aws

Guide de l’utilisateur

Amazon DataZone

Amazon DataZone: Guide de l’utilisateur

Table of Contents

Qu'est-ce qu'Amazon DataZone ?

Amazon DataZone est un service de gestion des données qui vous permet de cataloguer, de découvrir, de partager et de gérer plus rapidement et plus facilement les données stockées auprès de sources tierces AWS, sur site ou sur site. Avec Amazon DataZone, les administrateurs qui supervisent les actifs de données de l'organisation peuvent gérer et gouverner l'accès aux données à l'aide de contrôles précis. Ces contrôles permettent de garantir un accès avec le bon niveau de privilèges et de contexte. Amazon DataZone permet aux ingénieurs, aux data scientists, aux chefs de produit, aux analystes et aux utilisateurs professionnels de partager et d'accéder facilement aux données au sein d'une organisation afin qu'ils puissent découvrir, utiliser et collaborer pour obtenir des informations basées sur les données.

Amazon vous DataZone aide à fournir des données directement aux utilisateurs finaux et simplifie votre architecture en intégrant des services de gestion des données, notamment Amazon Redshift, Amazon Athena, QuickSight Amazon, Glue AWS , AWS Lake Formation, des sources sur site, des sources tierces, etc.

Rubriques

Que puis-je faire avec Amazon DataZone ?

Avec Amazon DataZone, vous pouvez effectuer les opérations suivantes :

- Gérez l'accès aux données au-delà des limites de l'organisation. Avec Amazon DataZone, vous pouvez garantir que les bonnes données sont accessibles par le bon utilisateur aux bonnes fins, conformément aux règles de sécurité de votre entreprise, sans vous fier à des informations d'identification individuelles. Vous pouvez également garantir la transparence sur l'utilisation des actifs de données et approuver les abonnements aux données grâce à un flux de travail régi. Vous pouvez également surveiller les actifs de données dans l'ensemble des projets grâce à des fonctionnalités d'audit d'utilisation.
- Connectez les travailleurs des données grâce à des données et à des outils partagés pour obtenir des informations commerciales. Avec Amazon DataZone, vous pouvez améliorer l'efficacité de

votre équipe commerciale en collaborant harmonieusement entre les équipes et en fournissant un accès en libre-service aux données et aux outils d'analyse. Vous pouvez utiliser des termes commerciaux pour rechercher, partager et accéder aux données cataloguées stockées chez AWS, sur site ou auprès de fournisseurs tiers. Vous pouvez également en savoir plus sur les données que vous souhaitez utiliser en utilisant les glossaires DataZone commerciaux d'Amazon.

- Automatisez la découverte et le catalogage des données grâce à l'apprentissage automatique. Amazon DataZone vous permet de réduire le temps consacré à la saisie manuelle des attributs de données dans le catalogue de données commerciales. Des données plus riches dans le catalogue de données améliorent également l'expérience de recherche.

Comment Amazon DataZone prend en charge les autres AWS services et s'y intègre ?

Amazon DataZone prend en charge trois types d'intégrations avec d'autres AWS services :

- Sources de données du producteur : vous pouvez publier des actifs de données dans le DataZone catalogue Amazon à partir des données stockées dans les tables et vues AWS Glue Data Catalog et Amazon Redshift. Vous pouvez également publier manuellement des objets depuis Amazon Simple Storage Service (S3) dans le catalogue Amazon DataZone .
- Outils grand public : vous pouvez utiliser les éditeurs de requêtes Amazon Athena ou Amazon Redshift pour accéder à vos actifs de données et les analyser.
- Contrôle d'accès et traitement des commandes : Amazon DataZone prend en charge l'octroi de l'accès aux tables AWS Glue gérées par AWS Lake Formation et aux tables et vues Amazon Redshift. Pour tous les autres actifs de données, Amazon DataZone publie des événements standard liés à vos actions (par exemple, l'approbation donnée à une demande d'abonnement) sur Amazon EventBridge. Vous pouvez utiliser ces événements standard pour intégrer d'autres AWS services ou des solutions tierces pour des intégrations personnalisées.

Comment accéder à Amazon DataZone ?

Vous pouvez accéder DataZone à Amazon de l'une des manières suivantes :

- DataZone Console Amazon

  Vous pouvez utiliser la console DataZone de gestion Amazon pour accéder à vos DataZone domaines, plans et utilisateurs Amazon et les configurer. Pour plus d'informations, consultez

https://console.aws.amazon.com/datazone. La console DataZone de gestion Amazon est également utilisée pour créer le portail de DataZone données Amazon.

- Portail DataZone de données Amazon

  Le portail de DataZone données Amazon est une application Web basée sur un navigateur dans laquelle vous pouvez cataloguer, découvrir, gérer, partager et analyser des données en libre-service. Le portail de données peut vous authentifier à l'aide des informations d'identification de votre fournisseur d'identité via AWS IAM Identity Center (successeur du AWS SSO) ou à l'aide de vos informations d'identification IAM. Vous pouvez obtenir l'URL du portail de données en accédant à la DataZone console Amazon à l'adresse https://console.aws.amazon.com/datazone.

- API DataZone HTTPS Amazon

  Vous pouvez accéder à Amazon par DataZone programmation en utilisant l'API Amazon DataZone HTTPS, qui vous permet d'envoyer des requêtes HTTPS directement au service. Pour plus d'informations, consultez le Amazon DataZone API Reference.

DataZone Terminologie et concepts d'Amazon

Lorsque vous débutez avec Amazon DataZone, il est important que vous compreniez ses concepts clés, sa terminologie et ses composants.

Rubriques

DataZone Composants Amazon

Amazon DataZone inclut les quatre principaux composants suivants :

- Catalogue de données commerciales : vous pouvez utiliser ce composant pour cataloguer les données de votre organisation en fonction du contexte commercial et permettre ainsi à tous les membres de votre organisation de trouver et de comprendre rapidement les données.
- Publiez et abonnez des flux de travail : vous pouvez utiliser ces flux de travail automatisés pour sécuriser les données entre les producteurs et les consommateurs en libre-service et pour garantir que tous les membres de votre organisation ont accès aux bonnes données aux bonnes fins.
- Projets et environnements
  - Dans Amazon, les DataZone projets sont des regroupements de personnes, d'actifs (données) et d'outils basés sur des cas d'utilisation professionnelle utilisés pour simplifier l'accès aux analyses. AWS Les projets fournissent des zones dans lesquelles les membres du projet peuvent collaborer, échanger des données et partager des actifs. Par défaut, les projets sont confiés de telle sorte que seuls ceux qui y sont explicitement ajoutés puissent accéder aux données et aux outils d'analyse qu'ils contiennent. Les projets gèrent la propriété des actifs produits conformément aux politiques du projet relatives à l'accès des consommateurs de données.

  - Au sein DataZone des projets Amazon, les environnements sont des ensembles de ressources configurées nulles ou plus (par exemple, un compartiment Amazon S3, une AWS Glue base de données ou un groupe de travail Amazon Athena) sur lesquels un ensemble donné de principes IAM (par exemple, les utilisateurs disposant d'autorisations de contributeur) peut opérer.
- Portail de données (en dehors de la console de AWS gestion) : il s'agit d'une application Web basée sur un navigateur dans laquelle différents utilisateurs peuvent accéder pour cataloguer, découvrir, gouverner, partager et analyser des données en libre-service. Le portail de données authentifie les utilisateurs à l'aide d'informations d'identification IAM ou d'informations d'identification existantes auprès de votre fournisseur d'identité via. AWS IAM Identity Center

Que sont les DataZone domaines Amazon ?

Vous pouvez utiliser DataZone les domaines Amazon pour organiser vos actifs, vos utilisateurs et leurs projets. En associant des AWS comptes supplémentaires à vos DataZone domaines Amazon, vous pouvez regrouper vos sources de données. Vous pouvez ensuite publier les ressources issues de ces sources de données dans le catalogue de votre domaine, à l'aide de formulaires de métadonnées et de glossaires qui améliorent l'exhaustivité et la qualité des métadonnées. Vous pouvez également rechercher et parcourir ces ressources pour voir quelles données sont publiées dans le domaine. En outre, vous pouvez rejoindre des projets pour collaborer avec d'autres utilisateurs, vous abonner à des ressources et utiliser des environnements de projet pour accéder à des outils d'analyse, notamment Amazon Athena et Amazon Redshift. Les DataZone domaines Amazon vous offrent la flexibilité nécessaire pour répondre aux besoins en données et en analyse de votre structure organisationnelle, qu'il s'agisse de créer un seul DataZone domaine Amazon pour votre entreprise ou plusieurs DataZone domaines Amazon pour différentes unités commerciales.

Quels sont les DataZone projets et les environnements Amazon ?

Amazon DataZone permet aux équipes et aux utilisateurs d'outils d'analyse de collaborer sur des projets en créant des groupes d'équipes, d'outils et de données basés sur des cas d'utilisation.

- Dans Amazon DataZone, les projets permettent à un groupe d'utilisateurs de collaborer sur divers cas d'utilisation commerciale impliquant la publication, la découverte, l'abonnement et la consommation de données du DataZone catalogue Amazon. Les membres du projet consomment les actifs du DataZone catalogue Amazon et en produisent de nouveaux à l'aide d'un ou de plusieurs flux de travail analytiques. Les projets soutiennent les activités suivantes au sein du portail de données :

- Les propriétaires de projets peuvent ajouter des membres avec des autorisations de propriétaire et de contributeur
- Les membres du projet peuvent être des utilisateurs SSO, des groupes SSO et des utilisateurs IAM
- Les membres du projet peuvent demander un abonnement aux actifs du catalogue de données

  Les approbations d'abonnement sont fournies aux projets
- Dans un DataZone projet Amazon, les environnements sont des ensembles de ressources configurées nulles ou plus (par exemple, un Amazon S3, une AWS Glue base de données ou un groupe de travail Amazon Athena), avec un ensemble donné de principes IAM capables d'opérer sur ces ressources. Les environnements sont créés à l'aide de profilés d'environnement, qui sont des ensembles préconfigurés de ressources et de plans qui fournissent des modèles réutilisables pour créer des environnements. Les profils d'environnement définissent des paramètres tels que la région Compte AWS ou la région dans laquelle les environnements sont déployés.

Que sont les DataZone plans Amazon ?

Un plan avec lequel l'environnement est créé définit les AWS outils et services (par exemple, AWS Glue ou Amazon Redshift) que les membres du projet auquel appartient l'environnement peuvent utiliser lorsqu'ils travaillent avec les actifs du catalogue Amazon DataZone .

Dans la version actuelle d'Amazon DataZone, les plans par défaut suivants sont pris en charge :

Nom du plan	Description	Ressources créées
Plan directeur de Data Lake	Permet aux membres DataZone du projet Amazon de lancer les services aux producteurs et aux consommateurs de Data Lake au sein de l'environnement. En tant que consommateur, il permet aux membres DataZone du projet Amazon d'accéder à une copie « en	Permet aux utilisateurs de créer et d'interroger des tables de Lake Formation à l'aide d'Amazon Athena. Groupe de travail Amazon Athena, AWS Glue base de données avec autorisations « lecture seule » sur Lake Formation, autorisations IAM « lecture seule » et accès à Amazon S3 géré par le projet. AWS Glue base de

Nom du plan	Description	Ressources créées
	lecture seule » des ressources gérées par Lake Formation directement dans Amazon Athena et dans d'autres moteurs de requêtes pris en charge par Lake Formation. En tant que producteur, il permet aux membres DataZone du projet Amazon de créer de nouvelles tables LakeFormation gérées à l'aide d'Amazon Athena et de les publier dans le catalogue Amazon DataZone.	données avec autorisations « créer » et « accorder » à Lake Formation, autorisations IAM « lecture » et « écriture », AWS Glue ETL (extraction, transformation et chargement) avec balisage.

Nom du plan	Description	Ressources créées
Plan d'entrepôt de données	En tant que consommateur, ce plan permet aux membres DataZone du projet Amazon de se connecter à leurs propres clusters Amazon Redshift pour interroger des magasins de données distants et créer et stocker de nouveaux ensembles de données. En tant que producteur, ce plan permet aux membres DataZone du projet Amazon de se connecter à leurs propres clusters Amazon Redshift pour interroger des magasins de données distants, créer de nouveaux ensembles de données et les publier dans le catalogue Amazon. DataZone	Accès à l'éditeur de requêtes Amazon Redshift, accès en « lecture » aux sources de données abonnées depuis le DataZone catalogue Amazon, possibilité de créer des ressources locales dans le cluster Amazon Redshift configuré. Accès à l'éditeur de requêtes Amazon Redshift, accès en « lecture » aux sources de données abonnées depuis le DataZone catalogue Amazon, possibilité de créer et de publier des ressource s à partir du cluster Amazon Redshift configuré.

Nom du plan	Description	Ressources créées
Plan Amazon Sagemaker	Ce plan aide les producteurs de données et les consommateurs à passer facilement SageMaker à Amazon pour collaborer sur des projets d'apprentissage automatique (ML) tout en renforçant la gouvernance de l'accès aux données et aux actifs de machine learning. Grâce à la nouvelle intégration intégrée entre Amazon DataZone et Amazon SageMaker, les consommateurs et les producteurs de données peuvent rationaliser la gouvernance du ML lors de la configuration de l'infrastructure, collaborer sur des initiatives commerciales et gérer facilement les données et les actifs de ML.	Vous pouvez créer un SageMaker domaine Amazon qui permet de rechercher, de souscrire et de publier des données et des actifs de machine learning sur Amazon DataZone. Vous pouvez également vous abonner et publier sur les bases de données AWS Glue et sur la formation des lacs selon la configuration.

Que sont les flux de DataZone production et de publication d'Amazon ?

Création des actifs d'inventaire du projet

Pour pouvoir utiliser Amazon DataZone pour cataloguer vos données, vous devez d'abord les importer (actifs) en tant qu'inventaire de votre projet sur Amazon DataZone. La création d'un inventaire pour un projet rend les actifs accessibles uniquement aux membres de ce projet. Les ressources de l'inventaire du projet ne sont pas accessibles à tous les utilisateurs du domaine lors de

la recherche ou de la navigation, sauf si elles sont publiées explicitement. Dans la version actuelle d'Amazon DataZone, vous pouvez ajouter des actifs à l'inventaire du projet de la manière suivante :

- Créez et exécutez des sources de données via le portail de données ou à l'aide des DataZone API Amazon. Dans la version actuelle d'Amazon DataZone, vous pouvez créer et exécuter des sources de données pour AWS Glue et Amazon Redshift. En créant et en exécutant des sources de données AWS Glue ou Amazon Redshift, vous créez des actifs dans l'inventaire d'un projet choisi et vous importez leurs métadonnées techniques depuis les tables de la base de données source ou les entrepôts de données sous forme d'inventaire sur Amazon. DataZone
- À l'aide des API, vous pouvez créer des actifs à partir des types de ressources système disponibles (AWS Glue, Amazon Redshift, objets Amazon S3) ou à partir de vos types de ressources personnalisés.
  - Créez des types d'actifs personnalisés dans l'inventaire d'un projet à l'aide des DataZone API Amazon. Les types d'actifs personnalisés peuvent inclure des modèles de machine learning, des tableaux de bord, des tables sur site, etc.
  - Créez des actifs à partir de ces types d'actifs personnalisés à l'aide DataZone des API Amazon.
- Créez manuellement des ressources pour les objets S3 à l'aide du portail DataZone de données Amazon.

Gestion des actifs d'inventaire de votre projet : après avoir créé un inventaire de projet, les propriétaires de données peuvent organiser leurs actifs d'inventaire avec les métadonnées commerciales requises en ajoutant ou en mettant à jour les noms commerciaux (actif et schéma), les descriptions (actif et schéma), lisez-moi, les termes du glossaire (actif et schéma) et les formulaires de métadonnées. Vous pouvez le faire via le portail de données ou en utilisant les DataZone API Amazon. Chaque modification apportée à votre actif crée une nouvelle version de l'inventaire.

Publication des actifs de l'inventaire du projet dans le DataZone catalogue Amazon

L'étape suivante de l'utilisation d'Amazon DataZone pour cataloguer vos données consiste à rendre les actifs d'inventaire de votre projet accessibles aux utilisateurs du domaine. Vous pouvez le faire en publiant les actifs d'inventaire dans le DataZone catalogue Amazon. Seule la dernière version de la ressource d'inventaire peut être publiée dans le catalogue et seule la dernière version publiée est active dans le catalogue de découverte. Si un actif d'inventaire est mis à jour après sa publication dans le DataZone catalogue Amazon, vous devez le republier explicitement pour que la dernière version figure dans le catalogue de découverte. Dans la version actuelle d'Amazon DataZone, vous

pouvez publier les actifs d'inventaire de votre projet dans le DataZone catalogue Amazon de la manière suivante :

- Publiez manuellement les actifs d'inventaire de votre projet dans le DataZone catalogue Amazon via le portail de données ou à l'aide des DataZone API Amazon.
- Dans le cadre de la création ou de la modification de sources de données, activez les paramètres facultatifs Publish your AWS Glue dans le catalogue ou Publiez vos actifs Amazon Redshift dans le catalogue à utiliser lors des exécutions planifiées ou automatisées des sources de données. Lorsque ce paramètre est activé, l'exécution d'une source de données ajoute des actifs à l'inventaire de votre projet, puis publie également les actifs d'inventaire dans le DataZone catalogue Amazon. Notez que si vous publiez directement, les ressources peuvent ne pas contenir de métadonnées commerciales et seront directement accessibles à tous les utilisateurs du domaine. Vous pouvez utiliser ce paramètre sur vos sources de données via le portail de données ou à l'aide des DataZone API Amazon.

Quels sont les processus DataZone d'abonnement et d'expédition d'Amazon ?

Une fois vos actifs publiés dans le DataZone catalogue Amazon, les utilisateurs de votre domaine peuvent les découvrir, demander et accéder à ces actifs, et continuer à utiliser Amazon DataZone pour gérer, partager et analyser ces actifs.

Les utilisateurs demandent l'accès à une ressource en s'abonnant à cette ressource pour le compte d'un projet. Une fois qu'une demande d'abonnement est créée, les propriétaires de l'actif reçoivent une notification et peuvent examiner la demande d'abonnement et décider de l'approuver ou de la rejeter. Si la demande d'abonnement est approuvée par le propriétaire des données, le projet abonné obtient l'accès à cette ressource.

Une fois qu'une demande d'abonnement est approuvée, Amazon DataZone lance un flux de traitement des abonnements qui ajoute automatiquement l'actif à tous les environnements applicables au sein du projet en créant les subventions nécessaires dans AWS Lake Formation ou Amazon Redshift. Cela permet aux membres du projet abonnés d'interroger la ressource à l'aide de l'un des outils de requête (Amazon Athena ou éditeur de requêtes Amazon Redshift) de leur environnement.

Amazon DataZone peut déclencher cette logique d'expédition automatisée uniquement pour les actifs gérés (cela inclut les tables AWS Glue et les tables et vues Amazon Redshift). Pour

tous les autres types d'actifs (actifs non gérés), Amazon ne DataZone peut pas déclencher automatiquement l'expédition, mais publie un événement sur Amazon Eventbridge avec tous les détails nécessaires dans la charge utile de l'événement afin que vous puissiez créer les subventions nécessaires en dehors d'Amazon. DataZone Amazon fournit DataZone également l'`updateSubscriptionStatus`API qui vous permet de mettre à jour le statut de l'abonnement une fois qu'il est rempli en dehors d'Amazon DataZone afin qu'Amazon DataZone puisse informer les membres du projet qu'ils peuvent commencer à consommer l'actif.

Les personas des utilisateurs d'Amazon DataZone

Les principaux DataZone utilisateurs d'Amazon sont les suivants :

- Administrateurs de domaine responsables de la configuration d'Amazon DataZone en tant que plateforme d'analyse pour leur organisation.

  Dans le contexte d'Amazon DataZone, les administrateurs de domaines installent Amazon DataZone dans les AWS comptes, créent des DataZone domaines Amazon et configurent les associations de AWS comptes et de fournisseurs d'identité avec les DataZone domaines Amazon. Les administrateurs de domaine utilisent également d'autres consoles de AWS service telles que AWS Organization et Service Catalog pour configurer Amazon DataZone.
- Utilisateurs de données qui sont les principaux utilisateurs d'Amazon DataZone (éditeurs d'actifs et abonnés) pour leurs tâches d'analyse et d'apprentissage automatique.

  Les utilisateurs de données incluent les professionnels de l'analyse des données, les scientifiques des données et les utilisateurs du système qui produisent et consomment des actifs de données. Dans le contexte d'Amazon DataZone, les utilisateurs de données créent et rejoignent des projets et des environnements, s'abonnent et consomment des actifs de données à l'aide d'outils d'analyse ou d'apprentissage automatique préconfigurés, et publient les actifs de données de sortie dans le catalogue de DataZone domaines Amazon pour les partager avec d'autres.
- Développeurs de systèmes qui créent des modèles d'infrastructure personnalisés et intègrent Amazon DataZone à des catalogues internes ou à des systèmes de production.

  Dans le contexte d'Amazon DataZone, les développeurs de systèmes élaborent des plans d'environnement (modèles d'infrastructure) ou un pipeline CI/CD Infrastructure-As-Code en tant que fournisseur d'environnement, des pipelines de données pour promouvoir les actifs de données dans différents environnements, des adaptateurs de synchronisation des catalogues et de gestion des subventions d'abonnement pour les intégrer aux catalogues internes, ou des intégrations entre

les API DataZone Amazon et les interfaces utilisateur internes ou les systèmes de production si nécessaire.

- Des responsables de la gouvernance des données qui maîtrisent les définitions et les risques liés à la sécurité organisationnelle, à la confidentialité et aux autres politiques de conformité et qui s'assurent que l'utilisation d'Amazon DataZone dans leur entreprise est conforme à ces définitions.

DataZone Terminologie Amazon

Domaine

Un DataZone domaine Amazon est l'entité organisatrice qui connecte vos actifs, vos utilisateurs et leurs projets. Avec DataZone les domaines Amazon, vous avez la flexibilité nécessaire pour répondre aux besoins en données et en analyse de votre structure organisationnelle, qu'il s'agisse de créer un seul DataZone domaine Amazon pour votre entreprise ou plusieurs zones de données, des domaines pour différentes unités commerciales ou équipes.

Compte associé

L'association de vos AWS comptes à des DataZone domaines Amazon vous permet de publier les données de ces AWS comptes dans le DataZone catalogue Amazon et de créer DataZone des projets Amazon pour exploiter vos données sur plusieurs AWS comptes. Les demandes d'association de comptes ne peuvent être initiées que sur AWS des comptes possédant un DataZone domaine Amazon. Les demandes d'association de comptes ne peuvent être acceptées que par les utilisateurs administratifs des AWS comptes invités. Une fois qu'un AWS compte est associé à un DataZone domaine Amazon, vous pouvez enregistrer vos sources de données telles que le catalogue AWS Glue et Amazon Redshift dans ce compte sur ce domaine. L'association permet également à un AWS compte de créer des DataZone projets et des environnements Amazon.

Un Compte AWS peut être associé à un ou plusieurs DataZone domaines Amazon.

Source de données

Dans Amazon DataZone, vous pouvez utiliser des sources de données pour importer les métadonnées techniques des actifs (données) depuis les bases de données sources ou les entrepôts de données vers Amazon DataZone. Dans la version actuelle d'Amazon DataZone, vous pouvez créer et exécuter des sources de données pour AWS Glue et Amazon Redshift. En créant une source de données, vous établissez une connexion entre Amazon DataZone et la source (AWS Glue Data Catalog ou Amazon Redshift Warehouse) qui vous permet de lire les

métadonnées techniques, notamment les noms de tables, les noms de colonnes et les types de données. En créant une source de données, vous lancez également l'exécution initiale de la source de données qui crée de nouvelles ressources ou met à jour des actifs existants sur Amazon DataZone. Lors de la création d'une source de données ou une fois celle-ci créée avec succès, vous avez également la possibilité de définir un calendrier pour les exécutions de votre source de données.

Exécution de la source de données

Dans Amazon DataZone, une exécution de source de données est une tâche qu'Amazon DataZone exécute afin de créer des actifs dans les inventaires de projets et également de publier éventuellement des actifs d'inventaire de projet dans le DataZone catalogue Amazon. Les exécutions de sources de données peuvent être automatisées (lancées lors de la création initiale d'une source de données), planifiées ou manuelles. Les critères de sélection des données vous permettent d'affiner les ensembles de données existants et futurs à intégrer dans les inventaires des projets ou le DataZone catalogue Amazon, ainsi que la fréquence des mises à jour des métadonnées de ces actifs d'inventaire ou de catalogue.

Objectif d'abonnement

Sur Amazon DataZone, les objectifs d'abonnement vous permettent d'accéder aux données auxquelles vous êtes abonné dans le cadre de vos projets. Un objectif d'abonnement indique l'emplacement (par exemple, une base de données ou un schéma) et les autorisations requises (par exemple, un rôle IAM) qu'Amazon DataZone peut utiliser pour établir une connexion avec les données sources et pour créer les autorisations nécessaires afin que les membres du DataZone projet Amazon puissent commencer à interroger les données auxquelles ils se sont abonnés.

Demande d'abonnement

Sur Amazon DataZone, une demande d'abonnement est un processus qu'un DataZone projet Amazon doit suivre pour avoir accès à un actif spécifique. Les demandes d'abonnement peuvent être approuvées, rejetées, révoquées ou accordées.

Ressource

Dans Amazon DataZone, un actif est une entité qui présente un seul objet de données physique (par exemple, un tableau, un tableau de bord, un fichier) ou un objet de données virtuel (par exemple, une vue).

Asset type

Les types d'actifs définissent la manière dont les actifs sont représentés dans le DataZone catalogue Amazon. Un type d'actif définit le schéma d'un type d'actif spécifique. Lorsque des

actifs sont créés, ils sont validés par rapport au schéma défini par leur type d'actif (par défaut, la dernière version). Lorsqu'une mise à jour d'un actif a lieu, Amazon DataZone crée une nouvelle version d'actif et permet aux DataZone utilisateurs d'Amazon d'opérer sur toutes les versions d'actifs.

Glossaire commercial

Sur Amazon DataZone, un glossaire commercial est un ensemble de termes commerciaux qui peuvent être associés à des actifs. Un glossaire métier permet de garantir que les mêmes termes et définitions sont utilisés au sein d'une organisation dans ses différentes tâches d'analyse de données.

Les termes d'un glossaire commercial peuvent être ajoutés aux actifs et aux colonnes pour classer ou améliorer l'identification de ces attributs lors de la recherche. Le glossaire peut être sélectionné comme type de valeur pour un champ dans un formulaire de métadonnées associé à une ressource. Lorsqu'un terme particulier est sélectionné comme valeur pour le champ du formulaire de métadonnées d'un actif, les utilisateurs peuvent rechercher le terme du glossaire commercial et trouver les actifs associés.

Type de formulaire de métadonnées

Un type de formulaire de métadonnées est un modèle qui définit les métadonnées collectées et enregistrées lorsque les actifs sont créés sous forme d'inventaire ou publiés dans un DataZone domaine Amazon. Les types de formulaires de métadonnées peuvent être associés à une ressource de données. Les types de formulaires de métadonnées aident les administrateurs de domaine à définir les formulaires de métadonnées nécessaires pour ce domaine, tels que les informations de conformité, les informations réglementaires ou les classifications. Il permet aux administrateurs de domaine de personnaliser des métadonnées supplémentaires pour leurs actifs. Amazon DataZone propose des types de formulaires de métadonnées système tels que asset-common-details-form -type, column-business-metadata-form -type, glue-table-form-type, glue-view-form-type, redshift-table-form-type, redshift-view-form-type, s3- object-collection-form-type subscription-terms-form-type, et. suggestion-form-type

Formulaire de métadonnées

Dans Amazon DataZone, les formulaires de métadonnées définissent les métadonnées collectées et enregistrées lorsque les actifs sont créés sous forme d'inventaire ou publiés dans un DataZone domaine Amazon. Les définitions des formulaires de métadonnées sont créées dans le domaine du catalogue par un administrateur de domaine. Une définition de formulaire de métadonnées est composée d'une ou de plusieurs définitions de champs, avec prise en charge des types

de données booléens, datés, décimaux, entiers, chaînes et valeurs de champs du glossaire commercial.

Un administrateur de domaine applique un formulaire de métadonnées aux actifs de son domaine en ajoutant le formulaire de métadonnées à son domaine. Les éditeurs de ressources fournissent ensuite toutes les valeurs de champ facultatives et obligatoires dans le formulaire de métadonnées.

Projet

Dans Amazon DataZone, les projets permettent à un groupe d'utilisateurs de collaborer sur divers cas d'utilisation commerciale qui impliquent de créer des actifs dans les inventaires de projets et de les rendre ainsi accessibles à tous les membres du projet, puis de publier, de découvrir, de souscrire et de consommer des actifs dans le catalogue Amazon DataZone . Les membres du projet consomment les actifs du DataZone catalogue Amazon et en produisent de nouveaux à l'aide d'un ou de plusieurs flux de travail analytiques. Les membres du projet peuvent être propriétaires ou contributeurs. Les propriétaires de projets peuvent ajouter ou supprimer d'autres utilisateurs en tant que propriétaires ou contributeurs, et ils peuvent modifier ou supprimer des projets. D'autres restrictions imposées aux contributeurs peuvent être définies à l'aide de politiques. Lorsqu'un utilisateur crée un projet, il en devient le premier propriétaire.

Environnement

Un environnement est un ensemble de ressources configurées (par exemple, un compartiment Amazon S3, une AWS Glue base de données ou un groupe de travail Amazon Athena), avec un ensemble donné de principes IAM (avec des autorisations de contributeur attribuées) qui peuvent opérer sur ces ressources. Chaque environnement peut également avoir des utilisateurs principaux autorisés à accéder aux ressources et aux données via un abonnement et un traitement des commandes. Les environnements sont conçus pour stocker des liens exploitables vers des AWS services, des IDE externes et des consoles. Les membres du projet peuvent accéder à des services tels que la console Amazon Athena et bien d'autres via des liens profonds configurés dans un environnement. Les utilisateurs SSO et IAM du projet peuvent être approfondis pour utiliser/accéder à des environnements spécifiques.

Profil environnemental

Sur Amazon DataZone, un profil d'environnement est un modèle que vous pouvez utiliser pour créer des environnements. Les profils d'environnement sont créés à l'aide de plans.

Avec les profils d'environnement, les administrateurs de domaine peuvent encapsuler des plans avec des paramètres préconfigurés, puis les travailleurs des données peuvent créer rapidement

un certain nombre de nouveaux environnements en sélectionnant les profils d'environnement existants et en spécifiant les noms des nouveaux environnements. Cela permet aux travailleurs des données de gérer efficacement leurs projets et leurs environnements tout en s'assurant qu'ils respectent les politiques de gouvernance des données appliquées par leurs administrateurs de domaine.

Plan

Un plan avec lequel l'environnement est créé définit les AWS outils et services (par exemple, AWS Glue ou Amazon Redshift) que les membres du projet auquel appartient l'environnement peuvent utiliser lorsqu'ils travaillent avec les actifs du catalogue Amazon DataZone .

Dans la version actuelle d'Amazon, DataZone les plans par défaut suivants sont pris en charge :

- Plan du lac de données
- Plan d'entrepôt de données
- Plan Amazon Sagemaker

Profil utilisateur

Un profil utilisateur représente DataZone les utilisateurs d'Amazon. Amazon DataZone prend en charge à la fois les rôles IAM et les identités SSO pour interagir avec Amazon DataZone Management Console et le portail de données à différentes fins. Les administrateurs de domaine utilisent les rôles IAM pour effectuer les tâches administratives initiales liées au domaine dans Amazon DataZone Management Console, notamment la création de nouveaux DataZone domaines Amazon, la configuration des types de formulaires de métadonnées et la mise en œuvre de politiques. Les travailleurs des données utilisent leur identité d'entreprise SSO via Identity Center pour se connecter à Amazon DataZone Data Portal et accéder aux projets auxquels ils sont membres.

Profil du groupe

Les profils de groupe représentent des groupes d' DataZone utilisateurs d'Amazon. Les groupes peuvent être créés manuellement ou mappés à des groupes Active Directory de clients professionnels. Sur Amazon DataZone, les groupes ont deux objectifs. Tout d'abord, un groupe peut être mappé à une équipe d'utilisateurs dans l'organigramme, réduisant ainsi le travail administratif du DataZone chef de projet Amazon lorsque de nouveaux employés rejoignent ou quittent une équipe. Ensuite, les administrateurs d'entreprise utilisent des groupes Active Directory pour gérer et mettre à jour les statuts des utilisateurs. Les administrateurs de DataZone domaine Amazon peuvent donc utiliser ces appartenances à des groupes pour mettre en œuvre les politiques de DataZone domaine Amazon.

Administrateur de domaine

Dans Amazon DataZone, le principal IAM qui crée un DataZone domaine Amazon est l'administrateur de domaine par défaut de ce domaine. Les administrateurs de domaine d'Amazon DataZone exécutent les fonctionnalités clés du domaine, notamment la création de domaines, l'affectation d'autres administrateurs de domaine, l'ajout de sources de données et de cibles d'abonnement, la création de projets et d'environnements et l'attribution de propriétaires de projets.

Editeur

Dans Amazon DataZone, les éditeurs publient des actifs dans le DataZone catalogue Amazon et peuvent modifier les métadonnées des actifs qu'ils publient. Si cette autorisation leur est accordée, les éditeurs peuvent approuver ou rejeter les demandes d'abonnement aux ressources qu'ils ont publiées dans le DataZone catalogue Amazon.

Subscriber

Dans Amazon DataZone, un abonné est un DataZone projet Amazon qui souhaite trouver, accéder et consommer des actifs du DataZone catalogue Amazon.

Compte AWS owner

Dans Amazon DataZone, Compte AWS les propriétaires créent des rôles, des politiques et des autorisations Comptes AWS qui permettent Comptes AWS de les associer à des DataZone domaines Amazon.

Quelles sont les nouveautés d'Amazon DataZone ?

Cette section décrit les nouvelles fonctionnalités et améliorations d'Amazon DataZone par date de sortie.

Rubriques

2024

Amazon DataZone lance l'intégration avec Amazon SageMaker

Publié le 05/06/2024

Amazon DataZone lance l'intégration avec Amazon SageMaker pour aider les producteurs de données et les consommateurs à passer facilement SageMaker à Amazon pour collaborer sur des projets d'apprentissage automatique (ML) tout en renforçant la gouvernance de l'accès aux données et aux actifs de machine learning. Grâce à la nouvelle intégration intégrée entre Amazon DataZone et Amazon SageMaker, les consommateurs et les producteurs de données peuvent rationaliser la gouvernance du machine learning lors de la configuration de l'infrastructure, collaborer sur des initiatives commerciales et gérer facilement les données et les actifs de machine learning. Pour plus d'informations, consultez Travailler avec les plans DataZone intégrés d'Amazon et Utilisation des comptes associés pour publier et consommer des données.

Amazon DataZone lance l'intégration avec AWS le mode d'accès hybride Lake Formation

Publié le 04/03/2024

Amazon DataZone a introduit une intégration avec AWS le mode d'accès hybride Lake Formation. Cette intégration vous permet de publier et de partager facilement vos tables AWS Glue via Amazon DataZone, sans avoir à les enregistrer au préalable dans AWS Lake Formation. Pour commencer, les administrateurs activent le paramètre d'enregistrement de la localisation des données dans le `DefaultDataLake` plan de la DataZone console Amazon. Ensuite, lorsqu'un consommateur de données s'abonne à une table AWS Glue gérée via des autorisations IAM, Amazon enregistre d' DataZone abord les emplacements Amazon S3 de cette table en mode hybride, puis accorde l'accès

au consommateur de données en gérant les autorisations sur la table via AWS Lake Formation. Cela garantit que les autorisations IAM disponibles continuent d'exister avec les autorisations AWS Lake Formation récemment accordées, sans perturber les flux de travail existants. Pour plus d'informations, consultez le DataZone Intégration d'Amazon au mode hybride de AWS Lake Formation .

Amazon DataZone lance l'intégration avec AWS Glue Data Quality

Publié le 04/03/2024

Amazon DataZone lance l'intégration avec AWS Glue Data Quality et propose des API pour intégrer les indicateurs de qualité des données issus de solutions de qualité des données tierces. La nouvelle intégration vous permet de publier automatiquement les scores de AWS Glue Data Quality dans le catalogue de données Amazon DataZone Business. DataZone Les API Amazon peuvent être utilisées pour ingérer des indicateurs de qualité provenant de sources tierces. Une fois publiées, les consommateurs de données peuvent facilement rechercher des actifs de données, consulter des indicateurs de qualité détaillés et identifier les contrôles et les règles défaillants, ce qui permet aux entreprises de prendre des décisions éclairées. Pour plus d'informations, consultez le Qualité des données sur Amazon DataZone.

Mise à disposition générale des recommandations relatives à l'IA pour les descriptions sur Amazon DataZone

Publié le 27/03/2024

Amazon DataZone a annoncé la mise à disposition générale de la nouvelle fonctionnalité générative basée sur l'IA afin d'améliorer la découverte des données, leur compréhension et leur utilisation en enrichissant le catalogue de données commerciales. En un seul clic, les producteurs de données peuvent générer des descriptions et un contexte complets des données commerciales, mettre en évidence les colonnes pertinentes et inclure des recommandations sur des cas d'utilisation analytiques. Le lancement ajoute la prise en charge des API que les producteurs de données peuvent utiliser pour générer par programmation des descriptions pour les actifs. Pour plus d'informations, consultez Utilisation de l'apprentissage automatique et de l'IA générative.

Amazon apporte DataZone des améliorations à l'intégration d'Amazon Redshift

Publié le 21/03/2024

Amazon DataZone a apporté plusieurs améliorations à son intégration avec Amazon Redshift, simplifiant le processus de publication et d'abonnement aux tables et aux vues Amazon Redshift. Ces mises à jour rationalisent l'expérience des producteurs de données et des consommateurs, en leur permettant de créer rapidement des environnements d'entrepôt de données à l'aide d'informations d'identification et de paramètres de connexion préconfigurés fournis par leurs DataZone administrateurs Amazon. En outre, ces améliorations permettent aux administrateurs de mieux contrôler qui peut utiliser les ressources de leurs AWS comptes et des clusters Amazon Redshift, et dans quel but.

- Configuration du plan : une fois que vous avez activé le `DefaultDataWarehouseBlueprint` plan, vous pouvez contrôler quels projets peuvent utiliser le `DefaultDataWarehouseBlueprint` plan dans votre compte pour créer des profils d'environnement en attribuant la gestion des projets au plan activé. Vous pouvez également créer des ensembles de paramètres en `DefaultDataWarehouseBlueprint` fournissant des paramètres tels que le cluster, la base de données et un AWS secret. Vous pouvez également créer des AWS secrets depuis la DataZone console Amazon.
- Profil d'environnement : lors de la création d'un profil d'environnement, vous pouvez choisir de fournir vos propres paramètres Amazon Redshift ou d'utiliser l'un des ensembles de paramètres de la configuration du plan. Si vous choisissez d'utiliser le jeu de paramètres créé dans la configuration du plan, le AWS secret ne nécessite qu'une `AmazonDataZoneDomain` balise (la `AmazonDataZoneProject` balise n'est requise que si vous choisissez de fournir vos propres ensembles de paramètres dans le profil d'environnement). Dans le profil d'environnement, vous pouvez spécifier une liste de projets autorisés. Seuls les projets autorisés peuvent utiliser ce profil d'environnement pour créer des environnements d'entrepôt de données. Vous pouvez également spécifier les données que les projets autorisés sont autorisés à publier. Actuellement, vous pouvez choisir l'une des options suivantes : 1) Publier à partir de n'importe quel schéma, 2) Publier à partir du schéma d'environnement par défaut, 3) Ne pas autoriser la publication.
- Environnement : les producteurs ou les consommateurs de données peuvent désormais sélectionner un profil d'environnement pour créer des environnements, sans avoir à fournir leurs propres paramètres Amazon Redshift, notamment AWS Secret, cluster, groupe de travail et base de données. Ces paramètres sont transférés vers l'environnement à partir du profil d'environnement. Parallèlement à la création de l'environnement, Amazon crée DataZone désormais également un schéma par défaut pour l'environnement. Les membres du projet ont un accès en lecture et en écriture à ce schéma et peuvent facilement publier les tables créées dans ce schéma dans le catalogue en exécutant la source de données par défaut créée dans le cadre de la création de l'environnement. Les paramètres Amazon Redshift utilisés pour créer

un environnement peuvent également être utilisés pour créer de nouvelles sources de données (au lieu que le producteur de données fournisse ses propres paramètres lors de la création de la source de données).

AWS Support à la formation dans le cloud pour Amazon DataZone

Publié le 18/01/2024

Les utilisateurs d'Amazon DataZone peuvent désormais en tirer parti AWS CloudFormation pour modéliser et gérer efficacement une suite de DataZone ressources Amazon. Cette approche facilite le provisionnement cohérent des ressources, tout en permettant la gestion du cycle de vie par le biais de pratiques liées à l'infrastructure en tant que code. Grâce aux modèles personnalisés, vous pouvez définir avec précision les ressources dont vous avez besoin et leurs interdépendances. Pour plus d'informations, consultez la référence DataZone des types de ressources Amazon.

Ajoutez des responsables IAM directement en tant que membres de projets Amazon DataZone

Publié le 01/05/2024

Vous pouvez désormais ajouter des responsables IAM en tant que membres du projet, même s'ils ne se sont pas encore connectés à Amazon DataZone (exigence précédente). Une fois qu'un administrateur de domaine ou un administrateur informatique a ajouté `iam:GetUser` et `iam:GetRole` au rôle d'exécution du domaine, les propriétaires de projet peuvent ajouter les principaux IAM en tant que membres en fournissant simplement le nom de ressource Amazon (ARN) du rôle IAM ou de l'utilisateur IAM. Le principal IAM doit toujours disposer des autorisations IAM requises pour accéder à Amazon DataZone et celles-ci peuvent être configurées dans la console IAM. Pour plus d'informations, consultez Ajouter des membres à un projet.

Support pour les types d'actifs personnalisés depuis le portail de données

Publié le 01/05/2024

La prise en charge des actifs personnalisés permet DataZone à Amazon de cataloguer les actifs via le portail de données pour les données non structurées, notamment les tableaux de bord, les requêtes et les modèles, ce qui vous permet d'ajouter plus facilement des actifs personnalisés directement dans le portail de données, en plus du support d'API précédemment disponible. La possibilité de créer, de mettre à jour et de publier des ressources personnalisées sur Amazon

DataZone vous permet de partager, de rechercher, de vous abonner à tout type d'actif et de créer un flux de travail qui assure la gouvernance de ces actifs. Pour plus d'informations, consultez Création de types d'actifs personnalisés.

2023

Supprimer le domaine

Publié le 27/12/2023

Il s'agit d'une fonctionnalité qui vous permet de supprimer plus facilement vos domaines. Vous pouvez désormais procéder à la suppression du domaine même s'il n'est pas vide (car il contient des projets, des environnements, des actifs, des sources de données, etc.). Pour plus d'informations, consultez Supprimer des domaines.

Mode hybride

Publié le 22/12/2023

Amazon DataZone a ajouté la prise en charge du mode hybride AWS Lake Formation. Grâce à ce support, si vous publiez une table AWS Glue sur Amazon DataZone dont l'emplacement AWS S3 est enregistré dans Lake Formation en mode hybride, Amazon DataZone traite cette table comme un actif géré et peut gérer les subventions d'abonnement à cette table. Avant la sortie de cette fonctionnalité, Amazon DataZone traitait ce tableau comme un actif non géré, c'est-à-dire DataZone qu'Amazon ne serait pas en mesure d'accorder des abonnements à ce tableau. Pour plus d'informations, consultez Configurer les autorisations de Lake Formation pour Amazon DataZone.

Éligibilité HIPAA

Publié le 14/12/2023

Amazon DataZone est désormais conforme à la loi américaine HIPAA (Health Insurance Portability and Accountability Act) de 1996. Pour consulter la liste des AWS services conformes à la loi HIPAA, consultez https://aws.amazon.com/compliance/ hipaa-eligible-services-reference/.

Recommandations de l'IA pour les descriptions dans Amazon DataZone (version préliminaire)

Publié le 28/11/2023

AWS annonce la prévisualisation d'une nouvelle fonctionnalité générative basée sur l'IA dans Amazon DataZone afin d'améliorer la découverte des données, leur compréhension et leur utilisation en enrichissant le catalogue de données commerciales. En un seul clic, les producteurs de données peuvent générer des descriptions et un contexte complets des données commerciales, mettre en évidence les colonnes pertinentes et inclure des recommandations sur des cas d'utilisation analytiques. Grâce aux recommandations de l'IA pour les descriptions sur Amazon DataZone, les consommateurs de données peuvent identifier les tables de données et les colonnes nécessaires à l'analyse, ce qui améliore la découvrabilité des données et réduit les back-and-forth communications avec les producteurs de données. La version préliminaire est disponible dans DataZone les domaines Amazon fournis dans les AWS régions suivantes : USA Est (Virginie du Nord), USA Ouest (Oregon). Pour plus d'informations, consultez Utilisation de l'apprentissage automatique et de l'IA générative.

DefaultDataLake amélioration du plan

Publié le 20/11/2023

Amazon DataZone a ajouté une amélioration au DefaultDataLake plan qui vous permet de mieux contrôler qui peut publier quelles données depuis votre AWS compte. Deux modifications majeures ont été introduites avec le lancement de cette fonctionnalité.

- Dans la console, une fois que vous avez activé le DefaultDataLake plan, vous pouvez contrôler quels projets peuvent utiliser le DefaultDataLake plan dans votre compte pour créer des profils d'environnement en attribuant la gestion des projets au plan activé.
- Le deuxième changement concerne le portail. Si vous créez un profil d'environnement à l'aide du DefaultDataLake plan, vous pouvez également sélectionner les projets autorisés autorisés à utiliser le profil d'environnement pour créer des environnements. Par défaut, tous les projets sont autorisés à utiliser le profil d'environnement du lac de données, mais vous pouvez restreindre le profil d'environnement à des projets spécifiques et également contrôler les données qui peuvent être publiées à l'aide des environnements créés avec le profil.

Pour plus d'informations, voir Création d'un profil d'environnement.

Configuration

Pour configurer Amazon DataZone, vous devez disposer d'un AWS compte et configurer les politiques et autorisations IAM requises pour Amazon DataZone.

Une fois que vous avez configuré vos DataZone autorisations Amazon, il est recommandé de suivre les étapes de la section Getting started qui vous explique comment créer le DataZone domaine Amazon, obtenir l'URL du portail de données et les DataZone flux de travail Amazon de base pour les producteurs et les consommateurs de données.

Rubriques

Créez un AWS compte

Si vous n'avez pas de AWS compte, procédez comme suit pour en créer un.

Si vous avez une AWS organisation, créez un compte :

1. Connectez-vous à la console de AWS gestion et ouvrez la console Organizations à l'adresse https://console.aws.amazon.com/organizations/.
2. Dans le volet de navigation, sélectionnez AWS Accounts.
3. Choisissez Ajouter un AWS compte.
4. Choisissez Créer un AWS compte et fournissez les informations demandées. Choisissez Créer un AWS compte.

Pour créer un AWS compte

1. Ouvrez https://portal.aws.amazon.com/billing/signup
2. Suivez les instructions en ligne.

   Dans le cadre de la procédure d'inscription, vous recevrez un appel téléphonique et vous saisirez un code de vérification en utilisant le clavier numérique du téléphone.

Lorsque vous créez un AWS compte, un AWS utilisateur root est créé. L'utilisateur root a accès à tous les AWS services et ressources du compte. La meilleure pratique de sécurité consiste à attribuer un accès administratif à un utilisateur administratif, et à utiliser uniquement l'utilisateur racine pour effectuer les tâches nécessitant un accès utilisateur racine.

Configurer les autorisations IAM requises pour utiliser la console de DataZone gestion Amazon

Tout utilisateur, groupe ou rôle qui souhaite utiliser la console DataZone de gestion Amazon doit disposer des autorisations requises.

Rubriques

- Associer des politiques obligatoires et facultatives à un utilisateur, un groupe ou un rôle pour accéder à DataZone la console Amazon
- Créez une politique personnalisée pour les autorisations IAM afin de permettre à la console de DataZone service Amazon de simplifier la création de rôles
- Créez une politique personnalisée pour les autorisations nécessaires à la gestion d'un compte associé à un DataZone domaine Amazon
- (Facultatif) Créez une politique personnalisée pour les autorisations AWS Identity Center afin d'activer l'authentification unique (SSO) pour votre domaine
- (Facultatif) Créez une politique personnalisée pour les autorisations AWS d'Identity Center afin d'ajouter et de supprimer l'accès des utilisateurs SSO et des groupes SSO à votre domaine Amazon DataZone .
- (Facultatif) Ajoutez votre principal IAM en tant qu'utilisateur clé pour créer votre DataZone domaine Amazon à l'aide d'une clé gérée par le client à partir du AWS Key Management Service (KMS)

Associer des politiques obligatoires et facultatives à un utilisateur, un groupe ou un rôle pour accéder à DataZone la console Amazon

Procédez comme suit pour associer les politiques personnalisées obligatoires et facultatives à un utilisateur, un groupe ou un rôle. Pour plus d'informations, consultez AWS politiques gérées pour Amazon DataZone.

1. Connectez-vous à la console de AWS gestion et ouvrez la console IAM à l'adresse https://console.aws.amazon.com/iam/.
2. Dans le panneau de navigation, choisissez Politiques.
3. Choisissez les politiques suivantes à associer à votre utilisateur, à votre groupe ou à un rôle.

   - Dans la liste des politiques, cochez la case à côté de AmazonDataZoneFullAccess. Vous pouvez utiliser le menu Filtre et la zone de recherche pour filtrer la liste de politiques. Pour plus d'informations, consultez AWS politique gérée : AmazonDataZoneFullAccess.
   - (Facultatif) Créez une politique personnalisée pour les autorisations IAM afin de permettre à la console de DataZone service Amazon de simplifier la création de rôles.
   - (Facultatif) Créez une politique personnalisée pour les autorisations AWS Identity Center afin d'activer l'authentification unique (SSO) pour votre domaine.
   - (Facultatif) Créez une politique personnalisée pour les autorisations AWS d'Identity Center afin d'ajouter et de supprimer l'accès des utilisateurs SSO et des groupes SSO à votre domaine Amazon DataZone .
4. Sélectionnez Actions, puis Attach (Attacher).
5. Choisissez l'utilisateur, le groupe ou le rôle auquel vous souhaitez associer la politique. Vous pouvez utiliser le menu Filtre et la zone de recherche pour filtrer la liste des entités du principal. Après avoir choisi l'utilisateur, le groupe ou le rôle, choisissez Attacher une politique.

Créez une politique personnalisée pour les autorisations IAM afin de permettre à la console de DataZone service Amazon de simplifier la création de rôles

Suivez la procédure suivante pour créer une politique en ligne personnalisée afin de disposer des autorisations nécessaires pour permettre DataZone à Amazon de créer les rôles nécessaires dans la console AWS de gestion en votre nom.

1. Connectez-vous à la console de AWS gestion et ouvrez la console IAM à l'adresse https://console.aws.amazon.com/iam/.
2. Dans le volet de navigation, choisissez Utilisateurs ou Groupes d'utilisateurs.
3. Dans la liste, sélectionnez le nom de l'utilisateur ou du groupe auquel intégrer une politique.
4. Sélectionnez l'onglet Autorisations et, si nécessaire, développez la section Politiques d'autorisations.

5. Choisissez Ajouter des autorisations et Créer un lien de politique intégré.
6. Sur l'écran Create Policy, dans la section Policy editor, sélectionnez JSON.

   Créez un document de politique avec les instructions JSON suivantes, puis choisissez Next.

```
{
    "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. Sur l'écran Révision de la politique, entrez le nom de la politique. Lorsque vous êtes satisfait de la politique, sélectionnez Create policy (Créer une politique). Assurez-vous qu'aucune erreur ne s'affiche dans un cadre rouge en haut de l'écran. Corrigez les erreurs signalées.

Créez une politique personnalisée pour les autorisations nécessaires à la gestion d'un compte associé à un DataZone domaine Amazon

Suivez la procédure ci-dessous pour créer une politique en ligne personnalisée afin de disposer des autorisations nécessaires dans un AWS compte associé pour répertorier, accepter et rejeter les partages de ressources d'un domaine, puis activer, configurer et désactiver les plans d'environnement dans le compte associé. Pour activer la création de rôles simplifiée optionnelle sur la console de DataZone service Amazon disponible lors de la configuration du Blueprint, vous devez égalementCréez une politique personnalisée pour les autorisations IAM afin de permettre à la console de DataZone service Amazon de simplifier la création de rôles .

1. Connectez-vous à la console de AWS gestion et ouvrez la console IAM à l'adresse https://console.aws.amazon.com/iam/.
2. Dans le volet de navigation, choisissez Utilisateurs ou Groupes d'utilisateurs.
3. Dans la liste, sélectionnez le nom de l'utilisateur ou du groupe auquel intégrer une politique.
4. Sélectionnez l'onglet Autorisations et, si nécessaire, développez la section Politiques d'autorisations.
5. Choisissez Ajouter des autorisations et Créer un lien de politique intégré.
6. Sur l'écran Create Policy, dans la section Policy editor, sélectionnez JSON. Créez un document de politique avec les instructions JSON suivantes, puis choisissez Next.

