garis keturunan yang sama. `sourceIdentifier` Berikut ini adalah contoh `sourceIdentifier` nilai untuk berbagai jenis node:

- Untuk node dataset dengan tipe dataset masing-masing:
  - Aset: assetId amazon.datazone.asset/< >
  - Daftar (aset yang diterbitkan): listingId amazon.datazone.listing/< >
  - AWS <region><account-id><database>Glue tabel: arn:aws:lem: ::meja//<table-name>

  - <redshift/redshift-serverless> <region><account-id><table-type (table/view etc) > <database><schema>Tabel/tampilan Amazon Redshift: arn:aws::: :/</>/// clusterIdentifierworkgroupName<table-name>
  - Untuk jenis node dataset lainnya yang diimpor menggunakan peristiwa run open lineage,<namespace>/<name>dari dataset input/output digunakan pada node. `sourceIdentifier`
- Untuk pekerjaan:
  - <jobs_namespace>Untuk node pekerjaan yang diimpor menggunakan event open lineage run,. <job_name>digunakan sebagaisourceIdentifier.
- Untuk pekerjaan berjalan:
  - <jobs_namespace>Untuk node job run yang diimpor menggunakan event open lineage run,. <job_name>/<run_id>digunakan sebagaisourceIdentifier.

Untuk aset yang dibuat menggunakan `createAsset`API, `sourceIdentifier` harus diperbarui menggunakan `createAssetRevision` API untuk mengaktifkan pemetaan aset ke sumber daya hulu.

Memvisualisasikan garis keturunan data

Halaman detail DataZone aset Amazon menyediakan representasi grafis dari garis keturunan data, sehingga lebih mudah untuk memvisualisasikan hubungan data hulu atau hilir. Halaman detail aset menyediakan kemampuan berikut untuk menavigasi grafik:

- Garis keturunan tingkat kolom: perluas garis keturunan tingkat kolom bila tersedia di node kumpulan data. Ini secara otomatis menampilkan hubungan dengan node dataset hulu atau hilir jika informasi kolom sumber tersedia.
- Pencarian kolom: ketika tampilan default untuk jumlah kolom adalah 10. Jika ada lebih dari 10 kolom, pagination diaktifkan untuk menavigasi ke kolom lainnya. Untuk melihat kolom tertentu dengan cepat, Anda dapat mencari di node dataset yang hanya mencantumkan kolom yang dicari.
- Lihat node kumpulan data saja: jika Anda ingin beralih untuk hanya melihat node garis keturunan kumpulan data dan memfilter node pekerjaan, Anda dapat memilih ikon Open view control di kiri atas penampil grafik dan beralih opsi Display dataset node only. Ini akan menghapus semua node pekerjaan dari grafik dan memungkinkan Anda menavigasi hanya node dataset. Perhatikan bahwa ketika tampilan hanya node dataset diaktifkan, grafik tidak dapat diperluas ke hulu atau hilir.

- Panel detail: Setiap simpul garis keturunan memiliki detail yang ditangkap dan ditampilkan saat dipilih.
  - Node dataset memiliki panel detail untuk menampilkan semua detail yang diambil untuk node tersebut untuk stempel waktu tertentu. Setiap node dataset memiliki 3 tab, yaitu: Info Lineage, Schema, dan tab History. Tab riwayat mencantumkan berbagai versi peristiwa garis keturunan yang diambil untuk node tersebut. Semua detail yang diambil dari API ditampilkan menggunakan formulir metadata atau penampil. JSON
  - Job node memiliki panel detail untuk menampilkan rincian pekerjaan dengan tab, yaitu: Info pekerjaan, dan History. Panel detail juga menangkap kueri atau ekspresi yang ditangkap sebagai bagian dari pekerjaan yang dijalankan. Tab histori mencantumkan versi berbeda dari acara job run yang diambil untuk pekerjaan itu. Semua detail yang diambil dari API ditampilkan menggunakan formulir metadata atau penampil. JSON
- Tab versi: semua node garis keturunan di garis keturunan DataZone data Amazon memiliki versi. Untuk setiap node dataset atau node pekerjaan, versi diambil sebagai riwayat dan memungkinkan Anda menavigasi di antara versi yang berbeda untuk mengidentifikasi apa yang telah berubah dari waktu ke waktu. Setiap versi membuka tab baru di halaman silsilah untuk membantu membandingkan atau membedakan.

Otorisasi garis keturunan data di Amazon DataZone

Menulis izin - untuk mempublikasikan data silsilah ke Amazon DataZone, Anda harus memiliki IAM peran dengan kebijakan izin yang menyertakan tindakan `ALLOW` pada. `PostLineageEvent` API IAMOtorisasi ini terjadi pada lapisan API Gateway.

Izin baca - ada dua operasi: `GetLineageNode` dan `ListLineageNodeHistory` yang disertakan dalam kebijakan `AmazonDataZoneDomainExecutionRolePolicy` terkelola dan oleh karena itu setiap pengguna di DataZone domain Amazon dapat memanggilnya untuk melintasi grafik garis keturunan data.

Pengalaman sampel garis keturunan data di Amazon DataZone

Anda dapat menggunakan pengalaman sampel garis keturunan data untuk menelusuri dan memahami garis keturunan data di DataZone Amazon, termasuk melintasi hulu atau hilir dalam grafik garis keturunan data Anda, menjelajahi versi, dan garis keturunan tingkat kolom.

Selesaikan prosedur berikut untuk mencoba pengalaman garis keturunan data sampel di Amazon: DataZone

1. Arahkan ke portal DataZone data Amazon URL dan masuk menggunakan single sign-on (SSO) atau AWS kredensialnya. 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 aset data apa pun yang tersedia untuk membuka halaman detail aset.
3. Pada halaman detail aset, pilih tab Lineage lalu pilih Pratinjau, lalu pilih Coba silsilah sampel.
4. Di jendela pop up garis keturunan data, pilih Mulai tur garis keturunan data yang dipandu.

   Pada titik ini, tab layar penuh yang menyediakan semua ruang informasi garis keturunan ditampilkan. Grafik garis keturunan data sampel awalnya ditampilkan dengan simpul dasar dengan kedalaman 1 di kedua ujungnya, hulu dan hilir. Anda dapat memperluas grafik hulu atau hilir. Informasi kolom juga tersedia bagi Anda untuk memilih dan melihat bagaimana garis keturunan mengalir melalui node.

Menggunakan garis keturunan DataZone data Amazon secara terprogram

Untuk menggunakan fungsionalitas garis keturunan data di Amazon DataZone, Anda dapat memanggil yang berikut ini: APIs

- GetLineageNode
- ListLineageNodeHistory
- PostLineageEvent

Produk DataZone data Amazon

Amazon DataZone memungkinkan produsen data untuk mengelompokkan aset data ke dalam paket mandiri yang terdefinisi dengan baik yang disebut produk data yang disesuaikan untuk kasus penggunaan bisnis tertentu. Menggunakan produk data yang kohesif dan selaras dengan bisnis meningkatkan proses penerbitan dan berlangganan. Konsumen data dapat dengan mudah mengidentifikasi aset data yang saling berhubungan dengan mencari dan menemukannya sebagai satu unit. Pendekatan ini mengurangi waktu dan upaya yang diperlukan untuk menemukan semua informasi yang relevan dan menurunkan risiko kehilangan data penting. Selain itu, produk data menyederhanakan akses ke data dengan satu permintaan dengan menerapkan model akses terpadu. Ini menghilangkan kebutuhan untuk beberapa izin, sehingga mempercepat inisiasi analisis data. Selain itu, dengan membuat katalog aset sebagai produk data, produsen data mengurangi overhead administratif dengan mengaktifkan metadata dan manajemen kontrol akses di tingkat produk data, bukan secara individual. Selain itu, kemampuan untuk memunculkan aset dikelompokkan yang dibangun khusus ini untuk konsumsi membuat tata kelola akses dan pemanfaatan data lebih efisien, memastikannya selaras dengan tujuan bisnis dan mudah diakses untuk tujuan penggunaannya. Tim tata kelola data dapat memantau tingkat konsumsi untuk produk data ini, memberikan wawasan berharga tentang kematangan literasi data. Untuk informasi selengkapnya, lihat DataZone Terminologi dan konsep Amazon.

Topik

- Buat produk data baru
- Publikasikan produk data
- Mengedit produk data
- Batalkan publikasi produk data
- Hapus produk data
- Berlangganan produk data
- Tinjau permintaan berlangganan dan berikan langganan ke produk data
- Publikasikan ulang produk data

Buat produk data baru

Amazon DataZone memungkinkan produsen data untuk mengelompokkan aset data ke dalam paket mandiri yang terdefinisi dengan baik yang disebut produk data yang disesuaikan untuk kasus

penggunaan bisnis tertentu. Untuk informasi selengkapnya, lihat DataZone Terminologi dan konsep Amazon.

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

Untuk membuat produk data baru, selesaikan langkah-langkah berikut.

1. Arahkan ke portal DataZone data Amazon URL dan masuk menggunakan single sign-on (SSO) atau AWS kredensialnya. 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 proyek tempat Anda ingin membuat produk data.
3. Pilih tab Data, lalu pilih Data inventaris, lalu pilih Buat produk data baru.
4. Di halaman Buat produk data baru, tentukan nama dan deskripsi untuk produk data, lalu pilih Pilih aset untuk menambahkan berbagai aset ke produk data Anda. Di jendela pop up Pilih aset, pilih aset yang ingin Anda tambahkan ke produk data ini, lalu pilih Pilih. Untuk menyelesaikan pembuatan produk data, pilih Buat.

Publikasikan produk data

Amazon DataZone memungkinkan produsen data untuk mengelompokkan aset data ke dalam paket mandiri yang terdefinisi dengan baik yang disebut produk data yang disesuaikan untuk kasus penggunaan bisnis tertentu. Untuk informasi selengkapnya, lihat DataZone Terminologi dan konsep Amazon.

Setiap DataZone pengguna Amazon dengan izin yang diperlukan untuk mengakses portal data dapat mempublikasikan produk DataZone data Amazon.

Untuk mempublikasikan produk data, lengkapi langkah-langkah berikut.

1. Arahkan ke portal DataZone data Amazon URL dan masuk menggunakan single sign-on (SSO) atau AWS kredensialnya. 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 proyek di mana produk data yang ingin Anda publikasikan hidup.

3. Pilih tab Data, lalu pilih Data inventaris, lalu pilih filter Produk data. Ini menampilkan semua produk data yang ada yang tidak dipublikasikan.
4. Pilih produk data yang ingin Anda publikasikan, lalu pilih Publikasikan. Konfirmasikan penerbitan produk data ini dengan memilih Publikasikan produk data.

> **Note**
>
> Setiap aset data yang tidak dipublikasikan yang ada dalam produk data ini akan dipublikasikan, tetapi hanya akan tersedia melalui produk data ini.

Mengedit produk data

Amazon DataZone memungkinkan produsen data untuk mengelompokkan aset data ke dalam paket mandiri yang terdefinisi dengan baik yang disebut produk data yang disesuaikan untuk kasus penggunaan bisnis tertentu. Untuk informasi selengkapnya, lihat DataZone Terminologi dan konsep Amazon.

Setiap DataZone pengguna Amazon dengan izin yang diperlukan untuk mengakses portal data dapat mengedit produk DataZone data Amazon.

Untuk mengedit produk data, selesaikan langkah-langkah berikut.

1. Arahkan ke portal DataZone data Amazon URL dan masuk menggunakan single sign-on (SSO) atau AWS kredensialnya. 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 proyek di mana produk data yang ingin Anda publikasikan hidup.
3. Pilih tab Data, lalu pilih Data inventaris atau Data yang diterbitkan, lalu pilih filter Produk data.
4. Pilih produk data yang ingin Anda edit. Sebagai bagian dari mengedit produk data, Anda dapat melakukan hal berikut:

   - Pilih Buat readme untuk menambahkan readme akan membantu pengguna memahami halaman ini dengan lebih baik.
   - Pilih Tambahkan istilah untuk menambahkan istilah glosarium. Buat pilihan istilah glosarium Anda di jendela dan kemudian pilih Tambahkan istilah.

- Pilih Tambahkan formulir metadata dan kemudian pilih formulir Anda di jendela Tambahkan formulir metadata dan pilih Tambah.
- Perluas Tindakan, pilih Edit, suntingan nama dan deskripsi produk data, lalu pilih Perbarui.

Batalkan publikasi produk data

Amazon DataZone memungkinkan produsen data untuk mengelompokkan aset data ke dalam paket mandiri yang terdefinisi dengan baik yang disebut produk data yang disesuaikan untuk kasus penggunaan bisnis tertentu. Untuk informasi selengkapnya, lihat DataZone Terminologi dan konsep Amazon.

Setiap DataZone pengguna Amazon dengan izin yang diperlukan untuk mengakses portal data dapat membatalkan publikasi produk DataZone data Amazon.

Untuk membatalkan publikasi produk data, selesaikan langkah-langkah berikut.

1. Arahkan ke portal DataZone data Amazon URL dan masuk menggunakan single sign-on (SSO) atau AWS kredensialnya. 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 proyek tempat produk data yang ingin Anda batalkan dipublikasikan.
3. Pilih tab Data, lalu pilih Data inventaris atau Data yang diterbitkan, lalu pilih filter Produk data. Ini menampilkan semua produk data yang ada.
4. Pilih produk data yang ingin Anda batalkan publikasi, lalu perluas Actions dan pilih Unpublish. Konfirmasikan pembatalan produk data ini dengan memilih Batalkan Publikasi.

> **Note**
>
> Membatalkan penerbitan produk data memiliki efek sebagai berikut:
>
> - Produk data ini tidak lagi tersedia untuk dilihat atau berlangganan.
> - Setiap aset data yang hanya tersedia melalui produk data ini tidak akan lagi tersedia.
> - Semua langganan aktif untuk produk data ini akan tetap ada.
> - Setiap aset data yang dipublikasikan secara individual tidak akan terpengaruh.

Hapus produk data

Amazon DataZone memungkinkan produsen data untuk mengelompokkan aset data ke dalam paket mandiri yang terdefinisi dengan baik yang disebut produk data yang disesuaikan untuk kasus penggunaan bisnis tertentu. Untuk informasi selengkapnya, lihat DataZone Terminologi dan konsep Amazon.

Setiap DataZone pengguna Amazon dengan izin yang diperlukan untuk mengakses portal data dapat menghapus produk DataZone data Amazon.

Untuk menghapus produk data, selesaikan langkah-langkah berikut.

1. Arahkan ke portal DataZone data Amazon URL dan masuk menggunakan single sign-on (SSO) atau AWS kredensialnya. 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 proyek di mana produk data yang ingin Anda hapus hidup.
3. Pilih tab Data, lalu pilih Data inventaris atau Data yang diterbitkan, lalu pilih filter Produk data. Ini menampilkan semua produk data yang ada.
4. Pilih produk data yang ingin Anda hapus, lalu perluas Tindakan dan pilih Hapus. Konfirmasikan penghapusan produk data ini dengan mengetik **`delete`** di bidang teks dan kemudian memilih Hapus.

> **Note**
>
> Menghapus produk data memiliki efek sebagai berikut:
>
> - Produk data tidak lagi tersedia untuk dipublikasikan, dilihat, atau berlangganan.
> - Setiap aset data yang hanya tersedia melalui produk data ini tidak akan lagi terlihat di katalog data. Mereka tidak akan dihapus dari aset inventaris Anda.

