aws

Manual do usuário

Amazon DataZone

Amazon DataZone: Manual do usuário

Table of Contents

O que é a Amazon DataZone?

DataZone A Amazon é um serviço de gerenciamento de dados que torna mais rápido e fácil catalogar, descobrir, compartilhar e controlar dados armazenados em AWS fontes locais e terceirizadas. Com a Amazon DataZone, os administradores que supervisionam os ativos de dados da organização podem gerenciar e controlar o acesso aos dados usando controles refinados. Esses controles ajudam a garantir o acesso com o nível certo de privilégios e contexto. A Amazon DataZone facilita que engenheiros, cientistas de dados, gerentes de produto, analistas e usuários corporativos compartilhem e acessem dados em toda a organização para que possam descobrir, usar e colaborar para obter insights baseados em dados.

DataZone A Amazon ajuda você a entregar dados diretamente aos usuários finais e simplifica sua arquitetura integrando serviços de gerenciamento de dados, incluindo Amazon Redshift, Amazon Athena, Amazon, QuickSight Glue, Lake AWS Formation, fontes locais AWS , fontes terceirizadas e muito mais.

Tópicos

O que posso fazer com a Amazon DataZone?

Com a Amazon DataZone, você pode fazer o seguinte:

- Controle o acesso aos dados além dos limites organizacionais. Com a Amazon DataZone, você pode ajudar a garantir que os dados certos sejam acessados pelo usuário certo para a finalidade certa, de acordo com os regulamentos de segurança da sua organização, sem depender de credenciais individuais. Você também pode fornecer transparência sobre o uso de ativos de dados e aprovar assinaturas de dados com um fluxo de trabalho controlado. Você também pode monitorar ativos de dados em todos os projetos por meio de recursos de auditoria de uso.
- Conecte profissionais de dados por meio de dados e ferramentas compartilhados para gerar insights de negócios. Com a Amazon DataZone, você pode aumentar a eficiência da equipe de negócios colaborando perfeitamente entre as equipes e fornecendo acesso de autoatendimento a ferramentas de dados e análises. Você pode usar termos comerciais para pesquisar, compartilhar

e acessar dados catalogados armazenados localmente ou com fornecedores terceirizados. AWS E você pode aprender mais sobre os dados que deseja usar usando os glossários de DataZone negócios da Amazon.

- Automatize a descoberta e a catalogação de dados com o aprendizado de máquina. Com a Amazon DataZone, você pode reduzir o tempo gasto na entrada manual de atributos de dados no catálogo de dados corporativos. Dados mais ricos no catálogo de dados também melhoram a experiência de pesquisa.

Como a Amazon DataZone oferece suporte e se integra a outros AWS serviços?

A Amazon DataZone oferece suporte a três tipos de integrações com outros AWS serviços:

- Fontes de dados do produtor — você pode publicar ativos de dados no DataZone catálogo da Amazon a partir dos dados armazenados nas tabelas e visualizações do AWS Glue Data Catalog e do Amazon Redshift. Você também pode publicar manualmente objetos do Amazon Simple Storage Service (S3) no catálogo da Amazon. DataZone
- Ferramentas para consumidores — você pode usar os editores de consulta do Amazon Athena ou do Amazon Redshift para acessar e analisar seus ativos de dados.
- Controle de acesso e atendimento — A Amazon DataZone oferece suporte à concessão de acesso às tabelas AWS Glue gerenciadas pelo AWS Lake Formation e às tabelas e visualizações do Amazon Redshift. Para todos os outros ativos de dados, a Amazon DataZone publica eventos padrão relacionados às suas ações (por exemplo, aprovação dada a uma solicitação de assinatura) na Amazon EventBridge. Você pode usar esses eventos padrão para se integrar a outros AWS serviços ou soluções de terceiros para integrações personalizadas.

Como posso acessar a Amazon DataZone?

Você pode acessar a Amazon DataZone de qualquer uma das seguintes formas:

- DataZone Console da Amazon

  Você pode usar o console DataZone de gerenciamento da Amazon para acessar e configurar seus DataZone domínios, planos e usuários da Amazon. Para obter mais informações, consulte https://console.aws.amazon.com/datazone. O console DataZone de gerenciamento da Amazon também é usado para criar o portal de DataZone dados da Amazon.

- Portal de DataZone dados da Amazon

  O portal de DataZone dados da Amazon é um aplicativo web baseado em navegador no qual você pode catalogar, descobrir, controlar, compartilhar e analisar dados de forma autossuficiente. O portal de dados pode autenticar você com credenciais do seu provedor de identidade por meio do AWS IAM Identity Center (sucessor do AWS SSO) ou com suas credenciais do IAM. Você pode obter a URL do portal de dados acessando o DataZone console da Amazon em https://console.aws.amazon.com/datazone.

- API DataZone HTTPS da Amazon

  Você pode acessar a Amazon DataZone programaticamente usando a API Amazon DataZone HTTPS, que permite emitir solicitações HTTPS diretamente para o serviço. Para obter mais informações, consulte a Amazon DataZone API Reference.

DataZone Terminologia e conceitos da Amazon

Ao começar a usar a Amazon DataZone, é importante que você entenda seus principais conceitos, terminologia e componentes.

Tópicos

DataZone Componentes da Amazon

A Amazon DataZone inclui os quatro componentes principais a seguir:

- Catálogo de dados corporativos - você pode usar esse componente para catalogar dados em toda a sua organização com contexto comercial e, assim, permitir que todos em sua organização encontrem e entendam os dados rapidamente.
- Publique e assine fluxos de trabalho — você pode usar esses fluxos de trabalho automatizados para proteger os dados entre produtores e consumidores de forma autônoma e para garantir que todos em sua organização tenham acesso aos dados certos para a finalidade certa.
- Projetos e ambientes
  - Nos DataZone projetos da Amazon, são agrupamentos de pessoas, ativos (dados) e ferramentas baseados em casos de uso comercial usados para simplificar o acesso às análises. AWS Os projetos fornecem áreas em que os membros do projeto podem colaborar, trocar dados e compartilhar ativos. Por padrão, os projetos são configurados para que somente aqueles que são explicitamente adicionados ao projeto possam acessar as ferramentas de dados e análises contidas neles. Os projetos gerenciam a propriedade dos ativos produzidos de acordo com as políticas do projeto para os consumidores de dados acessarem.

  - Nos DataZone projetos da Amazon, os ambientes são coleções de zero ou mais recursos configurados (por exemplo, um bucket do Amazon S3, um AWS Glue banco de dados ou um grupo de trabalho do Amazon Athena) nos quais um determinado conjunto de diretores do IAM (por exemplo, usuários com permissões de colaborador) pode operar.
- Portal de dados (fora do AWS Management Console) — é um aplicativo web baseado em navegador em que diferentes usuários podem catalogar, descobrir, controlar, compartilhar e analisar dados de forma autônoma. O portal de dados autentica usuários com credenciais do IAM ou credenciais existentes do seu provedor de identidade por meio de. AWS IAM Identity Center

O que são DataZone domínios da Amazon?

Você pode usar os DataZone domínios da Amazon para organizar seus ativos, usuários e seus projetos. Ao associar AWS contas adicionais aos seus DataZone domínios da Amazon, você pode reunir suas fontes de dados. Em seguida, você pode publicar ativos dessas fontes de dados no catálogo do seu domínio, com formulários de metadados e glossários que melhoram a integridade e a qualidade dos metadados. Você também pode pesquisar e navegar nesses ativos para ver quais dados são publicados no domínio. Além disso, você pode participar de projetos para colaborar com outros usuários, assinar ativos e usar ambientes de projeto para acessar ferramentas de análise, incluindo Amazon Athena e Amazon Redshift. Os DataZone domínios da Amazon permitem que você tenha a flexibilidade de refletir as necessidades de dados e análises de sua estrutura organizacional, seja criando um único DataZone domínio da Amazon para sua empresa ou vários DataZone domínios da Amazon para diferentes unidades de negócios.

O que são DataZone projetos e ambientes da Amazon?

A Amazon DataZone permite que equipes e usuários de análises colaborem em projetos criando grupos de equipes, ferramentas e dados baseados em casos de uso.

- Na Amazon DataZone, os projetos permitem que um grupo de usuários colabore em vários casos de uso comercial que envolvem publicação, descoberta, assinatura e consumo de dados no catálogo da Amazon. DataZone Os membros do projeto consomem ativos do DataZone catálogo da Amazon e produzem novos ativos usando um ou mais fluxos de trabalho analíticos. Os projetos apoiam as seguintes atividades no portal de dados:
  - Os proprietários do projeto podem adicionar membros com permissões de proprietário e colaborador
  - Os membros do projeto podem ser usuários de SSO, grupos de SSO e usuários do IAM

- Os membros do projeto podem solicitar a assinatura dos ativos no catálogo de dados

  As aprovações de assinatura são fornecidas aos projetos
- Em um DataZone projeto da Amazon, os ambientes são coleções de zero ou mais recursos configurados (por exemplo, um Amazon S3, um AWS Glue banco de dados ou um grupo de trabalho do Amazon Athena), com um determinado conjunto de diretores do IAM que podem operar com esses recursos. Os ambientes são criados usando perfis de ambiente que são conjuntos pré-configurados de recursos e esquemas que fornecem modelos reutilizáveis para a criação de ambientes. Os perfis de ambiente definem configurações como a região Conta da AWS ou na qual os ambientes são implantados.

O que são DataZone plantas da Amazon?

Um plano com o qual o ambiente é criado define quais AWS ferramentas e serviços (por exemplo, AWS Glue ou o Amazon Redshift) os membros do projeto ao qual o ambiente pertence podem usar ao trabalhar com ativos no catálogo da Amazon DataZone .

Na versão atual da Amazon DataZone, os seguintes esquemas padrão são compatíveis:

Nome do blueprint	Descrição	Recursos criados
Projeto do Data Lake	Permite que os membros DataZone do projeto da Amazon lancem serviços para produtores e consumidores do Data Lake dentro do ambiente. Como consumidor, ele permite que os membros do DataZone projeto da Amazon acessem uma cópia “somente para leitura” dos ativos gerenciados pelo Lake Formation diretamente no Amazon Athena e em outros mecanismos de consulta	Oferece aos usuários a capacidade de criar e consultar tabelas do Lake Formation usando o Amazon Athena. Grupo de trabalho do Amazon Athena, AWS Glue banco de dados com permissões “somente para leitura” do Lake Formation, permissões “somente para leitura” do IAM e acesso ao Amazon S3 que é gerenciado pelo projeto. AWS Glue banco de dados com permissões de 'criar' e 'conceder' Lake

Nome do blueprint	Descrição	Recursos criados
	compatíveis com o Lake Formation. Como produtor, ele permite que os membros DataZone do projeto da Amazon criem novas tabelas LakeForma tion gerenciadas usando o Amazon Athena e as publiquem no catálogo da Amazon DataZone.	Formation, permissões de 'leitura' e 'gravação' do IAM, AWS Glue ETL (extrair, transformar e carregar) com marcação.
Projeto do Data Warehouse	Como consumidor, esse plano permite que os membros DataZone do projeto da Amazon se conectem aos seus próprios clusters do Amazon Redshift para consultar datastores remotos e criar e armazenar novos conjuntos de dados. Como produtor, esse plano permite que os membros DataZone do projeto da Amazon se conectem aos seus próprios clusters do Amazon Redshift para consultar datastores remotos, criar novos conjuntos de dados e publicá-los no catálogo da Amazon. DataZone	Acesso ao editor de consultas do Amazon Redshift, acesso de “leitura” às fontes de dados inscritas do DataZone catálogo da Amazon, capacidade de criar ativos locais no cluster configurado do Amazon Redshift. Acesso ao editor de consultas do Amazon Redshift, acesso de “leitura” às fontes de dados inscritas do DataZone catálogo da Amazon, capacidade de criar e publicar ativos do cluster configurado do Amazon Redshift.

Nome do blueprint	Descrição	Recursos criados
Projeto do Amazon Sagemaker	Esse plano ajuda produtores e consumidores de dados a migrarem facilmente para a Amazon para SageMaker colaborar em projetos de aprendizado de máquina (ML) e, ao mesmo tempo, reforçar a governança do acesso a dados e ativos de ML. Com a nova integração integrada entre a Amazon DataZone e a Amazon SageMaker, consumidores e produtores de dados podem simplificar a governança de ML em toda a configuração da infraestrutura, colaborar em iniciativas de negócios e governar facilmente dados e ativos de ML.	Você pode criar um SageMaker domínio da Amazon que pode pesquisar, assinar e publicar dados e ativos de ML na Amazon DataZone. Também pode se inscrever e publicar nos bancos de dados AWS Glue e no Lake Formation conforme configurado.

O que são fluxos de trabalho DataZone de inventário e publicação da Amazon?

Criação de ativos de inventário do projeto

Para usar a Amazon DataZone para catalogar seus dados, você deve primeiro trazer seus dados (ativos) como inventário do seu projeto na Amazon DataZone. A criação de inventário para um projeto torna os ativos detectáveis somente para os membros desse projeto. Os ativos do inventário do projeto não estão disponíveis para todos os usuários do domínio na pesquisa/navegação, a menos que sejam publicados explicitamente. Na versão atual da Amazon DataZone, você pode adicionar ativos ao inventário do projeto das seguintes formas:

- Crie e execute fontes de dados por meio do portal de dados ou usando as DataZone APIs da Amazon. Na versão atual da Amazon DataZone, você pode criar e executar fontes de dados

para o AWS Glue e o Amazon Redshift. Ao criar e executar fontes de dados do AWS Glue ou do Amazon Redshift, você cria ativos em um inventário de projeto escolhido e importa seus metadados técnicos das tabelas do banco de dados de origem ou dos armazéns de dados como inventário para a Amazon. DataZone

- Usando APIs, você pode criar ativos a partir dos tipos de ativos do sistema disponíveis (objetos AWS Glue, Amazon Redshift, Amazon S3) ou de seus tipos de ativos personalizados.
  - Crie tipos de ativos personalizados em um inventário de projetos usando as DataZone APIs da Amazon. Os tipos de ativos personalizados podem incluir modelos de ML, painéis, tabelas locais etc.
  - Crie ativos a partir desses tipos de ativos personalizados usando as DataZone APIs da Amazon.
- Crie manualmente ativos para objetos do S3 usando o portal de DataZone dados da Amazon.

Organização dos ativos do inventário do projeto — depois de criar um inventário do projeto, os proprietários dos dados podem organizar seus ativos de inventário com os metadados comerciais necessários adicionando ou atualizando nomes comerciais (ativo e esquema), descrições (ativo e esquema), leia-me, termos do glossário (ativo e esquema) e formulários de metadados. Você pode fazer isso por meio do portal de dados ou usando as DataZone APIs da Amazon. Cada edição em seu ativo cria uma nova versão do inventário.

Publicação de ativos de inventário do projeto no DataZone catálogo da Amazon

A próxima etapa de usar DataZone a Amazon para catalogar seus dados é fazer com que os ativos de inventário do seu projeto possam ser descobertos pelos usuários do domínio. Você pode fazer isso publicando os ativos de inventário no DataZone catálogo da Amazon. Somente a versão mais recente do ativo de inventário pode ser publicada no catálogo e somente a versão mais recente publicada está ativa no catálogo de descobertas. Se um ativo de inventário for atualizado após ser publicado no DataZone catálogo da Amazon, você deverá publicá-lo explicitamente novamente para que a versão mais recente esteja no catálogo de descobertas. Na versão atual da Amazon DataZone, você pode publicar seus ativos de inventário do projeto no DataZone catálogo da Amazon das seguintes formas:

- Publique manualmente os ativos de inventário do seu projeto no DataZone catálogo da Amazon por meio do portal de dados ou usando as DataZone APIs da Amazon.
- Como parte da criação ou edição de fontes de dados, ative as configurações opcionais Publish your AWS Glue no catálogo ou Publish seus ativos do Amazon Redshift nas configurações do

catálogo para serem usadas durante as execuções programadas ou automatizadas da fonte de dados. Quando essa configuração está ativada, a execução de uma fonte de dados adiciona ativos ao inventário do seu projeto e, em seguida, também publica os ativos do inventário no DataZone catálogo da Amazon. Observe que, se você publicar diretamente, os ativos podem não ter metadados comerciais e poderão ser descobertos diretamente por todos os usuários do domínio. Você pode usar essa configuração em suas fontes de dados por meio do portal de dados ou usando as DataZone APIs da Amazon.

O que são fluxos de trabalho de DataZone assinatura e atendimento da Amazon?

Depois que seus ativos são publicados no DataZone catálogo da Amazon, os usuários do seu domínio podem descobrir esses ativos, solicitar e obter acesso a esses ativos e continuar a usar DataZone a Amazon para governar, compartilhar e analisar esses ativos.

Os usuários solicitam acesso a um ativo assinando esse ativo em nome de um projeto. Depois que uma solicitação de assinatura é criada, os proprietários do ativo recebem uma notificação e podem analisar a solicitação de assinatura e decidir se querem aprová-la ou rejeitá-la. Se a solicitação de assinatura for aprovada pelo proprietário dos dados, o projeto assinante terá acesso a esse ativo.

Depois que uma solicitação de assinatura é aprovada, DataZone a Amazon inicia um fluxo de trabalho de atendimento de assinaturas que adiciona automaticamente o ativo a todos os ambientes aplicáveis dentro do projeto, criando as doações necessárias no AWS Lake Formation ou no Amazon Redshift. Isso permite que os membros assinantes do projeto consultem o ativo usando uma das ferramentas de consulta (Amazon Athena ou editor de consultas Amazon Redshift) em seus ambientes.

A Amazon DataZone pode acionar essa lógica de atendimento automatizado somente para ativos gerenciados (isso inclui tabelas AWS Glue e tabelas e visualizações do Amazon Redshift). Para todos os outros tipos de ativos (ativos não gerenciados), a Amazon não DataZone pode acionar automaticamente o atendimento, mas publica um evento no Amazon Eventbridge com todos os detalhes necessários na carga útil do evento para que você possa criar as doações necessárias fora da Amazon. DataZone A Amazon DataZone também fornece a `updateSubscriptionStatus` API que permite que você atualize o status da assinatura assim que ela for preenchida fora da Amazon, DataZone para que a Amazon DataZone possa notificar os membros do projeto de que eles podem começar a consumir o ativo.

As personas dos usuários da Amazon DataZone

A seguir estão as principais personas dos DataZone usuários da Amazon:

- Administradores de domínio que possuem a configuração da Amazon DataZone como plataforma de análise para sua organização.

  No contexto da Amazon DataZone, os administradores de domínio instalam a Amazon DataZone em AWS contas, criam DataZone domínios da Amazon e configuram associações de AWS contas e associações de provedores de identidade com domínios da Amazon DataZone . Os administradores de domínio também usam outros consoles AWS de serviços, como AWS Organization e Service Catalog, para configurar a Amazon. DataZone
- Usuários de dados que são os principais usuários da Amazon DataZone (editores de ativos e assinantes) para suas tarefas de análise e aprendizado de máquina.

  Os usuários de dados incluem profissionais de análise de dados, cientistas de dados e usuários do sistema que produzem e consomem ativos de dados. No contexto da Amazon DataZone, os usuários de dados criam e participam de projetos e ambientes, assinam e consomem ativos de dados com ferramentas de análise ou aprendizado de máquina pré-configuradas e publicam ativos de dados de saída no catálogo de DataZone domínios da Amazon para compartilhar com outras pessoas.
- Desenvolvedores de sistemas que criam modelos de infraestrutura personalizados e integram a Amazon DataZone com catálogos internos ou sistemas de produção.

  No contexto da Amazon DataZone, os desenvolvedores de sistemas criam planos de ambiente (modelos de infraestrutura) ou pipeline de CI/CD de infraestrutura como código como provedor de ambiente, pipelines de dados para promover ativos de dados em todos os ambientes, adaptadores de sincronização de catálogos e distribuição de subsídios de assinatura para integração com catálogos internos ou integrações entre APIs da Amazon e interfaces de usuário internas ou sistemas de produção, se necessário. DataZone
- Agentes de governança de dados que possuem as definições e os riscos de segurança organizacional, privacidade e outras políticas de conformidade e que garantem que o uso da Amazon DataZone em suas organizações esteja em conformidade com essas definições.

DataZone Terminologia da Amazon

Domínio

Um DataZone domínio da Amazon é a entidade organizadora para conectar seus ativos, usuários e seus projetos. Com os DataZone domínios da Amazon, você tem a flexibilidade de refletir as necessidades de dados e análises de sua estrutura organizacional, seja criando um único DataZone domínio da Amazon para sua empresa ou várias zonas de dados; domínios para diferentes unidades de negócios ou equipes.

Conta associada

Associar suas AWS contas aos DataZone domínios da Amazon permite que você publique dados dessas AWS contas no DataZone catálogo da Amazon e crie DataZone projetos da Amazon para trabalhar com seus dados em várias AWS contas. Solicitações de associação de conta só podem ser iniciadas em AWS contas que possuem um DataZone domínio da Amazon. As solicitações de associação de conta só podem ser aceitas pelos usuários administrativos das AWS contas convidadas. Depois que uma AWS conta é associada a um DataZone domínio da Amazon, você pode registrar suas fontes de dados, como o catálogo AWS Glue e o Amazon Redshift, nessa conta para esse domínio. Estar associado também permite que uma AWS conta crie DataZone projetos e ambientes da Amazon.

Um Conta da AWS pode ser associado a um ou mais DataZone domínios da Amazon.

Fonte de dados

Na Amazon DataZone, você pode usar fontes de dados para importar metadados técnicos de ativos (dados) dos bancos de dados de origem ou armazéns de dados para a Amazon. DataZone Na versão atual da Amazon DataZone, você pode criar e executar fontes de dados para o AWS Glue e o Amazon Redshift. Ao criar uma fonte de dados, você estabelece uma conexão entre a Amazon DataZone e a fonte (AWS Glue Data Catalog ou Amazon Redshift Warehouse) que permite ler metadados técnicos, incluindo nomes de tabelas, nomes de colunas e tipos de dados. Ao criar uma fonte de dados, você também inicia a execução inicial da fonte de dados que cria novos ativos ou atualiza ativos existentes na Amazon DataZone. Ao criar uma fonte de dados ou após a criação bem-sucedida da fonte de dados, você também tem a opção de especificar um cronograma para a execução da fonte de dados.

Execução da fonte de dados

Na Amazon DataZone, a execução de uma fonte de dados é uma tarefa que DataZone a Amazon executa para criar ativos nos inventários do projeto e, opcionalmente, publicar ativos do inventário

do projeto no catálogo da Amazon DataZone . As execuções da fonte de dados podem ser automatizadas (iniciadas quando uma fonte de dados é criada inicialmente) ou programadas ou manuais. Os critérios de seleção de dados permitem que você ajuste os conjuntos de dados existentes e futuros a serem inseridos nos inventários do projeto ou no DataZone catálogo da Amazon e a frequência das atualizações de metadados nesses ativos de inventário ou catálogo.

Meta da assinatura

Na Amazon DataZone, as metas de assinatura permitem que você acesse os dados nos quais você se inscreveu em seus projetos. Uma meta de assinatura especifica a localização (por exemplo, um banco de dados ou um esquema) e as permissões necessárias (por exemplo, uma função do IAM) que a Amazon DataZone pode usar para estabelecer uma conexão com os dados de origem e criar as concessões necessárias para que os membros do DataZone projeto da Amazon possam começar a consultar os dados nos quais se inscreveram.

Solicitação de assinatura

Na Amazon DataZone, uma solicitação de assinatura é um processo que um DataZone projeto da Amazon deve seguir para ter acesso a um ativo específico. As solicitações de assinatura podem ser aprovadas, rejeitadas, revogadas ou concedidas.

Ativo

Na Amazon DataZone, um ativo é uma entidade que apresenta um único objeto de dados físicos (por exemplo, uma tabela, um painel, um arquivo) ou um objeto de dados virtual (por exemplo, uma visualização).

Asset type (Tipo de ativo)

Os tipos de ativos definem como os ativos são representados no DataZone catálogo da Amazon. Um tipo de ativo define o esquema para um tipo específico de ativo. Quando os ativos são criados, eles são validados em relação ao esquema definido pelo tipo de ativo (por padrão, a versão mais recente). Quando ocorre uma atualização de ativos, a Amazon DataZone cria uma nova versão do ativo e permite que DataZone os usuários da Amazon operem em todas as versões do ativo.

Glossário de negócios

Na Amazon DataZone, um glossário comercial é uma coleção de termos comerciais que podem estar associados a ativos. Um glossário de negócios ajuda a garantir que os mesmos termos e definições sejam usados em toda a organização em suas várias tarefas de análise de dados.

Os termos em um glossário comercial podem ser adicionados aos ativos e colunas para classificar ou aprimorar a identificação desses atributos durante a pesquisa. O glossário pode ser selecionado como o tipo de valor de um campo em um formulário de metadados associado a um ativo. Quando um termo específico é selecionado como o valor do campo do formulário de metadados de um ativo, os usuários podem pesquisar o termo do glossário comercial e encontrar os ativos associados.

Tipo de formulário de metadados

Um tipo de formulário de metadados é um modelo que define os metadados que são coletados e salvos quando os ativos são criados como inventário ou publicados em um domínio da Amazon DataZone . Os tipos de formulários de metadados podem ser associados a um ativo de dados. Os tipos de formulários de metadados ajudam os administradores de domínio a definir os formulários de metadados necessários para esse domínio, como informações de conformidade, informações regulamentares ou classificações. Ele permite que os administradores de domínio personalizem metadados adicionais para seus ativos. DataZone A Amazon tem tipos de formulários de metadados do sistema, como asset-common-details-form -type, column-business-metadata-form -type, glue-table-form-type,, glue-view-form-type, redshift-table-form-type redshift-view-form-type, s3-object-collection-form-type, e. subscription-terms-form-type suggestion-form-type

Formulário de metadados

Na Amazon DataZone, os formulários de metadados definem os metadados que são coletados e salvos quando os ativos são criados como inventário ou publicados em um domínio da Amazon DataZone . As definições do formulário de metadados são criadas no domínio do catálogo por um administrador do domínio. Uma definição de formulário de metadados é composta por uma ou mais definições de campo, com suporte para tipos de dados de valor de campo booleano, de data, decimal, inteiro, sequência de caracteres e glossário comercial.

Um administrador de domínio aplica um formulário de metadados aos ativos em seu domínio adicionando o formulário de metadados ao domínio. Em seguida, os editores de ativos fornecem todos os valores de campo opcionais e obrigatórios no formulário de metadados.

Projeto

Na Amazon DataZone, os projetos permitem que um grupo de usuários colabore em vários casos de uso comercial que envolvem a criação de ativos nos inventários do projeto e, assim, torná-los detectáveis por todos os membros do projeto e, em seguida, publicar, descobrir, assinar e consumir ativos no catálogo da Amazon. DataZone Os membros do projeto consomem ativos do DataZone catálogo da Amazon e produzem novos ativos usando um ou mais fluxos de trabalho

analíticos. Os membros do projeto podem ser proprietários ou colaboradores. Os proprietários do projeto podem adicionar ou remover outros usuários como proprietários ou colaboradores e podem modificar ou excluir projetos. Outras restrições aos colaboradores podem ser definidas com políticas. Quando um usuário cria um projeto, ele se torna o primeiro proprietário desse projeto.

Ambiente

Um ambiente é uma coleção de recursos configurados (por exemplo, um bucket do Amazon S3, um AWS Glue banco de dados ou um grupo de trabalho do Amazon Athena), com um determinado conjunto de diretores do IAM (com permissões de colaborador atribuídas) que podem operar nesses recursos. Cada ambiente também pode ter usuários principais autorizados a acessar os recursos e obter acesso aos dados por meio de assinatura e atendimento. Os ambientes são projetados para armazenar links acionáveis em AWS serviços, IDEs e consoles externos. Os membros do projeto podem acessar serviços como o console Amazon Athena e muito mais por meio de links diretos configurados em um ambiente. Os usuários de SSO e de IAM do projeto podem ser mais detalhados para usar/acessar ambientes específicos.

Perfil do ambiente

Na Amazon DataZone, um perfil de ambiente é um modelo que você pode usar para criar ambientes. Os perfis de ambiente são criados usando blueprints.

Com os perfis de ambiente, os administradores de domínio podem agrupar esquemas com parâmetros pré-configurados e, em seguida, os operadores de dados podem criar rapidamente qualquer número de novos ambientes selecionando perfis de ambiente existentes e especificando nomes para os novos ambientes. Isso permite que os profissionais de dados gerenciem com eficiência seus projetos e ambientes e, ao mesmo tempo, assegurem que satisfaçam as políticas de governança de dados impostas por seus administradores de domínio.

Blueprint

Um plano com o qual o ambiente é criado define quais AWS ferramentas e serviços (por exemplo, AWS Glue ou o Amazon Redshift) os membros do projeto ao qual o ambiente pertence podem usar ao trabalhar com ativos no catálogo da Amazon DataZone .

Na versão atual da Amazon, DataZone os seguintes esquemas padrão são suportados:

- Projeto do data lake
- Plano de data warehouse
- Projeto do Amazon Sagemaker

Perfis de usuário

Um perfil de usuário representa DataZone os usuários da Amazon. A Amazon DataZone suporta funções do IAM e identidades de SSO para interagir com o Amazon DataZone Management Console e o portal de dados para diferentes propósitos. Os administradores de domínio usam funções do IAM para realizar o trabalho administrativo inicial relacionado ao domínio no Amazon DataZone Management Console, incluindo a criação de novos DataZone domínios da Amazon, a configuração de tipos de formulários de metadados e a implementação de políticas. Os profissionais de dados usam suas identidades corporativas de SSO por meio do Identity Center para fazer login no Amazon DataZone Data Portal e acessar projetos nos quais têm associações.

Perfil do grupo

Os perfis de grupo representam grupos de DataZone usuários da Amazon. Os grupos podem ser criados manualmente ou mapeados para grupos do Active Directory de clientes corporativos. Na Amazon DataZone, os grupos têm dois propósitos. Primeiro, um grupo pode mapear uma equipe de usuários no organograma e, assim, reduzir o trabalho administrativo do proprietário de um DataZone projeto da Amazon quando há novos funcionários entrando ou saindo de uma equipe. Segundo, os administradores corporativos usam grupos do Active Directory para gerenciar e atualizar os status dos usuários e, portanto, os administradores de DataZone domínio da Amazon podem usar essas associações de grupos para implementar políticas de domínio da Amazon. DataZone

Administrador de domínio

Na Amazon DataZone, um diretor do IAM que cria um DataZone domínio da Amazon é o administrador padrão desse domínio. Os administradores de domínio na Amazon DataZone executam as principais funcionalidades do domínio, incluindo a criação de domínios, a atribuição de outros administradores de domínio, a adição de fontes de dados e metas de assinatura, a criação de projetos e ambientes e a designação de proprietários de projetos.

Editora

Na Amazon DataZone, os editores publicam ativos no DataZone catálogo da Amazon e podem editar os metadados dos ativos que publicam. Se essa autoridade for concedida, os editores podem aprovar ou rejeitar solicitações de assinatura dos ativos que publicaram no catálogo da Amazon DataZone .

Assinante

Na Amazon DataZone, um assinante é um DataZone projeto da Amazon que deseja encontrar, acessar e consumir ativos no catálogo da Amazon DataZone .

Conta da AWS owner

Na Amazon DataZone, Conta da AWS os proprietários criam funções, políticas e permissões Contas da AWS que permitem que elas Contas da AWS sejam associadas aos DataZone domínios da Amazon.

O que há de novo na Amazon DataZone?

Esta seção descreve novos recursos e melhorias na Amazon DataZone por data de lançamento.

Tópicos

2024

Amazon DataZone lança integração com a Amazon SageMaker

Lançado em 05/06/2024

A Amazon DataZone lança a integração com SageMaker a Amazon para ajudar produtores e consumidores de dados a migrarem facilmente para a Amazon SageMaker para colaborar em projetos de aprendizado de máquina (ML) e, ao mesmo tempo, impor a governança do acesso a dados e ativos de ML. Com a nova integração integrada entre a Amazon DataZone e a Amazon SageMaker, consumidores e produtores de dados podem simplificar a governança de ML em toda a configuração da infraestrutura, colaborar em iniciativas de negócios e governar facilmente dados e ativos de ML. Para obter mais informações, consulte Trabalhando com os projetos DataZone integrados da Amazon e Trabalhando com contas associadas para publicar e consumir dados.

Amazon DataZone lança integração com o modo de acesso híbrido AWS Lake Formation

Lançado em 04/03/2024

DataZone A Amazon introduziu uma integração com o modo de acesso híbrido AWS Lake Formation. Essa integração permite que você publique e compartilhe facilmente suas tabelas AWS Glue na Amazon DataZone, sem a necessidade de registrá-las primeiro no AWS Lake Formation. Para começar, os administradores habilitam a configuração de registro de localização de dados sob o `DefaultDataLake` blueprint no console da Amazon DataZone . Então, quando um consumidor de dados se inscreve em uma tabela AWS Glue gerenciada por meio de permissões do IAM, a Amazon DataZone primeiro registra as localizações dessa tabela no Amazon S3 no modo híbrido e, em seguida, concede acesso ao consumidor de dados gerenciando as permissões na tabela por meio

do Lake AWS Formation. Isso garante que as permissões do IAM na tabela continuem existindo com as permissões recém-concedidas do AWS Lake Formation, sem interromper os fluxos de trabalho existentes. Para obter mais informações, consulte DataZone Integração da Amazon com o modo híbrido AWS Lake Formation .

Amazon DataZone lança integração com AWS Glue Data Quality

Lançado em 04/03/2024

A Amazon DataZone lança a integração com o AWS Glue Data Quality e oferece APIs para integrar métricas de qualidade de dados de soluções de qualidade de dados de terceiros. A nova integração permite que você publique automaticamente as pontuações de qualidade do AWS Glue Data no catálogo de dados DataZone comerciais da Amazon. As DataZone APIs da Amazon podem ser usadas para ingerir métricas de qualidade de fontes terceirizadas. Depois de publicados, os consumidores de dados podem facilmente pesquisar ativos de dados, visualizar métricas granulares de qualidade e identificar falhas em verificações e regras, fortalecendo as decisões de negócios. Para obter mais informações, consulte Qualidade de dados na Amazon DataZone.

Lançamento de disponibilidade geral das recomendações de IA para descrições na Amazon DataZone

Lançado em 27/03/2024

A Amazon DataZone anunciou o lançamento de disponibilidade geral do novo recurso generativo baseado em IA para melhorar a descoberta, a compreensão e o uso de dados, enriquecendo o catálogo de dados comerciais. Com um único clique, os produtores de dados podem gerar descrições e contexto abrangentes de dados comerciais, destacar colunas impactantes e incluir recomendações sobre casos de uso analíticos. O lançamento adiciona suporte para APIs que os produtores de dados podem usar para gerar descrições de ativos de forma programática. Para ter mais informações, consulte Usando aprendizado de máquina e IA generativa.

Amazon DataZone lança aprimoramentos na integração com o Amazon Redshift

Lançado em 21/03/2024

DataZone A Amazon introduziu vários aprimoramentos em sua integração com o Amazon Redshift, simplificando o processo de publicação e assinatura de tabelas e visualizações do Amazon Redshift. Essas atualizações simplificam a experiência tanto para produtores quanto para consumidores de

dados, permitindo que eles criem rapidamente ambientes de data warehouse usando credenciais pré-configuradas e parâmetros de conexão fornecidos pelos administradores da Amazon. DataZone Além disso, esses aprimoramentos concedem aos administradores maior controle sobre quem pode usar os recursos em suas AWS contas e nos clusters do Amazon Redshift e com qual finalidade.

- Configuração do blueprint: depois de habilitar o `DefaultDataWarehouseBlueprint` blueprint, você pode controlar quais projetos podem usar o `DefaultDataWarehouseBlueprint` blueprint em sua conta para criar perfis de ambiente atribuindo projetos de gerenciamento ao blueprint ativado. Você também pode criar conjuntos de parâmetros em cima do `DefaultDataWarehouseBlueprint` fornecendo parâmetros como cluster, banco de dados e um AWS segredo. Você também pode criar AWS segredos a partir do DataZone console da Amazon.
- Perfil de ambiente: ao criar um perfil de ambiente, você pode optar por fornecer seus próprios parâmetros do Amazon Redshift ou usar um dos conjuntos de parâmetros da configuração do blueprint. Se você optar por usar o conjunto de parâmetros criado na configuração do blueprint, o AWS segredo exigirá apenas uma `AmazonDataZoneDomain` tag (a `AmazonDataZoneProject` tag só será necessária se você optar por fornecer seus próprios conjuntos de parâmetros no perfil do ambiente). No perfil do ambiente, você pode especificar uma lista de projetos autorizados. Somente projetos autorizados podem usar esse perfil de ambiente para criar ambientes de data warehouse. Você também pode especificar quais dados os projetos autorizados podem publicar. Atualmente, você pode escolher uma das seguintes opções: 1) Publicar de qualquer esquema, 2) Publicar a partir do esquema de ambiente padrão, 3) Não permitir a publicação.
- Ambiente: os produtores ou consumidores de dados agora podem selecionar um perfil de ambiente para criar ambientes, sem a necessidade de fornecer seus próprios parâmetros do Amazon Redshift, incluindo AWS segredo, cluster, grupo de trabalho e banco de dados. Esses parâmetros são transferidos para o ambiente a partir do perfil do ambiente. Além da criação do ambiente, a Amazon DataZone agora também cria um esquema padrão para o ambiente. Os membros do projeto têm acesso de leitura e gravação a esse esquema e podem publicar facilmente qualquer tabela criada nesse esquema no catálogo executando a fonte de dados padrão criada como parte da criação do ambiente. Os parâmetros do Amazon Redshift usados para criar o ambiente também podem ser usados para criar novas fontes de dados (em vez de o produtor de dados fornecer seus próprios parâmetros na criação da fonte de dados).

AWS Cloud Formation Support para Amazon DataZone

Lançado em 18/01/2024

Agora, os usuários da Amazon DataZone podem aproveitar AWS CloudFormation para modelar e gerenciar com eficácia um conjunto de DataZone recursos da Amazon. Essa abordagem facilita o provisionamento consistente de recursos, além de permitir o gerenciamento do ciclo de vida por meio de práticas de infraestrutura como código. Com modelos personalizados, você pode definir com precisão os recursos necessários e suas interdependências. Para obter mais informações, consulte a referência do tipo DataZone de recurso da Amazon.

Adicione diretores do IAM diretamente como membros dos projetos da Amazon DataZone

Lançado em 01/05/2024

Agora você pode adicionar diretores do IAM como membros do projeto, mesmo que esses diretores do IAM ainda não tenham feito login na Amazon DataZone (requisito anterior). Depois que um administrador de domínio ou administrador de TI adiciona `iam:GetUser` e `iam:GetRole` à função de execução do domínio, os proprietários do projeto podem adicionar diretores do IAM como membros simplesmente fornecendo o Amazon Resouce Name (ARN) da função do IAM ou do usuário do IAM. O diretor do IAM ainda precisa ter as permissões do IAM necessárias para acessar a Amazon DataZone e elas podem ser configuradas no console do IAM. Para ter mais informações, consulte Adicionar membros a um projeto.

Support para tipos de ativos personalizados a partir do Portal de Dados

Lançado em 01/05/2024

O suporte para ativos personalizados permite que DataZone a Amazon catalogue ativos por meio do Portal de dados para dados não estruturados, incluindo painéis, consultas e modelos, facilitando a adição de ativos personalizados diretamente no portal de dados junto com o suporte de API disponível anteriormente. A capacidade de criar, atualizar e publicar ativos personalizados na Amazon DataZone permite que você compartilhe, encontre, assine qualquer tipo de ativo e crie um fluxo de trabalho comercial que forneça governança desses ativos. Para ter mais informações, consulte Crie tipos de ativos personalizados.

2023

Excluir domínio

Lançado em 27/12/2023

Esse é um recurso que permite que você exclua seus domínios com mais facilidade. Agora, você pode continuar com a exclusão do domínio mesmo que ele não esteja vazio (pois contém projetos, ambientes, ativos, fontes de dados etc.). Para ter mais informações, consulte Excluir domínios.

Modo híbrido

Lançado em 22/12/2023

DataZone A Amazon adicionou suporte para o modo híbrido AWS Lake Formation. Com esse suporte, se você publicar uma tabela AWS Glue na Amazon DataZone com sua localização AWS S3 registrada em Lake Formation no modo híbrido, a Amazon DataZone tratará essa tabela como um ativo gerenciado e poderá gerenciar as concessões de assinatura dessa tabela. Antes do lançamento desse recurso, a Amazon DataZone tratava essa tabela como um ativo não gerenciado, ou seja, a Amazon não DataZone poderia conceder assinaturas para essa tabela. Para ter mais informações, consulte Configurar as permissões do Lake Formation para a Amazon DataZone.

Elegibilidade para HIPAA

Lançado em 14/12/2023

DataZone A Amazon agora está em conformidade com a Lei de Portabilidade e Responsabilidade de Seguros de Saúde dos EUA de 1996 (HIPAA). Para ver a lista de AWS serviços em conformidade com a HIPAA, consulte https://aws.amazon.com/compliance/ hipaa-eligible-services-reference/.

Recomendações de IA para descrições na Amazon DataZone (versão prévia)

Lançado em 28/11/2023

AWS anuncia a prévia de um novo recurso generativo baseado em IA na Amazon DataZone para melhorar a descoberta, a compreensão e o uso de dados, enriquecendo o catálogo de dados corporativos. Com um único clique, os produtores de dados podem gerar descrições e contexto abrangentes de dados comerciais, destacar colunas impactantes e incluir recomendações sobre casos de uso analíticos. Com as recomendações de IA para descrições na Amazon DataZone, os consumidores de dados podem identificar tabelas e colunas de dados necessárias para análise, o que aumenta a capacidade de descoberta dos dados e reduz a back-and-forth comunicação com os produtores de dados. A versão prévia está disponível em DataZone domínios da Amazon provisionados nas seguintes AWS regiões: Leste dos EUA (Norte da Virgínia), Oeste dos EUA (Oregon). Para ter mais informações, consulte Usando aprendizado de máquina e IA generativa.

DefaultDataLake aprimoramento do plano

Lançado em 20/11/2023

DataZone A Amazon adicionou um aprimoramento ao DefaultDataLake plano que fornece a você um melhor controle sobre quem pode publicar quais dados da sua AWS conta. Há duas mudanças principais que foram introduzidas com o lançamento desse recurso.

- No console, depois de habilitar o DefaultDataLake blueprint, você pode controlar quais projetos podem usar o DefaultDataLake blueprint em sua conta para criar perfis de ambiente atribuindo projetos de gerenciamento ao blueprint ativado.
- A segunda mudança está no portal. Se você criar um perfil de ambiente usando o DefaultDataLake blueprint, também poderá selecionar os projetos autorizados que têm permissão para usar o perfil de ambiente para criar ambientes. Por padrão, todos os projetos podem usar o perfil de ambiente do data lake, mas você pode restringir o perfil do ambiente a projetos específicos e também controlar quais dados podem ser publicados usando os ambientes criados com o perfil.

Para ter mais informações, consulte Crie um perfil de ambiente.

Configuração

Para configurar a Amazon DataZone, você deve ter uma AWS conta e configurar as políticas e permissões do IAM necessárias para a Amazon DataZone.

Depois de configurar suas DataZone permissões da Amazon, é recomendável que você conclua as etapas na seção Introdução, que mostra a criação do DataZone domínio da Amazon, a obtenção da URL do portal de dados e os DataZone fluxos de trabalho básicos da Amazon para produtores e consumidores de dados.

Tópicos

Cadastre-se para uma AWS conta

Se você não tiver uma AWS conta, conclua as etapas a seguir para criar uma.

Se você tiver uma AWS organização, crie uma conta:

1. Faça login no AWS Management Console e abra o console Organizations em https://console.aws.amazon.com/organizations/.
2. No painel de navegação, escolha AWS contas.
3. Escolha Adicionar uma AWS conta.
4. Escolha Criar uma AWS conta e forneça os detalhes solicitados. Escolha Criar AWS conta.

Para se inscrever em uma AWS conta

1. Abra https://portal.aws.amazon.com/billing/signup
2. Siga as instruções on-line.

   Parte do procedimento de inscrição envolve receber uma chamada telefônica e digitar um código de verificação no teclado do telefone.

Quando você se inscreve AWS em uma conta, um usuário raiz da AWS conta é criado. O usuário root tem acesso a todos os AWS serviços e recursos da conta. Como prática recomendada de segurança, atribua acesso administrativo a um usuário administrativo e use somente o usuário-raiz para realizar as tarefas que exigem acesso do usuário-raiz.

Configure as permissões do IAM necessárias para usar o console DataZone de gerenciamento da Amazon

Qualquer usuário, grupo ou função que queira usar o console DataZone de gerenciamento da Amazon deve ter as permissões necessárias.

Tópicos

- Anexe políticas obrigatórias e opcionais a um usuário, grupo ou função para acesso ao DataZone console da Amazon
- Crie uma política personalizada para permissões do IAM para permitir a criação simplificada de funções do console de DataZone serviços da Amazon
- Crie uma política personalizada de permissões para gerenciar uma conta associada a um DataZone domínio da Amazon
- (Opcional) Crie uma política personalizada para permissões do AWS Identity Center para habilitar o login único (SSO) para seu domínio
- (Opcional) Crie uma política personalizada para permissões do AWS Identity Center para adicionar e remover o acesso de usuários e grupos de SSO ao seu domínio da Amazon DataZone .
- (Opcional) Adicione seu principal do IAM como usuário-chave para criar seu DataZone domínio da Amazon com uma chave gerenciada pelo cliente do AWS Key Management Service (KMS)

Anexe políticas obrigatórias e opcionais a um usuário, grupo ou função para acesso ao DataZone console da Amazon

Conclua o procedimento a seguir para anexar as políticas personalizadas obrigatórias e opcionais a um usuário, grupo ou função. Para ter mais informações, consulte AWS políticas gerenciadas para a Amazon DataZone.

1. Faça login no AWS Management Console e abra o console do IAM em https://console.aws.amazon.com/iam/.

2. No painel de navegação, escolha Policies.
3. Escolha as políticas a seguir para anexar ao seu usuário, grupo ou função.

   - Na lista de políticas, marque a caixa de seleção ao lado do AmazonDataZoneFullAccess. Você pode usar o menu Filtro e a caixa de pesquisa para filtrar a lista de políticas. Para ter mais informações, consulte AWS política gerenciada: AmazonDataZoneFullAccess.
   - (Opcional) Crie uma política personalizada para permissões do IAM para permitir que o console de DataZone serviços da Amazon crie funções de forma simplificada.
   - (Opcional) Crie uma política personalizada para as permissões do AWS Identity Center para habilitar o login único (SSO) para seu domínio.
   - (Opcional) Crie uma política personalizada para permissões do AWS Identity Center para adicionar e remover o acesso de usuários e grupos de SSO ao seu domínio da Amazon DataZone .
4. Escolha Actions (Ações) e Attach (Anexar).
5. Escolha o usuário, grupo ou função ao qual você deseja anexar a política. Você pode usar o menu Filter (Filtro) e a caixa de pesquisa para filtrar a lista de entidades principais. Depois de escolher o usuário, o grupo ou a função, escolha Anexar política.

Crie uma política personalizada para permissões do IAM para permitir a criação simplificada de funções do console de DataZone serviços da Amazon

Conclua o procedimento a seguir para criar uma política embutida personalizada para ter as permissões necessárias para permitir DataZone que a Amazon crie as funções necessárias no console AWS de gerenciamento em seu nome.

1. Faça login no AWS Management Console e abra o console do IAM em https://console.aws.amazon.com/iam/.
2. No painel de navegação, selecione Grupos ou Usuários.
3. Na lista, escolha o nome do usuário ou do grupo ao qual deseja incorporar uma política.
4. Selecione a guia Permissions (Permissões) e expanda a seção Permissions policies (Políticas de permissões).
5. Escolha Adicionar permissões e Criar link de política em linha.
6. Na tela Criar política, na seção Editor de políticas, escolha JSON.

Crie um documento de política com as seguintes instruções JSON e escolha Avançar.

```
{
    "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. Na tela Revisar política, insira um nome para a política. Quando estiver satisfeito com a política, escolha Create policy (Criar política). Certifique-se de que nenhum erro seja exibido na caixa vermelha na parte superior da tela. Corrija os que foram relatados.

Crie uma política personalizada de permissões para gerenciar uma conta associada a um DataZone domínio da Amazon

Conclua o procedimento a seguir para criar uma política embutida personalizada para ter as permissões necessárias em uma AWS conta associada para listar, aceitar e rejeitar compartilhamentos de recursos de um domínio e, em seguida, habilitar, configurar e desabilitar blueprints de ambiente na conta associada. Para habilitar a criação simplificada de funções opcional do Amazon DataZone Service Console disponível durante a configuração do blueprint, você também [Crie uma política personalizada para permissões do IAM para permitir a criação simplificada de funções do console de DataZone serviços da Amazon](#) deve.

1. Faça login no AWS Management Console e abra o console do IAM em https://console.aws.amazon.com/iam/.
2. No painel de navegação, selecione Grupos ou Usuários.
3. Na lista, escolha o nome do usuário ou do grupo ao qual deseja incorporar uma política.
4. Selecione a guia Permissions (Permissões) e expanda a seção Permissions policies (Políticas de permissões).
5. Escolha Adicionar permissões e Criar link de política em linha.
6. Na tela Criar política, na seção Editor de políticas, escolha JSON. Crie um documento de política com as seguintes instruções JSON e escolha Avançar.

```
{
    "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. Na tela Revisar política, insira um nome para a política. Quando estiver satisfeito com a política, escolha Create policy (Criar política). Certifique-se de que nenhum erro seja exibido na caixa vermelha na parte superior da tela. Corrija os que foram relatados.

(Opcional) Crie uma política personalizada para permissões do AWS Identity Center para habilitar o login único (SSO) para seu domínio

Conclua o procedimento a seguir para criar uma política embutida personalizada para ter as permissões necessárias para habilitar o login único (SSO) usando o AWS IAM Identity Center na Amazon. DataZone

1. Faça login no AWS Management Console e abra o console do IAM em https://console.aws.amazon.com/iam/.
2. No painel de navegação, selecione Grupos ou Usuários.

3. Na lista, escolha o nome do usuário ou do grupo ao qual deseja incorporar uma política.
4. Selecione a guia Permissions (Permissões) e expanda a seção Permissions policies (Políticas de permissões).
5. Escolha Adicionar permissões e Criar política em linha.
6. Na tela Criar política, na seção Editor de políticas, escolha JSON.

   Crie um documento de política com as seguintes instruções JSON e escolha Avançar.

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

7. Na tela Revisar política, insira um nome para a política. Quando estiver satisfeito com a política, escolha Create policy (Criar política). Certifique-se de que nenhum erro seja exibido na caixa vermelha na parte superior da tela. Corrija os que foram relatados.

(Opcional) Crie uma política personalizada para permissões do AWS Identity Center para adicionar e remover o acesso de usuários e grupos de SSO ao seu domínio da Amazon DataZone .

Conclua o procedimento a seguir para criar uma política embutida personalizada para ter as permissões necessárias para adicionar e remover o acesso de usuários e grupos de SSO ao seu domínio da Amazon. DataZone

1. Faça login no AWS Management Console e abra o console do IAM em https://console.aws.amazon.com/iam/.

2. No painel de navegação, selecione Grupos ou Usuários.
3. Na lista, escolha o nome do usuário ou do grupo ao qual deseja incorporar uma política.
4. Selecione a guia Permissions (Permissões) e expanda a seção Permissions policies (Políticas de permissões).
5. Escolha Adicionar permissões e Criar política em linha.
6. Na tela Criar política, na seção Editor de políticas, escolha JSON.