```
{
    "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. Sur l'écran Révision de la politique, entrez le nom de la politique. Lorsque vous êtes satisfait de la politique, sélectionnez Create policy (Créer une politique). Assurez-vous qu'aucune erreur ne s'affiche dans un cadre rouge en haut de l'écran. Corrigez les erreurs signalées.

(Facultatif) Créez une politique personnalisée pour les autorisations AWS Identity Center afin d'activer l'authentification unique (SSO) pour votre domaine

Suivez la procédure suivante pour créer une politique en ligne personnalisée afin de disposer des autorisations nécessaires pour activer l'authentification unique (SSO) à l'aide du AWS IAM Identity Center d'Amazon. DataZone

1. Connectez-vous à la console de AWS gestion et ouvrez la console IAM à l'adresse https://console.aws.amazon.com/iam/.

2. Dans le volet de navigation, choisissez Utilisateurs ou Groupes d'utilisateurs.
3. Dans la liste, sélectionnez le nom de l'utilisateur ou du groupe auquel intégrer une politique.
4. Sélectionnez l'onglet Autorisations et, si nécessaire, développez la section Politiques d'autorisations.
5. Choisissez Ajouter des autorisations et Créer une politique intégrée.
6. Sur l'écran Create Policy, dans la section Policy editor, sélectionnez JSON.

   Créez un document de politique avec les instructions JSON suivantes, puis choisissez Next.

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

7. Sur l'écran Révision de la politique, entrez le nom de la politique. Lorsque vous êtes satisfait de la politique, sélectionnez Create policy (Créer une politique). Assurez-vous qu'aucune erreur ne s'affiche dans un cadre rouge en haut de l'écran. Corrigez les erreurs signalées.

(Facultatif) Créez une politique personnalisée pour les autorisations AWS d'Identity Center afin d'ajouter et de supprimer l'accès des utilisateurs SSO et des groupes SSO à votre domaine Amazon DataZone .

Suivez la procédure ci-dessous pour créer une politique en ligne personnalisée afin de disposer des autorisations nécessaires pour ajouter et supprimer l'accès d'un utilisateur SSO et d'un groupe SSO à votre domaine Amazon. DataZone

1. Connectez-vous à la console de AWS gestion et ouvrez la console IAM à l'adresse https://console.aws.amazon.com/iam/.
2. Dans le volet de navigation, choisissez Utilisateurs ou Groupes d'utilisateurs.
3. Dans la liste, sélectionnez le nom de l'utilisateur ou du groupe auquel intégrer une politique.
4. Sélectionnez l'onglet Autorisations et, si nécessaire, développez la section Politiques d'autorisations.
5. Choisissez Ajouter des autorisations et Créer une politique intégrée.
6. Sur l'écran Create Policy, dans la section Policy editor, sélectionnez JSON.

   Créez un document de politique avec les instructions JSON suivantes, puis choisissez Next.

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

7. Sur l'écran Révision de la politique, entrez le nom de la politique. Lorsque vous êtes satisfait de la politique, sélectionnez Create policy (Créer une politique). Assurez-vous qu'aucune erreur ne s'affiche dans un cadre rouge en haut de l'écran. Corrigez les erreurs signalées.

(Facultatif) Ajoutez votre principal IAM en tant qu'utilisateur clé pour créer votre DataZone domaine Amazon à l'aide d'une clé gérée par le client à partir du AWS Key Management Service (KMS)

Avant de pouvoir éventuellement créer votre DataZone domaine Amazon avec une clé gérée par le client (CMK) à partir du service de gestion des AWS clés (KMS), suivez la procédure suivante pour faire de votre principal IAM un utilisateur de votre clé KMS.

1. Connectez-vous à la console de AWS gestion et ouvrez la console KMS à l'adresse https://console.aws.amazon.com/kms/.
2. Pour afficher les clés de votre compte que vous créez et gérez vous-même, dans le volet de navigation, choisissez Clés gérées par le client.
3. Dans la liste des clés KMS, choisissez l'alias ou l'ID de clé de la clé KMS que vous souhaitez examiner.
4. Pour ajouter ou supprimer des utilisateurs clés, et pour autoriser ou interdire à AWS des comptes externes d'utiliser la clé KMS, utilisez les commandes de la section Utilisateurs clés de la page. Les utilisateurs de clé peuvent utiliser la clé KMS dans les opérations de chiffrement, telles que le chiffrement, le déchiffrement, le rechiffrement et la génération de clés de données.

Configurer les autorisations IAM requises pour utiliser le portail de DataZone données Amazon

Tout utilisateur, groupe ou rôle qui souhaite utiliser le portail de DataZone données ou le catalogue Amazon doit disposer des autorisations requises.

Rubriques

- Associer la politique requise à un utilisateur, un groupe ou un rôle pour accéder au portail de DataZone données Amazon
- Associer la politique requise à un utilisateur, un groupe ou un rôle pour accéder au DataZone catalogue Amazon
- Associez une politique facultative à un utilisateur, un groupe ou un rôle pour accéder au portail de DataZone données ou au catalogue Amazon si votre domaine est chiffré à l'aide d'une clé gérée par le client par le service de gestion des AWS clés (KMS)

Associer la politique requise à un utilisateur, un groupe ou un rôle pour accéder au portail de DataZone données Amazon

Vous pouvez accéder au portail de DataZone données Amazon en utilisant vos AWS informations d'identification ou vos informations d'identification unique (SSO). Suivez les instructions de la section ci-dessous pour configurer les autorisations requises pour accéder au portail de données avec vos AWS informations d'identification. Pour plus d'informations sur l'utilisation d'Amazon DataZone avec SSO, consultezConfiguration de l' AWS IAM Identity Center pour Amazon DataZone.

> **Note**
>
> Seuls les principaux IAM du AWS compte de votre domaine peuvent accéder au portail de données du domaine. Les principaux IAM d'autres AWS comptes ne peuvent pas accéder au portail de données du domaine.

Procédez comme suit pour associer la politique requise à un utilisateur, un groupe ou un rôle. Pour plus d'informations, consultez AWS politiques gérées pour Amazon DataZone.

1. Connectez-vous à la console de AWS gestion et ouvrez la console IAM à l'adresse https://console.aws.amazon.com/iam/.
2. Dans le volet de navigation, sélectionnez Utilisateurs, Groupes d'utilisateurs ou Rôles.
3. Dans la liste, choisissez le nom de l'utilisateur, du groupe ou du rôle dans lequel vous souhaitez intégrer une politique.
4. Sélectionnez l'onglet Autorisations et, si nécessaire, développez la section Politiques d'autorisations.
5. Choisissez Ajouter des autorisations et Créer un lien de politique intégré.
6. Sur l'écran Create Policy, dans la section Policy editor, sélectionnez JSON. Créez un document de politique avec les instructions JSON suivantes, puis choisissez Next.

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

```
                "datazone:GetIamPortalLoginUrl"
            ],
            "Resource": [
                "*"
            ]
        }
    ]
}
```

7. Sur l'écran Révision de la politique, entrez le nom de la politique. Lorsque vous êtes satisfait de la politique, sélectionnez Create policy (Créer une politique). Assurez-vous qu'aucune erreur ne s'affiche dans un cadre rouge en haut de l'écran. Corrigez les erreurs signalées.

Associer la politique requise à un utilisateur, un groupe ou un rôle pour accéder au DataZone catalogue Amazon

> **Note**
>
> Seuls les principaux IAM du AWS compte de votre domaine peuvent accéder au catalogue du domaine. Les principaux IAM d'autres AWS comptes ne peuvent pas accéder au catalogue du domaine.

Vous pouvez accorder à vos identités IAM l'accès au catalogue de votre DataZone domaine Amazon via l'API et le SDK en suivant la procédure suivante. Si vous souhaitez que ces identités IAM aient également accès au portail de DataZone données Amazon, suivez également la procédure ci-dessus pourAssocier la politique requise à un utilisateur, un groupe ou un rôle pour accéder au portail de DataZone données Amazon. Pour plus d'informations, consultez AWS politiques gérées pour Amazon DataZone.

1. Connectez-vous à la console de AWS gestion et ouvrez la console IAM à l'adresse https://console.aws.amazon.com/iam/.
2. Dans le panneau de navigation, choisissez Politiques.
3. Dans la liste des politiques, sélectionnez le bouton radio situé à côté de la AmazonDataZoneFullUserAccesspolitique. Vous pouvez utiliser le menu Filtre et la zone de recherche pour filtrer la liste de politiques. Pour plus d'informations, consultez AWS politique gérée : AmazonDataZoneFullUserAccess.

4. Sélectionnez Actions, puis Attach (Attacher).
5. Choisissez l'utilisateur, le groupe ou le rôle auquel vous souhaitez associer la politique en cochant la case à côté de chaque principal. Vous pouvez utiliser le menu Filtre et la zone de recherche pour filtrer la liste des entités du principal. Après avoir choisi l'utilisateur, le groupe ou le rôle, choisissez Attacher une politique.

Associez une politique facultative à un utilisateur, un groupe ou un rôle pour accéder au portail de DataZone données ou au catalogue Amazon si votre domaine est chiffré à l'aide d'une clé gérée par le client par le service de gestion des AWS clés (KMS)

Si vous créez votre DataZone domaine Amazon avec votre propre clé KMS pour le chiffrement des données, vous devez également créer une politique intégrée avec les autorisations suivantes et l'associer à vos principaux IAM afin qu'ils puissent accéder au portail de DataZone données ou au catalogue Amazon.

1. Connectez-vous à la console de AWS gestion et ouvrez la console IAM à l'adresse https://console.aws.amazon.com/iam/.
2. Dans le volet de navigation, sélectionnez Utilisateurs, Groupes d'utilisateurs ou Rôles.
3. Dans la liste, choisissez le nom de l'utilisateur, du groupe ou du rôle dans lequel vous souhaitez intégrer une politique.
4. Sélectionnez l'onglet Autorisations et, si nécessaire, développez la section Politiques d'autorisations.
5. Choisissez Ajouter des autorisations et Créer un lien de politique intégré.
6. Sur l'écran Create Policy, dans la section Policy editor, sélectionnez JSON. Créez un document de politique avec les instructions JSON suivantes, puis choisissez Next.

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

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

7. Sur l'écran Révision de la politique, entrez le nom de la politique. Lorsque vous êtes satisfait de la politique, sélectionnez Create policy (Créer une politique). Assurez-vous qu'aucune erreur ne s'affiche dans un cadre rouge en haut de l'écran. Corrigez les erreurs signalées.

Configuration de l' AWS IAM Identity Center pour Amazon DataZone

> **Note**
>
> AWS Identity Center doit être activé dans la même AWS région que votre DataZone domaine Amazon. Actuellement, AWS Identity Center ne peut être activé que dans une seule AWS région.

Vous pouvez accéder au portail de DataZone données Amazon en utilisant vos informations d'identification unique (SSO) ou AWS vos informations d'identification. Suivez les instructions de cette section pour configurer AWS IAM Identity Center pour Amazon DataZone. Pour plus d'informations sur l'utilisation d'Amazon DataZone avec vos AWS informations d'identification, consultezConfigurer les autorisations IAM requises pour utiliser la console de DataZone gestion Amazon.

Vous pouvez ignorer les procédures décrites dans cette section si AWS IAM Identity Center (successeur de Single Sign-On) est déjà activé et configuré dans la AWS région où vous souhaitez créer votre domaine Amazon DataZone . AWS

Procédez comme suit pour activer AWS IAM Identity Center (successeur de Single Sign-On). AWS

1. Pour activer AWS IAM Identity Center, vous devez vous connecter à la console de AWS gestion à l'aide des informations d'identification de votre compte de gestion AWS Organizations. Vous ne pouvez pas activer IAM Identity Center lorsque vous êtes connecté avec les informations d'identification d'un compte membre d' AWS Organizations. Pour plus d'informations, consultez

la section Création et gestion d'une organisation dans le Guide de l'utilisateur AWS des Organizations.

2. Ouvrez la console AWS IAM Identity Center (qui a succédé à AWS Single Sign-On) et utilisez le sélecteur de région dans la barre de navigation supérieure pour choisir la AWS région dans laquelle vous souhaitez créer votre domaine Amazon. DataZone
3. Sélectionnez Activer.
4. Choisissez votre source d'identité.

   Par défaut, vous disposez d'un magasin IAM Identity Center pour une gestion rapide et facile des utilisateurs. Vous pouvez éventuellement connecter un fournisseur d'identité externe à la place. Dans cette procédure, nous utilisons le magasin IAM Identity Center par défaut.

   Pour plus d'informations, voir Choisir votre source d'identité.
5. Dans le volet de navigation d'IAM Identity Center, choisissez Groups, puis Create group. Entrez le nom du groupe et choisissez Create.
6. Dans le volet de navigation d'IAM Identity Center, sélectionnez Users.
7. Sur l'écran Ajouter un utilisateur, entrez les informations requises et choisissez Envoyer un e-mail à l'utilisateur avec les instructions de configuration du mot de passe. L'utilisateur doit recevoir un e-mail concernant les prochaines étapes de configuration.
8. Choisissez Suivant : Groupes, choisissez le groupe de votre choix, puis choisissez Ajouter un utilisateur. Les utilisateurs devraient recevoir un e-mail les invitant à utiliser le SSO. Dans cet e-mail, ils doivent choisir Accepter l'invitation et définir le mot de passe.

Après avoir créé votre DataZone domaine Amazon, vous pouvez activer AWS Identity Center pour Amazon DataZone et donner accès à vos utilisateurs et groupes SSO. Pour plus d'informations, voir Activer IAM Identity Center pour Amazon DataZone.

Mise en route

Les informations contenues dans cette section vous aideront à commencer à utiliser Amazon DataZone. Si vous utilisez Amazon pour la première DataZone fois, commencez par vous familiariser avec les concepts et la terminologie présentés dans DataZone Terminologie et concepts d'Amazon.

Cette section de mise en route vous présente les flux de travail Amazon DataZone Quickstart suivants :

Rubriques

- Amazon DataZone Quickstart avec les données AWS Glue
- Amazon DataZone QuickStart avec les données Amazon Redshift
- Amazon DataZone QuickStart avec des exemples de scripts

> **Important**
>
> Avant de commencer les étapes de l'un ou l'autre de ces flux de travail de démarrage rapide, vous devez suivre les procédures décrites dans la section Configuration de ce guide. Si vous utilisez un tout nouveau AWS compte, vous devez configurer les autorisations requises pour utiliser la console DataZone de gestion Amazon. Si vous utilisez un AWS compte qui possède des objets AWS Glue Data Catalog existants, vous devez également configurer les autorisations Lake Formation pour Amazon DataZone.

Amazon DataZone Quickstart avec les données AWS Glue

Rubriques

- Étape 1 - Création du DataZone domaine Amazon et du portail de données
- Étape 2 - Création du projet de publication
- Étape 3 - Création de l'environnement
- Étape 4 - Produire des données pour publication
- Étape 5 - Collectez les métadonnées à partir de AWS Glue
- Étape 6 - Organiser et publier la ressource de données
- Étape 7 - Création du projet pour l'analyse des données

- Étape 8 - Création d'un environnement pour l'analyse des données
- Étape 9 - Rechercher dans le catalogue de données et s'abonner aux données
- Étape 10 - Approuver la demande d'abonnement
- Étape 11 - Création d'une requête et analyse des données dans Amazon Athena

Étape 1 - Création du DataZone domaine Amazon et du portail de données

Cette section décrit les étapes de création d'un DataZone domaine Amazon et d'un portail de données pour ce flux de travail.

Suivez la procédure ci-dessous pour créer un DataZone domaine Amazon. Pour plus d'informations sur DataZone les domaines Amazon, consultez DataZone Terminologie et concepts d'Amazon.

1. Accédez à la DataZone console Amazon à l'adresse https://console.aws.amazon.com/datazone, connectez-vous, puis choisissez Create domain.

   > **Note**
   >
   > Si vous souhaitez utiliser un DataZone domaine Amazon existant pour ce flux de travail, choisissez Afficher les domaines, puis choisissez le domaine que vous souhaitez utiliser, puis passez à l'étape 2 de création d'un projet de publication.

2. Sur la page Créer un domaine, entrez des valeurs pour les champs suivants :

   - Nom : spécifiez le nom de votre domaine. Dans le cadre de ce flux de travail, vous pouvez appeler ce domaine Marketing.
   - Description : spécifiez une description de domaine facultative.
   - Chiffrement des données : vos données sont cryptées par défaut à l'aide d'une clé qui vous AWS appartient et qui est gérée pour vous. Dans ce cas d'utilisation, vous pouvez conserver les paramètres de chiffrement des données par défaut.

     Pour plus d'informations sur l'utilisation des clés gérées par le client, consultezLe chiffrement des données est au repos pour Amazon DataZone. Si vous utilisez votre propre clé KMS pour le chiffrement des données, vous devez inclure l'instruction suivante dans votre clé par défautAmazonDataZoneDomainExecutionRole.

     ```
     {
     ```

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

- Accès au service : laissez inchangée l'option Utiliser un rôle par défaut sélectionnée par défaut.

> **Note**
>
> Si vous utilisez un DataZone domaine Amazon existant pour ce flux de travail, vous pouvez choisir l'option Utiliser un rôle de service existant, puis choisir un rôle existant dans le menu déroulant.

- Sous Configuration rapide, choisissez Configurer ce compte pour la consommation et la publication de données. Cette option active les DataZone plans Amazon intégrés du lac de données et de l'entrepôt de données, et configure les autorisations, les ressources, un projet par défaut et les profils d'environnement de lac de données et d'entrepôt de données par défaut pour ce compte. Pour plus d'informations sur les DataZone plans Amazon, consultez DataZone Terminologie et concepts d'Amazon.
- Conservez les champs restants sous Détails des autorisations inchangés.

> **Note**
>
> Si vous possédez déjà un DataZone domaine Amazon, vous pouvez choisir l'option Utiliser un rôle de service existant, puis choisir un rôle existant dans le menu déroulant pour le rôle Glue Manage Access, le rôle Redshift Manage Access et le rôle Provisioning.

- Ne modifiez pas les champs situés sous Tags.
- Choisissez Create domain (Créer un domaine).

3. Une fois le domaine créé avec succès, choisissez-le et, sur la page de résumé du domaine, notez l'URL du portail de données pour ce domaine. Vous pouvez utiliser cette URL pour accéder à votre portail de DataZone données Amazon afin d'effectuer les autres étapes de ce flux de travail. Vous pouvez également accéder au portail de données en choisissant Portail de données ouvertes.

> **Note**
>
> Dans la version actuelle d'Amazon DataZone, une fois le domaine créé, l'URL générée pour le portail de données ne peut pas être modifiée.

La création d'un domaine peut prendre plusieurs minutes. Attendez que le statut du domaine soit défini sur Disponible avant de passer à l'étape suivante.

Étape 2 - Création du projet de publication

Cette section décrit les étapes requises pour créer le projet de publication pour ce flux de travail.

1. Une fois que vous aurez terminé l'étape 1 ci-dessus et créé un domaine, vous verrez le message Welcome to Amazon DataZone ! fenêtre. Dans cette fenêtre, choisissez Créer un projet.
2. Spécifiez le nom du projet, par exemple, pour ce flux de travail SalesDataPublishingProject, vous pouvez le nommer, puis laisser les autres champs inchangés, puis choisir Créer.

Étape 3 - Création de l'environnement

Cette section décrit les étapes requises pour créer un environnement pour ce flux de travail.

1. Une fois que vous avez terminé l'étape 2 ci-dessus et créé votre projet, vous verrez la fenêtre Votre projet est prêt à être utilisé. Dans cette fenêtre, choisissez Create environment.
2. Sur la page Créer un environnement, spécifiez ce qui suit, puis choisissez Créer un environnement.
3. Spécifiez les valeurs suivantes :

   - Nom : spécifiez le nom de l'environnement. Pour cette procédure pas à pas, vous pouvez l'`Default data lake environment`appeler.
   - Description : spécifiez une description de l'environnement.

- Profil d'environnement : choisissez le profil d'DataLakeProfileenvironnement. Cela vous permet d'utiliser Amazon DataZone dans ce flux de travail pour travailler avec des données dans Amazon S3, AWS Glue Catalog et Amazon Athena.
- Pour cette procédure pas à pas, conservez les autres champs inchangés.

4. Choisissez Create environment.

Étape 4 - Produire des données pour publication

Cette section décrit les étapes requises pour produire des données destinées à être publiées dans ce flux de travail.

1. Une fois que vous avez terminé l'étape 3 ci-dessus, dans votre `SalesDataPublishingProject` projet, dans le panneau de droite, sous Outils d'analyse, sélectionnez Amazon Athena. Cela ouvre l'éditeur de requêtes Athena en utilisant les informations d'identification de votre projet pour l'authentification. Assurez-vous que votre environnement de publication est sélectionné dans le menu déroulant de DataZone l'environnement Amazon et que la `<environment_name>%_pub_db` base de données est sélectionnée comme dans l'éditeur de requêtes.
2. Pour cette procédure pas à pas, vous utilisez le script de requête Create Table as Select (CTAS) pour créer une nouvelle table que vous souhaitez publier sur Amazon. DataZone Dans votre éditeur de requêtes, exécutez ce script CTAS pour créer une `mkt_sls_table` table que vous pouvez publier et rendre disponible pour la recherche et l'abonnement.

```
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
```

Assurez-vous que la table mkt_sls_table est correctement créée dans la section Tables et vues sur le côté gauche. Vous disposez désormais d'un actif de données qui peut être publié dans le DataZone catalogue Amazon.

Étape 5 - Collectez les métadonnées à partir de AWS Glue

Cette section décrit l'étape de collecte des métadonnées à partir de AWS Glue pour ce flux de travail.

1. Une fois que vous avez terminé l'étape 4 ci-dessus, dans le portail de DataZone données Amazon, choisissez le `SalesDataPublishingProject` projet, puis choisissez l'onglet Données, puis choisissez Sources de données dans le panneau de gauche.
2. Choisissez la source créée dans le cadre du processus de création de l'environnement.
3. Choisissez Exécuter à côté du menu déroulant Action, puis cliquez sur le bouton d'actualisation. Une fois l'exécution de la source de données terminée, les actifs sont ajoutés à l' DataZone inventaire Amazon.

Étape 6 - Organiser et publier la ressource de données

Cette section décrit les étapes de conservation et de publication de la ressource de données dans ce flux de travail.

1. Une fois que vous avez terminé l'étape 5 ci-dessus, dans le portail de DataZone données Amazon, choisissez le `SalesDataPublishingProject` projet que vous avez créé à l'étape précédente, choisissez l'onglet Données, choisissez Données d'inventaire dans le panneau de gauche et recherchez le `mkt_sls_table` tableau.
2. Ouvrez la page de détails de l'`mkt_sls_table`actif pour voir les noms commerciaux générés automatiquement. Cliquez sur l'icône de métadonnées générées automatiquement pour afficher les noms générés automatiquement pour les actifs et les colonnes. Vous pouvez accepter ou rejeter chaque nom individuellement ou choisir Accepter tout pour appliquer les noms générés. Vous pouvez également éventuellement ajouter le formulaire de métadonnées disponible à votre ressource et sélectionner des termes du glossaire pour classer vos données.
3. Choisissez Publier la ressource pour publier la `mkt_sls_table` ressource.

Étape 7 - Création du projet pour l'analyse des données

Cette section décrit les étapes de création du projet pour l'analyse des données. C'est le début des étapes de consommation de données de ce flux de travail.

1. Une fois que vous avez terminé l'étape 6 ci-dessus, dans le portail de DataZone données Amazon, choisissez Create project dans le menu déroulant Project.
2. Sur la page Créer un projet, spécifiez le nom du projet. Par exemple, pour ce flux de travail MarketingDataAnalysisProject, vous pouvez le nommer, laisser les autres champs inchangés, puis choisir Créer.

Étape 8 - Création d'un environnement pour l'analyse des données

Cette section décrit les étapes de création d'un environnement pour l'analyse des données.

1. Une fois que vous avez terminé l'étape 7 ci-dessus, dans le portail de DataZone données Amazon, choisissez le `MarketingDataAnalysisProject` projet, puis choisissez l'onglet Environnements, puis choisissez Create environment.
2. Sur la page Créer un environnement, spécifiez ce qui suit, puis choisissez Créer un environnement.
   - Nom : spécifiez le nom de l'environnement. Pour cette procédure pas à pas, vous pouvez l'`Default data lake environment`appeler.
   - Description : spécifiez une description de l'environnement.
   - Profil d'environnement : choisissez le profil d'DataLakeProfileenvironnement intégré.
   - Pour cette procédure pas à pas, conservez les autres champs inchangés.

Étape 9 - Rechercher dans le catalogue de données et s'abonner aux données

Cette section décrit les étapes de recherche dans le catalogue de données et d'abonnement aux données.

1. Une fois que vous avez terminé l'étape 8 ci-dessus, dans le portail de DataZone données Amazon, choisissez l' DataZoneicône Amazon, et dans le champ de DataZone recherche

Amazon, recherchez des actifs de données à l'aide de mots clés (par exemple, « catalogue » ou « ventes ») dans la barre de recherche du portail de données.

Si nécessaire, appliquez des filtres ou effectuez un tri. Une fois que vous avez localisé la ressource Product Sales Data, vous pouvez la choisir pour ouvrir la page de détails de la ressource.

2. Sur la page de détails de la ressource Catalog Sales Data, choisissez Subscribe.
3. Dans la boîte de dialogue S'abonner, choisissez votre projet MarketingDataAnalysisProjectclient dans la liste déroulante, puis spécifiez le motif de votre demande d'abonnement, puis choisissez S'abonner.

Étape 10 - Approuver la demande d'abonnement

Cette section décrit les étapes d'approbation de la demande d'abonnement.

1. Une fois que vous avez terminé l'étape 9 ci-dessus, dans le portail de DataZone données Amazon, choisissez le SalesDataPublishingProjectprojet avec lequel vous avez publié votre ressource.
2. Cliquez sur l'onglet Données, puis sur Données publiées, puis sur Demandes entrantes.
3. Vous pouvez maintenant voir la ligne correspondant à la nouvelle demande qui nécessite une approbation. Choisissez Afficher la demande. Indiquez le motif de l'approbation et choisissez Approuver.

Étape 11 - Création d'une requête et analyse des données dans Amazon Athena

Maintenant que vous avez publié avec succès une ressource dans le DataZone catalogue Amazon et que vous vous y êtes abonné, vous pouvez l'analyser.

1. Sur le portail de DataZone données Amazon, choisissez votre projet MarketingDataAnalysisProjectclient, puis, dans le panneau de droite, sous Outils d'analyse, choisissez le lien de données Query avec Amazon Athena. Cela ouvre l'éditeur de requêtes Amazon Athena en utilisant les informations d'identification de votre projet pour l'authentification. Choisissez l'environnement du MarketingDataAnalysisProjectconsommateur dans le menu déroulant Amazon DataZone Environment de l'éditeur de requêtes, puis choisissez celui de votre projet dans le menu déroulant `<environment_name>%sub_db` de la base de données.

2. Vous pouvez désormais exécuter des requêtes sur la table abonnée. Vous pouvez choisir le tableau dans Tables et vues, puis choisir Aperçu pour afficher l'instruction de sélection sur l'écran de l'éditeur. Exécutez la requête pour voir les résultats.

Amazon DataZone QuickStart avec les données Amazon Redshift

Rubriques

Étape 1 - Création du DataZone domaine Amazon et du portail de données

Suivez la procédure ci-dessous pour créer un DataZone domaine Amazon. Pour plus d'informations sur DataZone les domaines Amazon, consultez DataZone Terminologie et concepts d'Amazon.

1. Accédez à la DataZone console Amazon à l'adresse https://console.aws.amazon.com/datazone, connectez-vous, puis choisissez Create domain.

   > **Note**
   >
   > Si vous souhaitez utiliser un DataZone domaine Amazon existant pour ce flux de travail, choisissez Afficher les domaines, puis choisissez le domaine que vous souhaitez utiliser, puis passez à l'étape 2 de création d'un projet de publication.

2. Sur la page Créer un domaine, entrez des valeurs pour les champs suivants :

- Nom : spécifiez le nom de votre domaine. Dans le cadre de ce flux de travail, vous pouvez appeler ce domaine`Marketing`.
- Description : spécifiez une description de domaine facultative.
- Chiffrement des données : vos données sont cryptées par défaut à l'aide d'une clé qui vous AWS appartient et qui est gérée pour vous. Pour cette procédure pas à pas, vous pouvez conserver les paramètres de chiffrement des données par défaut.

  Pour plus d'informations sur l'utilisation des clés gérées par le client, consultezLe chiffrement des données est au repos pour Amazon DataZone. Si vous utilisez votre propre clé KMS pour le chiffrement des données, vous devez inclure l'instruction suivante dans votre clé par défautAmazonDataZoneDomainExecutionRole.

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

- Accès au service : choisissez l'option Utiliser un rôle de service personnalisé, puis choisissez-la dans le AmazonDataZoneDomainExecutionRolemenu déroulant.
- Sous Configuration rapide, choisissez Configurer ce compte pour la consommation et la publication de données. Cette option active les DataZone plans Amazon intégrés du lac de données et de l'entrepôt de données, et configure les autorisations et les ressources requises pour effectuer les autres étapes de ce flux de travail. Pour plus d'informations sur les DataZone plans Amazon, consultez DataZone Terminologie et concepts d'Amazon.
- Conservez les champs restants sous Détails des autorisations et Tags inchangés, puis choisissez Créer un domaine.

3. Une fois le domaine créé avec succès, choisissez-le et, sur la page de résumé du domaine, notez l'URL du portail de données pour ce domaine. Vous pouvez utiliser cette URL pour accéder à votre portail de DataZone données Amazon afin d'effectuer les autres étapes de ce flux de travail.

> **Note**
>
> Dans la version actuelle d'Amazon DataZone, une fois le domaine créé, l'URL générée pour le portail de données ne peut pas être modifiée.

La création d'un domaine peut prendre plusieurs minutes. Attendez que le statut du domaine soit défini sur Disponible avant de passer à l'étape suivante.

Étape 2 - Création du projet de publication

La section suivante décrit les étapes de création du projet de publication dans ce flux de travail.

1. Une fois l'étape 1 terminée, accédez au portail de DataZone données Amazon à l'aide de l'URL du portail de données et connectez-vous à l'aide de vos informations d'identification unique (SSO) ou AWS IAM.
2. Choisissez Créer un projet, spécifiez le nom du projet. Par exemple, pour ce flux de travail SalesDataPublishingProject, vous pouvez le nommer, laisser les autres champs inchangés, puis choisir Créer.

Étape 3 - Création de l'environnement

La section suivante décrit les étapes de création d'un environnement dans ce flux de travail.

1. Une fois que vous avez terminé l'étape 2, dans le portail de DataZone données Amazon, choisissez le `SalesDataPublishingProject` projet que vous avez créé à l'étape précédente, puis choisissez l'onglet Environnements, puis choisissez Create environment.
2. Sur la page Créer un environnement, spécifiez ce qui suit, puis choisissez Créer un environnement.

   - Nom : spécifiez le nom de l'environnement. Pour cette procédure pas à pas, vous pouvez l'`Default data warehouse environment`appeler.

- Description : spécifiez une description de l'environnement.
- Profil d'environnement : choisissez le profil d'DataWarehouseProfileenvironnement.
- Indiquez le nom de votre cluster Amazon Redshift, le nom de la base de données et l'ARN secret du cluster Amazon Redshift dans lequel vos données sont stockées.

> **Note**
>
> Assurez-vous que votre secret dans AWS Secrets Manager inclut les balises suivantes (clé/valeur) :
>
> - Pour le cluster Amazon Redshift - datazone.rs.cluster : <cluster_name:database name>
>
> Pour le groupe de travail Amazon Redshift Serverless - datazone.rs.workgroup : <workgroup_name:database_name>
> - AmazonDataZoneProject: <projectID>
> - AmazonDataZoneDomain: <domainID>
>
> Pour plus d'informations, consultez Stockage des informations d'identification de base de données dans AWS Secrets Manager.
> L'utilisateur de base de données que vous indiquez dans le Gestionnaire AWS des Secrets doit disposer des autorisations de superutilisateur.

Étape 4 - Produire des données pour publication

La section suivante décrit les étapes de production des données destinées à être publiées dans ce flux de travail.

1. Une fois l'étape 3 terminée, dans le portail de DataZone données Amazon, choisissez le `SalesDataPublishingProject` projet, puis, dans le panneau de droite, sous Outils d'analyse, choisissez Amazon Redshift. Cela ouvre l'éditeur de requêtes Amazon Redshift en utilisant les informations d'identification de votre projet pour l'authentification.
2. Pour cette procédure pas à pas, vous utilisez le script de requête Create Table as Select (CTAS) pour créer une nouvelle table que vous souhaitez publier sur Amazon. DataZone Dans votre éditeur de requêtes, exécutez ce script CTAS pour créer une `mkt_sls_table` table que vous pouvez publier et rendre disponible pour la recherche et l'abonnement.

```
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
```

Assurez-vous que la table mkt_sls_table est correctement créée. Vous disposez désormais d'un actif de données qui peut être publié dans le DataZone catalogue Amazon.

Étape 5 - Collectez les métadonnées depuis Amazon Redshift

La section suivante décrit les étapes de collecte de métadonnées à partir d'Amazon Redshift.

1. Une fois l'étape 4 terminée, dans le portail de DataZone données Amazon, choisissez le `SalesDataPublishingProject` projet, puis l'onglet Données, puis choisissez Sources de données.
2. Choisissez la source créée dans le cadre du processus de création de l'environnement.
3. Choisissez Exécuter à côté du menu déroulant Action, puis cliquez sur le bouton d'actualisation. Une fois l'exécution de la source de données terminée, les actifs sont ajoutés à l' DataZone inventaire Amazon.

Étape 6 - Organiser et publier la ressource de données

La section suivante décrit les étapes de conservation et de publication de la ressource de données dans ce flux de travail.

1. Une fois l'étape 5 terminée, dans le portail de DataZone données Amazon, choisissez le `SalesDataPublishingProject` projet, puis l'onglet Données, choisissez les données d'inventaire et localisez le `mkt_sls_table` tableau.
2. Ouvrez la page de détails de l'`mkt_sls_table`actif pour voir les noms commerciaux générés automatiquement. Cliquez sur l'icône de métadonnées générées automatiquement pour afficher les noms générés automatiquement pour les actifs et les colonnes. Vous pouvez accepter ou rejeter chaque nom individuellement ou choisir Accepter tout pour appliquer les noms générés. Vous pouvez également éventuellement ajouter le formulaire de métadonnées disponible à votre ressource et sélectionner des termes du glossaire pour classer vos données.
3. Choisissez Publier pour publier la `mkt_sls_table` ressource.

Étape 7 - Création du projet pour l'analyse des données

La section suivante décrit les étapes de création du projet pour l'analyse des données dans ce flux de travail.

1. Une fois l'étape 6 terminée, dans le portail de DataZone données Amazon, choisissez Create project.
2. Dans la page Créer un projet, spécifiez le nom du projet. Par exemple, pour ce flux de travail MarketingDataAnalysisProject, vous pouvez le nommer, laisser les autres champs inchangés, puis choisir Créer.

Étape 8 - Création d'un environnement pour l'analyse des données

La section suivante décrit les étapes de création d'un environnement pour l'analyse des données dans ce flux de travail.

1. Une fois que vous avez terminé l'étape 7, dans le portail de DataZone données Amazon, choisissez le `MarketingDataAnalysisProject` projet que vous avez créé à l'étape précédente, puis choisissez l'onglet Environnements, puis choisissez Ajouter un environnement.
2. Sur la page Créer un environnement, spécifiez ce qui suit, puis choisissez Créer un environnement.

   - Nom : spécifiez le nom de l'environnement. Pour cette procédure pas à pas, vous pouvez l'`Default data warehouse environment`appeler.
   - Description : spécifiez une description de l'environnement.

- Profil d'environnement : choisissez le profil d'DataWarehouseProfileenvironnement.
- Indiquez le nom de votre cluster Amazon Redshift, le nom de la base de données et l'ARN secret du cluster Amazon Redshift dans lequel vos données sont stockées.

> **Note**
>
> Assurez-vous que votre secret dans AWS Secrets Manager inclut les balises suivantes (clé/valeur) :
>
> - Pour le cluster Amazon Redshift - datazone.rs.cluster : <cluster_name:database name>
>
> Pour le groupe de travail Amazon Redshift Serverless - datazone.rs.workgroup : <workgroup_name:database_name>
> - AmazonDataZoneProject: <projectID>
> - AmazonDataZoneDomain: <domainID>
>
> Pour plus d'informations, consultez Stockage des informations d'identification de base de données dans AWS Secrets Manager.
> L'utilisateur de base de données que vous indiquez dans le Gestionnaire AWS des Secrets doit disposer des autorisations de superutilisateur.

- Pour cette procédure pas à pas, conservez les autres champs inchangés.

Étape 9 - Rechercher dans le catalogue de données et s'abonner aux données

La section suivante décrit les étapes de recherche dans le catalogue de données et d'abonnement aux données.

1. Une fois l'étape 8 terminée, dans le portail de DataZone données Amazon, recherchez des actifs de données à l'aide de mots clés (par exemple, « catalogue » ou « ventes ») dans la barre de recherche du portail de données.

   Si nécessaire, appliquez des filtres ou effectuez un tri. Une fois que vous avez localisé la ressource Product Sales Data, vous pouvez la choisir pour ouvrir la page de détails de la ressource.
2. Sur la page de détails de la ressource Product Sales Data, choisissez S'abonner.

3. Dans la boîte de dialogue, choisissez votre projet client dans la liste déroulante, indiquez le motif de la demande d'accès, puis choisissez S'abonner.

Étape 10 - Approuver la demande d'abonnement

La section suivante décrit les étapes d'approbation de la demande d'abonnement dans ce flux de travail.

1. Une fois l'étape 9 terminée, dans le portail de DataZone données Amazon, choisissez le SalesDataPublishingProjectprojet avec lequel vous avez publié votre ressource.
2. Choisissez l'onglet Données, puis Données publiées, puis Demandes entrantes.
3. Choisissez le lien de demande de consultation, puis sélectionnez Approuver.

Étape 11 - Création d'une requête et analyse des données dans Amazon Redshift

Maintenant que vous avez publié avec succès une ressource dans le DataZone catalogue Amazon et que vous vous y êtes abonné, vous pouvez l'analyser.

1. Dans le portail de DataZone données Amazon, sur le panneau de droite, cliquez sur le lien Amazon Redshift. Cela ouvre l'éditeur de requêtes Amazon Redshift en utilisant les informations d'identification du projet pour l'authentification.
2. Vous pouvez désormais exécuter une requête (instruction select) sur la table abonnée. Vous pouvez cliquer sur le tableau (three-vertical-dots option) et choisir l'aperçu pour afficher l'instruction sélectionnée sur l'écran de l'éditeur. Exécutez la requête pour voir les résultats.

Amazon DataZone QuickStart avec des exemples de scripts

La section suivante décrit des exemples de scripts qui invoquent diverses DataZone API Amazon que vous pouvez utiliser pour effectuer les tâches suivantes :

Rubriques

- Création d'un DataZone domaine Amazon et d'un portail de données
- Création d'un projet de publication
- Création d'un profil d'environnement

- Création d'un environnement
- Collectez des métadonnées à partir de AWS Glue
- Organiser et publier un actif de données
- Rechercher dans le catalogue de données et s'abonner aux données
- Autres exemples de scripts utiles

Création d'un DataZone domaine Amazon et d'un portail de données

Vous pouvez utiliser l'exemple de script suivant pour créer un DataZone domaine Amazon. Pour plus d'informations sur DataZone les domaines Amazon, consultez DataZone Terminologie et concepts d'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",
    )
```

Création d'un projet de publication

Vous pouvez utiliser l'exemple de script suivant pour créer un projet de publication sur Amazon DataZone.

```
// Create Project
def create_project(domainId):
    return dzclient.create_project(
```

```
        domainIdentifier = domainId,
        name = "sample-project"
    )
```

Création d'un profil d'environnement

Vous pouvez utiliser les exemples de scripts suivants pour créer un profil d'environnement dans Amazon DataZone.

Cet exemple de charge utile est utilisé lorsque l'`CreateEnvironmentProfile`API est invoquée :

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

Cet exemple de script appelle l'`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
```

Voici l'exemple de charge utile de sortie une fois que l'`CreateEnvironmentProfile`API est invoquée :

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

Création d'un environnement

Vous pouvez utiliser l'exemple de script suivant pour créer un environnement dans 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
```

Collectez des métadonnées à partir de AWS Glue

Vous pouvez utiliser cet exemple de script pour collecter des métadonnées à partir de AWS Glue. Ce script s'exécute selon un calendrier standard. Vous pouvez récupérer les paramètres à partir de l'exemple de script et les rendre globaux. Récupérez le projet, l'environnement et l'ID de domaine à l'aide des fonctions standard. La source de données AWS Glue est créée et exécutée à une heure standard qui peut être mise à jour dans la section cron du 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"
    }
}
```

Organiser et publier un actif de données

Vous pouvez utiliser les exemples de scripts suivants pour organiser et publier des actifs de données sur Amazon DataZone.

Vous pouvez utiliser le script suivant pour créer des types de formulaires personnalisés :

```
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"
    )
```

Vous pouvez utiliser l'exemple de script suivant pour créer des types de ressources personnalisés :

```
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,
    )
```

Vous pouvez utiliser l'exemple de script suivant pour créer des ressources personnalisées :

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

Vous pouvez utiliser l'exemple de script suivant pour créer un glossaire :

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

Vous pouvez utiliser l'exemple de script suivant pour créer un terme de glossaire :

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

Vous pouvez utiliser l'exemple de script suivant pour créer une ressource à l'aide d'un type de ressource défini par le système :

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

Vous pouvez utiliser l'exemple de script suivant pour créer une révision de ressource et y joindre un terme du glossaire :

```
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:>"]
    )
```

Vous pouvez utiliser l'exemple de script suivant pour publier une ressource :

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

Rechercher dans le catalogue de données et s'abonner aux données

Vous pouvez utiliser les exemples de scripts suivants pour effectuer des recherches dans le catalogue de données et vous abonner aux données :

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

Vous pouvez utiliser l'exemple de script suivant pour obtenir l'ID de liste de l'actif :

```
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']
```

Vous pouvez utiliser les exemples de scripts suivants pour créer une demande d'abonnement à l'aide de l'ID de liste :

```
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."
    )
```

À l'aide de `create_subscription_response` ce qui précède, obtenez le `subscription_request_id`, puis acceptez/approuvez l'abonnement à l'aide de l'exemple de script suivant :

```
subscription_request_id = create_subscription_response["id"]
```

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

Autres exemples de scripts utiles

Vous pouvez utiliser les exemples de scripts suivants pour effectuer diverses tâches lorsque vous travaillez avec vos données sur Amazon DataZone.

Utilisez l'exemple de script suivant pour répertorier les DataZone domaines Amazon existants :

```
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
```

Utilisez l'exemple de script suivant pour répertorier les DataZone projets Amazon existants :

```
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
```

Utilisez l'exemple de script suivant pour répertorier les formulaires de DataZone métadonnées Amazon existants :

```
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
```

Gestion des DataZone domaines Amazon et de l'accès des utilisateurs

Rubriques

Création de domaines

> **Note**
>
> Si vous utilisez Amazon DataZone avec AWS Identity Center pour fournir un accès aux utilisateurs et aux groupes SSO, votre DataZone domaine Amazon doit actuellement se trouver dans la même AWS région que votre instance AWS Identity Center.

Amazon DataZone, un domaine est une entité organisatrice permettant de connecter vos actifs, vos utilisateurs et leurs projets. Pour plus d'informations, consultez DataZone Terminologie et concepts d'Amazon.

Pour créer un DataZone domaine Amazon, vous devez assumer un rôle IAM dans le compte avec des autorisations administratives. Configurer les autorisations IAM requises pour utiliser la console de DataZone gestion Amazonpour obtenir les autorisations minimales nécessaires à la création d'un domaine.

Amazon a besoin de rôles IAM supplémentaires DataZone pour effectuer des actions au nom des utilisateurs du domaine avec une configuration par défaut. Vous pouvez créer ces rôles IAM à l'avance ou demander à Amazon de les DataZone créer pour vous. Si vous souhaitez qu'Amazon DataZone crée ces rôles IAM pour vous pendant le processus

de création du domaine, vous devez alors assumer un rôle IAM avec des autorisations de création de rôles. veuillez consulter Créez une politique personnalisée pour les autorisations IAM afin de permettre à la console de DataZone service Amazon de simplifier la création de rôles . En fonction de vos choix de création de domaine, Amazon DataZone créera jusqu'à quatre nouveaux rôles IAM pour vous : AmazonDataZoneDomainExecutionRole, AmazonDataZoneGlueManageAccessRoleAmazonDataZoneRedshiftManageAccessRole, et AmazonDataZoneProvisioningRole.

Suivez la procédure ci-dessous pour créer un DataZone domaine Amazon.

1. Accédez à la DataZone console Amazon à l'adresse https://console.aws.amazon.com/datazone et utilisez le sélecteur de région dans la barre de navigation supérieure pour choisir la AWS région appropriée.
2. Choisissez Créer un domaine et entrez des valeurs pour les champs suivants :

   - Nom : spécifiez un nom convivial pour le domaine. Une fois le domaine créé, ce nom ne peut pas être modifié.
   - Description - (facultatif) spécifiez une description de domaine.
   - Chiffrement des données : votre DataZone domaine Amazon, vos métadonnées et vos données de reporting sont chiffrés par le AWS Key Management Service (KMS) à l'aide d'une clé spécifique à votre Amazon DataZone. Utilisez ce champ pour indiquer si vous souhaitez utiliser une clé AWS détenue ou choisir une autre clé AWS KMS.

     Pour plus d'informations sur l'utilisation des clés gérées par le client, consultezLe chiffrement des données est au repos pour Amazon DataZone. Si vous utilisez votre propre clé KMS pour le chiffrement des données, vous devez inclure l'instruction suivante dans votre clé par défautAmazonDataZoneDomainExecutionRole.

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

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

- Accès au service : choisissez si vous voulez qu'Amazon en DataZone crée et utilise un nouveau DomainExecutionRolepour vous, ou choisissez un rôle IAM existant.
- Configuration rapide : (facultatif) cochez cette case pour démarrer plus rapidement en demandant à Amazon de DataZone configurer votre compte pour la consommation et la publication de données. Amazon DataZone créera trois rôles IAM pour le provisionnement, l'ingestion et la gestion de l'accès aux ressources AWS Glue et Amazon Redshift, créera un nouveau compartiment Amazon S3, créera un DataZone projet Amazon administratif et créera des profils d'environnement pour les plans par défaut du lac de données et de l'entrepôt de données.
- Balises : (facultatif) spécifiez les AWS balises (paires clé/valeur) pour le domaine.
- Une fois le domaine créé avec succès, votre navigateur doit être actualisé pour afficher la page de détails de votre nouveau DataZone domaine Amazon.

Modifier des domaines

Dans Amazon DataZone, un domaine est une entité organisatrice permettant de relier vos actifs, vos utilisateurs et leurs projets. Pour plus d'informations, consultez DataZone Terminologie et concepts d'Amazon.

Après avoir créé un DataZone domaine Amazon, vous pouvez le modifier ultérieurement pour : modifier la description, activer IAM Identity Center et ajouter, modifier ou supprimer des clés de balise et leurs valeurs. Pour modifier un DataZone domaine Amazon, vous devez assumer un rôle IAM dans le compte avec des autorisations administratives. Configurer les autorisations IAM requises pour utiliser la console de DataZone gestion Amazonpour obtenir les autorisations minimales nécessaires pour modifier un domaine.

Pour modifier un domaine, procédez comme suit :

1. Connectez-vous à la console AWS de gestion et ouvrez la DataZone console Amazon à l'adresse https://console.aws.amazon.com/datazone.
2. Choisissez Afficher les domaines et choisissez le nom du domaine dans la liste. Le nom est un hyperlien.
3. Sur la page de détails du domaine, choisissez Modifier.
4.
   - Modifiez la description.
   - Définissez les paramètres du centre d'identité IAM. Pour en savoir plus sur ces paramètres, consultezConfiguration de l' AWS IAM Identity Center pour Amazon DataZone.
   - Ajoutez, modifiez ou supprimez les clés Tag et leurs valeurs.
5. Une fois que vous avez effectué vos modifications, choisissez Mettre à jour le domaine.

Supprimer des domaines

Dans Amazon DataZone, un domaine est une entité organisatrice permettant de relier vos actifs, vos utilisateurs et leurs projets. Pour plus d'informations, consultez DataZone Terminologie et concepts d'Amazon.

La suppression d'un domaine est définitive. La suppression supprime irrévocablement toutes les DataZone entités Amazon, y compris les sources de données, les projets, les environnements, les actifs, les glossaires et les formulaires de métadonnées. La suppression ne supprime pas les DataZone AWS ressources extérieures à Amazon qu'Amazon DataZone peut vous avoir aidé à créer, telles que les rôles IAM, les compartiments S3, les bases de données AWS Glue et les subventions d'abonnement via ou LakeFormation Redshift. Si vous n'avez plus besoin de ces ressources, supprimez-les dans le AWS service correspondant.

Pour empêcher quelqu'un de supprimer un domaine de manière malveillante, la suppression d'un domaine nécessite des autorisations administratives IAM pour Amazon DataZone, que vous pouvez configurer avec IAM. Pour empêcher quelqu'un de supprimer un domaine accidentellement, la suppression d'un domaine nécessite un mot de confirmation (dans la DataZone console Amazon).

Pour supprimer un domaine, procédez comme suit :

1. Connectez-vous à la console AWS de gestion et ouvrez la DataZone console Amazon à l'adresse https://console.aws.amazon.com/datazone.
2. Choisissez Afficher les domaines et choisissez le nom du domaine dans la liste. Le nom est un hyperlien.

3. Choisissez Supprimer et consultez les avertissements d'information.
4. Tapez le texte demandé pour confirmer que vous avez bien compris ces avertissements. Sélectionnez Delete (Supprimer).

> **Important**
>
> La suppression de votre domaine est une action irrévocable qui ne peut être annulée ni par vous ni par vous. AWS

> **Note**
>
> Lorsque vous ou les utilisateurs de votre domaine créez un environnement dans un projet, Amazon DataZone crée AWS des ressources dans votre domaine ou dans les comptes associés afin de vous fournir, ainsi qu'aux utilisateurs de votre domaine, des fonctionnalités. Vous trouverez ci-dessous la liste des AWS ressources qu'Amazon DataZone peut créer pour les projets de votre domaine, ainsi que le nom par défaut. La suppression d'un domaine ne supprime aucune de ces AWS ressources de vos AWS comptes.
>
> - <environmentId>Rôles IAM : datazone_usr_.
> - <environmentName>Bases de données Glue : (1) <environmentName>_pub_db-*, (2) _sub_db-*. S'il existe déjà une base de données portant ce nom, Amazon DataZone ajoutera l'ID d'environnement.
> - <environmentName>Groupes de travail Athena : -*. S'il existe déjà un groupe de travail portant ce nom, Amazon DataZone ajoutera l'ID d'environnement.
> - CloudWatch groupe de journaux : datazone_ <environmentId>

Activer IAM Identity Center pour Amazon DataZone

> **Note**
>
> Pour terminer cette procédure, le centre d'identité AWS IAM doit être activé dans la même AWS région que votre DataZone domaine Amazon.

Vous pouvez fournir aux utilisateurs et aux groupes SSO l'accès à votre portail de DataZone données Amazon à l'aide d' AWS IAM Identity Center. Une fois que vous avez terminéConfiguration de l' AWS IAM Identity Center pour Amazon DataZone, vous pouvez permettre à vos utilisateurs et groupes SSO d'accéder à votre portail de données de DataZone domaine Amazon.

Pour activer l'utilisation d' AWS IAM Identity Center avec votre DataZone domaine Amazon, vous devez assumer un rôle IAM dans le compte avec des autorisations administratives. Configurer les autorisations IAM requises pour utiliser la console de DataZone gestion Amazonet Créez une politique personnalisée pour les autorisations IAM afin de permettre à la console de DataZone service Amazon de simplifier la création de rôles pour obtenir les autorisations minimales nécessaires pour activer l'utilisation d'IAM Identity Center avec Amazon DataZone.

Suivez la procédure ci-dessous pour activer l' AWS IAM Identity Center pour Amazon DataZone.

1. Connectez-vous à la console AWS de gestion et ouvrez-la à l' DataZone adresse https://console.aws.amazon.com/datazone.
2. Sélectionnez Afficher les domaines et choisissez le nom du domaine dans la liste. Le nom est un hyperlien.
3. Sur la page détaillée du domaine, choisissez Modifier.
   - Cochez la case Activer les utilisateurs dans IAM Identity Center.
   - Choisissez entre les deux modes d'attribution des utilisateurs. Une fois que votre domaine est mis à jour avec votre sélection, il ne peut pas être modifié ultérieurement.
     - Avec l'attribution d'utilisateurs implicite, tout utilisateur ajouté à votre annuaire IAM Identity Center peut accéder à votre DataZone domaine Amazon.
     - Avec l'attribution d'utilisateurs explicite, vous ajouterez des utilisateurs ou des groupes spécifiques à partir de votre annuaire IAM Identity Center pour leur permettre d'accéder à votre DataZone domaine Amazon. Vous ajouterez et supprimerez ces utilisateurs et groupes ultérieurement dans la DataZone console Amazon.
4. Une fois que vous êtes satisfait de votre sélection, choisissez Mettre à jour le domaine.