Berlangganan produk data

Amazon DataZone memungkinkan produsen data untuk mengelompokkan aset data ke dalam paket mandiri yang terdefinisi dengan baik yang disebut produk data yang disesuaikan untuk kasus penggunaan bisnis tertentu. Untuk informasi selengkapnya, lihat DataZone Terminologi dan konsep Amazon.

Setiap DataZone pengguna Amazon dengan izin yang diperlukan untuk mengakses portal data dapat berlangganan produk DataZone data Amazon.

Untuk berlangganan atau berhenti berlangganan produk data, lengkapi langkah-langkah berikut.

1. Arahkan ke portal DataZone data Amazon URL dan masuk menggunakan single sign-on (SSO) atau AWS kredensialnya. 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 Browse catalog untuk menemukan produk data yang ingin Anda berlangganan dan kemudian pilih produk data tersebut.
3. Pada halaman detail produk data, pilih Berlangganan.
4. Tentukan proyek dan alasan berlangganan dan kemudian pilih Berlangganan.

Tinjau permintaan berlangganan dan berikan langganan ke produk data

Amazon DataZone memungkinkan produsen data untuk mengelompokkan aset data ke dalam paket mandiri yang terdefinisi dengan baik yang disebut produk data yang disesuaikan untuk kasus penggunaan bisnis tertentu. Untuk informasi selengkapnya, lihat DataZone Terminologi dan konsep Amazon.

Proyek pemilik produk data dapat meninjau dan memberikan langganan ke produk DataZone data Amazon.

Untuk meninjau permintaan berlangganan dan memberikan langganan ke produk data, selesaikan langkah-langkah berikut:

1. Arahkan ke portal DataZone data Amazon URL dan masuk menggunakan single sign-on (SSO) atau AWS kredensialnya. 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 proyek yang memiliki produk data yang ada permintaan berlangganan masuk yang ingin Anda tinjau.
3. Pilih tab Data dan kemudian pilih Permintaan masuk.

4. Pilih permintaan yang ingin Anda tinjau dan kemudian di jendela Permintaan langganan, pilih Approve atau Reject, dan ketik komentar desigion.

Publikasikan ulang produk data

Amazon DataZone memungkinkan produsen data untuk mengelompokkan aset data ke dalam paket mandiri yang terdefinisi dengan baik yang disebut produk data yang disesuaikan untuk kasus penggunaan bisnis tertentu. Untuk informasi selengkapnya, lihat DataZone Terminologi dan konsep Amazon.

Setiap DataZone pengguna Amazon dengan izin yang diperlukan untuk mengakses portal data dapat menerbitkan ulang produk DataZone data Amazon.

Untuk mempublikasikan ulang produk data, selesaikan langkah-langkah berikut.

1. Arahkan ke portal DataZone data Amazon URL dan masuk menggunakan single sign-on (SSO) atau AWS kredensialnya. 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 proyek tempat produk data yang ingin Anda publikasikan ulang hidup.
3. Pilih tab Data, lalu pilih Data yang diterbitkan, lalu pilih Filter produk data.
4. Pilih produk data yang ingin Anda publikasikan ulang, lalu pilih tab Aset.
5. Pada tab Aset, lakukan salah satu hal berikut:
   - hapus salah satu aset yang ada dalam produk data dengan memilih aset tersebut, lalu memperluas ikon tindakan dan memilih Hapus aset. Konfirmasikan penghapusan aset dengan memilih Hapus di jendela pop up Hapus aset. Setelah Anda menerbitkan ulang, aset ini akan dihapus dari semua pelanggan ke produk data ini.
   - Tambahkan aset baru ke produk data dengan memilih tombol Tambah dan kemudian pilih satu atau beberapa aset yang akan ditambahkan ke produk data.
6. Pada halaman detail produk data, pilih Publikasikan ulang. Konfirmasikan tindakan ini dengan memilih Publikasikan ulang di jendela pop up produk Republish data.

> **Note**
>
> Menerbitkan ulang produk data ini akan memperbarui yang berikut untuk semua pelanggan:
>
> - Jika aset telah dihapus dari produk data, pelanggan tidak akan lagi memiliki akses ke aset ini.
> - Jika aset telah ditambahkan ke produk data, pelanggan akan mendapatkan akses ke aset ini.
> - Versi baru yang diterbitkan dari aset data akan tersedia.

Penemuan DataZone data Amazon, berlangganan, dan konsumsi

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 dan 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 yang lain AWS layanan atau solusi pihak ketiga untuk integrasi khusus.

Topik

- Kueri data di Amazon Athena atau Amazon Redshift

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 mencari aset di katalog

1. Arahkan ke portal DataZone data Amazon URL dan masuk menggunakan single sign-on (SSO) atau AWS kredensialnya. 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 Wilayah AWS yang menjadi milik aset tersebut.
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), ketik (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.

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 portal DataZone data Amazon URL dan masuk menggunakan single sign-on (SSO) atau AWS kredensialnya. 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. Pemberi persetujuan 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 portal DataZone data Amazon URL dan masuk menggunakan single sign-on (SSO) atau AWS kredensialnya. 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. Untuk menyetujui, pilih di antara dua opsi:

   - Akses penuh: Jika Anda memilih untuk menyetujui langganan dengan opsi akses penuh, pelanggan akan mendapatkan akses ke semua baris dan kolom dalam aset data Anda.
   - Menyetujui dengan filter baris dan kolom: Untuk membatasi akses ke baris dan kolom data tertentu, Anda dapat memilih opsi untuk menyetujui dengan filter baris dan kolom. Untuk informasi selengkapnya, lihat Kontrol akses berbutir halus ke data di Amazon DataZone.
     - Pilih Pilih filter, lalu dari drop-down pilih satu atau beberapa filter yang tersedia yang ingin Anda terapkan ke langganan.

- Untuk membuat filter baru, Anda dapat memilih opsi Buat filter baru, yang membuka halaman baru untuk membuat filter baris atau kolom baru. Untuk informasi selengkapnya, silakan lihat Membuat filter kolom dan Membuat filter baris.

7. (Opsional) Masukkan respons yang menjelaskan alasan Anda menerima atau menolak permintaan.
8. 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, lihatPeristiwa dan notifikasi.

> **Note**
>
> Amazon DataZone mendukung kontrol akses berbutir halus untuk AWS Tabel lem, tabel Amazon Redshift, dan tampilan Amazon Redshift.

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 portal DataZone data Amazon URL dan masuk menggunakan single sign-on (SSO) atau AWS kredensialnya. 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 mencabutkannya. 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 portal DataZone data Amazon URL dan masuk menggunakan single sign-on (SSO) atau AWS kredensialnya. 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 portal DataZone data Amazon URL dan masuk menggunakan single sign-on (SSO) atau AWS kredensialnya. 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 IAM peran yang ada untuk memenuhi DataZone langganan Amazon

Dalam rilis saat ini, Amazon DataZone mendukung Anda menggunakan IAM peran 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 yang terkait AWS akun, Anda dapat menggunakan langkah-langkah berikut:

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

1. Arahkan ke halaman Dibagikan oleh saya: Berbagi sumber daya di AWS RAMkonsol.
2. Karena AWS RAMpembagian sumber daya ada secara spesifik AWS Daerah, pilih yang sesuai AWS Wilayah dari daftar dropdown di sudut kanan atas konsol.
3. Pilih pembagian sumber daya yang sesuai dengan DataZone domain Amazon Anda, lalu pilih Ubah. Anda dapat mengidentifikasi RAM pembagian untuk DataZone domain Amazon menggunakan nama atau ID domain saat RAM pembagian dibuat dengan nama:`DataZone-<domain-name>-<domain-id>`.
4. Pilih Berikutnya untuk melanjutkan ke langkah berikutnya di mana Anda dapat memeriksa versi RAM kebijakan dan memodifikasinya.
5. Pastikan bahwa versi RAM kebijakan 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 APIs hanya dengan menggunakan. Di bawah ini adalah beberapa contoh payload yang dapat Anda gunakan untuk membuat target berlangganan untuk memenuhi langganan Anda AWS Glue tabel dan tabel atau tampilan Amazon Redshift. 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

- Yang environmentIdentifier Anda gunakan dalam API panggilan di atas harus ada di akun terkait yang sama dari mana Anda melakukan API panggilan. Kalau tidak, API panggilan tidak akan berhasil.
- IAMPeran yang ARN Anda gunakan dalam authorizedPrincipals "" adalah peran yang DataZone akan diberikan 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 CREATE TABLE izin pada database ini.
- Juga pastikan bahwa peran (IAMperan untuk AWS Glue dan peran database untuk Amazon Redshift) disediakan sebagai prinsipal 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 tersebut. 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.

Berikan akses ke terkelola AWS Glue Data Catalog aset

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.

> **Note**
>
> Manajemen akses untuk AWS Glue Data Catalog Aset yang menggunakan AWS Lake Formation TBACMetode LF- tidak didukung.
> Support untuk berbagi aset lintas wilayah di AWS Glue Data Catalog tidak didukung.

Setelah permintaan berlangganan dikelola AWS Glue Data Catalog aset 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 yang disetujui AWS Glue Data Catalog tabel atas nama Anda melalui AWS Lake Formation. Untuk proyek pelanggan, aset yang diberikan muncul di AWS Glue Data Catalog sebagai sumber daya di akun Anda. Anda kemudian dapat menggunakan Amazon Athena untuk menanyakan tabel.

> **Note**
>
> Jika lingkungan data lake baru ditambahkan ke proyek setelah berlangganan AWS Glue Data Catalog aset telah ditambahkan secara otomatis ke lingkungan danau data yang ada, Anda harus menambahkan langganan ini secara manual AWS Glue Data Catalog aset 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.

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

- Bagian AWS Glue table harus dikelola Lake Formation karena Amazon DataZone memberikan akses dengan mengelola izin Lake Formation.
- Peran Kelola akses untuk lingkungan danau data yang digunakan untuk mempublikasikan AWS Tabel Glue Data Catalog harus memiliki izin Lake Formation berikut:
  - `DESCRIBE`dan `DESCRIBE GRANTABLE` izin pada AWS Glue database 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 AWS Lake Formation Panduan Pengembang.

Berikan akses ke aset Amazon Redshift yang dikelola

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.

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.
- Kluster 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.

Berikan akses untuk langganan yang disetujui ke aset yang tidak dikelola

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.

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 Lake Formation Managed AWS Tabel Glue Data Catalog dan 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 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 DataZone Acara dan pemberitahuan Amazon.

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 portal DataZone data Amazon URL dan masuk menggunakan single sign-on (SSO) atau AWS kredensialnya. 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
- Kueri data menggunakan Amazon Redshift

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 SQL kueri pada tabel dan melihat hasilnya di Amazon Athena. Untuk informasi lebih lanjut tentang penggunaan SQL di Amazon Athena, lihat SQLreferensi 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 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 CTAS sintaks, lihat CREATETABLEAS.