   Crie um documento de política com as seguintes instruções JSON e escolha Avançar.

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

7. Na tela Revisar política, insira um nome para a política. Quando estiver satisfeito com a política, escolha Create policy (Criar política). Certifique-se de que nenhum erro seja exibido na caixa vermelha na parte superior da tela. Corrija os que foram relatados.

(Opcional) Adicione seu principal do IAM como usuário-chave para criar seu DataZone domínio da Amazon com uma chave gerenciada pelo cliente do AWS Key Management Service (KMS)

Antes de criar opcionalmente seu DataZone domínio da Amazon com uma chave gerenciada pelo cliente (CMK) do AWS Key Management Service (KMS), conclua o procedimento a seguir para tornar seu principal do IAM um usuário da sua chave KMS.

1. Faça login no AWS Management Console e abra o console KMS em https://console.aws.amazon.com/kms/.
2. Para exibir as chaves em sua conta que você cria e gerencia, no painel de navegação, escolha Customer managed keys (Chaves gerenciadas de cliente).
3. Na lista de chaves do KMS, escolha o alias ou o ID de chave da chaves do KMS que você deseja examinar.
4. Para adicionar ou remover usuários-chave e permitir ou proibir que AWS contas externas usem a chave KMS, use os controles na seção Usuários principais da página. Usuários de chaves podem usar a chave do KMS em operações de criptografia, como criptografar, descriptografar, recriptografar e gerar chaves de dados.

Configure as permissões do IAM necessárias para usar o portal de DataZone dados da Amazon

Qualquer usuário, grupo ou função que queira usar o catálogo ou portal de DataZone dados da Amazon deve ter as permissões necessárias.

Tópicos

- Anexe a política necessária a um usuário, grupo ou função para acesso ao portal DataZone de dados da Amazon
- Anexe a política necessária a um usuário, grupo ou função para acesso ao DataZone catálogo da Amazon
- Anexe uma política opcional a um usuário, grupo ou função para acesso ao portal de DataZone dados ou catálogo da Amazon se seu domínio estiver criptografado com uma chave gerenciada pelo cliente do AWS Key Management Service (KMS)

Anexe a política necessária a um usuário, grupo ou função para acesso ao portal DataZone de dados da Amazon

Você pode acessar o portal de DataZone dados da Amazon usando suas AWS credenciais ou suas credenciais de login único (SSO). Siga as instruções na seção abaixo para configurar as permissões necessárias para acessar o portal de dados com suas AWS credenciais. Para obter mais informações sobre o uso da Amazon DataZone com SSO, consulteConfigurando o AWS IAM Identity Center para a Amazon DataZone.

> **Note**
>
> Somente os diretores do IAM na AWS conta do seu domínio podem acessar o portal de dados do domínio. Os diretores do IAM de outras AWS contas não podem acessar o portal de dados do domínio.

Conclua o procedimento a seguir para anexar a política necessária a um usuário, grupo ou função. Para ter mais informações, consulte AWS políticas gerenciadas para a Amazon DataZone.

1. Faça login no AWS Management Console e abra o console do IAM em https://console.aws.amazon.com/iam/.
2. No painel de navegação, escolha Usuários, Grupos de usuários ou Funções.
3. Na lista, escolha o nome do usuário, grupo ou função na qual incorporar uma política.
4. Selecione a guia Permissions (Permissões) e expanda a seção Permissions policies (Políticas de permissões).
5. Escolha Adicionar permissões e Criar link de política em linha.
6. Na tela Criar política, na seção Editor de políticas, escolha JSON. Crie um documento de política com as seguintes instruções JSON e escolha Avançar.

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

```
            "Resource": [
                "*"
            ]
        }
    ]
}
```

7. Na tela Revisar política, insira um nome para a política. Quando estiver satisfeito com a política, escolha Create policy (Criar política). Certifique-se de que nenhum erro seja exibido na caixa vermelha na parte superior da tela. Corrija os que foram relatados.

Anexe a política necessária a um usuário, grupo ou função para acesso ao DataZone catálogo da Amazon

> **Note**
>
> Somente os diretores do IAM na AWS conta do seu domínio podem acessar o catálogo do domínio. Os diretores do IAM de outras AWS contas não podem acessar o catálogo do domínio.

Você pode conceder às suas identidades do IAM acesso ao catálogo do seu DataZone domínio da Amazon por meio da API e do SDK com o procedimento a seguir. Se você quiser que essas identidades do IAM também tenham acesso ao portal de DataZone dados da Amazon, siga o procedimento acima paraAnexe a política necessária a um usuário, grupo ou função para acesso ao portal DataZone de dados da Amazon. Para ter mais informações, consulte AWS políticas gerenciadas para a Amazon DataZone.

1. Faça login no AWS Management Console e abra o console do IAM em https://console.aws.amazon.com/iam/.
2. No painel de navegação, escolha Policies.
3. Na lista de políticas, selecione o botão de rádio ao lado da AmazonDataZoneFullUserAccesspolítica. Você pode usar o menu Filtro e a caixa de pesquisa para filtrar a lista de políticas. Para mais informações, consulte AWS política gerenciada: AmazonDataZoneFullUserAccess.
4. Escolha Actions (Ações) e Attach (Anexar).

5. Escolha o usuário, grupo ou função ao qual você deseja anexar a política marcando a caixa de seleção ao lado de cada principal. Você pode usar o menu Filter (Filtro) e a caixa de pesquisa para filtrar a lista de entidades principais. Depois de escolher o usuário, o grupo ou a função, escolha Anexar política.

Anexe uma política opcional a um usuário, grupo ou função para acesso ao portal de DataZone dados ou catálogo da Amazon se seu domínio estiver criptografado com uma chave gerenciada pelo cliente do AWS Key Management Service (KMS)

Se você criar seu DataZone domínio da Amazon com sua própria chave KMS para criptografia de dados, também deverá criar uma política em linha com as seguintes permissões e anexá-la aos seus diretores do IAM para que eles possam acessar o portal ou catálogo de DataZone dados da Amazon.

1. Faça login no AWS Management Console e abra o console do IAM em https://console.aws.amazon.com/iam/.
2. No painel de navegação, escolha Usuários, Grupos de usuários ou Funções.
3. Na lista, escolha o nome do usuário, grupo ou função na qual incorporar uma política.
4. Selecione a guia Permissions (Permissões) e expanda a seção Permissions policies (Políticas de permissões).
5. Escolha Adicionar permissões e Criar link de política em linha.
6. Na tela Criar política, na seção Editor de políticas, escolha JSON. Crie um documento de política com as seguintes instruções JSON e escolha Avançar.

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

```
    ]
}
```

7. Na tela Revisar política, insira um nome para a política. Quando estiver satisfeito com a política, escolha Create policy (Criar política). Certifique-se de que nenhum erro seja exibido na caixa vermelha na parte superior da tela. Corrija os que foram relatados.

Configurando o AWS IAM Identity Center para a Amazon DataZone

> **Note**
>
> AWS O Identity Center deve estar habilitado na mesma AWS região do seu DataZone domínio da Amazon. Atualmente, o AWS Identity Center só pode ser ativado em uma única AWS região.

Você pode acessar o portal de DataZone dados da Amazon usando suas credenciais de login único (SSO) ou credenciais. AWS Siga as instruções nesta seção para configurar o AWS IAM Identity Center para a Amazon DataZone. Para obter mais informações sobre como usar a Amazon DataZone com suas AWS credenciais, consulteConfigure as permissões do IAM necessárias para usar o console DataZone de gerenciamento da Amazon.

Você pode ignorar os procedimentos nesta seção se já tiver o AWS IAM Identity Center (sucessor do AWS Single Sign-On) habilitado e configurado na mesma AWS região em que deseja criar seu domínio da Amazon. DataZone

Conclua o procedimento a seguir para ativar o AWS IAM Identity Center (sucessor do AWS Single Sign-On).

1. Para habilitar o AWS IAM Identity Center, você deve entrar no AWS Management Console usando as credenciais da sua conta de gerenciamento do AWS Organizations. Você não pode ativar o IAM Identity Center enquanto estiver conectado com as credenciais de uma conta membro do AWS Organizations. Para obter mais informações, consulte Criação e gerenciamento de uma organização no Guia do Usuário do AWS Organizations.
2. Abra o console AWS do IAM Identity Center (sucessor do AWS Single Sign-On) e use o seletor de região na barra de navegação superior para escolher a AWS região na qual você deseja criar seu domínio da Amazon. DataZone

3. Escolha Habilitar.
4. Escolha sua fonte de identidade.

   Por padrão, você obtém um repositório do IAM Identity Center para gerenciamento rápido e fácil de usuários. Opcionalmente, você pode conectar um provedor de identidade externo em vez disso. Nesse procedimento, usamos o armazenamento padrão do IAM Identity Center.

   Para obter mais informações, consulte Escolha sua fonte de identidade.
5. No painel de navegação do IAM Identity Center, escolha Grupos e escolha Criar grupo. Insira o nome do grupo e escolha Criar.
6. No painel de navegação do IAM Identity Center, escolha Usuários.
7. Na tela Adicionar usuário, insira as informações necessárias e escolha Enviar um e-mail para o usuário com instruções de configuração de senha. O usuário deve receber um e-mail sobre as próximas etapas de configuração.
8. Escolha Avançar: Grupos, escolha o grupo que você deseja e escolha Adicionar usuário. Os usuários devem receber um e-mail convidando-os a usar o SSO. Nesse e-mail, eles precisam escolher Aceitar convite e definir a senha.

Depois de criar seu DataZone domínio da Amazon, você pode habilitar o AWS Identity Center for Amazon DataZone e fornecer acesso aos seus usuários e grupos de SSO. Para ter mais informações, consulte Habilite o IAM Identity Center para Amazon DataZone.

Conceitos básicos

As informações nesta seção ajudam você a começar a usar a Amazon DataZone. Se você é novo na Amazon DataZone, comece se familiarizando com os conceitos e a terminologia apresentados em DataZone Terminologia e conceitos da Amazon.

Esta seção de introdução mostra os seguintes fluxos de trabalho de DataZone início rápido da Amazon:

Tópicos

- DataZone Início rápido da Amazon com dados AWS Glue
- Amazon DataZone quickstart com dados do Amazon Redshift
- DataZone Início rápido da Amazon com exemplos de scripts

> **Important**
>
> Antes de iniciar as etapas em qualquer um desses fluxos de trabalho de início rápido, você deve concluir os procedimentos descritos na seção Configuração deste guia. Se você estiver usando uma AWS conta totalmente nova, deverá configurar as permissões necessárias para usar o console DataZone de gerenciamento da Amazon. Se você estiver usando uma AWS conta que tenha objetos existentes do AWS Glue Data Catalog, você também deve configurar as permissões do Lake Formation para a Amazon DataZone.

DataZone Início rápido da Amazon com dados AWS Glue

Tópicos

- Etapa 1 - Crie o DataZone domínio e o portal de dados da Amazon
- Etapa 2 - Crie o projeto de publicação
- Etapa 3 - Crie o ambiente
- Etapa 4 - Produzir dados para publicação
- Etapa 5 - Colete metadados do Glue AWS
- Etapa 6 - Organize e publique o ativo de dados

- Etapa 7 - Crie o projeto para análise de dados
- Etapa 8 - Crie um ambiente para análise de dados
- Etapa 9 - Pesquise o catálogo de dados e assine os dados
- Etapa 10 - Aprovar a solicitação de assinatura
- Etapa 11 - Crie uma consulta e analise dados no Amazon Athena

Etapa 1 - Crie o DataZone domínio e o portal de dados da Amazon

Esta seção descreve as etapas da criação de um DataZone domínio e portal de dados da Amazon para esse fluxo de trabalho.

Conclua o procedimento a seguir para criar um DataZone domínio da Amazon. Para obter mais informações sobre os DataZone domínios da Amazon, consulte DataZone Terminologia e conceitos da Amazon.

1. Navegue até o DataZone console da Amazon em https://console.aws.amazon.com/datazone, faça login e escolha Criar domínio.

   > **Note**
   >
   > Se você quiser usar um DataZone domínio existente da Amazon para esse fluxo de trabalho, escolha Exibir domínios, escolha o domínio que deseja usar e prossiga para a Etapa 2 da criação de um projeto de publicação.

2. Na página Criar domínio, forneça valores para os seguintes campos:

   - Nome - especifique um nome para seu domínio. Para fins desse fluxo de trabalho, você pode chamar esse domínio de Marketing.
   - Descrição - especifique uma descrição de domínio opcional.
   - Criptografia de dados - seus dados são criptografados por padrão com uma chave que AWS possui e gerencia para você. Para esse caso de uso, você pode deixar as configurações padrão de criptografia de dados.

     Para obter mais informações sobre o uso de chaves gerenciadas pelo cliente, consulteCriptografia de dados em repouso para a Amazon DataZone. Se você usar sua própria chave KMS para criptografia de dados, deverá incluir a seguinte declaração em seu padrãoAmazonDataZoneDomainExecutionRole.

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

- Acesso ao serviço - deixe a opção selecionada por padrão Usar uma função padrão inalterada.

> **Note**
>
> Se você estiver usando um DataZone domínio existente da Amazon para esse fluxo de trabalho, poderá escolher a opção Usar uma função de serviço existente e, em seguida, escolher uma função existente no menu suspenso.

- Em Configuração rápida, escolha Configurar esta conta para consumo e publicação de dados. Essa opção habilita os DataZone blueprints integrados da Amazon de Data Lake e Data Warehouse e configura as permissões, os recursos, um projeto padrão e os perfis padrão de ambiente de data lake e data warehouse para essa conta. Para obter mais informações sobre os DataZone projetos da Amazon, consulte DataZone Terminologia e conceitos da Amazon.
- Mantenha os campos restantes em Detalhes de permissões inalterados.

> **Note**
>
> Se você já tiver um DataZone domínio da Amazon, poderá escolher a opção Usar uma função de serviço existente e, em seguida, escolher uma função existente no menu suspenso para a função Glue Manage Access, a função Redshift Manage Access e a função Provisioning.

- Mantenha os campos em Tags inalterados.
- Escolha Criar domínio.

3. Depois que o domínio for criado com sucesso, escolha esse domínio e, na página de resumo do domínio, anote o URL do portal de dados desse domínio. Você pode usar essa URL para acessar seu portal de DataZone dados da Amazon para concluir o restante das etapas desse fluxo de trabalho. Você também pode navegar até o portal de dados escolhendo Abrir portal de dados.

> **Note**
>
> Na versão atual da Amazon DataZone, depois que o domínio é criado, a URL gerada para o portal de dados não pode ser modificada.

A criação do domínio pode levar alguns minutos para ser concluída. Aguarde até que o domínio tenha um status de Disponível antes de prosseguir para a próxima etapa.

Etapa 2 - Crie o projeto de publicação

Esta seção descreve as etapas necessárias para criar o projeto de publicação para esse fluxo de trabalho.

1. Depois de concluir a Etapa 1 acima e criar um domínio, você verá a mensagem Bem-vindo à Amazon DataZone! janela. Nessa janela, escolha Criar projeto.
2. Especifique o nome do projeto, por exemplo, para esse fluxo de trabalho SalesDataPublishingProject, você pode nomeá-lo, deixar os demais campos inalterados e escolher Criar.

Etapa 3 - Crie o ambiente

Esta seção descreve as etapas necessárias para criar um ambiente para esse fluxo de trabalho.

1. Depois de concluir a Etapa 2 acima e criar seu projeto, você verá a janela Seu projeto está pronto para uso. Nessa janela, escolha Criar ambiente.
2. Na página Criar ambiente, especifique o seguinte e escolha Criar ambiente.
3. Especifique valores para o seguinte:

- Nome - especifique o nome do ambiente. Para este passo a passo, você pode ligar para ele. `Default data lake environment`
- Descrição - especifique uma descrição para o ambiente.
- Perfil do ambiente - escolha o perfil do DataLakeProfileambiente. Isso permite que você use a Amazon DataZone nesse fluxo de trabalho para trabalhar com dados no Amazon S3, no AWS Glue Catalog e no Amazon Athena.
- Para este passo a passo, mantenha o resto dos campos inalterados.

4. Selecione Create environment (Criar ambiente).

Etapa 4 - Produzir dados para publicação

Esta seção descreve as etapas necessárias para produzir dados para publicação nesse fluxo de trabalho.

1. Depois de concluir a etapa 3 acima, em seu `SalesDataPublishingProject` projeto, no painel direito, em Ferramentas de análise, escolha Amazon Athena. Isso abre o editor de consultas do Athena usando as credenciais do seu projeto para autenticação. Certifique-se de que seu ambiente de publicação esteja selecionado na lista suspensa do DataZone ambiente da Amazon e que o `<environment_name>%_pub_db` banco de dados esteja selecionado como no editor de consultas.
2. Para este passo a passo, você está usando o script de consulta Create Table as Select (CTAS) para criar uma nova tabela que você deseja publicar na Amazon. DataZone No seu editor de consultas, execute esse script CTAS para criar uma `mkt_sls_table` tabela que você possa publicar e disponibilizar para pesquisa e assinatura.

```
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
```

Certifique-se de que a tabela mkt_sls_table tenha sido criada com sucesso na seção Tabelas e visualizações no lado esquerdo. Agora você tem um ativo de dados que pode ser publicado no DataZone catálogo da Amazon.

Etapa 5 - Colete metadados do Glue AWS

Esta seção descreve a etapa de coleta de metadados do AWS Glue para esse fluxo de trabalho.

1. Depois de concluir a etapa 4 acima, no portal de DataZone dados da Amazon, escolha o `SalesDataPublishingProject` projeto, escolha a guia Dados e, em seguida, escolha Fontes de dados no painel esquerdo.
2. Escolha a fonte que foi criada como parte do processo de criação do ambiente.
3. Escolha Executar ao lado do menu suspenso Ação e, em seguida, escolha o botão Atualizar. Quando a execução da fonte de dados é concluída, os ativos são adicionados ao DataZone inventário da Amazon.

Etapa 6 - Organize e publique o ativo de dados

Esta seção descreve as etapas de curadoria e publicação do ativo de dados nesse fluxo de trabalho.

1. Depois de concluir a etapa 5 acima, no portal de DataZone dados da Amazon, escolha o `SalesDataPublishingProject` projeto que você criou na etapa anterior, escolha a guia Dados, escolha Dados de inventário no painel esquerdo e localize a `mkt_sls_table` tabela.
2. Abra a página de detalhes do `mkt_sls_table` ativo para ver os nomes comerciais gerados automaticamente. Escolha o ícone Metadados gerados automaticamente para visualizar os nomes gerados automaticamente para ativos e colunas. Você pode aceitar ou rejeitar cada nome individualmente ou escolher Aceitar tudo para aplicar os nomes gerados. Opcionalmente, você também pode adicionar o formulário de metadados disponível ao seu ativo e selecionar termos do glossário para classificar seus dados.
3. Escolha Publicar ativo para publicar o `mkt_sls_table` ativo.

Etapa 7 - Crie o projeto para análise de dados

Esta seção descreve as etapas da criação do projeto para análise de dados. Esse é o início das etapas do consumidor de dados desse fluxo de trabalho.

1. Depois de concluir a etapa 6 acima, no portal de DataZone dados da Amazon, escolha Criar projeto no menu suspenso Projeto.
2. Na página Criar projeto, especifique o nome do projeto, por exemplo, para esse fluxo de trabalho MarketingDataAnalysisProject, você pode nomeá-lo, deixar os demais campos inalterados e escolher Criar.

Etapa 8 - Crie um ambiente para análise de dados

Esta seção descreve as etapas da criação de um ambiente para análise de dados.

1. Depois de concluir a etapa 7 acima, no portal de DataZone dados da Amazon, escolha o `MarketingDataAnalysisProject` projeto, escolha a guia Ambientes e escolha Criar ambiente.
2. Na página Criar ambiente, especifique o seguinte e escolha Criar ambiente.

   - Nome - especifique o nome do ambiente. Para este passo a passo, você pode ligar para ele. `Default data lake environment`
   - Descrição - especifique uma descrição para o ambiente.
   - Perfil do ambiente - escolha o perfil do DataLakeProfileambiente incorporado.
   - Para este passo a passo, mantenha o resto dos campos inalterados.

Etapa 9 - Pesquise o catálogo de dados e assine os dados

Esta seção descreve as etapas de pesquisa no catálogo de dados e assinatura de dados.

1. Depois de concluir a etapa 8 acima, no portal de DataZone dados da Amazon, escolha o DataZone ícone da Amazon e, no campo Amazon DataZone Search, pesquise ativos de dados usando palavras-chave (por exemplo, 'catálogo' ou 'vendas') na barra de pesquisa do portal de dados.

   Se necessário, aplique filtros ou classificação e, depois de localizar o ativo de dados de vendas do produto, você poderá escolhê-lo para abrir a página de detalhes do ativo.

2. Na página de detalhes do ativo Catalog Sales Data, escolha Inscrever-se.
3. Na caixa de diálogo Inscrever-se, escolha seu projeto de MarketingDataAnalysisProjectconsumidor no menu suspenso, especifique o motivo da solicitação de assinatura e escolha Inscrever-se.

Etapa 10 - Aprovar a solicitação de assinatura

Esta seção descreve as etapas de aprovação da solicitação de assinatura.

1. Depois de concluir a etapa 9 acima, no portal de DataZone dados da Amazon, escolha o SalesDataPublishingProjectprojeto com o qual você publicou seu ativo.
2. Escolha a guia Dados, depois Dados publicados e escolha Solicitações recebidas.
3. Agora você pode ver a linha da nova solicitação que precisa de aprovação. Escolha Exibir solicitação. Forneça um motivo para a aprovação e escolha Aprovar.

Etapa 11 - Crie uma consulta e analise dados no Amazon Athena

Agora que você publicou com sucesso um ativo no DataZone catálogo da Amazon e se inscreveu nele, você pode analisá-lo.

1. No portal de DataZone dados da Amazon, escolha seu projeto de MarketingDataAnalysisProjectconsumidor e, no painel direito, em Ferramentas de análise, escolha o link de dados do Query com o Amazon Athena. Isso abre o editor de consultas do Amazon Athena usando as credenciais do seu projeto para autenticação. Escolha o ambiente do MarketingDataAnalysisProjectconsumidor na lista suspensa Amazon DataZone Environment no editor de consultas e, em seguida, escolha o do seu projeto na lista suspensa `<environment_name>%sub_db` do banco de dados.
2. Agora você pode executar consultas na tabela inscrita. Você pode escolher a tabela em Tabelas e Exibições e, em seguida, escolher Visualizar para que a instrução de seleção apareça na tela do editor. Execute a consulta para ver os resultados.

Amazon DataZone quickstart com dados do Amazon Redshift

Tópicos

- Etapa 2 - Crie o projeto de publicação
- Etapa 3 - Crie o ambiente
- Etapa 4 - Produzir dados para publicação
- Etapa 5 - Colete metadados do Amazon Redshift
- Etapa 6 - Organize e publique o ativo de dados
- Etapa 7 - Crie o projeto para análise de dados
- Etapa 8 - Crie um ambiente para análise de dados
- Etapa 9 - Pesquise o catálogo de dados e assine os dados
- Etapa 10 - Aprovar a solicitação de assinatura
- Etapa 11 - Crie uma consulta e analise dados no Amazon Redshift

Etapa 1 - Crie o DataZone domínio e o portal de dados da Amazon

Conclua o procedimento a seguir para criar um DataZone domínio da Amazon. Para obter mais informações sobre os DataZone domínios da Amazon, consulte DataZone Terminologia e conceitos da Amazon.

1. Navegue até o DataZone console da Amazon em https://console.aws.amazon.com/datazone, faça login e escolha Criar domínio.

   > **Note**
   >
   > Se você quiser usar um DataZone domínio existente da Amazon para esse fluxo de trabalho, escolha Exibir domínios, escolha o domínio que deseja usar e prossiga para a Etapa 2 da criação de um projeto de publicação.

2. Na página Criar domínio, forneça valores para os seguintes campos:

   - Nome - especifique um nome para seu domínio. Para fins desse fluxo de trabalho, você pode chamar esse domínio`Marketing`.
   - Descrição - especifique uma descrição de domínio opcional.
   - Criptografia de dados - seus dados são criptografados por padrão com uma chave que AWS possui e gerencia para você. Para este passo a passo, você pode deixar as configurações padrão de criptografia de dados.

Para obter mais informações sobre o uso de chaves gerenciadas pelo cliente, consulteCriptografia de dados em repouso para a Amazon DataZone. Se você usar sua própria chave KMS para criptografia de dados, deverá incluir a seguinte declaração em seu padrãoAmazonDataZoneDomainExecutionRole.

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

- Acesso ao serviço - escolha a opção Usar uma função de serviço personalizada e, em seguida, escolha a no AmazonDataZoneDomainExecutionRolemenu suspenso.
- Em Configuração rápida, escolha Configurar esta conta para consumo e publicação de dados. Essa opção habilita os DataZone blueprints integrados do Data Lake e do Data Warehouse da Amazon e configura as permissões e os recursos necessários para concluir o restante das etapas desse fluxo de trabalho. Para obter mais informações sobre os DataZone projetos da Amazon, consulte DataZone Terminologia e conceitos da Amazon.
- Mantenha os campos restantes em Detalhes de permissões e Tags inalterados e escolha Criar domínio.

3. Depois que o domínio for criado com sucesso, escolha esse domínio e, na página de resumo do domínio, anote o URL do portal de dados desse domínio. Você pode usar essa URL para acessar seu portal de DataZone dados da Amazon para concluir o restante das etapas desse fluxo de trabalho.

> **Note**
>
> Na versão atual da Amazon DataZone, depois que o domínio é criado, a URL gerada para o portal de dados não pode ser modificada.

A criação do domínio pode levar alguns minutos para ser concluída. Aguarde até que o domínio tenha um status de Disponível antes de prosseguir para a próxima etapa.

Etapa 2 - Crie o projeto de publicação

A seção a seguir descreve as etapas da criação do projeto de publicação nesse fluxo de trabalho.

1. Depois de concluir a Etapa 1, navegue até o portal de DataZone dados da Amazon usando a URL do portal de dados e faça login usando suas credenciais de login único (SSO) ou AWS IAM.
2. Escolha Criar projeto, especifique o nome do projeto, por exemplo, para esse fluxo de trabalho SalesDataPublishingProject, você pode nomeá-lo, deixar o resto dos campos inalterados e escolher Criar.

Etapa 3 - Crie o ambiente

A seção a seguir descreve as etapas da criação de um ambiente nesse fluxo de trabalho.

1. Depois de concluir a Etapa 2, no portal de DataZone dados da Amazon, escolha o `SalesDataPublishingProject` projeto que você criou na etapa anterior, escolha a guia Ambientes e escolha Criar ambiente.
2. Na página Criar ambiente, especifique o seguinte e escolha Criar ambiente.
   - Nome - especifique o nome do ambiente. Para este passo a passo, você pode ligar para ele. `Default data warehouse environment`
   - Descrição - especifique uma descrição para o ambiente.
   - Perfil do ambiente - escolha o perfil do DataWarehouseProfileambiente.
   - Forneça o nome do seu cluster do Amazon Redshift, o nome do banco de dados e o ARN secreto para o cluster do Amazon Redshift em que seus dados estão armazenados.

> **Note**
>
> Certifique-se de que seu segredo no AWS Secrets Manager inclua as seguintes tags (chave/valor):
>
> - Para o cluster Amazon Redshift - datazone.rs.cluster: <cluster_name:database name>
>
> Para o grupo de trabalho sem servidor do Amazon Redshift - datazone.rs.workgroup: <workgroup_name:database_name>
> - AmazonDataZoneProject: <projectID>
> - AmazonDataZoneDomain: <domainID>
>
> Para obter mais informações, consulte Armazenando credenciais do banco de dados no AWS Secrets Manager.
> O usuário do banco de dados que você fornece no AWS Secrets Manager deve ter permissões de superusuário.

Etapa 4 - Produzir dados para publicação

A seção a seguir descreve as etapas de produção de dados para publicação nesse fluxo de trabalho.

1. Depois de concluir a Etapa 3, no portal de DataZone dados da Amazon, escolha o `SalesDataPublishingProject` projeto e, no painel direito, em Ferramentas de análise, escolha Amazon Redshift. Isso abre o editor de consultas do Amazon Redshift usando as credenciais do seu projeto para autenticação.
2. Para este passo a passo, você está usando o script de consulta Create Table as Select (CTAS) para criar uma nova tabela que você deseja publicar na Amazon. DataZone No seu editor de consultas, execute esse script CTAS para criar uma `mkt_sls_table` tabela que você possa publicar e disponibilizar para pesquisa e assinatura.

```
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
```

Certifique-se de que a tabela mkt_sls_table tenha sido criada com sucesso. Agora você tem um ativo de dados que pode ser publicado no DataZone catálogo da Amazon.

Etapa 5 - Colete metadados do Amazon Redshift

A seção a seguir descreve as etapas da coleta de metadados do Amazon Redshift.

1. Depois de concluir a Etapa 4, no portal de DataZone dados da Amazon, escolha o `SalesDataPublishingProject` projeto, escolha a guia Dados e, em seguida, escolha Fontes de dados.
2. Escolha a fonte que foi criada como parte do processo de criação do ambiente.
3. Escolha Executar ao lado do menu suspenso Ação e, em seguida, escolha o botão Atualizar. Quando a execução da fonte de dados é concluída, os ativos são adicionados ao DataZone inventário da Amazon.

Etapa 6 - Organize e publique o ativo de dados

A seção a seguir descreve as etapas de curadoria e publicação do ativo de dados nesse fluxo de trabalho.

1. Depois de concluir a etapa 5, no portal de DataZone dados da Amazon, escolha o `SalesDataPublishingProject` projeto, escolha a guia Dados, escolha Dados de inventário e localize a `mkt_sls_table` tabela.
2. Abra a página de detalhes do `mkt_sls_table` ativo para ver os nomes comerciais gerados automaticamente. Escolha o ícone Metadados gerados automaticamente para visualizar os nomes gerados automaticamente para ativos e colunas. Você pode aceitar ou rejeitar cada nome individualmente ou escolher Aceitar tudo para aplicar os nomes gerados. Opcionalmente,

você também pode adicionar o formulário de metadados disponível ao seu ativo e selecionar termos do glossário para classificar seus dados.

3. Escolha Publicar para publicar o `mkt_sls_table` ativo.

Etapa 7 - Crie o projeto para análise de dados

A seção a seguir descreve as etapas da criação do projeto para análise de dados nesse fluxo de trabalho.

1. Depois de concluir a Etapa 6, no portal de DataZone dados da Amazon, escolha Criar projeto.
2. Na página Criar projeto, especifique o nome do projeto, por exemplo, para esse fluxo de trabalho MarketingDataAnalysisProject, você pode nomeá-lo, deixar os demais campos inalterados e escolher Criar.

Etapa 8 - Crie um ambiente para análise de dados

A seção a seguir descreve as etapas da criação de um ambiente para análise de dados nesse fluxo de trabalho.

1. Depois de concluir a Etapa 7, no portal de DataZone dados da Amazon, escolha o `MarketingDataAnalysisProject` projeto que você criou na etapa anterior, escolha a guia Ambientes e escolha Adicionar ambiente.
2. Na página Criar ambiente, especifique o seguinte e escolha Criar ambiente.

   - Nome - especifique o nome do ambiente. Para este passo a passo, você pode ligar para ele. `Default data warehouse environment`
   - Descrição - especifique uma descrição para o ambiente.
   - Perfil do ambiente - escolha o perfil do DataWarehouseProfileambiente.
   - Forneça o nome do seu cluster do Amazon Redshift, o nome do banco de dados e o ARN secreto para o cluster do Amazon Redshift em que seus dados estão armazenados.

   > **Note**
   >
   > Certifique-se de que seu segredo no AWS Secrets Manager inclua as seguintes tags (chave/valor):

- Para o cluster Amazon Redshift - datazone.rs.cluster: <cluster_name:database name>

  Para o grupo de trabalho sem servidor do Amazon Redshift - datazone.rs.workgroup: <workgroup_name:database_name>
- AmazonDataZoneProject: <projectID>
- AmazonDataZoneDomain: <domainID>

Para obter mais informações, consulte Armazenando credenciais do banco de dados no AWS Secrets Manager.

O usuário do banco de dados que você fornece no AWS Secrets Manager deve ter permissões de superusuário.

- Para este passo a passo, mantenha o resto dos campos inalterados.

Etapa 9 - Pesquise o catálogo de dados e assine os dados

A seção a seguir descreve as etapas de pesquisa no catálogo de dados e assinatura dos dados.

1. Depois de concluir a Etapa 8, no portal de DataZone dados da Amazon, pesquise ativos de dados usando palavras-chave (por exemplo, 'catálogo' ou 'vendas') na barra de pesquisa do portal de dados.

   Se necessário, aplique filtros ou classificação e, depois de localizar o ativo de dados de vendas do produto, você poderá escolhê-lo para abrir a página de detalhes do ativo.
2. Na página de detalhes do ativo de dados de vendas de produtos, escolha Inscrever-se.
3. Na caixa de diálogo, escolha seu projeto de consumidor no menu suspenso, forneça o motivo da solicitação de acesso e escolha Inscrever-se.

Etapa 10 - Aprovar a solicitação de assinatura

A seção a seguir descreve as etapas de aprovação da solicitação de assinatura nesse fluxo de trabalho.

1. Depois de concluir a Etapa 9, no portal de DataZone dados da Amazon, escolha o SalesDataPublishingProjectprojeto com o qual você publicou seu ativo.
2. Escolha a guia Dados, depois Dados publicados e, em seguida, Solicitações recebidas.

3. Escolha o link de exibição da solicitação e, em seguida, escolha Aprovar.

Etapa 11 - Crie uma consulta e analise dados no Amazon Redshift

Agora que você publicou com sucesso um ativo no DataZone catálogo da Amazon e se inscreveu nele, você pode analisá-lo.

1. No portal de DataZone dados da Amazon, no painel direito, clique no link Amazon Redshift. Isso abre o editor de consultas do Amazon Redshift usando a credencial do projeto para autenticação.
2. Agora você pode executar uma consulta (instrução de seleção) na tabela assinada. Você pode clicar na tabela (three-vertical-dots opção) e escolher a visualização para que a instrução de seleção apareça na tela do editor. Execute a consulta para ver os resultados.

DataZone Início rápido da Amazon com exemplos de scripts

A seção a seguir descreve exemplos de scripts que invocam várias DataZone APIs da Amazon que você pode usar para concluir as seguintes tarefas:

Tópicos

Crie um DataZone domínio e um portal de dados da Amazon

Você pode usar o seguinte exemplo de script para criar um DataZone domínio da Amazon. Para obter mais informações sobre os DataZone domínios da Amazon, consulte DataZone Terminologia e conceitos da 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",
    )
```

Crie um projeto de publicação

Você pode usar o seguinte exemplo de script para criar um projeto de publicação na Amazon DataZone.

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

Crie um perfil de ambiente

Você pode usar os seguintes exemplos de scripts para criar um perfil de ambiente na Amazon DataZone.

Esse exemplo de carga útil é usado quando a `CreateEnvironmentProfile` API é invocada:

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

Esse exemplo de script invoca a `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
```

Este é o exemplo de carga útil de saída quando a `CreateEnvironmentProfile` API é invocada:

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

```
}
```

Criar um ambiente

Você pode usar o seguinte exemplo de script para criar um ambiente na 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
```

Colete metadados do AWS Glue

Você pode usar esse script de amostra para coletar metadados do AWS Glue. Esse script é executado em uma programação padrão. Você pode recuperar os parâmetros do script de amostra e torná-los globais. Obtenha o ID do projeto, do ambiente e do domínio usando funções padrão. A fonte de dados AWS Glue é criada e executada em um horário padrão, que pode ser atualizado na seção cron do script.

```
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"
    }
}
```

Organize e publique um ativo de dados

Você pode usar os seguintes exemplos de scripts para organizar e publicar ativos de dados na Amazon DataZone.

Você pode usar o script a seguir para criar tipos de formulários personalizados:

```
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"
    )
```

Você pode usar o seguinte exemplo de script para criar tipos de ativos personalizados:

```
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,
    )
```

Você pode usar o seguinte exemplo de script para criar ativos personalizados:

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

Você pode usar o seguinte exemplo de script para criar um glossário:

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

Você pode usar o seguinte exemplo de script para criar um termo do glossário:

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

Você pode usar o seguinte exemplo de script para criar um ativo usando um tipo de ativo definido pelo sistema:

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

Você pode usar o seguinte exemplo de script para criar uma revisão do ativo e anexar um termo do glossário:

```
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:>"]
    )
```

Você pode usar o seguinte exemplo de script para publicar um ativo:

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

Pesquise o catálogo de dados e assine os dados

Você pode usar os seguintes exemplos de scripts para pesquisar o catálogo de dados e assinar os dados:

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

Você pode usar o seguinte exemplo de script para obter o ID do anúncio do ativo:

```
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']
```

Você pode usar os seguintes exemplos de scripts para criar uma solicitação de assinatura usando o ID do anúncio:

```
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."
    )
```

Usando o exemplo `create_subscription_response` acima, obtenha o e `subscription_request_id`, em seguida, aceite/aprove a assinatura usando o seguinte exemplo de script:

```
subscription_request_id = create_subscription_response["id"]

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

Outros scripts de amostra úteis

Você pode usar os seguintes exemplos de scripts para concluir várias tarefas enquanto trabalha com seus dados na Amazon DataZone.

Use o seguinte exemplo de script para listar os DataZone domínios existentes da Amazon:

```
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
```

Use o seguinte exemplo de script para listar DataZone projetos existentes da Amazon:

```
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
```

Use o seguinte exemplo de script para listar os formulários de DataZone metadados existentes da Amazon:

```
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
```

Gerenciando DataZone domínios da Amazon e acesso de usuários

Tópicos

Crie domínios

> **Note**
>
> Se você estiver usando a Amazon DataZone com o AWS Identity Center para fornecer acesso a usuários e grupos de SSO, atualmente seu DataZone domínio da Amazon deve estar na mesma AWS região da sua instância do AWS Identity Center.

Amazon DataZone, um domínio, é uma entidade organizadora para conectar seus ativos, usuários e seus projetos. Para ter mais informações, consulte DataZone Terminologia e conceitos da Amazon.

Para criar um DataZone domínio da Amazon, você deve assumir uma função do IAM na conta com permissões administrativas. Configure as permissões do IAM necessárias para usar o console DataZone de gerenciamento da Amazonpara obter as permissões mínimas necessárias para criar um domínio.

A Amazon precisa de funções adicionais do IAM DataZone para realizar ações em nome dos usuários do domínio com uma configuração padrão. Você pode criar essas funções do IAM com antecedência ou fazer com que a Amazon as DataZone crie para você. Se você quiser que DataZone a Amazon crie essas funções do IAM para você durante o processo de criação do domínio, então, para a criação do domínio, você deve assumir

uma função do IAM com permissões de criação de função. Consulte Crie uma política personalizada para permissões do IAM para permitir a criação simplificada de funções do console de DataZone serviços da Amazon . Dependendo das suas opções de criação de domínio, a Amazon DataZone criará até quatro novas funções do IAM para você: AmazonDataZoneDomainExecutionRoleAmazonDataZoneGlueManageAccessRoleAmazonDataZoneRedsh AmazonDataZoneProvisioningRolee.

Conclua o procedimento a seguir para criar um DataZone domínio da Amazon.

1. Navegue até o DataZone console da Amazon em https://console.aws.amazon.com/datazone e use o seletor de região na barra de navegação superior para escolher a AWS região apropriada.
2. Escolha Criar domínio e forneça valores para os seguintes campos:

   - Nome - especifique um nome amigável para o domínio. Depois que o domínio é criado, esse nome não pode ser alterado.
   - Descrição - (opcional) especifique uma descrição do domínio.
   - Criptografia de dados - seu DataZone domínio, metadados e dados de relatórios da Amazon são criptografados pelo AWS Key Management Service (KMS) usando uma chave específica para sua Amazon. DataZone Use esse campo para especificar se você deseja usar uma chave AWS própria ou escolher uma chave AWS KMS diferente.

     Para obter mais informações sobre o uso de chaves gerenciadas pelo cliente, consulteCriptografia de dados em repouso para a Amazon DataZone. Se você usar sua própria chave KMS para criptografia de dados, deverá incluir a seguinte declaração em seu padrãoAmazonDataZoneDomainExecutionRole.

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

```
      ]
    }
  ]
}
```

- Acesso ao serviço - escolha se deseja que a Amazon DataZone crie e use um novo DomainExecutionRolepara você ou escolha uma função existente do IAM.
- Configuração rápida - (opcional) marque esta caixa para começar mais rápido fazendo com que a Amazon DataZone configure sua conta para consumo e publicação de dados. A Amazon DataZone criará três funções do IAM para provisionar, ingerir e gerenciar o acesso aos recursos do AWS Glue e do Amazon Redshift, criar um novo bucket do Amazon S3, criar um DataZone projeto administrativo da Amazon e criar perfis de ambiente para os blueprints padrão do data lake e do data warehouse.
- Tags - (opcional) especifique AWS tags (pares de chave e valor) para o domínio.
- Depois que o domínio for criado com sucesso, seu navegador deverá ser atualizado para exibir a página de detalhes do seu novo DataZone domínio da Amazon.

Editar domínios

Na Amazon DataZone, um domínio é uma entidade organizadora para conectar seus ativos, usuários e seus projetos. Para ter mais informações, consulte DataZone Terminologia e conceitos da Amazon.

Depois de criar um DataZone domínio da Amazon, você pode posteriormente editar o domínio para: alterar a descrição, ativar o IAM Identity Center e adicionar, editar ou remover chaves de tag e seus valores. Para editar um DataZone domínio da Amazon, você deve assumir uma função do IAM na conta com permissões administrativas. Configure as permissões do IAM necessárias para usar o console DataZone de gerenciamento da Amazonpara obter as permissões mínimas necessárias para editar um domínio.

Para editar um domínio, conclua as seguintes etapas:

1. Faça login no AWS Management Console e abra o DataZone console da Amazon em https://console.aws.amazon.com/datazone.
2. Escolha Exibir domínios e escolha o nome do domínio na lista. O nome é um hiperlink.
3. Na página de detalhes do domínio, escolha Editar.

4. • Edite a descrição.
   • Defina as configurações do IAM Identity Center. Saiba mais sobre essas configurações emConfigurando o AWS IAM Identity Center para a Amazon DataZone.
   • Adicione, edite ou remova as chaves de tag e seus valores.
5. Depois de fazer suas edições, escolha Atualizar domínio.

Excluir domínios

Na Amazon DataZone, um domínio é uma entidade organizadora para conectar seus ativos, usuários e seus projetos. Para ter mais informações, consulte DataZone Terminologia e conceitos da Amazon.

O ato de excluir um domínio é definitivo. A exclusão remove irrevogavelmente todas as DataZone entidades da Amazon, incluindo fontes de dados, projetos, ambientes, ativos, glossários e formulários de metadados. A exclusão não exclui DataZone AWS recursos não pertencentes à Amazon que a Amazon DataZone possa ter ajudado você a criar, como funções do IAM, buckets do S3, bancos de dados AWS Glue e concessões de assinatura via LakeFormation Redshift ou Redshift. Se você não precisar mais desses recursos, exclua-os no respectivo AWS serviço.

Para evitar que alguém exclua um domínio de forma maliciosa, a exclusão de um domínio requer permissões administrativas do IAM para a Amazon DataZone, que você pode configurar com o IAM. Para evitar que alguém exclua um domínio acidentalmente, a exclusão de um domínio requer uma palavra de confirmação (no console da Amazon DataZone).

Para excluir um domínio, conclua as seguintes etapas:

1. Faça login no AWS Management Console e abra o DataZone console da Amazon em https://console.aws.amazon.com/datazone.
2. Escolha Exibir domínios e escolha o nome do domínio na lista. O nome é um hiperlink.
3. Escolha Excluir e revise os avisos informativos.
4. Digite o texto solicitado para confirmar que você entendeu esses avisos. Escolha Excluir.

> **Important**
>
> Excluir seu domínio é uma ação irrevogável que não pode ser desfeita por você ou pela. AWS

> **Note**
>
> Quando você ou os usuários do seu domínio criam um ambiente em um projeto, a Amazon DataZone cria AWS recursos em seu domínio ou contas associadas para fornecer funcionalidade a você e aos usuários do seu domínio. Abaixo está a lista de AWS recursos que a Amazon DataZone pode criar para projetos em seu domínio, junto com o nome padrão. A exclusão de um domínio não exclui nenhum desses AWS recursos em suas AWS contas.
>
> - <environmentId>Funções do IAM: datazone_usr_.
> - <environmentName>Bancos de dados Glue: (1) <environmentName>_pub_db-*, (2) _sub_db-*. Se já existisse um banco de dados com esse nome, a Amazon DataZone adicionará o ID do ambiente.
> - <environmentName>Grupos de trabalho do Athena: -*. Se já existisse um grupo de trabalho com esse nome, a Amazon DataZone adicionará o ID do ambiente.
> - CloudWatch grupo de registros: datazone_ <environmentId>

Habilite o IAM Identity Center para Amazon DataZone

> **Note**
>
> Para concluir esse procedimento, você deve ter o AWS IAM Identity Center habilitado na mesma AWS região do seu DataZone domínio da Amazon.

Você pode fornecer aos usuários e grupos do SSO acesso ao seu portal de DataZone dados da Amazon usando o AWS IAM Identity Center. Depois de concluirConfigurando o AWS IAM Identity Center para a Amazon DataZone, você pode permitir que seus usuários e grupos de SSO acessem seu portal de dados de DataZone domínio da Amazon.

Para habilitar o AWS IAM Identity Center para uso com seu DataZone domínio da Amazon, você deve assumir uma função do IAM na conta com permissões administrativas. Configure as permissões do IAM necessárias para usar o console DataZone de gerenciamento da Amazone Crie uma política personalizada para permissões do IAM para permitir a criação simplificada de funções do console de DataZone serviços da Amazon para obter as permissões mínimas necessárias para habilitar o IAM Identity Center para uso com a Amazon DataZone.

Conclua o procedimento a seguir para ativar o AWS IAM Identity Center para a Amazon DataZone.

1. Faça login no AWS Management Console e abra o DataZone console em https://console.aws.amazon.com/datazone.
2. Selecione Exibir domínios e escolha o nome do domínio na lista. O nome é um hiperlink.
3. Na página de detalhes do domínio, escolha Editar.
   - Marque a caixa de seleção Habilitar usuários no IAM Identity Center.
   - Escolha entre os dois modos de atribuição de usuário. Depois que seu domínio for atualizado com sua seleção, ele não poderá ser alterado posteriormente.
     - Com a atribuição implícita de usuários, qualquer usuário adicionado ao seu diretório do IAM Identity Center pode acessar seu domínio da Amazon DataZone .
     - Com a atribuição explícita de usuários, você adicionará usuários ou grupos específicos do seu diretório do IAM Identity Center para fornecer acesso ao seu domínio da Amazon DataZone . Você adicionará e removerá esses usuários e grupos posteriormente no Amazon DataZone Console.
4. Quando estiver satisfeito com sua seleção, escolha Atualizar domínio.

Desative o IAM Identity Center para Amazon DataZone

A desativação AWS do IAM Identity Center para um DataZone domínio da Amazon removerá o acesso de todos os usuários do SSO.

> **Note**
>
> A desativação do IAM Identity Center não interromperá a cobrança dos usuários de SSO. Para interromper a cobrança dos usuários do SSO, você deve desativá-los em seu domínio. O faturamento continua até o final do mês em que o usuário é desativado. Para desativar usuários, consulteGerencie usuários no DataZone console da Amazon.

Você pode fornecer aos usuários e grupos do SSO acesso ao seu portal de DataZone dados da Amazon usando o AWS IAM Identity Center. Se você ativou o AWS IAM Identity Center para a Amazon DataZone, poderá posteriormente desativar o acesso de todos os usuários.

Para desativar o AWS IAM Identity Center para uso com seu DataZone domínio da Amazon, você deve assumir uma função do IAM na conta com permissões administrativas. Configure as

permissões do IAM necessárias para usar o console DataZone de gerenciamento da Amazone Crie uma política personalizada para permissões do IAM para permitir a criação simplificada de funções do console de DataZone serviços da Amazon para obter as permissões mínimas necessárias para desabilitar o uso do IAM Identity Center com a Amazon DataZone.

Conclua o procedimento a seguir para desativar o AWS IAM Identity Center para Amazon DataZone.

1. Faça login no AWS Management Console e abra o DataZone console em https://console.aws.amazon.com/datazone.
2. Selecione Exibir domínios e escolha o nome do domínio na lista. O nome é um hiperlink.
3. <regionName><accountId><domainName>Copie o Amazon Resource Name (ARN) do seu domínio, que começa com arn:aws:datazone: ::domain/.
4. Abra o console do IAM Identity Center em https://console.aws.amazon.com/singlesignon/.
5. Selecione Aplicações.
6. Escolha o domínio para o qual você deseja desativar o AWS IAM Identity Center, o que, como resultado, removerá o acesso ao portal de dados do domínio para todos os usuários de SSO. Você pode usar o menu Filtro e a caixa de pesquisa para filtrar a lista de aplicativos.
7. No menu Ações, escolha Desativar.
8. Os usuários do SSO perderão o acesso ao DataZone domínio da Amazon.
9. Para reativar o AWS IAM Identity Center para o DataZone domínio da Amazon, escolha o domínio para o qual você deseja reativar o AWS IAM Identity Center e, no menu Ações, escolha Ativar.

Gerencie usuários no DataZone console da Amazon

Seus usuários podem acessar o portal de DataZone dados da Amazon usando suas AWS credenciais ou credenciais de login único (SSO). Para gerenciar usuários no DataZone console da Amazon para um DataZone domínio da Amazon, você deve assumir uma função do IAM na conta com permissões administrativas. Configure as permissões do IAM necessárias para usar o console DataZone de gerenciamento da Amazonpara obter as permissões mínimas necessárias para gerenciar usuários no DataZone console da Amazon.

Tópicos

- Gerencie funções e usuários do IAM
- Gerenciar usuários de SSO

- Gerenciar grupos de SSO

Gerencie funções e usuários do IAM

As funções e os usuários do IAM são criados usando AWS Identity and Access Management (IAM) e obtêm acesso aos seus domínios da DataZone Amazon por meio de permissões anexadas a eles por meio de políticas. Para ter mais informações, consulte Configure as permissões do IAM necessárias para usar o portal de DataZone dados da Amazon. Você pode ver a lista de funções e usuários do IAM que ativaram sua assinatura de DataZone domínio da Amazon, desativaram seu acesso e ativaram seu acesso, caso tenham sido desativados anteriormente.