Désactiver IAM Identity Center pour Amazon DataZone

La désactivation d' AWS IAM Identity Center pour un DataZone domaine Amazon supprimera l'accès de tous les utilisateurs SSO.

> **Note**
>
> La désactivation d'IAM Identity Center n'interrompra pas la facturation des utilisateurs SSO. Pour arrêter la facturation aux utilisateurs du SSO, vous devez les désactiver dans votre domaine. La facturation se poursuit jusqu'à la fin du mois au cours duquel un utilisateur est désactivé. Pour désactiver des utilisateurs, consultezGérer les utilisateurs dans la DataZone console Amazon.

Vous pouvez fournir aux utilisateurs et aux groupes SSO l'accès à votre portail de DataZone données Amazon à l'aide d' AWS IAM Identity Center. Si vous avez activé AWS IAM Identity Center pour Amazon DataZone, vous pourrez ultérieurement désactiver l'accès pour tous les utilisateurs.

Pour désactiver AWS IAM Identity Center afin de l'utiliser avec votre DataZone domaine Amazon, vous devez assumer un rôle IAM dans le compte avec des autorisations administratives. Configurer les autorisations IAM requises pour utiliser la console de DataZone gestion Amazonet Créez une politique personnalisée pour les autorisations IAM afin de permettre à la console de DataZone service Amazon de simplifier la création de rôles pour obtenir les autorisations minimales nécessaires pour désactiver l'utilisation d'IAM Identity Center avec Amazon DataZone.

Suivez la procédure ci-dessous pour désactiver l' AWS IAM Identity Center pour Amazon DataZone.

1. Connectez-vous à la console AWS de gestion et ouvrez-la à l' DataZone adresse https://console.aws.amazon.com/datazone.
2. Sélectionnez Afficher les domaines et choisissez le nom du domaine dans la liste. Le nom est un hyperlien.
3. <regionName><accountId><domainName>Copiez le nom de ressource Amazon (ARN) de votre domaine, qui commence par arn:aws:datazone : ::domain/.
4. Ouvrez la console IAM Identity Center à l'adresse https://console.aws.amazon.com/singlesignon/.
5. Choisissez Applications.
6. Choisissez le domaine pour lequel vous souhaitez désactiver AWS IAM Identity Center, ce qui supprimera l'accès au portail de données du domaine pour tous les utilisateurs de l'authentification unique. Vous pouvez utiliser le menu Filtre et le champ de recherche pour filtrer la liste des applications.
7. Dans le menu Actions, choisissez Désactiver.

8. Les utilisateurs du SSO perdront l'accès au DataZone domaine Amazon.
9. Pour réactiver AWS IAM Identity Center pour le DataZone domaine Amazon, choisissez le domaine pour lequel vous souhaitez réactiver AWS IAM Identity Center, puis dans le menu Actions, choisissez Activer.

Gérer les utilisateurs dans la DataZone console Amazon

Vos utilisateurs peuvent accéder au portail de DataZone données Amazon en utilisant leurs AWS informations d'identification ou leurs informations d'identification unique (SSO). Pour gérer les utilisateurs dans la DataZone console Amazon pour un DataZone domaine Amazon, vous devez assumer un rôle IAM dans le compte avec des autorisations administratives. Configurer les autorisations IAM requises pour utiliser la console de DataZone gestion Amazonpour obtenir les autorisations minimales nécessaires pour gérer les utilisateurs dans la DataZone console Amazon.

Rubriques

- Gérer les rôles et les utilisateurs IAM
- Gérer les utilisateurs SSO
- Gérer les groupes SSO

Gérer les rôles et les utilisateurs IAM

Les rôles et utilisateurs IAM sont créés à l'aide AWS d'Identity and Access Management (IAM) et accèdent à vos DataZone domaines Amazon grâce aux autorisations qui leur sont associées via des politiques. Pour plus d'informations, consultez Configurer les autorisations IAM requises pour utiliser le portail de DataZone données Amazon. Vous pouvez consulter la liste des rôles et utilisateurs IAM qui ont activé leur abonnement au DataZone domaine Amazon, désactivé leur accès et activé leur accès s'ils ont été précédemment désactivés.

1. Connectez-vous à la console AWS de gestion et ouvrez-la à l' DataZone adresse https://console.aws.amazon.com/datazone.
2. Sélectionnez Afficher les domaines et choisissez le nom du domaine dans la liste. Le nom est un hyperlien.
3. Sur la page de détails du domaine, choisissez Gestion des utilisateurs.
4. Pour le type d'utilisateur, sélectionnez Utilisateurs IAM pour afficher la liste actuelle des utilisateurs et des rôles IAM activés et désactivés.

- La colonne Nom indique l'ARN de l'utilisateur ou du rôle IAM.
- La colonne Status indique le statut actuel de l'utilisateur ou du rôle IAM dans le domaine.
  - Activé signifie que l'utilisateur ou le rôle IAM a appelé une API, émis une commande (via l'interface de ligne de commande) ou accédé au DataZone portail Amazon pour votre domaine, et que l'abonnement de l'utilisateur vous est facturé.
  - Désactivé signifie que l'accès de l'utilisateur ou du rôle IAM à votre domaine Amazon DataZone est bloqué.

5. Pour désactiver un utilisateur ou un rôle IAM actuellement activé, cochez la case à côté de l'utilisateur et sélectionnez Désactiver dans le menu Actions. L'utilisateur perdra l'accès au DataZone domaine Amazon. La facturation de l'utilisateur prendra fin à la fin du mois civil en cours.
6. Pour activer un utilisateur ou un rôle IAM actuellement désactivé, cochez la case à côté de l'utilisateur et sélectionnez Activer dans le menu Actions. L'utilisateur aura accès au DataZone domaine Amazon si l'utilisateur ou le rôle IAM dispose des autorisations appropriées. La facturation pour l'utilisateur recommencera.

Gérer les utilisateurs SSO

Les utilisateurs SSO sont créés ou synchronisés avec votre fournisseur d'identité dans AWS IAM Identity Center. Pour plus d'informations, consultez Configuration de l' AWS IAM Identity Center pour Amazon DataZone et Activer IAM Identity Center pour Amazon DataZone pour activer et configurer AWS IAM Identity Center pour Amazon DataZone. Vous pouvez consulter la liste des utilisateurs SSO affectés au domaine, ajouter des utilisateurs SSO et supprimer des utilisateurs SSO.

1. Connectez-vous à la console AWS de gestion et ouvrez-la à l' DataZone adresse https://console.aws.amazon.com/datazone.
2. Sélectionnez Afficher les domaines et choisissez le nom du domaine dans la liste. Le nom est un hyperlien.
3. Sur la page de détails du domaine, faites défiler la page vers le bas et choisissez Gestion des utilisateurs.
4. Pour le type d'utilisateur, sélectionnez Utilisateurs SSO pour afficher la liste actuelle des utilisateurs SSO.

   - La colonne Nom indique le nom de l'utilisateur SSO.

- La colonne Status indique le statut actuel de l'utilisateur SSO dans le domaine.
  - Attribué signifie que l'utilisateur SSO a été explicitement affecté au domaine. Par conséquent, l'utilisateur a accès à Amazon DataZone. Ce statut n'est utilisé que lorsque le mode fournisseur d'identité de votre domaine est défini sur une attribution explicite.
  - Activé signifie que l'utilisateur SSO a accédé au DataZone portail Amazon pour le domaine et que l'abonnement de l'utilisateur vous est facturé. L'activation se fait automatiquement.
  - Désactivé signifie que l'accès de l'utilisateur SSO au portail de données du domaine est bloqué. La facturation de l'utilisateur a pris fin à la fin du mois au cours duquel son accès a été désactivé.
  - Supprimé signifie que l'utilisateur SSO a déjà été affecté au domaine, mais qu'il a été supprimé avant d'y accéder.

5. Ajoutez des utilisateurs SSO en choisissant Ajouter et Ajouter des utilisateurs. Cette option n'est pas disponible si le domaine est défini sur une attribution d'utilisateur implicite, ce qui signifie que tous les utilisateurs du pool d'identités ont accès au DataZone domaine Amazon.

   - Sur la page Ajouter des utilisateurs, recherchez les alias des utilisateurs que vous souhaitez ajouter. Une liste de correspondances potentielles apparaîtra sous le champ de recherche.
   - Choisissez l'utilisateur que vous souhaitez ajouter. Leur alias apparaîtra sous la forme d'une puce sous le champ de recherche.
   - Lorsque vous êtes satisfait de la liste des utilisateurs que vous souhaitez ajouter, choisissez Ajouter un ou plusieurs utilisateurs.
   - Les utilisateurs sont affectés au DataZone domaine Amazon avec le statut Attribué.
   - Lorsque l'utilisateur a accédé pour la première fois au portail de données du domaine, le statut passe automatiquement à Activé, et l'abonnement de l'utilisateur commence à vous être facturé.

6. Supprimez un utilisateur SSO assigné en le sélectionnant et en choisissant Désactiver dans le menu Actions. Par conséquent, l'utilisateur perdra l'accès au DataZone domaine Amazon. Le statut de l'utilisateur s'affichera comme Supprimé. Cette option n'est pas disponible si le domaine est défini sur une attribution utilisateur implicite.
7. Désactivez un utilisateur SSO activé en le sélectionnant et en choisissant Désactiver dans le menu Actions. Par conséquent, l'accès de l'utilisateur au DataZone domaine Amazon sera perdu et bloqué. La facturation de l'abonnement de l'utilisateur se poursuivra jusqu'à la fin du mois. Le statut de l'utilisateur sera indiqué comme Désactivé.

8. Activez un utilisateur SSO désactivé en le sélectionnant et en choisissant Activer dans le menu Actions. Par conséquent, l'utilisateur retrouvera l'accès au DataZone domaine Amazon. La facturation débutera immédiatement. Celui de l'utilisateur s'affichera comme Activé.

Gérer les groupes SSO

Les groupes SSO sont créés ou synchronisés avec votre fournisseur d'identité dans AWS IAM Identity Center. Pour plus d'informations, consultez Configuration de l' AWS IAM Identity Center pour Amazon DataZone et Activer IAM Identity Center pour Amazon DataZone pour activer et configurer AWS IAM Identity Center pour Amazon DataZone. Vous pouvez consulter la liste des groupes SSO attribués au domaine, ajouter des groupes SSO et supprimer des groupes SSO.

1. Connectez-vous à la console AWS de gestion et ouvrez-la à l' DataZone adresse https://console.aws.amazon.com/datazone.
2. Sélectionnez Afficher les domaines et choisissez le nom du domaine dans la liste. Le nom est un hyperlien.
3. Sur la page de détails du domaine, faites défiler la page vers le bas et choisissez Gestion des utilisateurs.
4. Pour le type d'utilisateur, sélectionnez Groupes SSO pour afficher la liste actuelle des groupes SSO.

   - La colonne Nom indique le nom du groupe SSO.
   - La colonne Status indique le statut actuel du groupe SSO dans le domaine.
     - Attribué signifie que le groupe SSO a été explicitement attribué au domaine. Par conséquent, tous les utilisateurs du groupe ont accès au portail de données du domaine (sauf si l'utilisateur est désactivé).
     - Non attribué signifie que le groupe SSO a été supprimé du domaine. Les utilisateurs du groupe n'ont pas accès au portail de données du domaine via leur appartenance à ce groupe.
5. Ajoutez des groupes SSO en choisissant Ajouter et ajouter des groupes. Cette option n'est pas disponible si le domaine est défini sur une attribution d'utilisateur implicite, ce qui signifie que tous les utilisateurs du pool d'identités ont accès au DataZone domaine Amazon, quelle que soit leur appartenance au groupe.

   - Sur la page Ajouter des groupes, recherchez les alias des groupes que vous souhaitez ajouter. Une liste de correspondances potentielles apparaîtra sous le champ de recherche.

- Choisissez le groupe que vous souhaitez ajouter. Leur alias apparaîtra sous la forme d'une puce sous le champ de recherche.
- Lorsque vous êtes satisfait de la liste des groupes que vous souhaitez ajouter, choisissez Ajouter un ou plusieurs groupes.
- Les groupes sont affectés au DataZone domaine Amazon avec le statut Assigned.
- Lorsqu'un membre du groupe accède au portail de données du domaine, le statut passe automatiquement à Activé, et l'abonnement de l'utilisateur commence à vous être facturé.

6. Supprimez un groupe SSO attribué en le sélectionnant et en choisissant Annuler l'attribution dans le menu Actions. Par conséquent, le groupe perdra l'accès au DataZone domaine Amazon. Le statut du groupe sera indiqué comme Non attribué. Les utilisateurs qui ont obtenu leur accès à Amazon DataZone via leur appartenance à ce groupe perdront leur accès. Cette option n'est pas disponible si le domaine est défini sur une attribution utilisateur implicite. Pour arrêter de facturer les utilisateurs dont l'accès est supprimé en annulant l'attribution de leur groupe, vous devez ensuite sélectionner et désactiver manuellement leurs profils utilisateur.

Gestion des autorisations des utilisateurs sur le portail DataZone de données Amazon

Dans la version actuelle d'Amazon DataZone, le mécanisme d'autorisation par défaut permet à tous les utilisateurs authentifiés (IAM et SSO) des DataZone domaines Amazon de créer des projets, de créer des entités au sein des projets et d'effectuer des recherches. Les membres du projet doivent toujours respecter les autorisations qui leur sont accordées conformément à leurs rôles de propriétaire de projet ou de contributeur au projet désignés.

Travailler avec les plans DataZone intégrés d'Amazon

Un plan avec lequel un environnement est créé définit les outils et services que les membres du projet auquel appartient l'environnement peuvent utiliser lorsqu'ils travaillent avec les actifs du DataZone catalogue Amazon. Dans la version actuelle d'Amazon DataZone, il existe les plans intégrés suivants :

- Plan du lac de données
- Plan d'entrepôt de données
- SageMaker Plan Amazon

Rubriques

Activez les plans intégrés dans le AWS compte propriétaire du domaine Amazon DataZone

Un plan avec lequel un environnement est créé définit les outils et services que les membres du projet auquel appartient l'environnement peuvent utiliser lorsqu'ils travaillent avec les actifs du DataZone catalogue Amazon.

Dans la version actuelle d'Amazon DataZone, plusieurs plans sont intégrés : le plan du lac de données, le plan de l'entrepôt de données et le plan Amazon. SageMaker

- Le plan du lac de données contient la définition du lancement et de la configuration d'un ensemble de services (AWS Glue, AWS Lake Formation, Amazon Athena) pour publier et utiliser les actifs des lacs de données dans le catalogue Amazon DataZone .
- Le plan d'entrepôt de données contient la définition du lancement et de la configuration d'un ensemble de services (Amazon Redshift) pour publier et utiliser les actifs Amazon Redshift dans le catalogue Amazon. DataZone
- Le SageMaker plan Amazon contient la définition du lancement et de la configuration d'un ensemble de services (Amazon SageMaker Studio) pour publier et utiliser les SageMaker ressources Amazon dans le DataZone catalogue Amazon.

Pour plus d'informations, consultez DataZone Terminologie et concepts d'Amazon.

Lors de la création d'un DataZone domaine Amazon, vous avez la possibilité de choisir la configuration rapide qui active automatiquement le lac de données par défaut et les plans intégrés de l'entrepôt de données par défaut dans le cadre du processus de création du domaine. La configuration rapide crée également des profils d'environnement par défaut et des environnements par défaut pour vous à l'aide de ces plans intégrés.

Si vous ne choisissez pas Configuration rapide lors de la création de votre DataZone domaine Amazon, vous pouvez utiliser la procédure ci-dessous pour activer les plans intégrés disponibles dans le AWS compte hébergeant ce DataZone domaine Amazon. Vous devez activer ces plans intégrés avant de pouvoir les utiliser pour créer des profils d'environnement et des environnements dans ce domaine.

Pour activer les plans intégrés dans un DataZone domaine Amazon via la console de DataZone gestion Amazon, vous devez assumer un rôle IAM dans le compte avec des autorisations administratives. Configurer les autorisations IAM requises pour utiliser la console de DataZone gestion Amazonpour obtenir les autorisations minimales.

Activer les plans intégrés dans un domaine Amazon DataZone

1. Accédez à la DataZone console Amazon à l'adresse https://console.aws.amazon.com/datazone et connectez-vous à l'aide des informations d'identification de votre compte.
2. Choisissez Afficher les domaines et choisissez le domaine dans lequel vous souhaitez activer un ou plusieurs plans intégrés.
3. Sur la page des détails du domaine, accédez à l'onglet Blueprints.
4. Dans la liste des plans, choisissez le plan DefaultDataLakeou DefaultDataWarehousele SageMaker plan Amazon.
5. Sur la page de détails du plan choisi, choisissez Activer dans ce compte.
6. Sur la page Autorisations et ressources, spécifiez les éléments suivants :

    - Si vous activez le DefaultDataLakeplan, pour le rôle Glue Manage Access, spécifiez un rôle de service nouveau ou existant qui DataZone autorise Amazon à ingérer et à gérer l'accès aux tables dans AWS Glue and AWS Lake Formation.
    - Si vous activez le DefaultDataWarehouseplan, pour le rôle Redshift Manage Access, spécifiez un rôle de service nouveau ou existant qui autorise DataZone Amazon à ingérer et à gérer l'accès aux partages de données, aux tables et aux vues dans Amazon Redshift.

- Si vous activez le SageMaker plan Amazon, pour le rôle de SageMaker gestion des accès, spécifiez un rôle de service nouveau ou existant qui accorde à Amazon l' DataZoneautorisation de publier les SageMaker données Amazon dans le catalogue. Cela donne également à Amazon l' DataZone autorisation d'accorder ou de révoquer l'accès aux ressources SageMaker publiées par Amazon dans le catalogue.

  > **Important**
  >
  > Lorsque vous activez le SageMaker plan Amazon, Amazon DataZone vérifie si les rôles IAM suivants pour Amazon DataZone existent dans le compte et la région actuels. Si ces rôles n'existent pas, Amazon les crée DataZone automatiquement.
  >
  > - AmazonDataZoneGlueAccess- <region>- <domainId>
  > - AmazonDataZoneRedshiftAccess- <region>- <domainId>

- Pour le rôle de provisionnement, spécifiez un rôle de service nouveau ou existant qui accorde à Amazon DataZone l'autorisation de créer et de configurer les ressources de l'environnement AWS CloudFormation à l'aide du compte et de la région d'environnement.
- Si vous activez le SageMaker plan Amazon, pour le compartiment Amazon S3 pour la source de données SageMaker -Glue, spécifiez un compartiment Amazon S3 qui doit être utilisé par tous les SageMaker environnements du AWS compte. Le préfixe de compartiment que vous spécifiez doit être l'un des suivants :
  - zone de données Amazon*
  - créateur de zones de données*
  - zone de données SageMaker*
  - DataZone- Sagemaker*
  - Sagemaker- * DataZone
  - DataZone-SageMaker*
  - SageMaker-DataZone*

7. Choisissez Activer le plan.

Une fois que vous avez activé le ou les plans choisis, vous pouvez contrôler quels projets peuvent utiliser les plans dans votre compte pour créer des profils d'environnement. Vous pouvez le faire en affectant la gestion des projets à la configuration du plan.

Spécifiez la gestion des projets sur les plans activés

1. Accédez à la DataZone console Amazon à l'adresse https://console.aws.amazon.com/datazone et connectez-vous à l'aide des informations d'identification de votre compte.
2. Choisissez Afficher les domaines, puis choisissez le domaine dans lequel vous souhaitez ajouter le ou les projets de gestion pour le ou les plans choisis.
3. Choisissez l'onglet Blueprints, puis choisissez le plan avec lequel vous souhaitez travailler.
4. Par défaut, tous les projets du domaine peuvent utiliser les DefaultDataLake SageMaker plans ou Amazon du compte pour créer des profils d'environnement. DefaultDataWareshouse Toutefois, vous pouvez limiter cela en affectant la gestion des projets aux plans. Pour ajouter des projets de gestion, choisissez Sélectionner la gestion du projet, puis choisissez les projets que vous souhaitez ajouter en tant que gestion de projets dans le menu déroulant, puis sélectionnez Sélectionner la gestion de projets.

Une fois que vous avez activé le DefaultDataWarehouse plan dans votre AWS compte, vous pouvez ajouter des ensembles de paramètres à la configuration du plan. Un ensemble de paramètres est un groupe de clés et de valeurs, requis pour qu'Amazon DataZone établisse une connexion à votre cluster Amazon Redshift et est utilisé pour créer des environnements d'entrepôt de données. Ces paramètres incluent le nom de votre cluster Amazon Redshift, de votre base de données et le AWS secret contenant les informations d'identification du cluster.

Ajouter des ensembles de paramètres au DefaultDataWarehouse plan

1. Accédez à la DataZone console Amazon à l'adresse https://console.aws.amazon.com/datazone et connectez-vous à l'aide des informations d'identification de votre compte.
2. Choisissez Afficher les domaines, puis choisissez le domaine dans lequel vous souhaitez ajouter le jeu de paramètres.
3. Choisissez l'onglet Plans, puis choisissez le DefaultDataWareshouse plan pour ouvrir la page de détails du plan.
4. Dans l'onglet Ensembles de paramètres de la page de détails du plan, choisissez Créer un jeu de paramètres.

   - Entrez un nom pour le jeu de paramètres.
   - Fournissez éventuellement une description du jeu de paramètres.
   - Sélectionner une région
   - Sélectionnez le cluster Amazon Redshift ou Amazon Redshift Serverless.

- Sélectionnez l'ARN AWS secret qui contient les informations d'identification du cluster Amazon Redshift sélectionné ou du groupe de travail Amazon Redshift Serverless. Le AWS secret doit être étiqueté avec le `AmazonDataZoneDomain : [Domain_ID]` tag afin de pouvoir être utilisé dans un ensemble de paramètres.
  - Si vous n'avez pas de AWS secret existant, vous pouvez également en créer un nouveau en choisissant Créer un nouveau AWS secret. Cela ouvre une boîte de dialogue dans laquelle vous pouvez fournir le nom du secret, le nom d'utilisateur et le mot de passe. Une fois que vous avez choisi Create New AWS Secret, Amazon DataZone crée un nouveau secret dans le service AWS Secrets Manager et s'assure que le secret est étiqueté avec le domaine dans lequel vous essayez de créer le jeu de paramètres.
- Si vous avez choisi le cluster Amazon Redshift à l'étape ci-dessus, choisissez maintenant un cluster dans le menu déroulant. Si vous avez choisi le groupe de travail Amazon Redshift à l'étape ci-dessus, choisissez maintenant un groupe de travail dans le menu déroulant.
- Entrez le nom de la base de données au sein du cluster Amazon Redshift ou du groupe de travail Amazon Redshift Serverless sélectionné.
- Choisissez Créer un jeu de paramètres.

Une fois que vous avez activé le SageMaker plan Amazon dans votre AWS compte, vous pouvez ajouter des ensembles de paramètres à la configuration du plan. Un ensemble de paramètres est un groupe de clés et de valeurs, requis pour DataZone qu'Amazon puisse établir une connexion avec votre Amazon SageMaker et utilisé pour créer des environnements Sagemaker.

Ajouter des ensembles de paramètres au SageMaker plan Amazon

1. Accédez à la DataZone console Amazon à l'adresse https://console.aws.amazon.com/datazone et connectez-vous à l'aide des informations d'identification de votre compte.
2. Choisissez Afficher les domaines, puis choisissez le domaine contenant le plan activé dans lequel vous souhaitez ajouter le jeu de paramètres.
3. Choisissez l'onglet Blueprints, puis choisissez le SageMaker plan Amazon pour ouvrir la page de détails du plan.
4. Sous l'onglet Ensembles de paramètres de la page de détails du plan, choisissez Créer un jeu de paramètres, puis spécifiez les éléments suivants :
   - Entrez un nom pour le jeu de paramètres.
   - Vous pouvez éventuellement fournir une description pour le jeu de paramètres.

- Spécifiez le type d'authentification SageMaker du domaine Amazon. Vous pouvez choisir IAM ou IAM Identity Center (SSO).
- Spécifiez une AWS région.
- Spécifiez une clé AWS KMS pour le chiffrement des données. Vous pouvez choisir une clé existante ou en créer une nouvelle.
- Sous Paramètres d'environnement, spécifiez les éléments suivants :
  - ID VPC : ID que vous utilisez pour le VPC de l'environnement Amazon. SageMaker Vous pouvez spécifier un VPC existant ou en créer un nouveau.
  - Sous-réseaux : un ou plusieurs identifiants pour une plage d'adresses IP pour des ressources spécifiques au sein de votre VPC.
  - Accès au réseau : choisissez VPC uniquement ou Internet public uniquement.
  - Groupe de sécurité : groupe de sécurité à utiliser lors de la configuration du VPC et des sous-réseaux.
- Sous Paramètres de la source de données, sélectionnez l'une des options suivantes :
  - AWS Glue uniquement
  - AWS Glue + Amazon Redshift sans serveur. Si vous choisissez cette option, spécifiez les éléments suivants :
    - Spécifiez l'ARN AWS secret qui contient les informations d'identification du cluster Amazon Redshift sélectionné. Le AWS secret doit être étiqueté avec le `AmazonDataZoneDomain : [Domain_ID]` tag afin de pouvoir être utilisé dans un ensemble de paramètres.

      Si vous n'avez pas de AWS secret existant, vous pouvez également en créer un nouveau en choisissant Créer un nouveau AWS secret. Cela ouvre une boîte de dialogue dans laquelle vous pouvez fournir le nom du secret, le nom d'utilisateur et le mot de passe. Une fois que vous avez choisi Create New AWS Secret, Amazon DataZone crée un nouveau secret dans le service AWS Secrets Manager et s'assure que le secret est étiqueté avec le domaine dans lequel vous essayez de créer le jeu de paramètres.
    - Spécifiez le groupe de travail Amazon Redshift que vous souhaitez utiliser lors de la création d'environnements.
    - Spécifiez le nom de la base de données (au sein du groupe de travail que vous avez choisi) que vous souhaitez utiliser lors de la création d'environnements.
  - AWS Glue uniquement + Amazon Redshift Cluster

- Spécifiez l'ARN AWS secret qui contient les informations d'identification du cluster Amazon Redshift sélectionné. Le AWS secret doit être étiqueté avec le `AmazonDataZoneDomain : [Domain_ID]` tag afin de pouvoir être utilisé dans un ensemble de paramètres.

  Si vous n'avez pas de AWS secret existant, vous pouvez également en créer un nouveau en choisissant Créer un nouveau AWS secret. Cela ouvre une boîte de dialogue dans laquelle vous pouvez fournir le nom du secret, le nom d'utilisateur et le mot de passe. Une fois que vous avez choisi Create New AWS Secret, Amazon DataZone crée un nouveau secret dans le service AWS Secrets Manager et s'assure que le secret est étiqueté avec le domaine dans lequel vous essayez de créer le jeu de paramètres.
- Spécifiez le cluster Amazon Redshift que vous souhaitez utiliser lors de la création d'environnements.
- Spécifiez le nom de la base de données (au sein du cluster que vous avez choisi) que vous souhaitez utiliser lors de la création d'environnements.

5. Choisissez Créer un jeu de paramètres.

Ajoutez Amazon SageMaker en tant que service de confiance dans le AWS compte propriétaire du DataZone domaine Amazon

Si vous avez activé le SageMaker plan Amazon, vous devez également l'ajouter SageMaker comme l'un des services fiables d'Amazon DataZone. Pour ce faire, suivez la procédure suivante :

1. Accédez à la DataZone console Amazon à l'adresse https://console.aws.amazon.com/datazone et connectez-vous à l'aide des informations d'identification de votre compte.
2. Choisissez Afficher les domaines, puis choisissez le domaine qui contient le SageMaker plan activé.
3. Choisissez les services fiables, puis Amazon SageMaker, puis sélectionnez Activer.

Utilisation des comptes associés pour publier et consommer des données

L'association de vos AWS comptes à votre DataZone domaine Amazon permet aux utilisateurs du domaine de publier et de consommer les données de ces AWS comptes. La configuration d'une association de comptes se fait en trois étapes.

- Commencez par partager le domaine avec le AWS compte souhaité en demandant l'association. Amazon DataZone utilise AWS Resource Access Manager (RAM) si le AWS compte est différent du AWS compte du domaine. Une association de comptes ne peut être initiée que par le DataZone domaine Amazon.
- Ensuite, demandez au propriétaire du compte d'accepter la demande d'association.
- Troisièmement, demandez au propriétaire du compte d'activer les plans d'environnement souhaités. En activant un plan, le propriétaire du compte fournit aux utilisateurs du domaine les rôles IAM et les configurations de ressources nécessaires pour créer et accéder aux ressources de leur compte, telles que les bases de données AWS Glue et les clusters Amazon Redshift.

Rubriques

Demande d'association avec d'autres AWS comptes

> **Note**
>
> En envoyant une demande d'association à un autre AWS compte, vous partagez votre domaine avec l'autre AWS compte avec AWS Resource Access Manager (RAM). Assurez-vous de vérifier l'exactitude de l'identifiant de compte que vous entrez.

Pour demander une association avec d'autres AWS comptes dans la DataZone console Amazon pour un DataZone domaine Amazon, vous devez assumer un rôle IAM dans le compte avec des autorisations administratives. Configurer les autorisations IAM requises pour utiliser la console de DataZone gestion Amazonpour obtenir les autorisations minimales nécessaires pour demander une association de compte.

Procédez comme suit pour demander une association avec d'autres AWS comptes.

1. Connectez-vous à la console de AWS gestion et ouvrez la console de DataZone gestion Amazon à l'adresse https://console.aws.amazon.com/datazone.
2. Choisissez Afficher les domaines et choisissez le nom du domaine dans la liste. Le nom est un hyperlien.
3. Faites défiler l'écran jusqu'à l'onglet Comptes associés et sélectionnez Demander une association.
4. Entrez les identifiants des comptes dont vous souhaitez demander l'association. Lorsque vous êtes satisfait de la liste des identifiants de compte, choisissez Request association.
5. Amazon DataZone crée un partage de ressources dans le AWS Resource Access Manager au nom de votre compte, avec le ou les identifiants de compte saisis comme principaux.
6. Vous devez informer le propriétaire des autres AWS comptes pour qu'il accepte votre demande. Les invitations expirent au bout de sept (7) jours.

Fournissez un accès au compte à votre clé KMS gérée par le client

Les DataZone domaines Amazon et leurs métadonnées sont chiffrés, soit (par défaut) à l'aide d'une clé détenue par le client AWS, soit (facultativement) d'une clé gérée par le client par le biais du AWS Key Management Service (KMS) que vous possédez et que vous fournissez lors de la création du domaine. Si votre domaine est chiffré à l'aide d'une clé gérée par le client, suivez la procédure ci-dessous pour autoriser le compte associé à utiliser la clé KMS.

1. Connectez-vous à la console de AWS gestion et ouvrez la console KMS à l'adresse https://console.aws.amazon.com/kms/.
2. Pour afficher les clés de votre compte que vous créez et gérez vous-même, dans le volet de navigation, choisissez Clés gérées par le client.
3. Pour afficher les clés de votre compte que vous créez et gérez vous-même, dans le volet de navigation, choisissez Clés gérées par le client.

4. Dans la liste des clés KMS, choisissez l'alias ou l'ID de clé de la clé KMS que vous souhaitez examiner.
5. Pour autoriser ou interdire aux AWS comptes externes d'utiliser la clé KMS, utilisez les commandes de la section Autres AWS comptes de la page. Les principaux IAM de ces comptes (dotés eux-mêmes des autorisations KMS appropriées) peuvent utiliser la clé KMS dans le cadre d'opérations cryptographiques, telles que le chiffrement, le déchiffrement, le rechiffrement et la génération de clés de données.

Accepter une demande d'association de compte provenant d'un DataZone domaine Amazon et activer un plan d'environnement

Pour accepter l'association dans la console DataZone de gestion Amazon avec un DataZone domaine Amazon, vous devez assumer un rôle IAM dans le compte avec des autorisations administratives. Configurer les autorisations IAM requises pour utiliser la console de DataZone gestion Amazonpour obtenir les autorisations minimales.

Complétez ce qui suit pour accepter l'association avec un DataZone domaine Amazon.

1. Connectez-vous à la console de AWS gestion et ouvrez la console de DataZone gestion Amazon à l'adresse https://console.aws.amazon.com/datazone.
2. Choisissez Afficher les demandes et sélectionnez le domaine invitant dans la liste. L'état de l'invitation doit être demandé. Choisissez Demande de révision.
3. Choisissez d'activer les plans d'environnement de lac de données et/ou d'entrepôt de données par défaut en ne cochant aucune des cases, les deux ou l'une des cases. Tu pourras le faire plus tard.
   - Le plan d'environnement du lac de données permet aux utilisateurs du domaine de créer et de gérer les ressources AWS Glue, Amazon S3 et Amazon Athena à publier et à consommer à partir d'un lac de données.
   - Le plan d'environnement d'entrepôt de données permet aux utilisateurs du domaine de créer et de gérer des ressources Amazon Redshift à publier et à consommer à partir d'un entrepôt de données.
4. Si vous choisissez de sélectionner l'un des plans d'environnement par défaut ou les deux, configurez les autorisations et ressources suivantes.

- Le rôle IAM de gestion des accès fournit des autorisations à Amazon pour permettre DataZone aux utilisateurs du domaine d'ingérer et de gérer l'accès à des tables, telles que AWS Glue et Amazon Redshift. Vous pouvez choisir de demander à Amazon de DataZone créer et d'utiliser un nouveau rôle IAM, ou vous pouvez choisir parmi une liste de rôles IAM existants.
- Le rôle Provisioning IAM fournit des autorisations DataZone à Amazon pour permettre aux utilisateurs du domaine de créer et de configurer des ressources d'environnement, telles que les bases de données AWS Glue. Vous pouvez choisir de demander à Amazon de DataZone créer et d'utiliser un nouveau rôle IAM, ou vous pouvez choisir parmi une liste de rôles IAM existants.
- Le compartiment Amazon S3 pour Data Lake est le compartiment ou le chemin qu'Amazon utilisera lorsque les utilisateurs du domaine DataZone stockeront les données du lac de données. Vous pouvez utiliser le compartiment par défaut sélectionné par Amazon DataZone ou choisir votre propre chemin Amazon S3 existant en saisissant sa chaîne de chemin. Si vous sélectionnez votre propre chemin Amazon S3, vous devrez mettre à jour les politiques IAM afin de fournir à Amazon DataZone les autorisations nécessaires pour l'utiliser.

5. Lorsque vous êtes satisfait de vos configurations, choisissez Accepter et configurez l'association.

Rejeter une demande d'association de compte provenant d'un DataZone domaine Amazon

Pour rejeter une demande d'association dans la console de DataZone gestion Amazon depuis un DataZone domaine Amazon, vous devez assumer un rôle IAM dans le compte avec des autorisations administratives. Configurer les autorisations IAM requises pour utiliser la console de DataZone gestion Amazonpour obtenir les autorisations minimales.

Complétez ce qui suit pour rejeter une demande d'association provenant d'un DataZone domaine Amazon.

1. Connectez-vous à la console de AWS gestion et ouvrez la console de DataZone gestion Amazon à l'adresse https://console.aws.amazon.com/datazone.
2. Choisissez Afficher les demandes et sélectionnez le domaine invitant dans la liste. L'état de l'invitation doit être demandé. Choisissez Refuser l'association. Confirmez votre choix en choisissant Refuser l'association.

Activer un plan d'environnement dans un compte associé AWS

Pour activer un plan d'environnement dans la console de DataZone gestion Amazon, vous devez assumer un rôle IAM dans le compte avec des autorisations administratives. Configurer les autorisations IAM requises pour utiliser la console de DataZone gestion Amazonpour obtenir les autorisations minimales.

Procédez comme suit pour activer un plan dans un domaine associé.

1. Connectez-vous à la console de AWS gestion et ouvrez la console de DataZone gestion Amazon à l'adresse https://console.aws.amazon.com/datazone.
2. Ouvrez le panneau de navigation de gauche et choisissez Domaines associés.
3. Choisissez le domaine pour lequel vous souhaitez activer un plan d'environnement.
4. Dans la liste des plans, choisissez le plan DefaultDataLakeou DefaultDataWarehousele SageMaker plan Amazon.
5. Sur la page de détails du plan choisi, choisissez Activer dans ce compte.
6. Sur la page Autorisations et ressources, spécifiez les éléments suivants :

   - Si vous activez le DefaultDataLakeplan, pour le rôle Glue Manage Access, spécifiez un rôle de service nouveau ou existant qui DataZone autorise Amazon à ingérer et à gérer l'accès aux tables dans AWS Glue and AWS Lake Formation.
   - Si vous activez le DefaultDataWarehouseplan, pour le rôle Redshift Manage Access, spécifiez un rôle de service nouveau ou existant qui autorise DataZone Amazon à ingérer et à gérer l'accès aux partages de données, aux tables et aux vues dans Amazon Redshift.
   - Si vous activez le SageMaker plan Amazon, pour le rôle de SageMaker gestion des accès, spécifiez un rôle de service nouveau ou existant qui accorde à Amazon l' DataZone autorisation de publier les SageMaker données Amazon dans le catalogue. Cela donne également à Amazon l' DataZone autorisation d'accorder ou de révoquer l'accès aux ressources SageMaker publiées par Amazon dans le catalogue.

     > **Important**
     >
     > Lorsque vous activez le SageMaker plan Amazon, Amazon DataZone vérifie si les rôles IAM suivants pour Amazon DataZone existent dans le compte et la région actuels. Si ces rôles n'existent pas, Amazon les crée DataZone automatiquement.
     >
     > - AmazonDataZoneGlueAccess- <region>- <domainId>

- AmazonDataZoneRedshiftAccess- <region>- <domainId>

- Pour le rôle de provisionnement, spécifiez un rôle de service nouveau ou existant qui accorde à Amazon DataZone l'autorisation de créer et de configurer les ressources de l'environnement AWS CloudFormation à l'aide du compte et de la région d'environnement.
- Si vous activez le SageMaker plan Amazon, pour le compartiment Amazon S3 pour la source de données SageMaker -Glue, spécifiez un compartiment Amazon S3 qui doit être utilisé par tous les SageMaker environnements du AWS compte. Le préfixe de compartiment que vous spécifiez doit être l'un des suivants :
  - zone de données Amazon*
  - créateur de zones de données*
  - zone de données SageMaker*
  - DataZone- Sagemaker*
  - Sagemaker- * DataZone
  - DataZone-SageMaker*
  - SageMaker-DataZone*

7. Choisissez Activer le plan.

Une fois que vous avez activé le ou les plans choisis, vous pouvez contrôler quels projets peuvent utiliser les plans dans votre compte pour créer des profils d'environnement. Vous pouvez le faire en affectant la gestion des projets à la configuration du plan.

Spécifiez la gestion des projets sur Enabled DefaultDataLake ou DefaultDataWarehouse Blueprint

1. Accédez à la DataZone console Amazon à l'adresse https://console.aws.amazon.com/datazone et connectez-vous à l'aide des informations d'identification de votre compte.
2. Ouvrez le panneau de navigation de gauche et sélectionnez Domaines associés, puis choisissez le domaine dans lequel vous souhaitez ajouter la gestion de projets.
3. Choisissez l'onglet Blueprints, puis choisissez DefaultDataLake ou DefaultDataWareshouse Blueprint.
4. Par défaut, tous les projets du domaine peuvent utiliser le DefaultDataWareshouse plan DefaultDataLake ou le plan du compte pour créer des profils d'environnement. Toutefois, vous pouvez limiter cela en affectant la gestion des projets au plan. Pour ajouter des projets de gestion, choisissez Sélectionner la gestion du projet, puis choisissez les projets que vous

souhaitez ajouter en tant que gestion de projets dans le menu déroulant, puis sélectionnez Sélectionner la gestion de projets.

Une fois que vous avez activé le DefaultDataWarehouse plan dans votre AWS compte, vous pouvez ajouter des ensembles de paramètres à la configuration du plan. Un ensemble de paramètres est un groupe de clés et de valeurs, requis pour qu'Amazon DataZone établisse une connexion à votre cluster Amazon Redshift et est utilisé pour créer des environnements d'entrepôt de données. Ces paramètres incluent le nom de votre cluster Amazon Redshift, de votre base de données et le AWS secret contenant les informations d'identification du cluster.

Ajouter des ensembles de paramètres au DefaultDataWarehouse plan

1. Accédez à la DataZone console Amazon à l'adresse https://console.aws.amazon.com/datazone et connectez-vous à l'aide des informations d'identification de votre compte.
2. Ouvrez le panneau de navigation de gauche et sélectionnez Domaines associés, puis choisissez le domaine dans lequel vous souhaitez ajouter des ensembles de paramètres.
3. Choisissez l'onglet Plans, puis choisissez le DefaultDataWareshouse plan pour ouvrir la page de détails du plan.
4. Dans l'onglet Ensembles de paramètres de la page de détails du plan, choisissez Créer un jeu de paramètres.

    - Entrez un nom pour le jeu de paramètres.
    - Fournissez éventuellement une description du jeu de paramètres.
    - Sélectionner une région
    - Sélectionnez le cluster Amazon Redshift ou Amazon Redshift Serverless.
    - Sélectionnez l'ARN AWS secret qui contient les informations d'identification du cluster Amazon Redshift sélectionné ou du groupe de travail Amazon Redshift Serverless. Le AWS secret doit être étiqueté avec le `AmazonDataZoneDomain : [Domain_ID]` tag afin de pouvoir être utilisé dans un ensemble de paramètres.
        - Si vous n'avez pas de AWS secret existant, vous pouvez également en créer un nouveau en choisissant Créer un nouveau AWS secret. Cela ouvre une boîte de dialogue dans laquelle vous pouvez fournir le nom du secret, le nom d'utilisateur et le mot de passe. Une fois que vous avez choisi Create New AWS Secret, Amazon DataZone crée un nouveau secret dans le service AWS Secrets Manager et s'assure que le secret est étiqueté avec le domaine dans lequel vous essayez de créer le jeu de paramètres.

- Sélectionnez le cluster Amazon Redshift ou le groupe de travail Amazon Redshift Serverless.
- Entrez le nom de la base de données au sein du cluster Amazon Redshift ou du groupe de travail Amazon Redshift Serverless sélectionné.
- Choisissez Créer un jeu de paramètres.

Une fois que vous avez activé le SageMaker plan Amazon dans votre AWS compte, vous pouvez ajouter des ensembles de paramètres à la configuration du plan. Un ensemble de paramètres est un groupe de clés et de valeurs, requis pour DataZone qu'Amazon puisse établir une connexion avec votre Amazon SageMaker et utilisé pour créer des environnements Sagemaker.

Ajouter des ensembles de paramètres au SageMaker plan Amazon

1. Accédez à la DataZone console Amazon à l'adresse https://console.aws.amazon.com/datazone et connectez-vous à l'aide des informations d'identification de votre compte.
2. Choisissez Afficher les domaines, puis choisissez le domaine contenant le plan activé dans lequel vous souhaitez ajouter le jeu de paramètres.
3. Choisissez l'onglet Blueprints, puis choisissez le SageMaker plan Amazon pour ouvrir la page de détails du plan.
4. Sous l'onglet Ensembles de paramètres de la page de détails du plan, choisissez Créer un jeu de paramètres, puis spécifiez les éléments suivants :

   - Entrez un nom pour le jeu de paramètres.
   - Vous pouvez éventuellement fournir une description pour le jeu de paramètres.
   - Spécifiez le type d'authentification SageMaker du domaine Amazon. Vous pouvez choisir IAM ou IAM Identity Center (SSO).
   - Spécifiez une AWS région.
   - Spécifiez une clé AWS KMS pour le chiffrement des données. Vous pouvez choisir une clé existante ou en créer une nouvelle.
   - Sous Paramètres d'environnement, spécifiez les éléments suivants :
     - ID VPC : ID que vous utilisez pour le VPC de l'environnement Amazon. SageMaker Vous pouvez spécifier un VPC existant ou en créer un nouveau.
     - Sous-réseaux : un ou plusieurs identifiants pour une plage d'adresses IP pour des ressources spécifiques au sein de votre VPC.
     - Accès au réseau : choisissez VPC uniquement ou Internet public uniquement.

- Groupe de sécurité : groupe de sécurité à utiliser lors de la configuration du VPC et des sous-réseaux.

- Sous Paramètres de la source de données, sélectionnez l'une des options suivantes :
  - AWS Glue uniquement
  - AWS Glue + Amazon Redshift sans serveur. Si vous choisissez cette option, spécifiez les éléments suivants :
    - Spécifiez l'ARN AWS secret qui contient les informations d'identification du cluster Amazon Redshift sélectionné. Le AWS secret doit être étiqueté avec le `AmazonDataZoneDomain : [Domain_ID]` tag afin de pouvoir être utilisé dans un ensemble de paramètres.

      Si vous n'avez pas de AWS secret existant, vous pouvez également en créer un nouveau en choisissant Créer un nouveau AWS secret. Cela ouvre une boîte de dialogue dans laquelle vous pouvez fournir le nom du secret, le nom d'utilisateur et le mot de passe. Une fois que vous avez choisi Create New AWS Secret, Amazon DataZone crée un nouveau secret dans le service AWS Secrets Manager et s'assure que le secret est étiqueté avec le domaine dans lequel vous essayez de créer le jeu de paramètres.
    - Spécifiez le groupe de travail Amazon Redshift que vous souhaitez utiliser lors de la création d'environnements.
    - Spécifiez le nom de la base de données (au sein du groupe de travail que vous avez choisi) que vous souhaitez utiliser lors de la création d'environnements.
  - AWS Glue uniquement + Amazon Redshift Cluster
    - Spécifiez l'ARN AWS secret qui contient les informations d'identification du cluster Amazon Redshift sélectionné. Le AWS secret doit être étiqueté avec le `AmazonDataZoneDomain : [Domain_ID]` tag afin de pouvoir être utilisé dans un ensemble de paramètres.

      Si vous n'avez pas de AWS secret existant, vous pouvez également en créer un nouveau en choisissant Créer un nouveau AWS secret. Cela ouvre une boîte de dialogue dans laquelle vous pouvez fournir le nom du secret, le nom d'utilisateur et le mot de passe. Une fois que vous avez choisi Create New AWS Secret, Amazon DataZone crée un nouveau secret dans le service AWS Secrets Manager et s'assure que le secret est étiqueté avec le domaine dans lequel vous essayez de créer le jeu de paramètres.
    - Spécifiez le cluster Amazon Redshift que vous souhaitez utiliser lors de la création d'environnements.

- Spécifiez le nom de la base de données (au sein du cluster que vous avez choisi) que vous souhaitez utiliser lors de la création d'environnements.

5. Choisissez Créer un jeu de paramètres.

Ajoutez Amazon SageMaker en tant que service de confiance dans le AWS compte associé

Si vous avez activé le SageMaker plan Amazon, vous devez également l'ajouter SageMaker comme l'un des services fiables d'Amazon DataZone. Pour ce faire, suivez la procédure suivante :

1. Accédez à la DataZone console Amazon à l'adresse https://console.aws.amazon.com/datazone et connectez-vous à l'aide des informations d'identification de votre compte.
2. Choisissez Afficher les domaines, puis choisissez le domaine qui contient le SageMaker plan activé.
3. Choisissez les services fiables, puis Amazon SageMaker, puis sélectionnez Activer.

Supprimer un compte associé

Pour supprimer un AWS compte associé dans la console de DataZone gestion Amazon, vous devez assumer un rôle IAM dans le compte avec des autorisations administratives. Configurer les autorisations IAM requises pour utiliser la console de DataZone gestion Amazonpour obtenir les autorisations minimales.

Suivez la procédure ci-dessous pour supprimer un compte associé de votre domaine.

1. Connectez-vous à la console de AWS gestion et ouvrez la console de DataZone gestion Amazon à l'adresse https://console.aws.amazon.com/datazone.
2. Choisissez Afficher les domaines et choisissez le nom du domaine dans la liste. Le nom est un hyperlien.
3. Faites défiler la page jusqu'à l'onglet Comptes associés. Choisissez l'identifiant du AWS compte que vous souhaitez supprimer.
4. Choisissez Dissocier. Confirmez votre choix en saisissant Dissocier dans le champ et en choisissant Dissocier.
5. Le compte est désormais supprimé de votre domaine et ne peut pas être utilisé par les utilisateurs du domaine pour publier et consommer des données.

Utilisation du catalogue de DataZone données Amazon

Vous pouvez utiliser le catalogue de données Amazon DataZone Business pour cataloguer les données de votre organisation en fonction du contexte commercial et permettre ainsi à tous les membres de votre organisation de trouver et de comprendre rapidement les données. Pour plus d'informations, consultez DataZone Terminologie et concepts d'Amazon.

Rubriques

Création, modification ou suppression d'un glossaire professionnel

Sur Amazon DataZone, un glossaire commercial est un ensemble de termes commerciaux (mots) qui peuvent être associés à des actifs (données). Il fournit des vocabulaires appropriés avec une liste de termes commerciaux et leurs définitions à l'intention des utilisateurs professionnels afin de garantir que les mêmes définitions sont utilisées dans l'ensemble de l'organisation lors de l'analyse des données. Les glossaires commerciaux sont créés dans le domaine du catalogue et peuvent être appliqués aux actifs et aux colonnes pour aider à comprendre les principales caractéristiques de cet actif ou de cette colonne. Un ou plusieurs termes du glossaire peuvent être appliqués. Un glossaire commercial peut être une liste plate de termes dans laquelle n'importe quel terme du glossaire commercial peut être associé à une sous-liste d'autres termes. Pour plus d'informations, consultez DataZone Terminologie et concepts d'Amazon. Pour créer, modifier ou supprimer un glossaire dans votre DataZone domaine Amazon, vous devez être membre du projet propriétaire disposant des autorisations appropriées pour ce domaine.

Pour créer un glossaire, procédez comme suit :

1. Accédez au portail de DataZone données Amazon à l'aide de l'URL du portail de données et connectez-vous à l'aide de votre SSO ou de vos AWS informations d'identification. Si vous êtes DataZone administrateur Amazon, vous pouvez obtenir l'URL du portail de données en accédant à la DataZone console Amazon à l'adresse https://console.aws.amazon.com/datazone dans le AWS compte sur lequel le DataZone domaine Amazon a été créé.

2. Accédez au menu Catalogue dans la barre de navigation supérieure à côté de Rechercher.
3. Dans Amazon DataZone Data Portal, choisissez Glossaires, puis Create glossary.
4. Spécifiez le nom, la description et le propriétaire du glossaire, puis choisissez Créer un glossaire.
5. Activez le nouveau glossaire en choisissant le bouton Activé.
6. Sur la page de détails du glossaire, vous pouvez choisir Create readme pour ajouter des informations supplémentaires sur ce glossaire.

Pour désactiver ou activer un glossaire professionnel, procédez comme suit :

1. Accédez au portail de DataZone données Amazon à l'aide de l'URL du portail de données et connectez-vous à l'aide de votre SSO ou de vos AWS informations d'identification. Si vous êtes DataZone administrateur Amazon, vous pouvez obtenir l'URL du portail de données en accédant à la DataZone console Amazon à l'adresse https://console.aws.amazon.com/datazone dans le AWS compte sur lequel le DataZone domaine Amazon a été créé.
2. Accédez au menu Catalogue dans la barre de navigation supérieure à côté de Rechercher.
3. Dans le portail Amazon DataZone Data, choisissez Glossaires et recherchez le glossaire professionnel que vous souhaitez désactiver/activer.
4. Sur la page de détails du glossaire, recherchez le bouton Activer/Désactiver et utilisez-le pour activer ou désactiver le glossaire sélectionné.

> **Note**
>
> La désactivation d'un glossaire désactive également tous les termes qu'il contient.

Pour modifier un glossaire professionnel, procédez comme suit :

1. Accédez au portail de DataZone données Amazon à l'aide de l'URL du portail de données et connectez-vous à l'aide de votre SSO ou de vos AWS informations d'identification. Si vous êtes DataZone administrateur Amazon, vous pouvez obtenir l'URL du portail de données en accédant à la DataZone console Amazon à l'adresse https://console.aws.amazon.com/datazone dans le AWS compte sur lequel le DataZone domaine Amazon a été créé.
2. Accédez au menu Catalogue dans la barre de navigation supérieure à côté de Rechercher.
3. Sur Amazon DataZone Data Portal, choisissez Glossaires et recherchez le glossaire commercial que vous souhaitez modifier.

4. Sur la page de détails du glossaire, développez Actions, puis choisissez Modifier pour modifier le glossaire.
5. Modifiez le nom et la description, puis choisissez Enregistrer.

Pour supprimer un glossaire professionnel, procédez comme suit :

1. Accédez au portail de DataZone données Amazon à l'aide de l'URL du portail de données et connectez-vous à l'aide de votre SSO ou de vos AWS informations d'identification. Si vous êtes DataZone administrateur Amazon, vous pouvez obtenir l'URL du portail de données en accédant à la DataZone console Amazon à l'adresse https://console.aws.amazon.com/datazone dans le AWS compte sur lequel le DataZone domaine Amazon a été créé.
2. Accédez au menu Catalogue dans la barre de navigation supérieure à côté de Rechercher.
3. Sur Amazon DataZone Data Portal, choisissez Glossaires et recherchez le glossaire professionnel que vous souhaitez supprimer.
4. Sur la page de détails du glossaire, développez Actions, puis choisissez Supprimer pour supprimer le glossaire.