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, Anda`SELECT`pernyataan juga mencakup`WHERE`Klausul. Dalam kasus ini, kueri memilih hanya baris dari tabel yang memenuhi`WHERE`Klausul:

```
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 proyek Anda AWS Glue database, dan dapat dibuat 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 IAM identitas 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 IAM kredensi 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

Setiap tabel Amazon Redshift atau tampilan yang telah Anda langgani ditautkan ke cluster Amazon Redshift atau workgroup 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 Anda. IAM Setelah koneksi dibuat, Anda dapat melihat semua tabel dan tampilan yang dapat diakses lingkungan Anda di bawah database dev.

Kontrol akses berbutir halus ke data di Amazon DataZone

Dalam rilis Amazon saat ini DataZone, kontrol akses halus data Anda didukung, memungkinkan Anda memiliki kontrol akses terperinci atas data sensitif Anda. Anda dapat mengontrol proyek mana yang dapat mengakses catatan data tertentu dalam aset data yang dipublikasikan ke katalog data DataZone bisnis Amazon. Amazon DataZone mendukung filter baris dan kolom untuk menerapkan kontrol akses berbutir halus.

Filter baris memungkinkan Anda membatasi akses ke baris tertentu berdasarkan kriteria yang Anda tentukan. Misalnya, jika tabel Anda berisi data untuk dua wilayah (Amerika dan Eropa) dan Anda ingin memastikan bahwa karyawan di Eropa hanya dapat mengakses data yang relevan dengan wilayah mereka, Anda dapat membuat filter baris yang menyertakan baris di mana wilayahnya adalah Eropa (misalnya, wilayah = 'Eropa'). Dengan cara ini, karyawan di Eropa tidak akan memiliki akses ke data Amerika.

Filter kolom memungkinkan Anda membatasi akses ke kolom tertentu dalam aset data Anda. Misalnya, jika tabel Anda menyertakan informasi sensitif seperti Informasi Identifikasi Pribadi (PII), Anda dapat membuat filter kolom untuk mengecualikan PII kolom. Ini memastikan bahwa pelanggan hanya dapat mengakses data yang tidak sensitif.

Untuk memanfaatkan kontrol akses berbutir halus, Anda dapat membuat filter baris dan kolom untuk AWS Aset Glue dan Amazon Redshift di Amazon. DataZone Ketika permintaan berlangganan untuk mengakses aset data Anda diterima, Anda dapat menyetujuinya dengan menerapkan filter baris dan kolom yang sesuai. Amazon DataZone memastikan bahwa pelanggan hanya dapat mengakses baris dan kolom yang diizinkan oleh filter yang Anda terapkan pada saat persetujuan berlangganan.

Topik

Membuat filter baris

Amazon DataZone memungkinkan Anda membuat filter baris yang dapat Anda gunakan saat menyetujui langganan untuk memastikan bahwa pelanggan hanya dapat mengakses baris data seperti yang ditentukan dalam filter baris. Untuk membuat filter baris, ikuti langkah-langkah di bawah ini:

1. Arahkan ke portal DataZone data Amazon URL dan masuk menggunakan single sign-on (SSO) atau AWS kredensialnya. 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, lalu pilih aset yang ingin Anda buat filter baris. Anda dapat menambahkan filter baris jika aset data Anda di Amazon DataZone bertipe AWS Tabel lem, tabel Amazon Redshift, atau tampilan Amazon Redshift.
5. Pada halaman detail aset, buka tab Filter aset dan kemudian pilih Tambahkan filter aset.
6. Konfigurasi bidang berikut:
   - Nama - nama filter
   - Deskripsi — deskripsi filter
7. Di bawah jenis filter, pilih Filter baris.
8. Di bawah ekspresi filter baris, berikan satu atau lebih ekspresi untuk filter baris.
   - Pilih kolom dari kolom dari dropdown.
   - Pilih operator dari dropdown operator.
   - Masukkan nilai di bidang Nilai.
9. Untuk menambahkan kondisi lain ke ekspresi filter Anda, pilih Tambahkan kondisi.
10. Saat menggunakan beberapa kondisi dalam ekspresi filter baris, pilih Dan atau Atau untuk menautkan kondisi.
11. Pilih Buat filter.

Untuk informasi tentang cara menerapkan filter baris ke langganan, lihatMenyetujui atau menolak permintaan berlangganan.

Membuat filter kolom

Amazon DataZone memungkinkan Anda membuat filter kolom yang dapat Anda gunakan saat menyetujui langganan untuk memastikan bahwa pelanggan hanya dapat mengakses kolom data seperti yang ditentukan dalam filter kolom. Untuk membuat filter kolom, ikuti langkah-langkah di bawah ini:

1. Arahkan ke portal DataZone data Amazon URL dan masuk menggunakan single sign-on (SSO) atau AWS kredensialnya. 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, lalu pilih aset yang ingin Anda buat filter kolom. Anda dapat menambahkan filter kolom jika aset data Anda di Amazon DataZone bertipe AWS Tabel lem, tabel Amazon Redshift, atau tampilan Amazon Redshift.
5. Pada halaman detail aset, buka tab Filter aset dan kemudian pilih Tambahkan filter aset.
6. Konfigurasi bidang berikut:
   - Nama — nama filter
   - Deskripsi — deskripsi filter
7. Di bawah jenis filter, pilih Filter kolom.
8. Pilih kolom yang ingin Anda sertakan dalam filter menggunakan kotak centang lagi kolom dalam aset data.
9. Pilih Buat filter

Untuk informasi tentang cara menerapkan filter kolom ke langganan, lihatMenyetujui atau menolak permintaan berlangganan.

Menghapus filter baris atau kolom

Untuk menghapus filter baris atau kolom, ikuti langkah-langkah di bawah ini:

1. Arahkan ke portal DataZone data Amazon URL dan masuk menggunakan single sign-on (SSO) atau AWS kredensialnya. 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. Arahkan ke tab Data untuk proyek.
3. Pilih Data yang dipublikasikan atau Data inventaris dari panel navigasi kiri, lalu pilih aset tempat Anda ingin menghapus baris atau filter kolom.
4. Pada halaman detail aset, buka tab Filter aset dan kemudian buka filter yang ingin Anda hapus.
5. Pilih Tindakan, Hapus dan kemudian konfirmasikan penghapusan.

> **Note**
>
> Anda dapat menghapus filter hanya jika tidak digunakan dalam langganan aktif.

Mengedit filter baris atau kolom

Untuk mengedit filter baris atau kolom, ikuti langkah-langkah di bawah ini:

1. Arahkan ke portal DataZone data Amazon URL dan masuk menggunakan single sign-on (SSO) atau AWS kredensialnya. 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. Arahkan ke tab Data untuk proyek.
3. Pilih Data yang dipublikasikan atau Data inventaris dari panel navigasi kiri, lalu pilih aset tempat Anda ingin mengedit baris atau filter kolom.
4. Pada halaman detail aset, buka tab Filter aset dan kemudian buka filter yang ingin Anda edit.
5. Anda dapat mengedit bidang berikut:
   - Nama — nama filter
   - Deskripsi — deskripsi filter
6. Jika Anda mengedit filter baris, Anda dapat memperbarui ekspresi filter baris.
7. Jika Anda mengedit filter kolom, Anda dapat menambah atau menghapus kolom yang dipilih dalam filter.
8. Setelah Anda membuat perubahan, pilih Edit filter aset.

> **Note**
>
> Jika Anda mengedit filter yang digunakan dalam langganan aktif, Amazon DataZone akan secara otomatis memperbarui izin yang diberikan kepada proyek pelanggan. Ini berarti bahwa pelanggan hanya akan dapat mengakses baris atau kolom seperti yang didefinisikan dalam filter yang diperbarui, memastikan bahwa kebijakan akses data Anda diberlakukan secara konsisten.

Memberikan akses dengan filter

Amazon DataZone mengaktifkan kontrol akses berbutir halus dengan menerjemahkan filter baris dan kolom yang ditentukan ke dalam hibah yang sesuai AWS Lake Formation dan Amazon Redshift. Di bawah ini adalah penjelasan tentang bagaimana Amazon DataZone mewujudkan filter ini untuk keduanya AWS Glue tabel dan Amazon Redshift.

AWS Glue tabel

Saat berlangganan AWS Glue tabel dengan filter baris dan/atau kolom disetujui, Amazon DataZone mewujudkan langganan dengan membuat hibah di AWS Lake Formation dengan Filter Sel Data, memastikan bahwa anggota proyek pelanggan hanya dapat mengakses baris dan kolom yang diizinkan untuk diakses berdasarkan filter yang diterapkan pada langganan.

Amazon DataZone pertama-tama menerjemahkan filter baris dan kolom yang diterapkan di Amazon DataZone ke AWS Filter Sel Data Formasi Danau. Jika beberapa filter baris dan kolom digunakan, DataZone Amazon menyatukan semua kolom dan semua kondisi filter baris untuk menghitung izin efektif di tingkat baris dan kolom. Amazon DataZone kemudian membuat satu AWS Filter sel data Lake Formation menggunakan izin baris dan kolom yang efektif.

Setelah filter sel data dibuat, Amazon DataZone membagikan tabel berlangganan dengan proyek pelanggan dengan membuat izin read-only () di SELECT AWS Lake Formation menggunakan filter sel data ini.

Amazon Redshift

Saat berlangganan tabel/tampilan Amazon Redshift dengan filter baris dan/atau kolom disetujui, Amazon DataZone mewujudkan langganan dengan membuat tampilan pengikatan akhir yang tercakup ke bawah di Amazon Redshift, memastikan bahwa anggota proyek pelanggan hanya dapat

mengakses baris dan kolom yang diizinkan untuk diakses berdasarkan filter baris dan kolom yang diterapkan pada langganan.

Amazon DataZone pertama-tama menerjemahkan filter baris dan kolom yang diterapkan ke langganan di Amazon DataZone ke tampilan pengikatan akhir Amazon Redshift. Jika beberapa filter baris dan kolom digunakan, DataZone Amazon menyatukan semua kolom dan semua kondisi filter baris dari untuk menghitung izin efektif di tingkat baris dan kolom. Amazon DataZone kemudian membuat tampilan pengikatan akhir menggunakan izin baris dan kolom yang efektif.

Setelah tampilan pengikatan terlambat dibuat, Amazon DataZone membagikan tampilan ini dengan anggota proyek pelanggan dengan membuat izin read-only (SELECT) di Amazon Redshift.

DataZone Acara dan pemberitahuan 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.

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
Langganan	Permintaan berlangganan diterima	Acara dihasilkan saat permintaan berlangganan diterima	Peristiwa

Kategori acara	Nama peristiwa	Deskripsi acara	Jenis 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
Environment	Penerapan lingkungan gagal	Peristiwa dihasilkan saat penerapan lingkungan gagal	Peristiwa

Kategori acara	Nama peristiwa	Deskripsi acara	Jenis 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
Berlangganan	Langganan disetujui	Acara dihasilkan ketika langganan disetujui oleh pemilik proyek atau kontributor penerbitan	Peristiwa

Kategori acara	Nama peristiwa	Deskripsi acara	Jenis 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	Acara dihasilkan saat hibah langganan gagal	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

Kategori acara	Nama peristiwa	Deskripsi acara	Jenis 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
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 portal data URL dan masuk menggunakan SSO atau AWS kredensi. Jika Anda DataZone administrator Amazon, Anda dapat memperoleh portal data URL 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 portal data URL dan masuk menggunakan SSO atau AWS kredensi. Jika Anda DataZone administrator Amazon, Anda dapat memperoleh portal data URL 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.

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 dalam hal yang sama AWS akun 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 AWS dan kamu. Model tanggung jawab bersama menjelaskan hal ini sebagai keamanan cloud dan keamanan dalam cloud:

- Keamanan Cloud — AWS Bertanggung jawab untuk melindungi infrastruktur yang berjalan 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 AWS Program Kepatuhan . Untuk mempelajari tentang program kepatuhan yang berlaku untuk Amazon DataZone, lihat AWS Layanan dalam Lingkup oleh 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 belajar cara menggunakan yang lain AWS layanan yang membantu Anda memantau dan mengamankan DataZone sumber daya Amazon Anda.

Topik

- Domain untuk ditambahkan ke daftar izin Anda

Perlindungan data di Amazon DataZone

Bagian AWS model tanggung jawab bersama model berlaku untuk perlindungan data di Amazon DataZone. Seperti yang dijelaskan dalam model ini, AWS bertanggung jawab untuk melindungi infrastruktur global yang menjalankan semua AWS Cloud. Anda bertanggung jawab untuk menjaga kontrol atas konten Anda yang di-host di infrastruktur ini. Anda juga bertanggung jawab atas konfigurasi keamanan dan tugas manajemen untuk Layanan AWS yang Anda gunakan. Untuk informasi selengkapnya tentang privasi data, lihat Privasi Data FAQ. Untuk informasi tentang perlindungan data di Eropa, lihat AWS Model Tanggung Jawab Bersama dan posting GDPR blog di AWS Blog Keamanan.

Untuk tujuan perlindungan data, kami menyarankan Anda untuk melindungi Akun AWS kredensi 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 otentikasi multi-faktor (MFA) dengan setiap akun.
- GunakanSSL/TLSuntuk berkomunikasi dengan AWS sumber daya. Kami membutuhkan TLS 1.2 dan merekomendasikan TLS 1.3.
- Siapkan API dan pencatatan aktivitas pengguna dengan AWS CloudTrail. Untuk informasi tentang menggunakan CloudTrail jalur untuk menangkap AWS kegiatan, lihat Bekerja dengan CloudTrail jalan setapak di AWS CloudTrail Panduan Pengguna.
- Gunakan AWS solusi 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 FIPS 140-3 modul kriptografi yang divalidasi saat mengakses AWS melalui antarmuka baris perintah atauAPI, gunakan FIPS titik akhir. Untuk informasi selengkapnya tentang FIPS titik akhir yang tersedia, lihat Federal Information Processing Standard (FIPS) 140-3.

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 ketika Anda bekerja dengan Amazon DataZone atau lainnya Layanan

AWS menggunakan konsol,API, AWS CLI, atau AWS SDKs. 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. Jika Anda memberikan URL ke server eksternal, kami sangat menyarankan agar Anda tidak menyertakan informasi kredensil dalam URL untuk memvalidasi permintaan Anda ke server tersebut.

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

Enkripsi bergerak

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

Privasi lalu lintas antar jaringan

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

Topik

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

Meskipun Anda tidak dapat menonaktifkan lapisan enkripsi ini atau memilih jenis enkripsi alternatif, Anda dapat menambahkan lapisan enkripsi kedua di atas yang ada AWS memiliki kunci enkripsi 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 yang ada AWS enkripsi yang dimiliki. 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 IAM kebijakan dan hibah
- 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 AWS kunci yang dimiliki untuk melindungi data pelanggan tanpa biaya.

AWS KMSbiaya berlaku untuk menggunakan kunci yang dikelola pelanggan. Untuk informasi selengkapnya tentang harga, lihat AWS Harga Layanan Manajemen Kunci.

Bagaimana Amazon DataZone menggunakan hibah di AWS KMS

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 CreateGrant AWS KMS. Hibah di AWS KMSdigunakan untuk memberi Amazon DataZone akses ke KMS kunci 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 KMSuntuk memverifikasi bahwa ID KMS kunci terkelola pelanggan simetris yang dimasukkan saat membuat koleksi DataZone domain Amazon valid.
- Kirim GenerateDataKeyrequestske AWS KMSuntuk menghasilkan kunci data yang dienkripsi oleh kunci yang dikelola pelanggan Anda.
- Kirim permintaan Dekripsi ke AWS KMSuntuk 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 Konsol Manajemen, atau AWS KMS APIs.

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

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

- kms: CreateGrant — menambahkan hibah ke kunci yang dikelola pelanggan. Memberikan akses kontrol ke KMS kunci tertentu, yang memungkinkan akses ke operasi hibah yang DataZone dibutuhkan Amazon. Untuk informasi selengkapnya tentang Menggunakan Hibah, lihat AWS Panduan Pengembang Layanan Manajemen Kunci.
- kms: DescribeKey — menyediakan detail kunci yang dikelola pelanggan untuk memungkinkan Amazon DataZone memvalidasi kunci.
- kms: GenerateDataKey — mengembalikan kunci data simetris unik untuk digunakan di luar AWS KMS.
- 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 KMS kebijakan tidak diterapkan untuk sumber daya yang diakses melalui portal DataZone data Amazon.

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

Untuk informasi selengkapnya tentang pemecahan masalah akses kunci, lihat AWS Panduan Pengembang Layanan Manajemen 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 KMSmenggunakan konteks enkripsi sebagai data otentikasi tambahan untuk mendukung enkripsi yang diautentikasi. Bila Anda menyertakan konteks enkripsi dalam permintaan untuk mengenkripsi data, AWS KMSmengikat 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 CloudWatch Log Amazon.

Menggunakan konteks enkripsi untuk mengontrol akses ke kunci terkelola pelanggan Anda - Anda dapat menggunakan konteks enkripsi dalam kebijakan dan IAM kebijakan utama 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 AWS KMSkunci terkelola pelanggan dengan DataZone sumber daya Amazon Anda, Anda dapat menggunakan AWS CloudTrailuntuk melacak permintaan yang DataZone dikirimkan Amazon AWS KMS. Contoh berikut adalah AWS CloudTrail peristiwa untuk`CreateGrant`,, `GenerateDataKeyDecrypt`, dan `DescribeKey` untuk memantau KMS operasi yang dipanggil oleh Amazon DataZone untuk mengakses data yang dienkripsi oleh kunci yang dikelola pelanggan Anda. Saat Anda menggunakan AWS KMSkunci yang dikelola pelanggan untuk mengenkripsi DataZone domain Amazon Anda, Amazon DataZone mengirimkan `CreateGrant` permintaan atas nama Anda untuk mengakses KMS kunci di AWS akun. Hibah yang DataZone dibuat Amazon khusus untuk sumber daya yang terkait dengan AWS KMSkunci yang dikelola pelanggan. 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 terenkripsi AWS Katalog Glue

Dalam kasus penggunaan lanjutan, ketika Anda bekerja dengan AWS Glue katalog yang dienkripsi, Anda harus memberikan akses ke DataZone layanan Amazon untuk menggunakan kunci yang dikelola pelanggan KMS Anda. Anda dapat melakukan ini dengan memperbarui KMS kebijakan kustom Anda dan menambahkan tag ke kunci. Untuk memberikan akses ke DataZone layanan Amazon untuk bekerja dengan data dalam terenkripsi AWS Katalog Glue, lengkapi yang berikut ini:

- Tambahkan kebijakan berikut ke KMS kunci 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 KMS kunci kustom Anda. Untuk informasi selengkapnya, lihat Menggunakan tag untuk mengontrol akses ke KMS kunci.