1. Faça login no AWS Management Console e abra o DataZone console em https://console.aws.amazon.com/datazone.
2. Selecione Exibir domínios e escolha o nome do domínio na lista. O nome é um hiperlink.
3. Na página de detalhes do domínio, escolha Gerenciamento de usuários.
4. Para o tipo de usuário, selecione Usuários do IAM para ver a lista atual de usuários e funções do IAM ativados e desativados.
   - A coluna Nome mostra o arn do usuário ou função do IAM.
   - A coluna Status mostra o status atual do usuário ou da função do IAM no domínio.
     - Ativado significa que o usuário ou função do IAM chamou uma API, emitiu um comando (via interface de linha de comando) ou acessou o DataZone portal da Amazon para seu domínio, e você está sendo cobrado pela assinatura do usuário.
     - Desativado significa que o usuário ou função do IAM tem seu acesso bloqueado ao seu DataZone domínio da Amazon.
5. Para desativar um usuário ou função do IAM que está atualmente ativado, marque a caixa ao lado do usuário e selecione Desativar no menu Ações. O usuário perderá o acesso ao DataZone domínio da Amazon. A cobrança do usuário terminará no final do mês civil atual.
6. Para ativar um usuário ou função do IAM que está atualmente desativado, marque a caixa ao lado do usuário e selecione Ativar no menu Ações. O usuário obterá acesso ao DataZone domínio da Amazon se o usuário ou a função do IAM tiver as permissões apropriadas. A cobrança para o usuário começará novamente.

Gerenciar usuários de SSO

Os usuários de SSO são criados ou sincronizados com seu provedor de identidade no AWS IAM Identity Center. Para obter mais informações, consulte Configurando o AWS IAM Identity Center para a Amazon DataZone e Habilite o IAM Identity Center para Amazon DataZone para habilitar e configurar o AWS IAM Identity Center para Amazon DataZone. Você pode ver a lista de usuários de SSO atribuídos ao domínio, adicionar usuários de SSO e remover usuários de SSO.

1. Faça login no AWS Management Console e abra o DataZone console em https://console.aws.amazon.com/datazone.
2. Selecione Exibir domínios e escolha o nome do domínio na lista. O nome é um hiperlink.
3. Na página de detalhes do domínio, role para baixo e escolha Gerenciamento de usuários.
4. Para tipo de usuário, selecione Usuários de SSO para ver a lista atual de usuários de SSO.
   - A coluna Nome mostra o nome do usuário do SSO.
   - A coluna Status mostra o status atual do usuário SSO no domínio.
     - Atribuído significa que o usuário do SSO foi explicitamente atribuído ao domínio. Como resultado, o usuário tem acesso à Amazon DataZone. Esse status só é usado quando o modo de provedor de identidade do seu domínio está definido como atribuição explícita.
     - Ativado significa que o usuário do SSO acessou o DataZone portal da Amazon para o domínio e você está sendo cobrado pela assinatura do usuário. A ativação acontece automaticamente.
     - Desativado significa que o acesso do usuário do SSO está bloqueado ao portal de dados do domínio. A cobrança do usuário terminou no final do mês em que o acesso foi desativado.
     - Removido significa que o usuário do SSO foi previamente atribuído ao domínio, mas removido antes mesmo de ser acessado.
5. Adicione usuários de SSO escolhendo Adicionar e Adicionar usuários. Essa opção não estará disponível se o domínio estiver configurado para atribuição implícita de usuários, o que significa que todos os usuários no grupo de identidades têm acesso ao domínio da Amazon. DataZone
   - Na página Adicionar usuários, pesquise os aliases dos usuários que você deseja adicionar. Uma lista aparecerá abaixo da caixa de pesquisa com possíveis correspondências.
   - Escolha o usuário que você deseja adicionar. Seu alias aparecerá como um chip abaixo da caixa de pesquisa.

- Quando estiver satisfeito com a lista de usuários que deseja adicionar, escolha Adicionar usuário (s).
- Os usuários são atribuídos ao DataZone domínio da Amazon com o status Atribuído.
- Quando o usuário acessou pela primeira vez o portal de dados do domínio, o status mudará automaticamente para Ativado e você começará a ser cobrado pela assinatura do usuário.

6. Remova um usuário de SSO atribuído selecionando o usuário e escolhendo Desativar no menu Ações. Como resultado, o usuário perderá o acesso ao DataZone domínio da Amazon. O status do usuário será exibido como Removido. Essa opção não estará disponível se o domínio estiver definido para atribuição implícita de usuário.
7. Desative um usuário de SSO ativado selecionando o usuário e escolhendo Desativar no menu Ações. Como resultado, o acesso do usuário ao DataZone domínio da Amazon será perdido e bloqueado. A cobrança da assinatura do usuário continuará até o final do mês. O status do usuário será exibido como Desativado.
8. Ative um usuário de SSO desativado selecionando o usuário e escolhendo Ativar no menu Ações. Como resultado, o usuário recuperará o acesso ao DataZone domínio da Amazon. O faturamento começará imediatamente. O do usuário será exibido como Ativado.

Gerenciar grupos de SSO

Os grupos de SSO são criados ou sincronizados com seu provedor de identidade no AWS IAM Identity Center. Para obter mais informações, consulte Configurando o AWS IAM Identity Center para a Amazon DataZone e Habilite o IAM Identity Center para Amazon DataZone para habilitar e configurar o AWS IAM Identity Center para Amazon DataZone. Você pode ver a lista de grupos de SSO atribuídos ao domínio, adicionar grupos de SSO e remover grupos de SSO.

1. Faça login no AWS Management Console e abra o DataZone console em https://console.aws.amazon.com/datazone.
2. Selecione Exibir domínios e escolha o nome do domínio na lista. O nome é um hiperlink.
3. Na página de detalhes do domínio, role para baixo e escolha Gerenciamento de usuários.
4. Para o tipo de usuário, selecione Grupos de SSO para ver a lista atual de grupos de SSO.
   - A coluna Nome mostra o nome do grupo SSO.
   - A coluna Status mostra o status atual do grupo SSO no domínio.

- Atribuído significa que o grupo SSO foi explicitamente atribuído ao domínio. Como resultado, todos os usuários do grupo têm acesso ao portal de dados do domínio (a menos que o usuário esteja desativado).
- Não atribuído significa que o grupo SSO foi removido do domínio. Os usuários do grupo não têm acesso ao portal de dados do domínio por meio de sua associação a esse grupo.

5. Adicione grupos de SSO escolhendo Adicionar e Adicionar grupos. Essa opção não estará disponível se o domínio estiver configurado para atribuição implícita de usuários, o que significa que todos os usuários no grupo de identidades têm acesso ao DataZone domínio da Amazon, independentemente da associação ao grupo.

   - Na página Adicionar grupos, pesquise os aliases dos grupos que você deseja adicionar. Uma lista aparecerá abaixo da caixa de pesquisa com possíveis correspondências.
   - Escolha o grupo que você deseja adicionar. Seu alias aparecerá como um chip abaixo da caixa de pesquisa.
   - Quando estiver satisfeito com a lista de grupos que você deseja adicionar, escolha Adicionar grupo (s).
   - Os grupos são atribuídos ao DataZone domínio da Amazon com o status Atribuído.
   - Quando um membro do grupo acessa o portal de dados do domínio, o status mudará automaticamente para Ativado e você começará a ser cobrado pela assinatura do usuário.

6. Remova um grupo de SSO atribuído selecionando o grupo e escolhendo Cancelar atribuição no menu Ações. Como resultado, o grupo perderá o acesso ao DataZone domínio da Amazon. O status do grupo será exibido como Não atribuído. Os usuários que obtiveram acesso à Amazon DataZone por meio da associação a esse grupo perderão o acesso. Essa opção não estará disponível se o domínio estiver definido para atribuição implícita de usuário. Para interromper a cobrança de usuários cujo acesso foi removido ao cancelar a atribuição do grupo, você precisará selecionar e desativar manualmente seus perfis de usuário.

Gerenciamento de permissões de usuário no portal de DataZone dados da Amazon

Na versão atual da Amazon DataZone, o mecanismo de autorização padrão permite que todos os usuários autenticados (IAM e SSO) dos DataZone domínios da Amazon criem projetos, criem entidades dentro dos projetos e conduzam pesquisas. Os membros do projeto ainda devem

cumprir as permissões concedidas a eles de acordo com as funções designadas de proprietário ou colaborador do projeto.

Trabalhando com os projetos DataZone integrados da Amazon

Um plano com o qual um ambiente é criado define quais ferramentas e serviços os membros do projeto ao qual o ambiente pertence podem usar ao trabalhar com ativos no DataZone catálogo da Amazon. Na versão atual da Amazon DataZone, existem os seguintes esquemas integrados:

- Projeto do data lake
- Plano de data warehouse
- SageMaker Projeto da Amazon

Tópicos

Habilite esquemas integrados na AWS conta que possui o domínio da Amazon DataZone

Um plano com o qual um ambiente é criado define quais ferramentas e serviços os membros do projeto ao qual o ambiente pertence podem usar ao trabalhar com ativos no DataZone catálogo da Amazon.

Na versão atual da Amazon DataZone, há vários modelos integrados: plano de lago de dados, plano de armazém de dados e modelo da Amazon. SageMaker

- O Data Lake Blueprint contém a definição para lançar e configurar um conjunto de serviços (AWS Glue, AWS Lake Formation, Amazon Athena) para publicar e usar ativos de data lake no catálogo da Amazon. DataZone
- O plano de data warehouse contém a definição para iniciar e configurar um conjunto de serviços (Amazon Redshift) para publicar e usar ativos do Amazon Redshift no catálogo da Amazon. DataZone

- O Amazon SageMaker Blueprint contém a definição para iniciar e configurar um conjunto de serviços (Amazon SageMaker Studio) para publicar e usar SageMaker ativos da Amazon no catálogo da Amazon DataZone .

Para ter mais informações, consulte DataZone Terminologia e conceitos da Amazon.

Ao criar um DataZone domínio da Amazon, você tem a opção de escolher a configuração rápida, que ativa automaticamente o data lake padrão e os esquemas integrados do data warehouse padrão como parte do processo de criação do domínio. A configuração rápida também cria perfis de ambiente padrão e ambientes padrão para você usando esses blueprints integrados.

Se você não escolher a Configuração rápida como parte da criação do seu DataZone domínio da Amazon, você pode usar o procedimento abaixo para ativar os esquemas integrados disponíveis na AWS conta que abriga esse DataZone domínio da Amazon. Você deve habilitar esses blueprints integrados antes de poder usá-los para criar perfis de ambiente e ambientes nesse domínio.

Para habilitar esquemas integrados em um DataZone domínio da Amazon por meio do console DataZone de gerenciamento da Amazon, você deve assumir uma função do IAM na conta com permissões administrativas. Configure as permissões do IAM necessárias para usar o console DataZone de gerenciamento da Amazonpara obter as permissões mínimas.

Habilite esquemas integrados em um domínio da Amazon DataZone

1. Navegue até o DataZone console da Amazon em https://console.aws.amazon.com/datazone e faça login com as credenciais da sua conta.
2. Escolha Exibir domínios e escolha o domínio em que você deseja habilitar um ou mais blueprints integrados.
3. Na página de detalhes do domínio, navegue até a guia Blueprints.
4. Na lista de Blueprints, escolha o blueprint DefaultDataLakeou o DefaultDataWarehouse, ou o Amazon SageMaker blueprint.
5. Na página de detalhes do blueprint escolhido, escolha Habilitar nesta conta.
6. Na página Permissões e recursos, especifique o seguinte:

    - Se você estiver habilitando o DefaultDataLakeblueprint, para a função Glue Manage Access, especifique uma função de serviço nova ou existente que conceda à Amazon DataZone autorização para ingerir e gerenciar o acesso às tabelas no AWS Glue e no AWS Lake Formation.

- Se você estiver habilitando o DefaultDataWarehouseblueprint, para a função Redshift Manage Access, especifique uma função de serviço nova ou existente que conceda à DataZone Amazon autorização para ingerir e gerenciar o acesso a compartilhamentos de dados, tabelas e visualizações no Amazon Redshift.
- Se você estiver habilitando o Amazon SageMaker blueprint, para a função SageMaker Manage Access, especifique uma função de serviço nova ou existente que conceda à Amazon DataZone permissões para publicar SageMaker dados da Amazon no catálogo. Também concede à Amazon DataZone permissões para conceder acesso ou revogar o acesso aos ativos SageMaker publicados pela Amazon no catálogo.

  > **Important**
  >
  > Quando você está habilitando o Amazon SageMaker blueprint, a Amazon DataZone verifica se as seguintes funções do IAM para a Amazon DataZone existem na conta atual e na região. Se essas funções não existirem, a Amazon as DataZone criará automaticamente.
  >
  > - AmazonDataZoneGlueAccess- <region>- <domainId>
  > - AmazonDataZoneRedshiftAccess- <region>- <domainId>

- Para a função de provisionamento, especifique uma função de serviço nova ou existente que conceda à Amazon DataZone autorização para criar e configurar recursos ambientais usando AWS CloudFormation na conta do ambiente e na região.
- Se você estiver habilitando o Amazon SageMaker blueprint, para o bucket Amazon S3 SageMaker para a fonte de dados -Glue, especifique um bucket do Amazon S3 que deve ser usado por SageMaker todos os ambientes na conta. AWS O prefixo do bucket que você especificar deve ser um dos seguintes:
  - zona de dados da amazon*
  - data zone sagemaker*
  - zona de dados do sagemaker*
  - DataZone-Sagemaker*
  - Sábio- * DataZone
  - DataZone-SageMaker*
  - SageMaker-DataZone*

7. Escolha Habilitar blueprint.

Depois de habilitar o (s) blueprint (s) escolhido (s), você pode controlar quais projetos podem usar o (s) blueprint (s) em sua conta para criar perfis de ambiente. Você pode fazer isso atribuindo o gerenciamento de projetos à configuração do blueprint.

Especifique o gerenciamento de projetos em blueprints habilitados

1. Navegue até o DataZone console da Amazon em https://console.aws.amazon.com/datazone e faça login com as credenciais da sua conta.
2. Escolha Exibir domínios e, em seguida, escolha o domínio em que você deseja adicionar o (s) projeto (s) de gerenciamento para o (s) blueprint (s) escolhido (s).
3. Escolha a guia Blueprints e, em seguida, escolha o blueprint com o qual você deseja trabalhar.
4. Por padrão, todos os projetos dentro do domínio podem usar o DefaultDataLake ou DefaultDataWareshouse, ou os SageMaker blueprints da Amazon na conta para criar perfis de ambiente. No entanto, você pode restringir isso atribuindo projetos de gerenciamento aos blueprints. Para adicionar projetos de gerenciamento, escolha Selecionar projeto de gerenciamento e, em seguida, escolha os projetos que você deseja adicionar como projetos de gerenciamento no menu suspenso e escolha Selecionar projetos de gerenciamento.

Depois de habilitar o DefaultDataWarehouse blueprint em sua AWS conta, você pode adicionar conjuntos de parâmetros à configuração do blueprint. Um conjunto de parâmetros é um grupo de chaves e valores necessários para que DataZone a Amazon estabeleça uma conexão com seu cluster do Amazon Redshift e é usado para criar ambientes de armazém de dados. Esses parâmetros incluem o nome do seu cluster Amazon Redshift, banco de dados e o AWS segredo que contém as credenciais do cluster.

Adicionar conjuntos de parâmetros ao DefaultDataWarehouse blueprint

1. Navegue até o DataZone console da Amazon em https://console.aws.amazon.com/datazone e faça login com as credenciais da sua conta.
2. Escolha Exibir domínios e, em seguida, escolha o domínio ao qual você deseja adicionar o conjunto de parâmetros.
3. Escolha a guia Blueprints e, em seguida, escolha o DefaultDataWareshouse blueprint para abrir a página de detalhes do blueprint.
4. Na guia Conjuntos de parâmetros na página de detalhes do blueprint, escolha Criar conjunto de parâmetros.

    - Forneça um nome para o conjunto de parâmetros.

- Opcionalmente, forneça uma descrição para o conjunto de parâmetros.
- Selecione uma região
- Selecione o cluster Amazon Redshift ou o Amazon Redshift Serverless.
- Selecione o ARN AWS secreto que contém as credenciais do cluster selecionado do Amazon Redshift ou do grupo de trabalho Amazon Redshift Serverless. O AWS segredo deve ser marcado com a `AmazonDataZoneDomain : [Domain_ID]` tag para ser elegível para uso em um conjunto de parâmetros.
  - Se você não tiver um AWS segredo existente, também poderá criar um novo segredo escolhendo Criar novo AWS segredo. Isso abre uma caixa de diálogo na qual você pode fornecer o nome do segredo, nome de usuário e senha. Depois de escolher Create New AWS Secret, a Amazon DataZone cria um novo segredo no serviço AWS Secrets Manager e garante que o segredo seja marcado com o domínio no qual você está tentando criar o conjunto de parâmetros.
- Se você escolheu o cluster Amazon Redshift na etapa acima, agora escolha um cluster no menu suspenso. Se você escolheu o grupo de trabalho do Amazon Redshift na etapa acima, agora escolha um grupo de trabalho no menu suspenso.
- Insira o nome do banco de dados no cluster do Amazon Redshift ou no grupo de trabalho Amazon Redshift Serverless selecionado.
- Escolha Criar conjunto de parâmetros.

Depois de habilitar o Amazon SageMaker blueprint em sua AWS conta, você pode adicionar conjuntos de parâmetros à configuração do blueprint. Um conjunto de parâmetros é um grupo de chaves e valores necessários para que DataZone a Amazon estabeleça uma conexão com sua Amazon SageMaker e é usado para criar ambientes do Sagemaker.

Adicionar conjuntos de parâmetros ao SageMaker blueprint da Amazon

1. Navegue até o DataZone console da Amazon em https://console.aws.amazon.com/datazone e faça login com as credenciais da sua conta.
2. Escolha Exibir domínios e, em seguida, escolha o domínio que contém o blueprint ativado ao qual você deseja adicionar o conjunto de parâmetros.
3. Escolha a guia Blueprints e, em seguida, escolha o SageMaker blueprint da Amazon para abrir a página de detalhes do blueprint.
4. Na guia Conjuntos de parâmetros na página de detalhes do blueprint, escolha Criar conjunto de parâmetros e, em seguida, especifique o seguinte:

- Forneça um nome para o conjunto de parâmetros.
- Opcionalmente, forneça uma Descrição para o conjunto de parâmetros.
- Especifique o tipo de autenticação de SageMaker domínio da Amazon. Você pode escolher o IAM ou o IAM Identity Center (SSO).
- Especifique uma AWS região.
- Especifique uma chave AWS KMS para criptografia de dados. Você pode escolher uma chave existente ou criar uma nova chave.
- Em Parâmetros do ambiente, especifique o seguinte:
  - VPC ID - a ID que você está usando para a VPC do ambiente Amazon. SageMaker Você pode especificar uma VPC existente ou criar uma nova.
  - Sub-redes - uma ou mais IDs para uma variedade de endereços IP para recursos específicos em sua VPC.
  - Acesso à rede - escolha somente VPC ou somente Internet pública.
  - Grupo de segurança - o grupo de segurança a ser usado ao configurar a VPC e as sub-redes.
- Em Parâmetros da fonte de dados, escolha uma das seguintes opções:
  - AWS Glue somente
  - AWS Glue + Amazon Redshift sem servidor. Se você escolher essa opção, especifique o seguinte:
    - Especifique o ARN AWS secreto que contém as credenciais do cluster Amazon Redshift selecionado. O AWS segredo deve ser marcado com a `AmazonDataZoneDomain : [Domain_ID]` tag para ser elegível para uso em um conjunto de parâmetros.

      Se você não tiver um AWS segredo existente, também poderá criar um novo segredo escolhendo Criar novo AWS segredo. Isso abre uma caixa de diálogo na qual você pode fornecer o nome do segredo, nome de usuário e senha. Depois de escolher Create New AWS Secret, a Amazon DataZone cria um novo segredo no serviço AWS Secrets Manager e garante que o segredo seja marcado com o domínio no qual você está tentando criar o conjunto de parâmetros.
    - Especifique o grupo de trabalho do Amazon Redshift que você deseja usar ao criar ambientes.
    - Especifique o nome do banco de dados (dentro do grupo de trabalho que você escolheu) que você deseja usar ao criar ambientes.

- AWS Somente Glue + Amazon Redshift Cluster
  - Especifique o ARN AWS secreto que contém as credenciais do cluster Amazon Redshift selecionado. O AWS segredo deve ser marcado com a `AmazonDataZoneDomain : [Domain_ID]` tag para ser elegível para uso em um conjunto de parâmetros.

    Se você não tiver um AWS segredo existente, também poderá criar um novo segredo escolhendo Criar novo AWS segredo. Isso abre uma caixa de diálogo na qual você pode fornecer o nome do segredo, nome de usuário e senha. Depois de escolher Create New AWS Secret, a Amazon DataZone cria um novo segredo no serviço AWS Secrets Manager e garante que o segredo seja marcado com o domínio no qual você está tentando criar o conjunto de parâmetros.
  - Especifique o cluster do Amazon Redshift que você deseja usar ao criar ambientes.
  - Especifique o nome do banco de dados (dentro do cluster que você escolheu) que você deseja usar ao criar ambientes.

5. Escolha Criar conjunto de parâmetros.

Adicione a Amazon SageMaker como um serviço confiável na AWS conta que possui o DataZone domínio da Amazon

Se você habilitou o Amazon SageMaker blueprint, você também deve adicioná-lo SageMaker como um dos serviços confiáveis da Amazon DataZone. Para fazer isso, conclua o procedimento a seguir:

1. Navegue até o DataZone console da Amazon em https://console.aws.amazon.com/datazone e faça login com as credenciais da sua conta.
2. Escolha Exibir domínios e, em seguida, escolha o domínio que contém o SageMaker blueprint ativado.
3. Escolha os serviços confiáveis, depois escolha a Amazon e SageMaker, em seguida, escolha Ativar.

Trabalhando com contas associadas para publicar e consumir dados

Associar suas AWS contas ao seu DataZone domínio da Amazon permite que os usuários do domínio publiquem e consumam dados dessas AWS contas. Há três etapas para configurar uma associação de conta.

- Primeiro, compartilhe o domínio com a AWS conta desejada solicitando a associação. A Amazon DataZone usa o AWS Resource Access Manager (RAM) se a AWS conta for diferente da AWS conta do domínio. Uma associação de conta só pode ser iniciada pelo DataZone domínio da Amazon.
- Segundo, peça ao proprietário da conta que aceite a solicitação de associação.
- Em terceiro lugar, faça com que o proprietário da conta ative os esquemas de ambiente desejados. Ao habilitar um blueprint, o proprietário da conta está fornecendo aos usuários no domínio as funções do IAM e as configurações de recursos necessárias para criar e acessar recursos em sua conta, como bancos de dados AWS Glue e clusters do Amazon Redshift.

Tópicos

Solicitar associação com outras AWS contas

> **Note**
>
> Ao enviar uma solicitação de associação para outra AWS conta, você está compartilhando seu domínio com a outra AWS conta com o AWS Resource Access Manager (RAM). Certifique-se de verificar a precisão do ID da conta inserido.

Para solicitar a associação com outras AWS contas no DataZone console da Amazon para um DataZone domínio da Amazon, você deve assumir uma função do IAM na conta com permissões administrativas. Configure as permissões do IAM necessárias para usar o console DataZone de gerenciamento da Amazonpara obter as permissões mínimas necessárias para solicitar uma associação de conta.

Conclua o procedimento a seguir para solicitar a associação com outras AWS contas.

1. Faça login no AWS Management Console e abra o console DataZone de gerenciamento da Amazon em https://console.aws.amazon.com/datazone.
2. Escolha Exibir domínios e escolha o nome do domínio na lista. O nome é um hiperlink.
3. Role para baixo até a guia Contas associadas e escolha Solicitar associação.
4. Insira as IDs das contas que você deseja solicitar a associação. Quando estiver satisfeito com a lista de IDs de conta, escolha Solicitar associação.
5. DataZone A Amazon cria um compartilhamento de AWS recursos no Resource Access Manager em nome da sua conta, com os IDs de conta inseridos como principais.
6. Você deve notificar o proprietário da (s) outra (s) AWS conta (s) para aceitar sua solicitação. Os convites expiram após sete (7) dias.

Forneça acesso à conta à sua chave KMS gerenciada pelo cliente

Os DataZone domínios da Amazon e seus metadados são criptografados (por padrão) usando uma chave mantida por AWS ou (opcionalmente) uma chave gerenciada pelo cliente do AWS Key Management Service (KMS) que você possui e fornece durante a criação do domínio. Se seu domínio estiver criptografado com uma chave gerenciada pelo cliente, siga o procedimento abaixo para dar permissão à conta associada para usar a chave KMS.

1. Faça login no AWS Management Console e abra o console KMS em https://console.aws.amazon.com/kms/.
2. Para exibir as chaves em sua conta que você cria e gerencia, no painel de navegação, escolha Customer managed keys (Chaves gerenciadas de cliente).
3. Para exibir as chaves em sua conta que você cria e gerencia, no painel de navegação, escolha Customer managed keys (Chaves gerenciadas de cliente).
4. Na lista de chaves do KMS, escolha o alias ou o ID de chave da chaves do KMS que você deseja examinar.

5. Para permitir ou proibir que AWS contas externas usem a chave KMS, use os controles na seção Outras AWS contas da página. Os diretores do IAM nessas contas (com as próprias permissões de KMS adequadas) podem usar a chave KMS em operações criptográficas, como criptografia, descriptografia, recriptografia e geração de chaves de dados.

Aceite uma solicitação de associação de conta de um DataZone domínio da Amazon e habilite um plano de ambiente

Para aceitar a associação no console DataZone de gerenciamento da Amazon com um DataZone domínio da Amazon, você deve assumir uma função do IAM na conta com permissões administrativas. Configure as permissões do IAM necessárias para usar o console DataZone de gerenciamento da Amazonpara obter as permissões mínimas.

Preencha o seguinte para aceitar a associação com um DataZone domínio da Amazon.

1. Faça login no AWS Management Console e abra o console DataZone de gerenciamento da Amazon em https://console.aws.amazon.com/datazone.
2. Escolha Exibir solicitações e selecione o domínio convidativo na lista. O estado do convite deve ser solicitado. Escolha Solicitação de revisão.
3. Escolha se deseja ativar os esquemas padrão do ambiente de data lake e/ou data warehouse selecionando nenhuma, ambas ou uma das caixas. Você pode fazer isso mais tarde.
   - O plano do ambiente de data lake permite que os usuários do domínio criem e gerenciem recursos do AWS Glue, do Amazon S3 e do Amazon Athena para publicar e consumir em um data lake.
   - O esquema do ambiente de armazém de dados permite que os usuários do domínio criem e gerenciem recursos do Amazon Redshift para publicar e consumir a partir de um data warehouse.
4. Se você optar por selecionar um ou ambos os blueprints de ambiente padrão, configure as permissões e os recursos a seguir.
   - A função Gerenciar acesso do IAM fornece permissões à Amazon DataZone para permitir que os usuários do domínio consumam e gerenciem o acesso a tabelas, como AWS Glue e Amazon Redshift. Você pode optar por fazer com que a Amazon DataZone crie e use uma nova função do IAM, ou você pode escolher entre uma lista de funções do IAM existentes.

- A função Provisioning IAM fornece permissões DataZone à Amazon para permitir que os usuários do domínio criem e configurem recursos do ambiente, como bancos de dados AWS Glue. Você pode optar por fazer com que a Amazon DataZone crie e use uma nova função do IAM, ou você pode escolher entre uma lista de funções do IAM existentes.
- O bucket do Amazon S3 para Data Lake é o bucket ou caminho que a Amazon DataZone usará quando os usuários do domínio armazenarem dados do data lake. Você pode usar o bucket padrão selecionado pela Amazon DataZone ou escolher seu próprio caminho existente do Amazon S3 inserindo sua string de caminho. Se você selecionar seu próprio caminho do Amazon S3, precisará atualizar as políticas do IAM para fornecer à Amazon DataZone permissões para usá-lo.

5. Quando estiver satisfeito com suas configurações, escolha Aceitar e configurar a associação.

Rejeitar uma solicitação de associação de conta de um DataZone domínio da Amazon

Para rejeitar uma solicitação de associação no console DataZone de gerenciamento da Amazon de um DataZone domínio da Amazon, você deve assumir uma função do IAM na conta com permissões administrativas. Configure as permissões do IAM necessárias para usar o console DataZone de gerenciamento da Amazonpara obter as permissões mínimas.

Preencha o seguinte para rejeitar uma solicitação de associação de um DataZone domínio da Amazon.

1. Faça login no AWS Management Console e abra o console DataZone de gerenciamento da Amazon em https://console.aws.amazon.com/datazone.
2. Escolha Exibir solicitações e selecione o domínio convidativo na lista. O estado do convite deve ser solicitado. Escolha Rejeitar associação. Confirme sua escolha escolhendo Rejeitar associação.

Habilitar um blueprint de ambiente em uma conta associada AWS

Para habilitar um plano de ambiente no console DataZone de gerenciamento da Amazon, você deve assumir uma função do IAM na conta com permissões administrativas. Configure as permissões do IAM necessárias para usar o console DataZone de gerenciamento da Amazonpara obter as permissões mínimas.

Preencha o seguinte para habilitar um blueprint em um domínio associado.

1. Faça login no AWS Management Console e abra o console DataZone de gerenciamento da Amazon em https://console.aws.amazon.com/datazone.
2. Abra o painel de navegação esquerdo e escolha Domínios associados.
3. Escolha o domínio para o qual você deseja habilitar um blueprint de ambiente.
4. Na lista de Blueprints, escolha o blueprint DefaultDataLakeou o DefaultDataWarehouse, ou o Amazon SageMaker blueprint.
5. Na página de detalhes do blueprint escolhido, escolha Habilitar nesta conta.
6. Na página Permissões e recursos, especifique o seguinte:

   - Se você estiver habilitando o DefaultDataLakeblueprint, para a função Glue Manage Access, especifique uma função de serviço nova ou existente que conceda à Amazon DataZone autorização para ingerir e gerenciar o acesso às tabelas no AWS Glue e no AWS Lake Formation.
   - Se você estiver habilitando o DefaultDataWarehouseblueprint, para a função Redshift Manage Access, especifique uma função de serviço nova ou existente que conceda à DataZone Amazon autorização para ingerir e gerenciar o acesso a compartilhamentos de dados, tabelas e visualizações no Amazon Redshift.
   - Se você estiver habilitando o Amazon SageMaker blueprint, para a função SageMaker Manage Access, especifique uma função de serviço nova ou existente que conceda à Amazon DataZone permissões para publicar SageMaker dados da Amazon no catálogo. Também concede à Amazon DataZone permissões para conceder acesso ou revogar o acesso aos ativos SageMaker publicados pela Amazon no catálogo.

   > **Important**
   >
   > Quando você está habilitando o Amazon SageMaker blueprint, a Amazon DataZone verifica se as seguintes funções do IAM para a Amazon DataZone existem na conta atual e na região. Se essas funções não existirem, a Amazon as DataZone criará automaticamente.
   >
   > - AmazonDataZoneGlueAccess- <region>- <domainId>
   > - AmazonDataZoneRedshiftAccess- <region>- <domainId>

- Para a função de provisionamento, especifique uma função de serviço nova ou existente que conceda à Amazon DataZone autorização para criar e configurar recursos ambientais usando AWS CloudFormation na conta do ambiente e na região.
- Se você estiver habilitando o Amazon SageMaker blueprint, para o bucket Amazon S3 SageMaker para a fonte de dados -Glue, especifique um bucket do Amazon S3 que deve ser usado por SageMaker todos os ambientes na conta. AWS O prefixo do bucket que você especificar deve ser um dos seguintes:
  - zona de dados da amazon*
  - data zone sagemaker*
  - zona de dados do sagemaker*
  - DataZone-Sagemaker*
  - Sábio- * DataZone
  - DataZone-SageMaker*
  - SageMaker-DataZone*

7. Escolha Habilitar blueprint.

Depois de habilitar o (s) blueprint (s) escolhido (s), você pode controlar quais projetos podem usar o (s) blueprint (s) em sua conta para criar perfis de ambiente. Você pode fazer isso atribuindo o gerenciamento de projetos à configuração do blueprint.

Especifique o gerenciamento de projetos em habilitado DefaultDataLake ou em DefaultDataWarehouse blueprint

1. Navegue até o DataZone console da Amazon em https://console.aws.amazon.com/datazone e faça login com as credenciais da sua conta.
2. Abra o painel de navegação esquerdo e escolha Domínios associados e, em seguida, escolha o domínio ao qual você deseja adicionar o gerenciamento de projetos.
3. Escolha a guia Blueprints e, em seguida, escolha DefaultDataLake ou DefaultDataWareshouse blueprint.
4. Por padrão, todos os projetos dentro do domínio podem usar o DefaultDataWareshouse blueprint DefaultDataLake ou na conta para criar perfis de ambiente. No entanto, você pode restringir isso atribuindo o gerenciamento de projetos ao blueprint. Para adicionar projetos de gerenciamento, escolha Selecionar projeto de gerenciamento e, em seguida, escolha os projetos

que você deseja adicionar como projetos de gerenciamento no menu suspenso e escolha Selecionar projetos de gerenciamento.

Depois de habilitar o DefaultDataWarehouse blueprint em sua AWS conta, você pode adicionar conjuntos de parâmetros à configuração do blueprint. Um conjunto de parâmetros é um grupo de chaves e valores necessários para que DataZone a Amazon estabeleça uma conexão com seu cluster do Amazon Redshift e é usado para criar ambientes de armazém de dados. Esses parâmetros incluem o nome do seu cluster Amazon Redshift, banco de dados e o AWS segredo que contém as credenciais do cluster.

Adicionar conjuntos de parâmetros ao DefaultDataWarehouse blueprint

1. Navegue até o DataZone console da Amazon em https://console.aws.amazon.com/datazone e faça login com as credenciais da sua conta.
2. Abra o painel de navegação esquerdo e escolha Domínios associados e, em seguida, escolha o domínio ao qual você deseja adicionar conjuntos de parâmetros.
3. Escolha a guia Blueprints e, em seguida, escolha o DefaultDataWareshouse blueprint para abrir a página de detalhes do blueprint.
4. Na guia Conjuntos de parâmetros na página de detalhes do blueprint, escolha Criar conjunto de parâmetros.

    - Forneça um nome para o conjunto de parâmetros.
    - Opcionalmente, forneça uma descrição para o conjunto de parâmetros.
    - Selecione uma região
    - Selecione o cluster Amazon Redshift ou o Amazon Redshift Serverless.
    - Selecione o ARN AWS secreto que contém as credenciais do cluster selecionado do Amazon Redshift ou do grupo de trabalho Amazon Redshift Serverless. O AWS segredo deve ser marcado com a `AmazonDataZoneDomain : [Domain_ID]` tag para ser elegível para uso em um conjunto de parâmetros.
        - Se você não tiver um AWS segredo existente, também poderá criar um novo segredo escolhendo Criar novo AWS segredo. Isso abre uma caixa de diálogo na qual você pode fornecer o nome do segredo, nome de usuário e senha. Depois de escolher Create New AWS Secret, a Amazon DataZone cria um novo segredo no serviço AWS Secrets Manager e garante que o segredo seja marcado com o domínio no qual você está tentando criar o conjunto de parâmetros.

- Selecione o cluster Amazon Redshift ou o grupo de trabalho Amazon Redshift Serverless.
- Insira o nome do banco de dados no cluster do Amazon Redshift ou no grupo de trabalho Amazon Redshift Serverless selecionado.
- Escolha Criar conjunto de parâmetros.

Depois de habilitar o Amazon SageMaker blueprint em sua AWS conta, você pode adicionar conjuntos de parâmetros à configuração do blueprint. Um conjunto de parâmetros é um grupo de chaves e valores necessários para que DataZone a Amazon estabeleça uma conexão com sua Amazon SageMaker e é usado para criar ambientes do Sagemaker.

Adicionar conjuntos de parâmetros ao SageMaker blueprint da Amazon

1. Navegue até o DataZone console da Amazon em https://console.aws.amazon.com/datazone e faça login com as credenciais da sua conta.
2. Escolha Exibir domínios e, em seguida, escolha o domínio que contém o blueprint ativado ao qual você deseja adicionar o conjunto de parâmetros.
3. Escolha a guia Blueprints e, em seguida, escolha o SageMaker blueprint da Amazon para abrir a página de detalhes do blueprint.
4. Na guia Conjuntos de parâmetros na página de detalhes do blueprint, escolha Criar conjunto de parâmetros e, em seguida, especifique o seguinte:
   - Forneça um nome para o conjunto de parâmetros.
   - Opcionalmente, forneça uma Descrição para o conjunto de parâmetros.
   - Especifique o tipo de autenticação de SageMaker domínio da Amazon. Você pode escolher o IAM ou o IAM Identity Center (SSO).
   - Especifique uma AWS região.
   - Especifique uma chave AWS KMS para criptografia de dados. Você pode escolher uma chave existente ou criar uma nova chave.
   - Em Parâmetros do ambiente, especifique o seguinte:
     - VPC ID - a ID que você está usando para a VPC do ambiente Amazon. SageMaker Você pode especificar uma VPC existente ou criar uma nova.
     - Sub-redes - uma ou mais IDs para uma variedade de endereços IP para recursos específicos em sua VPC.
     - Acesso à rede - escolha somente VPC ou somente Internet pública.

- Grupo de segurança - o grupo de segurança a ser usado ao configurar a VPC e as sub-redes.

- Em Parâmetros da fonte de dados, escolha uma das seguintes opções:
  - AWS Glue somente
  - AWS Glue + Amazon Redshift sem servidor. Se você escolher essa opção, especifique o seguinte:
    - Especifique o ARN AWS secreto que contém as credenciais do cluster Amazon Redshift selecionado. O AWS segredo deve ser marcado com a `AmazonDataZoneDomain : [Domain_ID]` tag para ser elegível para uso em um conjunto de parâmetros.

      Se você não tiver um AWS segredo existente, também poderá criar um novo segredo escolhendo Criar novo AWS segredo. Isso abre uma caixa de diálogo na qual você pode fornecer o nome do segredo, nome de usuário e senha. Depois de escolher Create New AWS Secret, a Amazon DataZone cria um novo segredo no serviço AWS Secrets Manager e garante que o segredo seja marcado com o domínio no qual você está tentando criar o conjunto de parâmetros.
    - Especifique o grupo de trabalho do Amazon Redshift que você deseja usar ao criar ambientes.
    - Especifique o nome do banco de dados (dentro do grupo de trabalho que você escolheu) que você deseja usar ao criar ambientes.
  - AWS Somente Glue + Amazon Redshift Cluster
    - Especifique o ARN AWS secreto que contém as credenciais do cluster Amazon Redshift selecionado. O AWS segredo deve ser marcado com a `AmazonDataZoneDomain : [Domain_ID]` tag para ser elegível para uso em um conjunto de parâmetros.

      Se você não tiver um AWS segredo existente, também poderá criar um novo segredo escolhendo Criar novo AWS segredo. Isso abre uma caixa de diálogo na qual você pode fornecer o nome do segredo, nome de usuário e senha. Depois de escolher Create New AWS Secret, a Amazon DataZone cria um novo segredo no serviço AWS Secrets Manager e garante que o segredo seja marcado com o domínio no qual você está tentando criar o conjunto de parâmetros.
    - Especifique o cluster do Amazon Redshift que você deseja usar ao criar ambientes.
    - Especifique o nome do banco de dados (dentro do cluster que você escolheu) que você deseja usar ao criar ambientes.

5. Escolha Criar conjunto de parâmetros.

Adicione a Amazon SageMaker como um serviço confiável na AWS conta associada

Se você habilitou o Amazon SageMaker blueprint, você também deve adicioná-lo SageMaker como um dos serviços confiáveis da Amazon DataZone. Para fazer isso, conclua o procedimento a seguir:

1. Navegue até o DataZone console da Amazon em https://console.aws.amazon.com/datazone e faça login com as credenciais da sua conta.
2. Escolha Exibir domínios e, em seguida, escolha o domínio que contém o SageMaker blueprint ativado.
3. Escolha os serviços confiáveis, depois escolha a Amazon e SageMaker, em seguida, escolha Ativar.

Remover uma conta associada

Para remover uma AWS conta associada no console DataZone de gerenciamento da Amazon, você deve assumir uma função do IAM na conta com permissões administrativas. Configure as permissões do IAM necessárias para usar o console DataZone de gerenciamento da Amazonpara obter as permissões mínimas.

Conclua o procedimento a seguir para remover uma conta associada do seu domínio.

1. Faça login no AWS Management Console e abra o console DataZone de gerenciamento da Amazon em https://console.aws.amazon.com/datazone.
2. Escolha Exibir domínios e escolha o nome do domínio na lista. O nome é um hiperlink.
3. Role para baixo até a guia Contas associadas. Escolha o ID da AWS conta que você deseja remover.
4. Escolha Desassociar. Confirme sua escolha inserindo dissociar no campo e escolhendo Desassociar.
5. A conta agora foi removida do seu domínio e não pode ser usada pelos usuários do domínio para publicar e consumir dados.

Trabalhando com o catálogo de DataZone dados da Amazon

Você pode usar o catálogo de dados DataZone comerciais da Amazon para catalogar dados em toda a sua organização com contexto comercial e, assim, permitir que todos em sua organização encontrem e entendam dados rapidamente. Para ter mais informações, consulte DataZone Terminologia e conceitos da Amazon.

Tópicos

Crie, edite ou exclua um glossário comercial

Na Amazon DataZone, um glossário comercial é uma coleção de termos comerciais (palavras) que podem estar associados a ativos (dados). Ele fornece vocabulários apropriados com uma lista de termos comerciais e suas definições para usuários corporativos, a fim de garantir que as mesmas definições sejam usadas em toda a organização ao analisar dados. Os glossários de negócios são criados no domínio do catálogo e podem ser aplicados a ativos e colunas para ajudar a entender as principais características desse ativo ou coluna. Um ou mais termos do glossário podem ser aplicados. Um glossário comercial pode ser uma lista simples de termos em que qualquer termo no glossário comercial pode ser associado a uma sublista de outros termos. Para ter mais informações, consulte DataZone Terminologia e conceitos da Amazon. Para criar, editar ou excluir um glossário em seu DataZone domínio da Amazon, você deve ser membro do projeto proprietário com as permissões certas para esse domínio.

Para criar um glossário, conclua as seguintes etapas:

1. Navegue até o portal de DataZone dados da Amazon usando a URL do portal de dados e faça login usando seu SSO ou suas AWS credenciais. Se você for DataZone administrador da Amazon, poderá obter a URL do portal de dados acessando o DataZone console da Amazon em https://console.aws.amazon.com/datazone na AWS conta em que o DataZone domínio da Amazon foi criado.

2. Navegue até o menu Catálogo na barra de navegação superior ao lado de Pesquisar.
3. No Amazon DataZone Data Portal, escolha Glossários e, em seguida, escolha Criar glossário.
4. Especifique um nome, descrição e proprietário para o glossário e escolha Criar glossário.
5. Ative o novo glossário escolhendo o botão Ativado.
6. Na página de detalhes do glossário, você pode escolher Criar readme para adicionar mais informações sobre esse glossário.

Para desativar ou ativar um glossário comercial, conclua as seguintes etapas:

1. Navegue até o portal de DataZone dados da Amazon usando a URL do portal de dados e faça login usando seu SSO ou suas AWS credenciais. Se você for DataZone administrador da Amazon, poderá obter a URL do portal de dados acessando o DataZone console da Amazon em https://console.aws.amazon.com/datazone na AWS conta em que o DataZone domínio da Amazon foi criado.
2. Navegue até o menu Catálogo na barra de navegação superior ao lado de Pesquisar.
3. No Amazon DataZone Data Portal, escolha Glossários e localize o glossário de negócios que você deseja desativar/ativar.
4. Na página de detalhes do glossário, localize o botão Ativar/Desativar e use-o para ativar ou desativar o glossário selecionado.

> **Note**
>
> A desativação de um glossário também desativa todos os termos que ele contém.

Para editar um glossário comercial, conclua as seguintes etapas:

1. Navegue até o portal de DataZone dados da Amazon usando a URL do portal de dados e faça login usando seu SSO ou suas AWS credenciais. Se você for DataZone administrador da Amazon, poderá obter a URL do portal de dados acessando o DataZone console da Amazon em https://console.aws.amazon.com/datazone na AWS conta em que o DataZone domínio da Amazon foi criado.
2. Navegue até o menu Catálogo na barra de navegação superior ao lado de Pesquisar.
3. No Amazon DataZone Data Portal, escolha Glossários e localize o glossário de negócios que você deseja editar.

4. Na página de detalhes do glossário, expanda Ações e escolha Editar para editar o glossário.
5. Faça suas atualizações no nome, na descrição e escolha Salvar.

Para excluir um glossário comercial, conclua as seguintes etapas:

1. Navegue até o portal de DataZone dados da Amazon usando a URL do portal de dados e faça login usando seu SSO ou suas AWS credenciais. Se você for DataZone administrador da Amazon, poderá obter a URL do portal de dados acessando o DataZone console da Amazon em https://console.aws.amazon.com/datazone na AWS conta em que o DataZone domínio da Amazon foi criado.
2. Navegue até o menu Catálogo na barra de navegação superior ao lado de Pesquisar.
3. No Amazon DataZone Data Portal, escolha Glossários e localize o glossário de negócios que você deseja excluir.
4. Na página de detalhes do glossário, expanda Ações e escolha Excluir para excluir o glossário.

> **Note**
>
> Você deve excluir todos os termos existentes no glossário antes de excluir o glossário.

5. Confirme a exclusão do glossário escolhendo Excluir.

Criar, editar ou excluir um termo em um glossário

Na Amazon DataZone, um glossário de negócios é uma coleção de termos comerciais que podem estar associados a ativos (dados). Para ter mais informações, consulte DataZone Terminologia e conceitos da Amazon. Para criar, editar ou excluir termos em um glossário em seu DataZone domínio da Amazon, você deve ser membro do projeto proprietário com as permissões certas para esse domínio.

Na Amazon DataZone, os termos do glossário de negócios podem ter descrições detalhadas. Para definir o contexto de um termo específico, você pode especificar relações entre os termos. Quando você define um relacionamento para um termo, ele é automaticamente adicionado à definição do termo relacionado. Os relacionamentos de termos do glossário disponíveis na Amazon DataZone incluem o seguinte:

- É um tipo de - indica que o termo atual é um tipo do termo identificado. Indica que o termo identificado é pai do termo atual.

- Tem tipos - indica que o termo atual é um termo genérico para o termo ou termos específicos indicados. Essa relação pode denotar termos secundários para o termo genérico.

Para criar um novo termo, conclua as seguintes etapas:

1. Navegue até o portal de DataZone dados da Amazon usando a URL do portal de dados e faça login usando seu SSO ou suas AWS credenciais. Se você for DataZone administrador da Amazon, poderá obter a URL do portal de dados acessando o DataZone console da Amazon em https://console.aws.amazon.com/datazone na AWS conta em que o DataZone domínio da Amazon foi criado.
2. Navegue até o menu Catálogo na barra de navegação superior ao lado de Pesquisar.
3. No Amazon DataZone Data Portal, escolha Glossários e, em seguida, escolha o glossário em que você deseja criar o novo termo.
4. Especifique um nome, descrição e proprietário para o termo e escolha Criar termo.
5. Ative o novo termo escolhendo o botão Ativado.
6. Para adicionar um arquivo Readme, navegue até a página de detalhes do termo e escolha Criar arquivo readme para adicionar mais informações sobre esse glossário.
7. Para adicionar relacionamentos, navegue até a página de detalhes do termo, escolha a seção Relações entre termos e, em seguida, escolha Adicionar termos do glossário. Na caixa de diálogo, escolha o relacionamento e os termos que você deseja relacionar e, em seguida, escolha Fechar para adicionar um termo ao tipo de relacionamento apropriado. Esse relacionamento também é adicionado a todos os termos que você relacionou.

Para editar um termo em um glossário, conclua as seguintes etapas:

1. Navegue até o portal de DataZone dados da Amazon usando a URL do portal de dados e faça login usando seu SSO ou suas AWS credenciais. Se você for DataZone administrador da Amazon, poderá obter a URL do portal de dados acessando o DataZone console da Amazon em https://console.aws.amazon.com/datazone na AWS conta em que o DataZone domínio da Amazon foi criado.
2. Navegue até o menu Catálogo na barra de navegação superior ao lado de Pesquisar.
3. No Amazon DataZone Data Portal, escolha Glossários, localize o glossário que contém o termo que você deseja editar e, em seguida, escolha esse termo.
4. Na página de detalhes do termo, expanda Ações e escolha Editar para editar o termo.

5. Faça suas atualizações no nome, na descrição e escolha Salvar.

Para excluir um termo em um glossário, conclua as seguintes etapas:

1. Navegue até o portal de DataZone dados da Amazon usando a URL do portal de dados e faça login usando seu SSO ou suas AWS credenciais. Se você for DataZone administrador da Amazon, poderá obter a URL do portal de dados acessando o DataZone console da Amazon em https://console.aws.amazon.com/datazone na AWS conta em que o DataZone domínio da Amazon foi criado.
2. Navegue até o menu Catálogo na barra de navegação superior ao lado de Pesquisar.
3. No Amazon DataZone Data Portal, escolha Glossários, localize o glossário que contém o termo que você deseja excluir e, em seguida, escolha esse termo.
4. Na página de detalhes do glossário, expanda Ações e escolha Excluir para excluir o termo.
5. Confirme a exclusão do termo escolhendo Excluir.

Crie, edite ou exclua formulários de metadados

Na Amazon DataZone, os formulários de metadados são formulários simples para ampliar o contexto comercial adicional aos metadados de ativos no catálogo. Ele serve como um mecanismo extensível para que os proprietários de dados enriqueçam o ativo com informações que podem ajudar os usuários de dados a pesquisar e encontrar esses dados. Os formulários de metadados também podem servir como um mecanismo para garantir a consistência de todos os ativos publicados no catálogo da Amazon DataZone .

Uma definição de formulário de metadados é composta por uma ou mais definições de campo, com suporte para tipos de dados de valor de campo booleano, de data, decimal, inteiro, sequência de caracteres e glossário comercial. Para ter mais informações, consulte DataZone Terminologia e conceitos da Amazon. Para criar, editar ou excluir formulários de metadados em seu DataZone domínio da Amazon, você deve ser membro do projeto proprietário e ter as credenciais corretas.

Para criar um formulário de metadados, conclua as seguintes etapas:

1. Navegue até o portal de DataZone dados da Amazon usando a URL do portal de dados e faça login usando seu SSO ou suas AWS credenciais. Se você for DataZone administrador da Amazon, poderá obter a URL do portal de dados acessando o DataZone console da Amazon em https://console.aws.amazon.com/datazone na AWS conta em que o DataZone domínio da Amazon foi criado.

2. Navegue até o menu Catálogo na barra de navegação superior ao lado de Pesquisar.
3. No Amazon DataZone Data Portal, escolha Formulários de metadados e, em seguida, escolha Criar formulário.
4. Especifique o nome, a descrição e o proprietário do formulário de metadados e escolha Criar formulário.

Para editar um formulário de metadados, conclua as seguintes etapas:

1. Navegue até o portal de DataZone dados da Amazon usando a URL do portal de dados e faça login usando seu SSO ou suas AWS credenciais. Se você for DataZone administrador da Amazon, poderá obter a URL do portal de dados acessando o DataZone console da Amazon em https://console.aws.amazon.com/datazone na AWS conta em que o DataZone domínio da Amazon foi criado.
2. Navegue até o menu Catálogo na barra de navegação superior ao lado de Pesquisar.
3. No Amazon DataZone Data Portal, escolha Formulários de metadados e, em seguida, localize o formulário de metadados que você deseja editar.
4. Na página de detalhes do formulário de metadados, expanda Ações e escolha Editar.
5. Atualize seus campos de nome, descrição e proprietário e escolha Atualizar formulário.

Para excluir um formulário de metadados, conclua as seguintes etapas:

> **Note**
>
> Antes de excluir um formulário de metadados, você deve removê-lo de todos os tipos de ativos ou ativos aos quais ele é aplicado.