   > **Note**
   >
   > Vous devez supprimer tous les termes existants dans le glossaire avant de pouvoir supprimer le glossaire.

5. Confirmez la suppression du glossaire en choisissant Supprimer.

Création, modification ou suppression d'un terme dans un glossaire

Sur Amazon DataZone, un glossaire commercial est un ensemble de termes commerciaux qui peuvent être associés à des actifs (données). Pour plus d'informations, consultez DataZone Terminologie et concepts d'Amazon. Pour créer, modifier ou supprimer des termes dans un glossaire de votre DataZone domaine Amazon, vous devez être membre du projet propriétaire disposant des autorisations appropriées pour ce domaine.

Sur Amazon DataZone, les termes du glossaire commercial peuvent être décrits de manière détaillée. Pour définir le contexte d'un terme en particulier, vous pouvez définir les relations entre les termes. Lorsque vous définissez une relation pour un terme, celle-ci est automatiquement ajoutée à la

définition du terme associé. Les relations terminologiques du glossaire disponibles sur Amazon DataZone sont les suivantes :

- Est un type de - indique que le terme actuel est un type du terme identifié. Indique que le terme identifié est le parent du terme actuel.
- Dispose de types : indique que le terme actuel est un terme générique désignant le ou les termes spécifiques indiqués. Cette relation peut désigner des termes secondaires pour le terme générique.

Pour créer un nouveau terme, procédez comme suit :

1. Accédez au portail de DataZone données Amazon à l'aide de l'URL du portail de données et connectez-vous à l'aide de votre SSO ou de vos AWS informations d'identification. Si vous êtes DataZone administrateur Amazon, vous pouvez obtenir l'URL du portail de données en accédant à la DataZone console Amazon à l'adresse https://console.aws.amazon.com/datazone dans le AWS compte sur lequel le DataZone domaine Amazon a été créé.
2. Accédez au menu Catalogue dans la barre de navigation supérieure à côté de Rechercher.
3. Dans Amazon DataZone Data Portal, sélectionnez Glossaires, puis choisissez le glossaire dans lequel vous souhaitez créer le nouveau terme.
4. Spécifiez le nom, la description et le propriétaire du terme, puis choisissez Créer un terme.
5. Activez le nouveau terme en choisissant le bouton Activé.
6. Pour ajouter un fichier Lisez-moi, accédez à la page de détails des termes, puis vous pouvez choisir Créer un fichier Lisez-moi pour ajouter des informations supplémentaires sur ce glossaire.
7. Pour ajouter des relations, accédez à la page de détails des termes, choisissez la section Relations terminologiques, puis choisissez Ajouter des termes au glossaire. Dans la boîte de dialogue, choisissez la relation et les termes que vous souhaitez associer, puis choisissez Fermer pour ajouter un terme au type de relation approprié. Cette relation est également ajoutée à tous les termes que vous avez associés.

Pour modifier un terme dans un glossaire, procédez comme suit :

1. Accédez au portail de DataZone données Amazon à l'aide de l'URL du portail de données et connectez-vous à l'aide de votre SSO ou de vos AWS informations d'identification. Si vous êtes DataZone administrateur Amazon, vous pouvez obtenir l'URL du portail de données en accédant à la DataZone console Amazon à l'adresse https://console.aws.amazon.com/datazone dans le AWS compte sur lequel le DataZone domaine Amazon a été créé.

2. Accédez au menu Catalogue dans la barre de navigation supérieure à côté de Rechercher.
3. Sur Amazon DataZone Data Portal, choisissez Glossaires, recherchez le glossaire contenant le terme que vous souhaitez modifier, puis choisissez-le.
4. Sur la page de détails du terme, développez Actions, puis choisissez Modifier pour modifier le terme.
5. Modifiez le nom et la description, puis choisissez Enregistrer.

Pour supprimer un terme dans un glossaire, procédez comme suit :

1. Accédez au portail de DataZone données Amazon à l'aide de l'URL du portail de données et connectez-vous à l'aide de votre SSO ou de vos AWS informations d'identification. Si vous êtes DataZone administrateur Amazon, vous pouvez obtenir l'URL du portail de données en accédant à la DataZone console Amazon à l'adresse https://console.aws.amazon.com/datazone dans le AWS compte sur lequel le DataZone domaine Amazon a été créé.
2. Accédez au menu Catalogue dans la barre de navigation supérieure à côté de Rechercher.
3. Sur Amazon DataZone Data Portal, choisissez Glossaires, recherchez le glossaire contenant le terme que vous souhaitez supprimer, puis choisissez-le.
4. Sur la page de détails du glossaire, développez Actions, puis choisissez Supprimer pour supprimer le terme.
5. Confirmez la suppression du terme en choisissant Supprimer.

Création, modification ou suppression de formulaires de métadonnées

Sur Amazon DataZone, les formulaires de métadonnées sont des formulaires simples destinés à compléter le contexte commercial des métadonnées des actifs du catalogue. Il s'agit d'un mécanisme extensible permettant aux propriétaires de données d'enrichir la ressource avec des informations qui peuvent aider les utilisateurs des données lorsqu'ils recherchent et trouvent ces données. Les formulaires de métadonnées peuvent également servir de mécanisme pour assurer la cohérence de tous les actifs publiés dans le DataZone catalogue Amazon.

Une définition de formulaire de métadonnées est composée d'une ou de plusieurs définitions de champs, avec prise en charge des types de données booléens, datés, décimaux, entiers, chaînes et valeurs de champs du glossaire commercial. Pour plus d’informations, consultez

DataZone Terminologie et concepts d'Amazon. Pour créer, modifier ou supprimer des formulaires de métadonnées dans votre DataZone domaine Amazon, vous devez être membre du projet propriétaire et disposer des informations d'identification appropriées.

Pour créer un formulaire de métadonnées, procédez comme suit :

1. Accédez au portail de DataZone données Amazon à l'aide de l'URL du portail de données et connectez-vous à l'aide de votre SSO ou de vos AWS informations d'identification. Si vous êtes DataZone administrateur Amazon, vous pouvez obtenir l'URL du portail de données en accédant à la DataZone console Amazon à l'adresse https://console.aws.amazon.com/datazone dans le AWS compte sur lequel le DataZone domaine Amazon a été créé.
2. Accédez au menu Catalogue dans la barre de navigation supérieure à côté de Rechercher.
3. Dans Amazon DataZone Data Portal, sélectionnez Formulaires de métadonnées, puis sélectionnez Créer un formulaire.
4. Spécifiez le nom, la description et le propriétaire du formulaire de métadonnées, puis choisissez Créer un formulaire.

Pour modifier un formulaire de métadonnées, procédez comme suit :

1. Accédez au portail de DataZone données Amazon à l'aide de l'URL du portail de données et connectez-vous à l'aide de votre SSO ou de vos AWS informations d'identification. Si vous êtes DataZone administrateur Amazon, vous pouvez obtenir l'URL du portail de données en accédant à la DataZone console Amazon à l'adresse https://console.aws.amazon.com/datazone dans le AWS compte sur lequel le DataZone domaine Amazon a été créé.
2. Accédez au menu Catalogue dans la barre de navigation supérieure à côté de Rechercher.
3. Dans Amazon DataZone Data Portal, choisissez Formulaires de métadonnées, puis recherchez le formulaire de métadonnées que vous souhaitez modifier.
4. Sur la page de détails du formulaire de métadonnées, développez Actions, puis choisissez Modifier.
5. Mettez à jour les champs du nom, de la description et du propriétaire, puis choisissez Mettre à jour le formulaire.

Pour supprimer un formulaire de métadonnées, procédez comme suit :

> **Note**
>
> Avant de pouvoir supprimer un formulaire de métadonnées, vous devez le supprimer de tous les types de ressources ou de ressources auxquels il est appliqué.

1. Accédez au portail de DataZone données Amazon à l'aide de l'URL du portail de données et connectez-vous à l'aide de votre SSO ou de vos AWS informations d'identification. Si vous êtes DataZone administrateur Amazon, vous pouvez obtenir l'URL du portail de données en accédant à la DataZone console Amazon à l'adresse https://console.aws.amazon.com/datazone dans le AWS compte sur lequel le DataZone domaine Amazon a été créé.
2. Accédez au menu Catalogue dans la barre de navigation supérieure à côté de Rechercher.
3. Dans Amazon DataZone Data Portal, choisissez Formulaires de métadonnées, puis recherchez le formulaire de métadonnées que vous souhaitez supprimer.
4. Si le formulaire de métadonnées que vous souhaitez supprimer est activé, désactivez-le en choisissant le bouton Activé.
5. Sur la page de détails du formulaire de métadonnées, développez Actions, puis choisissez Supprimer.
6. Confirmez la suppression en choisissant Supprimer.

Création, modification ou suppression de champs dans les formulaires de métadonnées

Sur Amazon DataZone, les formulaires de métadonnées sont des formulaires simples destinés à compléter le contexte commercial des métadonnées des actifs du catalogue. Il s'agit d'un mécanisme extensible permettant aux propriétaires de données d'enrichir la ressource avec des informations qui peuvent aider les utilisateurs des données lorsqu'ils recherchent et trouvent ces données. Les formulaires de métadonnées peuvent également servir de mécanisme pour assurer la cohérence de tous les actifs publiés dans le DataZone catalogue Amazon.

Une définition de formulaire de métadonnées est composée d'une ou de plusieurs définitions de champs, avec prise en charge des types de données booléens, datés, décimaux, entiers, chaînes et valeurs de champs du glossaire commercial. Pour plus d'informations, consultez DataZone Terminologie et concepts d'Amazon. Pour créer, modifier ou supprimer des champs dans les

formulaires de métadonnées de votre DataZone domaine Amazon, vous devez être membre du projet propriétaire et disposer des informations d'identification appropriées.

Pour créer un champ dans un formulaire de métadonnées, procédez comme suit :

1. Accédez au portail de DataZone données Amazon à l'aide de l'URL du portail de données et connectez-vous à l'aide de votre SSO ou de vos AWS informations d'identification. Si vous êtes DataZone administrateur Amazon, vous pouvez obtenir l'URL du portail de données en accédant à la DataZone console Amazon à l'adresse https://console.aws.amazon.com/datazone dans le AWS compte sur lequel le DataZone domaine Amazon a été créé.
2. Accédez au menu Catalogue dans la barre de navigation supérieure à côté de Rechercher.
3. Dans Amazon DataZone Data Portal, choisissez Formulaires de métadonnées, puis choisissez le formulaire de métadonnées dans lequel vous souhaitez créer des champs.
4. Sur la page de détails du formulaire, choisissez Créer un champ.
5. Spécifiez le nom du champ, sa description, son type et indiquez s'il s'agit d'un champ obligatoire, puis choisissez Créer un champ.

Pour modifier un champ dans un formulaire de métadonnées, procédez comme suit :

1. Accédez au portail de DataZone données Amazon à l'aide de l'URL du portail de données et connectez-vous à l'aide de votre SSO ou de vos AWS informations d'identification. Si vous êtes DataZone administrateur Amazon, vous pouvez obtenir l'URL du portail de données en accédant à la DataZone console Amazon à l'adresse https://console.aws.amazon.com/datazone dans le AWS compte sur lequel le DataZone domaine Amazon a été créé.
2. Accédez au menu Catalogue dans la barre de navigation supérieure à côté de Rechercher.
3. Dans Amazon DataZone Data Portal, choisissez Formulaires de métadonnées, puis choisissez le formulaire de métadonnées dans lequel vous souhaitez modifier les champs.
4. Sur la page de détails du formulaire, choisissez le champ que vous souhaitez modifier, puis développez Actions et choisissez Modifier.
5. Modifiez le nom du champ, sa description, son type et indiquez s'il s'agit d'un champ obligatoire, puis choisissez Mettre à jour le champ.

Pour supprimer un champ dans un formulaire de métadonnées, procédez comme suit :

1. Accédez au portail de DataZone données Amazon à l'aide de l'URL du portail de données et connectez-vous à l'aide de votre SSO ou de vos AWS informations d'identification. Si vous êtes

DataZone administrateur Amazon, vous pouvez obtenir l'URL du portail de données en accédant à la DataZone console Amazon à l'adresse https://console.aws.amazon.com/datazone dans le AWS compte sur lequel le DataZone domaine Amazon a été créé.

2. Accédez au menu Catalogue dans la barre de navigation supérieure à côté de Rechercher.
3. Dans Amazon DataZone Data Portal, choisissez Formulaires de métadonnées, puis choisissez le formulaire de métadonnées dans lequel vous souhaitez supprimer des champs.
4. Sur la page de détails du formulaire, choisissez le champ que vous souhaitez supprimer, puis développez Actions et choisissez Supprimer.
5. Confirmez la suppression en choisissant Supprimer.

Travailler avec des projets et des environnements sur Amazon DataZone

Dans Amazon DataZone, les projets permettent à un groupe d'utilisateurs de collaborer sur divers cas d'utilisation commerciale impliquant la publication, la découverte, l'abonnement et la consommation de ressources de données du DataZone catalogue Amazon. Chaque DataZone projet Amazon est soumis à un ensemble de contrôles d'accès afin que seuls les individus, les groupes et les rôles autorisés puissent accéder au projet et aux actifs de données auxquels ce projet est abonné, et ne puissent utiliser que les outils définis par les autorisations du projet. Les projets agissent en tant que principal d'identité qui reçoit des autorisations d'accès aux ressources sous-jacentes, ce qui permet DataZone à Amazon d'opérer au sein de l'infrastructure d'une organisation sans se fier aux informations d'identification des utilisateurs individuels. Pour plus d'informations, consultez DataZone Terminologie et concepts d'Amazon.

Rubriques

Création d'un profil d'environnement

Sur Amazon DataZone, un profil d'environnement est un modèle que vous pouvez utiliser pour créer des environnements. L'objectif d'un profil d'environnement est de simplifier la création d'un environnement en intégrant des informations de placement telles que le AWS compte et la région

dans les profils. Pour plus d'informations, consultez DataZone Terminologie et concepts d'Amazon. Pour créer des profils d'environnement dans un DataZone domaine Amazon, vous devez appartenir à un DataZone projet Amazon. Tous les profils d'environnement appartiennent aux projets et peuvent être utilisés par tous les utilisateurs autorisés, quel que soit le projet, pour créer de nouveaux environnements.

Pour créer un profil d'environnement

1. Accédez au portail de DataZone données Amazon à l'aide de l'URL du portail de données et connectez-vous à l'aide de votre SSO ou de vos AWS informations d'identification. Si vous êtes DataZone administrateur Amazon, vous pouvez obtenir l'URL du portail de données en accédant à la DataZone console Amazon à l'adresse https://console.aws.amazon.com/datazone dans le AWS compte sur lequel le DataZone domaine Amazon a été créé.
2. Dans le portail de données, choisissez Parcourir les projets et sélectionnez le projet dans lequel vous souhaitez créer le profil d'environnement.
3. Accédez à l'onglet Environnements du projet, puis choisissez Créer un profil d'environnement.
4. Configurez les champs suivants :

   - Nom : nom de votre profil d'environnement.
   - Description — (Facultatif) Description de votre profil d'environnement.
   - Projet propriétaire - Le projet dans lequel le profil est créé est sélectionné par défaut dans ce champ.
   - Plan — Le plan pour lequel ce profil est créé. Vous pouvez choisir l'un des DataZone plans Amazon par défaut (Data Lake ou Data Warehouse).

     Si vous avez spécifié le plan de l'entrepôt de données, procédez comme suit :

     - Fournissez un ensemble de paramètres. Pour sélectionner un jeu de paramètres existant, choisissez l'option Choisir un jeu de paramètres. Si vous souhaitez entrer vos propres paramètres, choisissez Enter my own.
     - Si vous choisissez de sélectionner un paramètre existant, procédez comme suit :
       - Sélectionnez un AWS compte dans le menu déroulant.
       - Sélectionnez un ensemble de paramètres dans le menu déroulant.
     - Si vous choisissez de saisir vos propres paramètres, procédez comme suit :
       - Fournissez les AWS paramètres en sélectionnant le AWS compte et la région dans le menu déroulant.

- Fournissez les paramètres du magasin de données Redshift :
  - Sélectionnez le cluster Amazon Redshift ou Amazon Redshift Serverless
  - Entrez l'ARN AWS secret qui contient les informations d'identification du cluster Amazon Redshift ou du groupe de travail Amazon Redshift Serverless sélectionné. Le AWS secret doit être marqué avec l'identifiant du domaine et l'identifiant du projet dans lesquels vous créez le profil d'environnement.
    - `AmazonDataZoneDomain: [Domain_ID]`
    - `AmazonDataZoneProject: [Project_ID]`
  - Entrez le nom du cluster Amazon Redshift ou du groupe de travail Amazon Redshift Serverless.
  - Entrez le nom de la base de données au sein du cluster Amazon Redshift ou du groupe de travail Amazon Redshift Serverless sélectionné.
- Dans la section Projets autorisés, spécifiez les projets qui peuvent utiliser le profil d'environnement pour créer des environnements. Par défaut, tous les projets du domaine peuvent utiliser les profils d'environnement du compte pour créer des environnements. Pour conserver ce paramètre par défaut, choisissez Tous les projets. Toutefois, vous pouvez restreindre cela en affectant des projets autorisés à l'environnement. Pour ce faire, sélectionnez Projets autorisés uniquement, puis spécifiez les projets qui peuvent utiliser ce profil de projet pour créer des environnements.
- Dans la section Publication, choisissez l'une des options suivantes :
  - Publier à partir de n'importe quel schéma : si vous choisissez cette option, les environnements créés à l'aide de ce profil d'environnement peuvent être utilisés pour publier à partir de n'importe quel schéma de base de données sélectionné dans les paramètres Redshift fournis ci-dessus. Les utilisateurs de l'environnement créé à l'aide de ces profils d'environnement peuvent également fournir leurs propres paramètres Amazon Redshift pour publier à partir de n'importe quel schéma du AWS compte et de la région sélectionnés dans le profil d'environnement.
  - Publier uniquement à partir du schéma d'environnement par défaut : si vous choisissez cette option, les environnements créés à l'aide de cette option peuvent être utilisés pour publier uniquement à partir du schéma par défaut créé par Amazon DataZone pour cet environnement. Les utilisateurs de l'environnement créé à l'aide de ces profils d'environnement ne peuvent pas fournir leurs propres paramètres Amazon Redshift.
  - Interdire la publication : si vous choisissez cette option, les environnements créés à l'aide de ce profil d'environnement ne peuvent être utilisés que pour l'abonnement et la

consommation de données. Les environnements ne peuvent pas du tout être utilisés pour publier des données.

Si vous avez spécifié le plan Data Lake, procédez comme suit :

- Dans la section des paramètres du AWS compte, spécifiez le AWS numéro de AWS compte et la région du compte dans laquelle les environnements potentiels seront créés.
- Dans la section Projets autorisés, spécifiez les projets qui peuvent utiliser le profil d'environnement avec le profil d'environnement Data Lake intégré pour créer des environnements. Par défaut, tous les projets du domaine peuvent utiliser le plan du lac de données du compte pour créer des profils d'environnement. Pour conserver ce paramètre par défaut, choisissez Tous les projets. Toutefois, vous pouvez limiter cela en affectant des projets au plan. Pour ce faire, sélectionnez Projets autorisés uniquement, puis spécifiez les projets qui peuvent utiliser ce profil de projet pour créer des environnements.
- Dans la section Bases de données, choisissez N'importe quelle base de données pour activer la publication à partir de n'importe quelle base de données au sein du AWS compte et de la région où l'environnement est créé ou choisissez Seule la base de données par défaut pour activer la publication uniquement à partir de la base de données de publication par défaut créée avec l'environnement.

5. Choisissez Créer un profil d'environnement.

Modifier un profil d'environnement

Sur Amazon DataZone, un profil d'environnement est un modèle que vous pouvez utiliser pour créer des environnements. Pour plus d'informations, consultez DataZone Terminologie et concepts d'Amazon. Pour modifier un profil d'environnement existant dans un DataZone domaine Amazon, vous devez appartenir à un DataZone projet Amazon.

Pour modifier un profil d'environnement

1. Accédez à l'URL du portail de DataZone données Amazon et connectez-vous à l'aide de l'authentification unique (SSO) ou de vos AWS informations d'identification. Si vous êtes un DataZone administrateur Amazon, vous pouvez accéder à la DataZone console Amazon à l'adresse https://console.aws.amazon.com/datazone et vous connecter avec l'adresse Compte AWS où le domaine a été créé, puis choisir Open data portal.
2. Dans le portail de données, choisissez Parcourir les projets et sélectionnez le projet dans lequel vous souhaitez modifier le profil d'environnement.

3. Accédez à l'onglet Environnements du projet, puis choisissez Profils d'environnement, puis choisissez le profil d'environnement que vous souhaitez modifier.

   Si vous modifiez un profil d'environnement d'entrepôt de données, vous ne pouvez modifier que le nom et la description d'un profil d'environnement existant.

   Si vous modifiez un profil d'environnement Data Lake, vous pouvez modifier le nom et la description du profil. Vous pouvez également modifier les projets autorisés à utiliser ce profil pour créer des environnements et vous pouvez modifier des bases de données. Pour modifier ces paramètres, procédez comme suit :

   - Dans la section Projets autorisés, spécifiez les projets qui peuvent utiliser le profil d'environnement avec le profil d'environnement Data Lake intégré pour créer des environnements. Par défaut, tous les projets du domaine peuvent utiliser le plan du lac de données du compte pour créer des profils d'environnement. Pour conserver ce paramètre par défaut, choisissez Tous les projets. Toutefois, vous pouvez limiter cela en affectant des projets au plan. Pour ce faire, sélectionnez Projets autorisés uniquement, puis spécifiez les projets qui peuvent utiliser ce profil de projet pour créer des environnements.
   - Dans la section Bases de données, choisissez N'importe quelle base de données pour activer la publication à partir de n'importe quelle base de données au sein du AWS compte et de la région où l'environnement est créé ou choisissez Seule la base de données par défaut pour activer la publication uniquement à partir de la base de données de publication par défaut créée avec l'environnement.

   Lorsque vous avez terminé vos modifications, choisissez Modifier le profil d'environnement.

Supprimer un profil d'environnement

Sur Amazon DataZone, un profil d'environnement est un modèle que vous pouvez utiliser pour créer des environnements. L'objectif d'un profil d'environnement est de simplifier la création d'un environnement en intégrant des informations de placement telles que le AWS compte et la région dans les profils. Pour plus d'informations, consultez DataZone Terminologie et concepts d'Amazon. Pour supprimer des profils d'environnement dans un DataZone domaine Amazon, vous devez appartenir à un DataZone projet Amazon.

> **Note**
>
> Lorsque vous supprimez un profil d'environnement, vous ne pouvez plus créer d'autres environnements à l'aide de ce profil.

Pour supprimer un profil d'environnement

1. Accédez à l'URL du portail de DataZone données Amazon et connectez-vous à l'aide de l'authentification unique (SSO) ou de vos AWS informations d'identification. Si vous êtes un DataZone administrateur Amazon, vous pouvez accéder à la DataZone console Amazon à l'adresse https://console.aws.amazon.com/datazone et vous connecter avec l'adresse Compte AWS où le domaine a été créé, puis choisir Open data portal.
2. Dans le portail de données, choisissez Parcourir les projets et sélectionnez le projet dans lequel vous souhaitez supprimer le profil d'environnement.
3. Accédez à l'onglet Environnements du projet, puis choisissez Profils d'environnement, puis choisissez le profil d'environnement que vous souhaitez supprimer.
4. Sélectionnez le profil d'environnement que vous souhaitez supprimer, puis choisissez Actions, Supprimer et confirmez la suppression.

Créez un nouvel environnement

Dans les DataZone projets Amazon, les environnements sont des ensembles de ressources configurées (par exemple, un bucket Amazon S3, une base de données AWS Glue ou un groupe de travail Amazon Athena), avec un ensemble donné de principes IAM (rôles d'utilisateur de l'environnement) auxquels sont attribuées des autorisations de propriétaire ou de contributeur qui peuvent opérer sur ces ressources. Pour plus d'informations, consultez DataZone Terminologie et concepts d'Amazon.

Tout DataZone utilisateur Amazon disposant des autorisations requises pour accéder au portail de données peut créer un DataZone environnement Amazon au sein d'un projet.

Pour créer un nouvel environnement, procédez comme suit.

1. Accédez à l'URL du portail de DataZone données Amazon et connectez-vous à l'aide de l'authentification unique (SSO) ou de vos AWS informations d'identification. Si vous êtes un DataZone administrateur Amazon, vous pouvez accéder à la DataZone console Amazon

à l'adresse https://console.aws.amazon.com/datazone et vous connecter avec l'adresse Compte AWS où le domaine a été créé, puis choisir Open data portal.

2. Choisissez Parcourir tous les projets et sélectionnez le projet dans lequel vous souhaitez créer un nouvel environnement.
3. Choisissez Créer un environnement, spécifiez des valeurs pour les champs suivants, puis choisissez Créer un environnement :

   - Nom : nom de l'environnement
   - Description : description de l'environnement
   - Profile d'environnement : choisissez un profil d'environnement existant ou créez-en un nouveau. Un profil d'environnement est un modèle que vous pouvez utiliser pour créer des environnements. Pour plus d'informations, consultez DataZone Terminologie et concepts d'Amazon.

     Une fois que vous avez sélectionné le profil d'environnement, dans la section Paramètres, spécifiez les valeurs des champs qui font partie de ce profil d'environnement.

Modifier un environnement

Dans les DataZone projets Amazon, les environnements sont des ensembles de ressources configurées (par exemple, un bucket Amazon S3, une base de données AWS Glue ou un groupe de travail Amazon Athena), avec un ensemble donné de principes IAM (avec des autorisations de contributeur attribuées) qui peuvent opérer sur ces ressources. Pour plus d'informations, consultez DataZone Terminologie et concepts d'Amazon.

Tout DataZone utilisateur Amazon disposant des autorisations requises pour accéder au portail de données peut modifier un DataZone environnement Amazon au sein d'un projet.

Pour modifier un environnement existant, procédez comme suit.

1. Accédez à l'URL du portail de DataZone données Amazon et connectez-vous à l'aide de l'authentification unique (SSO) ou de vos AWS informations d'identification. Si vous êtes un DataZone administrateur Amazon, vous pouvez accéder à la DataZone console Amazon à l'adresse https://console.aws.amazon.com/datazone et vous connecter avec l'adresse Compte AWS où le domaine a été créé, puis choisir Open data portal.
2. Choisissez Parcourir les projets dans le volet de navigation supérieur et sélectionnez le projet contenant l'environnement que vous souhaitez modifier.

3. Localisez et sélectionnez l'environnement pour ouvrir sa page de détails. Développez ensuite Actions et choisissez Modifier l'environnement.
4. Modifiez le nom et la description de l'environnement, puis choisissez Enregistrer les modifications.

Supprimer un environnement

Dans les DataZone projets Amazon, les environnements sont des ensembles de ressources configurées (par exemple, un bucket Amazon S3, une base de données AWS Glue ou un groupe de travail Amazon Athena), avec un ensemble donné de principes IAM (avec des autorisations de contributeur attribuées) qui peuvent opérer sur ces ressources. Pour plus d'informations, consultez DataZone Terminologie et concepts d'Amazon.

Tout DataZone utilisateur Amazon disposant des autorisations requises pour accéder au portail de données peut supprimer un DataZone environnement Amazon au sein d'un projet.

Pour supprimer un environnement existant, procédez comme suit.

1. Accédez à l'URL du portail de DataZone données Amazon et connectez-vous à l'aide de l'authentification unique (SSO) ou de vos AWS informations d'identification. Si vous êtes un DataZone administrateur Amazon, vous pouvez accéder à la DataZone console Amazon à l'adresse https://console.aws.amazon.com/datazone et vous connecter avec l'adresse Compte AWS où le domaine a été créé, puis choisir Open data portal.
2. Choisissez Parcourir le projet dans le volet de navigation supérieur et sélectionnez le projet contenant l'environnement que vous souhaitez supprimer.
3. Localisez et choisissez l'environnement pour ouvrir sa page de détails, puis développez Actions et choisissez Supprimer l'environnement.
4. Dans la fenêtre contextuelle Supprimer l'environnement, confirmez la suppression `Delete` en tapant dans le champ, puis choisissez Supprimer l'environnement.

   Vous ne pouvez supprimer correctement un environnement qu'une fois que toutes les entités dépendantes de cet environnement ont été supprimées. Pour supprimer un environnement, vous devez d'abord supprimer toutes ses sources de données et cibles d'abonnement associées.

Création d'un nouveau projet.

Dans Amazon DataZone, les projets permettent à un groupe d'utilisateurs de collaborer sur divers cas d'utilisation commerciale impliquant la publication, la découverte, l'abonnement et la consommation de ressources de données du DataZone catalogue Amazon. Pour plus d'informations, consultez DataZone Terminologie et concepts d'Amazon.

Tout DataZone utilisateur Amazon disposant des autorisations requises pour accéder au portail de données peut créer un DataZone projet Amazon.

Pour créer un nouveau projet, procédez comme suit.

1. Accédez à l'URL du portail de DataZone données Amazon et connectez-vous à l'aide de l'authentification unique (SSO) ou de vos AWS informations d'identification. Si vous êtes un DataZone administrateur Amazon, vous pouvez accéder à la DataZone console Amazon à l'adresse https://console.aws.amazon.com/datazone et vous connecter avec l'adresse Compte AWS où le domaine a été créé, puis choisir Open data portal.
2. Dans le portail de DataZone données Amazon, choisissez Create Project.
3. Spécifiez des valeurs pour les champs suivants, puis choisissez Créer un projet :
   - Nom — Le nom du projet.
   - Description — Description du projet.

Modifier le projet

Dans Amazon DataZone, les projets permettent à un groupe d'utilisateurs de collaborer sur divers cas d'utilisation commerciale impliquant la publication, la découverte, l'abonnement et la consommation de ressources de données du DataZone catalogue Amazon. Pour plus d'informations, consultez DataZone Terminologie et concepts d'Amazon. Pour modifier un DataZone projet Amazon, vous devez être le propriétaire de ce projet ou l'administrateur du domaine qui contient ce projet.

Pour modifier un projet existant, procédez comme suit.

1. Accédez à l'URL du portail de DataZone données Amazon et connectez-vous à l'aide de l'authentification unique (SSO) ou de vos AWS informations d'identification. Si vous êtes un DataZone administrateur Amazon, vous pouvez accéder à la DataZone console Amazon à l'adresse https://console.aws.amazon.com/datazone et vous connecter avec l'adresse Compte AWS où le domaine a été créé, puis choisir Open data portal.

2. Choisissez Parcourir les projets.
3. Choisissez le projet que vous souhaitez modifier. Si vous ne le voyez pas facilement dans la liste des projets, vous pouvez le rechercher en spécifiant le nom du projet dans le champ Rechercher un projet.
4. Développez les actions et choisissez Modifier le projet.
5. Mettez à jour le nom et la description du projet, puis choisissez Enregistrer.

Supprimer le projet

Dans Amazon DataZone, les projets permettent à un groupe d'utilisateurs de collaborer sur divers cas d'utilisation commerciale impliquant la publication, la découverte, l'abonnement et/ou la consommation de ressources de données du DataZone catalogue Amazon. Pour plus d'informations, consultez DataZone Terminologie et concepts d'Amazon.

L'acte de supprimer un projet est définitif. La suppression entraîne la suppression irrévocable du contenu du projet, notamment les sources de données, les environnements, les ressources, les glossaires et les formulaires de métadonnées. Amazon DataZone révoque les subventions DataZone qu'Amazon a accordées aux actifs gérés via Lake Formation et Amazon Redshift. La suppression d'un projet ne supprime pas les DataZone AWS ressources non Amazon qu'Amazon DataZone peut vous avoir aidé à créer. Si vous n'avez plus besoin de ces AWS ressources, supprimez-les de leur AWS service et de leur compte respectifs.

Pour supprimer un DataZone projet Amazon, vous devez en être le propriétaire.

Pour supprimer un projet existant, procédez comme suit.

1. Accédez à l'URL du portail de DataZone données Amazon et connectez-vous à l'aide de l'authentification unique (SSO) ou de vos AWS informations d'identification. Un responsable IAM peut accéder à la DataZone console Amazon à l'adresse https://console.aws.amazon.com/datazone et se connecter avec l'adresse Compte AWS où le domaine a été créé, puis choisir Open data portal.
2. Choisissez Parcourir les projets dans le volet de navigation supérieur.
3. Choisissez le projet que vous souhaitez supprimer. S'il ne figure pas dans la liste des projets, vous pouvez le rechercher en spécifiant le nom du projet dans le champ Rechercher un projet.
4. Développez les actions et choisissez Supprimer le projet.

   Consultez les avertissements relatifs à l'impact potentiel de la suppression du projet.

5. Si vous acceptez les avertissements, saisissez le texte de confirmation et choisissez Supprimer.

> **Important**
>
> La suppression d'un projet est une action irrévocable qui ne peut être annulée ni par vous ni par vous. AWS

> **Note**
>
> Lorsque vous ou les utilisateurs de votre domaine créez un environnement dans un projet, Amazon DataZone crée AWS des ressources dans votre domaine ou dans les comptes associés afin de vous fournir, ainsi qu'aux utilisateurs de votre domaine, des fonctionnalités. Vous trouverez ci-dessous la liste des AWS ressources qu'Amazon DataZone peut créer pour un projet, ainsi que le nom par défaut. La suppression d'un projet ne supprime aucune de ces AWS ressources de vos AWS comptes.
>
> - <environmentId>Rôles IAM : datazone_usr_.
> - <environmentName>Bases de données Glue : (1) <environmentName>_pub_db-*, (2) _sub_db-*. S'il existe déjà une base de données portant ce nom, Amazon DataZone ajoutera l'ID d'environnement.
> - <environmentName>Groupes de travail Athena : -*. S'il existe déjà un groupe de travail portant ce nom, Amazon DataZone ajoutera l'ID d'environnement.
> - CloudWatch groupe de journaux : datazone_ <environmentId>

Quitter le projet

Dans Amazon DataZone, les projets permettent à un groupe d'utilisateurs de collaborer sur divers cas d'utilisation commerciale impliquant la publication, la découverte, l'abonnement et la consommation de ressources de données du DataZone catalogue Amazon. Pour plus d'informations, consultez DataZone Terminologie et concepts d'Amazon.

Pour quitter un projet existant, procédez comme suit.

1. Accédez à l'URL du portail de DataZone données Amazon et connectez-vous à l'aide de l'authentification unique (SSO) ou de vos AWS informations d'identification. Si vous êtes un

DataZone administrateur Amazon, vous pouvez accéder à la DataZone console Amazon à l'adresse https://console.aws.amazon.com/datazone et vous connecter avec l'adresse Compte AWS où le domaine a été créé, puis choisir Open data portal.

2. Choisissez Sélectionner un projet dans le volet de navigation supérieur et sélectionnez le projet.
3. Choisissez le projet que vous souhaitez quitter. Si vous ne le voyez pas facilement dans la liste des projets, vous pouvez le rechercher en spécifiant le nom du projet dans le champ Rechercher un projet.
4. Développez les actions et choisissez Quitter le projet.

Ajouter des membres à un projet

Dans Amazon DataZone, les projets permettent à un groupe d'utilisateurs de collaborer sur divers cas d'utilisation commerciale impliquant la publication, la découverte, l'abonnement et la consommation de ressources de données du DataZone catalogue Amazon. Pour plus d'informations, consultez DataZone Terminologie et concepts d'Amazon.

Vous devez être propriétaire ou contributeur du projet pour ajouter des membres à un projet. Vous pouvez ajouter des groupes SSO, des utilisateurs SSO ou des principaux IAM (rôles ou utilisateurs) en tant que membres du projet.

Pour ajouter des membres à un projet existant, procédez comme suit.

1. Accédez à l'URL du portail de DataZone données Amazon et connectez-vous à l'aide de l'authentification unique (SSO) ou de vos AWS informations d'identification. Si vous êtes un DataZone administrateur Amazon, vous pouvez accéder à la DataZone console Amazon à l'adresse https://console.aws.amazon.com/datazone et vous connecter avec l'adresse Compte AWS où le domaine a été créé, puis choisir Open data portal.
2. Choisissez Sélectionner un projet dans le volet de navigation supérieur et sélectionnez le projet.
3. Choisissez le projet auquel vous souhaitez ajouter des membres. Si vous ne le voyez pas facilement dans la liste des projets, vous pouvez le rechercher en spécifiant le nom du projet dans le champ Rechercher un projet.
4. Sur la page de détails du projet, sélectionnez l'onglet Membres, puis le nœud Choisir tous les membres.
5. Dans l'onglet Membres du projet, choisissez Ajouter des membres.

6. Dans la fenêtre contextuelle Ajouter des membres au projet, spécifiez le ou les utilisateurs que vous souhaitez ajouter et précisez leur rôle au sein du projet (propriétaire ou contributeur), puis choisissez Ajouter des membres.

> **Note**
>
> Vous pouvez ajouter un directeur IAM en tant que membre du projet s'il possède déjà un profil DataZone utilisateur Amazon dans le domaine. Amazon crée DataZone automatiquement un profil utilisateur pour un principal IAM lorsqu'il interagit avec succès avec le domaine via le portail, l'API ou la CLI. Vous ne pouvez pas créer de profil utilisateur pour un directeur IAM. Pour ajouter les principaux IAM en tant que membres du projet dans le cas où le principal IAM ne possède pas de profil DataZone utilisateur Amazon existant dans le domaine, demandez à votre administrateur d'ajouter les deux autorisations IAM suivantes à celles de votre domaine AmazonDataZoneDomainExecutionRoledans la console IAM : et. `iam:GetUser` `iam:GetRole` Séparément, pour effectuer des actions dans le domaine, le principal IAM doit disposer des autorisations IAM correspondantes pour ces actions.

Supprimer des membres d'un projet

Dans Amazon DataZone, les projets permettent à un groupe d'utilisateurs de collaborer sur divers cas d'utilisation commerciale impliquant la publication, la découverte, l'abonnement et la consommation de ressources de données du DataZone catalogue Amazon. Pour plus d'informations, consultez DataZone Terminologie et concepts d'Amazon. Vous devez être propriétaire d'un projet pour supprimer des membres d'un projet.

Pour supprimer des membres d'un projet existant, procédez comme suit.

1. Accédez au portail de DataZone données Amazon à l'aide de l'URL du portail de données et connectez-vous à l'aide de votre SSO ou de vos AWS informations d'identification. Si vous êtes DataZone administrateur Amazon, vous pouvez obtenir l'URL du portail de données en accédant à la DataZone console Amazon à l'adresse https://console.aws.amazon.com/datazone dans le AWS compte sur lequel le DataZone domaine Amazon a été créé.
2. Choisissez Sélectionner un projet dans le volet de navigation supérieur et sélectionnez le projet.
3. Choisissez le projet dans lequel vous souhaitez supprimer des membres. Si vous ne le voyez pas facilement dans la liste des projets, vous pouvez le rechercher en spécifiant le nom du projet dans le champ Rechercher un projet.

4. Sur la page de détails du projet, sélectionnez l'onglet Membres, puis le nœud Choisir tous les membres.
5. Dans l'onglet Membres du projet, choisissez le ou les membres que vous souhaitez supprimer du projet, puis sélectionnez Supprimer.
6. Dans la fenêtre contextuelle Supprimer des membres, confirmez la suppression en choisissant Supprimer des membres.

Création d'inventaire et publication de données sur Amazon DataZone

Cette section décrit les tâches et les procédures que vous souhaitez effectuer afin de créer un inventaire de vos données sur Amazon DataZone et de publier vos données sur Amazon DataZone.

Pour pouvoir utiliser Amazon DataZone pour cataloguer vos données, vous devez d'abord les importer (actifs) en tant qu'inventaire de votre projet sur Amazon DataZone. La création d'un inventaire pour un projet particulier rend les actifs accessibles uniquement aux membres de ce projet. Les ressources de l'inventaire du projet ne sont pas accessibles à tous les utilisateurs du domaine lors de la recherche ou de la navigation, sauf si elles sont publiées explicitement. Après avoir créé un inventaire de projet, les propriétaires de données peuvent organiser leurs actifs d'inventaire avec les métadonnées commerciales requises en ajoutant ou en mettant à jour les noms commerciaux (actif et schéma), les descriptions (actif et schéma), lisez-moi, les termes du glossaire (actif et schéma) et les formulaires de métadonnées.

L'étape suivante de l'utilisation d'Amazon DataZone pour cataloguer vos données consiste à rendre les actifs d'inventaire de votre projet accessibles aux utilisateurs du domaine. Vous pouvez le faire en publiant les actifs d'inventaire dans le DataZone catalogue Amazon. Seule la dernière version de la ressource d'inventaire peut être publiée dans le catalogue et seule la dernière version publiée est active dans le catalogue de découverte. Si un actif d'inventaire est mis à jour après sa publication dans le DataZone catalogue Amazon, vous devez le publier à nouveau de manière explicite pour que la dernière version figure dans le catalogue de découverte.

Rubriques

- Supprimer un DataZone actif Amazon
- Lancer manuellement l'exécution d'une source de données dans Amazon DataZone
- Révisions des actifs sur Amazon DataZone
- Qualité des données sur Amazon DataZone
- Utilisation de l'apprentissage automatique et de l'IA générative

Configurer les autorisations de Lake Formation pour Amazon DataZone

Lorsque vous créez un environnement à l'aide du plan de lac de données intégré (DefaultDataLake), une base de données AWS Glue est ajoutée à Amazon dans DataZone le cadre du processus de création de cet environnement. Si vous souhaitez publier des actifs à partir de cette base de données AWS Glue, aucune autorisation supplémentaire n'est requise.

Toutefois, si vous souhaitez publier des actifs et vous abonner à des actifs provenant d'une base de données AWS Glue qui existe en dehors de votre DataZone environnement Amazon, vous devez explicitement fournir à Amazon DataZone les autorisations d'accès aux tables de cette base de données AWS Glue externe. Pour ce faire, vous devez définir les paramètres suivants dans AWS Lake Formation et associer les autorisations Lake Formation nécessaires auAmazonDataZoneGlueAccess- <region>- <domainId>.

- Configurez l'emplacement Amazon S3 de votre lac de données dans AWS Lake Formation avec le mode d'autorisation Lake Formation ou le mode d'accès hybride. Pour plus d'informations, consultez https://docs.aws.amazon.com/lake-formation/latest/dg/ register-data-lake .html.
- Supprimez l'`IAMAllowedPrincipals`autorisation des tables Amazon Lake Formation pour lesquelles Amazon DataZone gère les autorisations. Pour plus d'informations, consultez https://docs.aws.amazon.com/lake-formation/latest/dg/ upgrade-glue-lake-formation -background.html.
- Associez les autorisations de AWS Lake Formation suivantes à AmazonDataZoneGlueAccess- <region>- <domainId> :
  - `Describe`et `Describe grantable` des autorisations sur la base de données où se trouvent les tables
  - `Describe`,`Select`,`Describe Grantable`, `Select Grantable` autorisations sur toutes les tables de la base de données ci-dessus auxquelles vous DataZone souhaitez gérer l'accès en votre nom.

> **Note**
>
> Amazon DataZone prend en charge le mode hybride AWS Lake Formation. Le mode hybride Lake Formation vous permet de commencer à gérer les autorisations sur vos bases de données et tables AWS Glue via Lake Formation, tout en conservant les autorisations IAM existantes sur ces tables et bases de données. Pour plus d'informations, consultez DataZone Intégration d'Amazon au mode hybride de AWS Lake Formation .

Pour plus d'informations, consultez Résolution des problèmes liés aux autorisations de AWS Lake Formation pour Amazon DataZone.

DataZone Intégration d'Amazon au mode hybride de AWS Lake Formation

Amazon DataZone est intégré au mode hybride AWS Lake Formation. Cette intégration vous permet de publier et de partager facilement vos tables AWS Glue via Amazon DataZone sans avoir à les enregistrer au préalable dans AWS Lake Formation. Le mode hybride vous permet de commencer à gérer les autorisations sur vos tables AWS Glue via AWS Lake Formation tout en conservant les autorisations IAM existantes sur ces tables.

Pour commencer, vous pouvez activer le paramètre d'enregistrement de l'emplacement des données dans le DefaultDataLakeplan de la console de DataZone gestion Amazon.

Permettre l'intégration avec AWS le mode hybride Lake Formation

1. Accédez à la DataZone console Amazon à l'adresse https://console.aws.amazon.com/datazone et connectez-vous à l'aide des informations d'identification de votre compte.
2. Choisissez Afficher les domaines et choisissez le domaine dans lequel vous souhaitez activer l'intégration avec le mode hybride AWS Lake Formation.
3. Sur la page des détails du domaine, accédez à l'onglet Blueprints.
4. Dans la liste des plans, choisissez le DefaultDataLakeplan.
5. Assurez-vous que le DefaultDataLake plan est activé. S'il n'est pas activé, suivez les étapes décrites Activez les plans intégrés dans le AWS compte propriétaire du domaine Amazon DataZone pour l'activer dans votre AWS compte.
6. Sur la page de DefaultDataLake détails, ouvrez l'onglet Provisioning et cliquez sur le bouton Modifier dans le coin supérieur droit de la page.

7. Sous Enregistrement de l'emplacement des données, cochez la case pour activer l'enregistrement de l'emplacement des données.
8. Pour le rôle de gestion de l'emplacement des données, vous pouvez créer un nouveau rôle IAM ou sélectionner un rôle IAM existant. Amazon DataZone utilise ce rôle pour gérer l'accès en lecture/écriture au (x) bucket (s) Amazon S3 choisi (s) pour Data Lake en utilisant le mode d'accès hybride AWS Lake Formation. Pour plus d'informations, consultez AmazonDataZone<region>S3 Manage- - <domainId>.
9. Vous pouvez éventuellement choisir d'exclure certains sites Amazon S3 si vous ne souhaitez pas qu'Amazon DataZone les enregistre automatiquement en mode hybride. Pour cela, procédez comme suit :

   - Cliquez sur le bouton à bascule pour exclure les sites Amazon S3 spécifiés.
   - Indiquez l'URI du compartiment Amazon S3 que vous souhaitez exclure.
   - Pour ajouter des compartiments supplémentaires, choisissez Ajouter un emplacement S3.

   > **Note**
   >
   > Amazon autorise DataZone uniquement l'exclusion d'un emplacement S3 racine. Tous les emplacements S3 situés sur le chemin d'un emplacement S3 racine seront automatiquement exclus de l'enregistrement.

   - Sélectionnez Enregistrer les modifications.

Une fois que vous avez activé le paramètre d'enregistrement de la localisation des données dans votre AWS compte, lorsqu'un consommateur de données s'abonne à une table AWS Glue gérée via des autorisations IAM, Amazon enregistre d'abord les emplacements Amazon S3 de cette table en mode hybride, puis accorde l'accès au consommateur de données en gérant les autorisations sur la table via AWS Lake Formation. DataZone Cela garantit que les autorisations IAM disponibles continuent d'exister avec les autorisations AWS Lake Formation récemment accordées, sans perturber les flux de travail existants.

Comment gérer les emplacements Amazon S3 chiffrés lors de l'activation de l'intégration du mode hybride de AWS Lake Formation dans Amazon DataZone

Si vous utilisez un emplacement Amazon S3 chiffré à l'aide d'une clé KMS AWS gérée par le client ou gérée par le client, le rôle AmazonDataZoneS3Manage doit être autorisé à chiffrer et à déchiffrer

les données avec la clé KMS, ou la politique de clé KMS doit accorder des autorisations sur la clé du rôle.

Si votre position Amazon S3 est chiffrée à l'aide d'une clé AWS gérée, ajoutez la politique en ligne suivante au AmazonDataZoneDataLocationManagementrôle :

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

Si votre position Amazon S3 est chiffrée à l'aide d'une clé gérée par le client, procédez comme suit :

1. Ouvrez la console AWS KMS à l'adresse https://console.aws.amazon.com/kms et connectez-vous en tant qu'utilisateur administratif d' AWS Identity and Access Management (IAM) ou en tant qu'utilisateur autorisé à modifier la politique de clé KMS utilisée pour chiffrer l'emplacement.
2. Dans le volet de navigation, sélectionnez Clés gérées par le client, puis choisissez le nom de la clé KMS souhaitée.
3. Sur la page de détails des clés KMS, choisissez l'onglet Politique clé, puis effectuez l'une des opérations suivantes pour ajouter votre rôle personnalisé ou le rôle lié au service Lake Formation en tant qu'utilisateur clé KMS :

   - Si la vue par défaut s'affiche (avec les sections Administrateurs clés, Suppression des clés, Utilisateurs clés et Autres AWS comptes), dans la section Utilisateurs clés, ajoutez le AmazonDataZoneDataLocationManagementrôle.

- Si la politique clé (JSON) s'affiche, modifiez la politique pour ajouter AmazonDataZoneDataLocationManagementun rôle à l'objet « Autoriser l'utilisation de la clé », comme indiqué dans l'exemple suivant

```
...
        {
            "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**
>
> Si la clé KMS ou l'emplacement Amazon S3 ne se trouvent pas dans le même AWS compte que le catalogue de données, suivez les instructions de la section Enregistrement d'un emplacement Amazon S3 chiffré sur plusieurs AWS comptes.

Création de types d'actifs personnalisés

Sur Amazon DataZone, les actifs représentent des types spécifiques de ressources de données, tels que des tables de base de données, des tableaux de bord ou des modèles d'apprentissage

automatique. Pour garantir la cohérence et la standardisation lors de la description des actifs du catalogue, un DataZone domaine Amazon doit disposer d'un ensemble de types d'actifs qui définissent la manière dont les actifs sont représentés dans le catalogue. Un type d'actif définit le schéma d'un type d'actif spécifique. Un type de ressource comporte un ensemble de types de formulaires de métadonnées nominables obligatoires et facultatifs (par exemple, GovForm ou GovernanceFormType). Les types d'actifs sur Amazon DataZone sont versionnés. Lorsque des actifs sont créés, ils sont validés par rapport au schéma défini par leur type d'actif (généralement la dernière version), et si une structure non valide est spécifiée, la création des actifs échoue.

Types de ressources système : Amazon DataZone fournit des types de ressources système appartenant au service (y compris GlueTableAssetType, GlueViewAssetType, RedshiftTableAssetType RedshiftViewAssetType, et S3ObjectCollectionAssetType) et des types de formulaires système (y compris DataSourceReferenceFormType AssetCommonDetailsFormType, et SubscriptionTermsFormType). Les types de ressources du système ne peuvent pas être modifiés.

Types de ressources personnalisés : pour créer des types de ressources personnalisés, vous devez commencer par créer les types de formulaires de métadonnées et les glossaires requis à utiliser dans les types de formulaires. Vous pouvez ensuite créer des types de ressources personnalisés en spécifiant le nom, la description et les formulaires de métadonnées associés, qui peuvent être obligatoires ou facultatifs.

Pour les types d'actifs contenant des données structurées, pour représenter le schéma des colonnes dans le portail de données, vous pouvez utiliser le `RelationalTableFormType` pour ajouter les métadonnées techniques à vos colonnes (y compris les noms des colonnes, les descriptions et les types de données) et le `ColumnBusinessMetadataForm` pour ajouter les descriptions commerciales des colonnes, y compris les noms commerciaux, les termes du glossaire et les paires clé-valeur personnalisées.

Pour créer un type de ressource personnalisé via le portail de données, procédez comme suit :

1. Accédez à l'URL du portail de DataZone données Amazon et connectez-vous à l'aide de l'authentification unique (SSO) ou de vos AWS informations d'identification. Si vous êtes un DataZone administrateur Amazon, vous pouvez accéder à la DataZone console Amazon à l'adresse https://console.aws.amazon.com/datazone et vous connecter avec l'adresse Compte AWS où le domaine a été créé, puis choisir Open data portal.
2. Choisissez Sélectionner un projet dans le volet de navigation supérieur et sélectionnez le projet dans lequel vous souhaitez créer un type de ressource personnalisé.
3. Accédez à l'onglet Données du projet.

4. Choisissez Types de ressources dans le volet de navigation de gauche, puis choisissez Créer un type de ressource.
5. Spécifiez ce qui suit, puis choisissez Create.
   - Nom : nom du type de ressource personnalisé
   - Description : description du type de ressource personnalisé.
   - Choisissez Ajouter des formulaires de métadonnées pour ajouter des formulaires de métadonnées à ce type de ressource personnalisé.
6. Une fois le type d'actif personnalisé créé, vous pouvez l'utiliser pour créer des actifs.

Pour créer un type de ressource personnalisé via les API, procédez comme suit :

1. Créez un type de formulaire de métadonnées en appelant l'action `CreateFormType` API.

   Voici un SageMaker exemple d'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. Ensuite, vous pouvez créer un type de ressource en appelant l'action `CreateAssetType` API. Vous pouvez créer des types de ressources uniquement via les DataZone API Amazon en utilisant les types de formulaires système disponibles (`SubscriptionTermsFormType`dans l'exemple ci-dessous) ou vos types de formulaires personnalisés. Pour les types de formulaires système, le nom du type doit commencer par`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,
        },
    },
)
```

Voici un exemple de création d'un type de ressource pour les données structurées :

```
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. Vous pouvez désormais créer un actif à l'aide des types d'actifs personnalisés que vous avez créés dans les étapes ci-dessus.