```
key: AmazonDataZoneEnvironment
value: all
```

Menggunakan VPC Endpoint Antarmuka untuk Amazon DataZone

Jika Anda menggunakan Amazon Virtual Private Cloud (AmazonVPC) untuk meng-host AWS sumber daya, Anda dapat membuat koneksi antara Amazon VPC dan Amazon Anda DataZone. Anda dapat menggunakan koneksi ini dengan Amazon DataZone tanpa melintasi internet publik.

Amazon VPC memungkinkan Anda meluncurkan AWS sumber daya dalam jaringan virtual kustom. Anda dapat menggunakan a VPC untuk mengontrol pengaturan jaringan Anda, seperti rentang alamat IP, subnet, tabel rute, dan gateway jaringan. Untuk informasi selengkapnyaVPCs, lihat Panduan VPC Pengguna Amazon.

Untuk menghubungkan Amazon Anda VPC ke Amazon DataZone, Anda harus terlebih dahulu menentukan VPC titik akhir antarmuka, yang memungkinkan Anda menghubungkan Anda VPC ke yang lain AWS layanan. Titik akhir menyediakan konektivitas yang andal dan dapat diskalakan, tanpa memerlukan gateway internet, instance terjemahan alamat jaringan (NAT), atau VPN koneksi. Untuk informasi selengkapnya dan langkah-langkah mendetail tentang cara membuat VPC titik akhir, lihat Titik VPC Akhir Antarmuka (AWS PrivateLink) di Panduan VPC Pengguna Amazon.

> **Important**
>
> DiVPC, kebijakan endpoint adalah kebijakan berbasis sumber daya yang dapat Anda lampirkan ke titik akhir untuk mengontrol yang mana VPC AWS prinsipal dapat menggunakan titik akhir untuk mengakses AWS layanan.
> Dalam rilis Amazon saat ini DataZone, penggunaan kebijakan endpoint tidak didukung untuk membuat dan menggunakan koneksi antara Amazon VPC dan Amazon DataZone Anda.
> Manajemen DataZone akses Amazon bergantung pada RAM konfigurasi dan kebijakan IAM utama yang ditentukan pada tingkat layanan.

Otorisasi di Amazon DataZone

Antarmuka DataZone Amazon terdiri dari konsol manajemen di dalamnya AWS dan aplikasi web off-console (portal data).

Konsol DataZone manajemen Amazon dapat digunakan oleh AWS administrator untuk top-level-resource APIs, termasuk membuat dan mengelola domain, AWS asosiasi akun untuk domain ini, dan sumber data yang ingin Anda delegasikan manajemen akses ke Amazon. DataZone Anda dapat menggunakan konsol DataZone manajemen Amazon untuk mengelola semua IAM peran dan konfigurasi yang diperlukan untuk mendelegasikan kontrol manajemen akses ke DataZone layanan Amazon untuk dikonfigurasi secara eksplisit AWS akun. Portal DataZone data Amazon adalah pihak pertama AWS Aplikasi Pusat Identitas untuk SSO pengguna. Jika diaktifkan, konsol juga dapat digunakan oleh IAM kepala sekolah yang berwenang untuk bergabung ke portal data alih-alih menggunakan identitas. SSO

Portal data Amazon DataZone dirancang untuk digunakan terutama oleh AWS IAMPengguna yang diautentikasi Pusat Identitas 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 IAM otorisasi. Konsol digunakan oleh administrator terutama untuk pengaturan. Amazon DataZone menggunakan konsep administrator domain AWS akun, dan anggota AWS akun, dan konsol digunakan dari semua akun ini untuk membangun hubungan kepercayaan sambil menghormati AWS Batasan organisasi.

Otorisasi di portal Amazon DataZone

Model otorisasi portal DataZone data Amazon adalah hierarkis ACL 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 IAM sesi 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 IAM pekerjaan 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 membutuhkan AWS Identity and Access Management (IAM) untuk menyelesaikan tugas-tugas terkait keamanan berikut:

- Buat pengguna dan grup di bawah 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.
- Buat peran untuk Anda Akun AWS dan menentukan pengguna atau layanan yang dapat mengasumsikan mereka.
- Gunakan identitas yang ada untuk perusahaan Anda untuk memberikan izin untuk melakukan tugas menggunakan AWS sumber daya

Untuk informasi selengkapnyaIAM, 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

Sesi AWS kebijakan 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 AWS kebijakan terkelola mungkin tidak memberikan izin hak istimewa paling sedikit untuk kasus penggunaan spesifik Anda karena tersedia untuk semua AWS pelanggan untuk digunakan. 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 AWS kebijakan terkelola. Jika AWS memperbarui izin yang ditentukan dalam AWS kebijakan terkelola, pembaruan memengaruhi semua identitas utama (pengguna, grup, dan peran) yang dilampirkan kebijakan tersebut. AWS kemungkinan besar akan memperbarui AWS kebijakan terkelola saat baru Layanan AWS diluncurkan atau API operasi baru tersedia untuk layanan yang ada.

Untuk informasi selengkapnya, silakan lihat AWS kebijakan terkelola dalam Panduan IAM Pengguna.

Daftar Isi

AWS kebijakan terkelola: AmazonDataZoneFullAccess

Anda dapat melampirkan `AmazonDataZoneFullAccess` kebijakan ke IAM identitas 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 di seluruh DataZone Akun AWS.
- `iam`— Memungkinkan kepala sekolah untuk membuat daftar dan meneruskan peran dan mendapatkan kebijakan.
- `sso`— Memungkinkan kepala sekolah untuk mendapatkan daerah di mana AWS IAM Identity Center diaktifkan.
- `secretsmanager`— Memungkinkan kepala sekolah untuk membuat, menandai, dan daftar rahasia dengan awalan tertentu.

```
{
    "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",
                "ram:ListResourceSharePermissions"
            ],
            "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": "DataZoneTagOnCreateDomainProjectTags",
            "Effect": "Allow",
```

```
            "Action": [
                "secretsmanager:TagResource"
            ],
            "Resource": "arn:aws:secretsmanager:*:*:secret:AmazonDataZone-*",
            "Condition": {
                "ForAllValues:StringEquals": {
                    "aws:TagKeys": [
                        "AmazonDataZoneDomain",
                        "AmazonDataZoneProject"
                    ]
                },
                "StringLike": {
                    "aws:RequestTag/AmazonDataZoneDomain": "dzd_*",
                    "aws:ResourceTag/AmazonDataZoneDomain": "dzd_*"
                }
            }
        },
        {
            "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_*"
                }
            }
        },
        {
            "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 milik Anda sendiri AWS KMS kunci, Anda harus memiliki izin agar `kms:CreateGrant` pembuatan domain berhasil, dan `kms:Decrypt` untuk`kms:GenerateDataKey`, agar kunci itu memanggil Amazon lain DataZone APIs 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 KMS kunci bawaan yang dimiliki layanan, maka ini tidak diperlukan.

  Untuk informasi selengkapnya, silakan 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 IAM izin yang diperlukan untuk membuat IAM peran 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 AWS IAM Identity Center login pengguna diaktifkan, atau jika Anda mengaktifkannya untuk domain yang ada di Amazon DataZone, Anda harus memiliki izin untuk yang berikut:
  - organisasi: DescribeOrganization
  - organisasi: ListDelegatedAdministrators
  - sso: CreateInstance
  - sso: ListInstances
  - sso: GetSharedSsoConfiguration
  - sso: PutApplicationGrant

- sso: PutApplicationAssignmentConfiguration
- sso: PutApplicationAuthenticationMethod
- sso: PutApplicationAccessScope
- sso: CreateApplication
- sso: DeleteApplication
- sso: CreateApplicationAssignment
- sso: DeleteApplicationAssignment

- Untuk menerima AWS permintaan asosiasi 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:AcceptPredictions",
    "datazone:AcceptSubscriptionRequest",
    "datazone:AddEntityOwner",
    "datazone:AddPolicyGrant",
    "datazone:CancelMetadataGenerationRun",
    "datazone:CancelSubscription",
    "datazone:CreateAsset",
    "datazone:CreateAssetFilter",
    "datazone:CreateAssetRevision",
    "datazone:CreateAssetType",
    "datazone:CreateDataProduct",
    "datazone:CreateDataProductRevision",
    "datazone:CreateDataSource",
    "datazone:CreateDomainUnit",
```

```
    "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:DeleteAssetFilter",
    "datazone:DeleteAssetType",
    "datazone:DeleteDataProduct",
    "datazone:DeleteDataSource",
    "datazone:DeleteDomainUnit",
    "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:DeleteTimeSeriesDataPoints",
    "datazone:GetAsset",
    "datazone:GetAssetFilter",
    "datazone:GetAssetType",
    "datazone:GetDataProduct",
    "datazone:GetDataSource",
    "datazone:GetDataSourceRun",
    "datazone:GetDomain",
    "datazone:GetDomainUnit",
    "datazone:GetEnvironment",
    "datazone:GetEnvironmentActionLink",
    "datazone:GetEnvironmentBlueprint",
    "datazone:GetEnvironmentCredentials",
    "datazone:GetEnvironmentProfile",
    "datazone:GetFormType",
```

```
    "datazone:GetGlossary",
    "datazone:GetGlossaryTerm",
    "datazone:GetGroupProfile",
    "datazone:GetIamPortalLoginUrl",
    "datazone:GetLineageNode",
    "datazone:GetListing",
    "datazone:GetMetadataGenerationRun",
    "datazone:GetProject",
    "datazone:GetSubscription",
    "datazone:GetSubscriptionEligibility",
    "datazone:GetSubscriptionGrant",
    "datazone:GetSubscriptionRequestDetails",
    "datazone:GetSubscriptionTarget",
    "datazone:GetTimeSeriesDataPoint",
    "datazone:GetUserProfile",
    "datazone:ListAccountEnvironments",
    "datazone:ListAssetFilters",
    "datazone:ListAssetRevisions",
    "datazone:ListDataProductRevisions",
    "datazone:ListDataSourceRunActivities",
    "datazone:ListDataSourceRuns",
    "datazone:ListDataSources",
    "datazone:ListDomainUnitsForParent",
    "datazone:ListEntityOwners",
    "datazone:ListEnvironmentBlueprintConfigurations",
    "datazone:ListEnvironmentBlueprints",
    "datazone:ListEnvironmentProfiles",
    "datazone:ListEnvironments",
    "datazone:ListGroupsForUser",
    "datazone:ListLineageNodeHistory",
    "datazone:ListMetadataGenerationRuns",
    "datazone:ListNotifications",
    "datazone:ListPolicyGrants",
    "datazone:ListProjectMemberships",
    "datazone:ListProjects",
    "datazone:ListSubscriptionGrants",
    "datazone:ListSubscriptionRequests",
    "datazone:ListSubscriptionTargets",
    "datazone:ListSubscriptions",
    "datazone:ListTimeSeriesDataPoints",
    "datazone:ListWarehouseMetadata",
    "datazone:PostTimeSeriesDataPoints",
    "datazone:RejectPredictions",
    "datazone:RejectSubscriptionRequest",
```

```
    "datazone:RemoveEntityOwner",
    "datazone:RemovePolicyGrant",
    "datazone:RevokeSubscription",
    "datazone:Search",
    "datazone:SearchGroupProfiles",
    "datazone:SearchListings",
    "datazone:SearchTypes",
    "datazone:SearchUserProfiles",
    "datazone:StartDataSourceRun",
    "datazone:StartMetadataGenerationRun",
    "datazone:UpdateAssetFilter",
    "datazone:UpdateDataSource",
    "datazone:UpdateDomainUnit",
    "datazone:UpdateEnvironment",
    "datazone:UpdateEnvironmentBlueprint",
    "datazone:UpdateEnvironmentDeploymentStatus",
    "datazone:UpdateEnvironmentProfile",
    "datazone:UpdateGlossary",
    "datazone:UpdateGlossaryTerm",
    "datazone:UpdateProject",
    "datazone:UpdateSubscriptionGrantStatus",
    "datazone:UpdateSubscriptionRequest"
   ],
   "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 IAM entitas di IAM Panduan Pengguna.

Saat Anda membuat lingkungan melalui portal DataZone data Amazon, Amazon DataZone menerapkan batas izin ini ke IAMperan 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 IAM prinsipal yang disediakan yang dilampirkan. Prinsipal mungkin mengambil bentuk peran pengguna yang DataZone dapat diasumsikan Amazon atas nama pengguna perusahaan interaktif atau layanan analitik (AWS Glue, misalnya), dan kemudian melakukan tindakan untuk memproses data seperti membaca dan menulis dari Amazon S3 atau menjalankan Perayap AWS Glue.

`AmazonDataZoneEnvironmentRolePermissionsBoundary`Kebijakan ini memberikan akses baca dan tulis untuk Amazon DataZone ke layanan seperti AWS Glue Amazon S3, AWS Lake 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 dan AWS KMS kunci.

Amazon DataZone menerapkan `AmazonDataZoneEnvironmentRolePermissionsBoundary` AWS kebijakan 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 meliputi pernyataan berikut: JSON

```
{
  "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

Bagian AmazonDataZoneRedshiftGlueProvisioningPolicy kebijakan memberikan 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 AWS Glue data ke katalog. Ini juga memberikan DataZone izin Amazon untuk memberikan akses atau mencabut akses ke AWS Glue menerbitkan aset dalam katalog.