1. Navegue até o portal de DataZone dados da Amazon usando a URL do portal de dados e faça login usando seu SSO ou suas AWS credenciais. Se você for DataZone administrador da Amazon, poderá obter a URL do portal de dados acessando o DataZone console da Amazon em https://console.aws.amazon.com/datazone na AWS conta em que o DataZone domínio da Amazon foi criado.
2. Navegue até o menu Catálogo na barra de navegação superior ao lado de Pesquisar.
3. No Amazon DataZone Data Portal, escolha Formulários de metadados e, em seguida, localize o formulário de metadados que você deseja excluir.

4. Se o formulário de metadados que você deseja excluir estiver ativado, desative o formulário de metadados escolhendo a opção Ativado.
5. Na página de detalhes do formulário de metadados, expanda Ações e escolha Excluir.
6. Confirme a exclusão escolhendo Excluir.

Crie, edite ou exclua campos em formulários de metadados

Na Amazon DataZone, os formulários de metadados são formulários simples para ampliar o contexto comercial adicional aos metadados de ativos no catálogo. Ele serve como um mecanismo extensível para que os proprietários de dados enriqueçam o ativo com informações que podem ajudar os usuários de dados a pesquisar e encontrar esses dados. Os formulários de metadados também podem servir como um mecanismo para garantir a consistência de todos os ativos publicados no catálogo da Amazon DataZone .

Uma definição de formulário de metadados é composta por uma ou mais definições de campo, com suporte para tipos de dados de valor de campo booleano, de data, decimal, inteiro, sequência de caracteres e glossário comercial. Para ter mais informações, consulte DataZone Terminologia e conceitos da Amazon. Para criar, editar ou excluir campos em formulários de metadados em seu DataZone domínio da Amazon, você deve ser membro do projeto proprietário e ter as credenciais corretas.

Para criar um campo em um formulário de metadados, conclua as seguintes etapas:

1. Navegue até o portal de DataZone dados da Amazon usando a URL do portal de dados e faça login usando seu SSO ou suas AWS credenciais. Se você for DataZone administrador da Amazon, poderá obter a URL do portal de dados acessando o DataZone console da Amazon em https://console.aws.amazon.com/datazone na AWS conta em que o DataZone domínio da Amazon foi criado.
2. Navegue até o menu Catálogo na barra de navegação superior ao lado de Pesquisar.
3. No Amazon DataZone Data Portal, escolha Formulários de metadados e, em seguida, escolha o formulário de metadados em que você deseja criar campo (s).
4. Na página de detalhes do formulário, escolha Criar campo.
5. Especifique o nome do campo, a descrição, o tipo e se esse é um campo obrigatório e, em seguida, escolha Criar campo.

Para editar um campo em um formulário de metadados, conclua as seguintes etapas:

1. Navegue até o portal de DataZone dados da Amazon usando a URL do portal de dados e faça login usando seu SSO ou suas AWS credenciais. Se você for DataZone administrador da Amazon, poderá obter a URL do portal de dados acessando o DataZone console da Amazon em https://console.aws.amazon.com/datazone na AWS conta em que o DataZone domínio da Amazon foi criado.
2. Navegue até o menu Catálogo na barra de navegação superior ao lado de Pesquisar.
3. No Amazon DataZone Data Portal, escolha Formulários de metadados e, em seguida, escolha o formulário de metadados em que você deseja editar o (s) campo (s).
4. Na página de detalhes do formulário, escolha o campo que você deseja editar, expanda Ações e escolha Editar.
5. Faça suas atualizações no nome do campo, descrição, tipo e se esse é um campo obrigatório e, em seguida, escolha Atualizar campo.

Para excluir um campo em um formulário de metadados, conclua as seguintes etapas:

1. Navegue até o portal de DataZone dados da Amazon usando a URL do portal de dados e faça login usando seu SSO ou suas AWS credenciais. Se você for DataZone administrador da Amazon, poderá obter a URL do portal de dados acessando o DataZone console da Amazon em https://console.aws.amazon.com/datazone na AWS conta em que o DataZone domínio da Amazon foi criado.
2. Navegue até o menu Catálogo na barra de navegação superior ao lado de Pesquisar.
3. No Amazon DataZone Data Portal, escolha Formulários de metadados e, em seguida, escolha o formulário de metadados em que você deseja excluir o (s) campo (s).
4. Na página de detalhes do formulário, escolha o campo que você deseja excluir, expanda Ações e escolha Excluir.
5. Confirme a exclusão escolhendo Excluir.

Trabalhando com projetos e ambientes na Amazon DataZone

Na Amazon DataZone, os projetos permitem que um grupo de usuários colabore em vários casos de uso comercial que envolvem publicação, descoberta, assinatura e consumo de ativos de dados no catálogo da Amazon. DataZone Cada DataZone projeto da Amazon tem um conjunto de controles de acesso aplicados a ele para que somente indivíduos, grupos e funções autorizados possam acessar o projeto e os ativos de dados que esse projeto subscreve e possam usar somente as ferramentas definidas pelas permissões do projeto. Os projetos atuam como um principal de identidade que recebe concessões de acesso aos recursos subjacentes, permitindo que DataZone a Amazon opere na infraestrutura de uma organização sem depender das credenciais individuais do usuário. Para mais informações, consulte DataZone Terminologia e conceitos da Amazon.

Tópicos

Crie um perfil de ambiente

Na Amazon DataZone, um perfil de ambiente é um modelo que você pode usar para criar ambientes. O objetivo de um perfil de ambiente é simplificar a criação do ambiente incorporando informações de posicionamento, como AWS conta e região, nos perfis. Para ter mais informações, consulte

DataZone Terminologia e conceitos da Amazon. Para criar perfis de ambiente em um DataZone domínio da Amazon, você deve pertencer a um DataZone projeto da Amazon. Todos os perfis de ambiente pertencem a projetos e podem ser usados por todos os usuários autorizados, de qualquer projeto, para criar novos ambientes.

Para criar um perfil de ambiente

1. Navegue até o portal de DataZone dados da Amazon usando a URL do portal de dados e faça login usando seu SSO ou suas AWS credenciais. Se você for DataZone administrador da Amazon, poderá obter a URL do portal de dados acessando o DataZone console da Amazon em https://console.aws.amazon.com/datazone na AWS conta em que o DataZone domínio da Amazon foi criado.
2. No portal de dados, escolha Procurar projetos e selecione o projeto no qual você deseja criar o perfil do ambiente.
3. Navegue até a guia Ambientes dentro do projeto e escolha Criar perfil de ambiente.
4. Configure os campos a seguir.

    - Nome — O nome do seu perfil de ambiente.
    - Descrição — (Opcional) Uma descrição para seu perfil de ambiente.
    - Projeto do proprietário - O projeto em que o perfil está sendo criado é selecionado por padrão nesse campo.
    - Blueprint — O blueprint para o qual esse perfil foi criado. Você pode escolher um dos DataZone blueprints padrão da Amazon (Data Lake ou Data Warehouse).

      Se você especificou o blueprint do Data Warehouse, faça o seguinte:

      - Forneça um conjunto de parâmetros. Para selecionar um conjunto de parâmetros existente, escolha a opção Escolher um conjunto de parâmetros. Se você quiser inserir seus próprios parâmetros, escolha Inserir meus próprios.
      - Se você optar por selecionar um parâmetro existente, faça o seguinte:
        - Selecione uma AWS conta no menu suspenso.
        - Selecione um conjunto de parâmetros no menu suspenso.
      - Se você optar por inserir seus próprios parâmetros, faça o seguinte:
        - Forneça os AWS parâmetros selecionando a AWS Conta e a Região no menu suspenso.
        - Forneça os parâmetros do Redshift Data Warehouse:
          - Selecione o cluster Amazon Redshift ou o Amazon Redshift Serverless

- Insira o ARN AWS secreto que contém as credenciais do cluster Amazon Redshift ou do grupo de trabalho Amazon Redshift Serverless selecionado. O AWS segredo deve ser marcado com o ID do domínio e o ID do projeto em que você está criando o perfil do ambiente.
  - `AmazonDataZoneDomain: [Domain_ID]`
  - `AmazonDataZoneProject: [Project_ID]`
- Insira o nome do cluster Amazon Redshift ou do grupo de trabalho Amazon Redshift Serverless.
- Insira o nome do banco de dados no cluster do Amazon Redshift ou no grupo de trabalho Amazon Redshift Serverless selecionado.

- Na seção Projetos autorizados, especifique os projetos que podem usar o perfil do ambiente para criar ambientes. Por padrão, todos os projetos dentro do domínio podem usar os perfis de ambiente na conta para criar ambientes. Para manter essa configuração padrão, escolha Todos os projetos. No entanto, você pode restringir isso atribuindo projetos autorizados ao ambiente. Para fazer isso, escolha Somente projetos autorizados e, em seguida, especifique os projetos que podem usar esse perfil de projeto para criar ambientes.
- Na seção Publicação, escolha uma das seguintes opções:
  - Publicar de qualquer esquema: Se você escolher essa opção, os ambientes criados usando esse perfil de ambiente poderão ser usados para publicar de qualquer esquema dentro do banco de dados selecionado nos parâmetros do Redshift fornecidos acima. Os usuários do ambiente criado usando esses perfis de ambiente também podem fornecer seus próprios parâmetros do Amazon Redshift para publicar a partir de qualquer esquema dentro da AWS conta e região selecionada no perfil do ambiente.
  - Publicar somente a partir do esquema de ambiente padrão: se você escolher essa opção, os ambientes criados usando isso poderão ser usados para publicar somente a partir do esquema padrão criado DataZone pela Amazon para esse ambiente. Os usuários do ambiente criado usando esses perfis de ambiente não podem fornecer seus próprios parâmetros do Amazon Redshift.
  - Não permitir publicação: se você escolher essa opção, os ambientes criados usando esse perfil de ambiente só poderão ser usados para assinatura e consumo de dados. Os ambientes não podem ser usados para publicar nenhum dado.

Se você especificou o blueprint do Data Lake, faça o seguinte:

- Na seção de parâmetros da AWS conta, especifique o número da AWS conta e a região da AWS conta em que os ambientes potenciais serão criados.
- Na seção Projetos autorizados, especifique os projetos que podem usar o perfil de ambiente com o perfil de ambiente integrado do Data Lake para criar ambientes. Por padrão, todos os projetos dentro do domínio podem usar o data lake blueprint na conta para criar perfis de ambiente. Para manter essa configuração padrão, escolha Todos os projetos. No entanto, você pode restringir isso atribuindo projetos ao blueprint. Para fazer isso, escolha Somente projetos autorizados e, em seguida, especifique os projetos que podem usar esse perfil de projeto para criar ambientes.
- Na seção Bancos de dados, escolha Qualquer banco de dados para permitir a publicação de qualquer banco de dados dentro da AWS conta e da região em que o ambiente foi criado ou escolha Somente banco de dados padrão para permitir a publicação somente do banco de dados de publicação padrão criado com o ambiente.

5. Escolha Criar perfil de ambiente.

Editar um perfil de ambiente

Na Amazon DataZone, um perfil de ambiente é um modelo que você pode usar para criar ambientes. Para ter mais informações, consulte DataZone Terminologia e conceitos da Amazon. Para editar perfis de ambiente existentes em um DataZone domínio da Amazon, você deve pertencer a um DataZone projeto da Amazon.

Para editar um perfil de ambiente

1. Navegue até o URL do portal de DataZone dados da Amazon e faça login usando o single sign-on (SSO) ou suas credenciais. AWS Se você for DataZone administrador da Amazon, poderá navegar até o DataZone console da Amazon em https://console.aws.amazon.com/datazone e fazer login com o Conta da AWS local onde o domínio foi criado e, em seguida, escolher Abrir portal de dados.
2. No portal de dados, escolha Procurar projetos e selecione o projeto no qual você deseja editar o perfil do ambiente.
3. Navegue até a guia Ambientes dentro do projeto, escolha Perfis de ambiente e escolha o perfil de ambiente que você deseja editar.

   Se você estiver editando um perfil de ambiente do Data Warehouse, só poderá editar o nome e a descrição de um perfil de ambiente existente.

Se você estiver editando um perfil de ambiente do Data Lake, poderá editar o nome e a descrição do perfil e também poderá editar os projetos autorizados a usar esse perfil para criar ambientes e editar bancos de dados. Para editar essas configurações, faça o seguinte:

- Na seção Projetos autorizados, especifique os projetos que podem usar o perfil de ambiente com o perfil de ambiente integrado do Data Lake para criar ambientes. Por padrão, todos os projetos dentro do domínio podem usar o data lake blueprint na conta para criar perfis de ambiente. Para manter essa configuração padrão, escolha Todos os projetos. No entanto, você pode restringir isso atribuindo projetos ao blueprint. Para fazer isso, escolha Somente projetos autorizados e, em seguida, especifique os projetos que podem usar esse perfil de projeto para criar ambientes.
- Na seção Bancos de dados, escolha Qualquer banco de dados para permitir a publicação de qualquer banco de dados dentro da AWS conta e da região em que o ambiente foi criado ou escolha Somente banco de dados padrão para permitir a publicação somente do banco de dados de publicação padrão criado com o ambiente.

Ao concluir suas edições, escolha Editar perfil do ambiente.

Excluir um perfil de ambiente

Na Amazon DataZone, um perfil de ambiente é um modelo que você pode usar para criar ambientes. O objetivo de um perfil de ambiente é simplificar a criação do ambiente incorporando informações de posicionamento, como AWS conta e região, nos perfis. Para ter mais informações, consulte DataZone Terminologia e conceitos da Amazon. Para excluir perfis de ambiente em um DataZone domínio da Amazon, você deve pertencer a um DataZone projeto da Amazon.

> **Note**
>
> Ao excluir um perfil de ambiente, você não pode criar mais ambientes usando esse perfil.

Para excluir um perfil de ambiente

1. Navegue até o URL do portal de DataZone dados da Amazon e faça login usando o single sign-on (SSO) ou suas credenciais. AWS Se você for DataZone administrador da Amazon, poderá navegar até o DataZone console da Amazon em https://console.aws.amazon.com/datazone e

fazer login com o Conta da AWS local onde o domínio foi criado e, em seguida, escolher Abrir portal de dados.

2. No portal de dados, escolha Procurar projetos e selecione o projeto no qual você deseja excluir o perfil do ambiente.
3. Navegue até a guia Ambientes dentro do projeto, escolha Perfis de ambiente e escolha o perfil de ambiente que você deseja excluir.
4. Selecione o perfil do ambiente que você deseja excluir e, em seguida, escolha Ações, Excluir e confirme a exclusão.

Criar um novo ambiente

Nos DataZone projetos da Amazon, os ambientes são coleções de recursos configurados (por exemplo, um bucket do Amazon S3, um banco de dados AWS Glue ou um grupo de trabalho do Amazon Athena), com um determinado conjunto de princípios do IAM (funções de usuário do ambiente) com permissões atribuídas de proprietário ou colaborador que podem operar com esses recursos. Para ter mais informações, consulte DataZone Terminologia e conceitos da Amazon.

Qualquer DataZone usuário da Amazon com as permissões necessárias para acessar o portal de dados pode criar um DataZone ambiente Amazon dentro de um projeto.

Para criar um novo ambiente, conclua as etapas a seguir.

1. Navegue até o URL do portal de DataZone dados da Amazon e faça login usando o single sign-on (SSO) ou suas credenciais. AWS Se você for DataZone administrador da Amazon, poderá navegar até o DataZone console da Amazon em https://console.aws.amazon.com/datazone e fazer login com o Conta da AWS local onde o domínio foi criado e, em seguida, escolher Abrir portal de dados.
2. Escolha Pesquisar todos os projetos e selecione o projeto no qual você deseja criar um novo ambiente.
3. Escolha Criar ambiente, especifique valores para os campos a seguir e escolha Criar ambiente:

   - Nome — o nome do ambiente
   - Descrição — uma descrição do ambiente
   - Perfil de ambiente — escolha um perfil de ambiente existente ou crie um novo. Um perfil de ambiente é um modelo que você pode usar para criar ambientes. Para ter mais informações, consulte DataZone Terminologia e conceitos da Amazon.

Depois de selecionar o perfil do ambiente, na seção Parâmetros, especifique os valores dos campos que fazem parte desse perfil do ambiente.

Editar um ambiente

Nos DataZone projetos da Amazon, os ambientes são coleções de recursos configurados (por exemplo, um bucket do Amazon S3, um banco de dados AWS Glue ou um grupo de trabalho do Amazon Athena), com um determinado conjunto de diretores do IAM (com permissões de colaborador atribuídas) que podem operar nesses recursos. Para ter mais informações, consulte DataZone Terminologia e conceitos da Amazon.

Qualquer DataZone usuário da Amazon com as permissões necessárias para acessar o portal de dados pode editar um DataZone ambiente da Amazon dentro de um projeto.

Para editar um ambiente existente, conclua as etapas a seguir.

1. Navegue até o URL do portal de DataZone dados da Amazon e faça login usando o single sign-on (SSO) ou suas credenciais. AWS Se você for DataZone administrador da Amazon, poderá navegar até o DataZone console da Amazon em https://console.aws.amazon.com/datazone e fazer login com o Conta da AWS local onde o domínio foi criado e, em seguida, escolher Abrir portal de dados.
2. Escolha Procurar projetos no painel de navegação superior e selecione o projeto que contém o ambiente que você deseja editar.
3. Localize e escolha o ambiente para abrir sua página de detalhes. Em seguida, expanda Ações e escolha Editar ambiente.
4. Faça suas edições no nome e na descrição do ambiente e escolha Salvar alterações.

Exclua um ambiente

Nos DataZone projetos da Amazon, os ambientes são coleções de recursos configurados (por exemplo, um bucket do Amazon S3, um banco de dados AWS Glue ou um grupo de trabalho do Amazon Athena), com um determinado conjunto de diretores do IAM (com permissões de colaborador atribuídas) que podem operar nesses recursos. Para ter mais informações, consulte DataZone Terminologia e conceitos da Amazon.

Qualquer DataZone usuário da Amazon com as permissões necessárias para acessar o portal de dados pode excluir um DataZone ambiente da Amazon dentro de um projeto.

Para excluir um ambiente existente, conclua as etapas a seguir.

1. Navegue até o URL do portal de DataZone dados da Amazon e faça login usando o single sign-on (SSO) ou suas credenciais. AWS Se você for DataZone administrador da Amazon, poderá navegar até o DataZone console da Amazon em https://console.aws.amazon.com/datazone e fazer login com o Conta da AWS local onde o domínio foi criado e, em seguida, escolher Abrir portal de dados.
2. Escolha Procurar projeto no painel de navegação superior e selecione o projeto que contém o ambiente que você deseja excluir.
3. Localize e escolha o ambiente para abrir sua página de detalhes, expanda Ações e escolha Excluir ambiente.
4. Na janela pop-up Excluir ambiente, confirme a exclusão digitando `Delete` no campo e escolha Excluir ambiente.

   Você pode excluir com êxito um ambiente somente depois que todas as entidades com dependência desse ambiente tiverem sido excluídas. Para excluir um ambiente, você deve primeiro excluir todas as fontes de dados e destinos de assinatura associados.

Criar um novo projeto da

Na Amazon DataZone, os projetos permitem que um grupo de usuários colabore em vários casos de uso comercial que envolvem publicação, descoberta, assinatura e consumo de ativos de dados no catálogo da Amazon. DataZone Para ter mais informações, consulte DataZone Terminologia e conceitos da Amazon.

Qualquer DataZone usuário da Amazon com as permissões necessárias para acessar o portal de dados pode criar um DataZone projeto da Amazon.

Para criar um novo projeto, conclua as etapas a seguir.

1. Navegue até o URL do portal de DataZone dados da Amazon e faça login usando o single sign-on (SSO) ou suas credenciais. AWS Se você for DataZone administrador da Amazon, poderá navegar até o DataZone console da Amazon em https://console.aws.amazon.com/datazone e fazer login com o Conta da AWS local onde o domínio foi criado e, em seguida, escolher Abrir portal de dados.

2. No portal de DataZone dados da Amazon, escolha Create Project.
3. Especifique valores para os campos a seguir e escolha Criar projeto:

   - Nome — O nome do projeto.
   - Descrição — Uma descrição do projeto.

Editar projeto

Na Amazon DataZone, os projetos permitem que um grupo de usuários colabore em vários casos de uso comercial que envolvem publicação, descoberta, assinatura e consumo de ativos de dados no catálogo da Amazon. DataZone Para ter mais informações, consulte DataZone Terminologia e conceitos da Amazon. Para editar um DataZone projeto da Amazon, você deve ser o proprietário desse projeto ou o administrador do domínio que contém esse projeto.

Para editar um projeto existente, conclua as etapas a seguir.

1. Navegue até o URL do portal de DataZone dados da Amazon e faça login usando o single sign-on (SSO) ou suas credenciais. AWS Se você for DataZone administrador da Amazon, poderá navegar até o DataZone console da Amazon em https://console.aws.amazon.com/datazone e fazer login com o Conta da AWS local onde o domínio foi criado e, em seguida, escolher Abrir portal de dados.
2. Escolha Procurar projetos.
3. Escolha o projeto que você deseja editar. Se você não o vê facilmente na lista de projetos, pode pesquisá-lo especificando o nome do projeto no campo Localizar projeto.
4. Expanda Ações e escolha Editar projeto.
5. Atualize o nome e a descrição do projeto e escolha Salvar.

Excluir projeto

Na Amazon DataZone, os projetos permitem que um grupo de usuários colabore em vários casos de uso comercial que envolvem publicação, descoberta, assinatura e/ou consumo de ativos de dados no catálogo da Amazon. DataZone Para ter mais informações, consulte DataZone Terminologia e conceitos da Amazon.

O ato de excluir um projeto é definitivo. A exclusão exclui irrevogavelmente o conteúdo do projeto, incluindo fontes de dados, ambientes, ativos, glossários e formulários de metadados. A Amazon

DataZone revoga as concessões que a Amazon DataZone concedeu a ativos gerenciados por meio do Lake Formation e do Amazon Redshift. A exclusão de um projeto não exclui DataZone AWS recursos não pertencentes à Amazon que a Amazon DataZone possa ter ajudado você a criar. Se você não precisar mais desses AWS recursos, exclua-os em seus respectivos AWS serviços e contas.

Para excluir um DataZone projeto da Amazon, você deve ser proprietário do projeto.

Para excluir um projeto existente, conclua as etapas a seguir.

1. Navegue até o URL do portal de DataZone dados da Amazon e faça login usando o single sign-on (SSO) ou suas credenciais. AWS Um diretor do IAM pode navegar até o DataZone console da Amazon em https://console.aws.amazon.com/datazone e fazer login com o Conta da AWS local onde o domínio foi criado e, em seguida, escolher Open data portal.
2. Escolha Procurar projetos no painel de navegação superior.
3. Escolha o projeto que você deseja excluir. Se você não o encontrar na lista de projetos, poderá pesquisá-lo especificando o nome do projeto no campo Localizar projeto.
4. Expanda Ações e escolha Excluir projeto.

   Analise os avisos informativos sobre o impacto potencial da exclusão do projeto.
5. Se você aceitar os avisos, digite o texto de confirmação e escolha Excluir.

> **Important**
>
> Excluir um projeto é uma ação irrevogável que não pode ser desfeita por você ou por. AWS

> **Note**
>
> Quando você ou os usuários do seu domínio criam um ambiente em um projeto, a Amazon DataZone cria AWS recursos em seu domínio ou contas associadas para fornecer funcionalidade a você e aos usuários do seu domínio. Abaixo está a lista de AWS recursos que a Amazon DataZone pode criar para um projeto, junto com o nome padrão. A exclusão de um projeto não exclui nenhum desses AWS recursos em suas AWS contas.
>
> - <environmentId>Funções do IAM: datazone_usr_.

- <environmentName>Bancos de dados Glue: (1) <environmentName>_pub_db-*, (2) _sub_db-*. Se já existisse um banco de dados com esse nome, a Amazon DataZone adicionará o ID do ambiente.
- <environmentName>Grupos de trabalho do Athena: -*. Se já existisse um grupo de trabalho com esse nome, a Amazon DataZone adicionará o ID do ambiente.
- CloudWatch grupo de registros: datazone_ <environmentId>

Sair do projeto

Na Amazon DataZone, os projetos permitem que um grupo de usuários colabore em vários casos de uso comercial que envolvem publicação, descoberta, assinatura e consumo de ativos de dados no catálogo da Amazon. DataZone Para ter mais informações, consulte DataZone Terminologia e conceitos da Amazon.

Para deixar um projeto existente, conclua as etapas a seguir.

1. Navegue até o URL do portal de DataZone dados da Amazon e faça login usando o single sign-on (SSO) ou suas credenciais. AWS Se você for DataZone administrador da Amazon, poderá navegar até o DataZone console da Amazon em https://console.aws.amazon.com/datazone e fazer login com o Conta da AWS local onde o domínio foi criado e, em seguida, escolher Abrir portal de dados.
2. Escolha Selecionar projeto no painel de navegação superior e selecione o projeto.
3. Escolha o projeto do qual você deseja sair. Se você não o vê facilmente na lista de projetos, pode pesquisá-lo especificando o nome do projeto no campo Localizar projeto.
4. Expanda Ações e escolha Sair do projeto.

Adicionar membros a um projeto

Na Amazon DataZone, os projetos permitem que um grupo de usuários colabore em vários casos de uso comercial que envolvem publicação, descoberta, assinatura e consumo de ativos de dados no catálogo da Amazon. DataZone Para ter mais informações, consulte DataZone Terminologia e conceitos da Amazon.

Você deve ser proprietário ou colaborador do projeto para adicionar membros a um projeto. Você pode adicionar grupos de SSO, usuários de SSO ou diretores do IAM (funções ou usuários) como membros do projeto.

Para adicionar membros a um projeto existente, conclua as etapas a seguir.

1. Navegue até o URL do portal de DataZone dados da Amazon e faça login usando o single sign-on (SSO) ou suas credenciais. AWS Se você for DataZone administrador da Amazon, poderá navegar até o DataZone console da Amazon em https://console.aws.amazon.com/datazone e fazer login com o Conta da AWS local onde o domínio foi criado e, em seguida, escolher Abrir portal de dados.
2. Escolha Selecionar projeto no painel de navegação superior e selecione o projeto.
3. Escolha o projeto ao qual você deseja adicionar membros. Se você não o vê facilmente na lista de projetos, pode pesquisá-lo especificando o nome do projeto no campo Localizar projeto.
4. Na página de detalhes do projeto, selecione a guia Membros e escolha o nó Todos os membros.
5. Na guia Membros do projeto, escolha Adicionar membros.
6. Na janela pop-up Adicionar membros ao projeto, especifique o (s) usuário (s) que você deseja adicionar e especifique sua função no projeto (proprietário ou colaborador) e escolha Adicionar membros.

> **Note**
>
> Você pode adicionar um diretor do IAM como membro do projeto se esse diretor já tiver um perfil de DataZone usuário da Amazon no domínio. A Amazon cria DataZone automaticamente um perfil de usuário para um diretor do IAM quando ele interage com sucesso com o domínio por meio do portal, da API ou da CLI. Você não pode criar um perfil de usuário para um diretor do IAM. Para adicionar diretores do IAM como membros do projeto no caso de o diretor do IAM não ter um perfil de DataZone usuário da Amazon existente no domínio, peça ao administrador que adicione as duas permissões do IAM a seguir às do seu domínio AmazonDataZoneDomainExecutionRoleno console do IAM: `iam:GetUser` e. `iam:GetRole` Separadamente, para realizar ações no domínio, o diretor do IAM deve ter as permissões correspondentes do IAM para essas ações.

Remover membros de um projeto

Na Amazon DataZone, os projetos permitem que um grupo de usuários colabore em vários casos de uso comercial que envolvem publicação, descoberta, assinatura e consumo de ativos de dados no catálogo da Amazon. DataZone Para ter mais informações, consulte DataZone Terminologia e conceitos da Amazon. Você precisa ser proprietário de um projeto para remover membros de um projeto.

Para remover membros de um projeto existente, conclua as etapas a seguir.

1. Navegue até o portal de DataZone dados da Amazon usando a URL do portal de dados e faça login usando seu SSO ou suas AWS credenciais. Se você for DataZone administrador da Amazon, poderá obter a URL do portal de dados acessando o DataZone console da Amazon em https://console.aws.amazon.com/datazone na AWS conta em que o DataZone domínio da Amazon foi criado.
2. Escolha Selecionar projeto no painel de navegação superior e selecione o projeto.
3. Escolha o projeto do qual você deseja remover membros. Se você não o vê facilmente na lista de projetos, pode pesquisá-lo especificando o nome do projeto no campo Localizar projeto.
4. Na página de detalhes do projeto, selecione a guia Membros e escolha o nó Todos os membros.
5. Na guia Membros do projeto, escolha os membros que você deseja remover do projeto e, em seguida, escolha Remover.
6. Na janela pop-up Remover membros, confirme a remoção escolhendo Remover membros.

Criação de inventário e publicação de dados na Amazon DataZone

Esta seção descreve as tarefas e os procedimentos que você deseja realizar para criar um inventário de seus dados na Amazon DataZone e publicar seus dados na Amazon DataZone.

Para usar a Amazon DataZone para catalogar seus dados, você deve primeiro trazer seus dados (ativos) como inventário do seu projeto na Amazon DataZone. A criação de inventário para um projeto específico torna os ativos detectáveis somente para os membros desse projeto. Os ativos do inventário do projeto não estão disponíveis para todos os usuários do domínio na pesquisa/navegação, a menos que sejam publicados explicitamente. Depois de criar um inventário do projeto, os proprietários dos dados podem organizar seus ativos de inventário com os metadados comerciais necessários adicionando ou atualizando nomes comerciais (ativo e esquema), descrições (ativo e esquema), leia-me, termos do glossário (ativo e esquema) e formulários de metadados.

A próxima etapa de usar DataZone a Amazon para catalogar seus dados é fazer com que os ativos de inventário do seu projeto possam ser descobertos pelos usuários do domínio. Você pode fazer isso publicando os ativos de inventário no DataZone catálogo da Amazon. Somente a versão mais recente do ativo de inventário pode ser publicada no catálogo e somente a versão mais recente publicada está ativa no catálogo de descobertas. Se um ativo de inventário for atualizado após ser publicado no DataZone catálogo da Amazon, você deverá publicá-lo explicitamente novamente para que a versão mais recente esteja no catálogo de descobertas.

Tópicos

- Inicie manualmente uma fonte de dados executada na Amazon DataZone
- Revisões de ativos na Amazon DataZone
- Qualidade de dados na Amazon DataZone
- Usando aprendizado de máquina e IA generativa

Configurar as permissões do Lake Formation para a Amazon DataZone

Quando você cria um ambiente usando o data lake blueprint (DefaultDataLake) integrado, um banco de dados AWS Glue é adicionado na Amazon DataZone como parte do processo de criação desse ambiente. Se você quiser publicar ativos desse banco de dados AWS Glue, nenhuma permissão adicional será necessária.

No entanto, se você quiser publicar ativos e assinar ativos de um banco de dados AWS Glue que existe fora do seu DataZone ambiente Amazon, você deve fornecer explicitamente à Amazon DataZone as permissões para acessar tabelas nesse banco de dados externo do AWS Glue. Para fazer isso, você deve preencher as seguintes configurações no AWS Lake Formation e anexar as permissões necessárias do Lake Formation aoAmazonDataZoneGlueAccess- <region>- <domainId>.

- Configure a localização do Amazon S3 para seu data lake em AWS Lake Formation com o modo de permissão Lake Formation ou o modo de acesso híbrido. Para obter mais informações, consulte https://docs.aws.amazon.com/lake-formation/latest/dg/ register-data-lake .html.
- Remova a `IAMAllowedPrincipals` permissão das tabelas do Amazon Lake Formation para as quais a Amazon DataZone gerencia as permissões. Para obter mais informações, consulte https://docs.aws.amazon.com/lake-formation/latest/dg/ upgrade-glue-lake-formation -background.html.
- Anexe as seguintes permissões do AWS Lake Formation aoAmazonDataZoneGlueAccess-<region>- <domainId>:
  - `Describee Describe grantable` permissões no banco de dados em que as tabelas existem
  - `Describe`,`Select`,`Describe Grantable`, `Select Grantable` permissões em todas as tabelas no banco de dados acima às quais você DataZone deseja gerenciar o acesso em seu nome.

> **Note**
>
> A Amazon DataZone suporta o modo AWS Lake Formation Hybrid. O modo híbrido do Lake Formation permite que você comece a gerenciar permissões em seus bancos de dados e tabelas do AWS Glue por meio do Lake Formation, enquanto continua mantendo todas as permissões existentes do IAM nessas tabelas e bancos de dados. Para mais informações, consulte DataZone Integração da Amazon com o modo híbrido AWS Lake Formation .

Para ter mais informações, consulte Solução de problemas de permissões do AWS Lake Formation para a Amazon DataZone.

DataZone Integração da Amazon com o modo híbrido AWS Lake Formation

A Amazon DataZone está integrada ao modo híbrido AWS Lake Formation. Essa integração permite que você publique e compartilhe facilmente suas tabelas AWS Glue na Amazon DataZone sem a necessidade de registrá-las primeiro no AWS Lake Formation. O modo híbrido permite que você comece a gerenciar as permissões em suas tabelas do AWS Glue por meio do AWS Lake Formation e, ao mesmo tempo, continue mantendo todas as permissões existentes do IAM nessas tabelas.

Para começar, você pode ativar a configuração de registro de localização de dados sob o DefaultDataLakeesquema no console de DataZone gerenciamento da Amazon.

Habilite a integração com o modo híbrido AWS Lake Formation

1. Navegue até o DataZone console da Amazon em https://console.aws.amazon.com/datazone e faça login com as credenciais da sua conta.
2. Escolha Exibir domínios e escolha o domínio em que você deseja habilitar a integração com o modo híbrido AWS Lake Formation.
3. Na página de detalhes do domínio, navegue até a guia Blueprints.
4. Na lista Blueprints, escolha o DefaultDataLakeblueprint.
5. Certifique-se de que o DefaultDataLake blueprint esteja ativado. Se não estiver ativado, siga as etapas Habilite esquemas integrados na AWS conta que possui o domínio da Amazon DataZone para habilitá-lo em sua AWS conta.
6. Na página de DefaultDataLake detalhes, abra a guia Provisionamento e escolha o botão Editar no canto superior direito da página.

7. Em Registro de localização de dados, marque a caixa para habilitar o registro de localização de dados.
8. Para a função de gerenciamento de localização de dados, você pode criar uma nova função do IAM ou selecionar uma função existente do IAM. A Amazon DataZone usa essa função para gerenciar o acesso de leitura/gravação ao (s) bucket (s) Amazon S3 escolhido (s) para Data Lake usando o modo de acesso híbrido Lake AWS Formation. Para ter mais informações, consulte AmazonDataZone<region>S3 Manage- - <domainId>.
9. Opcionalmente, você pode optar por excluir determinados locais do Amazon S3 se não quiser que a DataZone Amazon os registre automaticamente no modo híbrido. Para isso, conclua as seguintes etapas:

   - Escolha o botão de alternância para excluir locais específicos do Amazon S3.
   - Forneça o URI do bucket do Amazon S3 que você deseja excluir.
   - Para adicionar mais buckets, escolha Adicionar localização do S3.

   > **Note**
   >
   > A Amazon DataZone só permite excluir uma localização raiz do S3. Qualquer localização do S3 dentro do caminho de uma localização raiz do S3 será automaticamente excluída do registro.

   - Escolha Salvar alterações.

Depois de ativar a configuração de registro de localização de dados em sua AWS conta, quando um consumidor de dados se inscrever em uma tabela AWS Glue gerenciada por meio de permissões do IAM, a Amazon primeiro DataZone registrará as localizações dessa tabela no Amazon S3 no modo híbrido e, em seguida, concederá acesso ao consumidor de dados gerenciando as permissões na tabela por meio do Lake AWS Formation. Isso garante que as permissões do IAM na tabela continuem existindo com as permissões recém-concedidas do AWS Lake Formation, sem interromper os fluxos de trabalho existentes.

Como lidar com locais criptografados do Amazon S3 ao habilitar a integração do modo híbrido AWS Lake Formation na Amazon DataZone

Se você estiver usando uma localização do Amazon S3 criptografada com uma chave KMS gerenciada ou AWS gerenciada pelo cliente, a função AmazonDataZoneS3Manage deve ter a

permissão para criptografar e descriptografar dados com a chave KMS, ou a política da chave KMS deve conceder permissões sobre a chave da função.

Se sua localização no Amazon S3 estiver criptografada com uma chave AWS gerenciada, adicione a seguinte política em linha à função: AmazonDataZoneDataLocationManagement

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

Se sua localização no Amazon S3 estiver criptografada com uma chave gerenciada pelo cliente, faça o seguinte:

1. Abra o console AWS KMS em https://console.aws.amazon.com/kms e faça login como usuário administrativo do AWS Identity and Access Management (IAM) ou como um usuário que pode modificar a política de chaves da chave KMS usada para criptografar o local.
2. No painel de navegação, selecione Chaves gerenciadas pelo cliente e selecione o nome da chave do KMS desejada.
3. Na página de detalhes da chave KMS, escolha a guia Política de chaves e, em seguida, faça o seguinte para adicionar sua função personalizada ou a função vinculada ao serviço Lake Formation como usuário da chave KMS:

   - Se a exibição padrão estiver sendo exibida (com as seções Administradores de chaves, Exclusão de chaves, Usuários principais e Outras AWS contas), na seção Usuários principais, adicione a AmazonDataZoneDataLocationManagementfunção.

- Se a política de chaves (JSON) estiver sendo exibida, edite a política para adicionar uma AmazonDataZoneDataLocationManagementfunção ao objeto “Permitir o uso da chave”, conforme mostrado no exemplo a seguir

```
...
        {
            "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**
>
> Se a chave KMS ou a localização do Amazon S3 não estiverem na AWS mesma conta do catálogo de dados, siga as instruções em Registro de uma localização criptografada do Amazon S3 em todas as contas. AWS

Crie tipos de ativos personalizados

Na Amazon DataZone, os ativos representam tipos específicos de recursos de dados, como tabelas de banco de dados, painéis ou modelos de aprendizado de máquina. Para fornecer consistência e

padronização ao descrever os ativos do catálogo, um DataZone domínio da Amazon deve ter um conjunto de tipos de ativos que definam como os ativos são representados no catálogo. Um tipo de ativo define o esquema para um tipo específico de ativo. Um tipo de ativo tem um conjunto de tipos de formulários de metadados nomeáveis obrigatórios e opcionais (por exemplo, GovForm ou). GovernanceFormType Os tipos de ativos na Amazon DataZone são versionados. Quando os ativos são criados, eles são validados de acordo com o esquema definido pelo tipo de ativo (geralmente a versão mais recente) e, se uma estrutura inválida for especificada, a criação do ativo falhará.

Tipos de ativos do sistema - A Amazon DataZone provisiona tipos de ativos do sistema de propriedade do serviço (incluindo GlueTableAssetType GlueViewAssetType RedshiftTableAssetType, RedshiftViewAssetType,, e S3ObjectCollectionAssetType) e tipos de formulários do sistema (incluindo DataSourceReferenceFormType AssetCommonDetailsFormType, e). SubscriptionTermsFormType Os tipos de ativos do sistema não podem ser editados.

Tipos de ativos personalizados - para criar tipos de ativos personalizados, você começa criando os tipos de formulários de metadados e glossários necessários para usar nos tipos de formulário. Em seguida, você pode criar tipos de ativos personalizados especificando o nome, a descrição e os formulários de metadados associados, que podem ser obrigatórios ou opcionais.

Para tipos de ativos com dados estruturados, para representar o esquema da coluna no portal de dados, você pode usar o `RelationalTableFormType` para adicionar os metadados técnicos às suas colunas (incluindo nomes de colunas, descrições e tipos de dados) e o `ColumnBusinessMetadataForm` para adicionar as descrições comerciais das colunas, incluindo nomes comerciais, termos do glossário e pares de valores-chave personalizados.

Para criar um tipo de ativo personalizado por meio do portal de dados, conclua as seguintes etapas:

1. Navegue até o URL do portal de DataZone dados da Amazon e faça login usando o single sign-on (SSO) ou suas credenciais. AWS Se você for DataZone administrador da Amazon, poderá navegar até o DataZone console da Amazon em https://console.aws.amazon.com/datazone e fazer login com o Conta da AWS local onde o domínio foi criado e, em seguida, escolher Abrir portal de dados.
2. Escolha Selecionar projeto no painel de navegação superior e selecione o projeto em que você deseja criar um tipo de ativo personalizado.
3. Navegue até a guia Dados do projeto.
4. Escolha Tipos de ativos no painel de navegação esquerdo e, em seguida, escolha Criar tipo de ativo.
5. Especifique o seguinte e escolha Criar.

- Nome - o nome do tipo de ativo personalizado
- Descrição - a descrição do tipo de ativo personalizado.
- Escolha Adicionar formulários de metadados para adicionar formulários de metadados a esse tipo de ativo personalizado.

6. Depois que o tipo de ativo personalizado for criado, você poderá usá-lo para criar ativos.

Para criar um tipo de ativo personalizado por meio das APIs, conclua as seguintes etapas:

1. Crie um tipo de formulário de metadados invocando a ação da `CreateFormType` API.

   Veja a seguir um SageMaker exemplo da 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. Em seguida, você pode criar um tipo de ativo invocando a ação da `CreateAssetType` API. Você pode criar tipos de ativos somente por meio das DataZone APIs da Amazon usando os tipos de formulários do sistema disponíveis (`SubscriptionTermsFormType`no exemplo

abaixo) ou seus tipos de formulários personalizados. Para tipos de formulário do sistema, o nome do tipo deve começar com`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,
        },
    },
)
```

Veja a seguir um exemplo de criação de um tipo de ativo para dados estruturados:

```
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. E agora, você pode criar um ativo usando os tipos de ativos personalizados que você criou nas etapas acima.

```
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}"
        }
        ]
)
```

E neste exemplo, você está criando um ativo de dados estruturado:

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

Crie e execute uma fonte de DataZone dados da Amazon para o AWS Glue Data Catalog

Na Amazon DataZone, você pode criar uma fonte de AWS Glue Data Catalog dados para importar metadados técnicos das tabelas do banco de dados. AWS Glue Para adicionar uma fonte de dados para o AWS Glue Data Catalog, o banco de dados de origem já deve existir em AWS Glue.

Ao criar e executar uma fonte de AWS Glue dados, você adiciona ativos do AWS Glue banco de dados de origem ao inventário do seu DataZone projeto na Amazon. Você pode executar suas fontes de AWS Glue dados em um cronograma definido ou sob demanda para criar ou atualizar os metadados técnicos de seus ativos. Durante a execução da fonte de dados, você pode optar por publicar seus ativos no DataZone catálogo da Amazon e, assim, torná-los detectáveis por todos os usuários do domínio. Você também pode publicar os ativos do inventário do projeto depois de editar os metadados comerciais. Os usuários do domínio podem pesquisar e descobrir seus ativos publicados e solicitar assinaturas desses ativos.

Para adicionar uma fonte AWS Glue de dados

1. Navegue até o URL do portal de DataZone dados da Amazon e faça login usando o single sign-on (SSO) ou suas credenciais. AWS Se você for DataZone administrador da Amazon, poderá navegar até o DataZone console da Amazon em https://console.aws.amazon.com/datazone e fazer login com o Conta da AWS local onde o domínio foi criado e, em seguida, escolher Abrir portal de dados.
2. Escolha Selecionar projeto no painel de navegação superior e selecione o projeto ao qual você deseja adicionar a fonte de dados.
3. Navegue até a guia Dados do projeto.
4. Escolha Fontes de dados no painel de navegação esquerdo e escolha Criar fonte de dados.
5. Configure os campos a seguir.
   - Nome — O nome da fonte de dados.
   - Descrição — A descrição da fonte de dados.
6. Em Tipo de fonte de dados, escolha AWS Glue.
7. Em Selecionar um ambiente, especifique um ambiente no qual publicar as AWS Glue tabelas.
8. Em Seleção de dados, forneça um AWS Glue banco de dados e insira seus critérios de seleção de tabela. Por exemplo, se você escolher Incluir e inserir`*corporate`, o banco de dados incluirá todas as tabelas de origem que terminam com a palavra`corporate`.

   Você pode escolher um AWS Glue banco de dados no menu suspenso ou digitar o nome do banco de dados. O menu suspenso inclui dois bancos de dados: o banco de dados de publicação e o banco de dados de assinaturas do ambiente. Se você quiser trazer ativos de um banco de dados que não foi criado pelo ambiente, digite o nome do banco de dados em vez de selecioná-lo no menu suspenso.

   Você pode adicionar várias regras de inclusão e exclusão para tabelas em um único banco de dados. Você também pode adicionar vários bancos de dados usando o botão Adicionar outro banco de dados.

9. Em Qualidade dos dados, você pode escolher Habilitar a qualidade dos dados para essa fonte de dados. Se você fizer isso, a Amazon DataZone importará sua saída existente de qualidade de dados do AWS Glue para o seu DataZone catálogo da Amazon. Por padrão, a Amazon DataZone importa os 100 relatórios de qualidade mais recentes existentes sem data de expiração do AWS Glue.

As métricas de qualidade de dados na Amazon DataZone ajudam você a entender a integridade e a precisão de suas fontes de dados. A Amazon DataZone extrai essas métricas de qualidade de dados do AWS Glue para fornecer contexto em um determinado momento, por exemplo, durante uma pesquisa no catálogo de dados corporativos. Os usuários de dados podem ver como as métricas de qualidade de dados mudam com o tempo para seus ativos inscritos. Os produtores de dados podem ingerir as pontuações de qualidade de dados do AWS Glue de acordo com um cronograma. O catálogo de dados DataZone comerciais da Amazon também pode exibir métricas de qualidade de dados de sistemas de terceiros por meio de APIs de qualidade de dados. Para mais informações, consulte Qualidade de dados na Amazon DataZone.

10. Escolha Próximo.
11. Em Configurações de publicação, escolha se os ativos podem ser imediatamente descobertos no catálogo de dados corporativos. Se você adicioná-los apenas ao inventário, poderá escolher os termos de assinatura posteriormente e publicá-los no catálogo de dados corporativos. Para ter mais informações, consulte the section called “Gerencie fontes de dados existentes”.
12. Para Geração automatizada de nomes comerciais, escolha se deseja gerar automaticamente metadados para ativos à medida que eles são importados da fonte.
13. (Opcional) Para formulários de metadados, adicione formulários para definir os metadados que são coletados e salvos quando os ativos são importados para a Amazon. DataZone Para ter mais informações, consulte the section called “Crie, edite ou exclua formulários de metadados”.
14. Em Preferência de execução, escolha quando executar a fonte de dados.
    - Executar de acordo com um cronograma — especifique as datas e a hora de execução da fonte de dados.
    - Executar sob demanda — você pode iniciar manualmente as execuções da fonte de dados.
15. Escolha Próximo.
16. Revise a configuração da fonte de dados e escolha Criar.

Crie e execute uma fonte de DataZone dados da Amazon para o Amazon Redshift

Na Amazon DataZone, você pode criar uma fonte de dados do Amazon Redshift para importar metadados técnicos de tabelas e visualizações do banco de dados do armazém de dados do

Amazon Redshift. Para adicionar uma fonte de DataZone dados da Amazon para o Amazon Redshift, o data warehouse de origem já deve existir no Amazon Redshift.

Ao criar e executar uma fonte de dados do Amazon Redshift, você adiciona ativos do armazém de dados de origem do Amazon Redshift ao inventário do seu projeto da DataZone Amazon. Você pode executar suas fontes de dados do Amazon Redshift em um cronograma definido ou sob demanda para criar ou atualizar os metadados técnicos de seus ativos. Durante a execução da fonte de dados, você pode optar por publicar os ativos do inventário do projeto no DataZone catálogo da Amazon e, assim, torná-los detectáveis por todos os usuários do domínio. Você também pode publicar seus ativos de inventário depois de editar seus metadados comerciais. Os usuários do domínio podem pesquisar e descobrir seus ativos publicados e solicitar assinaturas desses ativos.

Para adicionar uma fonte de dados do Amazon Redshift

1. Navegue até o URL do portal de DataZone dados da Amazon e faça login usando o single sign-on (SSO) ou suas credenciais. AWS Se você for DataZone administrador da Amazon, poderá navegar até o DataZone console da Amazon em https://console.aws.amazon.com/datazone e fazer login com o Conta da AWS local onde o domínio foi criado e, em seguida, escolher Abrir portal de dados.
2. Escolha Selecionar projeto no painel de navegação superior e selecione o projeto ao qual você deseja adicionar a fonte de dados.
3. Navegue até a guia Dados do projeto.
4. Escolha Fontes de dados no painel de navegação esquerdo e escolha Criar fonte de dados.
5. Configure os campos a seguir.

   - Nome — O nome da fonte de dados.
   - Descrição — A descrição da fonte de dados.
6. Em Tipo de fonte de dados, escolha Amazon Redshift.
7. Em Selecionar um ambiente, especifique um ambiente no qual publicar as tabelas do Amazon Redshift.
8. Dependendo do ambiente selecionado, a Amazon DataZone aplicará automaticamente as credenciais do Amazon Redshift e outros parâmetros diretamente do ambiente ou oferecerá a opção de escolher o seu.

   - Se você selecionou um ambiente que só permite a publicação a partir do esquema padrão do Amazon Redshift do ambiente, a Amazon DataZone aplicará automaticamente as credenciais do Amazon Redshift e outros parâmetros, incluindo o nome do cluster ou grupo de trabalho,

segredo, AWS nome do banco de dados e nome do esquema do Amazon Redshift. Você não pode editar esses parâmetros preenchidos automaticamente.

- Se você selecionar um ambiente que não permita a publicação de dados, não poderá continuar com a criação da fonte de dados.
- Se você selecionar um ambiente que permita a publicação de dados de qualquer esquema, você verá a opção de usar as credenciais e outros parâmetros do Amazon Redshift do ambiente ou inserir suas próprias credenciais/parâmetros.

9. Se você optar por usar suas próprias credenciais para criar a fonte de dados, forneça os seguintes detalhes:

   - Em Fornecer credenciais do Amazon Redshift, escolha se deseja usar um cluster provisionado do Amazon Redshift ou um espaço de trabalho Amazon Redshift Serverless como sua fonte de dados.
   - Dependendo da sua seleção na etapa acima, escolha seu cluster ou espaço de trabalho do Amazon Redshift no menu suspenso e, em seguida, escolha o segredo no Secrets Manager a ser usado para AWS autenticação. Você pode escolher um segredo existente ou criar um novo.
   - Para que o segredo existente apareça no menu suspenso, certifique-se de que seu segredo no AWS Secrets Manager inclua as seguintes tags (chave/valor):
     - AmazonDataZoneProject: <projectID>
     - AmazonDataZoneDomain: <domainID>

     Se você optar por criar um novo segredo, o segredo será automaticamente marcado com as tags mencionadas acima e nenhuma etapa extra será necessária. Para obter mais informações, consulte Armazenamento de credenciais de banco de dados em AWS Secrets Manager.

     Os usuários do Amazon Redshift no AWS segredo fornecido para criar a fonte de dados devem ter `SELECT` permissões nas tabelas que serão publicadas. Se você quiser que DataZone a Amazon também gerencie as assinaturas (acesso) em seu nome, os usuários do banco de dados no AWS segredo também devem ter as seguintes permissões:

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

10. Em Seleção de dados, forneça um banco de dados e um esquema do Amazon Redshift e insira seus critérios de seleção de tabela ou visualização. Por exemplo, se você escolher Incluir e inserir`*corporate`, o ativo incluirá todas as tabelas de origem que terminam com a palavra`corporate`.

    Você pode adicionar várias regras de inclusão para tabelas em um único banco de dados. Você também pode adicionar vários bancos de dados usando o botão Adicionar outro banco de dados.
11. Escolha Próximo.
12. Em Configurações de publicação, escolha se os ativos podem ser imediatamente descobertos no catálogo de dados. Se você adicioná-los apenas ao inventário, poderá escolher os termos de assinatura posteriormente e publicá-los no catálogo de dados corporativos. Para ter mais informações, consulte the section called “Gerencie fontes de dados existentes”.
13. Para Geração automatizada de nomes comerciais, escolha se deseja gerar automaticamente metadados para ativos à medida que eles são publicados e atualizados a partir da fonte.
14. (Opcional) Para formulários de metadados, adicione formulários para definir os metadados que são coletados e salvos quando os ativos são importados para a Amazon. DataZone Para ter mais informações, consulte the section called “Crie, edite ou exclua formulários de metadados”.
15. Em Preferência de execução, escolha quando executar a fonte de dados.

    - Executar de acordo com um cronograma — especifique as datas e a hora de execução da fonte de dados.
    - Executar sob demanda — você pode iniciar manualmente as execuções da fonte de dados.
16. Escolha Próximo.
17. Revise a configuração da fonte de dados e escolha Criar.

Gerencie fontes de DataZone dados existentes da Amazon

Depois de criar uma fonte de DataZone dados da Amazon, você pode modificá-la a qualquer momento para alterar os detalhes da fonte ou os critérios de seleção de dados. Quando você não precisar mais de uma fonte de dados, poderá excluí-la.

Para concluir essas etapas, você deve ter a política AmazonDataZoneFullAccess AWS gerenciada anexada. Para ter mais informações, consulte the section called “AWS políticas gerenciadas”.

Tópicos

Editar uma fonte de dados

Você pode editar uma fonte de DataZone dados da Amazon para modificar suas configurações de seleção de dados, incluindo adicionar, remover ou alterar os critérios de seleção da tabela. Você também pode adicionar e remover bancos de dados. Você não pode alterar o tipo de fonte de dados ou o ambiente no qual uma fonte de dados é publicada.

Como editar uma fonte de dados

1. Navegue até o URL do portal de DataZone dados da Amazon e faça login usando o single sign-on (SSO) ou suas credenciais. AWS Se você for DataZone administrador da Amazon, poderá navegar até o DataZone console da Amazon em https://console.aws.amazon.com/datazone e fazer login com o Conta da AWS local onde o domínio foi criado e, em seguida, escolher Abrir portal de dados.
2. Escolha Selecionar projeto no painel de navegação superior e selecione o projeto ao qual a fonte de dados pertence.
3. Navegue até a guia Dados do projeto.
4. Escolha Fontes de dados no painel de navegação esquerdo e escolha a fonte de dados que você deseja modificar.
5. Navegue até a guia Definição da fonte de dados e escolha Editar.
6. Faça suas alterações na definição da fonte de dados. Você pode atualizar os detalhes da fonte de dados e fazer alterações nos critérios de seleção de dados.
7. Quando terminar de fazer as alterações, selecione Salvar.

Excluir uma fonte de dados

Quando você não precisar mais de uma fonte DataZone de dados da Amazon, poderá removê-la permanentemente. Depois de excluir uma fonte de dados, todos os ativos originados dessa fonte de dados ainda estarão disponíveis no catálogo e os usuários ainda poderão se inscrever neles. No entanto, os ativos deixarão de receber atualizações da fonte. Recomendamos que você primeiro mova os ativos dependentes para uma fonte de dados diferente antes de excluí-los.

> **Note**
>
> Você deve remover todos os processamentos na fonte de dados antes de excluí-la. Para ter mais informações, consulte Descobrindo, assinando e consumindo dados na Amazon DataZone.

Como excluir uma fonte de dados

1. Na guia Dados do projeto, escolha Fontes de dados no painel de navegação esquerdo.
2. Escolha a fonte de dados que você deseja excluir.
3. Escolha Ações, Excluir fonte de dados e confirme a exclusão.

Publique ativos no DataZone catálogo da Amazon a partir do inventário do projeto

Você pode publicar DataZone ativos da Amazon e seus metadados dos inventários do projeto no catálogo da Amazon DataZone . Você só pode publicar a versão mais recente de um ativo no catálogo.

Considere o seguinte ao publicar ativos no catálogo:

- Para publicar um ativo no catálogo, você deve ser o proprietário ou colaborador desse projeto.
- Para ativos do Amazon Redshift, certifique-se de que os clusters do Amazon Redshift associados aos clusters do editor e do assinante atendam a todos os requisitos de compartilhamento de dados do Amazon Redshift para que a Amazon gerencie o acesso às tabelas e visualizações DataZone do Redshift. Consulte Conceitos de compartilhamento de dados para o Amazon Redshift.
- A Amazon DataZone só oferece suporte ao gerenciamento de acesso para ativos publicados no AWS Glue Data Catalog e no Amazon Redshift. Para todos os outros ativos, como objetos do Amazon S3, a Amazon DataZone não gerencia o acesso para assinantes aprovados. Se você assinar esses ativos não gerenciados, será notificado com a seguinte mensagem:

  ```
  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.
  ```

Publicar um ativo

Se você não optou por tornar os ativos imediatamente detectáveis no catálogo de dados ao criar uma fonte de dados, execute as etapas a seguir para publicá-los posteriormente.

Para publicar um ativo

1. Navegue até o URL do portal de DataZone dados da Amazon e faça login usando o single sign-on (SSO) ou suas credenciais. AWS Se você for DataZone administrador da Amazon, poderá navegar até o DataZone console da Amazon em https://console.aws.amazon.com/datazone e fazer login com o Conta da AWS local onde o domínio foi criado e, em seguida, escolher Abrir portal de dados.
2. Escolha Selecionar projeto no painel de navegação superior e selecione o projeto ao qual o ativo pertence.
3. Navegue até a guia Dados do projeto.
4. Escolha Dados de inventário no painel de navegação esquerdo e selecione o ativo que você deseja publicar.

   > **Note**
   >
   > Por padrão, todos os ativos exigem a aprovação da assinatura, o que significa que o proprietário dos dados deve aprovar todas as solicitações de assinatura do ativo. Se você quiser alterar essa configuração antes de publicar o ativo, abra os detalhes do ativo e escolha Editar ao lado de Aprovação da assinatura. Você pode alterar essa configuração posteriormente modificando e republicando o ativo.

5. Escolha Publicar ativo. O ativo é publicado diretamente no catálogo.

   Se você fizer alterações no ativo, como modificar seus requisitos de aprovação, poderá escolher Republicar para publicar as atualizações no catálogo.

Gerencie o inventário e faça a curadoria de ativos

Para usar a Amazon DataZone para catalogar seus dados, você deve primeiro trazer seus dados (ativos) como inventário do seu projeto na Amazon DataZone. A criação de inventário para um projeto específico torna os ativos detectáveis somente para os membros desse projeto.

Depois que os ativos são criados no inventário do projeto, seus metadados podem ser selecionados. Por exemplo, você pode editar o nome e a descrição do ativo ou me ler. Cada edição no ativo cria uma nova versão do ativo. Você pode usar a guia Histórico na página de detalhes do ativo para visualizar todas as versões do ativo.

Você pode editar a seção Leia-me e adicionar descrições detalhadas para o ativo. A seção Leia-me oferece suporte ao markdown, permitindo que você formate suas descrições conforme necessário e descreva as principais informações sobre um ativo para os consumidores.

Os termos do glossário podem ser adicionados no nível do ativo preenchendo os formulários disponíveis.

Para organizar o esquema, você pode revisar as colunas, adicionar nomes comerciais, descrições e adicionar termos do glossário no nível da coluna.

Se a geração automatizada de metadados for ativada quando a fonte de dados for criada, os nomes comerciais dos ativos e das colunas estarão disponíveis para análise e aceitação ou rejeição individualmente ou de uma só vez.

Você também pode editar os termos da assinatura para especificar se a aprovação do ativo é necessária ou não.

Os formulários de metadados na Amazon DataZone permitem que você estenda o modelo de metadados de um ativo de dados adicionando atributos personalizados (por exemplo, região de vendas, ano de vendas e trimestre de vendas). Os formulários de metadados anexados a um tipo de ativo são aplicados a todos os ativos criados a partir desse tipo de ativo. Você também pode adicionar outros formulários de metadados a ativos individuais como parte da execução da fonte de dados ou após sua criação. Para criar novos formulários, consultethe section called “Crie, edite ou exclua formulários de metadados”.

Para atualizar os metadados de um ativo, você deve ser o proprietário ou colaborador do projeto ao qual o ativo pertence.

Para atualizar os metadados de um ativo

1. Navegue até o URL do portal de DataZone dados da Amazon e faça login usando o single sign-on (SSO) ou suas credenciais. AWS Se você for DataZone administrador da Amazon, poderá navegar até o DataZone console da Amazon em https://console.aws.amazon.com/datazone e fazer login com o Conta da AWS local onde o domínio foi criado e, em seguida, escolher Abrir portal de dados.

2. Escolha Selecionar projeto no painel de navegação superior e selecione o projeto que contém o ativo cujos metadados você deseja atualizar.
3. Navegue até a guia Dados do projeto.
4. Escolha Dados do inventário no painel de navegação esquerdo e, em seguida, escolha o nome do ativo cujos metadados você deseja atualizar.
5. Na página de detalhes do ativo, em Formulários de metadados, escolha Editar e edite os formulários existentes conforme necessário. Você também pode anexar formulários de metadados adicionais ao ativo. Para ter mais informações, consulte the section called “Anexe formulários de metadados adicionais aos ativos”.
6. Quando terminar de fazer as atualizações, escolha Salvar formulário.

   Quando você salva o formulário, a Amazon DataZone gera uma nova versão de inventário do ativo. Para publicar a versão atualizada no catálogo, escolha Republicar ativo.

Anexe formulários de metadados adicionais aos ativos

Por padrão, os formulários de metadados anexados a um domínio são anexados a todos os ativos publicados nesse domínio. Os editores de dados podem associar formulários de metadados adicionais a ativos individuais para fornecer contexto adicional.

Para anexar formulários de metadados adicionais a um ativo

1. Navegue até o URL do portal de DataZone dados da Amazon e faça login usando o single sign-on (SSO) ou suas credenciais. AWS Se você for DataZone administrador da Amazon, poderá navegar até o DataZone console da Amazon em https://console.aws.amazon.com/datazone e fazer login com o Conta da AWS local onde o domínio foi criado e, em seguida, escolher Abrir portal de dados.
2. Escolha Selecionar projeto no painel de navegação superior e selecione o projeto que contém o ativo cujos metadados você deseja adicionar.
3. Navegue até a guia Dados do projeto.
4. Escolha Dados do inventário no painel de navegação esquerdo e, em seguida, escolha o nome do ativo cujos metadados você deseja adicionar.
5. Na página de detalhes do ativo, em Formulários de metadados, escolha Adicionar formulários.
6. Selecione os formulários a serem adicionados ao ativo e escolha Adicionar formulários.
7. Insira valores para cada um dos campos de metadados e escolha Salvar formulário.

Quando você salva o formulário, a Amazon DataZone gera uma nova versão de inventário do ativo. Para publicar a versão atualizada no catálogo, escolha Republicar ativo.

Publique o ativo no catálogo após a curadoria

Quando estiver satisfeito com a curadoria de ativos, o proprietário dos dados pode publicar uma versão do ativo no DataZone catálogo da Amazon e, assim, torná-la detectável por todos os usuários do domínio. O ativo mostra a versão do inventário e a versão publicada. No catálogo de descobertas, somente a versão mais recente publicada aparece. Se os metadados forem atualizados após a publicação, uma nova versão do inventário estará disponível para publicação no catálogo.

Crie manualmente um ativo

Na Amazon DataZone, um ativo é uma entidade que apresenta um único objeto de dados físicos (por exemplo, uma tabela, um painel, um arquivo) ou um objeto de dados virtual (por exemplo, uma visualização). Para ter mais informações, consulte DataZone Terminologia e conceitos da Amazon. A publicação manual de um ativo é uma operação única. Você não especifica um cronograma de execução para o ativo, portanto, ele não é atualizado automaticamente se sua fonte mudar.

Para criar manualmente um ativo por meio de um projeto, você deve ser o proprietário ou colaborador desse projeto.

Para criar um ativo manualmente

1. Navegue até o URL do portal de DataZone dados da Amazon e faça login usando o single sign-on (SSO) ou suas credenciais. AWS Se você for DataZone administrador da Amazon, poderá navegar até o DataZone console da Amazon em https://console.aws.amazon.com/datazone e fazer login com o Conta da AWS local onde o domínio foi criado e, em seguida, escolher Abrir portal de dados.
2. Escolha Selecionar projeto no painel de navegação superior e selecione o projeto no qual criar o ativo.
3. Navegue até a guia Dados do projeto.
4. Escolha Fontes de dados no painel de navegação esquerdo e escolha Criar ativo de dados.
5. Para obter detalhes do ativo, defina as seguintes configurações:

   - Tipo de ativo — O tipo de ativo.

- Nome — O nome do ativo.
- Descrição — Uma descrição do ativo.

6. Para a localização do S3, insira o Amazon Resource Name (ARN) do bucket do S3 de origem.

   Opcionalmente, insira um ponto de acesso S3. Para obter mais informações, consulte Gerenciar o acesso a dados com pontos de acesso do Amazon S3.

7. Em Configurações de publicação, escolha se os ativos podem ser imediatamente descobertos no catálogo. Se você adicioná-los apenas ao inventário, poderá escolher os termos da assinatura posteriormente para publicá-los no catálogo.
8. Escolha Criar.

   Depois que o ativo for criado, ele será publicado diretamente como ativo no catálogo ou será armazenado no inventário até que você decida publicá-lo.

Cancelar a publicação de um ativo do catálogo da Amazon DataZone

Quando você cancela a publicação de um DataZone ativo da Amazon no catálogo, ele não aparece mais nos resultados de pesquisa global. Novos usuários não conseguirão encontrar ou assinar a lista de ativos no catálogo, mas todas as assinaturas existentes permanecerão as mesmas.

Para cancelar a publicação de um ativo, você deve ser o proprietário ou colaborador do projeto ao qual o ativo pertence:

Para cancelar a publicação de um ativo

1. Navegue até o URL do portal de DataZone dados da Amazon e faça login usando o single sign-on (SSO) ou suas credenciais. AWS Se você for DataZone administrador da Amazon, poderá navegar até o DataZone console da Amazon em https://console.aws.amazon.com/datazone e fazer login com o Conta da AWS local onde o domínio foi criado e, em seguida, escolher Abrir portal de dados.
2. Escolha Selecionar projeto no painel de navegação superior e selecione o projeto ao qual o ativo pertence.
3. Navegue até a guia Dados do projeto.
4. Escolha Dados publicados no painel de navegação esquerdo.

5. Localize o ativo na lista de ativos publicados e escolha Cancelar publicação.

   O ativo é removido do catálogo. Você pode republicar o ativo a qualquer momento escolhendo Publicar.

Excluir um DataZone ativo da Amazon

Quando você não precisar mais de um ativo na Amazon DataZone, poderá excluí-lo permanentemente. Excluir um ativo é diferente de cancelar a publicação de um ativo do catálogo. Você pode excluir um ativo e sua listagem relacionada no catálogo para que ele não fique visível em nenhum resultado da pesquisa. Para excluir a listagem de ativos, primeiro você deve revogar todas as assinaturas.

Para excluir um ativo, você deve ser o proprietário ou colaborador do projeto ao qual o ativo pertence:

> **Note**
>
> Para excluir uma listagem de ativos, primeiro você deve revogar todas as assinaturas existentes do ativo. Você não pode excluir uma listagem de ativos que tenha assinantes existentes.

Para excluir um ativo

1. Navegue até o URL do portal de DataZone dados da Amazon e faça login usando o single sign-on (SSO) ou suas credenciais. AWS Se você for DataZone administrador da Amazon, poderá navegar até o DataZone console da Amazon em https://console.aws.amazon.com/datazone e fazer login com o Conta da AWS local onde o domínio foi criado e, em seguida, escolher Abrir portal de dados.
2. Escolha Selecionar projeto no painel de navegação superior e selecione o projeto que contém o ativo que você deseja excluir.
3. Navegue até a guia Dados do projeto.
4. Escolha Dados publicados no painel de navegação esquerdo e, em seguida, localize e escolha o ativo que você deseja excluir. Isso abre a página de detalhes do ativo.
5. Escolha Ações, Excluir e confirme a exclusão.

Depois que o ativo é excluído, ele não está mais disponível para visualização e os usuários não podem se inscrever nele.

Inicie manualmente uma fonte de dados executada na Amazon DataZone

Quando você executa uma fonte de dados, a Amazon DataZone extrai todos os metadados novos ou modificados da fonte e atualiza os ativos associados no inventário. Ao adicionar uma fonte de dados à Amazon DataZone, você especifica a preferência de execução da fonte, que define se a fonte é executada de acordo com um cronograma ou sob demanda. Se sua fonte for executada sob demanda, você deverá iniciar a execução de uma fonte de dados manualmente.

Mesmo que sua fonte seja executada de acordo com um cronograma, você ainda pode executá-la manualmente a qualquer momento. Depois de adicionar metadados comerciais aos ativos, você pode selecionar ativos e publicá-los no DataZone catálogo da Amazon para que esses ativos possam ser descobertos por todos os usuários do domínio. Somente ativos publicados podem ser pesquisados por outros usuários do domínio.

Para executar uma fonte de dados manualmente

1. Navegue até o URL do portal de DataZone dados da Amazon e faça login usando o single sign-on (SSO) ou suas credenciais. AWS Se você for DataZone administrador da Amazon, poderá navegar até o DataZone console da Amazon em https://console.aws.amazon.com/datazone e fazer login com o Conta da AWS local onde o domínio foi criado e, em seguida, escolher Abrir portal de dados.
2. Escolha Selecionar projeto no painel de navegação superior e selecione o projeto ao qual a fonte de dados pertence.
3. Navegue até a guia Dados do projeto.
4. Escolha Fontes de dados no painel de navegação esquerdo e, em seguida, localize e escolha a fonte de dados que você deseja executar. Isso abre a página de detalhes da fonte de dados.
5. Escolha Executar sob demanda.

   O status da fonte de dados muda para `Running` quando a Amazon DataZone atualiza os metadados do ativo com os dados mais recentes da fonte. Você pode monitorar o status da execução na guia Execuções da fonte de dados.

Revisões de ativos na Amazon DataZone

A Amazon DataZone incrementa a revisão de um ativo quando você edita seus metadados comerciais ou técnicos. Essas edições incluem a modificação do nome do ativo, da descrição, dos termos do glossário, dos nomes das colunas, dos formulários de metadados e dos valores dos campos do formulário de metadados. Essas alterações podem resultar de edições manuais, execução de tarefas da fonte de dados ou operações de API. A Amazon gera DataZone automaticamente uma nova revisão de ativos sempre que você faz uma edição no ativo.

Depois de atualizar um ativo e gerar uma nova revisão, você deve publicar a nova revisão no catálogo para que ela seja atualizada e disponibilizada aos assinantes. Para ter mais informações, consulte the section called “Publique ativos no catálogo a partir do inventário do projeto”. Você só pode publicar a versão mais recente de um ativo no catálogo.

Para ver as revisões anteriores de um ativo

1. Navegue até o URL do portal de DataZone dados da Amazon e faça login usando o single sign-on (SSO) ou suas credenciais. AWS Se você for DataZone administrador da Amazon, poderá navegar até o DataZone console da Amazon em https://console.aws.amazon.com/datazone e fazer login com o Conta da AWS local onde o domínio foi criado e, em seguida, escolher Abrir portal de dados.
2. Escolha Selecionar projeto no painel de navegação superior e selecione o projeto que contém o ativo.
3. Navegue até a guia Dados do projeto e, em seguida, localize e escolha o ativo. Isso abre a página de detalhes do ativo.
4. Navegue até a guia Histórico, que exibe uma lista das revisões anteriores do ativo.

Qualidade de dados na Amazon DataZone

As métricas de qualidade de dados na Amazon DataZone ajudam você a entender as diferentes métricas de qualidade, como integridade, pontualidade e precisão de suas fontes de dados. A Amazon DataZone se integra ao AWS Glue Data Quality e oferece APIs para integrar métricas de qualidade de dados de soluções de qualidade de dados de terceiros. Os usuários de dados podem ver como as métricas de qualidade de dados mudam com o tempo para seus ativos inscritos. Para criar e executar as regras de qualidade de dados, você pode usar sua ferramenta de qualidade de dados preferida, como a qualidade de dados AWS Glue. Com as métricas de qualidade de dados

na Amazon DataZone, os consumidores de dados podem visualizar as pontuações de qualidade dos dados dos ativos e das colunas, ajudando a criar confiança nos dados que usam para tomar decisões.

Pré-requisitos e mudanças na função do IAM

Se você estiver usando as políticas AWS gerenciadas DataZone da Amazon, não há etapas adicionais de configuração e essas políticas gerenciadas são atualizadas automaticamente para oferecer suporte à qualidade dos dados. Se você estiver usando suas próprias políticas para as funções que concedem à Amazon DataZone as permissões necessárias para interoperar com os serviços suportados, você deve atualizar as políticas anexadas a essas funções para permitir o suporte à leitura das informações de qualidade de dados do AWS Glue no AWS política gerenciada: AmazonDataZoneGlueManageAccessRolePolicy e habilitar o suporte para as APIs de séries temporais no AWS política gerenciada: AmazonDataZoneDomainExecutionRolePolicy e no. AWS política gerenciada: AmazonDataZoneFullUserAccess

Habilitando a qualidade dos dados para ativos do AWS Glue

A Amazon DataZone extrai as métricas de qualidade de dados do AWS Glue para fornecer contexto em um determinado momento, por exemplo, durante uma pesquisa no catálogo de dados corporativos. Os usuários de dados podem ver como as métricas de qualidade de dados mudam com o tempo para seus ativos inscritos. Os produtores de dados podem ingerir as pontuações de qualidade de dados do AWS Glue de acordo com um cronograma. O catálogo de dados DataZone comerciais da Amazon também pode exibir métricas de qualidade de dados de sistemas de terceiros por meio de APIs de qualidade de dados. Para obter mais informações, consulte AWS Glue Data Quality e Introdução ao AWS Glue Data Quality for the Data Catalog.

Você pode habilitar métricas de qualidade de dados para seus DataZone ativos da Amazon das seguintes formas:

- Use o Portal de Dados ou as DataZone APIs da Amazon para habilitar a qualidade dos dados da sua fonte de dados AWS Glue por meio do portal de dados da Amazon ao criar uma nova fonte de DataZone dados Glue ou editar uma fonte de dados AWS Glue existente.

  Para obter mais informações sobre como habilitar a qualidade de dados para uma fonte de dados por meio do portal, consulte Crie e execute uma fonte de DataZone dados da Amazon para o AWS Glue Data Catalog Gerencie fontes de DataZone dados existentes da Amazon e.

> **Note**
>
> Você pode usar o Portal de Dados para habilitar a qualidade dos dados somente para seus ativos de inventário do AWS Glue. Nesta versão da Amazon, a DataZone habilitação da qualidade de dados para o Amazon Redshift ou tipos personalizados de ativos por meio do portal de dados não é suportada.

Você também pode usar as APIs para habilitar a qualidade dos dados para suas fontes de dados novas ou existentes. Você pode fazer isso invocando CreateDataSourceou UpdateDataSourcee definindo o `autoImportDataQualityResult` parâmetro como 'True'.

Depois que a qualidade dos dados estiver ativada, você poderá executar a fonte de dados sob demanda ou de acordo com o cronograma. Cada execução pode gerar até 100 métricas por ativo. Não há necessidade de criar formulários ou adicionar métricas manualmente ao usar a fonte de dados para obter qualidade de dados. Quando o ativo é publicado, as atualizações feitas no formulário de qualidade de dados (até 30 pontos de dados por regra do histórico) são refletidas na listagem para os consumidores. Posteriormente, cada nova adição de métricas ao ativo é adicionada automaticamente à listagem. Não há necessidade de republicar o ativo para disponibilizar as pontuações mais recentes aos consumidores.

Habilitando a qualidade dos dados para tipos de ativos personalizados

Você pode usar as DataZone APIs da Amazon para habilitar a qualidade dos dados para qualquer um dos seus ativos de tipo personalizado. Para mais informações, consulte:

- PostTimeSeriesDataPoints
- ListTimeSeriesDataPoints
- GetTimeSeriesDataPoint
- DeleteTimeSeriesDataPoints

As etapas a seguir fornecem um exemplo do uso de APIs ou CLI para importar métricas de terceiros para seus ativos na Amazon: DataZone

1. Invoque a `PostTimeSeriesDataPoints` API da seguinte forma:

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

com a seguinte carga útil:

```
{
"domainIdentifier": "dzd_bqqlk3nz21zp2f",
"entityIdentifier": "4nwl5ew0dsu27b",
"entityType": "ASSET",
"forms": [
{
"content": "{\n \"evaluationsCount\" : 11,\n \"evaluations\" : [ {\n \"description
\" : \"IsComplete \\\"Id\\\"\",\n \"details\" : {\n \"STATISTIC_NAME\" :
 \"Completeness\",\n \"COLUMN_NAME\" : \"Id\"\n },\n \"status\" : \"PASS\"\n },
 {\n \"description\" : \"Uniqueness \\\"Id\\\" > 0.95\",\n \"details\" : {\n
 \"STATISTIC_NAME\" : \"Uniqueness\",\n \"COLUMN_NAME\" : \"Id\"\n },\n \"status
\" : \"PASS\"\n }, {\n \"description\" : \"ColumnLength \\\"Id\\\" = 18\",\n
 \"details\" : {\n \"STATISTIC_NAME\" : \"MinimumLength,MaximumLength\",\n
 \"COLUMN_NAME\" : \"Id,Id\"\n },\n \"status\" : \"PASS\"\n }, {\n \"description
\" : \"IsComplete \\\"IsDeleted\\\"\",\n \"details\" : {\n \"STATISTIC_NAME\" :
 \"Completeness\",\n \"COLUMN_NAME\" : \"IsDeleted\"\n },\n \"status\" : \"PASS
\"\n }, {\n \"description\" : \"Completeness \\\"Type\\\" >= 0.59\",\n \"details
\" : {\n \"STATISTIC_NAME\" : \"Completeness\",\n \"COLUMN_NAME\" : \"Type\"\n },
\n \"status\" : \"PASS\"\n }, {\n \"description\" : \"ColumnValues \\\"Type\
\\" in [\\\"Customer - Direct\\\",\\\"Customer - Channel\\\"] with threshold
 >= 0.8\",\n \"details\" : {\n \"STATISTIC_NAME\" : \"\",\n \"COLUMN_NAME\" :
 \"\"\n },\n \"status\" : \"PASS\"\n }, {\n \"description\" : \"ColumnLength \\
\"Type\\\" <= 18\",\n \"details\" : {\n \"STATISTIC_NAME\" : \"MaximumLength\",\n
 \"COLUMN_NAME\" : \"Type\"\n },\n \"status\" : \"PASS\"\n }, {\n \"description
\" : \"ColumnLength \\\"ParentId\\\" <= 18\",\n \"details\" : {\n \"STATISTIC_NAME
\" : \"MaximumLength\",\n \"COLUMN_NAME\" : \"ParentId\"\n },\n \"status\" :
 \"PASS\"\n }, {\n \"description\" : \"Completeness \\\"AnnualRevenue\\\" >=
 0.28\",\n \"details\" : {\n \"STATISTIC_NAME\" : \"Completeness\",\n \"COLUMN_NAME
\" : \"AnnualRevenue\"\n },\n \"status\" : \"PASS\"\n }, {\n \"description
\" : \"StandardDeviation \\\"AnnualRevenue\\\" between 1658483123.39 and
 1833060294.28\",\n \"details\" : {\n \"STATISTIC_NAME\" : \"StandardDeviation
\",\n \"COLUMN_NAME\" : \"AnnualRevenue\"\n },\n \"status\" : \"PASS\"\n }, {\n
 \"description\" : \"ColumnValues \\\"AnnualRevenue\\\" between 29999999 and
 5600000001\",\n \"details\" : {\n \"STATISTIC_NAME\" : \"Minimum,Maximum\",\n
```

```
 \"COLUMN_NAME\" : \"AnnualRevenue,AnnualRevenue\"\n },\n \"status\" : \"PASS
\"\n } ],\n \"passingPercentage\" : 1.0\n}",
"formName": "GREAT_EXPECTATION_NEW",
"typeIdentifier": "amazon.datazone.DataQualityResultFormType",
"timestamp": 1608969556
}
]
}
```

2. Invoque a `DeleteTimeSeriesDataPoints` API da seguinte forma:

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

Usando aprendizado de máquina e IA generativa

> **Note**
>
> Desenvolvido pelo Amazon Bedrock: AWS implementa a detecção automática de abusos. Como as recomendações de IA para a funcionalidade de descrições na Amazon DataZone são criadas no Amazon Bedrock, os usuários herdam os controles implementados no Amazon Bedrock para garantir a segurança e o uso responsável da IA.

Na versão atual da Amazon DataZone, você pode usar as recomendações de IA para a funcionalidade de descrições para automatizar a descoberta e a catalogação de dados. O suporte para IA generativa e aprendizado de máquina na Amazon DataZone cria descrições para ativos e colunas. Você pode usar essas descrições para adicionar contexto comercial aos seus dados e recomendar análises para conjuntos de dados, o que pode ajudar a impulsionar os resultados da descoberta de dados.

Com base nos grandes modelos de linguagem do Amazon Bedrock, as recomendações de IA para descrições de ativos de dados na Amazon DataZone ajudam você a garantir que seus dados sejam

compreensíveis e facilmente descobertos. As recomendações de IA também sugerem as aplicações analíticas mais pertinentes para conjuntos de dados. Ao reduzir as tarefas de documentação manual e aconselhar sobre o uso adequado de dados, as descrições geradas automaticamente podem ajudar você a aumentar a confiabilidade de seus dados e minimizar a negligência de dados valiosos para acelerar a tomada de decisões informadas.

> **Important**
>
> Na DataZone versão atual da Amazon, o recurso de recomendações de IA para descrições só é suportado nas seguintes regiões:
>
> - Leste dos EUA (Norte da Virgínia)
> - Oeste dos EUA (Oregon)
> - Europa (Frankfurt)
> - Ásia-Pacífico (Tóquio)

O procedimento a seguir descreve como gerar recomendações de IA para descrições na Amazon DataZone:

1. Navegue até o URL do portal de DataZone dados da Amazon e, em seguida, faça login usando o single sign-on (SSO) ou suas credenciais. AWS Se você for um DataZone administrador da Amazon, navegue até o DataZone console da Amazon em https://console.aws.amazon.com/datazone e faça login com o Conta da AWS local onde o domínio foi criado e, em seguida, escolha Abrir portal de dados.
2. No painel de navegação superior, escolha Selecionar projeto e, em seguida, escolha o projeto que contém o ativo para o qual você deseja gerar recomendações de IA para descrições.
3. Navegue até a guia Dados do projeto.
4. No painel de navegação esquerdo, escolha Dados de inventário e, em seguida, escolha o nome do ativo para o qual você deseja gerar recomendações de IA para descrições do ativo.
5. Na página de detalhes do ativo, na guia Metadados comerciais, escolha Gerar descrições.
6. Depois que as descrições forem geradas, você poderá editá-las, aceitá-las ou rejeitá-las. Ícones verdes são exibidos ao lado de cada descrição de metadados gerada automaticamente para o ativo de dados. Na guia Metadados comerciais, você pode escolher o ícone verde ao lado do resumo gerado automaticamente e, em seguida, escolher Editar, Aceitar ou Rejeitar para abordar a descrição gerada. Você também pode escolher Aceitar tudo ou Rejeitar

todas as opções que são exibidas na parte superior da página quando a guia Metadados comerciais é selecionada e, assim, realizar a ação selecionada em todas as descrições geradas automaticamente.

Ou você pode escolher a guia Esquema e, em seguida, abordar individualmente as descrições geradas automaticamente escolhendo o ícone verde para uma descrição de coluna por vez e escolhendo Aceitar ou Rejeitar. Na guia Esquema, você também pode escolher Aceitar tudo ou Rejeitar tudo e, assim, executar a ação selecionada em todas as descrições geradas automaticamente.

7. Para publicar o ativo no catálogo com as descrições geradas, escolha Publicar ativo e confirme essa ação escolhendo Publicar ativo novamente na janela pop-up Publicar ativo.

> **Note**
>
> Se você não aceitar ou rejeitar as descrições geradas para um ativo e depois publicar esse ativo, esses metadados não revisados gerados automaticamente não serão incluídos no ativo de dados publicado.

Descobrindo, assinando e consumindo dados na Amazon DataZone

Na Amazon DataZone, quando um ativo é publicado em um domínio, os assinantes podem descobrir e solicitar uma assinatura desse ativo. O processo de assinatura começa com o assinante pesquisando e navegando no catálogo para encontrar o ativo que deseja. No DataZone portal da Amazon, eles optam por assinar o ativo enviando uma solicitação de assinatura que inclui a justificativa e o motivo da solicitação. O aprovador da assinatura, conforme definido no contrato de publicação, então analisa a solicitação de acesso. Eles podem aprovar ou rejeitar a solicitação.

Depois que uma assinatura é concedida, um processo de atendimento é iniciado para facilitar o acesso do assinante ao ativo. Há dois modos principais de controle de acesso e atendimento de ativos: aqueles para ativos DataZone gerenciados pela Amazon e aqueles para ativos que não são gerenciados pela Amazon. DataZone

- Ativos gerenciados — A Amazon DataZone pode gerenciar o cumprimento e as permissões de ativos gerenciados, como AWS Glue tabelas e tabelas e visualizações do Amazon Redshift.
- Ativos não gerenciados — A Amazon DataZone publica eventos padrão relacionados às suas ações (por exemplo, aprovação dada a uma solicitação de assinatura) na Amazon. EventBridge Você pode usar esses eventos padrão para se integrar a outros AWS serviços ou soluções de terceiros para integrações personalizadas.

Tópicos

Descobrindo dados

As tarefas a seguir descrevem várias maneiras de descobrir dados na Amazon DataZone.

Tópicos

Pesquise e visualize ativos no catálogo

A Amazon DataZone fornece uma forma simplificada de pesquisar dados. Qualquer DataZone usuário da Amazon com permissões para acessar o portal de dados pode pesquisar ativos no DataZone catálogo da Amazon e visualizar os nomes dos ativos e os metadados atribuídos a eles. Você pode examinar mais de perto um ativo examinando sua página de detalhes.

> **Note**
>
> Para visualizar os dados reais que um ativo contém, você deve primeiro assinar o ativo e ter sua solicitação de assinatura aprovada e o acesso concedido. Para ter mais informações, consulte Inscrevendo-se em dados.

Para pesquisar ativos no catálogo

1. Navegue até o URL do portal de DataZone dados da Amazon e faça login usando o single sign-on (SSO) ou suas credenciais. AWS Se você for DataZone administrador da Amazon, poderá navegar até o DataZone console da Amazon em https://console.aws.amazon.com/datazone e fazer login com o Conta da AWS local onde o domínio foi criado e, em seguida, escolher Abrir portal de dados.
2. Você pode digitar o nome do ativo que está procurando na barra de pesquisa na página inicial do portal de dados.
3. Para procurar namespaces, escolha Catálogo no canto superior direito da página para abrir o catálogo. O catálogo fornece uma experiência de pesquisa facetada para você encontrar ativos pesquisando critérios como proprietário dos dados e termos do glossário.
4. Insira seu termo de pesquisa em uma das caixas de pesquisa. Depois de executar uma pesquisa, você pode aplicar vários filtros para restringir os resultados. Os filtros incluem o tipo de ativo, a conta de origem e Região da AWS a que o ativo pertence.
5. Para ver detalhes sobre um ativo específico, escolha o ativo para abrir sua página de detalhes. A página de detalhes inclui as seguintes informações:

   - O nome do ativo, a fonte de dados (AWS Glue Amazon Redshift ou Amazon S3), tipo (tabela, visualização ou objeto do S3), número de colunas e tamanho.
   - Uma descrição do ativo.
   - A revisão atual publicada do ativo, o proprietário, se a aprovação é necessária para assinaturas, o namepace e o histórico de atualizações.

- Uma guia Visão geral que inclui termos do glossário e formulários de metadados.
- Uma guia Esquema que exibe o esquema do ativo, incluindo nomes de colunas comerciais e técnicas, tipos de dados e descrições comerciais das colunas. A guia do esquema é visível somente para tabelas e visualizações (não para objetos do Amazon S3).
- Uma guia Assinaturas que inclui uma lista de assinantes do domínio.
- Uma guia Histórico que inclui uma lista de revisões anteriores do ativo.

Inscrevendo-se em dados

As tarefas a seguir fornecem detalhes sobre a assinatura de ativos na Amazon DataZone.

Tópicos

Solicitar assinatura de ativos

A Amazon DataZone permite que você encontre, acesse e consuma os ativos no DataZone catálogo da Amazon. Quando você encontra um ativo no catálogo que deseja acessar, precisa assinar o ativo, o que cria uma solicitação de assinatura. Um aprovador pode então aprovar ou solicitar sua solicitação.

Você deve ser membro de um projeto para solicitar a assinatura de um ativo dentro desse projeto.

Para assinar um ativo

1. Navegue até o URL do portal de DataZone dados da Amazon e faça login usando o single sign-on (SSO) ou suas credenciais. AWS Se você for DataZone administrador da Amazon, poderá navegar até o DataZone console da Amazon em https://console.aws.amazon.com/datazone e fazer login com o Conta da AWS local onde o domínio foi criado e, em seguida, escolher Abrir portal de dados.

2. Use a barra de pesquisa para pesquisar e escolher o ativo que você deseja assinar e, em seguida, escolha Inscrever-se.
3. Na janela pop-up Inscrever-se, forneça as seguintes informações:
   - O projeto que você deseja inscrever no ativo.
   - Uma breve justificativa para sua solicitação de assinatura.
4. Escolha Assinar.

   Você recebe uma notificação no portal de dados quando o editor aprova sua solicitação.

Para ver o status da solicitação de assinatura, localize e escolha o projeto com o qual você se inscreveu no ativo. Navegue até a guia Dados do projeto e escolha Dados solicitados no painel de navegação esquerdo. Essa página lista os ativos aos quais o projeto solicitou acesso. Você pode filtrar a lista pelo status da solicitação.

Aprovar ou rejeitar uma solicitação de assinatura

A Amazon DataZone permite que você encontre, acesse e consuma os ativos no DataZone catálogo da Amazon. Ao encontrar um ativo no catálogo que você deseja acessar, você deve assinar o ativo, o que cria uma solicitação de assinatura. Um aprovador pode então aprovar ou rejeitar sua solicitação.

Você deve ser membro do projeto proprietário (o projeto que publicou o ativo) para aprovar ou rejeitar uma solicitação de assinatura.

Para aprovar ou rejeitar uma solicitação de assinatura

1. Navegue até o URL do portal de DataZone dados da Amazon e faça login usando o single sign-on (SSO) ou suas credenciais. AWS Se você for DataZone administrador da Amazon, poderá navegar até o DataZone console da Amazon em https://console.aws.amazon.com/datazone e fazer login com o Conta da AWS local onde o domínio foi criado e, em seguida, escolher Abrir portal de dados.
2. No portal de dados, escolha Pesquisar lista de projetos e selecione o projeto que contém o ativo com a solicitação de assinatura.
3. Navegue até a guia Dados e escolha Solicitações recebidas no painel de navegação esquerdo.
4. Localize a solicitação e escolha Exibir solicitação. Você pode filtrar por Pendente para ver somente as solicitações que ainda estão abertas.

5. Analise a solicitação de assinatura e o motivo do acesso e decida se deseja aprová-la ou rejeitá-la.
6. (Opcional) Insira uma resposta que explique o motivo para aceitar ou rejeitar a solicitação.
7. Escolha Aprovar ou Rejeitar.

Como proprietário do projeto, você pode revogar a assinatura a qualquer momento. Para ter mais informações, consulte the section called “Revogar uma assinatura existente”.

Para ver todas as solicitações de assinatura, consulteTrabalhando com DataZone eventos e notificações da Amazon.

Revogar uma assinatura existente

A Amazon DataZone permite que você encontre, acesse e consuma os ativos no DataZone catálogo da Amazon. Quando você encontra um ativo no catálogo que deseja acessar, precisa assinar o ativo, o que cria uma solicitação de assinatura. Um aprovador pode então aprovar ou solicitar sua solicitação. Talvez seja necessário revogar uma assinatura depois de aprová-la, seja porque a aprovação foi um erro ou porque o assinante não precisa mais acessar o ativo.

Você deve ser membro do projeto proprietário (o projeto que publicou o ativo) para revogar uma assinatura.

Para revogar uma assinatura

1. Navegue até o URL do portal de DataZone dados da Amazon e faça login usando o single sign-on (SSO) ou suas credenciais. AWS Se você for DataZone administrador da Amazon, poderá navegar até o DataZone console da Amazon em https://console.aws.amazon.com/datazone e fazer login com o Conta da AWS local onde o domínio foi criado e, em seguida, escolher Abrir portal de dados.
2. Escolha Selecionar projeto no painel de navegação superior e selecione o projeto que contém a assinatura que você deseja revogar.
3. Navegue até a guia Dados e escolha Solicitações recebidas no painel de navegação esquerdo.
4. Localize a assinatura que você deseja revogar e escolha Exibir assinatura.
5. (Opcional) Ative a caixa de seleção para permitir que o assinante mantenha o ativo nas metas de assinatura do projeto. Uma meta de assinatura é uma referência a um conjunto de recursos em que os dados assinados podem ser disponibilizados em um ambiente.

Se você quiser revogar o acesso ao ativo da meta de assinatura posteriormente, deverá fazê-lo em AWS Lake Formation.

6. Escolha Revogar assinatura.

Você não pode reaprovar uma assinatura depois de revogá-la. O assinante deve assinar o ativo novamente para que você o aprove.

Cancelar uma solicitação de assinatura

A Amazon DataZone permite que você encontre, acesse e consuma os ativos no DataZone catálogo da Amazon. Quando você encontra um ativo no catálogo que deseja acessar, precisa assinar o ativo, o que cria uma solicitação de assinatura. Um aprovador pode então aprovar ou solicitar sua solicitação. Talvez seja necessário cancelar uma solicitação de assinatura pendente, seja porque você a enviou por engano ou porque não precisa mais de acesso de leitura ao ativo.

Para cancelar uma solicitação de assinatura, você deve ser proprietário ou colaborador do projeto.

Para cancelar uma solicitação de assinatura

1. Navegue até o URL do portal de DataZone dados da Amazon e faça login usando o single sign-on (SSO) ou suas credenciais. AWS Se você for DataZone administrador da Amazon, poderá navegar até o DataZone console da Amazon em https://console.aws.amazon.com/datazone e fazer login com o Conta da AWS local onde o domínio foi criado e, em seguida, escolher Abrir portal de dados.
2. Escolha Selecionar projeto no painel de navegação superior e selecione o projeto que contém a solicitação de assinatura.
3. Navegue até a guia Dados do projeto e escolha Dados solicitados no painel de navegação esquerdo. Essa página lista os ativos aos quais o projeto solicitou acesso.
4. Filtre por Solicitado para ver somente as solicitações que ainda estão pendentes. Localize a solicitação e escolha Exibir solicitação.
5. Revise a solicitação de assinatura e escolha Cancelar solicitação.

Se você quiser assinar novamente o ativo (ou outro ativo), consultethe section called “Solicitar assinatura de ativos”.

Cancelar a assinatura de um ativo

A Amazon DataZone permite que você encontre, acesse e consuma os ativos no DataZone catálogo da Amazon. Quando você encontra um ativo no catálogo que deseja acessar, precisa assinar o ativo, o que cria uma solicitação de assinatura. Um aprovador pode então aprovar ou solicitar sua solicitação. Talvez seja necessário cancelar a assinatura de um ativo, seja porque você se inscreveu por engano e foi aprovado, seja porque não precisa mais de acesso de leitura ao ativo.

Você deve ser membro de um projeto para cancelar a assinatura de um de seus ativos.

Para cancelar a assinatura de um ativo

1. Navegue até o URL do portal de DataZone dados da Amazon e faça login usando o single sign-on (SSO) ou suas credenciais. AWS Se você for DataZone administrador da Amazon, poderá navegar até o DataZone console da Amazon em https://console.aws.amazon.com/datazone e fazer login com o Conta da AWS local onde o domínio foi criado e, em seguida, escolher Abrir portal de dados.
2. Escolha Selecionar projeto no painel de navegação superior e selecione o projeto que contém o ativo do qual você deseja cancelar a assinatura.
3. Navegue até a guia Dados do projeto e escolha Dados solicitados no painel de navegação esquerdo. Essa página lista os ativos aos quais o projeto solicitou acesso.
4. Filtre por Aprovado para ver somente as solicitações que foram aprovadas. Localize a solicitação e escolha Exibir assinatura.
5. Revise a assinatura e escolha Cancelar assinatura.

Se você quiser assinar novamente o ativo (ou outro ativo), consultethe section called “Solicitar assinatura de ativos”.

Usando funções existentes do IAM para atender às DataZone assinaturas da Amazon

Na versão atual, a Amazon DataZone oferece suporte ao uso de suas funções existentes do IAM para obter acesso aos dados. Para conseguir isso, você pode criar uma meta de assinatura no DataZone ambiente da Amazon que você está usando para cumprir sua assinatura. Para criar uma meta de assinatura para um ambiente em uma das AWS contas associadas, você pode usar as seguintes etapas:

Etapa 1: Certifique-se de que seu DataZone domínio da Amazon esteja usando a versão 2 ou superior da política de RAM

1. Navegue até a página Compartilhado por mim: compartilhamentos de recursos no console da AWS RAM.
2. Como os compartilhamentos de recursos de AWS RAM existem em AWS regiões específicas, escolha a AWS região apropriada na lista suspensa no canto superior direito do console.
3. Selecione o compartilhamento de recursos correspondente ao seu DataZone domínio da Amazon e escolha Modificar. Você pode identificar o compartilhamento de RAM para o DataZone domínio da Amazon usando o nome ou ID do domínio, pois o compartilhamento de RAM é criado com o nome:`DataZone-<domain-name>-<domain-id>`.
4. Escolha Avançar para prosseguir para a próxima etapa, na qual você pode verificar a versão da política de RAM e modificá-la.
5. Verifique se a versão da política de RAM é a versão 2 ou superior. Caso contrário, use o menu suspenso para selecionar a versão 2 ou superior.
6. Escolha Ir para a etapa 4: Revisar e atualizar.
7. Escolha Atualizar compartilhamento de recursos.

Etapa 2: criar uma meta de assinatura a partir de uma conta associada

- Na versão atual, a Amazon DataZone oferece suporte à criação de metas de assinatura usando somente APIs. Abaixo estão alguns exemplos da carga útil que você pode usar para criar uma meta de assinatura para atender às assinaturas de suas tabelas do AWS Glue e das tabelas ou visualizações do Amazon Redshift. Para obter mais informações, consulte CreateSubscriptionTarget.

  Exemplo de meta de assinatura do 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"
}
```

Exemplo de meta de assinatura para o 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

- O EnvironmentIdentifier que você usa na chamada de API acima deve existir na mesma conta associada da qual você está fazendo a chamada de API. Caso contrário, a chamada da API não será bem-sucedida.
- O ARN da função do IAM que você usa em “AuthorizedPrincipals” é a função à qual a Amazon DataZone concederá acesso depois que um ativo inscrito for adicionado à meta da assinatura. Esses diretores autorizados devem pertencer à mesma conta do ambiente no qual a meta de assinatura está sendo criada.
- O valor do campo do provedor deve ser “Amazon DataZone” para DataZone que a Amazon possa concluir o cumprimento da assinatura.
- O nome do banco de dados fornecido em já subscriptionTargetConfig deve existir na conta na qual o destino está sendo criado. A Amazon não DataZone criará esse banco

de dados. Certifique-se também de que a função de gerenciamento de acesso tenha a permissão CREATE TABLE nesse banco de dados.

- Além disso, certifique-se de que as funções (a função do IAM para o AWS Glue e a função do banco de dados para o Amazon Redshift) fornecidas como diretores autorizados já existam na conta do ambiente. Para destinos de assinatura do Amazon Redshift, atualizações adicionais são necessárias para a função que está sendo assumida ao se conectar ao cluster. Essa função deve ter uma RedshiftDbRoles tag anexada à função. O valor da tag pode ser uma lista separada por vírgulas. O valor deve ser a função do banco de dados fornecida como principal autorizado ao criar a meta de assinatura.

Etapa 3: Inscrever-se em uma nova tabela e cumprir a assinatura da nova meta

- Depois de criar a meta de assinatura, você pode se inscrever em uma nova tabela e a Amazon a DataZone cumprirá com a meta acima. Para ter mais informações, consulte Inscrevendo-se em dados.

Concedendo acesso aos dados

As tarefas a seguir fornecem detalhes sobre a concessão de acesso a assinaturas aprovadas de ativos na Amazon. DataZone

Na Amazon DataZone, as solicitações de assinatura e as assinaturas aprovadas ou concedidas para acesso de leitura aos ativos são gerenciadas pelos aprovadores de assinaturas. O aprovador da assinatura de um ativo é determinado pelo contrato de publicação com o qual esse ativo foi publicado no DataZone catálogo da Amazon.

Tópicos

Conceda acesso aos AWS Glue Data Catalog ativos gerenciados

> **Note**
>
> O gerenciamento de acesso para os AWS Glue Data Catalog ativos usando o método AWS Lake Formation LF-TBAC não é suportado.
> O suporte para compartilhamento de ativos entre regiões não AWS Glue Data Catalog é suportado.

Depois que uma solicitação de assinatura para AWS Glue Data Catalog ativos gerenciados é aprovada, a Amazon adiciona DataZone automaticamente esses ativos a todos os ambientes de data lake existentes no projeto. A Amazon DataZone então concede e gerencia o acesso às AWS Glue Data Catalog tabelas aprovadas em seu nome por meio de AWS Lake Formation. Para o projeto do assinante, os ativos concedidos aparecem AWS Glue Data Catalog como recursos em sua conta. Em seguida, você pode usar o Amazon Athena para consultar as tabelas.

> **Note**
>
> Se um novo ambiente de data lake for adicionado ao projeto após os AWS Glue Data Catalog ativos inscritos terem sido automaticamente adicionados aos ambientes de data lake existentes, você precisará adicionar manualmente esses AWS Glue Data Catalog ativos inscritos a esse novo ambiente de data lake. Você pode fazer isso escolhendo a opção Adicionar subsídio na guia Dados da página de visão geral do projeto no portal de DataZone dados da Amazon.

Para DataZone que a Amazon possa conceder acesso às tabelas do AWS Glue Data Catalog, as seguintes condições devem ser atendidas.

- A tabela AWS Glue deve ser gerenciada pelo Lake Formation, pois a Amazon DataZone concede acesso gerenciando as permissões do Lake Formation.
- A função Manage Access para o ambiente de data lake usada para publicar a tabela do AWS Glue Data Catalog deve ter as seguintes permissões do Lake Formation:
  - `DESCRIBE`e `DESCRIBE GRANTABLE` permissões no banco de dados AWS Glue que contém a tabela publicada.