```
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}"
        }
        ]
)
```

Dans cet exemple, vous créez un actif de données structuré :

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

Créez et exécutez une source DataZone de données Amazon pour AWS Glue Data Catalog

Dans Amazon DataZone, vous pouvez créer une source de AWS Glue Data Catalog données afin d'importer les métadonnées techniques des tables de base de données AWS Glue. Pour ajouter une source de données pour le AWS Glue Data Catalog, la base de données source doit déjà exister dans AWS Glue.

Lorsque vous créez et gérez une source de AWS Glue données, vous ajoutez des actifs de la AWS Glue base de données source à l'inventaire de votre DataZone projet Amazon. Vous pouvez exécuter vos sources de AWS Glue données selon un calendrier défini ou à la demande pour créer ou mettre à jour les métadonnées techniques de vos actifs. Lors de l'exécution des sources de données, vous pouvez éventuellement choisir de publier vos actifs dans le DataZone catalogue Amazon afin de les

rendre accessibles à tous les utilisateurs du domaine. Vous pouvez également publier les actifs de l'inventaire de votre projet après avoir modifié leurs métadonnées commerciales. Les utilisateurs du domaine peuvent rechercher et découvrir vos actifs publiés, et demander des abonnements à ces actifs.

Pour ajouter une source AWS Glue de données

1. Accédez à l'URL du portail de DataZone données Amazon et connectez-vous à l'aide de l'authentification unique (SSO) ou de vos AWS informations d'identification. Si vous êtes un DataZone administrateur Amazon, vous pouvez accéder à la DataZone console Amazon à l'adresse https://console.aws.amazon.com/datazone et vous connecter avec l'adresse Compte AWS où le domaine a été créé, puis choisir Open data portal.
2. Choisissez Sélectionner un projet dans le volet de navigation supérieur et sélectionnez le projet auquel vous souhaitez ajouter la source de données.
3. Accédez à l'onglet Données du projet.
4. Choisissez Sources de données dans le volet de navigation de gauche, puis choisissez Créer une source de données.
5. Configurez les champs suivants :

   - Nom : nom de la source de données.
   - Description — Description de la source de données.
6. Sous Type de source de données, sélectionnez AWS Glue.
7. Sous Sélectionnez un environnement, spécifiez l'environnement dans lequel vous souhaitez publier les AWS Glue tables.
8. Sous Sélection des données, fournissez une AWS Glue base de données et entrez vos critères de sélection de table. Par exemple, si vous choisissez Inclure et entrez`*corporate`, la base de données inclura toutes les tables sources qui se terminent par le mot`corporate`.

   Vous pouvez choisir une AWS Glue base de données dans la liste déroulante ou saisir un nom de base de données. La liste déroulante inclut deux bases de données : la base de données de publication et la base de données d'abonnement de l'environnement. Si vous souhaitez importer des actifs d'une base de données qui n'est pas créée par l'environnement, vous devez saisir le nom de la base de données au lieu de le sélectionner dans le menu déroulant.

   Vous pouvez ajouter plusieurs règles d'inclusion et d'exclusion pour les tables d'une même base de données. Vous pouvez également ajouter plusieurs bases de données à l'aide du bouton Ajouter une autre base de données.

9. Sous Qualité des données, vous pouvez choisir d'activer la qualité des données pour cette source de données. Dans ce cas, Amazon DataZone importe vos résultats de qualité des données AWS Glue existants dans votre DataZone catalogue Amazon. Par défaut, Amazon DataZone importe les 100 derniers rapports de qualité existants sans date d'expiration depuis AWS Glue.

   Les indicateurs de qualité des données d'Amazon vous DataZone aident à comprendre l'exhaustivité et l'exactitude de vos sources de données. Amazon DataZone extrait ces indicateurs de qualité des données de AWS Glue afin de fournir du contexte à un moment donné, par exemple lors d'une recherche dans un catalogue de données commerciales. Les utilisateurs des données peuvent voir comment les indicateurs de qualité des données évoluent au fil du temps pour les actifs auxquels ils ont souscrit. Les producteurs de données peuvent ingérer les scores de qualité des données de AWS Glue selon un calendrier. Le catalogue de données Amazon DataZone Business peut également afficher des indicateurs de qualité des données provenant de systèmes tiers via des API de qualité des données. Pour plus d'informations, consultez Qualité des données sur Amazon DataZone.
10. Choisissez Suivant.
11. Pour les paramètres de publication, choisissez si les actifs sont immédiatement détectables dans le catalogue de données commerciales. Si vous les ajoutez uniquement à l'inventaire, vous pourrez choisir les conditions d'abonnement ultérieurement et les publier dans le catalogue de données commerciales. Pour plus d'informations, consultez the section called "Gérer les sources de données existantes".
12. Pour la génération automatique de noms commerciaux, choisissez si vous souhaitez générer automatiquement des métadonnées pour les actifs lors de leur importation depuis la source.
13. (Facultatif) Pour les formulaires de métadonnées, ajoutez des formulaires pour définir les métadonnées collectées et enregistrées lorsque les actifs sont importés dans Amazon DataZone. Pour plus d'informations, consultez the section called "Création, modification ou suppression de formulaires de métadonnées".
14. Pour la préférence Exécuter, choisissez quand exécuter la source de données.

    - Exécuter selon un calendrier : spécifiez les dates et heures d'exécution de la source de données.
    - Exécuter à la demande : vous pouvez lancer manuellement des exécutions de sources de données.
15. Choisissez Suivant.

16. Vérifiez la configuration de votre source de données et choisissez Create.

Création et gestion d'une source de DataZone données Amazon pour Amazon Redshift

Dans Amazon DataZone, vous pouvez créer une source de données Amazon Redshift afin d'importer les métadonnées techniques des tables et des vues de base de données depuis l'entrepôt de données Amazon Redshift. Pour ajouter une source de DataZone données Amazon pour Amazon Redshift, l'entrepôt de données source doit déjà exister dans Amazon Redshift.

Lorsque vous créez et gérez une source de données Amazon Redshift, vous ajoutez des actifs de l'entrepôt de données Amazon Redshift source à l'inventaire de votre projet DataZone Amazon. Vous pouvez exécuter vos sources de données Amazon Redshift selon un calendrier défini ou à la demande pour créer ou mettre à jour les métadonnées techniques de vos actifs. Pendant l'exécution des sources de données, vous pouvez éventuellement choisir de publier les actifs de l'inventaire de votre projet dans le DataZone catalogue Amazon afin de les rendre accessibles à tous les utilisateurs du domaine. Vous pouvez également publier vos actifs d'inventaire après avoir modifié leurs métadonnées commerciales. Les utilisateurs du domaine peuvent rechercher et découvrir vos actifs publiés et demander des abonnements à ces actifs.

Pour ajouter une source de données Amazon Redshift

1. Accédez à l'URL du portail de DataZone données Amazon et connectez-vous à l'aide de l'authentification unique (SSO) ou de vos AWS informations d'identification. Si vous êtes un DataZone administrateur Amazon, vous pouvez accéder à la DataZone console Amazon à l'adresse https://console.aws.amazon.com/datazone et vous connecter avec l'adresse Compte AWS où le domaine a été créé, puis choisir Open data portal.
2. Choisissez Sélectionner un projet dans le volet de navigation supérieur et sélectionnez le projet auquel vous souhaitez ajouter la source de données.
3. Accédez à l'onglet Données du projet.
4. Choisissez Sources de données dans le volet de navigation de gauche, puis choisissez Créer une source de données.
5. Configurez les champs suivants :

   - Nom : nom de la source de données.
   - Description — Description de la source de données.

6. Sous Type de source de données, sélectionnez Amazon Redshift.
7. Sous Sélectionnez un environnement, spécifiez un environnement dans lequel publier les tables Amazon Redshift.
8. En fonction de l'environnement que vous sélectionnez, Amazon DataZone appliquera automatiquement les informations d'identification Amazon Redshift et les autres paramètres directement depuis l'environnement ou vous donnera la possibilité de choisir les vôtres.

   - Si vous avez sélectionné un environnement qui autorise uniquement la publication à partir du schéma Amazon Redshift par défaut de l'environnement, Amazon DataZone appliquera automatiquement les informations d'identification Amazon Redshift et d'autres paramètres, notamment le nom du cluster ou du groupe de travail Amazon Redshift, le secret AWS , le nom de la base de données et le nom du schéma. Vous ne pouvez pas modifier ces paramètres remplis automatiquement.
   - Si vous sélectionnez un environnement qui n'autorise pas la publication de données, vous ne pourrez pas procéder à la création de la source de données.
   - Si vous sélectionnez un environnement qui permet de publier des données à partir de n'importe quel schéma, vous aurez la possibilité d'utiliser les informations d'identification et les autres paramètres Amazon Redshift de l'environnement ou de saisir vos propres identifiants/paramètres.
9. Si vous choisissez d'utiliser vos propres informations d'identification pour créer la source de données, fournissez les informations suivantes :

   - Sous Fournir les informations d'identification Amazon Redshift, choisissez d'utiliser un cluster Amazon Redshift provisionné ou un espace de travail sans serveur Amazon Redshift comme source de données.
   - En fonction de votre sélection à l'étape ci-dessus, choisissez votre cluster ou espace de travail Amazon Redshift dans le menu déroulant, puis choisissez le secret à utiliser pour l'authentification dans AWS Secrets Manager. Vous pouvez choisir un secret existant ou en créer un nouveau.
   - Pour que le secret existant apparaisse dans le menu déroulant, assurez-vous que votre secret dans AWS Secrets Manager inclut les balises suivantes (clé/valeur) :
     - AmazonDataZoneProject: <projectID>
     - AmazonDataZoneDomain: <domainID>

     Si vous choisissez de créer un nouveau secret, celui-ci est automatiquement étiqueté avec les balises référencées ci-dessus et aucune étape supplémentaire n'est nécessaire. Pour

plus d'informations, consultez la section Stockage des informations d'identification de base de données dans AWS Secrets Manager.

Les utilisateurs d'Amazon Redshift dont le code AWS secret a été fourni pour créer la source de données doivent disposer d'`SELECT`autorisations sur les tables à publier. Si vous souhaitez qu'Amazon DataZone gère également les abonnements (accès) en votre nom, les utilisateurs de la base de données AWS secrète doivent également disposer des autorisations suivantes :

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

10. Sous Sélection des données, fournissez une base de données Amazon Redshift, un schéma et entrez les critères de sélection de votre table ou de votre vue. Par exemple, si vous choisissez Inclure et entrez`*corporate`, la ressource inclura toutes les tables sources qui se terminent par le mot`corporate`.

    Vous pouvez ajouter plusieurs règles d'inclusion pour les tables d'une même base de données. Vous pouvez également ajouter plusieurs bases de données à l'aide du bouton Ajouter une autre base de données.

11. Choisissez Suivant.
12. Pour les paramètres de publication, choisissez si les actifs sont immédiatement détectables dans le catalogue de données. Si vous les ajoutez uniquement à l'inventaire, vous pourrez choisir les conditions d'abonnement ultérieurement et les publier dans le catalogue de données commerciales. Pour plus d'informations, consultez the section called "Gérer les sources de données existantes".
13. Pour la génération automatique de noms commerciaux, choisissez si vous souhaitez générer automatiquement des métadonnées pour les actifs au fur et à mesure de leur publication et de leur mise à jour à partir de la source.
14. (Facultatif) Pour les formulaires de métadonnées, ajoutez des formulaires pour définir les métadonnées collectées et enregistrées lorsque les actifs sont importés dans Amazon DataZone. Pour plus d'informations, consultez the section called "Création, modification ou suppression de formulaires de métadonnées".
15. Pour la préférence Exécuter, choisissez quand exécuter la source de données.

    - Exécuter selon un calendrier : spécifiez les dates et heures d'exécution de la source de données.

- Exécuter à la demande : vous pouvez lancer manuellement des exécutions de sources de données.

16. Choisissez Suivant.
17. Vérifiez la configuration de votre source de données et choisissez Create.

Gérez les sources de DataZone données Amazon existantes

Après avoir créé une source de DataZone données Amazon, vous pouvez la modifier à tout moment pour modifier les détails de la source ou les critères de sélection des données. Lorsque vous n'avez plus besoin d'une source de données, vous pouvez la supprimer.

Pour effectuer ces étapes, la politique AmazonDataZoneFullAccess AWS gérée doit être jointe. Pour plus d'informations, consultez the section called "AWS politiques gérées".

Rubriques

Modifier une source de données

Vous pouvez modifier une source de DataZone données Amazon pour modifier ses paramètres de sélection de données, notamment en ajoutant, en supprimant ou en modifiant les critères de sélection des tables. Vous pouvez également ajouter et supprimer des bases de données. Vous ne pouvez pas modifier le type de source de données ni l'environnement dans lequel une source de données est publiée.

Pour modifier une source de données

1. Accédez à l'URL du portail de DataZone données Amazon et connectez-vous à l'aide de l'authentification unique (SSO) ou de vos AWS informations d'identification. Si vous êtes un DataZone administrateur Amazon, vous pouvez accéder à la DataZone console Amazon à l'adresse https://console.aws.amazon.com/datazone et vous connecter avec l'adresse Compte AWS où le domaine a été créé, puis choisir Open data portal.
2. Choisissez Sélectionner un projet dans le volet de navigation supérieur et sélectionnez le projet auquel appartient la source de données.
3. Accédez à l'onglet Données du projet.

4. Choisissez Sources de données dans le volet de navigation de gauche, puis choisissez la source de données que vous souhaitez modifier.
5. Accédez à l'onglet Définition de la source de données et choisissez Modifier.
6. Apportez vos modifications à la définition de la source de données. Vous pouvez mettre à jour les détails de la source de données et modifier les critères de sélection des données.
7. Une fois les modifications terminées, choisissez Save (Enregistrer).

Supprimer une source de données

Lorsque vous n'avez plus besoin d'une source de DataZone données Amazon, vous pouvez la supprimer définitivement. Une fois que vous avez supprimé une source de données, toutes les ressources provenant de cette source de données sont toujours disponibles dans le catalogue et les utilisateurs peuvent toujours s'y abonner. Cependant, les ressources cesseront de recevoir des mises à jour de la source. Nous vous recommandons de déplacer d'abord les ressources dépendantes vers une autre source de données avant de les supprimer.

> **Note**
>
> Vous devez supprimer tous les envois de la source de données avant de pouvoir la supprimer. Pour plus d'informations, consultez Découvrir, s'abonner et consommer des données sur Amazon DataZone.

Pour supprimer une source de données

1. Dans l'onglet Données du projet, sélectionnez Sources de données dans le volet de navigation de gauche.
2. Choisissez la source de données que vous souhaitez supprimer.
3. Choisissez Actions, Supprimer la source de données et confirmez la suppression.

Publier des actifs dans le DataZone catalogue Amazon à partir de l'inventaire du projet

Vous pouvez publier les DataZone actifs Amazon et leurs métadonnées à partir des inventaires de projets dans le DataZone catalogue Amazon. Vous ne pouvez publier que la version la plus récente d'une ressource dans le catalogue.

Tenez compte des points suivants lorsque vous publiez des actifs dans le catalogue :

- Pour publier une ressource dans le catalogue, vous devez être le propriétaire ou le contributeur de ce projet.
- Pour les actifs Amazon Redshift, assurez-vous que les clusters Amazon Redshift associés aux clusters d'éditeurs et d'abonnés répondent à toutes les exigences relatives au partage de données Amazon Redshift afin qu'Amazon puisse gérer l'accès aux tables et DataZone aux vues Redshift. Consultez la section Concepts de partage de données pour Amazon Redshift.
- Amazon prend DataZone uniquement en charge la gestion des accès pour les ressources publiées depuis Amazon AWS Glue Data Catalog Redshift et Amazon Redshift. Pour tous les autres actifs, tels que les objets Amazon S3, Amazon DataZone ne gère pas l'accès des abonnés approuvés. Si vous vous abonnez à ces actifs non gérés, le message suivant vous en informe :

  ```
  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.
  ```

Publier un actif

Si vous n'avez pas choisi de rendre les actifs immédiatement détectables dans le catalogue de données lorsque vous avez créé une source de données, effectuez les étapes suivantes pour les publier ultérieurement.

Pour publier un actif

1. Accédez à l'URL du portail de DataZone données Amazon et connectez-vous à l'aide de l'authentification unique (SSO) ou de vos AWS informations d'identification. Si vous êtes un DataZone administrateur Amazon, vous pouvez accéder à la DataZone console Amazon à l'adresse https://console.aws.amazon.com/datazone et vous connecter avec l'adresse Compte AWS où le domaine a été créé, puis choisir Open data portal.

2. Choisissez Sélectionner un projet dans le volet de navigation supérieur et sélectionnez le projet auquel appartient la ressource.
3. Accédez à l'onglet Données du projet.
4. Choisissez Données d'inventaire dans le volet de navigation de gauche, puis sélectionnez la ressource que vous souhaitez publier.

> **Note**
>
> Par défaut, toutes les ressources nécessitent une approbation d'abonnement, ce qui signifie que le propriétaire des données doit approuver toutes les demandes d'abonnement à la ressource. Si vous souhaitez modifier ce paramètre avant de publier la ressource, ouvrez les détails de la ressource et choisissez Modifier à côté de l'option Approbation de l'abonnement. Vous pouvez modifier ce paramètre ultérieurement en modifiant et en republiant la ressource.

5. Choisissez Publier la ressource. La ressource est directement publiée dans le catalogue.

   Si vous apportez des modifications à la ressource, par exemple en modifiant ses exigences d'approbation, vous pouvez choisir Republier pour publier les mises à jour du catalogue.

Gérez l'inventaire et organisez les actifs

Pour pouvoir utiliser Amazon DataZone pour cataloguer vos données, vous devez d'abord les importer (actifs) en tant qu'inventaire de votre projet sur Amazon DataZone. La création d'un inventaire pour un projet particulier rend les actifs accessibles uniquement aux membres de ce projet.

Une fois les actifs créés dans l'inventaire du projet, leurs métadonnées peuvent être conservées. Par exemple, vous pouvez modifier le nom et la description de la ressource ou me lire. Chaque modification de la ressource crée une nouvelle version de la ressource. Vous pouvez utiliser l'onglet Historique de la page de détails de la ressource pour afficher toutes les versions de la ressource.

Vous pouvez modifier la section Lisez-moi et ajouter des descriptions détaillées à la ressource. La section Read Me prend en charge le markdown, vous permettant ainsi de mettre en forme vos descriptions selon vos besoins et de décrire les informations clés sur un actif aux consommateurs.

Les termes du glossaire peuvent être ajoutés au niveau des actifs en remplissant les formulaires disponibles.

Pour modifier le schéma, vous pouvez consulter les colonnes, ajouter des noms commerciaux, des descriptions et ajouter des termes de glossaire au niveau des colonnes.

Si la génération automatique de métadonnées est activée lors de la création de la source de données, les noms commerciaux des actifs et des colonnes peuvent être examinés, acceptés ou rejetés individuellement ou en une seule fois.

Vous pouvez également modifier les conditions d'abonnement pour spécifier si l'approbation de la ressource est requise ou non.

Les formulaires de métadonnées d'Amazon vous DataZone permettent d'étendre le modèle de métadonnées d'un actif de données en ajoutant des attributs personnalisés (par exemple, région de vente, année de vente et trimestre de vente). Les formulaires de métadonnées attachés à un type de ressource sont appliqués à toutes les ressources créées à partir de ce type de ressource. Vous pouvez également ajouter des formulaires de métadonnées supplémentaires à des ressources individuelles dans le cadre de l'exécution de la source de données ou après sa création. Pour créer de nouveaux formulaires, voirthe section called “Création, modification ou suppression de formulaires de métadonnées”.

Pour mettre à jour les métadonnées d'une ressource, vous devez être le propriétaire ou le contributeur du projet auquel appartient la ressource.

Pour mettre à jour les métadonnées d'un actif

1. Accédez à l'URL du portail de DataZone données Amazon et connectez-vous à l'aide de l'authentification unique (SSO) ou de vos AWS informations d'identification. Si vous êtes un DataZone administrateur Amazon, vous pouvez accéder à la DataZone console Amazon à l'adresse https://console.aws.amazon.com/datazone et vous connecter avec l'adresse Compte AWS où le domaine a été créé, puis choisir Open data portal.
2. Choisissez Sélectionner un projet dans le volet de navigation supérieur et sélectionnez le projet contenant la ressource dont vous souhaitez mettre à jour les métadonnées.
3. Accédez à l'onglet Données du projet.
4. Choisissez Données d'inventaire dans le volet de navigation de gauche, puis choisissez le nom de la ressource dont vous souhaitez mettre à jour les métadonnées.
5. Sur la page des détails de la ressource, sous Formulaires de métadonnées, choisissez Modifier et modifiez les formulaires existants selon vos besoins. Vous pouvez également joindre des formulaires de métadonnées supplémentaires à la ressource. Pour plus d'informations, consultez the section called “Joindre des formulaires de métadonnées supplémentaires aux ressources”.

6. Lorsque vous avez terminé de faire des mises à jour, choisissez Enregistrer le formulaire.

   Lorsque vous enregistrez le formulaire, Amazon DataZone génère une nouvelle version d'inventaire de l'actif. Pour publier la version mise à jour dans le catalogue, sélectionnez Republier la ressource.

Joindre des formulaires de métadonnées supplémentaires aux ressources

Par défaut, les formulaires de métadonnées attachés à un domaine sont attachés à toutes les ressources publiées sur ce domaine. Les éditeurs de données peuvent associer des formulaires de métadonnées supplémentaires à des ressources individuelles afin de fournir un contexte supplémentaire.

Pour joindre des formulaires de métadonnées supplémentaires à une ressource

1. Accédez à l'URL du portail de DataZone données Amazon et connectez-vous à l'aide de l'authentification unique (SSO) ou de vos AWS informations d'identification. Si vous êtes un DataZone administrateur Amazon, vous pouvez accéder à la DataZone console Amazon à l'adresse https://console.aws.amazon.com/datazone et vous connecter avec l'adresse Compte AWS où le domaine a été créé, puis choisir Open data portal.
2. Choisissez Sélectionner un projet dans le volet de navigation supérieur et sélectionnez le projet contenant la ressource dont vous souhaitez ajouter les métadonnées.
3. Accédez à l'onglet Données du projet.
4. Choisissez Données d'inventaire dans le volet de navigation de gauche, puis choisissez le nom de la ressource dont vous souhaitez ajouter les métadonnées.
5. Sur la page des détails de la ressource, sous Formulaires de métadonnées, sélectionnez Ajouter des formulaires.
6. Sélectionnez le ou les formulaires à ajouter à la ressource, puis choisissez Ajouter des formulaires.
7. Entrez des valeurs pour chacun des champs de métadonnées, puis choisissez Enregistrer le formulaire.

   Lorsque vous enregistrez le formulaire, Amazon DataZone génère une nouvelle version d'inventaire de l'actif. Pour publier la version mise à jour dans le catalogue, sélectionnez Republier la ressource.

Publier la ressource dans le catalogue après curation

Une fois satisfait de la curation des actifs, le propriétaire des données peut publier une version des actifs dans le DataZone catalogue Amazon et ainsi la rendre visible par tous les utilisateurs du domaine. La ressource indique la version d'inventaire et la version publiée. Dans le catalogue de découverte, seule la dernière version publiée apparaît. Si les métadonnées sont mises à jour après la publication, une nouvelle version de l'inventaire sera disponible pour publication dans le catalogue.

Création manuelle d'un actif

Dans Amazon DataZone, un actif est une entité qui présente un seul objet de données physique (par exemple, un tableau, un tableau de bord, un fichier) ou un objet de données virtuel (par exemple, une vue). Pour plus d'informations, consultez DataZone Terminologie et concepts d'Amazon.
La publication manuelle d'une ressource est une opération ponctuelle. Vous ne spécifiez pas de calendrier d'exécution pour l'actif. Il n'est donc pas mis à jour automatiquement si sa source change.

Pour créer manuellement une ressource par le biais d'un projet, vous devez être le propriétaire ou le contributeur de ce projet.

Pour créer un actif manuellement

1. Accédez à l'URL du portail de DataZone données Amazon et connectez-vous à l'aide de l'authentification unique (SSO) ou de vos AWS informations d'identification. Si vous êtes un DataZone administrateur Amazon, vous pouvez accéder à la DataZone console Amazon à l'adresse https://console.aws.amazon.com/datazone et vous connecter avec l'adresse Compte AWS où le domaine a été créé, puis choisir Open data portal.
2. Choisissez Sélectionner un projet dans le volet de navigation supérieur et sélectionnez le projet pour lequel vous souhaitez créer la ressource.
3. Accédez à l'onglet Données du projet.
4. Choisissez Sources de données dans le volet de navigation de gauche, puis choisissez Créer une ressource de données.
5. Pour obtenir des informations détaillées sur les actifs, configurez les paramètres suivants :

   - Type d'actif : type d'actif.
   - Nom : nom de la ressource.
   - Description — Description de l'actif.

6. Pour l'emplacement S3, entrez le nom de ressource Amazon (ARN) du compartiment S3 source.

   Entrez éventuellement un point d'accès S3. Pour plus d'informations, veuillez consulter la rubrique Gestion de l'accès aux données à l'aide des points d'accès Amazon S3.

7. Pour les paramètres de publication, choisissez si les actifs sont immédiatement détectables dans le catalogue. Si vous les ajoutez uniquement à l'inventaire, vous pourrez choisir les conditions d'abonnement ultérieurement pour les publier dans le catalogue.

8. Choisissez Créer.

   Une fois la ressource créée, elle sera soit directement publiée en tant que ressource active dans le catalogue, soit stockée dans l'inventaire jusqu'à ce que vous décidiez de la publier.

Dépublier un actif du catalogue Amazon DataZone

Lorsque vous dépubliez une DataZone ressource Amazon du catalogue, elle n'apparaît plus dans les résultats de recherche globaux. Les nouveaux utilisateurs ne pourront pas trouver ou s'abonner à la liste des actifs dans le catalogue, mais tous les abonnements existants resteront les mêmes.

Pour dépublier une ressource, vous devez être le propriétaire ou le contributeur du projet auquel la ressource appartient :

Pour dépublier un actif

1. Accédez à l'URL du portail de DataZone données Amazon et connectez-vous à l'aide de l'authentification unique (SSO) ou de vos AWS informations d'identification. Si vous êtes un DataZone administrateur Amazon, vous pouvez accéder à la DataZone console Amazon à l'adresse https://console.aws.amazon.com/datazone et vous connecter avec l'adresse Compte AWS où le domaine a été créé, puis choisir Open data portal.
2. Choisissez Sélectionner un projet dans le volet de navigation supérieur et sélectionnez le projet auquel appartient la ressource.
3. Accédez à l'onglet Données du projet.
4. Choisissez Données publiées dans le volet de navigation de gauche.
5. Recherchez la ressource dans la liste des ressources publiées, puis choisissez Dépublier.

   La ressource est supprimée du catalogue. Vous pouvez republier la ressource à tout moment en choisissant Publier.

Supprimer un DataZone actif Amazon

Lorsque vous n'avez plus besoin d'un actif sur Amazon DataZone, vous pouvez le supprimer définitivement. La suppression d'une ressource est différente de la dépublication d'une ressource du catalogue. Vous pouvez supprimer une ressource et sa liste associée dans le catalogue afin qu'elle ne soit visible dans aucun résultat de recherche. Pour supprimer la liste des actifs, vous devez d'abord révoquer tous ses abonnements.

Pour supprimer un actif, vous devez être le propriétaire ou le contributeur du projet auquel appartient l'actif :

> **Note**
>
> Pour supprimer une liste d'actifs, vous devez d'abord révoquer tous les abonnements existants à l'actif. Vous ne pouvez pas supprimer une liste d'actifs qui compte déjà des abonnés.

Pour supprimer un actif

1. Accédez à l'URL du portail de DataZone données Amazon et connectez-vous à l'aide de l'authentification unique (SSO) ou de vos AWS informations d'identification. Si vous êtes un DataZone administrateur Amazon, vous pouvez accéder à la DataZone console Amazon à l'adresse https://console.aws.amazon.com/datazone et vous connecter avec l'adresse Compte AWS où le domaine a été créé, puis choisir Open data portal.
2. Choisissez Sélectionner un projet dans le volet de navigation supérieur et sélectionnez le projet contenant la ressource que vous souhaitez supprimer.
3. Accédez à l'onglet Données du projet.
4. Choisissez Données publiées dans le volet de navigation de gauche, puis recherchez et choisissez la ressource que vous souhaitez supprimer. Cela ouvre la page de détails de l'actif.
5. Choisissez Actions, Supprimer et confirmez la suppression.

   Une fois la ressource supprimée, elle n'est plus disponible et les utilisateurs ne peuvent plus s'y abonner.

Lancer manuellement l'exécution d'une source de données dans Amazon DataZone

Lorsque vous exécutez une source de données, Amazon DataZone extrait toutes les métadonnées nouvelles ou modifiées de la source et met à jour les actifs associés dans l'inventaire. Lorsque vous ajoutez une source de données à Amazon DataZone, vous spécifiez la préférence d'exécution de la source, qui définit si la source s'exécute selon un calendrier ou à la demande. Si votre source s'exécute à la demande, vous devez lancer une exécution manuelle de la source de données.

Même si votre source s'exécute selon un calendrier, vous pouvez toujours l'exécuter manuellement à tout moment. Après avoir ajouté des métadonnées commerciales aux actifs, vous pouvez sélectionner des actifs et les publier dans le DataZone catalogue Amazon afin que tous les utilisateurs du domaine puissent les découvrir. Seuls les actifs publiés sont consultables par les autres utilisateurs du domaine.

Pour exécuter une source de données manuellement

1. Accédez à l'URL du portail de DataZone données Amazon et connectez-vous à l'aide de l'authentification unique (SSO) ou de vos AWS informations d'identification. Si vous êtes un DataZone administrateur Amazon, vous pouvez accéder à la DataZone console Amazon à l'adresse https://console.aws.amazon.com/datazone et vous connecter avec l'adresse Compte AWS où le domaine a été créé, puis choisir Open data portal.
2. Choisissez Sélectionner un projet dans le volet de navigation supérieur et sélectionnez le projet auquel appartient la source de données.
3. Accédez à l'onglet Données du projet.
4. Choisissez Sources de données dans le volet de navigation de gauche, puis localisez et choisissez la source de données que vous souhaitez exécuter. Cela ouvre la page de détails de la source de données.
5. Choisissez Exécuter à la demande.

   Le statut de la source de données change au `Running` fur et à mesure qu'Amazon DataZone met à jour les métadonnées des actifs avec les données les plus récentes de la source. Vous pouvez surveiller l'état de l'exécution dans l'onglet Exécutions de la source de données.

Révisions des actifs sur Amazon DataZone

Amazon DataZone augmente la révision d'un actif lorsque vous modifiez ses métadonnées commerciales ou techniques. Ces modifications incluent la modification du nom de la ressource, de la description, des termes du glossaire, des noms de colonnes, des formulaires de métadonnées et des valeurs des champs de formulaires de métadonnées. Ces modifications peuvent résulter de modifications manuelles, de l'exécution de tâches de source de données ou d'opérations d'API. Amazon génère DataZone automatiquement une nouvelle révision d'actif chaque fois que vous apportez une modification à l'actif.

Une fois que vous avez mis à jour une ressource et qu'une nouvelle révision a été générée, vous devez publier la nouvelle révision dans le catalogue pour qu'elle soit mise à jour et disponible pour les abonnés. Pour plus d'informations, consultez the section called "Publier des actifs dans le catalogue à partir de l'inventaire du projet". Vous ne pouvez publier que la version la plus récente d'une ressource dans le catalogue.

Pour consulter les révisions passées d'un actif

1. Accédez à l'URL du portail de DataZone données Amazon et connectez-vous à l'aide de l'authentification unique (SSO) ou de vos AWS informations d'identification. Si vous êtes un DataZone administrateur Amazon, vous pouvez accéder à la DataZone console Amazon à l'adresse https://console.aws.amazon.com/datazone et vous connecter avec l'adresse Compte AWS où le domaine a été créé, puis choisir Open data portal.
2. Choisissez Sélectionner un projet dans le volet de navigation supérieur et sélectionnez le projet contenant la ressource.
3. Accédez à l'onglet Données du projet, puis localisez et sélectionnez la ressource. Cela ouvre la page de détails de l'actif.
4. Accédez à l'onglet Historique, qui affiche la liste des révisions passées de la ressource.

Qualité des données sur Amazon DataZone

Les indicateurs de qualité des données d'Amazon vous DataZone aident à comprendre les différents indicateurs de qualité tels que l'exhaustivité, l'actualité et l'exactitude de vos sources de données. Amazon DataZone s'intègre à AWS Glue Data Quality et propose des API pour intégrer les indicateurs de qualité des données issus de solutions de qualité des données tierces. Les utilisateurs des données peuvent voir comment les indicateurs de qualité des données évoluent au fil du temps

pour les actifs auxquels ils ont souscrit. Pour créer et appliquer les règles de qualité des données, vous pouvez utiliser l'outil de qualité des données de votre choix, tel que AWS Glue data quality. Grâce aux indicateurs de qualité des données d'Amazon DataZone, les consommateurs de données peuvent visualiser les scores de qualité des données pour les actifs et les colonnes, ce qui contribue à renforcer la confiance dans les données qu'ils utilisent pour prendre des décisions.

Conditions préalables et modifications des rôles IAM

Si vous utilisez les politiques AWS gérées DataZone d'Amazon, aucune étape de configuration supplémentaire n'est requise et ces politiques gérées sont automatiquement mises à jour pour garantir la qualité des données. Si vous utilisez vos propres politiques pour les rôles qui accordent à Amazon les autorisations requises pour interagir avec DataZone les services pris en charge, vous devez mettre à jour les politiques associées à ces rôles afin de permettre la lecture des informations sur la qualité des données de AWS Glue dans le AWS politique gérée : AmazonDataZoneGlueManageAccessRolePolicy et de permettre la prise en charge des API de séries chronologiques dans le AWS politique gérée : AmazonDataZoneDomainExecutionRolePolicy et leAWS politique gérée : AmazonDataZoneFullUserAccess.

Permettre la qualité des données pour les actifs AWS de Glue

Amazon DataZone extrait les indicateurs de qualité des données de AWS Glue afin de fournir du contexte à un moment donné, par exemple lors d'une recherche dans un catalogue de données commerciales. Les utilisateurs des données peuvent voir comment les indicateurs de qualité des données évoluent au fil du temps pour les actifs auxquels ils ont souscrit. Les producteurs de données peuvent ingérer les scores de qualité des données de AWS Glue selon un calendrier. Le catalogue de données Amazon DataZone Business peut également afficher des indicateurs de qualité des données provenant de systèmes tiers via des API de qualité des données. Pour plus d'informations, voir AWS Glue Data Quality et Getting started with AWS Glue Data Quality pour le catalogue de données.

Vous pouvez activer les mesures de qualité des données pour vos DataZone actifs Amazon de différentes manières :

- Utilisez le Data Portal ou les DataZone API Amazon pour garantir la qualité des données de votre source de données AWS Glue via le portail de données Amazon, soit lors de la création d'une nouvelle source de DataZone données Glue, soit lors de la modification d'une source de données AWS Glue existante.

Pour plus d'informations sur l'activation de la qualité des données pour une source de données via le portail, consultez Créez et exécutez une source DataZone de données Amazon pour AWS Glue Data Catalog etGérez les sources de DataZone données Amazon existantes.

> **Note**
>
> Vous pouvez utiliser le portail de données pour activer la qualité des données uniquement pour vos actifs d'inventaire AWS Glue. Dans cette version d'Amazon, l' DataZone activation de la qualité des données pour Amazon Redshift ou de types personnalisés de ressources via le portail de données n'est pas prise en charge.

Vous pouvez également utiliser les API pour améliorer la qualité des données pour vos sources de données nouvelles ou existantes. Vous pouvez le faire en invoquant le CreateDataSourceou UpdateDataSourceet en réglant le `autoImportDataQualityResult` paramètre sur « Vrai ».

Une fois la qualité des données activée, vous pouvez exécuter la source de données à la demande ou selon un calendrier. Chaque exécution peut générer jusqu'à 100 mesures par actif. Il n'est pas nécessaire de créer des formulaires ou d'ajouter des métriques manuellement lors de l'utilisation d'une source de données pour garantir la qualité des données. Lorsque l'actif est publié, les mises à jour apportées au formulaire de qualité des données (jusqu'à 30 points de données par règle d'historique) sont reflétées dans la liste destinée aux consommateurs. Par la suite, chaque nouvel ajout de métriques à l'actif est automatiquement ajouté à la liste. Il n'est pas nécessaire de republier la ressource pour mettre les derniers scores à la disposition des consommateurs.

Permettre la qualité des données pour les types d'actifs personnalisés

Vous pouvez utiliser les DataZone API Amazon pour garantir la qualité des données pour tous vos types d'actifs personnalisés. Pour plus d'informations, consultez les ressources suivantes :

- PostTimeSeriesDataPoints
- ListTimeSeriesDataPoints
- GetTimeSeriesDataPoint
- DeleteTimeSeriesDataPoints

Les étapes suivantes fournissent un exemple d'utilisation d'API ou de CLI pour importer des métriques tierces pour vos actifs sur Amazon DataZone :

1. Appelez l'`PostTimeSeriesDataPoints`API comme suit :

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

avec la charge utile suivante :

```
{
"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. Appelez l'`DeleteTimeSeriesDataPoints`API comme suit :

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

Utilisation de l'apprentissage automatique et de l'IA générative

> **Note**
>
> Propulsé par Amazon Bedrock : AWS implémente la détection automatique des abus. Comme les recommandations de l'IA pour les fonctionnalités de description dans Amazon DataZone sont basées sur Amazon Bedrock, les utilisateurs héritent des contrôles mis en œuvre dans Amazon Bedrock pour renforcer la sûreté, la sécurité et l'utilisation responsable de l'IA.

Dans la version actuelle d'Amazon DataZone, vous pouvez utiliser la fonctionnalité de recommandations de l'IA pour les descriptions afin d'automatiser la découverte et le catalogage des données. Support de l'IA générative et de l'apprentissage automatique dans Amazon : DataZone création de descriptions pour les actifs et les colonnes. Vous pouvez utiliser ces descriptions pour

ajouter un contexte métier à vos données et recommander des analyses pour les ensembles de données, ce qui peut contribuer à améliorer les résultats de découverte des données.

Basées sur les grands modèles linguistiques d'Amazon Bedrock, les recommandations de l'IA pour les descriptions des actifs de données dans Amazon vous DataZone aident à garantir que vos données sont compréhensibles et faciles à découvrir. Les recommandations de l'IA suggèrent également les applications analytiques les plus pertinentes pour les ensembles de données. En réduisant les tâches manuelles de documentation et en vous conseillant sur l'utilisation appropriée des données, les descriptions générées automatiquement peuvent vous aider à améliorer la fiabilité de vos données et à minimiser le fait de négliger des données importantes afin d'accélérer la prise de décisions éclairées.

> **Important**
>
> Dans la DataZone version actuelle d'Amazon, la fonctionnalité de recommandations basées sur l'IA pour les descriptions n'est prise en charge que dans les régions suivantes :
>
> - USA Est (Virginie du Nord)
> - USA Ouest (Oregon)
> - Europe (Francfort)
> - Asie-Pacifique (Tokyo)

La procédure suivante explique comment générer des recommandations basées sur l'IA pour les descriptions dans Amazon DataZone :

1. Accédez à l'URL du portail de DataZone données Amazon, puis connectez-vous à l'aide de l'authentification unique (SSO) ou de vos AWS informations d'identification. Si vous êtes un DataZone administrateur Amazon, accédez à la DataZone console Amazon à l'adresse https://console.aws.amazon.com/datazone et connectez-vous avec l' Compte AWS endroit où le domaine a été créé, puis choisissez Open data portal.
2. Dans le volet de navigation supérieur, choisissez Sélectionner un projet, puis choisissez le projet contenant la ressource pour laquelle vous souhaitez générer des recommandations d'IA pour les descriptions.
3. Accédez à l'onglet Données du projet.

4. Dans le volet de navigation de gauche, choisissez Données d'inventaire, puis choisissez le nom de la ressource pour laquelle vous souhaitez générer des recommandations d'IA pour les descriptions de la ressource.
5. Sur la page de détails de la ressource, dans l'onglet Métadonnées commerciales, choisissez Générer des descriptions.
6. Une fois les descriptions générées, vous pouvez les modifier, les accepter ou les rejeter. Des icônes vertes sont affichées à côté de chaque description de métadonnées générée automatiquement pour la ressource de données. Dans l'onglet Métadonnées commerciales, vous pouvez choisir l'icône verte à côté du résumé généré automatiquement, puis choisir Modifier, Accepter ou Rejeter pour répondre à la description générée. Vous pouvez également choisir Accepter tout ou Rejeter toutes les options affichées en haut de la page lorsque l'onglet Métadonnées commerciales est sélectionné, et ainsi exécuter l'action sélectionnée sur toutes les descriptions générées automatiquement.

   Vous pouvez également choisir l'onglet Schéma, puis traiter individuellement les descriptions générées automatiquement en choisissant l'icône verte pour une description de colonne à la fois, puis en choisissant Accepter ou Rejeter. Dans l'onglet Schéma, vous pouvez également choisir Tout accepter ou Tout rejeter et ainsi exécuter l'action sélectionnée sur toutes les descriptions générées automatiquement.
7. Pour publier la ressource dans le catalogue avec les descriptions générées, choisissez Publier la ressource, puis confirmez cette action en choisissant à nouveau Publier la ressource dans la fenêtre contextuelle Publier la ressource.

> **Note**
>
> Si vous n'acceptez pas ou ne rejetez pas les descriptions générées pour une ressource, puis que vous publiez cette ressource, les métadonnées générées automatiquement et non révisées ne sont pas incluses dans la ressource de données publiée.

Découvrir, s'abonner et consommer des données sur Amazon DataZone

Sur Amazon DataZone, une fois qu'un actif est publié sur un domaine, les abonnés peuvent le découvrir et demander un abonnement à cet actif. Le processus d'abonnement commence lorsque l'abonné recherche et parcourt le catalogue pour trouver l'actif qu'il souhaite. Depuis le DataZone portail Amazon, ils choisissent de s'abonner à l'actif en soumettant une demande d'abonnement incluant une justification et le motif de la demande. L'approbateur d'abonnement, tel que défini dans le contrat de publication, examine ensuite la demande d'accès. Ils peuvent approuver ou rejeter la demande.

Une fois l'abonnement accordé, un processus de traitement des commandes démarre afin de faciliter l'accès à l'actif pour l'abonné. Il existe deux principaux modes de contrôle d'accès et de traitement des actifs : ceux pour les actifs DataZone gérés par Amazon et ceux pour les actifs qui ne sont pas gérés par Amazon DataZone.

- Ressources gérées : Amazon DataZone peut gérer le traitement des commandes et les autorisations pour les actifs gérés, tels que AWS Glue les tables et les tables et vues Amazon Redshift.
- Actifs non gérés : Amazon DataZone publie des événements standard liés à vos actions (par exemple, l'approbation donnée à une demande d'abonnement) sur Amazon EventBridge. Vous pouvez utiliser ces événements standard pour intégrer d'autres AWS services ou des solutions tierces pour des intégrations personnalisées.

Rubriques

Découvrir des données

Les tâches suivantes décrivent les différentes manières de découvrir des données sur Amazon DataZone.

Rubriques

Rechercher et consulter des actifs dans le catalogue

Amazon DataZone propose un moyen simplifié de rechercher des données. Tout DataZone utilisateur Amazon autorisé à accéder au portail de données peut rechercher des actifs dans le DataZone catalogue Amazon et consulter les noms des actifs ainsi que les métadonnées qui leur sont attribuées. Vous pouvez examiner un actif de plus près en consultant sa page de détails.

> **Note**
>
> Pour consulter les données réelles contenues dans une ressource, vous devez d'abord vous abonner à la ressource, faire approuver votre demande d'abonnement et obtenir l'accès accordé. Pour plus d'informations, consultez Abonnement aux données.

Pour rechercher des actifs dans le catalogue

1. Accédez à l'URL du portail de DataZone données Amazon et connectez-vous à l'aide de l'authentification unique (SSO) ou de vos AWS informations d'identification. Si vous êtes un DataZone administrateur Amazon, vous pouvez accéder à la DataZone console Amazon à l'adresse https://console.aws.amazon.com/datazone et vous connecter avec l'adresse Compte AWS où le domaine a été créé, puis choisir Open data portal.
2. Vous pouvez saisir le nom de la ressource que vous recherchez dans la barre de recherche de la page d'accueil du portail de données.
3. Pour parcourir les espaces de noms, choisissez Catalogue en haut à droite de la page pour ouvrir le catalogue. Le catalogue propose une expérience de recherche à facettes qui vous permet de trouver des actifs en effectuant une recherche selon des critères tels que le propriétaire des données et les termes du glossaire.
4. Entrez votre terme de recherche dans l'un des champs de recherche. Après avoir effectué une recherche, vous pouvez appliquer différents filtres pour affiner les résultats. Les filtres incluent le type d'actif, le compte source et le type d'actif Région AWS auquel appartient l'actif.
5. Pour afficher les détails d'une ressource spécifique, sélectionnez la ressource pour ouvrir sa page de détails. La page de détails contient les informations suivantes :

- Le nom de la ressource, la source de données (AWS Glue Amazon Redshift ou Amazon S3), le type (table, vue ou objet S3), le nombre de colonnes et la taille.
- Description de l'actif.
- La version publiée en cours de la ressource, le propriétaire, si une approbation est requise pour les abonnements, le namepace et l'historique des mises à jour.
- Un onglet Aperçu qui inclut les termes du glossaire et les formulaires de métadonnées.
- Un onglet Schéma qui affiche le schéma de la ressource, y compris les noms des colonnes commerciales et techniques, les types de données et les descriptions commerciales des colonnes. L'onglet Schéma n'est visible que pour les tables et les vues (pas pour les objets Amazon S3).
- Un onglet Abonnements qui inclut une liste des abonnés au domaine.
- Un onglet Historique qui inclut une liste des révisions passées de la ressource.

Abonnement aux données

Les tâches suivantes fournissent des informations sur la souscription à des actifs sur Amazon DataZone.

Rubriques

Demander un abonnement à des actifs

Amazon vous DataZone permet de rechercher, d'accéder et de consommer les actifs du DataZone catalogue Amazon. Lorsque vous trouvez une ressource dans le catalogue à laquelle vous souhaitez accéder, vous devez vous y abonner, ce qui crée une demande d'abonnement. Un approbateur peut ensuite approuver ou demander votre demande.

Vous devez être membre d'un projet pour demander un abonnement à un actif de ce projet.

Pour souscrire à un actif

1. Accédez à l'URL du portail de DataZone données Amazon et connectez-vous à l'aide de l'authentification unique (SSO) ou de vos AWS informations d'identification. Si vous êtes un DataZone administrateur Amazon, vous pouvez accéder à la DataZone console Amazon à l'adresse https://console.aws.amazon.com/datazone et vous connecter avec l'adresse Compte AWS où le domaine a été créé, puis choisir Open data portal.
2. Utilisez la barre de recherche pour rechercher et choisir la ressource à laquelle vous souhaitez vous abonner, puis choisissez S'abonner.
3. Dans la fenêtre contextuelle S'abonner, saisissez les informations suivantes :
   - Le projet auquel vous souhaitez souscrire à la ressource.
   - Brève justification de votre demande d'abonnement.
4. Choisissez Souscrire.

   Vous recevez une notification sur le portail de données lorsque l'éditeur approuve votre demande.

Pour consulter le statut de la demande d'abonnement, recherchez et choisissez le projet avec lequel vous vous êtes abonné à la ressource. Accédez à l'onglet Données du projet, puis choisissez Données demandées dans le volet de navigation de gauche. Cette page répertorie les actifs auxquels le projet a demandé l'accès. Vous pouvez filtrer la liste en fonction du statut de la demande.

Approuver ou rejeter une demande d'abonnement

Amazon vous DataZone permet de rechercher, d'accéder et de consommer les actifs du DataZone catalogue Amazon. Lorsque vous trouvez une ressource dans le catalogue à laquelle vous souhaitez accéder, vous devez vous y abonner, ce qui crée une demande d'abonnement. Un approbateur peut ensuite approuver ou rejeter votre demande.

Vous devez être membre du projet propriétaire (le projet qui a publié la ressource) pour approuver ou rejeter une demande d'abonnement.

Pour approuver ou rejeter une demande d'abonnement

1. Accédez à l'URL du portail de DataZone données Amazon et connectez-vous à l'aide de l'authentification unique (SSO) ou de vos AWS informations d'identification. Si vous êtes un DataZone administrateur Amazon, vous pouvez accéder à la DataZone console Amazon

à l'adresse https://console.aws.amazon.com/datazone et vous connecter avec l'adresse Compte AWS où le domaine a été créé, puis choisir Open data portal.

2. Dans le portail de données, choisissez Parcourir la liste des projets et sélectionnez le projet contenant la ressource avec la demande d'abonnement.
3. Accédez à l'onglet Données, puis sélectionnez Demandes entrantes dans le volet de navigation de gauche.
4. Localisez la demande et choisissez Afficher la demande. Vous pouvez filtrer par En attente pour ne voir que les demandes encore ouvertes.
5. Passez en revue la demande d'abonnement et le motif de l'accès, puis décidez de l'approuver ou de la rejeter.
6. (Facultatif) Entrez une réponse expliquant les raisons pour lesquelles vous avez accepté ou rejeté la demande.
7. Choisissez Approuver ou Rejeter.

En tant que propriétaire du projet, vous pouvez révoquer l'abonnement à tout moment. Pour plus d'informations, consultez the section called "Révoquer un abonnement existant".

Pour consulter toutes les demandes d'abonnement, voirUtilisation des DataZone événements et des notifications Amazon.

Révoquer un abonnement existant

Amazon vous DataZone permet de rechercher, d'accéder et de consommer les actifs du DataZone catalogue Amazon. Lorsque vous trouvez une ressource dans le catalogue à laquelle vous souhaitez accéder, vous devez vous y abonner, ce qui crée une demande d'abonnement. Un approbateur peut ensuite approuver ou demander votre demande. Il se peut que vous deviez révoquer un abonnement après l'avoir approuvé, soit parce que l'approbation était une erreur, soit parce que l'abonné n'a plus besoin d'accéder à l'actif.

Vous devez être membre du projet propriétaire (le projet qui a publié la ressource) pour révoquer un abonnement.

Pour révoquer un abonnement

1. Accédez à l'URL du portail de DataZone données Amazon et connectez-vous à l'aide de l'authentification unique (SSO) ou de vos AWS informations d'identification. Si vous êtes un

DataZone administrateur Amazon, vous pouvez accéder à la DataZone console Amazon à l'adresse https://console.aws.amazon.com/datazone et vous connecter avec l'adresse Compte AWS où le domaine a été créé, puis choisir Open data portal.

2. Choisissez Sélectionner un projet dans le volet de navigation supérieur et sélectionnez le projet contenant l'abonnement que vous souhaitez révoquer.
3. Accédez à l'onglet Données, puis sélectionnez Demandes entrantes dans le volet de navigation de gauche.
4. Localisez l'abonnement que vous souhaitez révoquer et choisissez Afficher l'abonnement.
5. (Facultatif) Cochez la case pour permettre à l'abonné de conserver l'actif dans les objectifs d'abonnement du projet. Un objectif d'abonnement est une référence à un ensemble de ressources où les données souscrites peuvent être mises à disposition dans un environnement.

   Si vous souhaitez révoquer ultérieurement l'accès à la ressource depuis la cible d'abonnement, vous devez le faire dans AWS Lake Formation.
6. Choisissez Révoquer l'abonnement.

Vous ne pouvez pas réapprouver un abonnement après l'avoir révoqué. L'abonné doit s'abonner à nouveau à la ressource pour que vous puissiez l'approuver.

Annuler une demande d'abonnement

Amazon vous DataZone permet de rechercher, d'accéder et de consommer les actifs du DataZone catalogue Amazon. Lorsque vous trouvez une ressource dans le catalogue à laquelle vous souhaitez accéder, vous devez vous y abonner, ce qui crée une demande d'abonnement. Un approbateur peut ensuite approuver ou demander votre demande. Vous devrez peut-être annuler une demande d'abonnement en attente, soit parce que vous l'avez soumise par erreur, soit parce que vous n'avez plus besoin d'un accès en lecture à la ressource.

Pour annuler une demande d'abonnement, vous devez être propriétaire du projet ou contributeur.

Pour annuler une demande d'abonnement

1. Accédez à l'URL du portail de DataZone données Amazon et connectez-vous à l'aide de l'authentification unique (SSO) ou de vos AWS informations d'identification. Si vous êtes un DataZone administrateur Amazon, vous pouvez accéder à la DataZone console Amazon à l'adresse https://console.aws.amazon.com/datazone et vous connecter avec l'adresse Compte AWS où le domaine a été créé, puis choisir Open data portal.