```
{
 "Version": "2012-10-17",
 "Statement": [
  {
   "Sid": "GlueTagDatabasePermissions",
   "Effect": "Allow",
   "Action": [
    "glue:TagResource",
    "glue:UntagResource",
    "glue:GetTags"
   ],
   "Resource": "*",
   "Condition": {
    "StringEquals": {
     "aws:ResourceAccount": "${aws:PrincipalAccount}"
    },
    "ForAnyValue:StringLikeIfExists": {
     "aws:TagKeys": "DataZoneDiscoverable_*"
    }
   }
  },
  {
   "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:CreateDataCellsFilter",
    "lakeformation:CreateLakeFormationOptIn",
    "lakeformation:DeleteDataCellsFilter",
    "lakeformation:DeleteLakeFormationOptIn",
    "lakeformation:GrantPermissions",
    "lakeformation:GetDataCellsFilter",
    "lakeformation:GetResourceLFTags",
    "lakeformation:ListDataCellsFilter",
    "lakeformation:ListLakeFormationOptIns",
    "lakeformation:ListPermissions",
    "lakeformation:RegisterResource",
    "lakeformation:RevokePermissions",
    "lakeformation:UpdateDataCellsFilter",
```

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

AWS kebijakan terkelola: AmazonDataZoneCrossAccountAdmin

Anda dapat melampirkan AmazonDataZoneCrossAccountAdmin kebijakan ke IAM identitas 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. Peran ini menyediakan akses ke semua Amazon DataZone APIs yang diperlukan untuk penggunaan portal data, serta RAM izin untuk mendukung penggunaan akun terkait di 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:AddEntityOwner",
    "datazone:AddPolicyGrant",
    "datazone:CancelMetadataGenerationRun",
    "datazone:CancelSubscription",
    "datazone:CreateAsset",
    "datazone:CreateAssetFilter",
    "datazone:CreateAssetRevision",
    "datazone:CreateAssetType",
    "datazone:CreateDataProduct",
    "datazone:CreateDataProductRevision",
    "datazone:CreateDataSource",
    "datazone:CreateDomainUnit",
    "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:DeleteAssetFilter",
    "datazone:DeleteAssetType",
    "datazone:DeleteDataProduct",
    "datazone:DeleteDataSource",
    "datazone:DeleteDomainUnit",
    "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:DeleteTimeSeriesDataPoints",
    "datazone:GetAsset",
    "datazone:GetAssetFilter",
    "datazone:GetAssetType",
    "datazone:GetDataProduct",
    "datazone:GetDataSource",
    "datazone:GetDataSourceRun",
    "datazone:GetDomain",
    "datazone:GetDomainUnit",
    "datazone:GetEnvironment",
    "datazone:GetEnvironmentAction",
    "datazone:GetEnvironmentActionLink",
    "datazone:GetEnvironmentBlueprint",
    "datazone:GetEnvironmentCredentials",
    "datazone:GetEnvironmentProfile",
    "datazone:GetFormType",
    "datazone:GetGlossary",
    "datazone:GetGlossaryTerm",
    "datazone:GetGroupProfile",
    "datazone:GetLineageNode",
    "datazone:GetListing",
    "datazone:GetMetadataGenerationRun",
    "datazone:GetProject",
    "datazone:GetSubscription",
    "datazone:GetSubscriptionEligibility",
    "datazone:GetSubscriptionGrant",
    "datazone:GetSubscriptionRequestDetails",
    "datazone:GetSubscriptionTarget",
    "datazone:GetTimeSeriesDataPoint",
    "datazone:GetUserProfile",
    "datazone:ListAccountEnvironments",
    "datazone:ListAssetFilters",
    "datazone:ListAssetRevisions",
    "datazone:ListDataProductRevisions",
    "datazone:ListDataSourceRunActivities",
    "datazone:ListDataSourceRuns",
```

```
    "datazone:ListDataSources",
    "datazone:ListDomainUnitsForParent",
    "datazone:ListEntityOwners",
    "datazone:ListEnvironmentActions",
    "datazone:ListEnvironmentBlueprintConfigurationSummaries",
    "datazone:ListEnvironmentBlueprintConfigurations",
    "datazone:ListEnvironmentBlueprints",
    "datazone:ListEnvironmentProfiles",
    "datazone:ListEnvironments",
    "datazone:ListGroupsForUser",
    "datazone:ListLineageNodeHistory",
    "datazone:ListMetadataGenerationRuns",
    "datazone:ListNotifications",
    "datazone:ListPolicyGrants",
    "datazone:ListProjectMemberships",
    "datazone:ListProjects",
    "datazone:ListSubscriptionGrants",
    "datazone:ListSubscriptionRequests",
    "datazone:ListSubscriptionTargets",
    "datazone:ListSubscriptions",
    "datazone:ListTimeSeriesDataPoints",
    "datazone:ListWarehouseMetadata",
    "datazone:RejectPredictions",
    "datazone:RejectSubscriptionRequest",
    "datazone:RemoveEntityOwner",
    "datazone:RemovePolicyGrant",
    "datazone:RevokeSubscription",
    "datazone:Search",
    "datazone:SearchGroupProfiles",
    "datazone:SearchListings",
    "datazone:SearchTypes",
    "datazone:SearchUserProfiles",
    "datazone:StartDataSourceRun",
    "datazone:StartMetadataGenerationRun",
    "datazone:UpdateAssetFilter",
    "datazone:UpdateDataSource",
    "datazone:UpdateDomainUnit",
    "datazone:UpdateEnvironment",
    "datazone:UpdateEnvironmentBlueprint",
    "datazone:UpdateEnvironmentDeploymentStatus",
    "datazone:UpdateEnvironmentProfile",
    "datazone:UpdateGlossary",
    "datazone:UpdateGlossaryTerm",
    "datazone:UpdateProject",
```

```
    "datazone:UpdateSubscriptionGrantStatus",
    "datazone:UpdateSubscriptionRequest"
   ],
   "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 suatu topik. SNS
- config — mengambil informasi tentang perekam konfigurasi, sumber daya, dan AWS Aturan Config. Juga memungkinkan peran terkait layanan untuk membuat dan menghapus AWS Aturan konfigurasi, dan untuk 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 IAM entitas di IAM Panduan Pengguna.

Saat Anda membuat SageMaker lingkungan Amazon melalui portal DataZone data Amazon, Amazon DataZone menerapkan batas izin ini ke IAM peran 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 IAM prinsipal yang disediakan yang dilampirkan. Prinsipal mungkin mengambil bentuk peran pengguna yang DataZone dapat diasumsikan Amazon atas nama pengguna perusahaan interaktif atau layanan analitik (AWS SageMaker, misalnya), dan kemudian melakukan tindakan untuk memproses data seperti membaca dan menulis dari Amazon S3 atau Amazon Redshift atau menjalankan AWS Glue crawler.

`AmazonDataZoneSageMakerEnvironmentRolePermissionsBoundary`Kebijakan ini memberikan akses baca dan tulis untuk Amazon DataZone ke layanan seperti Amazon SageMaker, AWS Glue, Amazon S3, AWS Lake 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 AmazonECR, dan AWS KMSkunci. 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": "*"
  }
 ]
}
```

DataZone Pembaruan Amazon ke AWS kebijakan terkelola

Lihat detail tentang pembaruan AWS kebijakan terkelola untuk Amazon DataZone sejak layanan ini mulai melacak perubahan ini. Untuk peringatan otomatis tentang perubahan pada halaman ini, berlangganan RSS umpan di halaman riwayat DataZone Dokumen Amazon.

Perubahan	Deskripsi	Tanggal
AmazonDataZoneDomainExecutionRolePolicy dan AmazonDataZoneFullUserAccess - pembaruan kebijakan	Pembaruan kebijakan untuk AmazonDataZoneDomainExecutionRolePolicydan AmazonDataZoneFullUserAccess- untuk mengaktifkan dukungan untuk yang baru APIs yang digunakan untuk membuat dan mengelola unit DataZone domain Amazon dan produk data.	31 Juli 2024
AmazonDataZoneGlueManageAccessRolePolicy - pembaruan kebijakan	Pembaruan kebijakan ke AmazonDataZoneGlueManageAccessRolePo	2 Juli 2024

Perubahan	Deskripsi	Tanggal
	licy- Amazon DataZone menambahkan IAM izin yang digunakan untuk fungsiona litas kontrol akses berbutir halus untuk mengurang i pemberian izin di Lake Formation.	
AmazonDataZoneExec utionRolePolicy dan AmazonDataZoneFull UserAccess - pembaruan kebijakan	Pembaruan kebijakan ke AmazonDataZoneExec utionRolePolicy dan AmazonDataZoneFull UserAccessuntuk mengaktif kan dukungan untuk garis keturunan data dan kontrol akses berbutir halus. APIs	27 Juni 2024
AmazonDataZoneGlue ManageAccessRolePolicy - pembaruan kebijakan	Pembaruan kebijakan untuk AmazonDataZoneGlue ManageAccessRolePo licyyang menambahkan IAM izin yang diperlukan untuk fungsionalitas berlangga nan mandiri DataZone di Amazon untuk mengurang i izin yang diberikan dalam pembentukan danau. Dengan fungsi berlangganan mandiri, izin pembentukan danau hanya dapat diberikan kepada sumber daya yang ditandai.	14 Juni 2024

Perubahan	Deskripsi	Tanggal
AmazonDataZoneDomainExecutionRolePolicy - pembaruan kebijakan	Pembaruan kebijakan untuk AmazonDataZoneDomainExecutionRolePolicyyang menambahkan baru APIs ke Amazon DataZone yang memungkinkan pengguna mengonfigurasi tindakan untuk DataZone lingkungan Amazon mereka.	14 Juni 2024
AmazonDataZoneFullAccess - pembaruan kebijakan	Pembaruan kebijakan untuk AmazonDataZoneFullAccessyang memungkinkan konsol DataZone manajemen Amazon membuat rahasia atas nama pengguna dengan tag domain dan proyek. Juga termasuk `ram:ListResourceSharePermissions` tindakan untuk mengaktifkan administrasi dari akun pemilik domain untuk melihat status asosiasi akun dari akun terkait.	14 Juni 2024

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 IAM peran yang dihasilkan selama pembuatan lingkungan. Batas izin membatasi cakupan peran yang DataZone dibuat Amazon dan peran apa pun yang Anda tambahkan.	30 April 2024
AmazonDataZoneSageMakerAccess - kebijakan baru	Kebijakan baru yang disebut AmazonDataZoneSageMakerAccessmemberikan DataZone izin Amazon untuk mempublikasikan 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.	30 April 2024

Perubahan	Deskripsi	Tanggal
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.	30 April 2024
AmazonDataZoneSageMakerProvisioning - kebijakan baru	Kebijakan baru yang disebut AmazonDataZoneSageMakerProvisioningmemberikan Amazon izin DataZone yang diperlukan untuk berinteraksi dengan Amazon. SageMaker	30 April 2024
AmazonDataZoneS3Manage-<region>-< domainId > - peran baru	Peran baru yang disebut AmazonDataZoneS3Manage--< domainId > <region>yang digunakan saat Amazon memanggil DataZone 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

Perubahan	Deskripsi	Tanggal
AmazonDataZoneGlue ManageAccessRolePolicy - Pembaruan kebijakan	Memperbarui AmazonDat aZoneGlueManageAcc essRolePolicyuntuk mengaktif kan dukungan untuk izin yang memungkinkan Amazon DataZone mengaktifkan penerbitan dan akses hibah ke data.	1 April 2024
AmazonDataZoneDoma inExecutionRolePolicy dan AmazonDataZoneFull UserAccess - Pembaruan kebijakan	Memperbarui AmazonDat aZoneDomainExecuti onRolePolicydan AmazonDat aZoneFullUserAccessuntuk mengaktifkan dukungan untuk `CancelMetadataGene rationRun` API.	Maret 29, 2024
AmazonDataZoneFullAccess - Pembaruan kebijakan	Memperbarui `AmazonDat aZoneFullAccess` untuk memungkinkan pengguna memilih rahasia, cluster, vpc, dan subnet mereka di konsol DataZone manajemen Amazon daripada mengetikn ya di kotak teks.	Maret 13, 2024

Perubahan	Deskripsi	Tanggal
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
AmazonDataZoneGlueManageAccessRolePolicy - Pembaruan kebijakan	Memperbarui AmazonDataZoneGlueManageAccessRolePolicyuntuk mengaktifkan dukungan untuk AWS Mode hibrida Lake Formation.	14 Desember 2023
AmazonDataZoneFullUserAccess dan AmazonDataZoneDomainExecutionRolePolicy - Pembaruan kebijakan	Memperbarui AmazonDataZoneFullUserAccessdan AmazonDataZoneDomainExecutionRolePolicykebijakan untuk mendukung fungsionalitas deskripsi data bertenaga AI generatif di Amazon. DataZone	28 November 2023

Perubahan	Deskripsi	Tanggal
AmazonDataZoneEnvironmentRolePermissionsBoundary - Pembaruan kebijakan	Amazon DataZone membuat pembaruan pada kebijakan AmazonDataZoneEnvironmentRolePermissionsBoundaryterkelola yang terdiri dari `athena:GetQueryResultsStream` izin tambahan yang tercakup dengan kondisi tersebut`ResourceTag` .	17 November 2023
AmazonDataZoneRedshiftManageAccessRolePolicy - Pembaruan kebijakan	Amazon DataZone memperbarui AmazonDataZoneRedshiftManageAccessRolePolicydengan menghapus cek pada ID organisasi untuk `redshift:AssociateDataShareConsumer` tindakan tersebut. Ini memungkinkan Anda untuk berbagi sumber daya AWS organisasi.	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.	Oktober 02, 2023

Perubahan	Deskripsi	Tanggal
AmazonDataZonePortalFullAccessPolicy - kebijakan usang	Amazon DataZone menghentikan. AmazonDataZonePortalFullAccessPolicy	September 29, 2023
AmazonDataZonePreviewConsoleFullAccess - kebijakan usang	Amazon DataZone menghentikan. AmazonDataZonePreviewConsoleFullAccess	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` .	25 September 2023

Perubahan	Deskripsi	Tanggal
AmazonDataZoneCrossAccountAdmin - Kebijakan baru	Amazon DataZone menambahkan kebijakan baru yang disebut AmazonDataZoneCrossAccountAdminyang memungkinkan pengguna untuk bekerja dengan Amazon DataZone dan akun terkaitnya.	September 19, 2023
AmazonDataZoneFullUserAccess - Kebijakan baru	Amazon DataZone menambahkan kebijakan baru yang disebut AmazonDataZoneFullUserAccessyang memberikan akses penuh ke Amazon DataZone, tetapi tidak mengizinkan pengelolaan domain, pengguna, atau akun terkait.	12 September 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.	12 September 2023

Perubahan	Deskripsi	Tanggal
AmazonDataZoneGlue ManageAccessRolePolicy - Kebijakan baru	Amazon DataZone menambahkan kebijakan baru yang disebut AmazonDat aZoneGlueManageAcc essRolePolicyyang memberika n DataZone izin Amazon untuk mempublikasikan AWS Glue data ke katalog. Ini juga memberikan DataZone izin Amazon untuk memberikan akses atau mencabut akses ke AWS Glue menerbitkan aset dalam katalog.	12 September 2023
AmazonDataZoneReds hiftGlueProvisioningPolicy - Kebijakan baru	Amazon DataZone menambahkan kebijakan baru yang disebut AmazonDat aZoneRedshiftGlueProvisioni ngPolicyyang memberikan Amazon izin DataZone yang diperlukan untuk berinteraksi dengan sumber data yang didukung.	12 September 2023
AmazonDataZoneEnvi ronmentRolePermiss ionsBoundary - Kebijakan baru	Amazon DataZone menambahkan kebijakan baru yang disebut AmazonDat aZoneEnvironmentRo lePermissionsBoundaryyang membatasi IAM prinsipal yang disediakan yang dilampirkan.	12 September 2023

Perubahan	Deskripsi	Tanggal
AmazonDataZoneFullAccess - Kebijakan baru	Amazon DataZone menambahkan kebijakan baru yang disebut AmazonDataZoneFullAccessyang menyediakan akses penuh ke Amazon DataZone melalui AWS Konsol Manajemen.	12 September 2023
Pembaruan kebijakan terkelola	Pembaruan kebijakan AmazonDataZonePreviewConsoleFullAccessterkelola yang terdiri dari `iam:GetPolicy` izin tambahan.	13 Juni 2023
Amazon DataZone mulai melacak perubahan	Amazon DataZone mulai melacak perubahannya AWS kebijakan terkelola.	20 Maret 2023

IAMperan untuk Amazon DataZone

Topik

- AmazonDataZoneProvisioningRole-<domainAccountId>
- AmazonDataZoneDomainExecutionRole
- AmazonDataZoneGlueAccess- <region>-< > domainId
- AmazonDataZoneRedshiftAccess- <region>-< > domainId
- AmazonDataZone<region>S3Kelola- -< > domainId
- AmazonDataZoneSageMakerManageAccessRole- <region>-< > domainId
- AmazonDataZoneSageMakerProvisioningRole-<domainAccountId>