- `DESCRIBE`,`SELECT`,`DESCRIBE GRANTABLE`, `SELECT GRANTABLE` permissões em Lake Formation na própria tabela publicada.

Para obter mais informações, consulte Conceder e revogar permissões em recursos do catálogo no Guia do AWS Lake Formation desenvolvedor.

Conceda acesso aos ativos gerenciados do Amazon Redshift

Quando uma assinatura de uma tabela ou visualização do Amazon Redshift é aprovada, a Amazon DataZone pode adicionar automaticamente o ativo inscrito a todos os ambientes de armazém de dados dentro do projeto, para que os membros do projeto possam consultar os dados usando o link do editor de consultas do Amazon Redshift em seus ambientes. Nos bastidores, a Amazon DataZone cria as concessões e os compartilhamentos de dados necessários entre a fonte e a meta da assinatura.

O processo de concessão de acesso varia dependendo de onde o banco de dados de origem (editor) e o banco de dados de destino (assinante) estão localizados.

- Mesmo cluster, mesmo banco de dados — se os dados precisarem ser compartilhados no mesmo banco de dados, a Amazon DataZone concede permissões diretamente na tabela de origem.
- Mesmo cluster, banco de dados diferente - se os dados precisarem ser compartilhados entre dois bancos de dados dentro do mesmo cluster, a Amazon DataZone cria uma visualização no banco de dados de destino e as permissões são concedidas na visualização criada.
- Cluster diferente da mesma conta - a Amazon DataZone cria um compartilhamento de dados entre o cluster de origem e o de destino e cria uma visualização na parte superior da tabela compartilhada. As permissões são concedidas na exibição.
- Conta cruzada - igual à anterior, mas é necessária uma etapa adicional para autorizar o compartilhamento de dados entre contas no lado do cluster do produtor e outra etapa para associar o compartilhamento de dados no lado do cluster do consumidor.

> **Note**
>
> Se um novo ambiente de armazém de dados for adicionado ao projeto após os ativos inscritos do Amazon Redshift terem sido adicionados automaticamente aos ambientes de armazém de dados existentes, você deverá adicionar manualmente esses ativos assinados do Amazon Redshift a esse novo ambiente de armazém de dados. Você pode fazer isso

escolhendo a opção Adicionar subsídio na guia Dados da página de visão geral do projeto no portal de DataZone dados da Amazon.

Certifique-se de que seus clusters de publicação e assinatura do Amazon Redshift atendam a todos os requisitos para compartilhamentos de dados do Amazon Redshift. Para obter mais informações, consulte o Amazon Redshift Developer Guide.

> **Note**
>
> A Amazon DataZone oferece suporte à concessão automática de assinaturas para ativos do Amazon Redshift Cluster e do Amazon Redshift Serverless.
> O compartilhamento de dados entre regiões usando o Amazon Redshift não é suportado.

> **Note**
>
> Na versão atual, a Amazon DataZone pode gerenciar o acesso às tabelas e visualizações do Amazon Redshift somente se os clusters ou grupos de trabalho do Amazon Redshift de origem e de destino estiverem localizados nas AWS contas que pertencem à mesma organização. AWS

Conceda acesso para assinaturas aprovadas a ativos não gerenciados

A Amazon DataZone permite que os usuários publiquem qualquer tipo de ativo no catálogo de dados comerciais. Para alguns desses ativos, a Amazon DataZone pode gerenciar automaticamente as concessões de acesso. Esses ativos são chamados de ativos gerenciados e incluem tabelas do AWS Glue Data Catalog gerenciadas pelo Lake Formation e tabelas e visualizações do Amazon Redshift. Todos os outros ativos aos quais a Amazon não DataZone pode conceder assinaturas automaticamente são chamados de não gerenciados.

DataZone A Amazon fornece um caminho para você gerenciar concessões de acesso para seus ativos não gerenciados. Quando a assinatura de um ativo no catálogo de dados comerciais é aprovada pelo proprietário dos dados, a Amazon DataZone publica um evento na Amazon EventBridge em sua conta junto com todas as informações necessárias na carga útil que permitem criar as concessões de acesso entre a origem e o destino. Ao receber esse evento, você pode acionar um manipulador personalizado que pode usar as informações do evento para criar as

concessões ou permissões necessárias. Depois de conceder o acesso, você pode relatar e atualizar o status da assinatura na Amazon DataZone para que ela possa notificar os usuários que assinaram o ativo de que eles podem começar a consumir o ativo. Para ter mais informações, consulte Trabalhando com DataZone eventos e notificações da Amazon.

Consumindo dados

As tarefas a seguir fornecem detalhes sobre o consumo de dados que você assinou na Amazon DataZone.

Tópicos

- Consulte dados no Amazon Athena ou no Amazon Redshift

Consulte dados no Amazon Athena ou no Amazon Redshift

Na Amazon DataZone, quando um assinante tem acesso a um ativo no catálogo, ele pode consumi-lo (consultar e analisar) usando o Amazon Athena ou o editor de consultas v2 do Amazon Redshift. Você deve ser proprietário ou colaborador do projeto para concluir essa tarefa. Dependendo dos esquemas habilitados no projeto, a Amazon DataZone fornece links para o Amazon Athena e/ou o editor de consultas v2 do Amazon Redshift no painel direito da página do projeto no portal de dados.

1. Navegue até o URL do portal de DataZone dados da Amazon e faça login usando o single sign-on (SSO) ou suas credenciais. AWS Se você for DataZone administrador da Amazon, poderá navegar até o DataZone console da Amazon em https://console.aws.amazon.com/datazone e fazer login com o Conta da AWS local onde o domínio foi criado e, em seguida, escolher Abrir portal de dados.
2. No portal de DataZone dados da Amazon, escolha Procurar lista de projetos e, em seguida, encontre e escolha o projeto em que você tem os dados que deseja analisar.
3. Se o plano do Data Lake estiver ativado neste projeto, um link para o Amazon Athena será exibido no painel lateral direito da página inicial do projeto.

   Se o blueprint do Data Warehouse estiver ativado nesse projeto, um link para o editor de consultas será exibido no painel lateral direito da página inicial do projeto.

   > **Note**
   >
   > Os blueprints são definidos no perfil do ambiente com o qual um projeto é criado.

Tópicos

- Consulte dados usando o Amazon Athena
- Consulte dados usando o Amazon Redshift

Consulte dados usando o Amazon Athena

Escolha o link do Amazon Athena para abrir o editor de consultas do Amazon Athena em uma nova guia no navegador usando as credenciais do projeto para autenticação. O DataZone projeto da Amazon com o qual você está trabalhando é selecionado automaticamente como o grupo de trabalho atual no editor de consultas.

No editor de consultas do Amazon Athena, escreva e execute suas consultas. Algumas tarefas comuns incluem:

- Consulte e analise seus ativos inscritos
- Crie novas tabelas
- Crie uma tabela a partir dos resultados da consulta (CTAS) de um bucket externo do S3

Consulte e analise seus ativos inscritos

Se o acesso aos ativos nos quais seu projeto está inscrito não for concedido automaticamente pela Amazon DataZone, você deverá estar autorizado a acessar os dados subjacentes. Para obter mais informações sobre como conceder acesso a esses ativos, consulteConceda acesso para assinaturas aprovadas a ativos não gerenciados.

Se o acesso aos ativos nos quais seu projeto está inscrito for concedido automaticamente pela Amazon DataZone, você poderá executar consultas SQL nas tabelas e ver os resultados no Amazon Athena. Para obter mais informações sobre o uso do SQL no Amazon Athena, consulte a referência de SQL para o Athena.

Quando você navega até o editor de consultas do Amazon Athena depois de escolher o link do Amazon Athena no painel lateral direito da página inicial do projeto, uma lista suspensa Projeto é exibida no canto superior direito do editor de consultas do Amazon Athena e o contexto do seu projeto é selecionado automaticamente.

Você pode ver os seguintes bancos de dados na lista suspensa Banco de dados:

- Um banco de dados de publicação (*{environmentname}*_pub_db). O objetivo desse banco de dados é fornecer um ambiente em que você possa produzir novos dados dentro do contexto do seu projeto e depois publicar esses dados no DataZone catálogo da Amazon. Proprietários e colaboradores do projeto têm acesso de leitura e gravação a esse banco de dados. Os visualizadores do projeto só têm acesso de leitura a esse banco de dados.
- Um banco de dados de assinaturas (*{environmentname}*_sub_db). O objetivo desse banco de dados é compartilhar com você os dados que você assinou como membro do projeto no DataZone catálogo da Amazon e permitir que você consulte esses dados.

Crie novas tabelas

Se você se conectou a um bucket externo do S3, você pode usar o Amazon Athena para consultar e analisar os ativos de um bucket externo do Amazon S3. Nesse cenário, a Amazon DataZone não tem permissões para conceder acesso diretamente aos dados subjacentes no bucket externo do Amazon S3, e os dados externos do Amazon S3 criados fora do projeto não são gerenciados automaticamente no Lake Formation e não podem ser gerenciados pela Amazon. DataZone Uma alternativa é copiar os dados do bucket externo do Amazon S3 para uma nova tabela dentro do bucket Amazon S3 do projeto usando `CREATE TABLE` uma declaração no Amazon Athena. Ao executar uma `CREATE TABLE` consulta no Amazon Athena, você registra sua tabela com o. AWS Glue Data Catalog

Para especificar o caminho para os dados no Amazon S3, use a propriedade `LOCATION` conforme mostrado no seguinte exemplo:

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

Para obter mais informações, consulte Localização da tabela no Amazon S3.

Crie uma tabela a partir dos resultados da consulta (CTAS) de um bucket externo do S3

Quando você assina um ativo, o acesso aos dados subjacentes é somente para leitura. Você pode usar o Amazon Athena para criar uma cópia da tabela. No Amazon Athena, a `A CREATE TABLE AS SELECT (CTAS)` consulta cria uma nova tabela no Amazon Athena a partir dos resultados de `SELECT` uma declaração de outra consulta. Para obter informações sobre a sintaxe do CTAS, consulte CREATE TABLE AS.

O exemplo a seguir cria uma tabela copiando todas as colunas de uma tabela:

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

Na seguinte variação do mesmo exemplo, a instrução `SELECT` também inclui uma cláusula `WHERE`. Nesse caso, a consulta seleciona somente as linhas da tabela que satisfazem a cláusula `WHERE`:

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

O exemplo a seguir cria uma consulta que é executada em um conjunto de colunas de outra tabela:

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

Essa variação do mesmo exemplo cria uma tabela a partir de colunas específicas de várias tabelas:

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

Essas tabelas recém-criadas agora fazem parte do AWS Glue banco de dados de seus projetos e podem ser descobertas por outras pessoas e compartilhadas com outros DataZone projetos da Amazon publicando os dados como um ativo no catálogo da Amazon. DataZone

Consulte dados usando o Amazon Redshift

No portal de DataZone dados da Amazon, abra um ambiente que usa o esquema do data warehouse. Escolha o link do Amazon Redshift no painel direito na página do ambiente. Isso abre uma caixa de diálogo de confirmação com os detalhes necessários que ajudam você a estabelecer uma conexão com o cluster Amazon Redshift do seu ambiente ou com o grupo de trabalho Amazon Redshift Serverless no editor de consultas v2.0 do Amazon Redshift. Depois de identificar os detalhes necessários para estabelecer a conexão, escolha o botão Abrir Amazon Redshift. Isso abre o editor de consultas v2.0 do Amazon Redshift em uma nova guia no navegador usando credenciais temporárias do ambiente Amazon. DataZone

No editor de consultas, siga as etapas abaixo, dependendo se seu ambiente está usando um grupo de trabalho sem servidor do Amazon Redshift ou um cluster do Amazon Redshift.

Para um grupo de trabalho sem servidor do Amazon Redshift

1. No editor de consultas, identifique o grupo de trabalho Amazon Redshift Serverless do DataZone ambiente Amazon, clique com o botão direito nele e escolha Criar uma conexão.
2. Escolha Usuário federado para autenticação.
3. Forneça o nome do banco de dados do DataZone ambiente Amazon.
4. Escolha Criar conexão.

Para um cluster do Amazon Redshift:

1. No editor de consultas, identifique o cluster Amazon Redshift do seu DataZone ambiente Amazon, clique com o botão direito nele e escolha Criar uma conexão.
2. Selecione Credenciais temporárias usando sua identidade do IAM para autenticação.
3. Se o método de autenticação acima não estiver disponível, abra as configurações da conta escolhendo o botão de engrenagem no canto inferior esquerdo, escolha Autenticar com credenciais do IAM e salve. Essa é uma one-time-only configuração.
4. Forneça o nome do banco de dados do DataZone ambiente Amazon para criar a conexão.
5. Escolha Criar conexão.

Agora você pode começar a consultar as tabelas e visualizações dentro do cluster Amazon Redshift ou do grupo de trabalho Amazon Redshift Serverless configurado para seu ambiente Amazon. DataZone

Todas as tabelas ou visualizações do Amazon Redshift nas quais você se inscreveu estão vinculadas ao cluster do Amazon Redshift ou ao grupo de trabalho Amazon Redshift Serverless configurado para o ambiente. Você pode assinar as tabelas e visualizações, bem como publicar quaisquer novas tabelas e visualizações criadas no cluster ou banco de dados do seu ambiente.

Por exemplo, vamos considerar um cenário em que um ambiente está vinculado a um cluster do Amazon Redshift chamado `redshift-cluster-1` e a um banco de dados chamado `dev` nesse cluster. Usando o portal de DataZone dados da Amazon, você pode consultar as tabelas e visualizações que são adicionadas ao seu ambiente. Na `Analytics tools` seção no painel do lado direito do portal de dados, você pode escolher o link do Amazon Redshift para esse ambiente, que abre o editor de consultas. Em seguida, você pode clicar com o botão direito do mouse no `redshift-cluster-1` cluster e criar uma conexão usando credenciais temporárias usando sua identidade do IAM. Depois que a conexão for estabelecida, você poderá ver todas as tabelas e visualizações às quais seu ambiente tem acesso no banco de dados dev.

Trabalhando com DataZone eventos e notificações da Amazon

A Amazon DataZone mantém você informado sobre atividades importantes em seu portal de dados, como solicitações de assinatura, atualizações, comentários e eventos do sistema. DataZone A Amazon fornece essas informações entregando mensagens na caixa de entrada dedicada no portal de dados ou por meio do barramento EventBridge padrão da Amazon.

Tópicos

Trabalhando com eventos por meio da caixa de entrada dedicada no portal de DataZone dados da Amazon

DataZone A Amazon fornece uma caixa de entrada dedicada no portal de dados, onde você pode ver e agir em suas mensagens. As mensagens recentes também aparecem na página inicial, na página do projeto e na página do catálogo. Por exemplo, se um usuário solicitar acesso a um ativo de dados, os proprietários e colaboradores do projeto de publicação desse ativo verão a solicitação no portal de dados e, quando uma ação for tomada, os membros do projeto assinante relacionado a essa solicitação verão a notificação no portal de dados. Há dois tipos de mensagens:

- Tarefas - essas mensagens informam ao destinatário que é necessária uma ação em algum lugar. Eles têm um campo de status opcional que você pode usar para rastreamento.
- Eventos - essas mensagens são informativas e não têm status atribuído. Os eventos fornecem uma trilha de auditoria das atualizações recentes.

Na Amazon DataZone, as mensagens são geradas para os seguintes tipos de eventos:

Categoria de evento	Nome do evento	Descrição do evento	Tipo de evento
Assinatura	Solicitação de assinatura criada	O evento é gerado quando uma solicitaç	Tarefa

Categoria de evento	Nome do evento	Descrição do evento	Tipo de evento
		ão de assinatura é criada	
Assinatura	Solicitação de assinatura aceita	O evento é gerado quando uma solicitação de assinatura é aceita	Evento
Assinatura	Solicitação de assinatura rejeitada	O evento é gerado quando uma solicitação de assinatura é rejeitada	Evento
Assinatura	Solicitação de assinatura excluída	O evento é gerado quando uma solicitação de assinatura é excluída	Evento
Projeto	A criação do projeto foi bem-sucedida	O evento é gerado quando a criação do projeto é bem-sucedida	Evento
Participação no projeto	A adição de membros do projeto foi bem-sucedida	O evento é gerado quando um novo membro é adicionado a um projeto	Evento
Participação no projeto	A remoção do membro do projeto foi bem-sucedida	O evento é gerado quando um membro é removido de um projeto	Evento
Participação no projeto	A mudança de função do membro do projeto foi bem-sucedida	O evento é gerado, a função de um membro no projeto é alterada	Evento

Categoria de evento	Nome do evento	Descrição do evento	Tipo de evento
Ambiente	Iniciada a implantação do ambiente	O evento é gerado quando a implantação de um ambiente é iniciada	Evento
Ambiente	Implantação do ambiente concluída	O evento é gerado quando a implantação de um ambiente é concluída com êxito	Evento
Ambiente	Falha na implantação do ambiente	O evento é gerado quando a implantação de um ambiente falha	Evento
Ambiente	Fluxo de trabalho personalizado de implantação do ambiente iniciado	O evento é gerado quando um ambiente com fluxo de trabalho personalizado é iniciado	Evento
Ativo de dados	Ativo adicionado ao inventário	O evento é gerado quando um novo ativo de dados é adicionado ao inventário, ou seja, adicionado ao catálogo no estado de rascunho	Evento
Ativo de dados	Ativo publicado	O evento é gerado quando um novo ativo de dados é publicado, ou seja, disponível para assinatura	Evento

Categoria de evento	Nome do evento	Descrição do evento	Tipo de evento
Ativo de dados	Esquema de ativos alterado	O evento é gerado quando um esquema de ativos é alterado desde o trabalho de ingestão anterior	Evento
Assinatura	Assinatura criada	O evento é gerado quando alguém solicita a assinatura de um ativo de dados	Tarefa
Assinatura	Assinatura aprovada	O evento é gerado quando uma assinatura é aprovada pelo proprietário ou colaborador do projeto de publicação	Evento
Assinatura	Assinatura rejeitada	O evento é gerado quando uma assinatura é rejeitada pelo proprietário ou colaborador do projeto de publicação	Evento
Assinatura	Assinatura excluída	O evento é gerado quando uma assinatura é cancelada pelo assinante	Evento
Assinatura	Subsídio de assinatura solicitado	O evento é gerado quando alguém solicita acesso a um ativo	Evento

Categoria de evento	Nome do evento	Descrição do evento	Tipo de evento
Assinatura	Concessão de assinatura concluída	O evento é gerado quando uma assinatura recebe acesso ao ativo pelo proprietário ou colaborador do projeto de publicação	Evento
Assinatura	Falha na concessão da assinatura	O evento é gerado quando uma concessão de assinatura falha	Evento
Assinatura	Solicitada a revogação do subsídio de assinatura	O evento é gerado quando uma concessão de assinatura revogada é iniciada pelo proprietário ou colaborador do projeto de publicação	Evento
Assinatura	Revogação da concessão de assinatura concluída	O evento é gerado quando a revogação de uma concessão de assinatura é concluída	Evento
Assinatura	Falha na revogação da concessão de assinatura	O evento é gerado quando a revogação de uma concessão de assinatura falha	Evento
Geração automatizada de nomes comerciais	Nome comercial gerado com sucesso	O evento é gerado quando o trabalho automatizado gerado pelo nome comercial é concluído com êxito	Evento

Categoria de evento	Nome do evento	Descrição do evento	Tipo de evento
Geração automatizada de nomes comerciais	Falha na geração do nome comercial	O evento é gerado quando o trabalho automatizado gerado pelo nome comercial falha	Evento
Execução da fonte de dados	Fonte de dados criada	O evento é gerado quando uma nova fonte de dados é criada	Evento
Execução da fonte de dados	Fonte de dados atualizada	O evento é gerado quando uma fonte de dados existente é atualizada	Evento
Execução da fonte de dados	A execução da fonte de dados foi acionada	O evento é gerado quando a execução de uma fonte de dados é iniciada	Evento
Execução da fonte de dados	A execução da fonte de dados foi bem-sucedida	O evento é gerado quando a execução de uma fonte de dados é bem-sucedida	Evento
Execução da fonte de dados	Falha na execução da fonte de dados	O evento é gerado quando a execução de uma fonte de dados falha	Evento

Para visualizar tarefas na caixa de entrada do seu portal de dados, conclua as seguintes etapas:

1. Navegue até o portal de DataZone dados da Amazon usando a URL do portal de dados e faça login usando seu SSO ou suas AWS credenciais. Se você for DataZone administrador da

Amazon, poderá obter a URL do portal de dados acessando o DataZone console da Amazon em https://console.aws.amazon.com/datazone na AWS conta em que o DataZone domínio da Amazon foi criado.

2. No portal de dados, para ver um pop-up com o conjunto recente de tarefas, selecione o ícone de sino ao lado da barra de pesquisa.
3. Selecione Exibir tudo para ver todas as tarefas. Você pode alterar as visualizações e ver todos os eventos selecionando a guia Eventos.
4. Você pode filtrar a pesquisa pelo assunto do evento, status ativo ou inativo ou intervalo de datas.
5. Escolha qualquer tarefa individual para navegar até o local onde você pode responder à tarefa.

Para visualizar eventos na caixa de entrada do seu portal de dados, conclua as seguintes etapas:

1. Navegue até o portal de DataZone dados da Amazon usando a URL do portal de dados e faça login usando seu SSO ou suas AWS credenciais. Se você for DataZone administrador da Amazon, poderá obter a URL do portal de dados acessando o DataZone console da Amazon em https://console.aws.amazon.com/datazone na AWS conta em que o domínio DataZone raiz da Amazon foi criado.
2. No portal de dados, para ver o pop-up do conjunto recente de eventos, selecione o ícone de sino ao lado da barra de pesquisa.
3. Selecione Exibir tudo para ver todos os eventos. Você pode alterar as visualizações e ver todas as tarefas selecionando a guia Tarefas.
4. Filtre a pesquisa pelo assunto do evento ou intervalo de datas.
5. Escolha qualquer evento individual para navegar até o local onde você pode ver detalhes sobre esse evento.

Trabalhando com eventos por meio do barramento EventBridge padrão da Amazon

Além de enviar mensagens para sua caixa de entrada dedicada no portal de dados, DataZone também envia essas mensagens para seu barramento de eventos EventBridge padrão da Amazon na mesma AWS conta em que seu domínio DataZone raiz da Amazon está hospedado. Isso permite a automação orientada por eventos, como o cumprimento de assinaturas ou integrações personalizadas com outras ferramentas. Você pode criar regras que correspondam aos EventBridge eventos recebidos da Amazon e enviá-las aos EventBridge destinos da Amazon

para processamento. Uma única regra pode enviar um evento para vários destinos, que podem ser executados paralelamente.

Aqui está um exemplo de evento:


```
{
  "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"
        }
      ]
```

```
    }
  }
}
```

A lista completa de tipos de detalhes suportados pela Amazon DataZone inclui:

- Solicitação de assinatura criada
- Solicitação de assinatura aceita
- Solicitação de assinatura rejeitada
- Solicitação de assinatura excluída
- Subsídio de assinatura solicitado
- Concessão de assinatura concluída
- Falha na concessão da assinatura
- Solicitada a revogação do subsídio de assinatura
- Revogação da concessão de assinatura concluída
- Falha na revogação da concessão de assinatura
- Ativo adicionado ao inventário
- Ativo adicionado ao catálogo
- Esquema de ativos alterado
- Alteração do status da fonte de dados
- Fonte de dados criada
- Fonte de dados atualizada
- A execução da fonte de dados foi acionada
- A execução da fonte de dados foi bem-sucedida
- Falha na execução da fonte de dados
- Criação de domínio bem-sucedida
- Falha na criação do domínio
- A exclusão do domínio foi bem-sucedida
- Falha na exclusão do domínio
- Implantação do ambiente iniciada
- Implantação do ambiente concluída

- Falha na implantação do ambiente
- A exclusão do ambiente foi iniciada
- Exclusão do ambiente concluída
- Falha na exclusão do ambiente
- Criação do projeto bem-sucedida
- A adição de membros do projeto foi bem-sucedida
- A remoção do membro do projeto foi bem-sucedida
- Mudança de função de membro do projeto bem-sucedida
- Fluxo de trabalho do cliente de implantação do ambiente iniciado
- A geração do nome comercial foi bem-sucedida
- Falha na geração do nome comercial

Para obter mais informações, consulte Amazon EventBridge.

Segurança na Amazon DataZone

A segurança na nuvem AWS é a maior prioridade. Como AWS cliente, você se beneficia de data centers e arquiteturas de rede criados para atender aos requisitos das organizações mais sensíveis à segurança.

A segurança é uma responsabilidade compartilhada entre você AWS e você. O modelo de responsabilidade compartilhada descreve isso como a segurança da nuvem e segurança na nuvem:

- Segurança da nuvem — AWS é responsável por proteger a infraestrutura que executa AWS os serviços no Nuvem AWS. AWS também fornece serviços que você pode usar com segurança. Auditores terceirizados testam e verificam regularmente a eficácia de nossa segurança como parte dos Programas de Conformidade Programas de AWS de . Para saber mais sobre os programas de conformidade que se aplicam à Amazon DataZone, consulte AWS Serviços no escopo do programa de conformidade AWS .
- Segurança na nuvem — Sua responsabilidade é determinada pelo AWS serviço que você usa. Você também é responsável por outros fatores, incluindo a confidencialidade de seus dados, os requisitos da empresa e as leis e regulamentos aplicáveis.

Essa documentação ajuda você a entender como aplicar o modelo de responsabilidade compartilhada ao usar a Amazon DataZone. Os tópicos a seguir mostram como configurar a Amazon DataZone para atender aos seus objetivos de segurança e conformidade. Você também aprende a usar outros AWS serviços que ajudam a monitorar e proteger seus DataZone recursos da Amazon.

Tópicos

Proteção de dados na Amazon DataZone

O modelo de responsabilidade AWS compartilhada de se aplica à proteção de dados na Amazon DataZone. Conforme descrito neste modelo, AWS é responsável por proteger a infraestrutura global que executa todos os Nuvem AWS. Você é responsável por manter o controle sobre seu conteúdo hospedado nessa infraestrutura. Você também é responsável pelas tarefas de configuração e gerenciamento de segurança dos Serviços da AWS que usa. Para ter mais informações sobre a privacidade de dados, consulte as Perguntas frequentes sobre privacidade de dados. Para ter mais informações sobre a proteção de dados na Europa, consulte a AWS postagem do blog Shared Responsibility Model and GDPR no AWS Blog de segurança da.

Para fins de proteção de dados, recomendamos que você proteja Conta da AWS as credenciais e configure usuários individuais com AWS IAM Identity Center ou AWS Identity and Access Management (IAM). Dessa maneira, cada usuário receberá apenas as permissões necessárias para cumprir suas obrigações de trabalho. Recomendamos também que você proteja seus dados das seguintes formas:

- Use uma autenticação multifator (MFA) com cada conta.
- Use SSL/TLS para se comunicar com os recursos. AWS Exigimos TLS 1.2 e recomendamos TLS 1.3.
- Configure a API e o registro de atividades do usuário com AWS CloudTrail.
- Use soluções de AWS criptografia, juntamente com todos os controles de segurança padrão Serviços da AWS.
- Use serviços gerenciados de segurança avançada, como o Amazon Macie, que ajuda a localizar e proteger dados sigilosos armazenados no Amazon S3.
- Se você precisar de módulos criptográficos validados pelo FIPS 140-2 ao acessar AWS por meio de uma interface de linha de comando ou de uma API, use um endpoint FIPS. Para ter mais informações sobre endpoints do FIPS, consulte Federal Information Processing Standard (FIPS) 140-2.

É altamente recomendável que nunca sejam colocadas informações de identificação confidenciais, como endereços de email dos seus clientes, em marcações ou campos de formato livre, como um campo Name (Nome). Isso inclui quando você trabalha com a Amazon DataZone ou outros Serviços da AWS usando o console, a API ou AWS os SDKs. AWS CLI Quaisquer dados inseridos em tags ou campos de texto de formato livre usados para nomes podem ser usados para logs de faturamento ou

de diagnóstico. Se você fornecer um URL para um servidor externo, recomendemos fortemente que não sejam incluídas informações de credenciais no URL para validar a solicitação a esse servidor.

Criptografia de dados

Ao conceder permissões, você decide quem está recebendo quais permissões para quais DataZone recursos da Amazon. Você habilita ações específicas que quer permitir nesses atributos. Portanto, você deve conceder apenas as permissões necessárias para executar uma tarefa. A implementação do acesso de privilégio mínimo é fundamental para reduzir o risco de segurança e o impacto que pode resultar de erros ou usuários mal-intencionados.

Criptografia inativa

A Amazon DataZone criptografa todos os seus dados por padrão com uma AWS chave do Key Management Service (AWS KMS) que AWS possui e gerencia para você. Você também pode criptografar os dados armazenados no DataZone catálogo da Amazon usando chaves que você gerencia com o AWS KMS.

Ao criar um domínio na Amazon DataZone, você pode fornecer configurações de criptografia marcando a caixa de seleção ao lado de Personalizar configurações de criptografia (avançadas) em Criptografia de dados e fornecendo uma chave KMS.

Criptografia em trânsito

A Amazon DataZone usa Transport Layer Security (TLS) e criptografia do lado do cliente para criptografia em trânsito. A comunicação com a Amazon DataZone é sempre feita por HTTPS para que seus dados sejam sempre criptografados em trânsito.

Privacidade do tráfego entre redes

Para proteger as conexões entre contas, a Amazon DataZone usa funções de serviço e funções do IAM para se conectar com segurança às contas dos clientes e executar operações em nome do cliente.

Tópicos

- Criptografia de dados em repouso para a Amazon DataZone
- Usando endpoints de interface VPC para Amazon DataZone

Criptografia de dados em repouso para a Amazon DataZone

A criptografia de dados em repouso por padrão ajuda a reduzir a sobrecarga operacional e a complexidade envolvidas na proteção de dados confidenciais. Ao mesmo tempo, ela permite que você crie aplicações seguras que atendam aos rigorosos requisitos regulatórios e de conformidade de criptografia.

A Amazon DataZone usa chaves AWS de propriedade padrão para criptografar automaticamente seus dados em repouso. Você não pode visualizar, gerenciar ou auditar o uso de chaves AWS próprias. Para obter mais informações, consulte chaves AWS próprias.

Embora você não possa desativar essa camada de criptografia ou selecionar um tipo de criptografia alternativo, você pode adicionar uma segunda camada de criptografia sobre as chaves de AWS criptografia existentes escolhendo uma chave gerenciada pelo cliente ao criar seus domínios da Amazon DataZone . A Amazon DataZone oferece suporte ao uso de chaves simétricas gerenciadas pelo cliente que você pode criar, possuir e gerenciar para adicionar uma segunda camada de criptografia sobre a criptografia existente AWS . Como você tem controle total dessa camada de criptografia, nela você pode realizar as seguintes tarefas:

- Estabeleça e mantenha as principais políticas
- Estabelecer e manter políticas e subsídios do IAM
- Ativar e desativar as principais políticas
- Gire o material criptográfico da chave
- Adicionar tags
- Crie aliases de chave
- Programar chaves para exclusão

Para obter mais informações, consulte Chaves gerenciadas pelo cliente.

> **Note**
>
> A Amazon habilita DataZone automaticamente a criptografia em repouso usando chaves AWS próprias para proteger os dados do cliente sem nenhum custo.
> AWS As cobranças do KMS se aplicam ao uso de chaves gerenciadas pelo cliente. Para obter mais informações sobre preços, consulte AWS Key Management Service Pricing.

Como a Amazon DataZone usa subsídios no AWS KMS

A Amazon DataZone exige três concessões para usar sua chave gerenciada pelo cliente. Quando você cria um DataZone domínio da Amazon criptografado com uma chave gerenciada pelo cliente, a Amazon DataZone cria concessões e subconcessões em seu nome enviando CreateGrantsolicitações para o AWS KMS. Os subsídios no AWS KMS são usados para dar DataZone à Amazon acesso a uma chave KMS em sua conta. DataZone A Amazon cria as seguintes concessões para usar sua chave gerenciada pelo cliente para as seguintes operações internas:

Uma concessão para criptografar seus dados em repouso para as seguintes operações:

- Envie DescribeKeysolicitações ao AWS KMS para verificar se a ID simétrica da chave KMS gerenciada pelo cliente inserida ao criar uma coleção de DataZone domínios da Amazon é válida.
- Envie GenerateDataKeyrequestspara o AWS KMS para gerar chaves de dados criptografadas pela chave gerenciada pelo cliente.
- Envie solicitações de descriptografia ao AWS KMS para descriptografar as chaves de dados criptografadas para que elas possam ser usadas para criptografar seus dados.
- RetireGrantpara retirar a concessão quando o domínio for excluído.

Duas bolsas para pesquisa e descoberta de seus dados:

- Subsídio 2:
  - DescribeKey
  - GenerateDataKey
  - Criptografar, descriptografar, ReEncrypt
  - CreateGrantpara criar bolsas infantis para AWS serviços usados internamente pela DataZone.
  - RetireGrant
- Subsídio 3:
  - GenerateDataKey
  - Decrypt
  - RetireGrant

É possível revogar o acesso à concessão, ou remover o acesso do serviço à chave gerenciada pelo cliente a qualquer momento. Se você fizer isso, a Amazon DataZone não poderá acessar nenhum dos dados criptografados pela chave gerenciada pelo cliente, o que afeta as operações

que dependem desses dados. Por exemplo, se você tentar obter detalhes de ativos de dados que a Amazon não DataZone pode acessar, a operação retornará um `AccessDeniedException` erro.

Crie uma chave gerenciada pelo cliente

Você pode criar uma chave simétrica gerenciada pelo cliente usando o AWS Management Console ou as APIs do AWS KMS.

Para criar uma chave simétrica gerenciada pelo cliente, siga as etapas para Criar uma chave simétrica gerenciada pelo cliente no Guia do desenvolvedor do AWS Key Management Service.

Política-chave - as principais políticas controlam o acesso à sua chave gerenciada pelo cliente. Cada chave gerenciada pelo cliente deve ter exatamente uma política de chaves, que contém declarações que determinam quem pode usar a chave e como pode usá-la. Ao criar a chave gerenciada pelo cliente, você pode especificar uma política de chaves. Para obter mais informações, consulte Gerenciando o acesso às chaves gerenciadas pelo cliente no Guia do desenvolvedor do AWS Key Management Service.

Para usar sua chave gerenciada pelo cliente com seus DataZone recursos da Amazon, as seguintes operações de API devem ser permitidas na política de chaves:

- kms: CreateGrant — adiciona uma concessão a uma chave gerenciada pelo cliente. Concede acesso de controle a uma chave KMS especificada, que permite o acesso às operações de concessão DataZone exigidas pela Amazon. Para obter mais informações sobre o uso de concessões, consulte o Guia do desenvolvedor do AWS Key Management Service.
- kms: DescribeKey — fornece os detalhes da chave gerenciada pelo cliente para permitir que DataZone a Amazon valide a chave.
- kms: GenerateDataKey — retorna uma chave de dados simétrica exclusiva para uso fora do AWS KMS.
- kms:Decrypt — descriptografa o texto cifrado que foi criptografado por uma chave KMS.

Veja a seguir exemplos de declarações de política que você pode adicionar para a 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**
>
> A negação da política do KMS não é aplicada aos recursos acessados por meio do portal de DataZone dados da Amazon.

Para obter mais informações sobre a especificação de permissões em uma política, consulte o Guia do desenvolvedor do AWS Key Management Service.

Para obter mais informações sobre como solucionar problemas de acesso à chave, consulte o Guia do desenvolvedor do AWS Key Management Service.

Especificação de uma chave gerenciada pelo cliente para a Amazon DataZone

Contexto DataZone de criptografia da Amazon

Um contexto de criptografia é um conjunto opcional de pares chave-valor que contêm informações contextuais adicionais sobre os dados.

AWS O KMS usa o contexto de criptografia como dados autenticados adicionais para oferecer suporte à criptografia autenticada. Quando você inclui um contexto de criptografia em uma solicitação para criptografar dados, o AWS KMS vincula o contexto de criptografia aos dados criptografados. Para descriptografar os dados, você inclui o mesmo contexto de criptografia na solicitação.

A Amazon DataZone usa o seguinte contexto de criptografia:

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

Uso do contexto de criptografia para monitoramento — quando você usa uma chave simétrica gerenciada pelo cliente para criptografar a Amazon DataZone, você também pode usar o contexto de criptografia em registros e registros de auditoria para identificar como a chave gerenciada pelo cliente está sendo usada. O contexto de criptografia também aparece nos registros gerados pelo AWS CloudTrail ou Amazon CloudWatch Logs.

Usando o contexto de criptografia para controlar o acesso à sua chave gerenciada pelo cliente - você pode usar o contexto de criptografia nas políticas de chaves e nas políticas do IAM como condições para controlar o acesso à sua chave simétrica gerenciada pelo cliente. Você também pode usar restrições no contexto de criptografia em uma concessão.

A Amazon DataZone usa uma restrição de contexto de criptografia nas concessões para controlar o acesso à chave gerenciada pelo cliente em sua conta ou região. A restrição da concessão exige que as operações permitidas pela concessão usem o contexto de criptografia especificado.

Veja a seguir exemplos de declarações de políticas de chave para conceder acesso a uma chave gerenciada pelo cliente para um contexto de criptografia específico. A condição nesta declaração de política exige que as concessões tenham uma restrição de contexto de criptografia que especifique o contexto de criptografia.

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

Monitorando suas chaves de criptografia para a Amazon DataZone

Ao usar uma chave gerenciada pelo cliente do AWS KMS com seus DataZone recursos da Amazon, você pode usá-la AWS CloudTrailpara rastrear solicitações que a Amazon DataZone envia para o AWS KMS. Os exemplos a seguir são AWS CloudTrail eventos para`CreateGrant`, `GenerateDataKeyDecrypt`, e `DescribeKey` para monitorar operações KMS chamadas pela Amazon DataZone para acessar dados criptografados pela chave gerenciada pelo cliente. Quando você usa uma chave AWS KMS gerenciada pelo cliente para criptografar seu DataZone domínio Amazon, a Amazon DataZone envia uma `CreateGrant` solicitação em seu nome para acessar a chave KMS em sua conta. AWS As concessões que a Amazon DataZone cria são específicas para o recurso associado à chave gerenciada pelo cliente do AWS KMS. Além disso, a Amazon DataZone usa a `RetireGrant` operação para remover uma concessão quando você exclui um domínio. O evento de exemplo a seguir registra a operação `CreateGrant`:

```
{
    "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"
}
```

Criação de ambientes Data Lake que envolvam catálogos criptografados do AWS Glue

Em casos de uso avançados, ao trabalhar com um catálogo do AWS Glue criptografado, você deve conceder acesso ao DataZone serviço da Amazon para usar sua chave KMS gerenciada pelo cliente. Você pode fazer isso atualizando sua política personalizada do KMS e adicionando uma tag à chave. Para conceder acesso ao DataZone serviço da Amazon para trabalhar com dados em um catálogo criptografado do AWS Glue, preencha o seguinte:

- Adicione a política a seguir à sua chave KMS personalizada. Para obter mais informações, consulte Alterar uma política de chaves.

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

- Adicione a tag a seguir à sua chave KMS personalizada. Para obter mais informações, consulte Usando tags para controlar o acesso às chaves KMS.

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

Usando endpoints de interface VPC para Amazon DataZone

Se você usa a Amazon Virtual Private Cloud (Amazon VPC) para hospedar seus AWS recursos, você pode estabelecer uma conexão entre sua Amazon VPC e a Amazon. DataZone Você pode usar essa conexão com a Amazon DataZone sem cruzar a Internet pública.

A Amazon VPC permite que você lance AWS recursos em uma rede virtual personalizada. Você pode usar uma VPC para controlar as configurações de rede, como o intervalo de endereços IP, sub-redes, tabelas de rotas e gateways de rede. Para obter informações sobre como criar suas próprias VPCs, consulte o Guia do usuário da Amazon VPC.

Para conectar sua Amazon VPC à Amazon DataZone, você deve primeiro definir uma interface VPC endpoint, que permite conectar sua VPC a outros serviços. AWS O endpoint fornece conectividade confiável e escalável sem a necessidade de um gateway da Internet, da instância de conversão de endereço de rede (NAT) ou de uma conexão VPN. Para obter mais informações e etapas detalhadas sobre como criar um VPC endpoint, consulte Interface VPC Endpoints () no Guia do usuário AWS PrivateLink da Amazon VPC.

> **Important**
>
> Na VPC, uma política de endpoint é uma política baseada em recursos que você pode anexar a um endpoint da VPC para controlar quais AWS entidades principais podem usar o endpoint para acessar um serviço. AWS
> Na versão atual da Amazon DataZone, o uso de políticas de endpoint não é suportado para estabelecer e usar conexões entre sua Amazon VPC e a Amazon. DataZone O gerenciamento de DataZone acesso da Amazon depende da configuração da RAM e das principais políticas do IAM que são definidas no nível do serviço.

Autorização na Amazon DataZone

A interface DataZone da Amazon consiste em um console de gerenciamento dentro AWS e um aplicativo web fora do console (portal de dados).

O console DataZone de gerenciamento da Amazon pode ser usado por AWS administradores para top-level-resource APIs, incluindo a criação e o gerenciamento de domínios, associações de AWS contas para esses domínios e fontes de dados para as quais você deseja delegar o gerenciamento de acesso à Amazon. DataZone Você pode usar o console DataZone de gerenciamento da Amazon para gerenciar todas as funções e configurações do IAM necessárias para delegar o controle de gerenciamento de acesso ao DataZone serviço da Amazon para suas contas explicitamente configuradas AWS . O portal de DataZone dados da Amazon é um aplicativo primário do AWS Identity Center para usuários de SSO. Se ativado, o console também pode ser usado por diretores autorizados do IAM para se federar no portal de dados em vez de usar uma identidade de SSO.

O portal DataZone de dados da Amazon foi projetado para ser usado principalmente por usuários autenticados pelo AWS IAM Identity Center para gerenciar o acesso aos dados e realizar tarefas de publicação, descoberta, assinatura e análise de dados.

Autorização no DataZone console da Amazon

O modelo de autorização DataZone do console da Amazon usa a autorização do IAM. O console é usado pelos administradores principalmente para configuração. A Amazon DataZone usa o conceito de AWS conta de administrador de domínio e AWS contas de membros, e o console é usado em todas essas contas para criar relações de confiança, respeitando os limites AWS da organização.

Autorização no DataZone portal da Amazon

O modelo de autorização do portal de DataZone dados da Amazon é uma ACL hierárquica com arquétipos de função (perfis) estáticos que incluem administradores e visualizadores. Por exemplo, os usuários podem ter um perfil de administrador ou usuário. No nível de um domínio, eles podem ter uma designação de usuário de domínio como proprietário dos dados. No nível de um projeto, um usuário pode ser proprietário ou colaborador. Esses perfis podem ser configurados como um dos dois tipos: usuários e grupos. Esses perfis são então associados a domínios e projetos, e o estado dessas permissões é armazenado em uma tabela de associação.

Dentro desse modelo de autorização, a Amazon DataZone permite que os usuários gerenciem as permissões de usuários e grupos. Os usuários gerenciam a associação ao projeto, solicitam a

associação a projetos e aprovam as associações. Os usuários publicam dados, definem aprovadores de assinaturas de dados, assinam dados e aprovam assinaturas.

Os usuários realizam análises de dados em projetos específicos quando o cliente do portal de dados solicita credenciais de sessão do IAM que a Amazon DataZone gera com base no perfil efetivo do usuário no contexto específico do projeto. Essa sessão tem como escopo as permissões do usuário e também os recursos específicos do projeto. Em seguida, os usuários acessam o Athena ou o Redshift para consultar os dados relevantes, e todo o trabalho subjacente do IAM é completamente abstraído.

DataZone Perfis e funções da Amazon

Depois que um usuário é autenticado, o contexto autenticado é mapeado para uma ID de perfil de usuário. Esse perfil de usuário pode ter várias associações diferentes (proprietário do projeto, administrador do domínio etc.) que são usadas para autorizar usuários. Cada associação (por exemplo, proprietário do projeto, administrador do domínio etc.) tem permissões para determinadas atividades com base no contexto. Por exemplo, um usuário que tenha uma associação de administrador de domínio pode criar domínios adicionais, atribuir outros administradores de domínio ao domínio e criar modelos de projeto em seu domínio. O proprietário do projeto pode adicionar ou remover membros do projeto, criar contratos de publicação com um domínio e publicar ativos em um domínio.

Controle do acesso aos DataZone recursos da Amazon usando o IAM

Você precisa AWS Identity and Access Management (IAM) concluir as seguintes tarefas relacionadas à segurança:

- Crie usuários e grupos sob o seu Conta da AWS.
- Atribua credenciais de segurança exclusivas a cada usuário abaixo do seu Conta da AWS.
- Controle as permissões de cada usuário para realizar tarefas com AWS recursos.
- Permita que os usuários de outra pessoa Conta da AWS compartilhem seus AWS recursos.
- Crie funções para você Conta da AWS e defina os usuários ou serviços que podem assumi-las.
- Use identidades existentes para sua empresa para conceder permissões para realizar tarefas usando recursos AWS

Para obter mais informações sobre IAM, consulte o seguinte:

- AWS Identity and Access Management (IAM)
- Conceitos básicos
- Guia do usuário do IAM

As seções a seguir descrevem as políticas e permissões necessárias para configurar a Amazon DataZone e seus componentes, como domínios (incluindo o domínio), contas associadas, projetos e fontes de dados. Para ter mais informações, consulte DataZone Terminologia e conceitos da Amazon.

Conteúdo

AWS políticas gerenciadas para a Amazon DataZone

Uma política AWS gerenciada é uma política autônoma criada e administrada por AWS. AWS as políticas gerenciadas são projetadas para fornecer permissões para muitos casos de uso comuns, para que você possa começar a atribuir permissões a usuários, grupos e funções.

Lembre-se de que as políticas AWS gerenciadas podem não conceder permissões de privilégio mínimo para seus casos de uso específicos porque elas estão disponíveis para uso de todos os AWS clientes. Recomendamos que você reduza ainda mais as permissões definindo políticas gerenciadas pelo cliente da específicas para seus casos de uso.

Você não pode alterar as permissões definidas nas políticas AWS gerenciadas. Se AWS atualizar as permissões definidas em uma política AWS gerenciada, a atualização afetará todas as identidades principais (usuários, grupos e funções) às quais a política está anexada. AWS é mais provável que atualize uma política AWS gerenciada quando uma nova AWS service (Serviço da AWS) for lançada ou novas operações de API forem disponibilizadas para serviços existentes.

Para mais informações, consulte Políticas gerenciadas pela AWS no Manual do usuário do IAM.

Conteúdo

AWS política gerenciada: AmazonDataZoneFullAccess

É possível anexar a política `AmazonDataZoneFullAccess` a suas identidades do IAM.

Esta política fornece acesso total à Amazon DataZone por meio do AWS Management Console.

Detalhes de permissão

Esta política inclui as seguintes permissões:

- `datazone`— concede aos diretores acesso total à Amazon DataZone por meio do AWS Management Console.
- `kms`— Permite que os diretores listem aliases e descrevam as chaves.
- `s3`— Permite que os diretores escolham buckets S3 existentes ou criem novos para armazenar dados da Amazon. DataZone
- `ram`— Permite que os diretores compartilhem DataZone domínios da Amazon entre. Contas da AWS
- `iam`— Permite que os diretores listem e aprovem funções e obtenham políticas.
- `sso`— Permite que os diretores obtenham as regiões em que AWS IAM Identity Center está habilitado.