2. Choisissez Sélectionner un projet dans le volet de navigation supérieur et sélectionnez le projet contenant la demande d'abonnement.
3. Accédez à l'onglet Données du projet, puis choisissez Données demandées dans le volet de navigation de gauche. Cette page répertorie les actifs auxquels le projet a demandé l'accès.
4. Filtrez par Demandé pour ne voir que les demandes toujours en attente. Localisez la demande et choisissez Afficher la demande.
5. Passez en revue la demande d'abonnement et choisissez Annuler la demande.

Si vous souhaitez vous réabonner à la ressource (ou à une autre ressource), consultezthe section called "Demander un abonnement à des actifs".

Se désabonner d'un actif

Amazon vous DataZone permet de rechercher, d'accéder et de consommer les actifs du DataZone catalogue Amazon. Lorsque vous trouvez une ressource dans le catalogue à laquelle vous souhaitez accéder, vous devez vous y abonner, ce qui crée une demande d'abonnement. Un approbateur peut ensuite approuver ou demander votre demande. Il se peut que vous deviez vous désinscrire d'un actif, soit parce que vous vous êtes inscrit par erreur et que vous avez été approuvé, soit parce que vous n'avez plus besoin d'un accès en lecture à l'actif.

Vous devez être membre d'un projet pour vous désinscrire de l'un de ses actifs.

Pour vous désabonner d'un actif

1. Accédez à l'URL du portail de DataZone données Amazon et connectez-vous à l'aide de l'authentification unique (SSO) ou de vos AWS informations d'identification. Si vous êtes un DataZone administrateur Amazon, vous pouvez accéder à la DataZone console Amazon à l'adresse https://console.aws.amazon.com/datazone et vous connecter avec l'adresse Compte AWS où le domaine a été créé, puis choisir Open data portal.
2. Choisissez Sélectionner un projet dans le volet de navigation supérieur et sélectionnez le projet contenant la ressource dont vous souhaitez vous désabonner.
3. Accédez à l'onglet Données du projet, puis choisissez Données demandées dans le volet de navigation de gauche. Cette page répertorie les actifs auxquels le projet a demandé l'accès.
4. Filtrez par Approuvé pour ne voir que les demandes qui ont été approuvées. Localisez la demande et choisissez Afficher l'abonnement.
5. Vérifiez l'abonnement et choisissez Se désabonner.

Si vous souhaitez vous réabonner à la ressource (ou à une autre ressource), consultezthe section called “Demander un abonnement à des actifs”.

Utilisation des rôles IAM existants pour traiter les abonnements Amazon DataZone

Dans la version actuelle, Amazon vous DataZone aide à utiliser vos rôles IAM existants pour accéder aux données. Pour ce faire, vous pouvez créer un objectif d'abonnement dans l' DataZone environnement Amazon que vous utilisez pour exécuter votre abonnement. Pour créer un objectif d'abonnement pour un environnement dans l'un des AWS comptes associés, vous pouvez suivre les étapes suivantes :

Étape 1 : Assurez-vous que votre DataZone domaine Amazon utilise la version 2 ou supérieure de la politique de RAM

1. Accédez à la page Shared by me : Resource shares dans la console AWS RAM.
2. Étant donné que les partages de ressources AWS RAM existent dans des AWS régions spécifiques, choisissez la AWS région appropriée dans la liste déroulante située dans le coin supérieur droit de la console.
3. Sélectionnez le partage de ressources correspondant à votre DataZone domaine Amazon, puis choisissez Modifier. Vous pouvez identifier le partage de RAM pour le DataZone domaine Amazon à l'aide du nom ou de l'ID du domaine, car le partage de RAM est créé avec le nom :`DataZone-<domain-name>-<domain-id>`.
4. Choisissez Next pour passer à l'étape suivante où vous pouvez vérifier la version de la politique de RAM et la modifier.
5. Assurez-vous que la version de la politique de RAM est la version 2 ou supérieure. Si ce n'est pas le cas, utilisez le menu déroulant pour sélectionner la version 2 ou supérieure.
6. Choisissez Passer à l'étape 4 : Révision et mise à jour.
7. Choisissez Mettre à jour le partage de ressources.

Étape 2 : créer un objectif d'abonnement à partir d'un compte associé

- Dans la version actuelle, Amazon DataZone prend en charge la création d'objectifs d'abonnement en utilisant uniquement des API. Vous trouverez ci-dessous quelques exemples de charge utile que vous pouvez utiliser pour créer un objectif d'abonnement afin de satisfaire

les abonnements à vos tables AWS Glue et à vos tables ou vues Amazon Redshift. Pour plus d'informations, consultez CreateSubscriptionTarget.

Exemple d'objectif d'abonnement pour 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"
}
```

Exemple d'objectif d'abonnement pour 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**
>
> - L'EnvironmentIdentifier que vous utilisez dans l'appel d'API ci-dessus doit exister dans le même compte associé à partir duquel vous effectuez l'appel d'API. Dans le cas contraire, l'appel d'API échouera.
> - L'ARN du rôle IAM que vous utilisez dans les « AuthorizedPrincipals » est le rôle auquel Amazon DataZone accordera l'accès après l'ajout d'un actif souscrit à la cible d'abonnement. Ces principaux autorisés doivent appartenir au même compte que l'environnement dans lequel l'objectif d'abonnement est créé.
> - La valeur du champ fournisseur doit être « Amazon DataZone » pour qu'Amazon DataZone puisse terminer le traitement de l'abonnement.
> - Le nom de base de données fourni dans subscriptionTargetConfig doit déjà exister dans le compte dans lequel la cible est créée. Amazon ne DataZone créera pas cette base de données. Assurez-vous également que le rôle de gestion des accès dispose de l'autorisation CREATE TABLE sur cette base de données.
> - Assurez-vous également que les rôles (rôle IAM pour le AWS Glue et rôle de base de données pour Amazon Redshift) fournis en tant que principaux autorisés existent déjà dans le compte d'environnement. Pour les cibles d'abonnement Amazon Redshift, des mises à jour supplémentaires sont requises pour le rôle assumé lors de la connexion au cluster. Ce rôle doit être associé à une RedshiftDbRoles étiquette. La valeur de la balise peut être une liste séparée par des virgules. La valeur doit être le rôle de base de données fourni en tant que principal autorisé lors de la création de la cible d'abonnement.

Étape 3 : Abonnement à une nouvelle table et finalisation de l'abonnement à la nouvelle cible

- Une fois que vous avez créé l'objectif d'abonnement, vous pouvez vous abonner à un nouveau tableau et Amazon l' DataZone atteindra conformément à l'objectif ci-dessus. Pour plus d'informations, consultez Abonnement aux données.

Autoriser l'accès aux données

Les tâches suivantes fournissent des informations détaillées sur l'octroi de l'accès aux abonnements approuvés aux actifs d'Amazon DataZone.

Sur Amazon DataZone, les demandes d'abonnement et les abonnements approuvés ou accordés pour l'accès en lecture aux ressources sont gérés par les approbateurs d'abonnement. L'approbateur d'abonnement pour une ressource est déterminé par le contrat de publication en vertu duquel cette ressource a été publiée dans le DataZone catalogue Amazon.

Rubriques

Accorder l'accès aux AWS Glue Data Catalog actifs gérés

> **Note**
>
> La gestion de l'accès aux AWS Glue Data Catalog actifs à l'aide de la méthode AWS Lake Formation LF-TBAC n'est pas prise en charge.
> Support pour le partage d'actifs entre régions n' AWS Glue Data Catalog est pas pris en charge.

Une fois qu'une demande d'abonnement aux AWS Glue Data Catalog actifs gérés est approuvée, Amazon ajoute DataZone automatiquement ces actifs à tous les environnements de lac de données existants du projet. Amazon accorde et gère DataZone ensuite l'accès aux AWS Glue Data Catalog tables approuvées en votre nom par le biais de AWS Lake Formation. Pour le projet d'abonné, les actifs accordés apparaissent sous AWS Glue Data Catalog forme de ressources sur votre compte. Vous pouvez ensuite utiliser Amazon Athena pour interroger les tables.

> **Note**
>
> Si un nouvel environnement de lac de données est ajouté au projet après que les AWS Glue Data Catalog actifs souscrits ont été automatiquement ajoutés aux environnements de lac de données existants, vous devez ajouter manuellement ces AWS Glue Data Catalog actifs souscrits à ce nouvel environnement de lac de données. Vous pouvez le faire en choisissant l'option Ajouter une subvention dans l'onglet Données de la page de présentation du projet sur le portail de DataZone données Amazon.

Pour qu'Amazon DataZone puisse accorder l'accès aux tables du AWS Glue Data Catalog, les conditions suivantes doivent être remplies.

- La table AWS Glue doit être gérée par Lake Formation, car Amazon DataZone accorde l'accès en gérant les autorisations de Lake Formation.
- Le rôle Manage access pour l'environnement de lac de données utilisé pour publier la table AWS Glue Data Catalog doit disposer des autorisations Lake Formation suivantes :
  - `DESCRIBE`et `DESCRIBE GRANTABLE` des autorisations sur la base de données AWS Glue qui contient la table publiée.
  - `DESCRIBE`,`SELECT`,`DESCRIBE GRANTABLE`, `SELECT GRANTABLE` autorisations dans Lake Formation sur le tableau publié lui-même.

Pour plus d'informations, consultez la section Octroi et révocation d'autorisations sur les ressources du catalogue dans le Guide du AWS Lake Formation développeur.

Accorder l'accès aux actifs gérés par Amazon Redshift

Lorsqu'un abonnement à une table ou à une vue Amazon Redshift est approuvé, Amazon DataZone peut automatiquement ajouter la ressource abonnée à tous les environnements d'entrepôt de données du projet, afin que les membres du projet puissent interroger les données à l'aide du lien de l'éditeur de requêtes Amazon Redshift dans leur environnement. Amazon DataZone crée en sous-main les subventions et les partages de données nécessaires entre la source et la cible de l'abonnement.

Le processus d'octroi de l'accès varie en fonction de l'emplacement de la base de données source (éditeur) et de la base de données cible (abonné).

- Même cluster, même base de données : si les données doivent être partagées au sein de la même base de données, Amazon DataZone accorde les autorisations directement sur la table source.
- Même cluster, base de données différente : si les données doivent être partagées entre deux bases de données au sein du même cluster, Amazon DataZone crée une vue dans la base de données cible et des autorisations sont accordées sur la vue créée.
- Même compte, cluster différent : Amazon DataZone crée un partage de données entre le cluster source et le cluster cible et crée une vue au-dessus de la table partagée. Les autorisations sont accordées sur la vue.

- Compte croisé : comme ci-dessus, mais une étape supplémentaire est requise pour autoriser le partage de données entre comptes du côté du cluster producteur et une autre étape pour associer le partage de données du côté du cluster de consommateurs.

> **Note**
>
> Si un nouvel environnement d'entrepôt de données est ajouté au projet après que les actifs Amazon Redshift souscrits ont été automatiquement ajoutés aux environnements d'entrepôt de données existants, vous devez ajouter manuellement ces actifs Amazon Redshift souscrits à ce nouvel environnement d'entrepôt de données. Vous pouvez le faire en choisissant l'option Ajouter une subvention dans l'onglet Données de la page de présentation du projet sur le portail de DataZone données Amazon.

Assurez-vous que les clusters Amazon Redshift que vous publiez et auxquels vous vous abonnez répondent à toutes les exigences relatives aux partages de données Amazon Redshift. Pour plus d'informations, consultez le guide du développeur Amazon Redshift.

> **Note**
>
> Amazon DataZone prend en charge l'attribution automatique d'abonnements aux actifs Amazon Redshift Cluster et Amazon Redshift Serverless.
> Le partage de données entre régions à l'aide d'Amazon Redshift n'est pas pris en charge.

> **Note**
>
> Dans la version actuelle, Amazon DataZone peut gérer l'accès aux tables et aux vues Amazon Redshift uniquement si la source et les clusters ou groupes de travail Amazon Redshift cibles se trouvent dans les comptes appartenant à AWS la même organisation. AWS

Accorder l'accès aux actifs non gérés pour les abonnements approuvés

Amazon DataZone permet aux utilisateurs de publier n'importe quel type d'actif dans le catalogue de données commerciales. Pour certains de ces actifs, Amazon DataZone peut gérer automatiquement les autorisations d'accès. Ces actifs sont appelés actifs gérés et incluent les tables AWS Glue

Data Catalog gérées par Lake Formation et les tables et vues Amazon Redshift. Tous les autres actifs auxquels Amazon ne DataZone peut pas automatiquement octroyer des abonnements sont considérés comme non gérés.

Amazon vous DataZone propose un moyen de gérer les autorisations d'accès pour vos actifs non gérés. Lorsqu'un abonnement à un actif du catalogue de données commerciales est approuvé par le propriétaire des données, Amazon DataZone publie un événement sur Amazon EventBridge dans votre compte avec toutes les informations nécessaires dans la charge utile qui vous permet de créer les autorisations d'accès entre la source et la cible. Lorsque vous recevez cet événement, vous pouvez déclencher un gestionnaire personnalisé qui peut utiliser les informations de l'événement pour créer les autorisations ou les autorisations nécessaires. Une fois que vous avez accordé l'accès, vous pouvez signaler et mettre à jour le statut de l'abonnement sur Amazon DataZone afin que celui-ci puisse informer les utilisateurs abonnés à l'actif qu'ils peuvent commencer à consommer l'actif. Pour plus d'informations, consultez Utilisation des DataZone événements et des notifications Amazon.

Consommer des données

Les tâches suivantes fournissent des informations sur la consommation des données auxquelles vous vous êtes abonné sur Amazon DataZone.

Rubriques

- Interrogez des données dans Amazon Athena ou Amazon Redshift

Interrogez des données dans Amazon Athena ou Amazon Redshift

Dans Amazon DataZone, une fois qu'un abonné a accès à un actif du catalogue, il peut l'utiliser (interroger et analyser) à l'aide d'Amazon Athena ou de l'éditeur de requêtes Amazon Redshift v2. Vous devez être propriétaire du projet ou contributeur pour effectuer cette tâche. En fonction des plans activés dans le projet, Amazon DataZone fournit des liens vers Amazon Athena et/ou l'éditeur de requêtes Amazon Redshift v2 dans le volet droit de la page du projet dans le portail de données.

1. Accédez à l'URL du portail de DataZone données Amazon et connectez-vous à l'aide de l'authentification unique (SSO) ou de vos AWS informations d'identification. Si vous êtes un DataZone administrateur Amazon, vous pouvez accéder à la DataZone console Amazon à l'adresse https://console.aws.amazon.com/datazone et vous connecter avec l'adresse Compte AWS où le domaine a été créé, puis choisir Open data portal.

2. Sur le portail de DataZone données Amazon, choisissez Parcourir la liste des projets, puis recherchez et choisissez le projet pour lequel vous avez les données que vous souhaitez analyser.
3. Si le plan Data Lake est activé sur ce projet, un lien vers Amazon Athena s'affiche dans le panneau de droite de la page d'accueil du projet.

   Si le plan de l'entrepôt de données est activé sur ce projet, un lien vers l'éditeur de requêtes s'affiche dans le panneau de droite de la page d'accueil du projet.

   > **Note**
   >
   > Les plans sont définis dans le profil d'environnement avec lequel un projet est créé.

Rubriques

- Interrogez des données à l'aide d'Amazon Athena
- Interrogez des données à l'aide d'Amazon Redshift

Interrogez des données à l'aide d'Amazon Athena

Cliquez sur le lien Amazon Athena pour ouvrir l'éditeur de requêtes Amazon Athena dans un nouvel onglet du navigateur en utilisant les informations d'identification du projet pour l'authentification. Le DataZone projet Amazon sur lequel vous travaillez est automatiquement sélectionné comme groupe de travail actuel dans l'éditeur de requêtes.

Dans l'éditeur de requêtes Amazon Athena, rédigez et exécutez vos requêtes. Parmi les tâches les plus courantes, citons :

- Interrogez et analysez vos actifs souscrits
- Création de nouvelles tables
- Création d'une table à partir des résultats de requête (CTAS) d'un compartiment S3 externe

Interrogez et analysez vos actifs souscrits

Si l'accès aux actifs auxquels votre projet est abonné n'est pas automatiquement accordé par Amazon DataZone, vous devez être autorisé à accéder aux données sous-jacentes. Pour plus

d'informations sur la manière d'accorder l'accès à ces actifs, consultezAccorder l'accès aux actifs non gérés pour les abonnements approuvés.

Si l'accès aux ressources auxquelles votre projet est abonné est automatiquement accordé par Amazon DataZone, vous pouvez exécuter des requêtes SQL sur les tables et consulter les résultats dans Amazon Athena. Pour plus d'informations sur l'utilisation de SQL dans Amazon Athena, consultez la référence SQL pour Athena.

Lorsque vous accédez à l'éditeur de requêtes Amazon Athena après avoir choisi le lien Amazon Athena dans le panneau de droite de la page d'accueil du projet, une liste déroulante de projets s'affiche dans le coin supérieur droit de l'éditeur de requêtes Amazon Athena et le contexte de votre projet est automatiquement sélectionné.

Vous pouvez voir les bases de données suivantes dans le menu déroulant Base de données :

- Une base de données de publication (*{environmentname}*_pub_db). L'objectif de cette base de données est de vous fournir un environnement dans lequel vous pouvez produire de nouvelles données dans le contexte de votre projet, puis publier ces données dans le DataZone catalogue Amazon. Les propriétaires de projets et les contributeurs ont un accès en lecture et en écriture à cette base de données. Les spectateurs du projet n'ont qu'un accès en lecture à cette base de données.
- Une base de données d'abonnement (*{environmentname}*_sub_db). Le but de cette base de données est de partager avec vous les données auxquelles vous vous êtes abonné en tant que membre du projet dans le DataZone catalogue Amazon, et de vous permettre d'interroger ces données.

Création de nouvelles tables

Si vous êtes connecté à un compartiment S3 externe, vous pouvez utiliser Amazon Athena pour interroger et analyser les actifs d'un compartiment Amazon S3 externe. Dans ce scénario, Amazon DataZone n'est pas autorisé à accorder l'accès directement aux données sous-jacentes dans le compartiment externe Amazon S3, et les données Amazon S3 externes créées en dehors du projet ne sont pas automatiquement gérées dans Lake Formation et ne peuvent pas être gérées par Amazon DataZone. Une autre solution consiste à copier les données du compartiment Amazon S3 externe vers une nouvelle table à l'intérieur du compartiment Amazon S3 du projet à l'aide d'une `CREATE TABLE` instruction dans Amazon Athena. Lorsque vous exécutez une `CREATE TABLE` requête dans Amazon Athena, vous enregistrez votre table auprès du. AWS Glue Data Catalog

Pour spécifier le chemin d'accès à vos données dans Simple Storage Service (Amazon S3), utilisez la propriété `LOCATION`, comme illustré dans l'exemple suivant :

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

Pour plus d'informations, consultez la section Emplacement des tables dans Amazon S3.

Création d'une table à partir des résultats de requête (CTAS) d'un compartiment S3 externe

Lorsque vous souscrivez à un actif, l'accès aux données sous-jacentes est en lecture seule. Vous pouvez utiliser Amazon Athena pour créer une copie du tableau. Dans Amazon Athena, `A CREATE TABLE AS SELECT (CTAS)` query crée une nouvelle table dans Amazon Athena à partir des résultats d'`SELECT`une instruction issue d'une autre requête. Pour plus d'informations sur la syntaxe CTAS, voir CREATE TABLE AS.

L'exemple suivant crée une table en copiant toutes les colonnes d'une table :

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

Dans la variation suivante du même exemple, votre instruction `SELECT` inclut également une clause `WHERE`. Dans ce cas, la requête sélectionne uniquement les lignes du tableau qui respectent la clause `WHERE` :

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

L'exemple suivant crée une nouvelle requête qui s'exécute sur un ensemble de colonnes à partir d'une autre table :

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

Cette variante du même exemple crée une nouvelle table à partir de colonnes spécifiques provenant de plusieurs tables :

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

Ces tables nouvellement créées font désormais partie de la AWS Glue base de données de vos projets et peuvent être rendues accessibles à d'autres personnes et partagées avec d'autres DataZone projets Amazon en publiant les données en tant que ressource dans le catalogue Amazon DataZone.

Interrogez des données à l'aide d'Amazon Redshift

Dans le portail de DataZone données Amazon, ouvrez un environnement qui utilise le plan de l'entrepôt de données. Cliquez sur le lien Amazon Redshift dans le panneau de droite de la page d'environnement. Cela ouvre une boîte de dialogue de confirmation contenant les informations nécessaires pour vous aider à établir une connexion au cluster Amazon Redshift ou au groupe de travail Amazon Redshift Serverless de votre environnement dans l'éditeur de requêtes Amazon Redshift v2.0. Une fois que vous avez identifié les informations nécessaires pour établir la connexion, cliquez sur le bouton Ouvrir Amazon Redshift. Cela ouvre l'éditeur de requêtes Amazon Redshift v2.0 dans un nouvel onglet du navigateur à l'aide des informations d'identification temporaires de l'environnement Amazon. DataZone

Dans l'éditeur de requêtes, suivez les étapes ci-dessous selon que votre environnement utilise un groupe de travail Amazon Redshift Serverless ou un cluster Amazon Redshift.

Pour un groupe de travail Amazon Redshift Serverless

1. Dans l'éditeur de requêtes, identifiez le groupe de travail Amazon Redshift Serverless de votre DataZone environnement Amazon, cliquez dessus avec le bouton droit de la souris et choisissez Create a connection.
2. Choisissez Federated User pour l'authentification.
3. Indiquez le nom de la base de données de DataZone l'environnement Amazon.
4. Choisissez Créer une connexion.

Pour un cluster Amazon Redshift :

1. Dans l'éditeur de requêtes, identifiez le cluster Amazon Redshift de votre DataZone environnement Amazon, cliquez dessus avec le bouton droit de la souris et choisissez Create a connection.
2. Sélectionnez Informations d'identification temporaires utilisant votre identité IAM pour l'authentification.
3. Si la méthode d'authentification ci-dessus n'est pas disponible, ouvrez les paramètres du compte en cliquant sur le bouton en forme de roue dentée dans le coin inférieur gauche, choisissez Authentifier avec les informations d'identification IAM et enregistrez. Il s'agit d'un one-time-only réglage.
4. Indiquez le nom de la base de données de DataZone l'environnement Amazon pour créer la connexion.
5. Choisissez Créer une connexion.

Vous pouvez maintenant commencer à interroger les tables et les vues du cluster Amazon Redshift ou du groupe de travail Amazon Redshift Serverless configuré pour votre environnement Amazon. DataZone

Toutes les tables ou vues Amazon Redshift auxquelles vous êtes abonné sont liées au cluster Amazon Redshift ou au groupe de travail Amazon Redshift Serverless configuré pour l'environnement. Vous pouvez vous abonner aux tables et aux vues ainsi que publier les nouvelles tables et vues que vous créez dans le cluster ou la base de données de votre environnement.

Prenons par exemple un scénario dans lequel un environnement est lié à un cluster Amazon Redshift appelé `redshift-cluster-1` et une base de données appelée `dev` dans ce cluster. À l'aide du portail de DataZone données Amazon, vous pouvez interroger les tables et les vues ajoutées à votre environnement. Dans la `Analytics tools` section du volet droit du portail de données, vous pouvez choisir le lien Amazon Redshift pour cet environnement, qui ouvre l'éditeur de requêtes.

Vous pouvez ensuite cliquer avec le bouton droit sur le `redshift-cluster-1` cluster et créer une connexion à l'aide d'informations d'identification temporaires utilisant votre identité IAM. Une fois la connexion établie, vous pouvez voir toutes les tables et vues auxquelles votre environnement a accès dans la base de données de développement.

Utilisation des DataZone événements et des notifications Amazon

Amazon vous DataZone tient informé des activités importantes au sein de votre portail de données, telles que les demandes d'abonnement, les mises à jour, les commentaires et les événements du système. Amazon vous DataZone fournit ces informations en envoyant des messages dans la boîte de réception dédiée du portail de données ou via le bus EventBridge par défaut d'Amazon.

Rubriques

Gestion des événements via la boîte de réception dédiée du portail de DataZone données Amazon

Amazon DataZone fournit une boîte de réception dédiée dans le portail de données, dans laquelle vous pouvez consulter vos messages et y donner suite. Les messages récents apparaissent également sur la page d'accueil, la page du projet et la page du catalogue. Par exemple, si un utilisateur demande l'accès à une ressource de données, les propriétaires du projet de publication et les contributeurs de cette ressource voient la demande dans le portail de données et une fois qu'une action est entreprise, les membres du projet abonné lié à cette demande voient la notification dans le portail de données. Il existe deux types de messages :

- Tâches : ces messages informent le destinataire qu'une action est nécessaire quelque part. Ils ont un champ de statut facultatif que vous pouvez utiliser pour le suivi.
- Événements : ces messages sont informatifs et n'ont aucun statut attribué. Les événements fournissent une piste d'audit des mises à jour récentes.

Dans Amazon DataZone, des messages sont générés pour les types d'événements suivants :

Catégorie d'événement	Nom de l'événement	Description de l'événement	Type d'événement
Abonnement	Demande d'abonnement créée	L'événement est généré lors de la création d'une demande d'abonnement	Tâche
Abonnement	Demande d'abonnement acceptée	L'événement est généré lorsqu'une demande d'abonnement est acceptée	Événement
Abonnement	Demande d'abonnement rejetée	Un événement est généré lorsqu'une demande d'abonnement est rejetée	Événement
Abonnement	Demande d'abonnement supprimée	L'événement est généré lorsqu'une demande d'abonnement est supprimée	Événement
Projet	Création du projet réussie	L'événement est généré lorsque la création du projet réussit	Événement
Adhésion au projet	L'ajout d'un membre au projet a réussi	L'événement est généré lorsqu'un nouveau membre est ajouté à un projet	Événement
Adhésion au projet	Suppression d'un membre du projet réussie	L'événement est généré lorsqu'un membre est supprimé d'un projet	Événement

Catégorie d'événement	Nom de l’événement	Description de l'événement	Type d’événement
Adhésion au projet	Changement de rôle du membre du projet réussi	Un événement est généré, le rôle d'un membre dans le projet est modifié	Événement
Environnement	Déploiement de l'environnement lancé	L'événement est généré lorsqu'un déploiement d'environnement est lancé	Événement
Environnement	Déploiement de l'environnement terminé	Un événement est généré lorsqu'un déploiement d'environnement est terminé avec succès	Événement
Environnement	Le déploiement de l'environnement a échoué	Un événement est généré en cas d'échec du déploiement d'un environnement	Événement
Environnement	Flux de travail personnalisé de déploiement de l'environnement lancé	L'événement est généré lorsqu'un environnement avec un flux de travail personnalisé est lancé	Événement
Actif de données	Actif ajouté à l'inventaire	L'événement est généré lorsqu'une nouvelle ressource de données est ajoutée à l'inventaire, c'est-à-dire ajoutée au catalogue à l'état de brouillon	Événement

Catégorie d'événement	Nom de l'événement	Description de l'événement	Type d'événement
Actif de données	Ressource publiée	L'événement est généré lorsqu'une nouvelle ressource de données est publiée, c'est-à-dire disponible pour abonnement	Événement
Actif de données	Schéma des actifs modifié	Un événement est généré lorsqu'un schéma d'actif a changé depuis une tâche d'ingestion précédente	Événement
Abonnement en cours	Abonnement créé	L'événement est généré lorsqu'une personne demande à s'abonner à un actif de données	Tâche
Abonnement en cours	Abonnement approuvé	L'événement est généré lorsqu'un abonnement est approuvé par le propriétaire ou le contributeur du projet de publication	Événement

Catégorie d'événement	Nom de l'événement	Description de l'événement	Type d'événement
Abonnement en cours	Abonnement refusé	L'événement est généré lorsqu'un abonnement est refusé par le propriétaire ou le contributeur du projet de publication	Événement
Abonnement en cours	Abonnement supprimé	L'événement est généré lorsqu'un abonnement est annulé par l'abonné	Événement
Abonnement en cours	Subvention d'abonnement demandée	L'événement est généré lorsqu'une personne demande l'accès à un actif	Événement
Abonnement en cours	Subvention d'abonnement terminée	L'événement est généré lorsqu'un abonnement est autorisé à accéder à la ressource par le propriétaire ou le contributeur du projet de publication	Événement
Abonnement en cours	Échec de la subvention d'abonnement	Un événement est généré lorsqu'une subvention d'abonnement échoue	Événement

Catégorie d'événement	Nom de l’événement	Description de l'événement	Type d’événement
Abonnement en cours	Demande de révocation de la subvention d'abonnement	Un événement est généré lorsqu'une subvention d'abonnement révoquée est initiée par le propriétaire ou le contributeur du projet de publication	Événement
Abonnement en cours	La révocation de l'autorisation d'abonnement est terminée	L'événement est généré lorsqu'une révocation d'une subvention d'abonnement est terminée	Événement
Abonnement en cours	Échec de la révocation de l'autorisation d'abonnement	Un événement est généré en cas d'échec de la révocation d'une autorisation d'abonnement	Événement
Génération automatique de noms commerciaux	Nom commercial généré avec succès	Un événement est généré lorsque la tâche générée automatiquement par le nom de l'entreprise s'achève avec succès	Événement

Catégorie d'événement	Nom de l'événement	Description de l'événement	Type d'événement
Génération automatique de noms commerciaux	Le nom commercial généré a échoué	L'événement est généré lorsque la tâche générée automatiquement par le nom de l'entreprise échoue	Événement
Exécution de la source de données	Source de données créée	L'événement est généré lorsqu'une nouvelle source de données est créée	Événement
Exécution de la source de données	Source de données mise à jour	L'événement est généré lorsqu'une source de données existante est mise à jour	Événement
Exécution de la source de données	Exécution de la source de données déclenchée	L'événement est généré lorsqu'une exécution de source de données est lancée	Événement
Exécution de la source de données	L'exécution de la source de données a réussi	L'événement est généré lorsqu'une exécution de source de données réussit	Événement
Exécution de la source de données	L'exécution de la source de données a échoué	Un événement est généré en cas d'échec de l'exécution d'une source de données	Événement

Pour afficher les tâches dans la boîte de réception de votre portail de données, procédez comme suit :

1. Accédez au portail de DataZone données Amazon à l'aide de l'URL du portail de données et connectez-vous à l'aide de votre SSO ou de vos AWS informations d'identification. Si vous êtes DataZone administrateur Amazon, vous pouvez obtenir l'URL du portail de données en accédant à la DataZone console Amazon à l'adresse https://console.aws.amazon.com/datazone dans le AWS compte sur lequel le DataZone domaine Amazon a été créé.
2. Dans le portail de données, pour afficher une fenêtre contextuelle présentant les tâches récentes, sélectionnez l'icône en forme de cloche à côté de la barre de recherche.
3. Sélectionnez Afficher tout pour afficher toutes les tâches. Vous pouvez changer de vue et voir tous les événements en sélectionnant l'onglet Événements.
4. Vous pouvez filtrer la recherche en fonction du sujet de l'événement, du statut actif ou inactif ou de la plage de dates.
5. Choisissez une tâche individuelle pour accéder à l'emplacement où vous pouvez répondre à la tâche.

Pour consulter les événements dans la boîte de réception de votre portail de données, procédez comme suit :

1. Accédez au portail de DataZone données Amazon à l'aide de l'URL du portail de données et connectez-vous à l'aide de votre SSO ou de vos AWS informations d'identification. Si vous êtes DataZone administrateur Amazon, vous pouvez obtenir l'URL du portail de données en accédant à la DataZone console Amazon à l'adresse https://console.aws.amazon.com/datazone dans le AWS compte sur lequel le domaine DataZone racine Amazon a été créé.
2. Dans le portail de données, pour afficher la fenêtre contextuelle des derniers événements, sélectionnez l'icône en forme de cloche à côté de la barre de recherche.
3. Sélectionnez Afficher tout pour afficher tous les événements. Vous pouvez modifier les vues et voir toutes les tâches en sélectionnant l'onglet Tâches.
4. Filtrez la recherche par sujet de l'événement ou par plage de dates.
5. Choisissez un événement individuel pour accéder à l'emplacement où vous pouvez consulter les détails de cet événement.

Utilisation des événements via le bus EventBridge par défaut d'Amazon

En plus d'envoyer des messages à votre boîte de réception dédiée dans le portail de données, il envoie DataZone également ces messages à votre bus d'événements EventBridge par défaut Amazon sur le même AWS compte où est hébergé votre domaine DataZone racine Amazon. Cela permet une automatisation axée sur les événements, telle que le traitement des abonnements ou des intégrations personnalisées avec d'autres outils. Vous pouvez créer des règles qui correspondent aux EventBridge événements Amazon entrants et les envoyer aux EventBridge cibles Amazon pour traitement. Une seule règle peut envoyer un événement à plusieurs cibles, qui peuvent ensuite s'exécuter en parallèle.

Voici un exemple d'événement :


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

La liste complète des types de détails pris en charge par Amazon DataZone inclut :

- Demande d'abonnement créée
- Demande d'abonnement acceptée
- Demande d'abonnement rejetée
- Demande d'abonnement supprimée
- Subvention d'abonnement demandée
- Subvention d'abonnement terminée
- Échec de la subvention d'abonnement
- Demande de révocation de la subvention d'abonnement
- La révocation de l'autorisation d'abonnement est terminée
- Échec de la révocation de l'autorisation d'abonnement
- Actif ajouté à l'inventaire
- Ressource ajoutée au catalogue
- Schéma des actifs modifié
- Modification du statut de la source de données
- Source de données créée
- Source de données mise à jour
- Exécution de la source de données déclenchée

- Exécution de la source de données réussie
- L'exécution de la source de données a échoué
- Création de domaine réussie
- Echec de la création du domaine
- Suppression du domaine réussie
- Echec de la suppression du domaine
- Déploiement de l'environnement commencé
- Déploiement de l'environnement terminé
- Échec du déploiement de l'environnement
- La suppression de l'environnement a commencé
- Suppression de l'environnement terminée
- La suppression de l'environnement a échoué
- Création du projet réussie
- L'ajout d'un membre au projet a réussi
- Suppression d'un membre du projet réussie
- Changement de rôle du membre du projet réussi
- Déploiement de l'environnement : flux de travail client
- Génération de noms commerciaux réussie
- Échec de la génération du nom commercial

Pour plus d'informations, consultez Amazon EventBridge.

Sécurité sur Amazon DataZone

La sécurité du cloud AWS est la priorité absolue. En tant que AWS client, vous bénéficiez de centres de données et d'architectures réseau conçus pour répondre aux exigences des entreprises les plus sensibles en matière de sécurité.

La sécurité est une responsabilité partagée entre vous AWS et vous. Le modèle de responsabilité partagée décrit cela comme la sécurité du cloud et la sécurité dans le cloud :

- Sécurité du cloud : AWS est chargée de protéger l'infrastructure qui exécute les AWS services dans le AWS Cloud. AWS vous fournit également des services que vous pouvez utiliser en toute sécurité. Des auditeurs tiers testent et vérifient régulièrement l'efficacité de notre sécurité dans le cadre des programmes de AWS conformité Programmes de de conformité. Pour en savoir plus sur les programmes de conformité applicables à Amazon DataZone, consultez la section AWS Services concernés par programme de conformitéAWS .
- Sécurité dans le cloud — Votre responsabilité est déterminée par le AWS service que vous utilisez. Vous êtes également responsable d'autres facteurs, y compris de la sensibilité de vos données, des exigences de votre entreprise, ainsi que de la législation et de la réglementation applicables.

Cette documentation vous aide à comprendre comment appliquer le modèle de responsabilité partagée lors de l'utilisation d'Amazon DataZone. Les rubriques suivantes expliquent comment configurer Amazon pour répondre DataZone à vos objectifs de sécurité et de conformité. Vous apprendrez également à utiliser d'autres AWS services qui vous aident à surveiller et à sécuriser vos DataZone ressources Amazon.

Rubriques

Protection des données sur Amazon DataZone

Le modèle de responsabilité AWS partagée de s'applique à la protection des données sur Amazon DataZone. Comme décrit dans ce modèle, AWS est chargé de protéger l'infrastructure mondiale qui gère tous les AWS Cloud. La gestion du contrôle de votre contenu hébergé sur cette infrastructure relève de votre responsabilité. Vous êtes également responsable des tâches de configuration et de gestion de la sécurité des Services AWS que vous utilisez. Pour plus d'informations sur la confidentialité des données, consultez Questions fréquentes (FAQ) sur la confidentialité des données. Pour en savoir plus sur la protection des données en Europe, consultez le billet de blog Modèle de responsabilité partagée AWS et RGPD (Règlement général sur la protection des données) sur le Blog de sécuritéAWS .

À des fins de protection des données, nous vous recommandons de protéger les Compte AWS informations d'identification et de configurer les utilisateurs individuels avec AWS IAM Identity Center ou AWS Identity and Access Management (IAM). Ainsi, chaque utilisateur se voit attribuer uniquement les autorisations nécessaires pour exécuter ses tâches. Nous vous recommandons également de sécuriser vos données comme indiqué ci-dessous :

- Utilisez l'authentification multifactorielle (MFA) avec chaque compte.
- Utilisez le protocole SSL/TLS pour communiquer avec les ressources. AWS Nous exigeons TLS 1.2 et recommandons TLS 1.3.
- Configurez l'API et la journalisation de l'activité des utilisateurs avec AWS CloudTrail.
- Utilisez des solutions de AWS chiffrement, ainsi que tous les contrôles de sécurité par défaut qu'ils contiennent Services AWS.
- Utilisez des services de sécurité gérés avancés tels qu'Amazon Macie, qui contribuent à la découverte et à la sécurisation des données sensibles stockées dans Amazon S3.
- Si vous avez besoin de modules cryptographiques validés par la norme FIPS 140-2 pour accéder AWS via une interface de ligne de commande ou une API, utilisez un point de terminaison FIPS. Pour plus d'informations sur les points de terminaison FIPS (Federal Information Processing Standard) disponibles, consultez Federal Information Processing Standard (FIPS) 140-2 (Normes de traitement de l'information fédérale).

Nous vous recommandons fortement de ne jamais placer d'informations confidentielles ou sensibles, telles que les adresses e-mail de vos clients, dans des balises ou des champs de texte libre tels que le champ Name (Nom). Cela inclut lorsque vous travaillez avec Amazon DataZone ou une autre entreprise Services AWS à l'aide de la console, de l'API ou AWS des SDK. AWS CLI Toutes les

données que vous entrez dans des balises ou des champs de texte de forme libre utilisés pour les noms peuvent être utilisées à des fins de facturation ou dans les journaux de diagnostic. Si vous fournissez une adresse URL à un serveur externe, nous vous recommandons fortement de ne pas inclure d'informations d'identification dans l'adresse URL permettant de valider votre demande adressée à ce serveur.

Chiffrement des données

Lorsque vous accordez des autorisations, vous décidez qui obtient quelles autorisations pour quelles DataZone ressources Amazon. Vous activez des actions spécifiques que vous souhaitez autoriser sur ces ressources. Par conséquent, vous devez accorder uniquement les autorisations qui sont requises pour exécuter une tâche. L'implémentation d'un accès sur la base du moindre privilège est fondamentale pour réduire les risques de sécurité et l'impact que pourraient avoir des d'erreurs ou des actes de malveillance.

Chiffrement au repos

Amazon DataZone chiffre toutes vos données par défaut à l'aide d'une AWS clé de service de gestion des clés (AWS KMS) qui vous AWS appartient et gère pour vous. Vous pouvez également chiffrer les données stockées dans le DataZone catalogue Amazon à l'aide de clés que vous gérez avec AWS KMS.

Lorsque vous créez un domaine sur Amazon DataZone, vous pouvez fournir des paramètres de chiffrement en cochant la case à côté de Personnaliser les paramètres de chiffrement (avancés) sous Chiffrement des données, et en fournissant une clé KMS.

Chiffrement en transit

Amazon DataZone utilise le protocole TLS (Transport Layer Security) et le chiffrement côté client pour le chiffrement en transit. La communication avec Amazon DataZone se fait toujours via HTTPS, de sorte que vos données sont toujours cryptées pendant le transport.

Confidentialité du trafic inter-réseaux

Pour sécuriser les connexions entre les comptes, Amazon DataZone utilise des rôles de service et des rôles IAM pour se connecter en toute sécurité aux comptes clients et exécuter des opérations pour le compte du client.

Rubriques

Le chiffrement des données est au repos pour Amazon DataZone

Le chiffrement des données au repos par défaut permet de réduire les frais opérationnels et la complexité liés à la protection des données sensibles. Dans le même temps, il vous permet de créer des applications sécurisées qui répondent aux exigences réglementaires et de conformité strictes en matière de chiffrement.

Amazon DataZone utilise des clés AWS détenues par défaut pour chiffrer automatiquement vos données au repos. Vous ne pouvez pas consulter, gérer ou auditer l'utilisation des clés que vous AWS possédez. Pour plus d'informations, consultez la section Clés AWS détenues.

Bien que vous ne puissiez pas désactiver cette couche de chiffrement ou sélectionner un autre type de chiffrement, vous pouvez ajouter une deuxième couche de chiffrement aux clés de chiffrement AWS détenues existantes en choisissant une clé gérée par le client lorsque vous créez vos domaines Amazon DataZone . Amazon DataZone prend en charge l'utilisation de clés symétriques gérées par le client que vous pouvez créer, posséder et gérer afin d'ajouter une deuxième couche de chiffrement par rapport au chiffrement AWS détenu existant. Comme vous avez le contrôle total de cette couche de chiffrement, vous pouvez y effectuer les tâches suivantes :

- Établir et maintenir des politiques clés
- Établir et maintenir les politiques et les subventions IAM
- Activer et désactiver les politiques clés
- Faire pivoter le matériel cryptographique clé
- Ajout de balises
- Création d'alias clés
- Planifier la suppression des clés

Pour plus d'informations, consultez la section Clés gérées par le client.

> **Note**
>
> Amazon active DataZone automatiquement le chiffrement au repos à l'aide de clés AWS détenues pour protéger gratuitement les données des clients.

AWS Des frais KMS s'appliquent pour l'utilisation de clés gérées par le client. Pour plus d'informations sur la tarification, consultez la section Tarification des services de gestion des AWS clés.

Comment Amazon DataZone utilise les subventions dans AWS KMS

Amazon a DataZone besoin de trois autorisations pour utiliser votre clé gérée par le client. Lorsque vous créez un DataZone domaine Amazon chiffré à l'aide d'une clé gérée par le client, Amazon DataZone crée des subventions et des sous-subventions en votre nom en envoyant des CreateGrantdemandes à AWS KMS. Les subventions dans AWS KMS sont utilisées pour donner à Amazon DataZone l'accès à une clé KMS dans votre compte. Amazon DataZone crée les autorisations suivantes pour utiliser votre clé gérée par le client pour les opérations internes suivantes :

Une autorisation pour le chiffrement de vos données au repos pour les opérations suivantes :

- Envoyez DescribeKeydes demandes à AWS KMS pour vérifier que l'ID de clé KMS symétrique géré par le client saisi lors de la création d'une collection de DataZone domaines Amazon est valide.
- Envoyez GenerateDataKeyrequestsà AWS KMS pour générer des clés de données chiffrées par votre clé gérée par le client.
- Envoyez des demandes de déchiffrement à AWS KMS pour déchiffrer les clés de données chiffrées afin qu'elles puissent être utilisées pour chiffrer vos données.
- RetireGrantpour annuler la subvention lorsque le domaine est supprimé.

Deux subventions pour la recherche et la découverte de vos données :

- Subvention 2 :
  - DescribeKey
  - GenerateDataKey
  - Chiffrer, déchiffrer, ReEncrypt
  - CreateGrantpour créer des allocations familiales pour les AWS services utilisés en interne par DataZone.
  - RetireGrant
- Subvention 3 :

- GenerateDataKey
- Decrypt
- RetireGrant

Vous pouvez révoquer l'accès à l'octroi ou supprimer l'accès du service à la clé gérée par le client à tout moment. Si vous le faites, Amazon DataZone ne pourra accéder à aucune des données chiffrées par la clé gérée par le client, ce qui affectera les opérations qui dépendent de ces données. Par exemple, si vous tentez d'obtenir les détails d'une ressource de données auxquels Amazon ne DataZone peut pas accéder, l'opération renverra une `AccessDeniedException` erreur.

Création d'une clé gérée par le client

Vous pouvez créer une clé symétrique gérée par le client à l'aide de la console AWS de gestion ou des API AWS KMS.

Pour créer une clé symétrique gérée par le client, suivez les étapes de création d'une clé symétrique gérée par le client dans le guide du développeur du service de gestion des AWS clés.

Politique clé : les politiques clés contrôlent l'accès à votre clé gérée par le client. Chaque clé gérée par le client doit avoir exactement une stratégie de clé, qui contient des instructions qui déterminent les personnes pouvant utiliser la clé et comment elles peuvent l'utiliser. Lorsque vous créez votre clé gérée par le client, vous pouvez spécifier une stratégie de clé. Pour plus d'informations, consultez la section Gestion de l'accès aux clés gérées par le client dans le Guide du développeur du service de gestion des AWS clés.

Pour utiliser votre clé gérée par le client avec vos DataZone ressources Amazon, les opérations d'API suivantes doivent être autorisées dans la politique relative aux clés :

- kms : CreateGrant — ajoute une autorisation à une clé gérée par le client. Accorde un accès de contrôle à une clé KMS spécifiée, ce qui permet d'accéder aux opérations d'octroi DataZone requises par Amazon. Pour plus d'informations sur l'utilisation des subventions, consultez le guide du développeur du service de gestion des AWS clés.
- kms : DescribeKey — fournit les informations relatives aux clés gérées par le client pour permettre DataZone à Amazon de valider la clé.
- kms : GenerateDataKey — renvoie une clé de données symétrique unique à utiliser en dehors de AWS KMS.
- KMS:Decrypt — Déchiffre le texte chiffré par une clé KMS.

Voici des exemples de déclarations de politique que vous pouvez ajouter pour 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**
>
> La politique de refus du KMS n'est pas appliquée aux ressources accessibles via le portail de DataZone données Amazon.

Pour plus d'informations sur la spécification des autorisations dans une politique, consultez le Guide du développeur du service de gestion des AWS clés.

Pour plus d'informations sur la résolution des problèmes d'accès par clé, consultez le Guide du développeur du service de gestion des AWS clés.

Spécifier une clé gérée par le client pour Amazon DataZone

Contexte DataZone de chiffrement Amazon

Un contexte de chiffrement est un ensemble facultatif de paires clé-valeur qui contient des informations contextuelles supplémentaires sur les données.

AWS KMS utilise le contexte de chiffrement comme données authentifiées supplémentaires pour prendre en charge le chiffrement authentifié. Lorsque vous incluez un contexte de chiffrement dans

une demande de chiffrement de données, AWS KMS lie le contexte de chiffrement aux données chiffrées. Pour déchiffrer les données, vous devez inclure le même contexte de chiffrement dans la demande.

Amazon DataZone utilise le contexte de chiffrement suivant :

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

Utilisation du contexte de chiffrement à des fins de surveillance : lorsque vous utilisez une clé symétrique gérée par le client pour chiffrer Amazon DataZone, vous pouvez également utiliser le contexte de chiffrement dans les dossiers d'audit et les journaux pour identifier la manière dont la clé gérée par le client est utilisée. Le contexte de chiffrement apparaît également dans les journaux générés par Amazon Logs AWS CloudTrail ou Amazon CloudWatch Logs.

Utilisation du contexte de chiffrement pour contrôler l'accès à votre clé gérée par le client : vous pouvez utiliser le contexte de chiffrement dans les politiques clés et les politiques IAM comme conditions pour contrôler l'accès à votre clé symétrique gérée par le client. Vous pouvez également utiliser des contraintes de contexte de chiffrement dans un octroi.

Amazon DataZone utilise une contrainte de contexte de chiffrement dans les autorisations afin de contrôler l'accès à la clé gérée par le client dans votre compte ou votre région. La contrainte d'octroi exige que les opérations autorisées par l'octroi utilisent le contexte de chiffrement spécifié.

Vous trouverez ci-dessous des exemples de déclarations de stratégie de clé permettant d'accorder l'accès à une clé gérée par le client dans un contexte de chiffrement spécifique. La condition énoncée dans cette déclaration de stratégie exige que les octrois comportent une contrainte de contexte de chiffrement qui spécifie le contexte de chiffrement.

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

Surveillance de vos clés de chiffrement pour Amazon DataZone

Lorsque vous utilisez une clé gérée par le client AWS KMS avec vos DataZone ressources Amazon, vous pouvez l'utiliser AWS CloudTrailpour suivre les demandes qu'Amazon DataZone envoie à AWS KMS. Les exemples suivants sont AWS CloudTrail des événements pour`CreateGrant`, `GenerateDataKeyDecrypt`, et `DescribeKey` pour surveiller les opérations KMS appelées par Amazon DataZone pour accéder aux données chiffrées par votre clé gérée par le client. Lorsque vous utilisez une clé gérée par le client AWS KMS pour chiffrer votre DataZone domaine Amazon, Amazon DataZone envoie une `CreateGrant` demande en votre nom pour accéder à la clé KMS de votre AWS compte. Les subventions créées par Amazon DataZone sont spécifiques à la ressource associée à la clé gérée par le client AWS KMS. En outre, Amazon DataZone utilise cette `RetireGrant` opération pour supprimer une autorisation lorsque vous supprimez un domaine. L'exemple d'événement suivant enregistre l'opération `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"
}
```

Création d'environnements Data Lake impliquant des catalogues AWS Glue cryptés

Dans les cas d'utilisation avancés, lorsque vous travaillez avec un catalogue AWS Glue chiffré, vous devez autoriser l'accès au DataZone service Amazon pour utiliser votre clé KMS gérée par le client. Vous pouvez le faire en mettant à jour votre politique KMS personnalisée et en ajoutant une balise à la clé. Pour autoriser l'accès au DataZone service Amazon afin de travailler avec les données d'un catalogue AWS Glue crypté, procédez comme suit :

- Ajoutez la politique suivante à votre clé KMS personnalisée. Consultez Modification d'une stratégie de clé pour de plus amples informations.

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

- Ajoutez la balise suivante à votre clé KMS personnalisée. Pour plus d'informations, consultez la section Utilisation de balises pour contrôler l'accès aux clés KMS.

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

Utilisation des points de terminaison VPC d'interface pour Amazon DataZone

Si vous utilisez Amazon Virtual Private Cloud (Amazon VPC) pour héberger vos AWS ressources, vous pouvez établir une connexion entre votre Amazon VPC et Amazon. DataZone Vous pouvez utiliser cette connexion avec Amazon DataZone sans passer par l'Internet public.

Amazon VPC vous permet de lancer AWS des ressources dans un réseau virtuel personnalisé. Vous pouvez utiliser un VPC pour contrôler vos paramètres réseau, tels que la plage d'adresses IP, les sous-réseaux, les tables de routage et les passerelles réseau. Pour plus d'informations sur les VPC, consultez le Guide de l'utilisateur Amazon VPC.

Pour connecter votre Amazon VPC à Amazon DataZone, vous devez d'abord définir un point de terminaison VPC d'interface, qui vous permet de connecter votre VPC à d'autres services. AWS Le point de terminaison assure une connectivité évolutive et fiable, sans qu'une passerelle Internet, une instance NAT (Network Address Translation) ou une connexion VPN ne soit nécessaire. Pour plus d'informations et des étapes détaillées sur la création d'un point de terminaison VPC, consultez Interface VPC Endpoints () dans le guide de AWS PrivateLink l'utilisateur Amazon VPC.

> **Important**
>
> Dans un VPC, une politique de point de terminaison est une politique basée sur les ressources que vous pouvez associer à un point de terminaison VPC pour contrôler quels AWS principaux peuvent utiliser le point de terminaison pour accéder à un service. AWS Dans la version actuelle d'Amazon DataZone, l'utilisation de politiques relatives aux terminaux n'est pas prise en charge pour établir et utiliser des connexions entre votre Amazon VPC et Amazon. DataZone La gestion des DataZone accès Amazon repose sur la configuration de la RAM et sur les principales politiques IAM définies au niveau du service.

Autorisation sur Amazon DataZone

L'interface DataZone d'Amazon se compose d'une console de gestion intégrée à la console AWS et d'une application Web hors console (portail de données).

La console DataZone de gestion Amazon peut être utilisée par AWS les administrateurs pour les top-level-resource API, notamment pour créer et gérer des domaines, les associations de AWS comptes pour ces domaines et les sources de données pour lesquelles vous souhaitez déléguer la gestion des accès à Amazon DataZone. Vous pouvez utiliser la console de DataZone gestion Amazon pour gérer tous les rôles IAM et toutes les configurations nécessaires pour déléguer le contrôle de gestion des accès au DataZone service Amazon pour leurs AWS comptes configurés de manière explicite. Le portail de DataZone données Amazon est une application de centre d' AWS identité propriétaire destinée aux utilisateurs du SSO. Si elle est activée, la console peut également être utilisée par les principaux IAM autorisés pour se fédérer dans le portail de données au lieu d'utiliser une identité SSO.

Le portail DataZone de données d'Amazon est principalement conçu pour être utilisé par les utilisateurs authentifiés par l' AWS IAM Identity Center afin de gérer l'accès aux données et d'effectuer des tâches de publication, de découverte, d'abonnement et d'analyse des données.