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

Yang AmazonDataZoneDomainExecutionRolememiliki AWS kebijakan 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 tersebut 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 AWS Glue data ke katalog. Ini juga memberikan DataZone izin Amazon untuk memberikan akses atau mencabut akses ke AWS Glue menerbitkan aset dalam 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 memanggil DataZone 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}}"
        }
      }
    }
  ]
}
```

Kredensial Sementara

Beberapa AWS layanan tidak berfungsi saat Anda masuk menggunakan kredensi sementara. Untuk informasi tambahan, termasuk yang AWS layanan bekerja dengan kredensi sementara, lihat AWS layanan yang bekerja dengan IAM dalam Panduan IAM Pengguna.

Anda menggunakan kredensi sementara jika Anda masuk ke AWS Management Console menggunakan metode apa pun kecuali nama pengguna dan kata sandi. Misalnya, ketika Anda mengakses AWS menggunakan tautan single sign-on (SSO) perusahaan Anda, proses itu secara otomatis membuat kredensi sementara. Anda juga akan secara otomatis membuat kredensial sementara ketika Anda masuk ke konsol sebagai seorang pengguna lalu beralih peran. Untuk informasi selengkapnya tentang beralih peran, lihat Beralih ke peran (konsol) di Panduan IAM Pengguna.

Anda dapat secara manual membuat kredensi sementara menggunakan AWS CLI atau AWS API. Anda kemudian dapat menggunakan kredensi 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 Kredensi keamanan sementara di. IAM

Izin prinsipal

Saat Anda menggunakan IAM pengguna atau peran untuk melakukan tindakan AWS Anda dianggap sebagai kepala sekolah. 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 AWS Dokumentasi Penting dalam Referensi Otorisasi Layanan.

Validasi kepatuhan untuk Amazon DataZone

Untuk mengetahui apakah Layanan AWS berada dalam lingkup program kepatuhan tertentu, lihat Layanan AWS dalam Lingkup oleh Program Kepatuhan dan pilih program kepatuhan yang Anda minati. Untuk informasi umum, lihat AWS Program Kepatuhan .

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 HIPAA Keamanan dan Kepatuhan di Amazon Web Services — Whitepaper ini menjelaskan bagaimana perusahaan dapat menggunakan AWS untuk membuat aplikasi HIPAA yang memenuhi syarat.

  > **Note**
  >
  > Tidak semua Layanan AWS HIPAAmemenuhi syarat. Untuk informasi selengkapnya, lihat Referensi Layanan yang HIPAA Memenuhi Syarat.

- AWS Sumber Daya Kepatuhan — 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 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 di AWS Config Panduan Pengembang — The 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 dalam AWS. Security Hub menggunakan kontrol keamanan untuk mengevaluasi AWS sumber daya dan 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 Akun AWS, beban kerja, kontainer, dan data dengan memantau lingkungan Anda untuk aktivitas yang mencurigakan dan berbahaya. GuardDuty dapat membantu Anda mengatasi berbagai persyaratan kepatuhan, seperti PCIDSS, dengan memenuhi persyaratan deteksi intrusi yang diamanatkan oleh kerangka kerja kepatuhan tertentu.
- AWS Audit Manager— Ini Layanan AWS membantu Anda terus mengaudit AWS penggunaan 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 peran

Aplikasi produsen dan klien harus memiliki kredensil yang valid untuk mengakses sumber daya Amazon DataZone. Anda tidak harus menyimpan AWS kredensil 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 IAM peran 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 IAM Pengguna:

- IAMPeran
- 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 API Panggilan

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

Bagian AWS Infrastruktur global dibangun di sekitar Wilayah AWS dan Availability Zone. 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 lebih lanjut tentang Wilayah AWS dan Availability Zone, lihat AWS Infrastruktur Global.

Selain AWS Infrastruktur global, Amazon DataZone menawarkan beberapa fitur untuk membantu mendukung ketahanan data dan kebutuhan pencadangan 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 KMS kunci, dan AmazonDataZoneDomainExecutionRole kehilangan akses ke kunci ini selama menjalankan pekerjaan, proses akan berakhir di `INACCESSIBLE` status. Setelah KMS akses dipulihkan, pekerjaan harus diperbarui secara manual untuk memicu transisi kembali ke status 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 digulirkan kembali ke versi aset tertentu dengan menerbitkan ulang versi tersebut. Ini tidak akan mempengaruhi langganan yang ada.

Ketahanan berlangganan

Di Amazon DataZone, subscriptionGrant pemenuhan akan mencoba dua pensiun 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` tanda dapat digunakan dalam `DeleteSubscriptionGrant` API operasi untuk memaksa penghapusan hibah dari Amazon DataZone tanpa mencabut izin.

Jika DataZone domain Amazon dikonfigurasi dengan KMS kunci, dan `AmazonDataZoneDomainExecutionRole` kehilangan akses ke kunci ini selama `SubscriptionGrant` alur kerja, hibah akan ditandai`INACCESSIBLE`. Setelah KMS akses dipulihkan, `INACCESSIBLE` hibah harus dihapus dan dibuat ulang.

Ketahanan lingkungan

Jika DataZone domain Amazon dikonfigurasi dengan KMS kunci, dan `AmazonDataZoneDomainExecutionRole` kehilangan akses ke kunci ini selama alur kerja lingkungan, lingkungan akan ditandai`INACCESSIBLE`. Setelah KMS akses 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.

RAMketahanan

Untuk informasi RAM ketahanan, lihat https://docs.aws.amazon.com/ram/security-disaster-recovery-resiliencyterbaru/userguide/ .html.

Ketahanan manajemen profil pengguna

Untuk informasi ketahanan profil pengguna, lihat AWS Pusat 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 AWS keamanan jaringan global. Untuk informasi tentang AWS Layanan keamanan dan bagaimana AWS melindungi infrastruktur, lihat AWS Keamanan Cloud. Untuk mendesain Anda AWS lingkungan menggunakan praktik terbaik untuk keamanan infrastruktur, lihat Perlindungan Infrastruktur di Pilar Keamanan AWS Kerangka Kerja yang Diarsiteksikan dengan Baik.

Anda menggunakan AWS APIpanggilan yang diterbitkan untuk mengakses Amazon DataZone melalui jaringan. Klien harus mendukung hal-hal berikut:

- Keamanan Lapisan Transportasi (TLS). Kami membutuhkan TLS 1.2 dan merekomendasikan TLS 1.3.
- Suite cipher dengan kerahasiaan maju yang sempurna (PFS) seperti (Ephemeral Diffie-Hellman) atau DHE (Elliptic Curve Ephemeral Diffie-Hellman). ECDHE Sebagian besar sistem modern seperti Java 7 dan versi lebih baru mendukung mode-mode ini.

Selain itu, permintaan harus ditandatangani dengan menggunakan ID kunci akses dan kunci akses rahasia yang terkait dengan IAM prinsipal. Atau Anda dapat menggunakan AWS Security Token Service (AWS STS) untuk menghasilkan kredensil 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. Masuk 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 menyediakan alat yang membantu Anda melindungi data Anda untuk semua layanan dengan prinsipal 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 lebih lanjut, lihat AWS model tanggung jawab 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 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 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 AWS IAM konsol 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, silakan lihat AmazonDataZoneGlue Access- <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, buka AWS IAM konsol di akun tempat aset data Anda ada dan pastikan bahwa peran tersebut telah AmazonDataZoneGlueManageAccessRolePo licymelampirkannya. Untuk informasi selengkap

Pesan galat di Portal Data	Resolusi
	nya, 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 KMS dan/atau pengaturan S3 mungkin diperlukan. Untuk informasi selengkap nya, lihat Mendaftarkan lokasi Amazon S3 terenkripsi. • Lokasi Amazon S3 terdaftar dalam mode AWS Lake Formation tetapi IAMAllowe dPrincipalditambahkan ke izin tabel. Untuk memperbaiki masalah, Anda dapat menghapus izin IAMAllowedPrincipaldari 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

Memecahkan masalah penautan aset DataZone garis keturunan Amazon dengan kumpulan data hulu

Bagian ini berisi petunjuk pemecahan masalah untuk masalah yang mungkin Anda temui dengan garis keturunan Amazon DataZone . Untuk beberapa peristiwa open lineage run terkait Amazon RedShift, Anda mungkin melihat bahwa garis keturunan aset tidak ditautkan ke kumpulan data hulu. AWS Glue Topik ini menjelaskan skenario dan beberapa pendekatan untuk mengurangi masalah. Untuk informasi lebih lanjut tentang garis keturunan, lihat. Garis keturunan data di Amazon DataZone (Pratinjau)

SourceIdentifier pada simpul garis keturunan

`sourceIdentifier`Atribut dalam simpul garis keturunan mewakili peristiwa yang terjadi pada kumpulan data. Untuk informasi selengkapnya, lihat Atribut kunci di simpul garis keturunan.

Simpul garis keturunan mewakili semua peristiwa yang terjadi pada kumpulan data atau pekerjaan yang sesuai. Simpul garis keturunan berisi atribut "sourceIdentifier" yang berisi pengenal dataset/pekerjaan yang sesuai. Saat kami mendukung peristiwa garis keturunan terbuka, `sourceIdentifier` nilainya secara default diisi sebagai kombinasi “namespace” dan “name” untuk kumpulan data, pekerjaan, dan pekerjaan yang berjalan.

Untuk AWS sumber daya seperti AWS Glue dan Amazon Redshift, tabel `sourceIdentifier` ARN dan AWS Glue tabel Redshift ARNs tempat Amazon DataZone akan membuat run-event dan detail lainnya sebagai berikut:

> **Note**
>
> Di AWS, ARN berisi informasi sepertiaccountId, wilayah, database, dan tabel untuk setiap sumber daya.

- OpenLineage event untuk dataset ini berisi database dan nama tabel.
- Wilayah ditangkap dalam aspek “properti lingkungan” dari lari. Jika tidak ada, sistem menggunakan wilayah dari kredenal pemanggil.
- AccountId diambil dari kredensi penelepon.

SourceIdentifier pada aset di dalam DataZone

`AssetCommonDetailForm`memiliki atribut yang disebut "sourceIdentifier" yang mewakili pengidentifikasi dataset yang diwakili oleh aset. Agar node garis keturunan aset ditautkan dengan dataset hulu, atribut harus diisi dengan nilai yang cocok dengan node dataset. `sourceIdentifier` Jika aset diimpor oleh sumber data, alur kerja terisi `sourceIdentifier` sebagai tabel AWS Glue / tabel ARN Redshift ARN secara otomatis sementara aset lain (termasuk aset kustom) yang dibuat melalui `CreateAsset` API seharusnya memiliki nilai tersebut diisi oleh pemanggil.

Bagaimana Amazon DataZone membangun sourceIdentifier dari OpenLineage Acara?

Aset For AWS Glue dan Redshift, dibuat dari `sourceIdentifier` Glue dan Redshift. ARNs Inilah cara Amazon DataZone membangunnya:

AWS Glue ARN

Tujuannya adalah untuk membangun sebuah OpenLineage Event di mana node garis keturunan keluaran adalah: `sourceIdentifier`

```
arn:aws:glue:us-east-1:123456789012:table/testlfdb/testlftb-1
```

Untuk menentukan apakah suatu run menggunakan data dari AWS Glue, cari keberadaan kata kunci tertentu di `environment-properties` faset tersebut. Secara khusus, jika salah satu bidang yang ditunjuk ini ada, sistem mengasumsikan `RunEvent` asalnya. AWS Glue

- GLUE_VERSION
- GLUE_COMMAND_CRITERIA
- GLUE_PYTHON_VERSION

```
"run": {
   "runId":"4e3da9e8-6228-4679-b0a2-fa916119fthr",
   "facets":{
      "environment-properties":{
         "_producer":"https://github.com/OpenLineage/OpenLineage/tree/1.9.1/
integration/spark",
         "_schemaURL":"https://openlineage.io/spec/2-0-2/OpenLineage.json#/$defs/
RunFacet",
         "environment-properties":{
            "GLUE_VERSION":"3.0",
            "GLUE_COMMAND_CRITERIA":"glueetl",
            "GLUE_PYTHON_VERSION":"3"
         }
      }
   }
```

Untuk AWS Glue menjalankan, Anda dapat menggunakan nama dari `symlinks` segi untuk mendapatkan database dan nama tabel, yang dapat digunakan untuk membangun. ARN

Perlu memastikan namanya adalah`databaseName.tableName`:

```
"symlinks": {
   "_producer":"https://github.com/OpenLineage/OpenLineage/tree/1.9.1/integration/
spark",
   "_schemaURL":"https://openlineage.io/spec/facets/1-0-0/SymlinksDatasetFacet.json#/
$defs/SymlinksDatasetFacet",
   "identifiers":[
      {
         "namespace":"s3://object-path",
         "name":"testlfdb.testlftb-1",
         "type":"TABLE"
      }
   ]
}
```

Contoh COMPLETE Acara:

```
{
   "eventTime":"2024-07-01T12:00:00.000000Z",
   "producer":"https://github.com/OpenLineage/OpenLineage/tree/1.9.1/integration/glue",
   "schemaURL":"https://openlineage.io/spec/2-0-2/OpenLineage.json#/$defs/RunEvent",
   "eventType":"COMPLETE",
   "run": {
      "runId":"4e3da9e8-6228-4679-b0a2-fa916119fthr",
      "facets":{
         "environment-properties":{
            "_producer":"https://github.com/OpenLineage/OpenLineage/tree/1.9.1/
integration/spark",
            "_schemaURL":"https://openlineage.io/spec/2-0-2/OpenLineage.json#/$defs/
RunFacet",
            "environment-properties":{
               "GLUE_VERSION":"3.0",
               "GLUE_COMMAND_CRITERIA":"glueetl",
               "GLUE_PYTHON_VERSION":"3"
            }
         }
      }
   },
   "job":{
      "namespace":"namespace",
      "name":"job_name",
      "facets":{
```

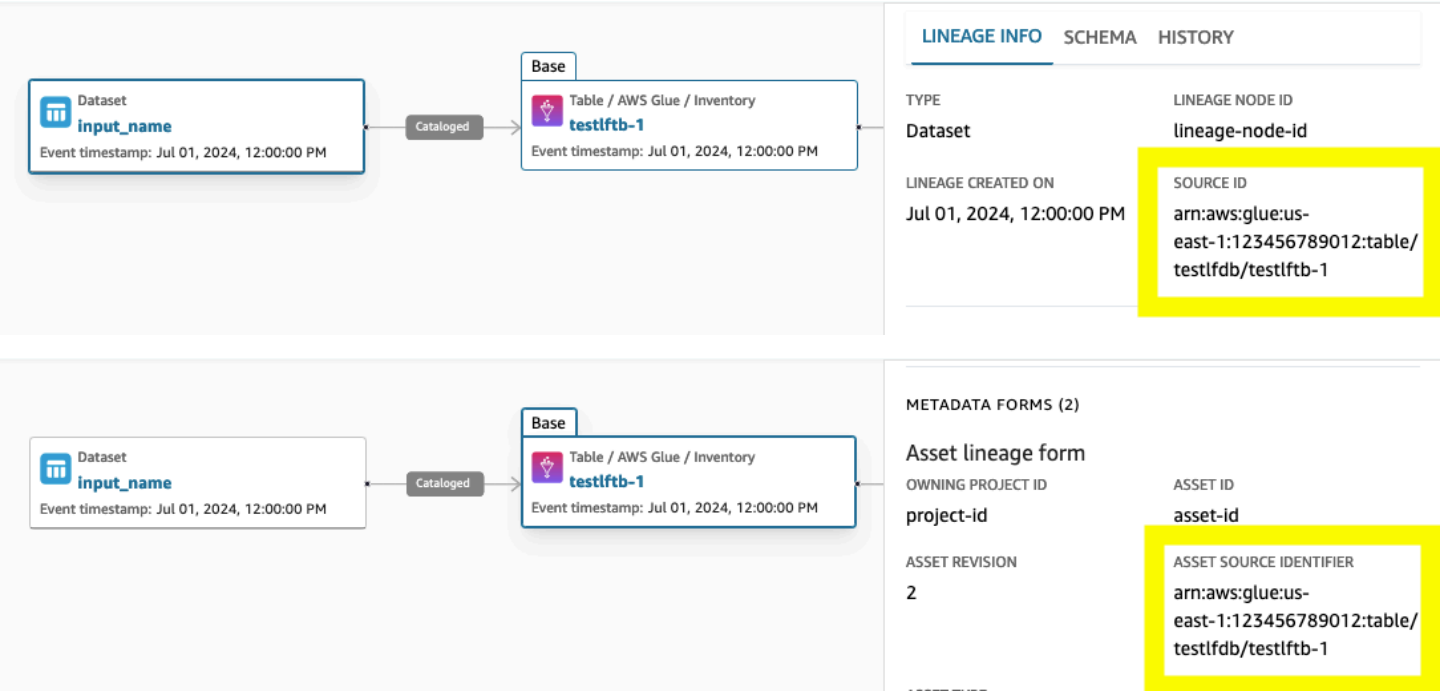
```
         "jobType":{
            "_producer":"https://github.com/OpenLineage/OpenLineage/tree/1.9.1/
integration/glue",
            "_schemaURL":"https://openlineage.io/spec/facets/2-0-2/
JobTypeJobFacet.json#/$defs/JobTypeJobFacet",
            "processingType":"BATCH",
            "integration":"glue",
            "jobType":"JOB"
         }
      }
   },
   "inputs":[
      {
         "namespace":"namespace",
         "name":"input_name"
      }
   ],
   "outputs":[
      {
         "namespace":"namespace.output",
         "name":"output_name",
         "facets":{
            "symlinks":{
               "_producer":"https://github.com/OpenLineage/OpenLineage/tree/1.9.1/
integration/spark",
               "_schemaURL":"https://openlineage.io/spec/facets/1-0-0/
SymlinksDatasetFacet.json#/$defs/SymlinksDatasetFacet",
               "identifiers":[
                  {
                     "namespace":"s3://object-path",
                     "name":"testlfdb.testlftb-1",
                     "type":"TABLE"
                  }
               ]
            }
         }
      }
   ]
}
```

Berdasarkan `OpenLineage` acara yang `sourceIdentifier` dikirimkan, node garis keturunan keluaran adalah:

```
arn:aws:glue:us-east-1:123456789012:table/testlfdb/testlftb-1
```

Node garis keturunan keluaran akan terhubung ke simpul garis keturunan aset di mana aset tersebut berada: `sourceIdentifier`

```
arn:aws:glue:us-east-1:123456789012:table/testlfdb/testlftb-1
```



Pergeseran Merah Amazon ARN

Tujuannya adalah untuk membangun sebuah OpenLineage Event di mana node garis keturunan keluaran adalah: `sourceIdentifier`

```
arn:aws:redshift:us-east-1:123456789012:table/workgroup-20240715/tpcds_data/public/
dws_tpcds_7
```

Sistem menentukan apakah input atau output disimpan dalam Redshift berdasarkan namespace. Secara khusus, jika namespace dimulai dengan redshift://atau berisi string `redshift-serverless.amazonaws.com` atau, `redshift.amazonaws.com` itu adalah sumber daya Redshift.