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Sid": "AmazonDataZoneStatement",
      "Effect": "Allow",
      "Action": [
        "datazone:*"
      ],
      "Resource": [
        "*"
      ]
    },
    {
      "Sid": "ReadOnlyStatement",
      "Effect": "Allow",
      "Action": [
        "kms:DescribeKey",
        "kms:ListAliases",
        "iam:ListRoles",
        "sso:DescribeRegisteredRegions",
        "s3:ListAllMyBuckets",
        "redshift:DescribeClusters",
        "redshift-serverless:ListWorkgroups",
        "ec2:DescribeSecurityGroups",
        "ec2:DescribeSubnets",
        "ec2:DescribeVpcs",
        "secretsmanager:ListSecrets"
      ],
      "Resource": [
        "*"
      ]
    },
    {
      "Sid": "BucketReadOnlyStatement",
      "Effect": "Allow",
      "Action": [
        "s3:ListBucket",
        "s3:GetBucketLocation"
      ],
      "Resource": "arn:aws:s3:::*"
    },
```

```
    {
      "Sid": "CreateBucketStatement",
      "Effect": "Allow",
      "Action": "s3:CreateBucket",
      "Resource": "arn:aws:s3:::amazon-datazone*"
    },
    {
      "Sid": "RamCreateResourceStatement",
      "Effect": "Allow",
      "Action": [
        "ram:CreateResourceShare"
      ],
      "Resource": "*",
      "Condition": {
        "StringEqualsIfExists": {
          "ram:RequestedResourceType": "datazone:Domain"
        }
      }
    },
    {
      "Sid": "RamResourceStatement",
      "Effect": "Allow",
      "Action": [
        "ram:DeleteResourceShare",
        "ram:AssociateResourceShare",
        "ram:DisassociateResourceShare",
        "ram:RejectResourceShareInvitation"
      ],
      "Resource": "*",
      "Condition": {
        "StringLike": {
          "ram:ResourceShareName": [
            "DataZone*"
          ]
        }
      }
    },
    {
      "Sid": "RamResourceReadOnlyStatement",
      "Effect": "Allow",
      "Action": [
        "ram:GetResourceShares",
        "ram:GetResourceShareInvitations",
        "ram:GetResourceShareAssociations"
```

```
      ],
      "Resource": "*"
    },
    {
      "Sid": "IAMPassRoleStatement",
      "Effect": "Allow",
      "Action": "iam:PassRole",
      "Resource": [
        "arn:aws:iam::*:role/AmazonDataZone*",
        "arn:aws:iam::*:role/service-role/AmazonDataZone*"
      ],
      "Condition": {
        "StringEquals": {
          "iam:passedToService": "datazone.amazonaws.com"
        }
      }
    },
    {
      "Sid": "IAMGetPolicyStatement",
      "Effect": "Allow",
      "Action": "iam:GetPolicy",
      "Resource": [
        "arn:aws:iam::*:policy/service-role/AmazonDataZoneRedshiftAccessPolicy*"
      ]
    },
    {
      "Sid": "DataZoneTagOnCreate",
      "Effect": "Allow",
      "Action": [
        "secretsmanager:TagResource"
      ],
      "Resource": "arn:aws:secretsmanager:*:*:secret:AmazonDataZone-*",
      "Condition": {
        "ForAllValues:StringEquals": {
          "aws:TagKeys": [
            "AmazonDataZoneDomain"
          ]
        },
        "StringLike": {
          "aws:RequestTag/AmazonDataZoneDomain": "dzd_*",
          "aws:ResourceTag/AmazonDataZoneDomain": "dzd_*"
        },
        "Null": {
          "aws:TagKeys": "false"
```

```
        }
      }
    },
    {
      "Sid": "CreateSecretStatement",
      "Effect": "Allow",
      "Action": [
        "secretsmanager:CreateSecret"
      ],
      "Resource": "arn:aws:secretsmanager:*:*:secret:AmazonDataZone-*",
      "Condition": {
        "StringLike": {
          "aws:RequestTag/AmazonDataZoneDomain": "dzd_*"
        }
      }
    }
  ]
}
```

Considerações e limitações políticas

Há certas funcionalidades que a `AmazonDataZoneFullAccess` apólice não cobre.

- Se você criar um DataZone domínio da Amazon com sua própria AWS KMS chave, deverá ter as permissões `kms:CreateGrant` para que a criação do domínio seja bem-sucedida e `kms:Decrypt` para `kms:GenerateDataKey` que essa chave invoque outras DataZone APIs da Amazon, como e. `listDataSources` `createDataSource` E você também deve ter as permissões para `kms:CreateGrant``kms:Decrypt`,`kms:GenerateDataKey`, e `kms:DescribeKey` na política de recursos dessa chave.

  Se você usar a chave KMS padrão de propriedade do serviço, isso não será necessário.

  Para ter mais informações, consulte AWS Key Management Service.
- Se você quiser usar as funcionalidades de criação e atualização de funções no DataZone console da Amazon, você deve ter privilégios de administrador ou ter as permissões necessárias do IAM para criar funções do IAM e criar/atualizar políticas. As permissões necessárias incluem `iam:CreateRole``iam:CreatePolicy`,`iam:CreatePolicyVersion`,`iam:DeletePolicyVersion`, e `iam:AttachRolePolicy` permissões.
- Se você criar um novo domínio na Amazon DataZone com o login de AWS IAM Identity Center usuário ativado, ou se você ativá-lo para um domínio

existente na Amazon DataZone, você deve ter permissões para o seguinte: `sso:CreateManagedApplicationInstancesso:DeleteManagedApplicationInstance`,, `sso:PutApplicationAssignmentConfiguration` e.

- Para aceitar uma solicitação de associação de AWS conta na Amazon DataZone, você deve ter a `ram:AcceptResourceShareInvitation` permissão.

AWS política gerenciada: AmazonDataZoneFullUserAccess

Essa política concede acesso total à Amazon DataZone, mas não permite o gerenciamento de domínios, usuários ou contas associadas.

Detalhes da permissão

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Sid": "AmazonDataZoneUserOperations",
      "Effect": "Allow",
      "Action": [
        "datazone:GetDomain",
        "datazone:CreateFormType",
        "datazone:GetFormType",
        "datazone:GetIamPortalLoginUrl",
        "datazone:SearchUserProfiles",
        "datazone:SearchGroupProfiles",
        "datazone:GetUserProfile",
        "datazone:GetGroupProfile",
        "datazone:ListGroupsForUser",
        "datazone:DeleteFormType",
        "datazone:CreateAssetType",
        "datazone:GetAssetType",
        "datazone:DeleteAssetType",
        "datazone:CreateGlossary",
        "datazone:GetGlossary",
        "datazone:DeleteGlossary",
        "datazone:UpdateGlossary",
        "datazone:CreateGlossaryTerm",
        "datazone:GetGlossaryTerm",
        "datazone:DeleteGlossaryTerm",
        "datazone:UpdateGlossaryTerm",
```

```
        "datazone:CreateAsset",
        "datazone:GetAsset",
        "datazone:DeleteAsset",
        "datazone:CreateAssetRevision",
        "datazone:ListAssetRevisions",
        "datazone:AcceptPredictions",
        "datazone:RejectPredictions",
        "datazone:Search",
        "datazone:SearchTypes",
        "datazone:CreateListingChangeSet",
        "datazone:DeleteListing",
        "datazone:SearchListings",
        "datazone:GetListing",
        "datazone:CreateDataSource",
        "datazone:GetDataSource",
        "datazone:DeleteDataSource",
        "datazone:UpdateDataSource",
        "datazone:ListDataSources",
        "datazone:StartDataSourceRun",
        "datazone:GetDataSourceRun",
        "datazone:ListDataSourceRuns",
        "datazone:ListDataSourceRunActivities",
        "datazone:ListEnvironmentBlueprintConfigurations",
        "datazone:CreateEnvironmentBlueprint",
        "datazone:GetEnvironmentBlueprint",
        "datazone:DeleteEnvironmentBlueprint",
        "datazone:UpdateEnvironmentBlueprint",
        "datazone:ListEnvironmentBlueprints",
        "datazone:CreateProject",
        "datazone:UpdateProject",
        "datazone:GetProject",
        "datazone:DeleteProject",
        "datazone:ListProjects",
        "datazone:CreateProjectMembership",
        "datazone:DeleteProjectMembership",
        "datazone:ListProjectMemberships",
        "datazone:CreateEnvironmentProfile",
        "datazone:GetEnvironmentProfile",
        "datazone:UpdateEnvironmentProfile",
        "datazone:DeleteEnvironmentProfile",
        "datazone:ListEnvironmentProfiles",
        "datazone:CreateEnvironment",
        "datazone:GetEnvironment",
        "datazone:DeleteEnvironment",
```

```
        "datazone:UpdateEnvironment",
        "datazone:UpdateEnvironmentDeploymentStatus",
        "datazone:ListEnvironments",
        "datazone:ListAccountEnvironments",
        "datazone:GetEnvironmentActionLink",
        "datazone:GetEnvironmentCredentials",
        "datazone:GetSubscriptionTarget",
        "datazone:DeleteSubscriptionTarget",
        "datazone:ListSubscriptionTargets",
        "datazone:CreateSubscriptionRequest",
        "datazone:AcceptSubscriptionRequest",
        "datazone:UpdateSubscriptionRequest",
        "datazone:ListWarehouseMetadata",
        "datazone:RejectSubscriptionRequest",
        "datazone:GetSubscriptionRequestDetails",
        "datazone:ListSubscriptionRequests",
        "datazone:DeleteSubscriptionRequest",
        "datazone:GetSubscription",
        "datazone:CancelSubscription",
        "datazone:GetSubscriptionEligibility",
        "datazone:ListSubscriptions",
        "datazone:RevokeSubscription",
        "datazone:CreateSubscriptionGrant",
        "datazone:DeleteSubscriptionGrant",
        "datazone:GetSubscriptionGrant",
        "datazone:ListSubscriptionGrants",
        "datazone:UpdateSubscriptionGrantStatus",
        "datazone:ListNotifications",
        "datazone:StartMetadataGenerationRun",
        "datazone:GetMetadataGenerationRun",
        "datazone:CancelMetadataGenerationRun",
        "datazone:ListMetadataGenerationRuns"
      ],
      "Resource": "*"
    },
    {
      "Sid": "RAMResourceShareOperations",
      "Effect": "Allow",
      "Action": "ram:GetResourceShareAssociations",
      "Resource": "*"
    }
  ]
}
```

AWS política gerenciada: AmazonDataZoneCustomEnvironmentDeploymentPolicy

Você pode usar essa política para atualizar a configuração de ambientes criados usando blueprints personalizados. Essa política também pode ser usada para criar metas de DataZone assinatura e fontes de dados da Amazon.

Detalhes da permissão

```
{
 "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 política gerenciada: AmazonDataZoneEnvironmentRolePermissionsBoundary

> **Note**
>
> Essa política é um limite de permissões. Um limite de permissões define o máximo de permissões que uma política baseada em identidade pode conceder a uma entidade do IAM. Você não deve usar e anexar as políticas de limite de DataZone permissões da Amazon

sozinho. As políticas de limite de DataZone permissões da Amazon só devem ser anexadas às funções DataZone gerenciadas pela Amazon. Para obter mais informações sobre limites de permissões, consulte Limites de permissões para entidades do IAM no Guia do usuário do IAM.

Quando você cria um ambiente por meio do portal de DataZone dados da Amazon, a Amazon DataZone aplica esse limite de permissões às funções do IAM que são produzidas durante a criação do ambiente. O limite de permissões limita o escopo das funções que a Amazon DataZone cria e de todas as funções que você adiciona.

A Amazon DataZone usa a política `AmazonDataZoneEnvironmentRolePermissionsBoundary` gerenciada para limitar o principal do IAM provisionado ao qual ela está vinculada. Os diretores podem assumir a forma das funções de usuário que a Amazon DataZone pode assumir em nome de usuários corporativos interativos ou serviços analíticos (AWS Glue por exemplo) e, em seguida, realizar ações para processar dados, como leitura e gravação do Amazon S3 ou execução. Crawler do AWS Glue

A `AmazonDataZoneEnvironmentRolePermissionsBoundary` política concede acesso de leitura e gravação para DataZone a Amazon a serviços como AWS Glue Amazon S3 AWS Lake Formation, Amazon Redshift e Amazon Athena. A política também concede permissões de leitura e gravação a alguns recursos de infraestrutura necessários para usar esses serviços, como AWS KMS chaves e interfaces de rede.

A Amazon DataZone aplica a política `AmazonDataZoneEnvironmentRolePermissionsBoundary` AWS gerenciada como um limite de permissões para todas as funções do DataZone ambiente da Amazon (proprietário e colaborador). Esse limite de permissões restringe essas funções para permitir apenas o acesso aos recursos e ações necessários para um ambiente.

O limite inclui as seguintes declarações 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 política gerenciada: AmazonDataZoneRedshiftGlueProvisioningPolicy

A AmazonDataZoneRedshiftGlueProvisioningPolicy política concede à Amazon DataZone as permissões necessárias para interoperar com o AWS Glue e o 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 política gerenciada: AmazonDataZoneGlueManageAccessRolePolicy

Essa política concede à Amazon DataZone permissões para publicar dados do AWS Glue no catálogo. Também concede à Amazon DataZone permissões para conceder acesso ou revogar o acesso aos ativos publicados do AWS Glue no catálogo.

```
{
 "Version": "2012-10-17",
 "Statement": [
  {
   "Sid": "GlueDataQualityPermissions",
   "Effect": "Allow",
   "Action": [
    "glue:ListDataQualityResults",
    "glue:GetDataQualityResult"
   ],
   "Resource": "arn:aws:glue:*:*:dataQualityRuleset/*",
   "Condition": {
    "StringEquals": {
     "aws:ResourceAccount": "${aws:PrincipalAccount}"
    }
   }
  },
  {
   "Sid": "GlueTableDatabasePermissions",
```

```
    "Effect": "Allow",
    "Action": [
     "glue:CreateTable",
     "glue:DeleteTable",
     "glue:GetDatabases",
     "glue:GetTables"
    ],
    "Resource": [
     "arn:aws:glue:*:*:catalog",
     "arn:aws:glue:*:*:database/*",
     "arn:aws:glue:*:*:table/*"
    ],
    "Condition": {
     "StringEquals": {
      "aws:ResourceAccount": "${aws:PrincipalAccount}"
     }
    }
   },
   {
    "Sid": "LakeformationResourceSharingPermissions",
    "Effect": "Allow",
    "Action": [
     "lakeformation:BatchGrantPermissions",
     "lakeformation:BatchRevokePermissions",
     "lakeformation:CreateLakeFormationOptIn",
     "lakeformation:DeleteLakeFormationOptIn",
     "lakeformation:GrantPermissions",
     "lakeformation:GetResourceLFTags",
     "lakeformation:ListLakeFormationOptIns",
     "lakeformation:ListPermissions",
     "lakeformation:RegisterResource",
     "lakeformation:RevokePermissions",
     "glue:GetDatabase",
     "glue:GetTable",
     "organizations:DescribeOrganization",
     "ram:GetResourceShareInvitations",
     "ram:ListResources"
    ],
    "Resource": "*"
   },
   {
    "Sid": "CrossAccountRAMResourceSharingPermissions",
    "Effect": "Allow",
    "Action": [
```

```
    "glue:DeleteResourcePolicy",
    "glue:PutResourcePolicy"
   ],
   "Resource": [
    "arn:aws:glue:*:*:catalog",
    "arn:aws:glue:*:*:database/*",
    "arn:aws:glue:*:*:table/*"
   ],
   "Condition": {
    "ForAnyValue:StringEquals": {
     "aws:CalledVia": [
      "ram.amazonaws.com"
     ]
    }
   }
  },
  {
   "Sid": "CrossAccountLakeFormationResourceSharingPermissions",
   "Effect": "Allow",
   "Action": [
    "ram:CreateResourceShare"
   ],
   "Resource": "*",
   "Condition": {
    "StringEqualsIfExists": {
     "ram:RequestedResourceType": [
      "glue:Table",
      "glue:Database",
      "glue:Catalog"
     ]
    },
    "ForAnyValue:StringEquals": {
     "aws:CalledVia": [
      "lakeformation.amazonaws.com"
     ]
    }
   }
  },
  {
   "Sid": "CrossAccountRAMResourceShareInvitationPermission",
   "Effect": "Allow",
   "Action": [
    "ram:AcceptResourceShareInvitation"
   ],
```

```
    "Resource": "arn:aws:ram:*:*:resource-share-invitation/*"
   },
   {
    "Sid": "CrossAccountRAMResourceSharingViaLakeFormationPermissions",
    "Effect": "Allow",
    "Action": [
     "ram:AssociateResourceShare",
     "ram:DeleteResourceShare",
     "ram:DisassociateResourceShare",
     "ram:GetResourceShares",
     "ram:ListResourceSharePermissions",
     "ram:UpdateResourceShare"
    ],
    "Resource": "*",
    "Condition": {
     "StringLike": {
      "ram:ResourceShareName": [
       "LakeFormation*"
      ]
     },
     "ForAnyValue:StringEquals": {
      "aws:CalledVia": [
       "lakeformation.amazonaws.com"
      ]
     }
    }
   },
   {
    "Sid": "CrossAccountRAMResourceSharingViaLakeFormationHybrid",
    "Effect": "Allow",
    "Action": "ram:AssociateResourceSharePermission",
    "Resource": "*",
    "Condition": {
     "StringLike": {
      "ram:PermissionArn": "arn:aws:ram::aws:permission/AWSRAMLFEnabled*"
     },
     "ForAnyValue:StringEquals": {
      "aws:CalledVia": [
       "lakeformation.amazonaws.com"
      ]
     }
    }
   },
   {
```

```
    "Sid": "KMSDecryptPermission",
    "Effect": "Allow",
    "Action": [
     "kms:Decrypt"
    ],
    "Resource": "*",
    "Condition": {
     "StringEquals": {
      "aws:ResourceTag/datazone:projectId": "proj-all"
     }
    }
   },
   {
    "Sid": "GetRoleForDataZone",
    "Effect": "Allow",
    "Action": [
     "iam:GetRole"
    ],
    "Resource": [
     "arn:aws:iam::*:role/AmazonDataZone*",
     "arn:aws:iam::*:role/service-role/AmazonDataZone*"
    ]
   },
   {
    "Sid": "PassRoleForDataLocationRegistration",
    "Effect": "Allow",
    "Action": [
     "iam:PassRole"
    ],
    "Resource": [
     "arn:aws:iam::*:role/AmazonDataZone*",
     "arn:aws:iam::*:role/service-role/AmazonDataZone*"
    ],
    "Condition": {
     "StringEquals": {
      "iam:PassedToService": [
       "lakeformation.amazonaws.com"
      ]
     }
    }
   }
  ]
}
```

AWS política gerenciada: AmazonDataZoneRedshiftManageAccessRolePolicy

Essa política concede à Amazon DataZone permissões para publicar dados do Amazon Redshift no catálogo. Também concede à Amazon DataZone permissões para conceder acesso ou revogar o acesso aos ativos publicados do Amazon Redshift ou do Amazon Redshift Serverless no catálogo.

```
{
 "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 Política gerenciada da : AmazonDataZoneCrossAccountAdmin

Você pode anexar a AmazonDataZoneCrossAccountAdmin política às suas identidades do IAM.

Essa política permite que os usuários trabalhem com contas DataZone associadas da 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 política gerenciada: AmazonDataZoneDomainExecutionRolePolicy

Essa é a política padrão para a função de DataZone `DomainExecutionRole` serviço da Amazon. Essa função é usada pela Amazon DataZone para catalogar, descobrir, controlar, compartilhar e analisar dados no DataZone domínio da Amazon.

Você pode anexar a AmazonDataZoneDomainExecutionRolePolicy política ao seu`AmazonDataZoneDomainExecutionRole`.

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Sid": "DomainExecutionRoleStatement",
      "Effect": "Allow",
      "Action": [
        "datazone:AcceptPredictions",
        "datazone:AcceptSubscriptionRequest",
        "datazone:CancelSubscription",
        "datazone:CreateAsset",
```

```
        "datazone:CreateAssetRevision",
        "datazone:CreateAssetType",
        "datazone:CreateDataSource",
        "datazone:CreateEnvironment",
        "datazone:CreateEnvironmentBlueprint",
        "datazone:CreateEnvironmentProfile",
        "datazone:CreateFormType",
        "datazone:CreateGlossary",
        "datazone:CreateGlossaryTerm",
        "datazone:CreateListingChangeSet",
        "datazone:CreateProject",
        "datazone:CreateProjectMembership",
        "datazone:CreateSubscriptionGrant",
        "datazone:CreateSubscriptionRequest",
        "datazone:DeleteAsset",
        "datazone:DeleteAssetType",
        "datazone:DeleteDataSource",
        "datazone:DeleteEnvironment",
        "datazone:DeleteEnvironmentBlueprint",
        "datazone:DeleteEnvironmentProfile",
        "datazone:DeleteFormType",
        "datazone:DeleteGlossary",
        "datazone:DeleteGlossaryTerm",
        "datazone:DeleteListing",
        "datazone:DeleteProject",
        "datazone:DeleteProjectMembership",
        "datazone:DeleteSubscriptionGrant",
        "datazone:DeleteSubscriptionRequest",
        "datazone:DeleteSubscriptionTarget",
        "datazone:GetAsset",
        "datazone:GetAssetType",
        "datazone:GetDataSource",
        "datazone:GetDataSourceRun",
        "datazone:GetDomain",
        "datazone:GetEnvironment",
        "datazone:GetEnvironmentActionLink",
        "datazone:GetEnvironmentBlueprint",
        "datazone:GetEnvironmentCredentials",
        "datazone:GetEnvironmentProfile",
        "datazone:GetFormType",
        "datazone:GetGlossary",
        "datazone:GetGlossaryTerm",
        "datazone:GetGroupProfile",
        "datazone:GetListing",
```

```
        "datazone:GetProject",
        "datazone:GetSubscription",
        "datazone:GetSubscriptionEligibility",
        "datazone:GetSubscriptionGrant",
        "datazone:GetSubscriptionRequestDetails",
        "datazone:GetSubscriptionTarget",
        "datazone:GetUserProfile",
        "datazone:ListAccountEnvironments",
        "datazone:ListAssetRevisions",
        "datazone:ListDataSourceRunActivities",
        "datazone:ListDataSourceRuns",
        "datazone:ListDataSources",
        "datazone:ListEnvironmentBlueprintConfigurations",
        "datazone:ListEnvironmentBlueprintConfigurationSummaries",
        "datazone:ListEnvironmentBlueprints",
        "datazone:ListEnvironmentProfiles",
        "datazone:ListEnvironments",
        "datazone:ListGroupsForUser",
        "datazone:ListNotifications",
        "datazone:ListProjectMemberships",
        "datazone:ListProjects",
        "datazone:ListSubscriptionGrants",
        "datazone:ListSubscriptionRequests",
        "datazone:ListSubscriptionTargets",
        "datazone:ListSubscriptions",
        "datazone:ListWarehouseMetadata",
        "datazone:RejectPredictions",
        "datazone:RejectSubscriptionRequest",
        "datazone:RevokeSubscription",
        "datazone:Search",
        "datazone:SearchGroupProfiles",
        "datazone:SearchListings",
        "datazone:SearchTypes",
        "datazone:SearchUserProfiles",
        "datazone:StartDataSourceRun",
        "datazone:UpdateDataSource",
        "datazone:UpdateEnvironment",
        "datazone:UpdateEnvironmentBlueprint",
        "datazone:UpdateEnvironmentDeploymentStatus",
        "datazone:UpdateEnvironmentProfile",
        "datazone:UpdateGlossary",
        "datazone:UpdateGlossaryTerm",
        "datazone:UpdateProject",
        "datazone:UpdateSubscriptionGrantStatus",
```

```
        "datazone:UpdateSubscriptionRequest",
        "datazone:StartMetadataGenerationRun",
        "datazone:GetMetadataGenerationRun",
        "datazone:CancelMetadataGenerationRun",
        "datazone:ListMetadataGenerationRuns"
      ],
      "Resource": "*"
    },
    {
      "Sid": "RAMResourceShareStatement",
      "Effect": "Allow",
      "Action": "ram:GetResourceShareAssociations",
      "Resource": "*"
    }
  ]
}
```

AWS política gerenciada: AmazonDataZoneSageMakerProvisioning

A AmazonDataZoneSageMakerProvisioning política concede à Amazon DataZone as permissões necessárias para interoperar com a 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 política gerenciada: AmazonDataZoneSageMakerAccess

Essa política concede à Amazon DataZone permissões para publicar SageMaker ativos da Amazon no catálogo. Também concede à Amazon DataZone permissões para conceder acesso ou revogar o acesso aos ativos SageMaker publicados pela Amazon no catálogo.

Esta política inclui permissões para fazer o seguinte:

- cloudtrail — recupere informações sobre trilhas. CloudTrail
- cloudwatch — recupera os alarmes atuais. CloudWatch
- logs — recupere os filtros métricos dos CloudWatch registros.
- sns — recupera a lista de assinaturas de um tópico do SNS.
- config — recupera informações sobre gravadores de configuração, recursos e regras de configuração AWS . Também permite que a função vinculada ao serviço crie e exclua regras AWS Config e execute avaliações com base nas regras.
- iam — obtenha e gere relatórios de credenciais para contas.
- organizações — recupere informações da conta e da unidade organizacional (OU) de uma organização.
- securityhub — recupere informações sobre como o serviço, os padrões e os controles do Security Hub estão configurados.
- tag — recupera informações sobre tags de recursos.

```
{
 "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 política gerenciada: AmazonDataZoneSageMakerEnvironmentRolePermissionsBoundary

> **Note**
>
> Essa política é um limite de permissões. Um limite de permissões define o máximo de permissões que uma política baseada em identidade pode conceder a uma entidade do IAM. Você não deve usar e anexar as políticas de limite de DataZone permissões da Amazon sozinho. As políticas de limite de DataZone permissões da Amazon só devem ser anexadas às funções DataZone gerenciadas pela Amazon. Para obter mais informações sobre limites de permissões, consulte Limites de permissões para entidades do IAM no Guia do usuário do IAM.

Quando você cria um SageMaker ambiente Amazon por meio do portal de DataZone dados da Amazon, a Amazon DataZone aplica esse limite de permissões às funções do IAM que são produzidas durante a criação do ambiente. O limite de permissões limita o escopo das funções que a Amazon DataZone cria e de todas as funções que você adiciona.

A Amazon DataZone usa a política `AmazonDataZoneSageMakerEnvironmentRolePermissionsBoundary` gerenciada para limitar o principal do IAM provisionado ao qual ela está vinculada. Os diretores podem assumir a forma das funções de usuário que a Amazon DataZone pode assumir em nome de usuários corporativos interativos ou serviços analíticos (por exemplo) e AWS SageMaker, em seguida, realizar ações para processar dados, como leitura e gravação do Amazon S3 ou do Amazon Redshift ou executar o Glue Crawler. AWS

A `AmazonDataZoneSageMakerEnvironmentRolePermissionsBoundary` política concede acesso de leitura e gravação para DataZone a Amazon a serviços como Amazon SageMaker, AWS Glue, Amazon S3, AWS Lake Formation, Amazon Redshift e Amazon Athena. A política também concede permissões de leitura e gravação para alguns recursos de infraestrutura necessários para usar esses serviços, como interfaces de rede, repositórios Amazon ECR e chaves AWS KMS. Ele também dá acesso a SageMaker aplicativos da Amazon, como o Amazon SageMaker Canvas.

A Amazon DataZone aplica a política `AmazonDataZoneSageMakerEnvironmentRolePermissionsBoundary` gerenciada como um limite de permissões para todas as funções do DataZone ambiente da Amazon (proprietário e colaborador). Esse limite de permissões restringe essas funções para permitir apenas o acesso aos recursos e ações necessários para um ambiente.

```
       {
"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 Atualizações da Amazon para políticas AWS gerenciadas

Veja detalhes sobre as atualizações das políticas AWS gerenciadas da Amazon DataZone desde que esse serviço começou a monitorar essas mudanças. Para receber alertas automáticos sobre alterações nessa página, assine o feed RSS na página de histórico de DataZone documentos da Amazon.

Alteração	Descrição	Data
AmazonDataZoneSageMakerEnvironmentRolePermissionsBoundary - novo limite de permissões	Novo limite de permissões chamado AmazonDataZoneSageMakerEnvironmentRolePermissionsBoundary. Quando você cria um SageMaker ambiente Amazon por meio do portal de DataZone dados da Amazon, a Amazon DataZone aplica esse limite de permissões às funções do IAM que são	30 de abril de 2024

Alteração	Descrição	Data
	produzidas durante a criação do ambiente. O limite de permissões limita o escopo das funções que a Amazon DataZone cria e de todas as funções que você adiciona.	
AmazonDataZoneSage MakerAccess - nova política	A nova política chamada AmazonDataZoneSage MakerAccessconcede à Amazon DataZone permissõe s para publicar SageMaker ativos da Amazon no catálogo. Também concede à Amazon DataZone permissões para conceder acesso ou revogar o acesso aos ativos SageMaker publicados pela Amazon no catálogo.	30 de abril de 2024
AmazonDataZoneFullAccess - atualização da política	Uma atualização da AmazonDataZoneFull Accesspolítica que adiciona acesso à `DescribeS ecurityGroups` ação para melhorar a usabilida de dos administradores de contas, configurando esquemas no console e `GetPolicy` ações para ajudar a recuperar informaçõ es sobre a política gerenciada especificada.	30 de abril de 2024

Alteração	Descrição	Data
AmazonDataZoneSage MakerProvisioning - nova política	A nova política chamada AmazonDataZoneSage MakerProvisioningconcede à Amazon DataZone as permissões necessárias para interoperar com a Amazon SageMaker.	30 de abril de 2024
AmazonDataZoneS3Manage- - <region><domainId>- nova função	Nova função chamada AmazonDataZoneS3Manage- - <region><domainId>que é usada quando a Amazon DataZone chama a AWS Lake Formation para registrar uma localização do Amazon Simple Storage Service (Amazon S3). AWS Lake Formation assume essa função ao acessar os dados naquele local.	1º de abril de 2024
AmazonDataZoneGlue ManageAccessRolePolicy - Atualização da política	Atualizou o AmazonDat aZoneGlueManageAcc essRolePolicypara permitir o suporte a permissões que permitem DataZone à Amazon habilitar concessõe s de publicação e acesso aos dados.	1º de abril de 2024

Alteração	Descrição	Data
AmazonDataZoneDomainExecutionRolePolicy e AmazonDataZoneFullUserAccess - Atualização da política	Atualizou o AmazonDataZoneDomainExecutionRolePolicye AmazonDataZoneFullUserAccesspara habilitar o suporte para a `CancelMetadataGenerationRun` API.	29 de março de 2024
AmazonDataZoneFullAccess - Atualização da política	Atualizado `AmazonDataZoneFullAccess` para permitir que os usuários escolham seus segredos, clusters, vPCs e sub-redes no console de DataZone gerenciamento da Amazon em vez de digitá-los em uma caixa de texto.	13 de março de 2024
AmazonDataZoneDomainExecutionRolePolicy - Atualização da política	Atualizou o AmazonDataZoneDomainExecutionRolePolicypara habilitar o suporte para a `ListEnvironmentBlueprintConfigurationSummaries` API necessária para criar perfis de ambiente, identificando quais blueprints estão habilitados em qual conta e região.	01 de fevereiro de 2024
AmazonDataZoneGlueManageAccessRolePolicy - Atualização da política	Atualizado AmazonDataZoneGlueManageAccessRolePolicypara habilitar o suporte ao modo híbrido AWS Lake Formation.	14 de dezembro de 2023

Alteração	Descrição	Data
AmazonDataZoneFull UserAccess e AmazonDat aZoneDomainExecuti onRolePolicy - Atualizações da política	Atualizou as políticas AmazonDataZoneFull UserAccesse as AmazonDat aZoneDomainExecuti onRolePolicypolíticas para apoiar a funcionalidade generativa de descrições de dados com inteligência artificia l na Amazon. DataZone	28 de novembro de 2023
AmazonDataZoneEnvi ronmentRolePermiss ionsBoundary - Atualização da política	A Amazon DataZone fez uma atualização na política AmazonDataZoneEnvi ronmentRolePermiss ionsBoundarygerenciada que consiste em uma `athena:Ge tQueryResultsStrea m` permissão adicional com o escopo da `ResourceTag` condição.	17 de novembro de 2023
AmazonDataZoneReds hiftManageAccessRolePolicy - Atualização da política	A Amazon DataZone atualizou o AmazonDataZoneReds hiftManageAccessRo lePolicyremovendo a verificaç ão do ID da organização para a `redshift:Associate DataShareConsumer` ação. Isso permite que você compartilhe recursos entre AWS organizações.	16 de novembro de 2023

Alteração	Descrição	Data
AmazonDataZoneFull UserAccess - Atualização da política	A Amazon DataZone atualizou a AmazonDataZoneFull UserAccesspolítica que concede acesso total à Amazon DataZone, mas não permite o gerenciamento de domínios, usuários ou contas associadas.	02 de outubro de 2023
AmazonDataZonePort alFullAccessPolicy - política obsoleta	A Amazon DataZone descontinuou o. AmazonDat aZonePortalFullAccessPolicy	29 de setembro de 2023
AmazonDataZonePrev iewConsoleFullAccess - política obsoleta	A Amazon DataZone descontinuou o. AmazonDat aZonePreviewConsol eFullAccess	29 de setembro de 2023

Alteração	Descrição	Data
AmazonDataZoneDomainExecutionRolePolicy - Nova política	A Amazon DataZone adicionou uma nova política chamada AmazonDataZoneDomainExecutionRolePolicy. Essa é a política padrão para a função de DataZone `AmazonDataZoneDomainExecutionRole` serviço da Amazon. Essa função é usada pela Amazon DataZone para catalogar, descobrir, controlar, compartilhar e analisar dados no DataZone domínio da Amazon. Você pode anexar a `AmazonDataZoneDomainExecutionRolePolicy` política ao seu`AmazonDataZoneDomainExecutionRole` .	25 de setembro de 2023
AmazonDataZoneCrossAccountAdmin - Nova política	A Amazon DataZone adicionou uma nova política chamada AmazonDataZoneCrossAccountAdminque permite que os usuários trabalhem com a Amazon DataZone e suas contas associadas.	19 de setembro de 2023

Alteração	Descrição	Data
AmazonDataZoneFull UserAccess - Nova política	A Amazon DataZone adicionou uma nova política chamada AmazonDat aZoneFullUserAccessque concede acesso total à Amazon DataZone, mas não permite o gerenciamento de domínios, usuários ou contas associadas.	12 de setembro de 2023
AmazonDataZoneReds hiftManageAccessRolePolicy - Nova política	A Amazon DataZone adicionou uma nova política chamada AmazonDat aZoneRedshiftManag eAccessRolePolicyque concede permissões para permitir que a Amazon habilite DataZone a publicação e o acesso a subsídios aos dados.	12 de setembro de 2023
AmazonDataZoneGlue ManageAccessRolePolicy - Nova política	A Amazon DataZone adicionou uma nova política chamada AmazonDat aZoneGlueManageAcc essRolePolicyque concede à Amazon DataZone permissõe s para publicar dados do AWS Glue no catálogo. Também concede à Amazon DataZone permissões para conceder acesso ou revogar o acesso aos ativos publicados do AWS Glue no catálogo.	12 de setembro de 2023

Alteração	Descrição	Data
AmazonDataZoneRedshiftGlueProvisioningPolicy - Nova política	A Amazon DataZone adicionou uma nova política chamada AmazonDataZoneRedshiftGlueProvisioningPolicyque concede à Amazon DataZone as permissões necessárias para interoperar com as fontes de dados suportadas.	12 de setembro de 2023
AmazonDataZoneEnvironmentRolePermissionsBoundary - Nova política	A Amazon DataZone adicionou uma nova política chamada AmazonDataZoneEnvironmentRolePermissionsBoundaryque limita o principal do IAM provisionado ao qual ela está vinculada.	12 de setembro de 2023
AmazonDataZoneFullAccess - Nova política	A Amazon DataZone adicionou uma nova política chamada AmazonDataZoneFullAccessque fornece acesso total à Amazon DataZone por meio do AWS Management Console.	12 de setembro de 2023
Atualização da política gerenciada	Atualizações na política AmazonDataZonePreviewConsoleFullAccessgerenciada que consiste em `iam:GetPolicy` permissões adicionais.	13 de junho de 2023

Alteração	Descrição	Data
A Amazon DataZone começou a monitorar as mudanças	A Amazon DataZone começou a monitorar as mudanças em suas políticas AWS gerenciadas.	20 de março de 2023

Funções do IAM para a Amazon DataZone

Tópicos

AmazonDataZoneProvisioningRole-<domainAccountId>

O `AmazonDataZoneProvisioningRole-<domainAccountId>` tem o `AmazonDataZoneRedshiftGlueProvisioningPolicy` anexo. Essa função concede à Amazon DataZone as permissões necessárias para interoperar com o AWS Glue e o Amazon Redshift.

O padrão `AmazonDataZoneProvisioningRole-<domainAccountId>` tem a seguinte política de confiança anexada:

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

```
      "Condition": {
        "StringEquals": {
            "aws:SourceAccount": "{{domain_account}}"
        }
      }
    }
  ]
}
```

AmazonDataZoneDomainExecutionRole

AmazonDataZoneDomainExecutionRoleTem a política AWS gerenciada AmazonDataZoneDomainExecutionRolePolicyanexada. DataZone A Amazon cria essa função para você em seu nome. Para determinadas ações no portal de dados, a Amazon DataZone assume essa função na conta na qual a função foi criada e verifica se essa função está autorizada a realizar a ação.

A AmazonDataZoneDomainExecutionRolefunção é necessária no Conta da AWS que hospeda seu DataZone domínio da Amazon. Essa função é criada automaticamente para você quando você cria seu DataZone domínio na Amazon.

A AmazonDataZoneDomainExecutionRolefunção padrão tem a seguinte política de confiança.

```
{
    "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>

A `AmazonDataZoneGlueAccess-<region>-<domainId>` função tem o `AmazonDataZoneGlueManageAccessRolePolicy` anexo. Essa função concede à Amazon DataZone permissões para publicar dados do AWS Glue no catálogo. Também concede à Amazon DataZone permissões para conceder acesso ou revogar o acesso aos ativos publicados do AWS Glue no catálogo.

A `AmazonDataZoneGlueAccess-<region>-<domainId>` função padrão tem a seguinte política de confiança anexada:

```
{
  "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>

A `AmazonDataZoneRedshiftAccess-<region>-<domainId>` função tem o `AmazonDataZoneRedshiftManageAccessRolePolicy` anexo. Essa função concede à Amazon DataZone permissões para publicar dados do Amazon Redshift no catálogo. Também concede à Amazon DataZone permissões para conceder acesso ou revogar o acesso aos ativos publicados do Amazon Redshift ou do Amazon Redshift Serverless no catálogo.

A `AmazonDataZoneRedshiftAccess-<region>-<domainId>` função padrão tem a seguinte política de permissões em linha anexada:

```
{
   "Version":"2012-10-17",
   "Statement":[
      {
         "Sid": "RedshiftSecretStatement",
         "Effect":"Allow",
         "Action":"secretsmanager:GetSecretValue",
         "Resource":"*",
         "Condition":{
            "StringEquals":{
               "secretsmanager:ResourceTag/AmazonDataZoneDomain":"{{domainId}}"
            }
         }
      }
   ]
}
```

O padrão `AmazonDataZoneRedshiftManageAccessRole<timestamp>` tem a seguinte política de confiança anexada:

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

```
      "Effect": "Allow",
      "Principal": {
        "Service": "datazone.amazonaws.com"
      },
      "Action": "sts:AssumeRole",
      "Condition": {
            "StringEquals": {
                "aws:SourceAccount": "{{domain_account}}"
            },
            "ArnEquals": {
                "aws:SourceArn": "arn:aws:datazone:{{region}}:
{{domain_account}}:domain/{{root_domain_id}}"
            }
        }
    }
  ]
}
```

AmazonDataZone<region>S3 Manage- - <domainId>

O AmazonDataZone S3Manage- <region>- <domainId>é usado quando a Amazon DataZone chama o AWS Lake Formation para registrar uma localização do Amazon Simple Storage Service (Amazon S3). AWS Lake Formation assume essa função ao acessar os dados naquele local. Para obter mais informações, consulte Requisitos para funções usadas para registrar locais.

Essa função tem a seguinte política de permissões em linha anexada.

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

O AmazonDataZone S3Manage- <region>- <domainId>tem a seguinte política de confiança anexada:

```
{
    "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>

A `AmazonDataZoneSageMakerManageAccessRole` função tem o `AmazonDataZoneSageMakerAccessAmazonDataZoneRedshiftManageAccessRolePolicy`, o e o `AmazonDataZoneGlueManageAccessRolePolicy` anexado. Essa função concede à Amazon DataZone permissões para publicar e gerenciar assinaturas de data lake, data warehouse e ativos do Amazon Sagemaker.

A `AmazonDataZoneSageMakerManageAccessRole` função tem a seguinte política em linha anexada:

```
{
   "Version":"2012-10-17",
   "Statement":[
      {
         "Sid": "RedshiftSecretStatement",
         "Effect":"Allow",
         "Action":"secretsmanager:GetSecretValue",
         "Resource":"*",
         "Condition":{
            "StringEquals":{
               "secretsmanager:ResourceTag/AmazonDataZoneDomain":"{{domainId}}"
            }
         }
      }
   ]
}
```

A `AmazonDataZoneSageMakerManageAccessRole` função tem a seguinte política de confiança anexada:

```
{
  "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>

A `AmazonDataZoneSageMakerProvisioningRole` função tem o `AmazonDataZoneSageMakerProvisioning` e o `AmazonDataZoneRedshiftGlueProvisioningPolicy` anexado. Essa função concede à Amazon DataZone as permissões necessárias para interoperar com o AWS Glue, o Amazon Redshift e o Amazon Sagemaker.

A `AmazonDataZoneSageMakerProvisioningRole` função tem a seguinte política em linha anexada:

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Sid": "SageMakerStudioTagOnCreate",
            "Effect": "Allow",
            "Action": [
                "sagemaker:AddTags"
            ],
            "Resource": "arn:aws:sagemaker:*:{{AccountId}}:*/*",
            "Condition": {
```

```
                "Null": {
                    "sagemaker:TaggingAction": "false"
                }
            }
        }
    ]
}
```

A `AmazonDataZoneSageMakerProvisioningRole` função tem a seguinte política de confiança anexada:

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Sid": "DataZoneTrustPolicyStatement",
      "Effect": "Allow",
      "Principal": {
        "Service": "datazone.amazonaws.com"
      },
      "Action": "sts:AssumeRole",
      "Condition": {
        "StringEquals": {
            "aws:SourceAccount": "{{domain_account}}"
        }
      }
    }
  ]
}
```

Funções baseadas em identidade

As políticas baseadas em identidade são documentos de políticas de permissões JSON que você pode anexar a uma identidade, como usuário do IAM, grupo de usuários ou perfil do IAM. Essas políticas controlam quais ações os usuários e funções podem realizar, em quais recursos e em que condições. Para saber como criar uma política baseada em identidade, consulte Criar políticas do IAM no Guia do usuário do IAM.

Com as políticas baseadas em identidade do IAM, é possível especificar ações ou atributos permitidos ou negados, bem como as condições sob as quais as ações são permitidas ou negadas. Não é possível especificar a entidade principal em uma política baseada em identidade porque ela se aplica ao usuário ou função à qual ela está anexado. Para saber mais sobre todos os elementos que podem ser usados em uma política JSON, consulte Referência de elementos da política JSON do IAM no Guia do Usuário do IAM.

Quando você cria um DataZone projeto da Amazon, no portal, três funções do IAM são criadas para esse projeto, uma para cada tipo de função de membro do projeto: proprietário e colaborador. As permissões associadas a cada função têm como escopo a função do projeto, e as políticas de permissões anexadas dependem dos recursos com os quais o projeto é implantado.

Para que DataZone a Amazon gerencie permissões e compartilhe ativos com projetos de assinantes, as funções de usuário do projeto de assinante são adicionadas automaticamente como administrador do data lake AWS Lake Formation no Conta da AWS que está publicando ativos.

Você pode ver a up-to-date versão mais completa da função no console de gerenciamento AWS do IAM ou analisar as diferentes permissões de função na tabela abaixo.

Permissões do proprietário do projeto

Tipo de ambiente	Permissões do IAM
Data Lake padrão	Essa é a combinação dos recursos Essential, Data Lake Producer e Data Lake Consumer.
Essential	{ "Version": "2012-10-17", "Statement": [{ "Effect": "Allow", "Action": ["s3:List*", "s3:Get*", "s3:Describe*", "s3:DeleteObjectVersion",

Tipo de ambiente	Permissões do IAM	

```
        "s3:Resto
reObject",
        "s3:Repli
cateObject",
        "s3:PutObject",
        "s3:Abort
MultipartUpload",
        "s3:PutOb
jectRetention",
        "s3:Delet
eObject"
      ],
      "Resource":
 ["s3BucketArn",
 "s3BucketArn/*"]
    },
    { "Action":
 ["s3:List*"],
 "Resource": "*",
 "Effect": "Allow" },
    {
      "Action": [
        "kms:List*",
        "kms:Get*",
        "kms:Desc
ribe*",
        "kms:Decrypt",
        "kms:Encrypt",
        "kms:ReEn
crypt*",
        "kms:Verify",
        "kms:Sign",
        "kms:Gene
rateDataKey"
      ],
      "Resource":
 "keyArn",
      "Effect": "Allow"
    },
    {
```

Tipo de ambiente	Permissões do IAM	

```
      "Action":
 ["kms:ListKeys",
 "kms:ListAliases"],
      "Resource": "*",
      "Effect": "Allow"
    },
    {
      "Action": [
        "ec2:Desc
ribeSecurityGroups",
        "ec2:Desc
ribeSecurityGroupR
ules",
        "ec2:Desc
ribeTags"
      ],
      "Resource": "*",
      "Effect": "Allow"
    },
    {
      "Action": [
        "logs:Des
cribe*",
        "logs:Sta
rtQuery",
        "logs:Sto
pQuery",
        "logs:Get*",
        "logs:List*",
        "logs:Put
LogEvents",
        "logs:Cre
ateLogStream",
        "logs:Fil
terLogEvents"
      ],
      "Resource":
 "arn:aws:logs:regi
on:account-id:log-
group:log-group-na
me:*",
      "Effect": "Allow"
```

Tipo de ambiente	Permissões do IAM	

```
    },
    {
      "Effect": "Allow",
      "Action": [
        "s3:Get*",
        "s3:List*",
        "kms:List*",
        "kms:Get*",
        "kms:Desc
ribe*",
        "kms:Decrypt"
      ],
      "Resource": "*",
      "Condition": {
        "StringNo
tEquals": {
          "aws:Reso
urceAccount":
 "project-account-id"
        }
      }
    }
  ]
}
```

Tipo de ambiente	Permissões do IAM	
Produtor de Data Lake	{ "Version": "2012-10-17", "Statement": [{ "Effect": "Allow", "Action": ["glue:BatchGet*", "glue:Get*", "glue:SearchTables", "glue:List*", "glue:BatchCreateP artition", "glue:CreatePartit ionIndex", "glue:CreateTable", "glue:BatchUpdateP artition", "glue:BatchDeleteP artition", "glue:UpdateTable", "glue:DeleteTableV ersion", "glue:DeleteTable", "glue:DeleteColumn	

Tipo de ambiente	Permissões do IAM	

```
StatisticsForParti
tion",

 "glue:DeleteColumn
StatisticsForTable",

 "glue:DeletePartit
ionIndex",

 "glue:UpdateColumn
StatisticsForParti
tion",

 "glue:UpdateColumn
StatisticsForTable",

 "glue:BatchDeleteT
ableVersion",

 "glue:BatchDeleteT
able",

 "glue:CreatePartit
ion",

 "glue:DeletePartit
ion",

 "glue:UpdatePartit
ion"
            ],
            "Resource":
 [

 "arn:aws:glue:regi
on:account:database/
dbName",

 "arn:aws:glue:regi
on:account:catalog",

 "arn:aws:glue:regi
```

Tipo de ambiente	Permissões do IAM	

```
on:account:table/d
bName/*"
            ]
        },
        {
            "Sid":
 "VisualEditor0",
            "Effect":
 "Allow",
            "Action": [

 "glue:SearchTables",

 "glue:NotifyEvent",

 "glue:StartBluepri
ntRun",

 "glue:PutWorkflowR
unProperties",

 "glue:StopCrawler",

 "glue:DeleteJob",

 "glue:DeleteWorkfl
ow",

 "glue:UpdateCrawler",

 "glue:DeleteBluepr
int",

 "glue:UpdateWorkfl
ow",

 "glue:StartCrawler",

 "glue:ResetJobBook
mark",

 "glue:UpdateJob",
```

Tipo de ambiente	Permissões do IAM	

```
 "glue:StartWorkflo
wRun",

 "glue:StopCrawlerS
chedule",

 "glue:ResumeWorkfl
owRun",

 "glue:List*",

 "glue:DeleteCrawler",

 "glue:UpdateBluepr
int",

 "glue:BatchStopJob
Run",

 "glue:StopWorkflow
Run",

 "glue:BatchGet*",

 "glue:UpdateCrawle
rSchedule",

 "glue:DeleteConnec
tion",

 "glue:UpdateConnec
tion",

 "glue:Get*",

 "glue:BatchDeleteC
onnection",

 "glue:StartCrawler
Schedule",
```

Tipo de ambiente	Permissões do IAM	

```
 "glue:StartJobRun",

 "glue:CreateWorkfl
ow",

 "glue:PublishDataQ
uality",

 "glue:*DataQuality*"
           ],
           "Resource":
 "*",
           "Conditio
n": {

 "ForAnyValue:Strin
gEquals": {

 "aws:ResourceTag/n
oah-analytics:proj
ectId": "projectId"
               }
           }
       },
       {
           "Sid":
 "CreateGlueResourc
es",
           "Effect":
 "Allow",
           "Action": [

 "glue:CreateBluepr
int",

 "glue:CreateJob",

 "glue:CreateConnec
tion",

 "glue:CreateCrawler",
```

Tipo de ambiente	Permissões do IAM	

```
 "glue:CreateDataQu
alityRuleset"
            ],
            "Resource":
 "*"
        },
        {
            "Sid":
 "VisualEditor0",
            "Effect":
 "Allow",
            "Action": [

 "iam:ListRoles",

 "iam:ListUsers",

 "iam:ListGroups",

 "iam:ListRolePolic
ies",

 "iam:GetRole",

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

Tipo de ambiente	Permissões do IAM

Consumidor do Data Lake	{
	  "Version": "2012-10-17",
	  "Statement": [
	  {
	  "Effect": "Allow",
	  "Action": [
	  "athena:TerminateSession",
	  "athena:CreatePreparedStatement",
	  "athena:StopCalculationExecution",
	  "athena:StartQueryExecution",
	  "athena:UpdatePreparedStatement",
	  "athena:BatchGet*",
	  "athena:UpdateNotebook",
	  "athena:DeleteNotebook",
	  "athena:DeletePreparedStatement",
	  "athena:UpdateNotebookMetadata",
	  "athena:DeleteNamedQuery",
	  "athena:Get*",
	  "athena:UpdateNamedQuery",
	  "athena:CreateNamedQuery",

Tipo de ambiente	Permissões do IAM	

```
        "athena:E
xportNotebook",
        "athena:S
topQueryExecution",
        "athena:S
tartCalculationExe
cution",
        "athena:S
tartSession",
        "athena:C
reatePresignedNote
bookUrl",
        "athena:C
reateNotebook",
        "athena:I
mportNotebook"
      ],
      "Resource": [
        "arn:aws:
athena:region:acco
unt-id:workgroup/w
orkGroupName",
        "arn:aws:
athena:region:acco
unt-id:datacatalog/
AwsDataCatalog"
      ]
    },
    {
      "Effect": "Allow",
      "Action": [
        "athena:L
istWorkGroups",
        "athena:L
istDataCatalogs",
        "athena:List*"
      ],
      "Resource": ["*"]
    },
    {
      "Effect": "Allow",
      "Action": [
```

Tipo de ambiente	Permissões do IAM	

```
        "glue:Bat
chGet*",
        "glue:Get*",
        "glue:Sea
rchTables",
        "glue:List*"
      ],
      "Resource": [
        "arn:aws:
glue:region:account-
id:database/dbName",
        "arn:aws:
glue:region:account-
id:catalog",
        "arn:aws:
glue:region:account-
id:table/dbName/*"
      ]
    }
  ]
}
```

Tipo de ambiente	Permissões do IAM

Produtor de data warehouse	{
	  "Version": "2012-10-17",
	  "Statement": [
	    {
	      "Effect": "Allow",
	      "Action": [
	        "redshift:GetClusterCredentials",
	        "redshift:JoinGroup",
	        "redshift:CreateClusterUser",
	        "redshift:DescribeClusters"
	      ],
	      "Resource": "arn:aws:redshift:region:account:cluster:producerRedshiftCluster"
	    },
	    {
	      "Effect": "Allow",
	      "Action": [
	        "redshift-data:DescribeStatement",
	        "redshift-data:ExecuteStatement"
	      ],
	      "Resource": "arn:aws:redshift:region:account:cluster:producerRedshiftCluster"
	    }
	  ]
	}

Tipo de ambiente	Permissões do IAM	

Tipo de ambiente	Permissões do IAM

Consumidor de data warehouse	{
	  "Version": "2012-10-17",
	  "Statement": [
	  {
	  "Effect": "Allow",
	  "Action": [
	  "redshift:GetClusterCredentials",
	  "redshift:JoinGroup",
	  "redshift:CreateClusterUser",
	  "redshift:DescribeClusters"
	  ],
	  "Resource": [
	  "arn:aws:redshift:region:account:dbuser:cluster-identifier/dbUser",
	  "arn:aws:redshift:region:account:dbgroup:cluster-identifier/project_owner@projectName",
	  "arn:aws:redshift:region:account:dbname:cluster-identifier/*"
	  ],
	  "Condition": {
	  "ForAnyValue:StringEquals": {
	  "aws:PrincipalTag/RedshiftDbUser": "dbUser"
	  }

Tipo de ambiente	Permissões do IAM	

```
      }
    },
    {
      "Sid": "VisualEd
itor2",
      "Effect": "Allow",
      "Action": [
        "redshift-
data:DescribeStat
ement",
        "redshift-
data:ExecuteStatement"
      ],
      "Resource":
 "arn:aws:redshift:
region:account-id:
cluster:cluster-id
entifier"
    }
  ]
}
```

Tipo de ambiente	Permissões do IAM	

Editor de Consultas do Amazon Redshift v2	{
	  "Version": "2012-10-17",
	  "Statement": [
	  {
	  "Action": "redshift:DescribeClusters",
	  "Effect": "Allow",
	  "Resource": "arn:aws:redshift:region:account-id:cluster:*",
	  "Sid": "RedshiftPermissions"
	  },
	  {
	  "Action": "tag:GetResources",
	  "Condition": {
	  "StringEquals": { "aws:CalledViaLast": "sqlworkbench.amazonaws.com" }
	  },
	  "Effect": "Allow",
	  "Resource": "*",
	  "Sid": "ResourceGroupsTaggingPermissions"
	  },
	  {
	  "Action": [
	  "sqlworkbench:DriverExecute",
	  "sqlworkbench:GenerateSession",	