Autorisation dans la DataZone console Amazon

Le modèle d'autorisation de DataZone la console Amazon utilise l'autorisation IAM. La console est principalement utilisée par les administrateurs pour la configuration. Amazon DataZone utilise le concept d'un AWS compte d'administrateur de domaine et de AWS comptes de membres, et la console est utilisée à partir de tous ces comptes pour établir des relations de confiance tout en respectant les limites de AWS l'organisation.

Autorisation sur le DataZone portail Amazon

Le modèle d'autorisation du portail de DataZone données Amazon est une ACL hiérarchique avec des archétypes de rôles statiques (profils) qui incluent les administrateurs et les utilisateurs. Par exemple, les utilisateurs peuvent avoir un profil d'administrateur ou d'utilisateur. Au niveau d'un domaine, ils peuvent avoir une désignation d'utilisateur du domaine en tant que propriétaire des données. Au niveau d'un projet, un utilisateur peut être propriétaire ou contributeur. Ces profils peuvent être configurés selon l'un des deux types suivants : utilisateurs et groupes. Ces profils sont ensuite associés à des domaines et à des projets, et l'état de ces autorisations est stocké dans une table d'association.

Dans le cadre de ce modèle d'autorisation, Amazon DataZone permet aux utilisateurs de gérer les autorisations des utilisateurs et des groupes. Les utilisateurs gèrent l'adhésion aux projets, demandent l'adhésion aux projets et approuvent les adhésions. Les utilisateurs publient des données, définissent les approbateurs d'abonnement aux données, s'abonnent aux données et approuvent les abonnements.

Les utilisateurs effectuent des analyses de données dans le cadre de projets spécifiques lorsque le client de leur portail de données demande des informations d'identification de session IAM qu'Amazon DataZone génère en fonction du profil effectif de l'utilisateur dans le contexte du projet spécifique. Cette session est limitée à la fois aux autorisations de l'utilisateur et aux ressources spécifiques du projet. Les utilisateurs se rendent ensuite sur Athena ou Redshift pour rechercher les données pertinentes, et tout le travail IAM sous-jacent est complètement abstrait.

DataZone Profils et rôles Amazon

Une fois qu'un utilisateur est authentifié, le contexte authentifié correspond à un ID de profil utilisateur. Ce profil utilisateur peut comporter plusieurs associations différentes (propriétaire du projet, administrateur de domaine, etc.) utilisées pour autoriser les utilisateurs. Chaque association (par exemple, propriétaire du projet, administrateur de domaine, etc.) dispose d'autorisations pour certaines activités en fonction du contexte. Par exemple, un utilisateur qui possède une association d'administrateurs de domaine peut créer des domaines supplémentaires, affecter d'autres administrateurs de domaine au domaine et créer des modèles de projet au sein de son domaine. Un propriétaire de projet peut ajouter ou supprimer des membres pour son projet, créer des accords de publication avec un domaine et publier des actifs dans un domaine.

Contrôle de l'accès aux DataZone ressources Amazon à l'aide d'IAM

Vous devez AWS Identity and Access Management (IAM) effectuer les tâches liées à la sécurité suivantes :

- Créez des utilisateurs et des groupes sous votre Compte AWS.
- Attribuez des informations de sécurité uniques à chaque utilisateur situé sous votre Compte AWS.
- Contrôlez les autorisations de chaque utilisateur pour effectuer des tâches avec AWS des ressources.
- Autorisez les utilisateurs d'un autre Compte AWS pays à partager vos AWS ressources.
- Créez des rôles pour vous Compte AWS et définissez les utilisateurs ou les services qui peuvent les assumer.
- Utilisez les identités existantes pour que votre entreprise accorde des autorisations pour effectuer des tâches à l'aide de AWS ressources

Pour plus d'informations sur IAM, consultez les ressources suivantes :

- AWS Identity and Access Management (JE SUIS)
- Prise en main
- Guide de l'utilisateur IAM

Les sections suivantes décrivent les politiques et les autorisations requises pour configurer Amazon DataZone et ses composants, tels que les domaines (y compris le domaine), les comptes associés, les projets et les sources de données. Pour plus d'informations, consultez DataZone Terminologie et concepts d'Amazon.

Table des matières

AWS politiques gérées pour Amazon DataZone

Une politique AWS gérée est une politique autonome créée et administrée par AWS. AWS les politiques gérées sont conçues pour fournir des autorisations pour de nombreux cas d'utilisation courants afin que vous puissiez commencer à attribuer des autorisations aux utilisateurs, aux groupes et aux rôles.

N'oubliez pas que les politiques AWS gérées peuvent ne pas accorder d'autorisations de moindre privilège pour vos cas d'utilisation spécifiques, car elles sont accessibles à tous les AWS clients. Nous vous recommandons de réduire encore les autorisations en définissant des politiques gérées par le client qui sont propres à vos cas d'utilisation.

Vous ne pouvez pas modifier les autorisations définies dans les politiques AWS gérées. Si les autorisations définies dans une politique AWS gérée sont AWS mises à jour, la mise à jour affecte toutes les identités principales (utilisateurs, groupes et rôles) auxquelles la politique est attachée. AWS est le plus susceptible de mettre à jour une politique AWS gérée lorsqu'une nouvelle politique Service AWS est lancée ou lorsque de nouvelles opérations d'API sont disponibles pour les services existants.

Pour plus d'informations, consultez la section Politiques gérées par AWS dans le Guide de l'utilisateur IAM.

Table des matières

AWS politique gérée : AmazonDataZoneFullAccess

Vous pouvez associer la politique `AmazonDataZoneFullAccess` à vos identités IAM.

Cette politique fournit un accès complet à Amazon DataZone via le AWS Management Console.

Détails de l'autorisation

Cette politique inclut les autorisations suivantes :

- `datazone`— accorde aux principaux un accès complet à Amazon DataZone via le AWS Management Console.
- `kms`— Permet aux principaux de répertorier les alias et de décrire les clés.
- `s3`— Permet aux principaux de choisir des compartiments S3 existants ou d'en créer de nouveaux pour stocker les données Amazon DataZone .
- `ram`— Permet aux principaux de partager des DataZone domaines Comptes AWS Amazon entre eux.
- `iam`— Permet aux directeurs de répertorier et de transmettre des rôles et d'obtenir des politiques.
- `sso`— Permet aux principaux d'obtenir les régions où cette option AWS IAM Identity Center est activée.

```
{
  "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_*"
        }
      }
    }
  ]
}
```

Considérations et limites relatives aux politiques

Certaines fonctionnalités ne sont pas couvertes par la `AmazonDataZoneFullAccess` politique.

- Si vous créez un DataZone domaine Amazon avec votre propre AWS KMS clé, vous devez disposer des autorisations nécessaires `kms:CreateGrant` pour que la création du domaine réussisse, et `kms:Decrypt` pour `kms:GenerateDataKey` que cette clé puisse invoquer d'autres DataZone API Amazon telles que `listDataSources` et`createDataSource`. Et vous devez également disposer des autorisations nécessaires pour `kms:CreateGrant``kms:Decrypt`,`kms:GenerateDataKey`, et `kms:DescribeKey` dans la politique de ressources de cette clé.

  Si vous utilisez la clé KMS appartenant au service par défaut, cela n'est pas obligatoire.

  Pour plus d'informations, consultez AWS Key Management Service.
- Si vous souhaitez utiliser les fonctionnalités de création et de mise à jour de rôles dans la DataZone console Amazon, vous devez disposer des privilèges d'administrateur ou des autorisations IAM requises pour créer des rôles IAM et créer/mettre à jour des politiques. Les autorisations requises incluent`iam:CreateRole`,`iam:CreatePolicy`, `iam:CreatePolicyVersion``iam:DeletePolicyVersion`, et `iam:AttachRolePolicy` les autorisations.
- Si vous créez un nouveau domaine sur Amazon DataZone avec la connexion des AWS IAM Identity Center utilisateurs activée, ou si vous l'activez pour un domaine existant sur Amazon DataZone, vous devez disposer des autorisations suivantes :`sso:CreateManagedApplicationInstance`,`sso:DeleteManagedApplicationInstan` et`sso:PutApplicationAssignmentConfiguration`.
- Pour accepter une demande d'association de AWS compte sur Amazon DataZone, vous devez en avoir l'`ram:AcceptResourceShareInvitation`autorisation.

AWS politique gérée : AmazonDataZoneFullUserAccess

Cette politique accorde un accès complet à Amazon DataZone, mais elle n'autorise pas la gestion des domaines, des utilisateurs ou des comptes associés.

Détails de l'autorisation

```
{
```

```
  "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 politique gérée : AmazonDataZoneCustomEnvironmentDeploymentPolicy

Vous pouvez utiliser cette politique pour mettre à jour la configuration des environnements créés à l'aide de plans personnalisés. Cette politique peut également être utilisée pour créer des cibles DataZone d'abonnement et des sources de données Amazon.

Détails de l'autorisation

```
{
 "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 politique gérée : AmazonDataZoneEnvironmentRolePermissionsBoundary

> **Note**
>
> Cette politique est une limite d'autorisations. Une limite d'autorisations définit le nombre maximum d'autorisations qu'une politique basée sur l'identité peut accorder à une entité IAM. Vous ne devez pas utiliser et joindre vous-même les politiques relatives aux limites des DataZone autorisations d'Amazon. Les politiques DataZone relatives aux limites des autorisations Amazon ne doivent être associées qu'aux rôles DataZone gérés par Amazon. Pour plus d'informations sur les limites d'autorisations, consultez la section Limites d'autorisations pour les entités IAM dans le guide de l'utilisateur IAM.

Lorsque vous créez un environnement via le portail de DataZone données Amazon, Amazon DataZone applique cette limite d'autorisations aux rôles IAM produits lors de la création de l'environnement. La limite des autorisations limite l'étendue des rôles créés par Amazon DataZone et de tous les rôles que vous ajoutez.

Amazon DataZone utilise la politique `AmazonDataZoneEnvironmentRolePermissionsBoundary` gérée pour limiter le principal IAM provisionné auquel elle est attachée. Les principes peuvent prendre la forme des rôles d'utilisateur qu'Amazon DataZone peut assumer pour le compte des utilisateurs d'entreprise interactifs ou des

services d'analyse (par exemple)AWS Glue, puis effectuer des actions pour traiter des données telles que la lecture et l'écriture depuis Amazon S3 ou l'exécution. AWS Glue crawler

La `AmazonDataZoneEnvironmentRolePermissionsBoundary` politique accorde DataZone à Amazon un accès en lecture et en écriture à des services tels qu' AWS Glue Amazon S3 AWS Lake Formation, Amazon Redshift et Amazon Athena. La politique accorde également des autorisations de lecture et d'écriture à certaines ressources d'infrastructure requises pour utiliser ces services, telles que les interfaces réseau et AWS KMS les clés.

Amazon DataZone applique la politique `AmazonDataZoneEnvironmentRolePermissionsBoundary` AWS gérée en tant que limite d'autorisations pour tous les rôles de DataZone l'environnement Amazon (propriétaire et contributeur). Cette limite d'autorisations restreint ces rôles afin de n'autoriser l'accès qu'aux ressources requises et aux actions nécessaires à un environnement.

La limite inclut les instructions JSON suivantes :

```
{
  "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 politique gérée : AmazonDataZoneRedshiftGlueProvisioningPolicy

La AmazonDataZoneRedshiftGlueProvisioningPolicy politique accorde à Amazon DataZone les autorisations nécessaires pour interagir avec AWS Glue et 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 politique gérée : AmazonDataZoneGlueManageAccessRolePolicy

Cette politique autorise Amazon DataZone à publier les données AWS Glue dans le catalogue. Cela donne également à Amazon l' DataZone autorisation d'accorder ou de révoquer l'accès aux ressources publiées par AWS Glue dans le catalogue.

```
{
 "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 politique gérée : AmazonDataZoneRedshiftManageAccessRolePolicy

Cette politique autorise Amazon DataZone à publier les données Amazon Redshift dans le catalogue. Cela donne également à Amazon l' DataZone autorisation d'accorder ou de révoquer l'accès aux ressources publiées par Amazon Redshift ou Amazon Redshift Serverless dans le catalogue.

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

Politique gérée par AWS : AmazonDataZoneCrossAccountAdmin

Vous pouvez associer la AmazonDataZoneCrossAccountAdmin politique à vos identités IAM.

Cette politique permet aux utilisateurs de travailler avec les comptes DataZone associés à 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 politique gérée : AmazonDataZoneDomainExecutionRolePolicy

Il s'agit de la politique par défaut pour le rôle DataZone `DomainExecutionRole` de service Amazon. Ce rôle est utilisé par Amazon DataZone pour cataloguer, découvrir, gérer, partager et analyser les données du DataZone domaine Amazon.

Vous pouvez joindre la AmazonDataZoneDomainExecutionRolePolicy politique à votre`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 politique gérée : AmazonDataZoneSageMakerProvisioning

La AmazonDataZoneSageMakerProvisioning politique accorde à Amazon DataZone les autorisations nécessaires pour interagir avec 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 politique gérée : AmazonDataZoneSageMakerAccess

Cette politique autorise Amazon DataZone à publier des SageMaker actifs Amazon dans le catalogue. Cela donne également à Amazon l' DataZone autorisation d'accorder ou de révoquer l'accès aux actifs SageMaker publiés par Amazon dans le catalogue.

Cette politique inclut les autorisations pour effectuer les opérations suivantes :

- cloudtrail — récupère des informations sur les CloudTrail sentiers.
- cloudwatch — récupère les CloudWatch alarmes actuelles.

- logs — récupère les filtres métriques pour les CloudWatch journaux.
- sns — récupère la liste des abonnements à une rubrique SNS.
- config — récupère des informations sur les enregistreurs de configuration, les ressources et les règles de AWS configuration. Permet également au rôle lié au service de créer et de supprimer des règles de AWS configuration, et d'exécuter des évaluations par rapport à ces règles.
- iam — Obtenir et générer des rapports d'identification pour les comptes.
- organisations : récupérer les informations relatives au compte et à l'unité organisationnelle (UO) d'une organisation.
- securityhub : récupère des informations sur la manière dont le service, les normes et les contrôles Security Hub sont configurés.
- tag — récupère des informations sur les balises de ressources.

```
{
 "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 politique gérée : AmazonDataZoneSageMakerEnvironmentRolePermissionsBoundary

> **Note**
>
> Cette politique est une limite d'autorisations. Une limite d'autorisations définit le nombre maximum d'autorisations qu'une politique basée sur l'identité peut accorder à une entité IAM. Vous ne devez pas utiliser et joindre vous-même les politiques relatives aux limites des DataZone autorisations d'Amazon. Les politiques DataZone relatives aux limites des autorisations Amazon ne doivent être associées qu'aux rôles DataZone gérés par Amazon. Pour plus d'informations sur les limites d'autorisations, consultez la section Limites d'autorisations pour les entités IAM dans le guide de l'utilisateur IAM.

Lorsque vous créez un SageMaker environnement Amazon via le portail de DataZone données Amazon, Amazon DataZone applique cette limite d'autorisations aux rôles IAM produits lors de la création de l'environnement. La limite des autorisations limite l'étendue des rôles créés par Amazon DataZone et de tous les rôles que vous ajoutez.

Amazon DataZone utilise la politique `AmazonDataZoneSageMakerEnvironmentRolePermissionsBoundary` gérée pour limiter le principal IAM provisionné auquel elle est attachée. Les principes peuvent prendre la forme des rôles d'utilisateur qu'Amazon DataZone peut assumer pour le compte des utilisateurs d'entreprise interactifs ou des services d'analyse (par exemple)AWS SageMaker, puis effectuer des actions pour traiter des données telles que la lecture et l'écriture depuis Amazon S3 ou Amazon Redshift ou l'exécution AWS du robot d'exploration Glue.

Cette `AmazonDataZoneSageMakerEnvironmentRolePermissionsBoundary` politique accorde DataZone à Amazon un accès en lecture et en écriture à des services tels qu'Amazon SageMaker, AWS Glue, Amazon S3, AWS Lake Formation, Amazon Redshift et Amazon Athena. La politique accorde également des autorisations de lecture et d'écriture à certaines ressources d'infrastructure requises pour utiliser ces services, telles que les interfaces réseau, les référentiels Amazon ECR et les clés AWS KMS. Il donne également accès à des SageMaker applications Amazon comme Amazon SageMaker Canvas.

Amazon DataZone applique la politique `AmazonDataZoneSageMakerEnvironmentRolePermissionsBoundary` gérée en tant que limite d'autorisations pour tous les rôles de DataZone l'environnement Amazon (propriétaire et

contributeur). Cette limite d'autorisations restreint ces rôles afin de n'autoriser l'accès qu'aux ressources requises et aux actions nécessaires à un environnement.

```
       {
"Version": "2012-10-17",
"Statement": [
 {
  "Sid": "AllowAllNonAdminSageMakerActions",
  "Effect": "Allow",
  "Action": [
   "sagemaker:*",
   "sagemaker-geospatial:*"
  ],
  "NotResource": [
   "arn:aws:sagemaker:*:*:domain/*",
   "arn:aws:sagemaker:*:*:user-profile/*",
   "arn:aws:sagemaker:*:*:app/*",
   "arn:aws:sagemaker:*:*:space/*",
   "arn:aws:sagemaker:*:*:flow-definition/*"
  ]
 },
 {
  "Sid": "AllowSageMakerProfileManagement",
  "Effect": "Allow",
  "Action": [
   "sagemaker:CreateUserProfile",
   "sagemaker:DescribeUserProfile",
   "sagemaker:UpdateUserProfile",
   "sagemaker:CreatePresignedDomainUrl"
  ],
  "Resource": "arn:aws:sagemaker:*:*:*/*"
 },
 {
  "Sid": "AllowLakeFormation",
  "Effect": "Allow",
  "Action": [
   "lakeformation:GetDataAccess"
  ],
  "Resource": "*"
 },
 {
  "Sid": "AllowAddTagsForAppAndSpace",
```

```
    "Effect": "Allow",
    "Action": [
     "sagemaker:AddTags"
    ],
    "Resource": [
     "arn:aws:sagemaker:*:*:app/*",
     "arn:aws:sagemaker:*:*:space/*"
    ],
    "Condition": {
     "StringEquals": {
      "sagemaker:TaggingAction": [
       "CreateApp",
       "CreateSpace"
      ]
     }
    }
   },
   {
    "Sid": "AllowStudioActions",
    "Effect": "Allow",
    "Action": [
     "sagemaker:CreatePresignedDomainUrl",
     "sagemaker:DescribeApp",
     "sagemaker:DescribeDomain",
     "sagemaker:DescribeSpace",
     "sagemaker:DescribeUserProfile",
     "sagemaker:ListApps",
     "sagemaker:ListDomains",
     "sagemaker:ListSpaces",
     "sagemaker:ListUserProfiles"
    ],
    "Resource": "*"
   },
   {
    "Sid": "AllowAppActionsForUserProfile",
    "Effect": "Allow",
    "Action": [
     "sagemaker:CreateApp",
     "sagemaker:DeleteApp"
    ],
    "Resource": "arn:aws:sagemaker:*:*:app/*/*/*/*",
    "Condition": {
     "Null": {
      "sagemaker:OwnerUserProfileArn": "true"
```

```
    }
   }
  },
  {
   "Sid": "AllowAppActionsForSharedSpaces",
   "Effect": "Allow",
   "Action": [
    "sagemaker:CreateApp",
    "sagemaker:DeleteApp"
   ],
   "Resource": "arn:aws:sagemaker:*:*:app/${sagemaker:DomainId}/*/*/*",
   "Condition": {
    "StringEquals": {
     "sagemaker:SpaceSharingType": [
      "Shared"
     ]
    }
   }
  },
  {
   "Sid": "AllowMutatingActionsOnSharedSpacesWithoutOwner",
   "Effect": "Allow",
   "Action": [
    "sagemaker:CreateSpace",
    "sagemaker:DeleteSpace",
    "sagemaker:UpdateSpace"
   ],
   "Resource": "arn:aws:sagemaker:*:*:space/${sagemaker:DomainId}/*",
   "Condition": {
    "Null": {
     "sagemaker:OwnerUserProfileArn": "true"
    }
   }
  },
  {
   "Sid": "RestrictMutatingActionsOnSpacesToOwnerUserProfile",
   "Effect": "Allow",
   "Action": [
    "sagemaker:CreateSpace",
    "sagemaker:DeleteSpace",
    "sagemaker:UpdateSpace"
   ],
   "Resource": "arn:aws:sagemaker:*:*:space/${sagemaker:DomainId}/*",
   "Condition": {
```

```
    "ArnLike": {
     "sagemaker:OwnerUserProfileArn": "arn:aws:sagemaker:*:*:user-profile/
${sagemaker:DomainId}/${sagemaker:UserProfileName}"
    },
    "StringEquals": {
     "sagemaker:SpaceSharingType": [
      "Private",
      "Shared"
     ]
    }
   }
  },
  {
   "Sid": "RestrictMutatingActionsOnPrivateSpaceAppsToOwnerUserProfile",
   "Effect": "Allow",
   "Action": [
    "sagemaker:CreateApp",
    "sagemaker:DeleteApp"
   ],
   "Resource": "arn:aws:sagemaker:*:*:app/${sagemaker:DomainId}/*/*/*",
   "Condition": {
    "ArnLike": {
     "sagemaker:OwnerUserProfileArn": "arn:aws:sagemaker:*:*:user-profile/
${sagemaker:DomainId}/${sagemaker:UserProfileName}"
    },
    "StringEquals": {
     "sagemaker:SpaceSharingType": [
      "Private"
     ]
    }
   }
  },
  {
   "Sid": "AllowFlowDefinitionActions",
   "Effect": "Allow",
   "Action": "sagemaker:*",
   "Resource": [
    "arn:aws:sagemaker:*:*:flow-definition/*"
   ],
   "Condition": {
    "StringEqualsIfExists": {
     "sagemaker:WorkteamType": [
      "private-crowd",
      "vendor-crowd"
```

```
      ]
     }
    }
   },
   {
    "Sid": "AllowAWSServiceActions",
    "Effect": "Allow",
    "Action": [
     "sqlworkbench:*",
     "datazone:*",
     "application-autoscaling:DeleteScalingPolicy",
     "application-autoscaling:DeleteScheduledAction",
     "application-autoscaling:DeregisterScalableTarget",
     "application-autoscaling:DescribeScalableTargets",
     "application-autoscaling:DescribeScalingActivities",
     "application-autoscaling:DescribeScalingPolicies",
     "application-autoscaling:DescribeScheduledActions",
     "application-autoscaling:PutScalingPolicy",
     "application-autoscaling:PutScheduledAction",
     "application-autoscaling:RegisterScalableTarget",
     "aws-marketplace:ViewSubscriptions",
     "cloudformation:GetTemplateSummary",
     "cloudwatch:DeleteAlarms",
     "cloudwatch:DescribeAlarms",
     "cloudwatch:GetMetricData",
     "cloudwatch:GetMetricStatistics",
     "cloudwatch:ListMetrics",
     "cloudwatch:PutMetricAlarm",
     "cloudwatch:PutMetricData",
     "codecommit:BatchGetRepositories",
     "codecommit:CreateRepository",
     "codecommit:GetRepository",
     "codecommit:List*",
     "ec2:CreateNetworkInterface",
     "ec2:CreateNetworkInterfacePermission",
     "ec2:DeleteNetworkInterface",
     "ec2:DeleteNetworkInterfacePermission",
     "ec2:DescribeDhcpOptions",
     "ec2:DescribeNetworkInterfaces",
     "ec2:DescribeRouteTables",
     "ec2:DescribeSecurityGroups",
     "ec2:DescribeSubnets",
     "ec2:DescribeVpcEndpoints",
     "ec2:DescribeVpcEndpointServices",
```

```
    "ec2:DescribeVpcs",
    "ecr:BatchCheckLayerAvailability",
    "ecr:BatchGetImage",
    "ecr:Describe*",
    "ecr:GetAuthorizationToken",
    "ecr:GetDownloadUrlForLayer",
    "ecr:StartImageScan",
    "elastic-inference:Connect",
    "elasticfilesystem:DescribeFileSystems",
    "elasticfilesystem:DescribeMountTargets",
    "fsx:DescribeFileSystems",
    "groundtruthlabeling:*",
    "iam:GetRole",
    "iam:ListRoles",
    "kms:DescribeKey",
    "kms:ListAliases",
    "lambda:ListFunctions",
    "logs:CreateLogDelivery",
    "logs:CreateLogGroup",
    "logs:CreateLogStream",
    "logs:DeleteLogDelivery",
    "logs:DescribeLogGroups",
    "logs:DescribeLogStreams",
    "logs:GetLogDelivery",
    "logs:GetLogEvents",
    "logs:ListLogDeliveries",
    "logs:PutLogEvents",
    "logs:UpdateLogDelivery",
    "redshift-data:BatchExecuteStatement",
    "redshift-data:CancelStatement",
    "redshift-data:DescribeStatement",
    "redshift-data:DescribeTable",
    "redshift-data:ExecuteStatement",
    "redshift-data:GetStatementResult",
    "redshift-data:ListSchemas",
    "redshift-data:ListTables",
    "redshift-serverless:GetCredentials",
    "redshift-serverless:GetNamespace",
    "redshift-serverless:GetWorkgroup",
    "redshift-serverless:ListNamespaces",
    "redshift-serverless:ListWorkgroups",
    "secretsmanager:ListSecrets",
    "servicecatalog:Describe*",
    "servicecatalog:List*",
```

```
    "servicecatalog:ScanProvisionedProducts",
    "servicecatalog:SearchProducts",
    "servicecatalog:SearchProvisionedProducts",
    "sns:ListTopics",
    "tag:GetResources"
   ],
   "Resource": "*"
  },
  {
   "Sid": "AllowRAMInvitation",
   "Effect": "Allow",
   "Action": "ram:AcceptResourceShareInvitation",
   "Resource": "*",
   "Condition": {
    "StringLike": {
     "ram:ResourceShareName": "dzd_*"
    }
   }
  },
  {
   "Sid": "AllowECRActions",
   "Effect": "Allow",
   "Action": [
    "ecr:SetRepositoryPolicy",
    "ecr:CompleteLayerUpload",
    "ecr:CreateRepository",
    "ecr:BatchDeleteImage",
    "ecr:UploadLayerPart",
    "ecr:DeleteRepositoryPolicy",
    "ecr:InitiateLayerUpload",
    "ecr:DeleteRepository",
    "ecr:PutImage",
    "ecr:TagResource",
    "ecr:UntagResource"
   ],
   "Resource": [
    "arn:aws:ecr:*:*:repository/sagemaker*",
    "arn:aws:ecr:*:*:repository/datazone*"
   ]
  },
  {
   "Sid": "AllowCodeCommitActions",
   "Effect": "Allow",
   "Action": [
```

```
    "codecommit:GitPull",
    "codecommit:GitPush"
   ],
   "Resource": [
    "arn:aws:codecommit:*:*:*sagemaker*",
    "arn:aws:codecommit:*:*:*SageMaker*",
    "arn:aws:codecommit:*:*:*Sagemaker*"
   ]
  },
  {
   "Sid": "AllowCodeBuildActions",
   "Action": [
    "codebuild:BatchGetBuilds",
    "codebuild:StartBuild"
   ],
   "Resource": [
    "arn:aws:codebuild:*:*:project/sagemaker*",
    "arn:aws:codebuild:*:*:build/*"
   ],
   "Effect": "Allow"
  },
  {
   "Sid": "AllowStepFunctionsActions",
   "Action": [
    "states:DescribeExecution",
    "states:GetExecutionHistory",
    "states:StartExecution",
    "states:StopExecution",
    "states:UpdateStateMachine"
   ],
   "Resource": [
    "arn:aws:states:*:*:statemachine:*sagemaker*",
    "arn:aws:states:*:*:execution:*sagemaker*:*"
   ],
   "Effect": "Allow"
  },
  {
   "Sid": "AllowSecretManagerActions",
   "Effect": "Allow",
   "Action": [
    "secretsmanager:DescribeSecret",
    "secretsmanager:GetSecretValue",
    "secretsmanager:CreateSecret",
    "secretsmanager:PutResourcePolicy"
```

```
    ],
    "Resource": [
     "arn:aws:secretsmanager:*:*:secret:AmazonSageMaker-*"
    ]
   },
   {
    "Sid": "AllowServiceCatalogProvisionProduct",
    "Effect": "Allow",
    "Action": [
     "servicecatalog:ProvisionProduct"
    ],
    "Resource": "*"
   },
   {
    "Sid": "AllowServiceCatalogTerminateUpdateProvisionProduct",
    "Effect": "Allow",
    "Action": [
     "servicecatalog:TerminateProvisionedProduct",
     "servicecatalog:UpdateProvisionedProduct"
    ],
    "Resource": "*",
    "Condition": {
     "StringEquals": {
      "servicecatalog:userLevel": "self"
     }
    }
   },
   {
    "Sid": "AllowS3ObjectActions",
    "Effect": "Allow",
    "Action": [
     "s3:AbortMultipartUpload",
     "s3:DeleteObject",
     "s3:DeleteObjectVersion",
     "s3:GetObject",
     "s3:PutObject",
     "s3:PutObjectRetention",
     "s3:ReplicateObject",
     "s3:RestoreObject",
     "s3:GetBucketAcl",
     "s3:PutObjectAcl"
    ],
    "Resource": [
     "arn:aws:s3:::SageMaker-DataZone*",
```

```
    "arn:aws:s3:::DataZone-SageMaker*",
    "arn:aws:s3:::Sagemaker-DataZone*",
    "arn:aws:s3:::DataZone-Sagemaker*",
    "arn:aws:s3:::sagemaker-datazone*",
    "arn:aws:s3:::datazone-sagemaker*",
    "arn:aws:s3:::amazon-datazone*"
   ]
  },
  {
   "Sid": "AllowS3GetObjectWithSageMakerExistingObjectTag",
   "Effect": "Allow",
   "Action": [
    "s3:GetObject"
   ],
   "Resource": [
    "arn:aws:s3:::*"
   ],
   "Condition": {
    "StringEqualsIgnoreCase": {
     "s3:ExistingObjectTag/SageMaker": "true"
    }
   }
  },
  {
   "Sid": "AllowS3GetObjectWithServiceCatalogProvisioningExistingObjectTag",
   "Effect": "Allow",
   "Action": [
    "s3:GetObject"
   ],
   "Resource": [
    "arn:aws:s3:::*"
   ],
   "Condition": {
    "StringEquals": {
     "s3:ExistingObjectTag/servicecatalog:provisioning": "true"
    }
   }
  },
  {
   "Sid": "AllowS3BucketActions",
   "Effect": "Allow",
   "Action": [
    "s3:GetBucketLocation",
    "s3:ListBucket",
```

```
    "s3:ListAllMyBuckets",
    "s3:GetBucketCors",
    "s3:PutBucketCors"
   ],
   "Resource": [
    "arn:aws:s3:::SageMaker-DataZone*",
    "arn:aws:s3:::DataZone-SageMaker*",
    "arn:aws:s3:::Sagemaker-DataZone*",
    "arn:aws:s3:::DataZone-Sagemaker*",
    "arn:aws:s3:::sagemaker-datazone*",
    "arn:aws:s3:::datazone-sagemaker*",
    "arn:aws:s3:::amazon-datazone*"
   ]
  },
  {
   "Sid": "ReadSageMakerJumpstartArtifacts",
   "Effect": "Allow",
   "Action": "s3:GetObject",
   "Resource": [
    "arn:aws:s3:::jumpstart-cache-prod-us-west-2/*",
    "arn:aws:s3:::jumpstart-cache-prod-us-east-1/*",
    "arn:aws:s3:::jumpstart-cache-prod-us-east-2/*",
    "arn:aws:s3:::jumpstart-cache-prod-eu-west-1/*",
    "arn:aws:s3:::jumpstart-cache-prod-eu-central-1/*",
    "arn:aws:s3:::jumpstart-cache-prod-ap-south-1/*",
    "arn:aws:s3:::jumpstart-cache-prod-ap-northeast-2/*",
    "arn:aws:s3:::jumpstart-cache-prod-ap-northeast-1/*",
    "arn:aws:s3:::jumpstart-cache-prod-ap-southeast-1/*",
    "arn:aws:s3:::jumpstart-cache-prod-ap-southeast-2/*"
   ]
  },
  {
   "Sid": "AllowLambdaInvokeFunction",
   "Effect": "Allow",
   "Action": [
    "lambda:InvokeFunction"
   ],
   "Resource": [
    "arn:aws:lambda:*:*:function:*SageMaker*",
    "arn:aws:lambda:*:*:function:*sagemaker*",
    "arn:aws:lambda:*:*:function:*Sagemaker*",
    "arn:aws:lambda:*:*:function:*LabelingFunction*"
   ]
  },
```

```
  {
   "Sid": "AllowCreateServiceLinkedRoleForSageMakerApplicationAutoscaling",
   "Action": "iam:CreateServiceLinkedRole",
   "Effect": "Allow",
   "Resource": "arn:aws:iam::*:role/aws-service-role/sagemaker.application-
autoscaling.amazonaws.com/AWSServiceRoleForApplicationAutoScaling_SageMakerEndpoint",
   "Condition": {
    "StringLike": {
     "iam:AWSServiceName": "sagemaker.application-autoscaling.amazonaws.com"
    }
   }
  },
  {
   "Sid": "AllowSNSActions",
   "Effect": "Allow",
   "Action": [
    "sns:Subscribe",
    "sns:CreateTopic",
    "sns:Publish"
   ],
   "Resource": [
    "arn:aws:sns:*:*:*SageMaker*",
    "arn:aws:sns:*:*:*Sagemaker*",
    "arn:aws:sns:*:*:*sagemaker*"
   ]
  },
  {
   "Sid": "AllowPassRoleForSageMakerRoles",
   "Effect": "Allow",
   "Action": [
    "iam:PassRole"
   ],
   "Resource": [
    "arn:aws:iam::*:role/sm-provisioning/datazone_usr_sagemaker_execution_role_*"
   ],
   "Condition": {
    "StringEquals": {
     "iam:PassedToService": [
      "glue.amazonaws.com",
      "bedrock.amazonaws.com",
      "states.amazonaws.com",
      "lakeformation.amazonaws.com",
      "events.amazonaws.com",
      "sagemaker.amazonaws.com",
```

```
      "forecast.amazonaws.com"
     ]
    }
   }
  },
  {
   "Sid": "CrossAccountKmsOperations",
   "Effect": "Allow",
   "Action": [
    "kms:DescribeKey",
    "kms:Decrypt",
    "kms:ListKeys"
   ],
   "Resource": "*",
   "Condition": {
    "StringNotEquals": {
     "aws:ResourceAccount": "${aws:PrincipalAccount}"
    }
   }
  },
  {
   "Sid": "KmsOperationsWithResourceTag",
   "Effect": "Allow",
   "Action": [
    "kms:DescribeKey",
    "kms:Decrypt",
    "kms:ListKeys",
    "kms:Encrypt",
    "kms:GenerateDataKey",
    "kms:RetireGrant"
   ],
   "Resource": "*",
   "Condition": {
    "Null": {
     "aws:ResourceTag/AmazonDataZoneEnvironment": "false"
    }
   }
  },
  {
   "Sid": "AllowAthenaActions",
   "Effect": "Allow",
   "Action": [
    "athena:BatchGetNamedQuery",
    "athena:BatchGetPreparedStatement",
```

```
    "athena:BatchGetQueryExecution",
    "athena:CreateNamedQuery",
    "athena:CreateNotebook",
    "athena:CreatePreparedStatement",
    "athena:CreatePresignedNotebookUrl",
    "athena:DeleteNamedQuery",
    "athena:DeleteNotebook",
    "athena:DeletePreparedStatement",
    "athena:ExportNotebook",
    "athena:GetDatabase",
    "athena:GetDataCatalog",
    "athena:GetNamedQuery",
    "athena:GetPreparedStatement",
    "athena:GetQueryExecution",
    "athena:GetQueryResults",
    "athena:GetQueryResultsStream",
    "athena:GetQueryRuntimeStatistics",
    "athena:GetTableMetadata",
    "athena:GetWorkGroup",
    "athena:ImportNotebook",
    "athena:ListDatabases",
    "athena:ListDataCatalogs",
    "athena:ListEngineVersions",
    "athena:ListNamedQueries",
    "athena:ListPreparedStatements",
    "athena:ListQueryExecutions",
    "athena:ListTableMetadata",
    "athena:ListTagsForResource",
    "athena:ListWorkGroups",
    "athena:StartCalculationExecution",
    "athena:StartQueryExecution",
    "athena:StartSession",
    "athena:StopCalculationExecution",
    "athena:StopQueryExecution",
    "athena:TerminateSession",
    "athena:UpdateNamedQuery",
    "athena:UpdateNotebook",
    "athena:UpdateNotebookMetadata",
    "athena:UpdatePreparedStatement"
   ],
   "Resource": [
    "*"
   ]
  },
```

```
{
 "Sid": "AllowGlueCreateDatabase",
 "Effect": "Allow",
 "Action": [
  "glue:CreateDatabase"
 ],
 "Resource": [
  "arn:aws:glue:*:*:catalog",
  "arn:aws:glue:*:*:database/default"
 ]
},
{
 "Sid": "AllowRedshiftGetClusterCredentials",
 "Effect": "Allow",
 "Action": [
  "redshift:GetClusterCredentials"
 ],
 "Resource": [
  "arn:aws:redshift:*:*:dbuser:*/sagemaker_access*",
  "arn:aws:redshift:*:*:dbname:*"
 ]
},
{
 "Sid": "AllowListTags",
 "Effect": "Allow",
 "Action": [
  "sagemaker:ListTags"
 ],
 "Resource": [
  "arn:aws:sagemaker:*:*:user-profile/*",
  "arn:aws:sagemaker:*:*:domain/*"
 ]
},
{
 "Sid": "AllowCloudformationListStackResources",
 "Effect": "Allow",
 "Action": [
  "cloudformation:ListStackResources"
 ],
 "Resource": "arn:aws:cloudformation:*:*:stack/SC-*"
},
{
 "Sid": "AllowGlueActions",
 "Effect": "Allow",
```

```
    "Action": [
     "glue:GetColumnStatisticsForPartition",
     "glue:GetColumnStatisticsForTable",
     "glue:ListJobs",
     "glue:CreateSession",
     "glue:RunStatement",
     "glue:BatchCreatePartition",
     "glue:CreatePartitionIndex",
     "glue:CreateTable",
     "glue:BatchGetWorkflows",
     "glue:BatchUpdatePartition",
     "glue:BatchDeletePartition",
     "glue:GetPartition",
     "glue:GetPartitions",
     "glue:UpdateTable",
     "glue:DeleteTableVersion",
     "glue:DeleteTable",
     "glue:DeleteColumnStatisticsForPartition",
     "glue:DeleteColumnStatisticsForTable",
     "glue:DeletePartitionIndex",
     "glue:UpdateColumnStatisticsForPartition",
     "glue:UpdateColumnStatisticsForTable",
     "glue:BatchDeleteTableVersion",
     "glue:BatchDeleteTable",
     "glue:CreatePartition",
     "glue:DeletePartition",
     "glue:UpdatePartition",
     "glue:CreateBlueprint",
     "glue:CreateJob",
     "glue:CreateConnection",
     "glue:CreateCrawler",
     "glue:CreateDataQualityRuleset",
     "glue:CreateWorkflow",
     "glue:GetDatabases",
     "glue:GetTables",
     "glue:GetTable",
     "glue:SearchTables",
     "glue:NotifyEvent",
     "glue:ListSchemas",
     "glue:BatchGetJobs",
     "glue:GetConnection",
     "glue:GetDatabase"
    ],
    "Resource": [
```

```
    "*"
   ]
  },
  {
   "Sid": "AllowGlueActionsWithEnvironmentTag",
   "Effect": "Allow",
   "Action": [
    "glue:SearchTables",
    "glue:NotifyEvent",
    "glue:StartBlueprintRun",
    "glue:PutWorkflowRunProperties",
    "glue:StopCrawler",
    "glue:DeleteJob",
    "glue:DeleteWorkflow",
    "glue:UpdateCrawler",
    "glue:DeleteBlueprint",
    "glue:UpdateWorkflow",
    "glue:StartCrawler",
    "glue:ResetJobBookmark",
    "glue:UpdateJob",
    "glue:StartWorkflowRun",
    "glue:StopCrawlerSchedule",
    "glue:ResumeWorkflowRun",
    "glue:ListSchemas",
    "glue:DeleteCrawler",
    "glue:UpdateBlueprint",
    "glue:BatchStopJobRun",
    "glue:StopWorkflowRun",
    "glue:BatchGetJobs",
    "glue:BatchGetWorkflows",
    "glue:UpdateCrawlerSchedule",
    "glue:DeleteConnection",
    "glue:UpdateConnection",
    "glue:GetConnection",
    "glue:GetDatabase",
    "glue:GetTable",
    "glue:GetPartition",
    "glue:GetPartitions",
    "glue:BatchDeleteConnection",
    "glue:StartCrawlerSchedule",
    "glue:StartJobRun",
    "glue:CreateWorkflow",
    "glue:*DataQuality*"
   ],
```

```
    "Resource": "*",
    "Condition": {
     "Null": {
      "aws:ResourceTag/AmazonDataZoneEnvironment": "false"
     }
    }
   },
   {
    "Sid": "AllowGlueDefaultAccess",
    "Effect": "Allow",
    "Action": [
     "glue:BatchGet*",
     "glue:Get*",
     "glue:SearchTables",
     "glue:List*",
     "glue:RunStatement"
    ],
    "Resource": [
     "arn:aws:glue:*:*:catalog",
     "arn:aws:glue:*:*:database/default",
     "arn:aws:glue:*:*:connection/dz-sm-*",
     "arn:aws:glue:*:*:session/*"
    ]
   },
   {
    "Sid": "AllowRedshiftClusterActions",
    "Effect": "Allow",
    "Action": [
     "redshift:GetClusterCredentialsWithIAM",
     "redshift:DescribeClusters"
    ],
    "Resource": [
     "arn:aws:redshift:*:*:cluster:*",
     "arn:aws:redshift:*:*:dbname:*"
    ]
   },
   {
    "Sid": "AllowCreateClusterUser",
    "Effect": "Allow",
    "Action": [
     "redshift:CreateClusterUser"
    ],
    "Resource": [
     "arn:aws:redshift:*:*:dbuser:*"
```

```
    ]
   },
   {
    "Sid": "AllowCreateSecretActions",
    "Effect": "Allow",
    "Action": [
     "secretsmanager:CreateSecret",
     "secretsmanager:TagResource"
    ],
    "Resource": "arn:aws:secretsmanager:*:*:secret:AmazonDataZone-*",
    "Condition": {
     "StringLike": {
      "aws:ResourceTag/AmazonDataZoneDomain": "dzd_*",
      "aws:RequestTag/AmazonDataZoneDomain": "dzd_*"
     },
     "Null": {
      "aws:TagKeys": "false",
      "aws:ResourceTag/AmazonDataZoneProject": "false",
      "aws:ResourceTag/AmazonDataZoneDomain": "false",
      "aws:RequestTag/AmazonDataZoneDomain": "false",
      "aws:RequestTag/AmazonDataZoneProject": "false"
     },
     "ForAllValues:StringEquals": {
      "aws:TagKeys": [
       "AmazonDataZoneDomain",
       "AmazonDataZoneProject"
      ]
     }
    }
   },
   {
    "Sid": "ForecastOperations",
    "Effect": "Allow",
    "Action": [
     "forecast:CreateExplainabilityExport",
     "forecast:CreateExplainability",
     "forecast:CreateForecastEndpoint",
     "forecast:CreateAutoPredictor",
     "forecast:CreateDatasetImportJob",
     "forecast:CreateDatasetGroup",
     "forecast:CreateDataset",
     "forecast:CreateForecast",
     "forecast:CreateForecastExportJob",
     "forecast:CreatePredictorBacktestExportJob",
```

```
    "forecast:CreatePredictor",
    "forecast:DescribeExplainabilityExport",
    "forecast:DescribeExplainability",
    "forecast:DescribeAutoPredictor",
    "forecast:DescribeForecastEndpoint",
    "forecast:DescribeDatasetImportJob",
    "forecast:DescribeDataset",
    "forecast:DescribeForecast",
    "forecast:DescribeForecastExportJob",
    "forecast:DescribePredictorBacktestExportJob",
    "forecast:GetAccuracyMetrics",
    "forecast:InvokeForecastEndpoint",
    "forecast:GetRecentForecastContext",
    "forecast:DescribePredictor",
    "forecast:TagResource",
    "forecast:DeleteResourceTree"
   ],
   "Resource": [
    "arn:aws:forecast:*:*:*Canvas*"
   ]
  },
  {
   "Sid": "RDSOperation",
   "Effect": "Allow",
   "Action": "rds:DescribeDBInstances",
   "Resource": "*"
  },
  {
   "Sid": "AllowEventBridgeRule",
   "Effect": "Allow",
   "Action": [
    "events:PutRule"
   ],
   "Resource": "arn:aws:events:*:*:rule/*",
   "Condition": {
    "StringEquals": {
     "aws:RequestTag/sagemaker:is-canvas-data-prep-job": "true"
    }
   }
  },
  {
   "Sid": "EventBridgeOperations",
   "Effect": "Allow",
   "Action": [
```

```
    "events:DescribeRule",
    "events:PutTargets"
   ],
   "Resource": "arn:aws:events:*:*:rule/*",
   "Condition": {
    "StringEquals": {
     "aws:ResourceTag/sagemaker:is-canvas-data-prep-job": "true"
    }
   }
  },
  {
   "Sid": "EventBridgeTagBasedOperations",
   "Effect": "Allow",
   "Action": [
    "events:TagResource"
   ],
   "Resource": "arn:aws:events:*:*:rule/*",
   "Condition": {
    "StringEquals": {
     "aws:RequestTag/sagemaker:is-canvas-data-prep-job": "true",
     "aws:ResourceTag/sagemaker:is-canvas-data-prep-job": "true"
    }
   }
  },
  {
   "Sid": "EventBridgeListTagOperation",
   "Effect": "Allow",
   "Action": "events:ListTagsForResource",
   "Resource": "*"
  },
  {
   "Sid": "AllowEMR",
   "Effect": "Allow",
   "Action": [
    "elasticmapreduce:DescribeCluster",
    "elasticmapreduce:ListInstanceGroups",
    "elasticmapreduce:ListClusters"
   ],
   "Resource": "*"
  },
  {
   "Sid": "AllowSSOAction",
   "Effect": "Allow",
   "Action": [
```

```
    "sso:CreateApplicationAssignment",
    "sso:AssociateProfile"
   ],
   "Resource": "*"
  },
  {
   "Sid": "DenyNotAction",
   "Effect": "Deny",
   "NotAction": [
    "sagemaker:*",
    "sagemaker-geospatial:*",
    "sqlworkbench:*",
    "datazone:*",
    "forecast:*",
    "application-autoscaling:DeleteScalingPolicy",
    "application-autoscaling:DeleteScheduledAction",
    "application-autoscaling:DeregisterScalableTarget",
    "application-autoscaling:DescribeScalableTargets",
    "application-autoscaling:DescribeScalingActivities",
    "application-autoscaling:DescribeScalingPolicies",
    "application-autoscaling:DescribeScheduledActions",
    "application-autoscaling:PutScalingPolicy",
    "application-autoscaling:PutScheduledAction",
    "application-autoscaling:RegisterScalableTarget",
    "athena:BatchGetNamedQuery",
    "athena:BatchGetPreparedStatement",
    "athena:BatchGetQueryExecution",
    "athena:CreateNamedQuery",
    "athena:CreateNotebook",
    "athena:CreatePreparedStatement",
    "athena:CreatePresignedNotebookUrl",
    "athena:DeleteNamedQuery",
    "athena:DeleteNotebook",
    "athena:DeletePreparedStatement",
    "athena:ExportNotebook",
    "athena:GetDatabase",
    "athena:GetDataCatalog",
    "athena:GetNamedQuery",
    "athena:GetPreparedStatement",
    "athena:GetQueryExecution",
    "athena:GetQueryResults",
    "athena:GetQueryResultsStream",
    "athena:GetQueryRuntimeStatistics",
    "athena:GetTableMetadata",
```

```
    "athena:GetWorkGroup",
    "athena:ImportNotebook",
    "athena:ListDatabases",
    "athena:ListDataCatalogs",
    "athena:ListEngineVersions",
    "athena:ListNamedQueries",
    "athena:ListPreparedStatements",
    "athena:ListQueryExecutions",
    "athena:ListTableMetadata",
    "athena:ListTagsForResource",
    "athena:ListWorkGroups",
    "athena:StartCalculationExecution",
    "athena:StartQueryExecution",
    "athena:StartSession",
    "athena:StopCalculationExecution",
    "athena:StopQueryExecution",
    "athena:TerminateSession",
    "athena:UpdateNamedQuery",
    "athena:UpdateNotebook",
    "athena:UpdateNotebookMetadata",
    "athena:UpdatePreparedStatement",
    "aws-marketplace:ViewSubscriptions",
    "cloudformation:GetTemplateSummary",
    "cloudformation:ListStackResources",
    "cloudwatch:DeleteAlarms",
    "cloudwatch:DescribeAlarms",
    "cloudwatch:GetMetricData",
    "cloudwatch:GetMetricStatistics",
    "cloudwatch:ListMetrics",
    "cloudwatch:PutMetricAlarm",
    "cloudwatch:PutMetricData",
    "codebuild:BatchGetBuilds",
    "codebuild:StartBuild",
    "codecommit:BatchGetRepositories",
    "codecommit:CreateRepository",
    "codecommit:GetRepository",
    "codecommit:List*",
    "codecommit:GitPull",
    "codecommit:GitPush",
    "ec2:CreateNetworkInterface",
    "ec2:CreateNetworkInterfacePermission",
    "ec2:DeleteNetworkInterface",
    "ec2:DeleteNetworkInterfacePermission",
    "ec2:DescribeDhcpOptions",
```

```
    "ec2:DescribeNetworkInterfaces",
    "ec2:DescribeRouteTables",
    "ec2:DescribeSecurityGroups",
    "ec2:DescribeSubnets",
    "ec2:DescribeVpcEndpoints",
    "ec2:DescribeVpcEndpointServices",
    "ec2:DescribeVpcs",
    "ecr:BatchCheckLayerAvailability",
    "ecr:BatchGetImage",
    "ecr:CreateRepository",
    "ecr:Describe*",
    "ecr:GetAuthorizationToken",
    "ecr:GetDownloadUrlForLayer",
    "ecr:SetRepositoryPolicy",
    "ecr:CompleteLayerUpload",
    "ecr:BatchDeleteImage",
    "ecr:UploadLayerPart",
    "ecr:DeleteRepositoryPolicy",
    "ecr:InitiateLayerUpload",
    "ecr:DeleteRepository",
    "ecr:PutImage",
    "ecr:StartImageScan",
    "ecr:TagResource",
    "ecr:UntagResource",
    "elastic-inference:Connect",
    "elasticfilesystem:DescribeFileSystems",
    "elasticfilesystem:DescribeMountTargets",
    "elasticmapreduce:DescribeCluster",
    "elasticmapreduce:ListInstanceGroups",
    "elasticmapreduce:ListClusters",
    "events:PutRule",
    "events:DescribeRule",
    "events:PutTargets",
    "events:TagResource",
    "events:ListTagsForResource",
    "fsx:DescribeFileSystems",
    "glue:SearchTables",
    "glue:NotifyEvent",
    "glue:StartBlueprintRun",
    "glue:PutWorkflowRunProperties",
    "glue:StopCrawler",
    "glue:DeleteJob",
    "glue:DeleteWorkflow",
    "glue:UpdateCrawler",
```

```
    "glue:DeleteBlueprint",
    "glue:UpdateWorkflow",
    "glue:StartCrawler",
    "glue:ResetJobBookmark",
    "glue:UpdateJob",
    "glue:StartWorkflowRun",
    "glue:StopCrawlerSchedule",
    "glue:ResumeWorkflowRun",
    "glue:DeleteCrawler",
    "glue:UpdateBlueprint",
    "glue:BatchStopJobRun",
    "glue:StopWorkflowRun",
    "glue:BatchGet*",
    "glue:UpdateCrawlerSchedule",
    "glue:DeleteConnection",
    "glue:UpdateConnection",
    "glue:Get*",
    "glue:BatchDeleteConnection",
    "glue:StartCrawlerSchedule",
    "glue:StartJobRun",
    "glue:CreateWorkflow",
    "glue:*DataQuality*",
    "glue:List*",
    "glue:CreateSession",
    "glue:RunStatement",
    "glue:BatchCreatePartition",
    "glue:CreateDatabase",
    "glue:CreatePartitionIndex",
    "glue:CreateTable",
    "glue:BatchUpdatePartition",
    "glue:BatchDeletePartition",
    "glue:UpdateTable",
    "glue:DeleteTableVersion",
    "glue:DeleteTable",
    "glue:DeleteColumnStatisticsForPartition",
    "glue:DeleteColumnStatisticsForTable",
    "glue:DeletePartitionIndex",
    "glue:UpdateColumnStatisticsForPartition",
    "glue:UpdateColumnStatisticsForTable",
    "glue:BatchDeleteTableVersion",
    "glue:BatchDeleteTable",
    "glue:CreatePartition",
    "glue:DeletePartition",
    "glue:UpdatePartition",
```