```
"outputs": [
    {
```

```
        "namespace":"redshift://workgroup-20240715.123456789012.us-
east-1.redshift.amazonaws.com:5439",
        "name":"tpcds_data.public.dws_tpcds_7"
    }
]
```

Perhatikan bahwa namespace harus dalam format berikut:

```
provider://{cluster_identifier}.{region_name}:{port}
```

Untuk `redshift-serverless`:

```
"outputs": [
    {
        "namespace":"redshift://workgroup-20240715.123456789012.us-east-1.redshift-
serverless.amazonaws.com:5439",
        "name":"tpcds_data.public.dws_tpcds_7"
    }
]
```

Hasil dalam hal berikut `sourceIdentifier`

```
arn:aws:redshift-serverless:us-east-1:123456789012:table/workgroup-20240715/tpcds_data/
public/dws_tpcds_7
```

Berdasarkan OpenLineage peristiwa yang dikirimkan, `sourceIdentifier` simpul garis keturunan yang akan dipetakan ke hilir (yaitu, output dari acara) adalah:

```
arn:aws:redshift-serverless:us-e:us-east-1:123456789012:table/workgroup-20240715/
tpcds_data/public/dws_tpcds_7
```

Ini adalah pemetaan yang membantu Anda memvisualisasikan garis keturunan aset dalam katalog.

Pendekatan alternatif

Ketika tidak ada kondisi di atas yang terpenuhi, sistem menggunakan namespace/name untuk membangun: `sourceIdentifier`

```
"inputs": [
```

```
  {
     "namespace":"arn:aws:redshift:us-east-1:123456789012:table",
     "name":"workgroup-20240715/tpcds_data/public/dws_tpcds_7"
  }
],
"outputs": [
  {
     "namespace":"arn:aws:glue:us-east-1:123456789012:table",
     "name":"testlfdb/testlftb-1"
  }
]
```

Memecahkan masalah kekurangan hulu untuk node garis keturunan aset

Jika Anda tidak melihat hulu node garis keturunan aset, Anda dapat melakukan hal berikut untuk memecahkan masalah mengapa node tersebut tidak ditautkan dengan kumpulan data:

1. Memohon `GetAsset` sambil memberikan `domainId` dan`assetId`:

   ```
   aws datazone get-asset --domain-identifier <domain-id> --identifier <asset-id>
   ```

   Responsnya muncul sebagai berikut:

   ```
   {
       .....
       "formsOutput": [
           .....
           {
               "content": "{\"sourceIdentifier\":\"arn:aws:glue:eu-
   west-1:123456789012:table/testlfdb/testlftb-1\"}",
               "formName": "AssetCommonDetailsForm",
               "typeName": "amazon.datazone.AssetCommonDetailsFormType",
               "typeRevision": "6"
           },
           .....
       ],
       "id": "<asset-id>",
       ....
   }
   ```

2. Memanggil `GetLineageNode` untuk mendapatkan node `sourceIdentifier` garis keturunan dataset. Karena tidak ada cara untuk mendapatkan simpul garis keturunan untuk node kumpulan

data yang sesuai secara langsung, Anda dapat memulai dengan menjalankan `GetLineageNode` pekerjaan:

```
aws datazone get-lineage-node --domain-identifier <domain-id> --identifier
 <job_namespace>.<job_name>/<run_id>

if you are using the getting started scripts, job name and run ID are printed in the
 console
and namespace is "default". Otherwise you can get these values from run event
 content.
```

Respons sampel terlihat seperti berikut:

```
{
    .....
    "downstreamNodes": [
        {
            "eventTimestamp": "2024-07-24T18:08:55+08:00",
            "id": "afymge5k4v0euf"
        }
    ],
    "formsOutput": [
        <some forms corresponding to run and job>
    ],
    "id": "<system generated node-id for run>",
    "sourceIdentifier": "default.redshift.create/2f41298b-1ee7-3302-
a14b-09addffa7580",
    "typeName": "amazon.datazone.JobRunLineageNodeType",
    ....
    "upstreamNodes": [
        {
            "eventTimestamp": "2024-07-24T18:08:55+08:00",
            "id": "6wf2z27c8hghev"
        },
        {
            "eventTimestamp": "2024-07-24T18:08:55+08:00",
            "id": "4tjbcsnre6banb"
        }
    ]
}
```

3. Panggil `GetLineageNode` lagi dengan meneruskan pengidentifikasi node hilir/hulu (yang menurut Anda harus ditautkan ke node aset) karena ini sesuai dengan kumpulan data:

   Contoh perintah menggunakan contoh respon di atas:

   ```
   aws datazone get-lineage-node --domain-identifier <domain-id> --identifier
    afymge5k4v0euf
   ```

   Ini mengembalikan detail simpul garis keturunan yang sesuai dengan kumpulan data: afymge5k4v0euf

   ```
   {
       .....
       "domainId": "dzd_cklzc5s2jcr7on",
       "downstreamNodes": [],
       "eventTimestamp": "2024-07-24T18:08:55+08:00",
       "formsOutput": [
           .....
       ],
       "id": "afymge5k4v0euf",
       "sourceIdentifier": "arn:aws:redshift:us-east-1:123456789012:table/
   workgroup-20240715/tpcds_data/public/dws_tpcds_7",
       "typeName": "amazon.datazone.DatasetLineageNodeType",
       "typeRevision": "1",
       ....
       "upstreamNodes": [
           ...
       ]
   }
   ```

4. Bandingkan `sourceIdentifier` node dataset ini dan respons dari`GetAsset`. Jika tidak ditautkan, ini tidak akan cocok, dan karenanya tidak akan terlihat di UI garis keturunan.

Skenario dan mitigasi yang tidak cocok

Berikut ini adalah skenario yang umum diketahui di mana ini tidak akan cocok dan kemungkinan mitigasi:

Akar penyebab: Tabel hadir di akun yang berbeda dari akun DataZone domain Amazon.

Mitigasi: Anda dapat menjalankan `PostLineageEvent` operasi dari akun terkait. Karena `accountId` untuk membangun ARN diambil dari kredenal pemanggil, Anda dapat mengambil peran dari akun yang berisi tabel saat menjalankan skrip atau pemanggilan memulai. `PostLineageEvent` Melakukannya akan membantu dalam membangun ARNs dengan benar dan menghubungkan dengan node aset.

Akar penyebab: Tabel/tampilan ARN for Redshift berisi RedShift/RedShift-Serverless berdasarkan namespace dan atribut nama dari informasi kumpulan data yang sesuai dalam acara run. OpenLineage

Mitigasi: Karena tidak ada cara deterministik untuk mengetahui apakah nama yang diberikan milik cluster atau workgroup, kami menggunakan heuristik berikut:

- Jika “nama” yang sesuai dengan kumpulan data berisi "`redshift-serverless.amazonaws.com`“, kami menggunakan redshift-serverless sebagai bagian dariARN, jika tidak default ke “pergeseran merah”.
- Di atas berarti alias pada nama workgroup tidak akan berfungsi.

Akar penyebab: Kumpulan data hulu tidak ditautkan dengan benar untuk aset khusus.

Mitigasi<name>: Pastikan untuk mengisi aset dengan memanggil`CreateAsset`/`CreateAssetRevision`yang cocok dengan node dataset (`sourceIdentifier`yang akan menjadi<namespace>/untuk node khusus). `sourceIdentifier`

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
Jumlah filter aset per aset	Jumlah maksimum filter aset per DataZone aset Amazon	100
Jumlah filter per langganan	Jumlah maksimum filter per DataZone langganan Amazon	5
Unit domain dalam domain	Jumlah maksimum unit domain dalam DataZone domain Amazon	100

Sumber Daya	Deskripsi	Nilai
Tingkat hierarki dalam unit domain	Jumlah maksimum tingkat hierarki untuk unit domain	5
Hibah per polis per unit domain	Jumlah maksimum hibah per polis per unit domain	20
Produk data	Jumlah maksimum produk data yang dapat dibuat dalam DataZone domain	500.000

Riwayat dokumen untuk Panduan DataZone Pengguna Amazon

Tabel berikut menjelaskan rilis dokumentasi untuk Amazon DataZone.

Perubahan	Deskripsi	Tanggal
Unit domain	Amazon DataZone memperkenalkan serangkaian kemampuan tata kelola data baru yang disebut unit domain dan kebijakan otorisasi yang memungkinkan pelanggan membuat organisasi unit bisnis/tingkat tim dan mengelola kebijakan sesuai kebutuhan bisnis mereka. Dengan penambahan unit domain, pengguna dapat mengatur, membuat, mencari, dan menemukan aset data dan proyek yang terkait dengan unit bisnis atau tim. Dengan kebijakan otorisasi, pengguna unit domain tersebut dapat menetapkan kebijakan akses untuk membuat proyek, glosarium, dan menggunakan sumber daya komputasi di Amazon. DataZone	Agustus 5, 2024
Produk data	Amazon DataZone memperkenalkan produk data, yang memungkinkan pengelompokan aset data	Agustus 5, 2024

	ke dalam paket mandiri yang terdefinisi dengan baik yang disesuaikan untuk kasus penggunaan bisnis tertentu. Misalnya, produk data analisis pemasaran dapat menggabungkan berbagai aset data, seperti data kampanye pemasaran, data pipa, dan data pelanggan. Dengan produk data, pelanggan dapat menyederhanakan proses penemuan dan berlangganan, menyelaraskannya dengan tujuan bisnis dan mengurangi redundansi dalam menangani aset individu.	
AmazonDataZoneDomainExecutionRolePolicy dan AmazonDataZoneFullUserAccess - pembaruan kebijakan	Pembaruan kebijakan untuk AmazonDataZoneDomainExecutionRolePolicydan AmazonDataZoneFullUserAccessuntuk mengaktifkan dukungan untuk yang baru APIs yang digunakan untuk membuat dan mengelola unit DataZone domain Amazon dan produk data. Untuk informasi selengkapnya, lihat DataZone pembaruan Amazon ke AWS kebijakan terkelola.	Agustus 5, 2024

Kontrol akses berbutir halus	Amazon DataZone telah memperkenalkan kontrol akses berbutir halus, memberi Anda kontrol terperinci atas aset data Anda di katalog data bisnis Amazon DataZone di seluruh danau data dan gudang data. Dengan kemampuan baru, pemilik data sekarang dapat membatasi akses ke catatan data tertentu pada tingkat baris dan kolom, alih-alih memberikan akses ke seluruh aset data. Misalnya, jika data Anda berisi kolom dengan informasi sensitif seperti Informasi Identifik asi Pribadi (PII), Anda dapat membatasi akses hanya ke kolom yang diperlukan, memastikan bahwa informasi sensitif dilindungi sambil tetap mengizinkan akses ke data yang tidak sensitif. Demikian pula, Anda dapat mengontro l akses di tingkat baris, memungkinkan pengguna untuk hanya melihat catatan yang relevan dengan peran atau tugas mereka.	Juli 2, 2024

AmazonDataZoneGlueManageAccessRolePolicy - pembaruan kebijakan	Pembaruan kebijakan ke AmazonDataZoneGlueManageAccessRolePolicy- Amazon DataZone menambahkan IAM izin yang digunakan untuk fungsionalitas kontrol akses berbutir halus untuk mengurangi pemberian izin di Lake Formation. Untuk informasi selengkapnya, lihat DataZone pembaruan Amazon ke AWS kebijakan terkelola.	Juli 2, 2024

Silsilah data	Amazon DataZone meluncurkan garis keturunan data dalam pratinjau, membantu pelanggan memvisualisasikan peristiwa garis keturunan dari sistem yang OpenLineage diaktifkan atau melalui API dan melacak pergerakan data dari sumber ke konsumsi. Menggunakan DataZone Amazon OpenLineage - compatibleAPIs, administrator domain dan produsen data dapat menangkap dan menyimpan peristiwa silsilah di luar apa yang tersedia di Amazon, termasuk transformasi di Amazon DataZone S3, AWS Glue, dan layanan lainnya. Selain itu, DataZone Amazon membuat garis keturunan dengan setiap peristiwa, memungkinkan pengguna untuk memvisualisasikan garis keturunan kapan saja atau membandingkan transformasi di seluruh aset atau riwayat pekerjaan. Garis keturunan historis ini memberikan pemahaman yang lebih dalam tentang bagaimana data telah berevolusi, penting untuk pemecahan masalah, audit, dan memvalidasi integritas aset data.	27 Juni 2024

AmazonDataZoneExecutionRolePolicy dan AmazonDataZoneFullUserAccess - pembaruan kebijakan	Pembaruan kebijakan ke AmazonDataZoneExecutionRolePolicydan AmazonDataZoneFullUserAccessuntuk mengaktifkan dukungan untuk garis keturunan data dan kontrol akses berbutir halus. APIs Untuk informasi selengkapnya, lihat DataZone pembaruan Amazon ke AWS kebijakan terkelola.	27 Juni 2024

Kustom AWS cetak biru layanan	Dengan kustom AWS cetak biru layanan, jika Anda sudah ada AWS sumber daya termasuk IAM peran, data lake, jerat data, bucket Amazon S3, dan kluster Amazon Redshift, Anda sekarang dapat menentukan izin ke sumber daya yang ada ini menggunakan IAM peran kustom Anda sendiri, sehingga pengguna DataZone Amazon Anda dapat memanfaatkan publikasi dan langganan untuk berbagi dan mengatur sumber daya ini. Dengan kustom AWS cetak biru layanan, administrator Amazon DataZone dapat mengonfig urasi AWS lingkungan layanan menggunakan peran kustom mereka sendiri. Mereka dapat mengonfigurasi tautan tindakan untuk ini AWS lingkungan layanan dan dengan demikian menyediak an akses federasi ke salah satu yang ada AWS sumber daya. Mereka juga dapat mengonfigurasi target langganan dan sumber data dalam kustom ini AWS lingkungan layanan. Administr ator dapat mengatur AWS lingkungan layanan di akun DataZone domain Amazon	Juni 17, 2024

	mereka sendiri atau di akun terkait tempat mereka ingin mempublikasikan, berlangga nan, menemukan, atau mengatur data.	
AmazonDataZoneGlue ManageAccessRolePolicy - pembaruan kebijakan	Pembaruan kebijakan untuk AmazonDataZoneGlue ManageAccessRolePolicy yang menambahkan IAM izin yang diperlukan untuk fungsionalitas berlangga nan mandiri DataZone di Amazon untuk mengurang i izin yang diberikan dalam pembentukan danau. Dengan fungsi berlangganan mandiri, izin pembentukan danau hanya dapat diberikan kepada sumber daya yang ditandai. Untuk informasi selengkapnya, lihat DataZone pembaruan Amazon ke AWS kebijakan terkelola.	Juni 14, 2024

AmazonDataZoneFullAccess - pembaruan kebijakan	Pembaruan kebijakan untuk AmazonDataZoneFullAccess yang memungkinkan konsol DataZone manajemen Amazon membuat rahasia atas nama pengguna dengan tag domain dan proyek. Juga termasuk `ram:ListResourceSharePermissions` tindakan untuk mengaktifkan administrasi dari akun pemilik domain untuk melihat status asosiasi akun dari akun terkait. Untuk informasi selengkapnya, lihat DataZone pembaruan Amazon ke AWS kebijakan terkelola.	Juni 14, 2024
AmazonDataZoneDomainExecutionRolePolicy - pembaruan kebijakan	Pembaruan kebijakan untuk AmazonDataZoneDomainExecutionRolePolicy yang menambahkan baru APIs ke Amazon DataZone yang memungkinkan pengguna mengonfigurasi tindakan untuk DataZone lingkungan Amazon mereka. Untuk informasi selengkapnya, lihat DataZone pembaruan Amazon ke AWS kebijakan terkelola.	Juni 14, 2024

Peningkatan pembuatan sumber data	Amazon DataZone telah menambahkan penyempurnaan pada alur pembuatan sumber data untuk menyederhanakan manajemen akses bagi produsen data. Dengan pembaruan ini, ketika produsen data membuat sumber data untuk mempublikasikannya AWS Glue dan aset Amazon Redshift, Amazon memberikan izin DataZone hanya-baca kepada anggota proyek. Saat membuat AWS Glue sumber data, Amazon DataZone secara otomatis memberikan izin 'hanya-baca' untuk IAM peran lingkungan yang digunakan untuk membuat sumber data, memungkinkan akses ke semua tabel di terkait AWS Basis data Glue. Demikian pula, untuk sumber data Amazon Redshift, Amazon DataZone memberikan akses 'hanya-baca' ke semua tabel dalam skema Amazon Redshift yang digunakan dalam sumber data.	Juni 10, 2024

Integrasi dengan Amazon SageMaker	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.	6 Mei 2024
AmazonDataZoneSageMakerProvisioning - kebijakan baru	Kebijakan baru yang disebut AmazonDataZoneSageMakerProvisioningmemberikan Amazon izin DataZone yang diperlukan untuk berinteraksi dengan Amazon. SageMaker Untuk informasi selengkapnya, lihat DataZone pembaruan Amazon ke AWS kebijakan 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 IAM peran 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 DataZone pembaruan Amazon ke AWS kebijakan terkelola.	April 30, 2024
AmazonDataZoneSageMakerAccess - kebijakan baru	Kebijakan baru yang disebut AmazonDataZoneSageMakerAccess memberi Amazon izin DataZone yang diperlukan untuk memberikan akses pengguna ke berbagai sumber daya di lingkungan Amazon SageMaker . Untuk informasi selengkapnya, lihat DataZone pembaruan Amazon ke AWS kebijakan 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 DataZone pembaruan Amazon ke AWS kebijakan terkelola.	April 30, 2024

Mode akses hibrida Lake Formation	Amazon DataZone telah memperkenalkan integrasi dengan AWS Mode akses hibrida Lake Formation. Integrasi ini memungkinkan Anda untuk dengan mudah mempublikasikan dan berbagi AWS Glue tabel melalui Amazon DataZone, tanpa perlu mendaftarkannya AWS Lake Formation terlebih dahulu. Untuk memulai, administrator mengaktifkan pengaturan pendaftaran lokasi data di bawah `DefaultDataLake` cetak biru di konsol Amazon. DataZone Kemudian, ketika konsumen data berlangganan AWS Glue table dikelola melalui IAM izin, Amazon DataZone pertama-tama mendaftarkan lokasi Amazon S3 dari tabel ini dalam mode hybrid, dan kemudian memberikan akses ke konsumen data dengan mengelola izin pada tabel melalui AWS Formasi Danau. Ini memastikan bahwa IAM izin pada tabel terus ada dengan yang baru diberikan AWS Izin Lake Formation, tanpa mengganggu alur kerja yang ada. Untuk informasi selengkapnya, lihat DataZone Integrasi Amazon dengan	April 3, 2024

	mode hybrid AWS Lake Formation.	
Kualitas data	Amazon DataZone meluncurkan integrasi dengan AWS Glue Data Quality dan menawarkan APIs untuk mengintegrasikan metrik kualitas data dari solusi kualitas data pihak ketiga. Integrasi baru memungkinkan Anda untuk mempublikasikan secara otomatis AWS Glue Data Quality skor ke dalam katalog data DataZone bisnis Amazon. Amazon DataZone APIs dapat digunakan untuk menelan 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.	April 3, 2024

AmazonDataZoneS3Manage--< domainId > - peran baru <region>	Peran baru yang disebut AmazonDataZoneS3Manage--< domainId > <region>yang digunakan saat Amazon memanggil DataZone 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 DataZone pembaruan Amazon ke AWS kebijakan terkelola.	April 1, 2024
AmazonDataZoneGlue ManageAccessRolePolicy - Pembaruan kebijakan	Memperbarui AmazonDataZoneGlueManageAccessRolePolicyuntuk mengaktifkan dukungan untuk izin yang memungkinkan Amazon DataZone mengaktifkan penerbitan dan akses hibah ke data. Untuk informasi selengkapnya, lihat DataZone pembaruan Amazon ke AWS kebijakan terkelola.	April 1, 2024

AmazonDataZoneDomainExecutionRolePolicy dan AmazonDataZoneFullUserAccess - Pembaruan kebijakan	Memperbarui AmazonDataZoneDomainExecutionRolePolicydan AmazonDataZoneFullUserAccessuntuk mengaktifkan dukungan untuk `CancelMetadataGenerationRun` API. Untuk informasi selengkapnya, lihat DataZone pembaruan Amazon ke AWS kebijakan terkelola.	Maret 29, 2024
AmazonDataZoneFullAccess - Pembaruan kebijakan	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 produsen data APIs yang dapat digunakan untuk menghasilkan deskripsi aset secara terprogram.	Maret 27, 2024

AmazonDataZoneFullAccess - Pembaruan kebijakan	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 di dalamnya AWS akun dan cluster Amazon Redshift, dan untuk tujuan apa.	Maret 21, 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 DataZone pembaruan Amazon ke AWS kebijakan 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 DataZone pembaruan Amazon ke AWS kebijakan terkelola.	Februari 1, 2024

Penyempurnaan penggunaan Cloud Formation	Pengguna Amazon sekarang DataZone dapat memanfaat kan AWS CloudForm ation untuk secara efektif memodelkan dan mengelola serangkaian DataZone sumber daya Amazon. Pendekatan ini memfasilitasi penyediaan sumber daya yang konsisten , sementara juga memungkin kan 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.	Januari 18, 2024

Aset kustom	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 yang tersedia sebelumny a. API Kemampuan untuk membuat, memperbarui, dan mempublikasikan aset khusus di Amazon DataZone, memungkinkan Anda berbagi, menemukan, berlangga nan semua jenis aset, dan membangun alur kerja bisnis yang menyediakan tata kelola aset tersebut. Untuk informasi selengkapnya, lihat Membuat jenis aset kustom.	Januari 5, 2024

Tambahkan IAM kepala sekolah sebagai anggota proyek	Anda sekarang dapat menambahkan IAM prinsipal sebagai anggota proyek, bahkan jika IAM prinsipal 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 IAM prinsipal sebagai anggota hanya dengan memberikan Amazon Resouce Name (ARN) peran atau pengguna. IAM IAM IAMKepala sekolah masih harus memiliki IAM izin yang diperlukan untuk mengakses Amazon DataZone dan yang dapat dikonfigurasi di IAM konsol. Untuk informasi selengkapnya, lihat Menambahkan anggota ke proyek.	Januari 5, 2024

Hapus domain	Hapus domain adalah fitur yang memungkinkan Anda untuk lebih mudah menghapus domain Anda. Sekarang, Anda dapat melanjutk an dengan penghapusan domain meskipun tidak kosong (seperti dalam berisi proyek, lingkungan, aset, sumber data, dll.). Untuk informasi selengkapnya, lihat Menghapus DataZone domain Amazon.	27 Desember 2023

Mode hibrida Lake Formation	Amazon DataZone telah menambahkan dukungan untuk AWS Mode hibrida Lake Formation. Dengan dukungan ini, jika Anda mempublik asikan AWS Glue tabel ke Amazon DataZone dengan miliknya AWS Lokasi S3 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 memperlak ukan tabel ini sebagai aset yang tidak dikelola yaitu, Amazon tidak DataZone akan dapat memberikan langganan ke tabel ini. Untuk informasi selengkapnya, lihat Mengonfig urasi izin Lake Formation untuk Amazon DataZone.	22 Desember 2023
HIPAAkepatuhan	Amazon DataZone sekarang mematuhi Undang-Undang Portabilitas dan Akuntabilitas Asuransi Kesehatan AS tahun 1996 ()HIPAA. Untuk melihat daftar AWS layanan dengan HIPAA kepatuhan lihat https:// aws.amazon.com/compliance/ hipaa-eligible-services-re ference/.	14 Desember 2023

AmazonDataZoneGlueManageAccessRolePolicy - Pembaruan kebijakan	Memperbarui AmazonDataZoneGlueManageAccessRolePolicyuntuk mengaktifkan dukungan untuk AWS Mode hibrida Lake Formation. Untuk informasi selengkapnya, lihat DataZone pembaruan Amazon ke AWS kebijakan 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 DataZone pembaruan Amazon ke AWS kebijakan terkelola.	28 November 2023

Rekomendasi AI	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 rekomenda si AI untuk deskripsi di Amazon DataZone, konsumen data dapat mengident ifikasi tabel dan kolom data yang diperlukan untuk analisis, yang meningkat kan kemampuan ditemukan data dan mengurangi back-and-forth komunikasi dengan produsen data. Pratinjau tersedia di DataZone domain Amazon yang disediaka n sebagai berikut AWS Wilayah: AS Timur (Virginia N.), AS Barat (Oregon). Untuk informasi selengkapnya, lihat Menggunakan pembelajaran mesin dan AI generatif.	28 November 2023

DefaultDataLake cetak biru	Amazon DataZone telah menambahkan peningkatan pada DefaultDataLake cetak biru yang memberi Anda kontrol yang lebih baik atas siapa yang dapat mempublikasikan data apa dari Anda AWS akun. Ada dua perubahan utama yang diperkenalkan dengan peluncuran fitur ini.	20 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 DataZone pembaruan Amazon ke AWS kebijakan terkelola.	17 November 2023

AmazonDataZoneRedshiftManageAccessRolePolicy - Pembaruan kebijakan	Amazon DataZone memperbarui AmazonDataZoneRedshiftManageAccessRolePolicykebijakan dengan menghapus cek pada ID organisasi untuk `redshift:AssociateDataShareConsumer` tindakan tersebut. Hal ini memungkinkan Anda untuk berbagi sumber daya di AWS organisasi. Untuk informasi selengkapnya, lihat DataZone pembaruan Amazon ke AWS kebijakan terkelola.	16 November 2023
Rilis GA dari Panduan Pengguna	Rilis General Availability (GA) dari Panduan DataZone Pengguna Amazon.	Oktober 15, 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 pembaruan Amazon DataZone AWS kebijakan terkelola.	2 Oktober 2023

AmazonDataZonePreviewConsoleFullAccess - kebijakan usang	Amazon tidak DataZone digunakan lagi. AmazonDataZonePreviewConsoleFullAccessUntuk informasi selengkapnya, lihat pembaruan Amazon ke DataZone AWS kebijakan terkelola.	September 29, 2023
AmazonDataZonePortalFullAccessPolicy - kebijakan usang	Amazon tidak DataZone digunakan lagi. AmazonDataZonePortalFullAccessPolicy Untuk informasi selengkapnya, lihat pembaruan Amazon ke DataZone AWS kebijakan terkelola.	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 DataZone pembaruan Amazon ke AWS kebijakan 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 DataZone pembaruan Amazon ke AWS kebijakan 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 DataZone pembaruan Amazon ke AWS kebijakan 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 DataZone pembaruan Amazon ke AWS kebijakan terkelola.	12 September 2023
AmazonDataZoneGlueManageAccessRolePolicy - Kebijakan baru	Amazon DataZone menambahkan kebijakan baru yang disebut AmazonDataZoneGlueManageAccessRolePolicymemberikan DataZone izin Amazon untuk mempublikasikan AWS Glue data ke katalog. Ini juga memberikan DataZone izin Amazon untuk memberikan akses atau mencabut akses ke AWS Glue menerbitkan aset dalam katalog. Untuk informasi selengkapnya, lihat DataZone pembaruan Amazon ke AWS kebijakan 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 DataZone pembaruan Amazon ke AWS kebijakan terkelola.	12 September 2023
AmazonDataZoneFullAccess - Kebijakan baru	Amazon DataZone menambahkan kebijakan baru yang disebut AmazonDat aZoneFullAccessyang menyediakan akses penuh ke Amazon DataZone melalui AWS Konsol Manajemen. Untuk informasi selengkapnya, lihat DataZone pembaruan Amazon ke AWS kebijakan terkelola.	12 September 2023
AmazonDataZoneEnvi ronmentRolePermiss ionsBoundary - Kebijakan baru	Amazon DataZone menambahkan kebijakan baru yang disebut AmazonDat aZoneEnvironmentRo lePermissionsBoundaryyang membatasi IAM prinsipal yang disediakan yang dilampirkan. Untuk informasi selengkapnya, lihat DataZone pembaruan Amazon ke AWS kebijakan terkelola.	12 September 2023

Pembaruan kebijakan terkelola	Pembaruan kebijakan AmazonDataZonePrev iewConsoleFullAccess terkelola. Untuk informasi selengkapnya, lihat DataZone pembaruan Amazon ke AWS kebijakan terkelola.	13 Juni 2023
Pembaruan kebijakan terkelola	Pembaruan kebijakan AmazonDataZoneProj ectDeploymentPermi ssionsBoundary terkelola. Untuk informasi selengkapnya, lihat DataZone pembaruan Amazon ke AWS kebijakan 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.