Tipo de ambiente	Permissões do IAM	

```
        "sqlworkb
ench:ListConnectio
ns",
        "sqlworkb
ench:ListDatabases",
        "sqlworkb
ench:ListFiles",
        "sqlworkb
ench:ListNotebooks",
        "sqlworkb
ench:ListQueryExec
utionHistory",
        "sqlworkb
ench:ListRedshiftC
lusters",
        "sqlworkb
ench:ListSampleDat
abases",
        "sqlworkb
ench:ListTabs",
        "sqlworkb
ench:ListTaggedRes
ources"
      ],
      "Effect": "Allow",
      "Resource": "*",
      "Sid": "AmazonRe
dshiftQueryEditorV
2PermissionsPart1"
    },
    {
      "Action":
 "sqlworkbench:*",
      "Effect": "Allow",
      "Resource": [
        "arn:aws:
sqlworkbench:regio
n:account-id:query/
*",
        "arn:aws:
sqlworkbench:regio
```

Tipo de ambiente	Permissões do IAM
	n:account-id:noteb ook/*", "arn:aws: sqlworkbench:regio n:account-id:conne ction/*", "arn:aws: sqlworkbench:regio n:account-id:chart/ *", "arn:aws: sqlworkbench:regio n:account-id:/*"], "Sid": "AmazonRe dshiftQueryEditorV 2PermissionsPart2" }] }

Permissões de colaborador do projeto

Tipo de ambiente	Permissões do IAM
Data Lake padrão	Essa é a combinação dos recursos Essential, Data Lake Producer e Data Lake Consumer.
Essential	{ "Version": "2012-10- 17", "Statement": [{ "Effect": "Allow",

Tipo de ambiente	Permissões do IAM	

```
      "Action": [
        "s3:List*",
        "s3:Get*",
        "s3:Describe*",
        "s3:Delet
eObjectVersion",
        "s3:Resto
reObject",
        "s3:Repli
cateObject",
        "s3:PutObject",
        "s3:Abort
MultipartUpload",
        "s3:PutOb
jectRetention",
        "s3:Delet
eObject"
      ],
      "Resource":
 ["s3BucketArn",
 "s3BucketArn/*"]
    },
    { "Action":
 ["s3:List*"],
 "Resource": "*",
 "Effect": "Allow" },
    {
      "Action": [
        "kms:List*",
        "kms:Get*",
        "kms:Desc
ribe*",
        "kms:Decrypt",
        "kms:Encrypt",
        "kms:ReEn
crypt*",
        "kms:Verify",
        "kms:Sign",
        "kms:Gene
rateDataKey"
      ],
```

Tipo de ambiente	Permissões do IAM	

```
      "Resource":
 "keyArn",
      "Effect": "Allow"
    },
    {
      "Action":
 ["kms:ListKeys",
 "kms:ListAliases"],
      "Resource": "*",
      "Effect": "Allow"
    },
    {
      "Action": [
        "ec2:Desc
ribeSecurityGroups",
        "ec2:Desc
ribeSecurityGroupR
ules",
        "ec2:Desc
ribeTags"
      ],
      "Resource": "*",
      "Effect": "Allow"
    },
    {
      "Action": [
        "logs:Des
cribe*",
        "logs:Sta
rtQuery",
        "logs:Sto
pQuery",
        "logs:Get*",
        "logs:List*",
        "logs:Put
LogEvents",
        "logs:Cre
ateLogStream",
        "logs:Fil
terLogEvents"
      ],
```

Tipo de ambiente	Permissões do IAM	

```
      "Resource":
 "arn:aws:logs:regi
on:account-id:log-
group:log-group-na
me:*",
      "Effect": "Allow"
    },
    {
      "Effect": "Allow",
      "Action": [
        "s3:Get*",
        "s3:List*",
        "kms:List*",
        "kms:Get*",
        "kms:Desc
ribe*",
        "kms:Decrypt"
      ],
      "Resource": "*",
      "Condition": {
        "StringNo
tEquals": {
          "aws:Reso
urceAccount":
 "project-account-id"
        }
      }
    }
  ]
}
```

Tipo de ambiente	Permissões do IAM

Produtor de Data Lake	{
	  "Version": "2012-10-17",
	  "Statement": [
	  {
	  "Effect": "Allow",
	  "Action": [
	  "glue:BatchGet*",
	  "glue:Get*",
	  "glue:SearchTables",
	  "glue:List*",
	  "glue:BatchCreatePartition",
	  "glue:CreatePartitionIndex",
	  "glue:CreateTable",
	  "glue:BatchUpdatePartition",
	  "glue:BatchDeletePartition",
	  "glue:UpdateTable",
	  "glue:DeleteTableVersion",
	  "glue:DeleteTable",
	  "glue:DeleteColumnStatisticsForPartition",
	  "glue:DeleteColumnStatisticsForTable",
	  "glue:DeletePartitionIndex",
	  "glue:UpdateColumnStatisticsForPartition",

Tipo de ambiente	Permissões do IAM	

```
        "glue:Upd
ateColumnStatistic
sForTable",
        "glue:Bat
chDeleteTableVersi
on",
        "glue:Bat
chDeleteTable",
        "glue:Cre
atePartition",
        "glue:Del
etePartition",
        "glue:Upd
atePartition"
      ],
      "Resource": [
        "arn:aws:
glue:region:accoun
t:database/dbName",
        "arn:aws:
glue:region:accoun
t:catalog",
        "arn:aws:
glue:region:accoun
t:table/dbName/*"
      ]
    },
    {
      "Sid": "VisualEd
itor0",
      "Effect": "Allow",
      "Action": [
        "glue:Sea
rchTables",
        "glue:Not
ifyEvent",
        "glue:Sta
rtBlueprintRun",
        "glue:Put
WorkflowRunPropert
ies",
```

Tipo de ambiente	Permissões do IAM	

```
        "glue:Sto
pCrawler",
        "glue:Del
eteJob",
        "glue:Del
eteWorkflow",
        "glue:Upd
ateCrawler",
        "glue:Del
eteBlueprint",
        "glue:Upd
ateWorkflow",
        "glue:Sta
rtCrawler",
        "glue:Res
etJobBookmark",
        "glue:Upd
ateJob",
        "glue:Sta
rtWorkflowRun",
        "glue:Sto
pCrawlerSchedule",
        "glue:Res
umeWorkflowRun",
        "glue:List*",
        "glue:Del
eteCrawler",
        "glue:Upd
ateBlueprint",
        "glue:Bat
chStopJobRun",
        "glue:Sto
pWorkflowRun",
        "glue:Bat
chGet*",
        "glue:Upd
ateCrawlerSchedule",
        "glue:Del
eteConnection",
        "glue:Upd
ateConnection",
        "glue:Get*",
```

Tipo de ambiente	Permissões do IAM	

```
        "glue:Bat
chDeleteConnection",
        "glue:Sta
rtCrawlerSchedule",
        "glue:Sta
rtJobRun",
        "glue:Cre
ateWorkflow",
        "glue:Pub
lishDataQuality",
        "glue:*Da
taQuality*"
      ],
      "Resource": "*",
      "Condition": {
        "ForAnyVa
lue:StringEquals": {
          "aws:Reso
urceTag/noah-analy
tics:projectId":
 "projectId"
        }
      }
    },
    {
      "Sid": "CreateGl
ueResources",
      "Effect": "Allow",
      "Action": [
        "glue:Cre
ateBlueprint",
        "glue:Cre
ateJob",
        "glue:Cre
ateConnection",
        "glue:Cre
ateCrawler",
        "glue:Cre
ateDataQualityRule
set"
      ],
      "Resource": "*"
```

Tipo de ambiente	Permissões do IAM	

```
    },
    {
      "Sid": "VisualEd
itor0",
      "Effect": "Allow",
      "Action": [
        "iam:List
Roles",
        "iam:List
Users",
        "iam:List
Groups",
        "iam:List
RolePolicies",
        "iam:GetRole",
        "iam:GetR
olePolicy"
      ],
      "Resource": "*"
    }
  ]
}
```

Tipo de ambiente	Permissões do IAM

Consumidor do Data Lake	{
	  "Version": "2012-10-17",
	  "Statement": [
	  {
	  "Effect": "Allow",
	  "Action": [
	  "athena:TerminateSession",
	  "athena:CreatePreparedStatement",
	  "athena:StopCalculationExecution",
	  "athena:StartQueryExecution",
	  "athena:UpdatePreparedStatement",
	  "athena:BatchGet*",
	  "athena:UpdateNotebook",
	  "athena:DeleteNotebook",
	  "athena:DeletePreparedStatement",
	  "athena:UpdateNotebookMetadata",
	  "athena:DeleteNamedQuery",
	  "athena:Get*",
	  "athena:UpdateNamedQuery",
	  "athena:CreateNamedQuery",

Tipo de ambiente	Permissões do IAM	

```
        "athena:E
xportNotebook",
        "athena:S
topQueryExecution",
        "athena:S
tartCalculationExe
cution",
        "athena:S
tartSession",
        "athena:C
reatePresignedNote
bookUrl",
        "athena:C
reateNotebook",
        "athena:I
mportNotebook"
      ],
      "Resource": [
        "arn:aws:
athena:region:acco
unt-id:workgroup/w
orkGroupName",
        "arn:aws:
athena:region:acco
unt-id:datacatalog/
AwsDataCatalog"
      ]
    },
    {
      "Effect": "Allow",
      "Action": [
        "athena:L
istWorkGroups",
        "athena:L
istDataCatalogs",
        "athena:List*"
      ],
      "Resource": ["*"]
    },
    {
      "Effect": "Allow",
      "Action": [
```

Tipo de ambiente	Permissões do IAM	

```
        "glue:Bat
chGet*",
        "glue:Get*",
        "glue:Sea
rchTables",
        "glue:List*"
      ],
      "Resource": [
        "arn:aws:
glue:region:account-
id:database/dbName",
        "arn:aws:
glue:region:account-
id:catalog",
        "arn:aws:
glue:region:account-
id:table/dbName/*"
      ]
    }
  ]
}
```

Tipo de ambiente	Permissões do IAM

Produtor de data warehouse	{
	  "Version": "2012-10-17",
	  "Statement": [
	    {
	      "Effect": "Allow",
	      "Action": [
	        "redshift:GetClusterCredentials",
	        "redshift:JoinGroup",
	        "redshift:CreateClusterUser",
	        "redshift:DescribeClusters"
	      ],
	      "Resource": "arn:aws:redshift:region:account:cluster:producerRedshiftCluster"
	    },
	    {
	      "Effect": "Allow",
	      "Action": [
	        "redshift-data:DescribeStatement",
	        "redshift-data:ExecuteStatement"
	      ],
	      "Resource": "arn:aws:redshift:region:account:cluster:producerRedshiftCluster"
	    }
	  ]
	}

Tipo de ambiente	Permissões do IAM	

Tipo de ambiente	Permissões do IAM

Consumidor de data warehouse	{
	  "Version": "2012-10-17",
	  "Statement": [
	  {
	  "Effect": "Allow",
	  "Action": [
	  "redshift:GetClusterCredentials",
	  "redshift:JoinGroup",
	  "redshift:CreateClusterUser",
	  "redshift:DescribeClusters"
	  ],
	  "Resource": [
	  "arn:aws:redshift:region:account:dbuser:cluster-identifier/dbUser",
	  "arn:aws:redshift:region:account:dbgroup:cluster-identifier/project_owner@projectName",
	  "arn:aws:redshift:region:account:dbname:cluster-identifier/*"
	  ],
	  "Condition": {
	  "ForAnyValue:StringEquals": {
	  "aws:PrincipalTag/RedshiftDbUser": "dbUser"
	  }

Tipo de ambiente	Permissões do IAM	

```
      }
    },
    {
      "Sid": "VisualEd
itor2",
      "Effect": "Allow",
      "Action": [
        "redshift-
data:DescribeStat
ement",
        "redshift-
data:ExecuteStatement"
      ],
      "Resource":
 "arn:aws:redshift:
region:account-id:
cluster:cluster-id
entifier"
    }
  ]
}
```

Tipo de ambiente	Permissões do IAM

Editor de Consultas do Amazon Redshift v2	{
	  "Version": "2012-10-17",
	  "Statement": [
	    {
	      "Action": "redshift:DescribeClusters",
	      "Effect": "Allow",
	      "Resource": "arn:aws:redshift:region:account-id:cluster:*",
	      "Sid": "RedshiftPermissions"
	    },
	    {
	      "Action": "tag:GetResources",
	      "Condition": {
	        "StringEquals": { "aws:CalledViaLast": "sqlworkbench.amazonaws.com" }
	      },
	      "Effect": "Allow",
	      "Resource": "*",
	      "Sid": "ResourceGroupsTaggingPermissions"
	    },
	    {
	      "Action": [
	        "sqlworkbench:DriverExecute",
	        "sqlworkbench:GenerateSession",

Tipo de ambiente	Permissões do IAM	

```
        "sqlworkb
ench:ListConnectio
ns",
        "sqlworkb
ench:ListDatabases",
        "sqlworkb
ench:ListFiles",
        "sqlworkb
ench:ListNotebooks",
        "sqlworkb
ench:ListQueryExec
utionHistory",
        "sqlworkb
ench:ListRedshiftC
lusters",
        "sqlworkb
ench:ListSampleDat
abases",
        "sqlworkb
ench:ListTabs",
        "sqlworkb
ench:ListTaggedRes
ources"
      ],
      "Effect": "Allow",
      "Resource": "*",
      "Sid": "AmazonRe
dshiftQueryEditorV
2PermissionsPart1"
    },
    {
      "Action":
 "sqlworkbench:*",
      "Effect": "Allow",
      "Resource": [
        "arn:aws:
sqlworkbench:regio
n:account-id:query/
*",
        "arn:aws:
sqlworkbench:regio
```

Tipo de ambiente	Permissões do IAM

```
n:account-id:noteb
ook/*",
        "arn:aws:
sqlworkbench:regio
n:account-id:conne
ction/*",
        "arn:aws:
sqlworkbench:regio
n:account-id:chart/
*",
        "arn:aws:
sqlworkbench:regio
n:account-id:/*"
      ],
      "Sid": "AmazonRe
dshiftQueryEditorV
2PermissionsPart2"
    }
  ]
}
```

Credenciais temporárias

Alguns AWS serviços não funcionam quando você faz login usando credenciais temporárias. Para obter informações adicionais, incluindo quais AWS serviços funcionam com credenciais temporárias, consulte AWS serviços que funcionam com o IAM no Guia do usuário do IAM.

Você está usando credenciais temporárias se fizer login AWS Management Console usando qualquer método, exceto um nome de usuário e senha. Por exemplo, quando você acessa AWS usando o link de login único (SSO) da sua empresa, esse processo cria automaticamente credenciais temporárias. Você também cria automaticamente credenciais temporárias quando faz login no console como usuário e, em seguida, alterna perfis. Para obter mais informações sobre como alternar perfis, consulte Alternar para um perfil (console) no Guia do usuário do IAM.

Você pode criar manualmente credenciais temporárias usando a AWS API AWS CLI ou. Em seguida, você pode usar essas credenciais temporárias para acessar AWS. AWS recomenda que você gere

credenciais temporárias dinamicamente em vez de usar chaves de acesso de longo prazo. Para mais informações, consulte Credenciais de segurança temporárias no IAM.

Permissões de entidade principal

Quando você usa um usuário ou uma função do IAM para realizar ações AWS, você é considerado um principal. As políticas concedem permissões a uma entidade principal. Quando você usa alguns serviços, pode executar uma ação que, em seguida, aciona outra ação em outro serviço. Nesse caso, você precisa ter permissões para executar ambas as ações. Para ver se uma ação requer ações dependentes adicionais em uma política, consulte Ações, recursos e chaves de condição para obter a AWS documentação essencial na Referência de autorização de serviço.

Validação de conformidade para a Amazon DataZone

Para saber se um AWS service (Serviço da AWS) está dentro do escopo de programas de conformidade específicos, consulte Serviços da AWS Escopo por Programa de Conformidade Serviços da AWS e escolha o programa de conformidade em que você está interessado. Para obter informações gerais, consulte Programas de AWS conformidade Programas AWS de .

Você pode baixar relatórios de auditoria de terceiros usando AWS Artifact. Para obter mais informações, consulte Baixar relatórios em AWS Artifact .

Sua responsabilidade de conformidade ao usar Serviços da AWS é determinada pela confidencialidade de seus dados, pelos objetivos de conformidade de sua empresa e pelas leis e regulamentações aplicáveis. AWS fornece os seguintes recursos para ajudar na conformidade:

- Guias de início rápido sobre segurança e conformidade — Esses guias de implantação discutem considerações arquitetônicas e fornecem etapas para a implantação de ambientes básicos AWS focados em segurança e conformidade.
- Arquitetura para segurança e conformidade com a HIPAA na Amazon Web Services — Este whitepaper descreve como as empresas podem usar AWS para criar aplicativos qualificados para a HIPAA.

> **Note**
>
> Nem todos Serviços da AWS são elegíveis para a HIPAA. Para obter mais informações, consulte a Referência dos serviços qualificados pela HIPAA.

- AWS Recursos de https://aws.amazon.com/compliance/resources/ de conformidade — Essa coleção de pastas de trabalho e guias pode ser aplicada ao seu setor e local.
- AWS Guias de conformidade do cliente — Entenda o modelo de responsabilidade compartilhada sob a ótica da conformidade. Os guias resumem as melhores práticas de proteção Serviços da AWS e mapeiam as diretrizes para controles de segurança em várias estruturas (incluindo o Instituto Nacional de Padrões e Tecnologia (NIST), o Conselho de Padrões de Segurança do Setor de Cartões de Pagamento (PCI) e a Organização Internacional de Padronização (ISO)).
- Avaliação de recursos com regras no Guia do AWS Config desenvolvedor — O AWS Config serviço avalia o quão bem suas configurações de recursos estão em conformidade com as práticas internas, as diretrizes e os regulamentos do setor.
- AWS Security Hub— Isso AWS service (Serviço da AWS) fornece uma visão abrangente do seu estado de segurança interno AWS. O Security Hub usa controles de segurança para avaliar os atributos da AWS e verificar a conformidade com os padrões e as práticas recomendadas do setor de segurança. Para obter uma lista dos serviços e controles aceitos, consulte a Referência de controles do Security Hub.
- Amazon GuardDuty — Isso AWS service (Serviço da AWS) detecta possíveis ameaças às suas cargas de trabalho Contas da AWS, contêineres e dados monitorando seu ambiente em busca de atividades suspeitas e maliciosas. GuardDuty pode ajudá-lo a atender a vários requisitos de conformidade, como o PCI DSS, atendendo aos requisitos de detecção de intrusões exigidos por determinadas estruturas de conformidade.
- AWS Audit Manager— Isso AWS service (Serviço da AWS) ajuda você a auditar continuamente seu AWS uso para simplificar a forma como você gerencia o risco e a conformidade com as regulamentações e os padrões do setor.

Melhores práticas de segurança para a Amazon DataZone

DataZone A Amazon fornece vários recursos de segurança a serem considerados ao desenvolver e implementar suas próprias políticas de segurança. As melhores práticas a seguir são diretrizes gerais e não representam uma solução completa de segurança. Como essas práticas recomendadas podem não ser adequadas ou suficientes no seu ambiente, trate-as como considerações úteis em vez de requisitos.

Implemente o acesso de privilégio mínimo

Ao conceder permissões, você decide quem está recebendo quais permissões para quais DataZone recursos da Amazon. Você habilita ações específicas que quer permitir nesses recursos.

Portanto, você deve conceder somente as permissões necessárias para executar uma tarefa. A implementação do privilégio de acesso mínimo é fundamental para reduzir o risco de segurança e o impacto que pode resultar de erros ou usuários mal-intencionados.

Usar funções do IAM

Os aplicativos de produtores e clientes devem ter credenciais válidas para acessar os DataZone recursos da Amazon. Você não deve armazenar AWS credenciais diretamente em um aplicativo cliente ou em um bucket do Amazon S3. Essas são credenciais de longo prazo que não são automaticamente alternadas e podem ter um impacto comercial significativo se forem comprometidas.

Em vez disso, você deve usar uma função do IAM para gerenciar credenciais temporárias para que seus aplicativos de produtor e cliente acessem DataZone os recursos da Amazon. Quando você usa uma função, não precisa usar credenciais de longo prazo (como um nome de usuário e uma senha ou chaves de acesso) para acessar outros recursos.

Para obter mais informações, consulte os seguintes tópicos no Manual do usuário do IAM:

- Funções do IAM
- Cenários comuns para funções: usuários, aplicativos e serviços

Implemente a criptografia do lado do servidor em recursos dependentes

Dados em repouso e dados em trânsito podem ser criptografados na Amazon DataZone.

Use CloudTrail para monitorar chamadas de API

DataZone A Amazon está integrada com AWS CloudTrail, um serviço que fornece um registro das ações realizadas por um usuário, função ou AWS serviço na Amazon DataZone.

Usando as informações coletadas por CloudTrail, você pode determinar a solicitação que foi feita à Amazon DataZone, o endereço IP a partir do qual a solicitação foi feita, quem fez a solicitação, quando ela foi feita e detalhes adicionais.

Resiliência na Amazon DataZone

A infraestrutura AWS global é construída em torno Regiões da AWS de zonas de disponibilidade. Regiões da AWS fornecem várias zonas de disponibilidade fisicamente separadas e isoladas,

conectadas a redes de baixa latência, alta taxa de transferência e alta redundância. Com as zonas de disponibilidade, é possível projetar e operar aplicações e bancos de dados que automaticamente executam o failover entre as zonas sem interrupção. As zonas de disponibilidade são mais altamente disponíveis, tolerantes a falhas e escaláveis que uma ou várias infraestruturas de datacenter tradicionais.

Para obter mais informações sobre zonas de disponibilidade Regiões da AWS e zonas de disponibilidade, consulte Infraestrutura AWS global.

Além da infraestrutura AWS global, a Amazon DataZone oferece vários recursos para ajudar a suportar suas necessidades de resiliência e backup de dados.

Tópicos

Resiliência da fonte de dados

Durante um evento de DataZone disponibilidade da Amazon, os `DataSource` trabalhos serão repetidos periodicamente por até 24 horas. Se um trabalho falhar devido a uma configuração incorreta, um `DataSourceRunFailed` evento será emitido. Se o DataZone domínio da Amazon estiver configurado com uma chave KMS e AmazonDataZoneDomainExecutionRole perder o acesso a essa chave durante a execução de um trabalho, a execução terminará no `INACCESSIBLE` estado. Depois que o acesso ao KMS for restaurado, o trabalho deverá ser atualizado manualmente para acionar a transição de volta ao estado utilizável.

Resiliência de ativos

Na Amazon DataZone, os ativos são versionados. Se uma versão de um ativo precisar ser revertida, você poderá criar uma nova versão usando o conteúdo da última versão estável. Uma versão do ativo pode ser publicada. Uma versão publicada de um ativo não pode ser editada, exceto pela publicação de uma nova versão. Um ativo publicado (também conhecido como listagem) pode ser inscrito. Para evitar novas assinaturas de um ativo, a publicação pode ser cancelada. Cancelar a publicação de um ativo não afeta as assinaturas existentes. A exclusão de um ativo excluirá todas as versões não publicadas do ativo. As versões publicadas do ativo devem ser excluídas separadamente. Uma versão publicada de um ativo só pode ser excluída se não houver assinaturas.

Resiliência do tipo de ativo e do formulário de metadados

Na Amazon DataZone, os tipos de ativos e os tipos de formulários de metadados são versionados. Um tipo de ativo não pode ser excluído se estiver sendo usado por um ativo. Um tipo de formulário de metadados não pode ser excluído se estiver sendo usado por um tipo de ativo ou ativo. Se você não quiser que o específico metadata-form-type seja usado para curadoria, você pode desativá-lo, o que não afeta aqueles aos quais ele já está anexado.

Resiliência do glossário

Na Amazon DataZone, glossários e termos do glossário não podem ser excluídos se estiverem em uso. Se você não quiser que um glossário ou termo específico do glossário seja usado para curadoria, você pode desativá-los, o que não afeta aqueles aos quais ele já está anexado.

Resiliência de pesquisa global

Na Amazon DataZone, os ativos publicados (também conhecidos como listagens) podem ser descobertos por meio da pesquisa global. A publicação de um ativo pode ser revertida cancelando a publicação do ativo. Cancelar a publicação de um ativo não afeta as assinaturas existentes. Um ativo publicado pode ser revertido para uma versão específica do ativo republicando essa versão. Isso não afetará as assinaturas existentes.

Resiliência da assinatura

Na Amazon DataZone, o preenchimento do SubscriptionGrant tentará se aposentar duas vezes antes de falhar. Se falhar, ele deverá ser excluído manualmente para tentar novamente. Se a Amazon DataZone não puder revogar as permissões de uma assinatura, a exclusão da assinatura poderá falhar. O erro subjacente deve ser resolvido ou a `retainPermissions` bandeira pode ser

usada na operação da `DeleteSubscriptionGrant` API para forçar a exclusão da concessão da Amazon DataZone sem revogar as permissões.

Se o DataZone domínio da Amazon estiver configurado com uma chave KMS e `AmazonDataZoneDomainExecutionRole` ele perder o acesso a essa chave durante o `SubscriptionGrant` fluxo de trabalho, a concessão será marcada`INACCESSIBLE`. Depois que o acesso ao KMS for restaurado, as `INACCESSIBLE` concessões deverão ser excluídas e recriadas.

Resiliência ambiental

Se o DataZone domínio da Amazon estiver configurado com uma chave KMS e `AmazonDataZoneDomainExecutionRole` perder o acesso a essa chave durante o fluxo de trabalho do ambiente, o ambiente será marcado`INACCESSIBLE`. Depois que o acesso ao KMS for restaurado, o `INACCESSIBLE` ambiente deverá ser excluído e recriado. A criação do ambiente tentará duas aposentadorias antes de falhar. Se falhar, ele deverá ser excluído manualmente para tentar novamente. Se o fluxo de trabalho do ambiente falhar, o ambiente entrará em um estado de falha. Nesse momento, ele só pode ser excluído e recriado.

Resiliência do plano ambiental

Na Amazon DataZone, um blueprint de ambiente não pode ser excluído se houver algum perfil de ambiente subjacente.

Resiliência do projeto

Na Amazon DataZone, um projeto não pode ser excluído se houver algum ambiente contido.

Resiliência de RAM

Para obter informações sobre resiliência de RAM, consulte https://docs.aws.amazon.com/ram/latest/ userguide/ security-disaster-recovery-resiliency .html.

Resiliência no gerenciamento do perfil de usuário

Para obter informações sobre resiliência do perfil do usuário, consulte AWS Identity Center.

Resiliência do domínio

Na Amazon DataZone, um domínio não pode ser excluído se ele contiver projetos ou fontes de dados.

Segurança de infraestrutura na Amazon DataZone

Como um serviço gerenciado, a Amazon DataZone é protegida pela segurança de rede AWS global. Para obter informações sobre serviços AWS de segurança e como AWS proteger a infraestrutura, consulte AWS Cloud Security. Para projetar seu AWS ambiente usando as melhores práticas de segurança de infraestrutura, consulte Proteção de infraestrutura no Security Pillar AWS Well-Architected Framework.

Você usa chamadas de API AWS publicadas para acessar a Amazon DataZone pela rede. Os clientes devem ser compatíveis com:

- Transport Layer Security (TLS). Exigimos TLS 1.2 e recomendamos TLS 1.3.
- Conjuntos de criptografia com sigilo de encaminhamento perfeito (perfect forward secrecy, ou PFS) como DHE (Ephemeral Diffie-Hellman, ou Efêmero Diffie-Hellman) ou ECDHE (Ephemeral Elliptic Curve Diffie-Hellman, ou Curva elíptica efêmera Diffie-Hellman). A maioria dos sistemas modernos, como Java 7 e versões posteriores, são compatíveis com esses modos.

Além disso, as solicitações devem ser assinadas utilizando um ID da chave de acesso e uma chave de acesso secreta associada a uma entidade principal do IAM. Ou é possível usar o AWS Security Token Service (AWS STS) para gerar credenciais de segurança temporárias para assinar solicitações.

Deputado confuso entre serviços de prevenção na Amazon DataZone

O problema “confused deputy” é um problema de segurança em que uma entidade que não tem permissão para executar uma ação pode coagir uma entidade mais privilegiada a executá-la. Em AWS, a falsificação de identidade entre serviços pode resultar em um problema confuso de delegado. A imitação entre serviços pode ocorrer quando um serviço (o serviço de chamada) chama outro serviço (o serviço chamado). O serviço de chamada pode ser manipulado para utilizar as suas permissões para atuar nos recursos de outro cliente em que, de outra forma, ele não teria permissão para acessar. Para evitar isso, AWS fornece ferramentas que ajudam você a proteger seus dados para todos os serviços com diretores de serviços que receberam acesso aos recursos em sua conta.

Recomendamos usar a chave de contexto aws: SourceAccount global condition nas políticas de recursos para limitar as permissões que a Amazon DataZone concede a outro serviço ao recurso.

Use aws: SourceAccount se você quiser permitir que qualquer recurso dessa conta seja associado ao uso cruzado de serviços.

Análise de configuração e vulnerabilidade para a Amazon DataZone

AWS lida com tarefas básicas de segurança, como sistema operacional (SO) convidado e aplicação de patches em bancos de dados, configuração de firewall e recuperação de desastres. Esses procedimentos foram revisados e certificados por terceiros certificados. Para obter mais informações, consulte o modelo de responsabilidade AWS compartilhada.

Domínios para adicionar à sua lista de permissões

Para que o portal de DataZone dados da Amazon acesse o DataZone serviço da Amazon, você deve adicionar os seguintes domínios à lista de permissões na rede a partir da qual o portal de dados está tentando acessar o serviço.

- `*.api.aws`
- `*.on.aws`

Monitorando a Amazon DataZone

O monitoramento é uma parte importante da manutenção da confiabilidade, disponibilidade e desempenho da Amazon DataZone e de suas outras AWS soluções. AWS fornece as seguintes ferramentas de monitoramento para monitorar a Amazon DataZone, relatar quando algo está errado e realizar ações automáticas quando apropriado:

- A Amazon CloudWatch monitora seus AWS recursos e os aplicativos em que você executa AWS em tempo real. É possível coletar e rastrear métricas, criar painéis personalizados e definir alarmes que o notificam ou que realizam ações quando uma métrica especificada atinge um limite definido. Por exemplo, você pode CloudWatch rastrear o uso da CPU ou outras métricas de suas instâncias do Amazon EC2 e iniciar automaticamente novas instâncias quando necessário. Para obter mais informações, consulte o Guia CloudWatch do usuário da Amazon.
- O Amazon CloudWatch Logs permite que você monitore, armazene e acesse seus arquivos de log a partir de instâncias do Amazon EC2 e de outras fontes. CloudTrail CloudWatch Os registros podem monitorar as informações nos arquivos de log e notificá-lo quando determinados limites forem atingidos. É possível também arquivar seus dados de log em armazenamento resiliente. Para obter mais informações, consulte o Guia do usuário do Amazon CloudWatch Logs.
- A Amazon EventBridge pode ser usada para automatizar seus AWS serviços e responder automaticamente a eventos do sistema, como problemas de disponibilidade de aplicativos ou alterações de recursos. Os eventos dos AWS serviços são entregues quase EventBridge em tempo real. Você pode escrever regras simples para indicar quais eventos são do seu interesse, e as ações automatizadas a serem tomadas quando um evento corresponder à regra. Para obter mais informações, consulte o Guia EventBridge do usuário da Amazon.
- AWS CloudTrailcaptura chamadas de API e eventos relacionados feitos por ou em nome de sua AWS conta e entrega os arquivos de log para um bucket do Amazon S3 que você especificar. Você pode identificar quais usuários e contas ligaram AWS, o endereço IP de origem a partir do qual as chamadas foram feitas e quando elas ocorreram. Para mais informações, consulte o Guia do usuário do AWS CloudTrail.

Monitorando a Amazon DataZone com a Amazon CloudWatch

Você pode monitorar a Amazon DataZone usando CloudWatch, que coleta dados brutos e os processa em métricas legíveis, quase em tempo real. Essas estatísticas são mantidas por 15 meses, de maneira que você possa acessar informações históricas e ter uma perspectiva melhor de como

o aplicativo web ou o serviço está se saindo. Você também pode definir alarmes que observam determinados limites e enviam notificações ou realizam ações quando esses limites são atingidos. Para obter mais informações, consulte o Guia CloudWatch do usuário da Amazon.

O portal de DataZone dados da Amazon usa APIs DataZone de plano de dados da Amazon com autenticação e autorização do JWT. A Amazon DataZone assume a função de serviço DataZone padrão da Amazon e registra todas as chamadas de DataZone API da Amazon feitas por meio do portal de DataZone dados da Amazon em um grupo de registros chamado DataZoneDataPortalAPI CallLogs.

Monitorando DataZone eventos da Amazon na Amazon EventBridge

Você pode monitorar DataZone eventos da Amazon em EventBridge, que fornece um fluxo de dados em tempo real de seus próprios aplicativos, aplicativos software-as-a-service (SaaS) e AWS serviços. EventBridgeencaminha esses dados para destinos como o AWS Lambda Amazon Simple Notification Service. Esses eventos são os mesmos que aparecem no Amazon CloudWatch Events, que fornece um fluxo quase em tempo real de eventos do sistema que descrevem mudanças nos AWS recursos.

Para ter mais informações, consulte Trabalhando com eventos por meio do barramento EventBridge padrão da Amazon.

Registrando chamadas de DataZone API da Amazon usando AWS CloudTrail

DataZone A Amazon está integrada com AWS CloudTrail, um serviço que fornece um registro das ações realizadas por um usuário, função ou AWS serviço na Amazon DataZone. CloudTrail captura todas as chamadas de API para a Amazon DataZone como eventos. As chamadas capturadas incluem chamadas do DataZone console da Amazon e chamadas de código para as operações de DataZone API da Amazon. Se você criar uma trilha, poderá habilitar a entrega contínua de CloudTrail eventos para um bucket do Amazon S3, incluindo eventos para a Amazon. DataZone Se você não configurar uma trilha, ainda poderá ver os eventos mais recentes no CloudTrail console no Histórico de eventos. Usando as informações coletadas por CloudTrail, você pode determinar a solicitação que foi feita à Amazon DataZone, o endereço IP a partir do qual a solicitação foi feita, quem fez a solicitação, quando ela foi feita e detalhes adicionais.

Para saber mais sobre isso CloudTrail, consulte o Guia AWS CloudTrail do usuário.

DataZone Informações da Amazon em CloudTrail

CloudTrail é ativado no seu Conta da AWS quando você cria a conta. Quando a atividade ocorre no console DataZone de gerenciamento da Amazon, essa atividade é registrada em um CloudTrail evento junto com outros eventos AWS de serviço no histórico de eventos. Você pode visualizar, pesquisar e baixar eventos recentes no seu Conta da AWS. Para obter mais informações, consulte Visualização de eventos com histórico de CloudTrail eventos.

Para um registro contínuo de eventos em seu Conta da AWS, incluindo eventos para a Amazon DataZone, crie uma trilha. Uma trilha permite CloudTrail entregar arquivos de log para um bucket do Amazon S3. Por padrão, quando você cria uma trilha no console, ela é aplicada a todas as Regiões da AWS. A trilha registra eventos de todas as regiões na AWS partição e entrega os arquivos de log ao bucket do Amazon S3 que você especificar. Além disso, você pode configurar outros AWS serviços para analisar e agir com base nos dados de eventos coletados nos CloudTrail registros. Para mais informações, consulte:

- Visão geral da criação de uma trilha
- CloudTrail serviços e integrações suportados
- Configurando notificações do Amazon SNS para CloudTrail
- Recebendo arquivos de CloudTrail log de várias regiões e Recebendo arquivos de CloudTrail log de várias contas

Todas as DataZone ações da Amazon são registradas por CloudTrail.

Solução de problemas da Amazon DataZone

Se você encontrar problemas de acesso negado ou dificuldades semelhantes ao trabalhar com a Amazon, DataZone consulte os tópicos desta seção.

Solução de problemas de permissões do AWS Lake Formation para a Amazon DataZone

Esta seção contém instruções de solução de problemas que você pode encontrar aoConfigurar as permissões do Lake Formation para a Amazon DataZone.

Mensagem de erro no Portal de Dados	Resolução
Não é possível assumir a função de acesso a dados.	Esse erro é exibido quando a Amazon DataZone não consegue assumir o AmazonDataZoneGlueDataAccessRoleque você usou para habilitá-lo DefaultDataLakeBlueprintem sua conta. Para corrigir o problema, acesse o console AWS do IAM na conta em que seu ativo de dados existe e verifique se ele AmazonDataZoneGlueDataAccessRoletem a relação de confiança correta com o responsável pelo DataZone serviço principal da Amazon. Para mais informações, consulte AmazonDataZoneGlueAccess- <region>- <domainId>.
A função de acesso a dados não tem as permissões necessárias para ler os metadados do ativo que você está tentando assinar.	Esse erro é exibido quando a Amazon assume DataZone com sucesso a AmazonDataZoneGlueDataAccessRolefunção, mas a função não tem as permissões necessárias. Para corrigir o problema, acesse o console AWS do IAM na conta em que seu ativo de dados existe e verifique se a função está AmazonDataZoneGlueManageAccessRolePolicyanexada. Para ter mais informações,

Mensagem de erro no Portal de Dados	Resolução
	consulte AmazonDataZoneGlueAccess-<region>- <domainId>.
O ativo é um link de recurso. A Amazon DataZone não oferece suporte a assinaturas de links de recursos.	Esse erro é exibido quando o ativo que você está tentando publicar na Amazon DataZone é um link de recurso para uma tabela do AWS Glue.

Mensagem de erro no Portal de Dados	Resolução
O ativo não é gerenciado pela AWS Lake Formation.	Esse erro indica que as permissões do AWS Lake Formation não são aplicadas ao ativo que você deseja publicar. Isso pode acontecer nos seguintes casos. • A localização do ativo no Amazon S3 não está registrada no AWS Lake Formation . Para corrigir o problema, faça login no console do AWS Lake Formation na conta em que a tabela existe e registre a localizaç ão do Amazon S3 no modo AWS Lake Formation ou no modo Hybrid. Para obter mais informações, consulte Registering an Amazon S3 location (Registrar um local do Amazon S3). Há vários cenários que exigem modificações adicionais. Isso inclui buckets criptografados do AmazonS3 ou um bucket S3 com várias contas e uma configuração do Glue Catalog. AWS Nesses casos, modificaç ões nas configurações do KMS e/ou do S3 podem ser necessárias. Para obter mais informações, consulte Registrar um local do Amazon S3. • A localização do Amazon S3 é registrada no modo AWS Lake Formation, mas o IAM AllowedPrincipal é adicionado às permissõe s da tabela. Para corrigir o problema, você pode remover o IAM AllowedPrincipal das permissões da tabela ou registrar a localizaç ão do S3 no modo híbrido. Para obter mais informações, consulte Sobre a atualizaç ão para o modelo de permissões do Lake Formation. Se sua localização do S3 estiver criptografada ou estiver em uma conta diferente da tabela AWS Glue, siga as

Mensagem de erro no Portal de Dados	Resolução
	instruções em Registro de uma localização criptografada do Amazon S3.
A função Data Access não tem as permissões necessárias do Lake Formation para conceder acesso a esse ativo.	Esse erro indica que o AmazonDataZoneGlueDataAccessRoleque você está usando para habilitar o DefaultDataLakeBlueprintem sua conta não tem as permissões necessárias para que DataZone a Amazon gerencie as permissões no ativo publicado. Você pode resolver o problema adicionando o AmazonDataZoneGlueDataAccessRolecomo administrador do AWS Lake Formation ou concedendo as seguintes permissões ao AmazonDataZoneGlueDataAccessRoleativo que você deseja publicar. • Descreva e descreva as permissões concedidas no banco de dados em que o ativo existe • Descreva, selecione, descreva as permissões concedidas, selecione as permissões concedidas em todos os ativos do banco de dados cujo acesso você deseja que a Amazon gerencie em seu nome. DataZone

Cotas para a Amazon DataZone

Sua AWS conta tem cotas padrão, anteriormente chamadas de limites, para cada AWS serviço. A menos que especificado de outra forma, cada cota é específica da região.

A Amazon DataZone tem as seguintes cotas e limites.

Recurso	Descrição	Valor
Tipos de ativos de dados	O número máximo de tipos de ativos de dados que podem ser criados em um DataZone domínio	1000
Ativos de dados	O número máximo de ativos de dados que podem ser criados em um DataZone domínio da Amazon	1 milhão
Glossários	O número máximo de glossários de negócios que você pode criar em um domínio	1000
Termos do glossário de negócios	O número máximo de termos totais do glossário de negócios que você pode criar em um domínio	10000
Ambientes em um domínio	O número máximo de ambientes em um DataZone domínio da Amazon	500

Histórico de documentos do Guia do DataZone usuário da Amazon

A tabela a seguir descreve os lançamentos da documentação da Amazon DataZone.

Alteração	Descrição	Data
AmazonDataZoneSageMakerProvisioning - nova política	A nova política chamada AmazonDataZoneSageMakerProvisioningconcede à Amazon DataZone as permissões necessárias para interoperar com a Amazon SageMaker. Para obter mais informações, consulte as DataZone atualizações da Amazon para políticas AWS gerenciadas.	30 de abril de 2024
AmazonDataZoneSageMakerEnvironmentRolePermissionsBoundary - novo limite de permissões	Novo limite de permissões chamado AmazonDataZoneSageMakerEnvironmentRolePermissionsBoundary. Quando você cria um SageMaker ambiente Amazon por meio do portal de DataZone dados da Amazon, a Amazon DataZone aplica esse limite de permissões às funções do IAM que são produzidas durante a criação do ambiente. O limite de permissões limita o escopo das funções que a Amazon DataZone cria e de todas as funções que você adiciona.	30 de abril de 2024

	Para obter mais informaçõ es, consulte as DataZone atualizações da Amazon para políticas AWS gerenciadas.	
AmazonDataZoneSage MakerAccess - nova política	A nova política chamada AmazonDataZoneSage MakerAccessconcede DataZone à Amazon as permissões necessárias para conceder ao usuário acesso a vários recursos no SageMaker ambiente da Amazon. Para obter mais informações, consulte as DataZone atualizações da Amazon para políticas AWS gerenciadas.	30 de abril de 2024
AmazonDataZoneFullAccess - atualização da política	Uma atualização da AmazonDataZoneFull Accesspolítica que adiciona acesso à `DescribeS ecurityGroups` ação para melhorar a usabilidade dos administradores de contas, configurando esquemas no console e `GetPolicy` ações para ajudar a recuperar informações sobre a política gerenciada especificada. Para obter mais informaçõ es, consulte as DataZone atualizações da Amazon para políticas AWS gerenciadas.	30 de abril de 2024

AmazonDataZoneS3Manage- - nova função <region>< domainId>	Nova função chamada AmazonDataZoneS3Manage- - <region><domainId>que é usada quando a Amazon DataZone chama a AWS Lake Formation para registrar uma localização do Amazon Simple Storage Service (Amazon S3). AWS Lake Formation assume essa função ao acessar os dados naquele local. Para obter mais informaçõ es, consulte as DataZone atualizações da Amazon para políticas AWS gerenciadas.	1º de abril de 2024
AmazonDataZoneGlue ManageAccessRolePolicy - Atualização da política	Atualizou o AmazonDat aZoneGlueManageAcc essRolePolicypara permitir o suporte a permissões que permitem DataZone à Amazon habilitar concessõe s de publicação e acesso aos dados. Para obter mais informações, consulte as DataZone atualizações da Amazon para políticas AWS gerenciadas.	1º de abril de 2024

AmazonDataZoneDomainExecutionRolePolicy e AmazonDataZoneFullUserAccess - Atualização da política	Atualizou o AmazonDataZoneDomainExecutionRolePolicye AmazonDataZoneFullUserAccesspara habilitar o suporte para a `CancelMetadataGenerationRun` API. Para obter mais informações, consulte as DataZone atualizações da Amazon para políticas AWS gerenciadas.	29 de março de 2024
AmazonDataZoneFullAccess - Atualização da política	Atualizado `AmazonDataZoneFullAccess` para permitir que os usuários escolham seus segredos, clusters, vPCs e sub-redes no console de DataZone gerenciamento da Amazon em vez de digitá-los em uma caixa de texto. Para obter mais informações, consulte as DataZone atualizações da Amazon para políticas AWS gerenciadas.	13 de março de 2024

AmazonDataZoneDomainExecutionRolePolicy - Atualização da política	Atualizou o AmazonDataZoneDomainExecutionRolePolicypara habilitar o suporte para a ListEnvironmentBlueprintConfigurationSummaries API necessária para criar perfis de ambiente, identificando quais blueprints estão habilitados em qual conta e região. Para obter mais informações, consulte as DataZone atualizações da Amazon para políticas AWS gerenciadas.	1 de fevereiro de 2024
AmazonDataZoneGlueManageAccessRolePolicy - Atualização da política	Atualizado o AmazonDataZoneGlueManageAccessRolePolicypara habilitar o suporte ao modo híbrido AWS Lake Formation. Para obter mais informações, consulte as DataZone atualizações da Amazon para políticas AWS gerenciadas.	14 de dezembro de 2023

AmazonDataZoneFullUserAccess e AmazonDataZoneDomainExecutionRolePolicy - Atualizações da política	A Amazon DataZone atualizou AmazonDataZoneFullUserAccessas AmazonDataZoneDomainExecutionRolePolicypolíticas para apoiar o recurso generativo de descrições de dados baseado em IA na Amazon. DataZone Para obter mais informações, consulte as DataZone atualizações da Amazon para políticas AWS gerenciadas.	28 de novembro de 2023
AmazonDataZoneEnvironmentRolePermissionsBoundary - Atualização da política	A Amazon DataZone fez uma atualização na política AmazonDataZoneEnvironmentRolePermissionsBoundarygerenciada que consiste em uma `athena:GetQueryResultsStream` permissão adicional com o escopo da `ResourceTag` condição. Para obter mais informações, consulte as DataZone atualizações da Amazon para políticas AWS gerenciadas.	17 de novembro de 2023

AmazonDataZoneRedshiftManageAccessRolePolicy - Atualização da política	A Amazon DataZone atualizou a AmazonDataZoneRedshiftManageAccessRolePolicypolítica removendo a verificação do ID da organização para a `redshift:AssociateDataShareConsumer` ação. Isso permite que você compartilhe recursos entre AWS organizações. Para obter mais informações, consulte as DataZone atualizações da Amazon para políticas AWS gerenciadas.	16 de novembro de 2023
AmazonDataZoneFullUserAccess - Atualização da política	A Amazon DataZone atualizou a AmazonDataZoneFullUserAccesspolítica que concede acesso total à Amazon DataZone, mas não permite o gerenciamento de domínios, usuários ou contas associadas. Para obter mais informações, consulte DataZone Atualizações da Amazon para políticas AWS gerenciadas.	2 de outubro de 2023

AmazonDataZonePreviewConsoleFullAccess - política obsoleta	A Amazon DataZone suspendeu o uso do AmazonDataZonePreviewConsoleFullAccess. Para obter mais informações, consulte as DataZone atualizações da Amazon para políticas gerenciadas. AWS	29 de setembro de 2023
AmazonDataZonePortalFullAccessPolicy - política obsoleta	A Amazon DataZone suspendeu o uso do AmazonDataZonePortalFullAccessPolicy. Para obter mais informações, consulte as DataZone atualizações da Amazon para políticas gerenciadas. AWS	29 de setembro de 2023

AmazonDataZoneDomainExecutionRolePolicy - Nova política	A Amazon DataZone adicionou uma nova política chamada AmazonDataZoneDomainExecutionRolePolicy. Essa é a política padrão para a função de DataZone `AmazonDataZoneDomainExecutionRole` serviço da Amazon. Essa função é usada pela Amazon DataZone para catalogar, descobrir, controlar, compartilhar e analisar dados no DataZone domínio da Amazon. Você pode anexar a `AmazonDataZoneDomainExecutionRolePolicy` política ao seu`AmazonDataZoneDomainExecutionRole` . Para obter mais informações, consulte as DataZone atualizações da Amazon para políticas AWS gerenciadas.	25 de setembro de 2023

AmazonDataZoneCrossAccountAdmin - Nova política	A Amazon DataZone adicionou uma nova política chamada AmazonDataZoneCrossAccountAdminque permite que os usuários trabalhem com a Amazon DataZone e suas contas associadas. Para obter mais informações, consulte as DataZone atualizações da Amazon para políticas AWS gerenciadas.	19 de setembro de 2023
AmazonDataZoneRedshiftManageAccessRolePolicy - Nova política	A Amazon DataZone adicionou uma nova política chamada AmazonDataZoneRedshiftManageAccessRolePolicyque concede permissões para permitir que a Amazon habilite DataZone a publicação e o acesso a subsídios aos dados. Para obter mais informações, consulte as DataZone atualizações da Amazon para políticas AWS gerenciadas.	12 de setembro de 2023

AmazonDataZoneRedshiftGlueProvisioningPolicy - Nova política	A Amazon DataZone adicionou uma nova política chamada AmazonDataZoneRedshiftGlueProvisioningPolicyque concede à Amazon DataZone as permissões necessárias para interoperar com as fontes de dados suportadas. Para obter mais informações, consulte as DataZone atualizações da Amazon para políticas AWS gerenciadas.	12 de setembro de 2023
AmazonDataZoneGlueManageAccessRolePolicy - Nova política	A Amazon DataZone adicionou uma nova política chamada AmazonDataZoneGlueManageAccessRolePolicyconcede DataZone permissões à Amazon para publicar dados do AWS Glue no catálogo. Também concede à Amazon DataZone permissões para conceder acesso ou revogar o acesso aos ativos publicados do AWS Glue no catálogo. Para obter mais informações, consulte as DataZone atualizações da Amazon para políticas AWS gerenciadas.	12 de setembro de 2023

AmazonDataZoneFull UserAccess - Nova política	A Amazon DataZone adicionou uma nova política chamada AmazonDat aZoneFullUserAccessque concede acesso total à Amazon DataZone por meio do portal de dados. Para obter mais informações, consulte as DataZone atualizações da Amazon para políticas AWS gerenciadas.	12 de setembro de 2023
AmazonDataZoneFullAccess - Nova política	A Amazon DataZone adicionou uma nova política chamada AmazonDat aZoneFullAccessque fornece acesso total à Amazon DataZone por meio do AWS Management Console. Para obter mais informaçõ es, consulte as DataZone atualizações da Amazon para políticas AWS gerenciadas.	12 de setembro de 2023
AmazonDataZoneEnvi ronmentRolePermiss ionsBoundary - Nova política	A Amazon DataZone adicionou uma nova política chamada AmazonDat aZoneEnvironmentRo lePermissionsBoundaryque limita o principal do IAM provisionado ao qual ela está vinculada. Para obter mais informações, consulte as DataZone atualizações da Amazon para políticas AWS gerenciadas.	12 de setembro de 2023

Atualização gerenciada da política	Atualizações na política AmazonDataZonePreviewConsoleFullAccess gerenciada. Para obter mais informações, consulte as DataZone atualizações da Amazon para políticas AWS gerenciadas.	13 de junho de 2023
Atualização gerenciada da política	Atualizações na política AmazonDataZoneProjectDeploymentPermissionsBoundary gerenciada. Para obter mais informações, consulte as DataZone atualizações da Amazon para políticas AWS gerenciadas.	3 de abril de 2023
???	Versão inicial do Guia do usuário da Amazon DataZone (Preview).	29 de março de 2023

As traduções são geradas por tradução automática. Em caso de conflito entre o conteúdo da tradução e da versão original em inglês, a versão em inglês prevalecerá.