```
    "glue:CreateBlueprint",
    "glue:CreateJob",
    "glue:CreateConnection",
    "glue:CreateCrawler",
    "groundtruthlabeling:*",
    "iam:CreateServiceLinkedRole",
    "iam:GetRole",
    "iam:ListRoles",
    "iam:PassRole",
    "kms:DescribeKey",
    "kms:ListAliases",
    "kms:Decrypt",
    "kms:ListKeys",
    "kms:Encrypt",
    "kms:GenerateDataKey",
    "kms:RetireGrant",
    "lakeformation:GetDataAccess",
    "lambda:ListFunctions",
    "lambda:InvokeFunction",
    "logs:CreateLogDelivery",
    "logs:CreateLogGroup",
    "logs:CreateLogStream",
    "logs:DeleteLogDelivery",
    "logs:Describe*",
    "logs:GetLogDelivery",
    "logs:GetLogEvents",
    "logs:ListLogDeliveries",
    "logs:PutLogEvents",
    "logs:UpdateLogDelivery",
    "ram:AcceptResourceShareInvitation",
    "rds:DescribeDBInstances",
    "redshift:CreateClusterUser",
    "redshift:GetClusterCredentials",
    "redshift:GetClusterCredentialsWithIAM",
    "redshift:DescribeClusters",
    "redshift-data:BatchExecuteStatement",
    "redshift-data:CancelStatement",
    "redshift-data:DescribeStatement",
    "redshift-data:DescribeTable",
    "redshift-data:ExecuteStatement",
    "redshift-data:GetStatementResult",
    "redshift-data:ListSchemas",
    "redshift-data:ListTables",
    "redshift-serverless:ListNamespaces",
```

```
    "redshift-serverless:ListWorkgroups",
    "redshift-serverless:GetNamespace",
    "redshift-serverless:GetWorkgroup",
    "redshift-serverless:GetCredentials",
    "s3:GetBucketAcl",
    "s3:PutObjectAcl",
    "s3:GetObject",
    "s3:PutObject",
    "s3:DeleteObject",
    "s3:AbortMultipartUpload",
    "s3:CreateBucket",
    "s3:GetBucketLocation",
    "s3:ListBucket",
    "s3:ListAllMyBuckets",
    "s3:GetBucketCors",
    "s3:PutBucketCors",
    "s3:DeleteObjectVersion",
    "s3:PutObjectRetention",
    "s3:ReplicateObject",
    "s3:RestoreObject",
    "secretsmanager:ListSecrets",
    "secretsmanager:DescribeSecret",
    "secretsmanager:GetSecretValue",
    "secretsmanager:CreateSecret",
    "secretsmanager:PutResourcePolicy",
    "secretsmanager:TagResource",
    "servicecatalog:Describe*",
    "servicecatalog:List*",
    "servicecatalog:ScanProvisionedProducts",
    "servicecatalog:SearchProducts",
    "servicecatalog:SearchProvisionedProducts",
    "servicecatalog:ProvisionProduct",
    "servicecatalog:TerminateProvisionedProduct",
    "servicecatalog:UpdateProvisionedProduct",
    "sns:ListTopics",
    "sns:Subscribe",
    "sns:CreateTopic",
    "sns:Publish",
    "states:DescribeExecution",
    "states:GetExecutionHistory",
    "states:StartExecution",
    "states:StopExecution",
    "states:UpdateStateMachine",
    "tag:GetResources",
```

```
    "sso:CreateApplicationAssignment",
    "sso:AssociateProfile"
   ],
   "Resource": "*"
  }
 ]
}
```

Amazon DataZone met à jour AWS ses politiques gérées

Consultez les informations relatives aux mises à jour des politiques AWS gérées pour Amazon DataZone depuis que ce service a commencé à suivre ces modifications. Pour recevoir des alertes automatiques concernant les modifications apportées à cette page, abonnez-vous au flux RSS sur la page d'historique des DataZone documents Amazon.

Modification	Description	Date
AmazonDataZoneSageMakerEnvironmentRolePermissionsBoundary - nouvelle limite d'autorisations	Nouvelle limite d'autorisations appelée AmazonDataZoneSageMakerEnvironmentRolePermissionsBoundary. Lorsque vous créez un SageMaker environnement Amazon via le portail de DataZone données Amazon, Amazon DataZone applique cette limite d'autorisations aux rôles IAM produits lors de la création de l'environnement. La limite des autorisations limite l'étendue des rôles créés par Amazon DataZone et de tous les rôles que vous ajoutez.	30 avril 2024

Modification	Description	Date
AmazonDataZoneSage MakerAccess - nouvelle politique	La nouvelle politique appelée AmazonDataZoneSage MakerAccessdonne à Amazon l' DataZone autorisation de publier SageMaker les actifs Amazon dans le catalogue . Cela donne également à Amazon l' DataZoneautorisation d'accorder ou de révoquer l'accès aux actifs SageMaker publiés par Amazon dans le catalogue.	30 avril 2024
AmazonDataZoneFullAccess - mise à jour de la politique	Une mise à jour de la AmazonDataZoneFull Accesspolitique qui ajoute un accès à l'`DescribeS ecurityGroups` action pour améliorer la facilité d'utilisation pour les administrateurs de compte qui configurent des plans dans la console et des `GetPolicy` actions pour aider à récupérer des informations sur la politique gérée spécifiée.	30 avril 2024
AmazonDataZoneSage MakerProvisioning - nouvelle politique	La nouvelle politique appelée AmazonDataZoneSage MakerProvisioningaccorde à Amazon DataZone les autorisations nécessaires pour interagir avec Amazon SageMaker.	30 avril 2024

Modification	Description	Date
AmazonDataZoneS3Manage- <region>- <domainId>- nouveau rôle	Nouveau rôle appelé AmazonDataZoneS3Manage-<region>, <domainId>utilisé lorsqu'Amazon DataZone appelle AWS Lake Formation pour enregistrer un emplacement Amazon Simple Storage Service (Amazon S3). AWS Lake Formation assume ce rôle lors de l'accès aux données à cet emplacement.	1er avril 2024
AmazonDataZoneGlueManageAccessRolePolicy - Mise à jour de la politique	Mise à jour du AmazonDataZoneGlueManageAccessRolePolicypour permettre la prise en charge des autorisations permettant DataZone à Amazon d'activer les autorisations de publication et d'accès aux données.	1er avril 2024
AmazonDataZoneDomainExecutionRolePolicy et AmazonDataZoneFullUserAccess - Mise à jour de la politique	Mise à jour du AmazonDataZoneDomainExecutionRolePolicyet AmazonDataZoneFullUserAccesspour permettre la prise en charge de l'`CancelMetadataGenerationRun` API.	29 mars 2024

Modification	Description	Date
AmazonDataZoneFullAccess - Mise à jour de la politique	Mise à jour du `AmazonDataZoneFullAccess` pour permettre aux utilisateurs de choisir leurs secrets, leurs clusters, leurs VPC et leurs sous-réseaux dans la console de DataZone gestion Amazon plutôt que de les saisir dans une zone de texte.	13 mars 2024
AmazonDataZoneDomainExecutionRolePolicy - Mise à jour de la politique	Mise à jour du AmazonDataZoneDomainExecutionRolePolicypour permettre la prise en charge de l'`ListEnvironmentBlueprintConfigurationSummaries` API requise pour créer des profils d'environnement en identifiant quels plans sont activés dans quel compte et dans quelle région.	01 février 2024
AmazonDataZoneGlueManageAccessRolePolicy - Mise à jour de la politique	Mise à jour du AmazonDataZoneGlueManageAccessRolePolicypour permettre la prise en charge du mode hybride AWS Lake Formation.	14 décembre 2023

Modification	Description	Date
AmazonDataZoneFull UserAccess et AmazonDat aZoneDomainExecuti onRolePolicy - Mises à jour des politiques	Mise à jour des politique s AmazonDataZoneFull UserAccesset des AmazonDat aZoneDomainExecuti onRolePolicypolitiques afin de prendre en charge la fonctionnalité de descripti on des données basée sur l'IA générative sur Amazon. DataZone	28 novembre 2023
AmazonDataZoneEnvi ronmentRolePermiss ionsBoundary - Mise à jour de la politique	Amazon DataZone a mis à jour la politique AmazonDat aZoneEnvironmentRo lePermissionsBound arygérée qui consiste en une `athena:GetQueryRes ultsStream` autorisation supplémentaire limitée à la `ResourceTag` condition.	17 novembre 2023
AmazonDataZoneReds hiftManageAccessRolePolicy - Mise à jour de la politique	Amazon a DataZone mis à jour le AmazonDat aZoneRedshiftManag eAccessRolePolicyen supprimant la vérification de l'identifiant de l'organis ation pour l'`redshift: AssociateDataShare Consumer` action. Cela vous permet de partager les ressources entre les AWS organisations.	16 novembre 2023

Modification	Description	Date
AmazonDataZoneFull UserAccess - Mise à jour de la politique	Amazon a DataZone mis à jour la AmazonDataZoneFull UserAccesspolitique qui accorde un accès complet à Amazon DataZone, mais elle n'autorise pas la gestion des domaines, des utilisateurs ou des comptes associés.	2 octobre 2023
AmazonDataZonePort alFullAccessPolicy - politique déconseillée	Amazon DataZone a déconseil lé le. AmazonDataZonePort alFullAccessPolicy	29 septembre 2023
AmazonDataZonePrev iewConsoleFullAccess - politique déconseillée	Amazon DataZone a déconseil lé le. AmazonDataZonePrev iewConsoleFullAccess	29 septembre 2023

Modification	Description	Date
AmazonDataZoneDomainExecutionRolePolicy - Nouvelle politique	Amazon DataZone a ajouté une nouvelle politique appelée AmazonDataZoneDomainExecutionRolePolicy. Il s'agit de la politique par défaut pour le rôle DataZone de service Amazon `AmazonDataZoneDomainExecutionRole`. Ce rôle est utilisé par Amazon DataZone pour cataloguer, découvrir, gérer, partager et analyser les données du DataZone domaine Amazon. Vous pouvez joindre la politique `AmazonDataZoneDomainExecutionRolePolicy` à votre `AmazonDataZoneDomainExecutionRole`.	25 septembre 2023
AmazonDataZoneCrossAccountAdmin - Nouvelle politique	Amazon DataZone a ajouté une nouvelle politique appelée AmazonDataZoneCrossAccountAdminqui permet aux utilisateurs de travailler avec Amazon DataZone et ses comptes associés.	19 septembre 2023

Modification	Description	Date
AmazonDataZoneFull UserAccess - Nouvelle politique	Amazon DataZone a ajouté une nouvelle politique appelée AmazonDataZoneFull UserAccessqui accorde un accès complet à Amazon DataZone, mais elle n'autorise pas la gestion des domaines, des utilisateurs ou des comptes associés.	12 septembre 2023
AmazonDataZoneReds hiftManageAccessRolePolicy - Nouvelle politique	Amazon DataZone a ajouté une nouvelle politique appelée AmazonDataZoneReds hiftManageAccessRo lePolicyqui accorde des autorisations permettant DataZone à Amazon d'activer les autorisations de publication et d'accès aux données.	12 septembre 2023
AmazonDataZoneGlue ManageAccessRolePolicy - Nouvelle politique	Amazon DataZone a ajouté une nouvelle politique AmazonDataZoneGlue ManageAccessRolePo licyqui accorde à Amazon l' DataZone autorisation de publier les données AWS Glue dans le catalogue. Cela donne également à Amazon l' DataZone autorisation d'accorder ou de révoquer l'accès aux ressources publiées par AWS Glue dans le catalogue.	12 septembre 2023

Modification	Description	Date
AmazonDataZoneRedshiftGlueProvisioningPolicy - Nouvelle politique	Amazon DataZone a ajouté une nouvelle politique appelée AmazonDataZoneRedshiftGlueProvisioningPolicyqui accorde à Amazon DataZone les autorisations nécessaires pour interagir avec les sources de données prises en charge.	12 septembre 2023
AmazonDataZoneEnvironmentRolePermissionsBoundary - Nouvelle politique	Amazon DataZone a ajouté une nouvelle politique appelée AmazonDataZoneEnvironmentRolePermissionsBoundaryqui limite le principal IAM provisionné auquel il est attaché.	12 septembre 2023
AmazonDataZoneFullAccess - Nouvelle politique	Amazon DataZone a ajouté une nouvelle politique appelée AmazonDataZoneFullAccessqui fournit un accès complet à Amazon DataZone via la console AWS de gestion.	12 septembre 2023
Mise à jour de la stratégie gérée	Mises à jour de la politique AmazonDataZonePreviewConsoleFullAccessgérée qui consiste en des `iam:GetPolicy` autorisations supplémentaires.	13 juin 2023

Modification	Description	Date
Amazon DataZone a commencé à suivre les modifications	Amazon DataZone a commencé à suivre les modifications apportées AWS à ses politiques gérées.	20 mars 2023

Rôles IAM pour Amazon DataZone

Rubriques

AmazonDataZoneProvisioningRole-<domainAccountId>

`AmazonDataZoneProvisioningRole-<domainAccountId>`Il a la `AmazonDataZoneRedshiftGlueProvisioningPolicy` pièce jointe. Ce rôle accorde à Amazon DataZone les autorisations nécessaires pour interagir avec AWS Glue et Amazon Redshift.

La politique de confiance suivante `AmazonDataZoneProvisioningRole-<domainAccountId>` est attachée à la valeur par défaut :

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

```
      "Condition": {
        "StringEquals": {
            "aws:SourceAccount": "{{domain_account}}"
        }
      }
    }
  ]
}
```

AmazonDataZoneDomainExecutionRole

AmazonDataZoneDomainExecutionRoleLa politique AWS gérée est AmazonDataZoneDomainExecutionRolePolicyjointe. Amazon DataZone crée ce rôle pour vous en votre nom. Pour certaines actions sur le portail de données, Amazon DataZone assume ce rôle dans le compte dans lequel le rôle est créé et vérifie que ce rôle est autorisé à effectuer l'action.

Le AmazonDataZoneDomainExecutionRolerôle est obligatoire dans celui Compte AWS qui héberge votre DataZone domaine Amazon. Ce rôle est automatiquement créé pour vous lorsque vous créez votre DataZone domaine Amazon.

Le AmazonDataZoneDomainExecutionRolerôle par défaut est soumis à la politique de confiance suivante.

```
{
    "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>

Le `AmazonDataZoneGlueAccess-<region>-<domainId>` rôle comporte ce qui est `AmazonDataZoneGlueManageAccessRolePolicy` joint. Ce rôle autorise Amazon DataZone à publier les données AWS Glue dans le catalogue. Cela donne également à Amazon l' DataZone autorisation d'accorder ou de révoquer l'accès aux ressources publiées par AWS Glue dans le catalogue.

Le `AmazonDataZoneGlueAccess-<region>-<domainId>` rôle par défaut est associé à la politique de confiance suivante :

```
{
  "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>

Le `AmazonDataZoneRedshiftAccess-<region>-<domainId>` rôle comporte ce qui est `AmazonDataZoneRedshiftManageAccessRolePolicy` joint. Ce rôle autorise Amazon DataZone à publier les données Amazon Redshift dans le catalogue. Cela donne également à Amazon l' DataZone autorisation d'accorder ou de révoquer l'accès aux ressources publiées par Amazon Redshift ou Amazon Redshift Serverless dans le catalogue.

Le `AmazonDataZoneRedshiftAccess-<region>-<domainId>` rôle par défaut est associé à la politique d'autorisation intégrée suivante :

```
{
   "Version":"2012-10-17",
   "Statement":[
      {
         "Sid": "RedshiftSecretStatement",
         "Effect":"Allow",
         "Action":"secretsmanager:GetSecretValue",
         "Resource":"*",
         "Condition":{
            "StringEquals":{
               "secretsmanager:ResourceTag/AmazonDataZoneDomain":"{{domainId}}"
            }
         }
      }
   ]
}
```

La politique de confiance suivante `AmazonDataZoneRedshiftManageAccessRole<timestamp>` est attachée à la valeur par défaut :

```
{
  "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>

Le AmazonDataZone S3Manage- <region>- <domainId>est utilisé lorsqu'Amazon DataZone appelle AWS Lake Formation pour enregistrer un site Amazon Simple Storage Service (Amazon S3). AWS Lake Formation assume ce rôle lors de l'accès aux données à cet emplacement. Pour plus d'informations, consultez la section Exigences relatives aux rôles utilisés pour enregistrer des sites.

La politique d'autorisation intégrée suivante est jointe à ce rôle.

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

Le AmazonDataZone S3Manage <region>- <domainId>est associé à la politique de confiance suivante :

```
{
    "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>

Le `AmazonDataZoneSageMakerManageAccessRole` rôle a le`AmazonDataZoneSageMakerAccess`, le`AmazonDataZoneRedshiftManageAccessRolePolicy`, et ce qui `AmazonDataZoneGlueManageAccessRolePolicy` y est attaché. Ce rôle autorise Amazon à DataZone publier et à gérer les abonnements pour les actifs Data Lake, Data Warehouse et Amazon Sagemaker.

Le `AmazonDataZoneSageMakerManageAccessRole` rôle est associé à la politique en ligne suivante :

```
{
   "Version":"2012-10-17",
   "Statement":[
      {
         "Sid": "RedshiftSecretStatement",
         "Effect":"Allow",
         "Action":"secretsmanager:GetSecretValue",
         "Resource":"*",
         "Condition":{
            "StringEquals":{
               "secretsmanager:ResourceTag/AmazonDataZoneDomain":"{{domainId}}"
            }
         }
      }
   ]
}
```

Le `AmazonDataZoneSageMakerManageAccessRole` rôle est associé à la politique de confiance suivante :

```
{
  "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>

Le `AmazonDataZoneSageMakerProvisioningRole` rôle a `AmazonDataZoneSageMakerProvisioning` et ce qui `AmazonDataZoneRedshiftGlueProvisioningPolicy` y est attaché. Ce rôle accorde à Amazon DataZone les autorisations nécessaires pour interagir avec AWS Glue, Amazon Redshift et Amazon Sagemaker.

Le `AmazonDataZoneSageMakerProvisioningRole` rôle est associé à la politique en ligne suivante :

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Sid": "SageMakerStudioTagOnCreate",
            "Effect": "Allow",
            "Action": [
                "sagemaker:AddTags"
            ],
```

```
            "Resource": "arn:aws:sagemaker:*:{{AccountId}}:*/*",
            "Condition": {
                "Null": {
                    "sagemaker:TaggingAction": "false"
                }
            }
        }
    ]
}
```

Le `AmazonDataZoneSageMakerProvisioningRole` rôle est associé à la politique de confiance suivante :

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Sid": "DataZoneTrustPolicyStatement",
      "Effect": "Allow",
      "Principal": {
        "Service": "datazone.amazonaws.com"
      },
      "Action": "sts:AssumeRole",
      "Condition": {
        "StringEquals": {
            "aws:SourceAccount": "{{domain_account}}"
        }
      }
    }
  ]
}
```

Rôles basés sur l'identité

Les politiques basées sur l'identité sont des documents de politique d'autorisations JSON que vous pouvez attacher à une identité telle qu'un utilisateur, un groupe d'utilisateurs ou un rôle IAM. Ces politiques contrôlent quel type d'actions des utilisateurs et des rôles peuvent exécuter, sur quelles ressources et dans quelles conditions. Pour découvrir comment créer une politique basée sur l'identité, consultez Création de politiques IAM dans le Guide de l'utilisateur IAM.

Avec les politiques IAM basées sur l'identité, vous pouvez spécifier des actions et ressources autorisées ou refusées, ainsi que les conditions dans lesquelles les actions sont autorisées ou refusées. Vous ne pouvez pas spécifier le principal dans une politique basée sur une identité car celle-ci s'applique à l'utilisateur ou au rôle auquel elle est attachée. Pour découvrir tous les éléments que vous utilisez dans une politique JSON, consultez Références des éléments de politique JSON IAM dans le Guide de l'utilisateur IAM.

Lorsque vous créez un DataZone projet Amazon, sur le portail, trois rôles IAM sont créés pour ce projet, un pour chaque type de rôle de membre du projet : propriétaire et contributeur. Les autorisations associées à chaque rôle sont limitées au rôle du projet, et les politiques d'autorisations associées dépendent des fonctionnalités avec lesquelles le projet est déployé.

Afin qu'Amazon puisse DataZone gérer les autorisations et partager les actifs avec les projets des abonnés, les rôles d'utilisateur du projet abonné sont automatiquement ajoutés en tant qu'administrateur du lac de données AWS Lake Formation dans les actifs Compte AWS qui publient les actifs.

Vous pouvez consulter la up-to-date version la plus complète du rôle dans la console de gestion AWS IAM ou consulter les différentes autorisations de rôle dans le tableau ci-dessous.

Autorisations du propriétaire du projet

Type d'environnement	Autorisations IAM
Lac de données par défaut	Il s'agit de la combinaison des fonctionnalités Essential, Data Lake Producer et Data Lake Consumer.
Essential	{ "Version": "2012-10-17", "Statement": [{ "Effect": "Allow", "Action": ["s3:List*", "s3:Get*", "s3:Describe*",

Type d'environnement	Autorisations IAM	

```
        "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"
      ],
      "Resource":
 "keyArn",
      "Effect": "Allow"
    },
    {
```

Type d'environnement	Autorisations 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"
```

Type d'environnement	Autorisations 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"
        }
      }
    }
  ]
}
```

Type d'environnement	Autorisations IAM
Producteur 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

Type d'environnement	Autorisations 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
```

Type d'environnement	Autorisations 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",
```

Type d'environnement	Autorisations 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",
```

Type d'environnement	Autorisations 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",
```

Type d'environnement	Autorisations IAM

```
 "glue:CreateDataQu
alityRuleset"
            ],
            "Resource":
 "*"
        },
        {
            "Sid":
 "VisualEditor0",
            "Effect":
 "Allow",
            "Action": [

 "iam:ListRoles",

 "iam:ListUsers",

 "iam:ListGroups",

 "iam:ListRolePolic
ies",

 "iam:GetRole",

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

Type d'environnement	Autorisations IAM

Consommateur de 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",

Type d'environnement	Autorisations 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": [
```

Type d'environnement	Autorisations 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/*"
      ]
    }
  ]
}
```

Type d'environnement	Autorisations IAM

Producteur d'entrepôts de données	{
	  "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"
	    }
	  ]
	}

Type d'environnement	Autorisations IAM	

Type d'environnement	Autorisations IAM

Consommateur d'entrepôts de données	{
	"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"
	}

Type d'environnement	Autorisations 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" } ] }`	

Type d'environnement	Autorisations IAM	

Éditeur de requête 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",	

Type d'environnement	Autorisations 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
```

Type d'environnement	Autorisations IAM
	n:account-id:notebook/*", "arn:aws:sqlworkbench:region:account-id:connection/*", "arn:aws:sqlworkbench:region:account-id:chart/*", "arn:aws:sqlworkbench:region:account-id:/*"], "Sid": "AmazonRedshiftQueryEditorV2PermissionsPart2" }] }

Autorisations des contributeurs au projet

Type d'environnement	Autorisations IAM
Lac de données par défaut	Il s'agit de la combinaison des fonctionnalités Essential, Data Lake Producer et Data Lake Consumer.
Essential	{ "Version": "2012-10-17", "Statement": [{ "Effect": "Allow",

Type d'environnement	Autorisations 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"
      ],
```

Type d'environnement	Autorisations 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"
      ],
```

Type d'environnement	Autorisations 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"
        }
      }
    }
  ]
}
```

Type d'environnement	Autorisations IAM

Producteur 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",

Type d'environnement	Autorisations 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",
```

Type d'environnement	Autorisations 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*",
```

Type d'environnement	Autorisations 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": "*"
```

Type d'environnement	Autorisations 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": "*"
    }
  ]
}
```

Type d'environnement	Autorisations IAM

Consommateur de 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",

Type d'environnement	Autorisations 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": [
```

Type d'environnement	Autorisations 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/*"
      ]
    }
  ]
}
```

Type d'environnement	Autorisations IAM

Producteur d'entrepôts de données	{
	  "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"
	  }
	  ]
	}

Type d'environnement	Autorisations IAM	

Type d'environnement	Autorisations IAM

Consommateur d'entrepôts de données	{
	"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"
	}

Type d'environnement	Autorisations IAM	
	`}, { "Sid": "VisualEditor2", "Effect": "Allow", "Action": [ "redshift-data:DescribeStatement", "redshift-data:ExecuteStatement" ], "Resource": "arn:aws:redshift:region:account-id:cluster:cluster-identifier" } ] }`	

Type d'environnement	Autorisations IAM	

Éditeur de requête 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",	

Type d'environnement	Autorisations 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
```

Type d'environnement	Autorisations 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"
    }
  ]
}
```

Informations d'identification temporaires

Certains AWS services ne fonctionnent pas lorsque vous vous connectez à l'aide d'informations d'identification temporaires. Pour plus d'informations, notamment sur les AWS services qui fonctionnent avec des informations d'identification temporaires, consultez la section AWS Services compatibles avec IAM dans le Guide de l'utilisateur IAM.

Vous utilisez des informations d'identification temporaires si vous vous connectez à l' AWS Management Console aide d'une méthode autre qu'un nom d'utilisateur et un mot de passe. Par exemple, lorsque vous accédez à AWS l'aide du lien d'authentification unique (SSO) de votre entreprise, ce processus crée automatiquement des informations d'identification temporaires. Vous créez également automatiquement des informations d'identification temporaires lorsque vous vous connectez à la console en tant qu'utilisateur, puis changez de rôle. Pour plus d'informations sur le changement de rôle, consultez Changement de rôle (console) dans le Guide de l'utilisateur IAM.

Vous pouvez créer manuellement des informations d'identification temporaires à l'aide de l' AWS API AWS CLI or. Vous pouvez ensuite utiliser ces informations d'identification temporaires pour y accéder AWS. AWS recommande de générer dynamiquement des informations d'identification temporaires au lieu d'utiliser des clés d'accès à long terme. Pour plus d'informations, consultez Informations d'identification de sécurité temporaires dans IAM.

Autorisations de principal

Lorsque vous utilisez un utilisateur ou un rôle IAM pour effectuer des actions AWS, vous êtes considéré comme un mandant. Les politiques accordent des autorisations au principal. Lorsque vous utilisez certains services, vous pouvez effectuer une action qui déclenche une autre action dans un autre service. Dans ce cas, vous devez disposer d'autorisations nécessaires pour effectuer les deux actions. Pour savoir si une action nécessite des actions dépendantes supplémentaires dans une politique, consultez la section Actions, ressources et clés de condition pour AWS Documentation Essentials dans la référence d'autorisation de service.

Validation de conformité pour Amazon DataZone

Pour savoir si un programme Services AWS de conformité Service AWS s'inscrit dans le champ d'application de programmes de conformité spécifiques, consultez Services AWS la section de conformité et sélectionnez le programme de conformité qui vous intéresse. Pour des informations générales, voir Programmes de AWS conformité Programmes AWS de .

Vous pouvez télécharger des rapports d'audit tiers à l'aide de AWS Artifact. Pour plus d'informations, voir Téléchargement de rapports dans AWS Artifact .

Votre responsabilité en matière de conformité lors de l'utilisation Services AWS est déterminée par la sensibilité de vos données, les objectifs de conformité de votre entreprise et les lois et réglementations applicables. AWS fournit les ressources suivantes pour faciliter la mise en conformité :

- Guides de démarrage rapide sur la sécurité et la conformité : ces guides de déploiement abordent les considérations architecturales et indiquent les étapes à suivre pour déployer des environnements de base axés sur AWS la sécurité et la conformité.
- Architecture axée sur la sécurité et la conformité HIPAA sur Amazon Web Services : ce livre blanc décrit comment les entreprises peuvent créer des applications AWS conformes à la loi HIPAA.

> **Note**
>
> Tous ne Services AWS sont pas éligibles à la loi HIPAA. Pour plus d'informations, consultez le HIPAA Eligible Services Reference.

- AWS Ressources de https://aws.amazon.com/compliance/resources/ de conformité — Cette collection de classeurs et de guides peut s'appliquer à votre secteur d'activité et à votre région.
- AWS Guides de conformité destinés aux clients — Comprenez le modèle de responsabilité partagée sous l'angle de la conformité. Les guides résument les meilleures pratiques en matière de sécurisation Services AWS et décrivent les directives relatives aux contrôles de sécurité dans de nombreux cadres (notamment le National Institute of Standards and Technology (NIST), le Payment Card Industry Security Standards Council (PCI) et l'Organisation internationale de normalisation (ISO)).
- Évaluation des ressources à l'aide des règles du guide du AWS Config développeur : le AWS Config service évalue dans quelle mesure les configurations de vos ressources sont conformes aux pratiques internes, aux directives du secteur et aux réglementations.
- AWS Security Hub— Cela Service AWS fournit une vue complète de votre état de sécurité interne AWS. Security Hub utilise des contrôles de sécurité pour évaluer vos ressources AWS et vérifier votre conformité par rapport aux normes et aux bonnes pratiques du secteur de la sécurité. Pour obtenir la liste des services et des contrôles pris en charge, consultez Référence des contrôles Security Hub.
- Amazon GuardDuty — Cela Service AWS détecte les menaces potentielles qui pèsent sur vos charges de travail Comptes AWS, vos conteneurs et vos données en surveillant votre environnement pour détecter toute activité suspecte et malveillante. GuardDuty peut vous aider à répondre à diverses exigences de conformité, telles que la norme PCI DSS, en répondant aux exigences de détection des intrusions imposées par certains cadres de conformité.
- AWS Audit Manager— Cela vous Service AWS permet d'auditer en permanence votre AWS utilisation afin de simplifier la gestion des risques et la conformité aux réglementations et aux normes du secteur.

Bonnes pratiques en matière de sécurité pour Amazon DataZone

Amazon DataZone propose un certain nombre de fonctionnalités de sécurité à prendre en compte lors de l'élaboration et de la mise en œuvre de vos propres politiques de sécurité. Les bonnes

pratiques suivantes doivent être considérées comme des instructions générales et ne représentent pas une solution de sécurité complète. Étant donné que ces bonnes pratiques peuvent ne pas être appropriées ou suffisantes pour votre environnement, considérez-les comme des remarques utiles plutôt que comme des recommandations.

Implémentation d'un accès sur la base du moindre privilège

Lorsque vous accordez des autorisations, vous décidez qui obtient quelles autorisations pour quelles DataZone ressources Amazon. Vous activez des actions spécifiques que vous souhaitez autoriser sur ces ressources. Par conséquent, vous devez accorder uniquement les autorisations qui sont requises pour exécuter une tâche. L'implémentation d'un accès sur la base du moindre privilège est fondamentale pour réduire les risques en matière de sécurité et l'impact que pourraient avoir des d'erreurs ou des actes de malveillance.

Utilisation des rôles IAM

Les applications productrices et clientes doivent disposer d'informations d'identification valides pour accéder aux DataZone ressources Amazon. Vous ne devez pas stocker les AWS informations d'identification directement dans une application cliente ou dans un compartiment Amazon S3. Il s'agit d'autorisations à long terme qui ne font pas automatiquement l'objet d'une rotation et qui pourraient avoir un impact commercial important si elles étaient compromises.

Vous devez plutôt utiliser un rôle IAM pour gérer les informations d'identification temporaires permettant à vos applications productrices et clientes d'accéder aux DataZone ressources Amazon. Lorsque vous utilisez un rôle, vous n'avez pas à utiliser d'informations d'identification à long terme (par exemple, un nom d'utilisateur et un mot de passe ou des clés d'accès) pour accéder à d'autres ressources.

Pour plus d'informations, consultez les rubriques suivantes dans le Guide de l'utilisateur IAM :

- Rôles IAM
- Scénarios courants pour les rôles : utilisateurs, applications et services.

Implémentation d'un chiffrement côté serveur dans des ressources dépendantes

Les données au repos et les données en transit peuvent être cryptées sur Amazon DataZone.

CloudTrail À utiliser pour surveiller les appels d'API

Amazon DataZone est intégré à AWS CloudTrail un service qui fournit un enregistrement des actions entreprises par un utilisateur, un rôle ou un AWS service sur Amazon DataZone.

À l'aide des informations collectées par CloudTrail, vous pouvez déterminer la demande qui a été faite à Amazon DataZone, l'adresse IP à partir de laquelle la demande a été faite, l'auteur de la demande, la date à laquelle elle a été faite et des informations supplémentaires.

Résilience chez Amazon DataZone

L'infrastructure AWS mondiale est construite autour Régions AWS de zones de disponibilité. Régions AWS fournissent plusieurs zones de disponibilité physiquement séparées et isolées, connectées par un réseau à faible latence, à haut débit et hautement redondant. Avec les zones de disponibilité, vous pouvez concevoir et exploiter des applications et des bases de données qui basculent automatiquement d'une zone à l'autre sans interruption. Les zones de disponibilité sont davantage disponibles, tolérantes aux pannes et ont une plus grande capacité de mise à l'échelle que les infrastructures traditionnelles à un ou plusieurs centres de données.

Pour plus d'informations sur les zones de disponibilité Régions AWS et les zones de disponibilité, consultez la section Infrastructure AWS globale.

Outre l'infrastructure AWS mondiale, Amazon DataZone propose plusieurs fonctionnalités pour répondre à vos besoins en matière de résilience et de sauvegarde des données.

Rubriques

- Résilience des sources de données
- Résilience des actifs
- Résilience des types d'actifs et des formulaires de métadonnées
- Glossaire : résilience
- Résilience des recherches mondiales
- Résilience des abonnements
- Résilience environnementale
- Résilience du plan environnemental
- Résilience des projets
- résilience de la RAM

- Résilience de la gestion des profils utilisateur
- Résilience du domaine

Résilience des sources de données

Lors d'un événement de DataZone disponibilité d'Amazon, les `DataSource` offres d'emploi seront régulièrement réessayées pendant 24 heures au maximum. Si une tâche échoue en raison d'une mauvaise configuration, un `DataSourceRunFailed` événement sera émis. Si le DataZone domaine Amazon est configuré avec une clé KMS et qu' AmazonDataZoneDomainExecutionRole il perd l'accès à cette clé pendant l'exécution d'une tâche, l'exécution se terminera dans son `INACCESSIBLE` état actuel. Une fois l'accès KMS rétabli, la tâche doit être mise à jour manuellement pour déclencher le retour à un état utilisable.

Résilience des actifs

Dans Amazon DataZone, les actifs sont versionnés. Si une version d'un actif doit être annulée, vous pouvez créer une nouvelle version en utilisant le contenu de la dernière version stable. Une version d'un actif peut être publiée. Une version publiée d'une ressource ne peut pas être modifiée, sauf en publiant une nouvelle version. Il est possible de s'abonner à un actif publié (alias une liste). Pour empêcher de nouveaux abonnements à un actif, celui-ci peut être dépublié. L'annulation de la publication d'un actif n'a aucun effet sur les abonnements existants. La suppression d'une ressource entraîne la suppression de toutes les versions non publiées de cette ressource. Les versions publiées de la ressource doivent être supprimées séparément. Une version publiée d'un actif ne peut être supprimée que s'il n'y a aucun abonnement.

Résilience des types d'actifs et des formulaires de métadonnées

Dans Amazon DataZone, les types de ressources et les types de formulaires de métadonnées sont versionnés. Un type de ressource ne peut pas être supprimé s'il est utilisé par une ressource. Un type de formulaire de métadonnées ne peut pas être supprimé s'il est utilisé par un type de ressource ou une ressource. Si vous ne souhaitez pas que des metadata-form-type informations spécifiques soient utilisées pour la curation, vous pouvez les désactiver, sans affecter celles auxquelles elles sont déjà associées.

Glossaire : résilience

Sur Amazon DataZone, les glossaires et les termes du glossaire ne peuvent pas être supprimés s'ils sont utilisés. Si vous ne souhaitez pas qu'un glossaire ou un terme de glossaire spécifique soit utilisé pour la curation, vous pouvez les désactiver sans affecter ceux auxquels ils sont déjà attachés.

Résilience des recherches mondiales

Sur Amazon DataZone, les actifs publiés (alias listes) peuvent être découverts par le biais d'une recherche globale. La publication d'une ressource peut être annulée en annulant la publication de la ressource. L'annulation de la publication d'un actif n'a aucune incidence sur les abonnements existants. Une ressource publiée peut être ramenée à une version spécifique de la ressource en republiant cette version. Cela n'affectera pas les abonnements existants.

Résilience des abonnements

Sur Amazon DataZone, SubscriptionGrant Fulfillment tentera deux tentatives de retrait avant d'échouer. En cas d'échec, il doit être supprimé manuellement pour réessayer.
Si Amazon DataZone ne parvient pas à révoquer les autorisations relatives à un abonnement, la suppression de l'abonnement risque d'échouer. L'erreur sous-jacente doit être corrigée, ou l'`retainPermissions`indicateur peut être utilisé dans l'opération d'`DeleteSubscriptionGrant`API pour forcer la suppression de la subvention auprès d'Amazon DataZone sans révoquer les autorisations.

Si le DataZone domaine Amazon est configuré avec une clé KMS et qu'`AmazonDataZoneDomainExecutionRole`il perd l'accès à cette clé pendant le `SubscriptionGrant` flux de travail, l'autorisation est marquée`INACCESSIBLE`. Une fois l'accès KMS rétabli, les `INACCESSIBLE` autorisations doivent être supprimées et recréées.

Résilience environnementale

Si le DataZone domaine Amazon est configuré avec une clé KMS et qu'`AmazonDataZoneDomainExecutionRole`il perd l'accès à cette clé pendant le flux de travail environnemental, l'environnement sera marqué`INACCESSIBLE`. Une fois l'accès KMS rétabli, l'`INACCESSIBLE`environnement doit être supprimé et recréé. La création de l'environnement tentera deux fois de se retirer avant d'échouer. En cas d'échec, il doit être supprimé manuellement pour réessayer. Si le flux de travail environnemental échoue, l'environnement passe à l'état d'échec. À ce stade, il ne peut être que supprimé et recréé.

Résilience du plan environnemental

Dans Amazon DataZone, un plan d'environnement ne peut pas être supprimé s'il existe des profils d'environnement sous-jacents.

Résilience des projets

Dans Amazon DataZone, un projet ne peut pas être supprimé s'il existe des environnements confinés.

résilience de la RAM

Pour obtenir des informations sur la résilience de la RAM, consultez https://docs.aws.amazon.com/ram/latest/userguide/ security-disaster-recovery-resiliency .html.

Résilience de la gestion des profils utilisateur

Pour obtenir des informations sur la résilience des profils utilisateur, consultez AWS Identity Center.

Résilience du domaine

Sur Amazon DataZone, un domaine ne peut pas être supprimé s'il contient des projets ou des sources de données.

Sécurité de l'infrastructure sur Amazon DataZone

En tant que service géré, Amazon DataZone est protégé par la sécurité du réseau AWS mondial. Pour plus d'informations sur les services AWS de sécurité et sur la manière dont AWS l'infrastructure est protégée, consultez la section Sécurité du AWS cloud. Pour concevoir votre AWS environnement en utilisant les meilleures pratiques en matière de sécurité de l'infrastructure, consultez la section Protection de l'infrastructure dans le cadre AWS bien architecturé du pilier de sécurité.

Vous utilisez des appels d'API AWS publiés pour accéder à Amazon DataZone via le réseau. Les clients doivent prendre en charge les éléments suivants :

- Protocole TLS (Transport Layer Security). Nous exigeons TLS 1.2 et recommandons TLS 1.3.
- Ses suites de chiffrement PFS (Perfect Forward Secrecy) comme DHE (Ephemeral Diffie-Hellman) ou ECDHE (Elliptic Curve Ephemeral Diffie-Hellman). La plupart des systèmes modernes tels que Java 7 et les versions ultérieures prennent en charge ces modes.

En outre, les demandes doivent être signées à l'aide d'un ID de clé d'accès et d'une clé d'accès secrète associée à un principal IAM. Vous pouvez également utiliser AWS Security Token Service (AWS STS) pour générer des informations d'identification de sécurité temporaires et signer les demandes.

Prévention interservices confuse des adjoints sur Amazon DataZone

Le problème de député confus est un problème de sécurité dans lequel une entité qui n'est pas autorisée à effectuer une action peut contraindre une entité plus privilégiée à le faire. En AWS, l'usurpation d'identité interservices peut entraîner la confusion des adjoints. L'usurpation d'identité entre services peut se produire lorsqu'un service (le service appelant) appelle un autre service (le service appelé). Le service appelant peut être manipulé et ses autorisations utilisées pour agir sur les ressources d'un autre client auxquelles on ne serait pas autorisé d'accéder autrement. Pour éviter cela, AWS fournit des outils qui vous aident à protéger vos données pour tous les services auprès des principaux fournisseurs de services qui ont obtenu l'accès aux ressources de votre compte.

Nous recommandons d'utiliser la clé de contexte aws : SourceAccount global condition dans les politiques relatives aux ressources afin de limiter les autorisations qu'Amazon DataZone accorde à un autre service sur la ressource. Utilisez aws : SourceAccount si vous souhaitez autoriser l'association de toute ressource de ce compte à l'utilisation interservices.

Analyse de configuration et de vulnérabilité pour Amazon DataZone

AWS gère les tâches de sécurité de base telles que l'application de correctifs au système d'exploitation client (OS) et aux bases de données, la configuration du pare-feu et la reprise après sinistre. Ces procédures ont été vérifiées et certifiées par les tiers appropriés. Pour plus d'informations, consultez le modèle de responsabilité AWS partagée.

Domaines à ajouter à votre liste d'autorisations

Pour que le portail de DataZone données Amazon puisse accéder au DataZone service Amazon, vous devez ajouter les domaines suivants à la liste d'autorisation sur le réseau à partir duquel le portail de données tente d'accéder au service.

- `*.api.aws`
- `*.on.aws`

Surveillance d'Amazon DataZone

La surveillance joue un rôle important dans le maintien de la fiabilité, de la disponibilité et des performances d'Amazon DataZone et de vos autres AWS solutions. AWS fournit les outils de surveillance suivants pour surveiller Amazon DataZone, signaler un problème et prendre des mesures automatiques le cas échéant :

- Amazon CloudWatch surveille vos AWS ressources et les applications que vous utilisez AWS en temps réel. Vous pouvez collecter et suivre les métriques, créer des tableaux de bord personnalisés, et définir des alarmes qui vous informent ou prennent des mesures lorsqu'une métrique spécifique atteint un seuil que vous spécifiez. Par exemple, vous pouvez CloudWatch suivre l'utilisation du processeur ou d'autres indicateurs de vos instances Amazon EC2 et lancer automatiquement de nouvelles instances en cas de besoin. Pour plus d'informations, consultez le guide de CloudWatch l'utilisateur Amazon.
- Amazon CloudWatch Logs vous permet de surveiller, de stocker et d'accéder à vos fichiers journaux à partir d'instances Amazon EC2 et d'autres sources. CloudTrail CloudWatch Les journaux peuvent surveiller les informations contenues dans les fichiers journaux et vous avertir lorsque certains seuils sont atteints. Vous pouvez également archiver vos données de journaux dans une solution de stockage hautement durable. Pour plus d'informations, consultez le guide de l'utilisateur d'Amazon CloudWatch Logs.
- Amazon EventBridge peut être utilisé pour automatiser vos AWS services et répondre automatiquement aux événements du système, tels que les problèmes de disponibilité des applications ou les modifications des ressources. Les événements AWS liés aux services sont diffusés EventBridge en temps quasi réel. Vous pouvez écrire des règles simples pour préciser les événements qui vous intéressent et les actions automatisées à effectuer quand un événement correspond à une règle. Pour plus d'informations, consultez le guide de EventBridge l'utilisateur Amazon.
- AWS CloudTrailcapture les appels d'API et les événements associés effectués par ou pour le compte de votre AWS compte et envoie les fichiers journaux dans un compartiment Amazon S3 que vous spécifiez. Vous pouvez identifier les utilisateurs et les comptes appelés AWS, l'adresse IP source à partir de laquelle les appels ont été effectués et la date des appels. Pour plus d'informations, consultez le Guide de l'utilisateur AWS CloudTrail.

Surveillance d'Amazon DataZone avec Amazon CloudWatch

Vous pouvez surveiller Amazon DataZone en utilisant CloudWatch, qui collecte les données brutes et les traite en métriques lisibles en temps quasi réel. Ces statistiques sont enregistrées pour une durée de 15 mois ; par conséquent, vous pouvez accéder aux informations historiques et acquérir un meilleur point de vue de la façon dont votre service ou application web s'exécute. Vous pouvez également définir des alarmes qui surveillent certains seuils et envoient des notifications ou prennent des mesures lorsque ces seuils sont atteints. Pour plus d'informations, consultez le guide de CloudWatch l'utilisateur Amazon.

Le portail de DataZone données Amazon utilise les API du plan de DataZone données Amazon avec authentification et autorisation JWT. Amazon DataZone assume le rôle de service DataZone par défaut d'Amazon et enregistre tous les appels d' DataZoneAPI Amazon effectués via le portail de DataZone données Amazon dans un groupe de journaux nommé DataZoneDataPortalAPI CallLogs.

Surveillance des DataZone événements Amazon sur Amazon EventBridge

Vous pouvez surveiller les DataZone événements Amazon dans EventBridge, qui fournit un flux de données en temps réel à partir de vos propres applications, applications software-as-a-service (SaaS) et AWS services. EventBridgeachemine ces données vers des cibles telles qu' AWS Lambda Amazon Simple Notification Service. Ces événements sont les mêmes que ceux qui apparaissent dans Amazon CloudWatch Events, qui fournit un flux quasi en temps réel d'événements système décrivant les modifications apportées aux AWS ressources.

Pour plus d'informations, voir Utilisation des événements via le bus EventBridge par défaut d'Amazon.

Journalisation des appels d' DataZone API Amazon à l'aide de AWS CloudTrail

Amazon DataZone est intégré à AWS CloudTrail un service qui fournit un enregistrement des actions entreprises par un utilisateur, un rôle ou un AWS service sur Amazon DataZone. CloudTrail capture tous les appels d'API pour Amazon DataZone sous forme d'événements. Les appels capturés incluent des appels provenant de la DataZone console Amazon et des appels de code vers les opérations de DataZone l'API Amazon. Si vous créez un suivi, vous pouvez activer la diffusion

continue d' CloudTrailévénements vers un compartiment Amazon S3, y compris des événements pour Amazon DataZone. Si vous ne configurez pas de suivi, vous pouvez toujours consulter les événements les plus récents dans la CloudTrail console dans Historique des événements. À l'aide des informations collectées par CloudTrail, vous pouvez déterminer la demande qui a été faite à Amazon DataZone, l'adresse IP à partir de laquelle la demande a été faite, l'auteur de la demande, la date à laquelle elle a été faite et des informations supplémentaires.

Pour en savoir plus CloudTrail, consultez le guide de AWS CloudTrail l'utilisateur.

DataZone Informations Amazon dans CloudTrail

CloudTrail est activé sur votre compte Compte AWS lorsque vous créez le compte. Lorsqu'une activité se produit dans la console DataZone de gestion Amazon, cette activité est enregistrée dans un CloudTrail événement avec d'autres événements de AWS service dans l'historique des événements. Vous pouvez consulter, rechercher et télécharger les événements récents dans votre Compte AWS. Pour plus d'informations, consultez la section Affichage des événements à l'aide de l'historique des CloudTrail événements.

Pour un enregistrement continu des événements de votre entreprise Compte AWS, y compris des événements pour Amazon DataZone, créez un parcours. Un suivi permet CloudTrail de fournir des fichiers journaux à un compartiment Amazon S3. Par défaut, lorsque vous créez un journal d'activité dans la console, il s'applique à toutes les régions Régions AWS. Le journal enregistre les événements de toutes les régions de la AWS partition et transmet les fichiers journaux au compartiment Amazon S3 que vous spécifiez. En outre, vous pouvez configurer d'autres AWS services pour analyser plus en détail les données d'événements collectées dans les CloudTrail journaux et agir en conséquence. Pour plus d'informations, consultez les ressources suivantes :

- Présentation de la création d'un journal de suivi
- CloudTrail services et intégrations pris en charge
- Configuration des notifications Amazon SNS pour CloudTrail
- Réception de fichiers CloudTrail journaux de plusieurs régions et réception de fichiers CloudTrail journaux de plusieurs comptes

Toutes les DataZone actions d'Amazon sont enregistrées par CloudTrail.

Résolution des problèmes liés à Amazon DataZone

Si vous rencontrez des problèmes de refus d'accès ou des difficultés similaires lorsque vous travaillez avec Amazon, DataZone consultez les rubriques de cette section.

Résolution des problèmes liés aux autorisations de AWS Lake Formation pour Amazon DataZone

Cette section contient des instructions de dépannage pour les problèmes que vous pourriez rencontrer lorsque vous Configurer les autorisations de Lake Formation pour Amazon DataZone

Message d'erreur dans le portail de données	Résolution
Impossible d'assumer le rôle d'accès aux données.	Cette erreur s'affiche lorsqu'Amazon n' DataZone est pas en mesure de supposer AmazonDataZoneGlueDataAccessRoleque vous avez utilisé pour activer le DefaultDa taLakeBlueprintdans votre compte. Pour résoudre le problème, accédez à la console AWS IAM du compte sur lequel se trouve votre ressource de données et assurez-vous qu'il existe AmazonDataZoneGlueDataAcces sRoleune relation de confiance appropriée avec le responsable du DataZone service Amazon. Pour plus d'informations, consultez AmazonDat aZoneGlueAccess- <region>- <domainId>.
Le rôle d'accès aux données ne dispose pas des autorisations nécessaires pour lire les métadonnées de la ressource à laquelle vous essayez de vous abonner.	Cette erreur s'affiche lorsqu'Amazon assume DataZone avec succès le AmazonDat aZoneGlueDataAccessRolerôle, mais que celui-ci ne dispose pas des autorisations nécessaires. Pour résoudre le problème, accédez à la console AWS IAM du compte auquel se trouve votre ressource de données et assurez-vous que le rôle est AmazonDat aZoneGlueManageAccessRolePolicyassocié à

Message d'erreur dans le portail de données	Résolution
	ce dernier. Pour plus d'informations, consultez AmazonDataZoneGlueAccess- <region>-<domainId>.
L'actif est un lien vers une ressource. Amazon DataZone ne prend pas en charge les abonnements à des liens vers des ressources.	Cette erreur s'affiche lorsque la ressource que vous essayez de publier sur Amazon DataZone est un lien de ressource vers une table AWS Glue.

Message d'erreur dans le portail de données	Résolution
L'actif n'est pas géré par AWS Lake Formation.	Cette erreur indique que les autorisations de AWS Lake Formation ne sont pas appliquées à la ressource que vous souhaitez publier. Cela peut se produire dans les cas suivants. • L'emplacement Amazon S3 de la ressource n'est pas enregistré dans AWS Lake Formation. Pour résoudre le problème, connectez-vous à votre console AWS Lake Formation dans le compte sur lequel se trouve la table et enregistrez l'emplacement Amazon S3 en mode AWS Lake Formation ou en mode hybride. Pour plus d'informations, consultez la rubrique Enregistrement d'un emplacement Amazon S3. Plusieurs scénarios nécessitent des modifications supplémentaires. Il s'agit notamment de compartiments Amazon S3 cryptés ou d'un compartiment S3 multi-comptes et d'une configuration Glue AWS Catalog. Dans de tels cas, des modifications des paramètres KMS et/ou S3 peuvent être nécessaires. Pour plus d'informations, consultez la rubrique Enregistrement d'un emplacement Amazon S3 chiffré. • L'emplacement Amazon S3 est enregistré en mode AWS Lake Formation mais IAM AllowedPrincipal est ajouté aux autorisations de la table. Pour résoudre le problème, vous pouvez soit supprimer l'IAM AllowedPrincipal des autorisations de la table, soit enregistrer l'emplacement S3 en mode hybride. Pour plus d'informations, voir À propos de la mise à niveau vers le modèle d'autorisations de Lake Formation. Si votre position S3 est

Message d'erreur dans le portail de données	Résolution
	cryptée ou si elle se trouve sur un compte différent de celui de votre table AWS Glue, suivez les instructions de la section Enregistrer une position Amazon S3 cryptée.
Le rôle Data Access ne dispose pas des autorisations Lake Formation nécessaires pour accorder l'accès à cette ressource.	Cette erreur indique que le AmazonDataZoneGlueDataAccessRolefichier que vous utilisez pour activer le DefaultDataLakeBlueprintdans votre compte ne dispose pas des autorisations nécessaires pour qu'Amazon puisse DataZone gérer les autorisations sur l'actif publié. Vous pouvez résoudre le problème soit en l'ajoutant en AmazonDataZoneGlueDataAccessRoletant qu'administrateur de AWS Lake Formation, soit en accordant les autorisations suivantes AmazonDataZoneGlueDataAccessRoleà la ressource que vous souhaitez publier. • Décrire et décrire les autorisations pouvant être accordées sur la base de données où se trouve l'actif • Décrivez, sélectionnez, décrivez les autorisations pouvant être accordées, sélectionnez les autorisations pouvant être accordées sur tous les actifs de la base de données dont vous souhaitez qu'Amazon gère l'accès en votre nom. DataZone

Quotas pour Amazon DataZone

Votre AWS compte dispose de quotas par défaut, anciennement appelés limites, pour chaque AWS service. Sauf indication contraire, chaque quota est spécifique à une région.

Amazon DataZone applique les quotas et limites suivants.

Ressource	Description	Valeur
Types de ressources de données	Nombre maximal de types de ressources de données pouvant être créés dans un DataZone domaine	1 000
Actifs de données	Le nombre maximum de ressources de données pouvant être créées dans un DataZone domaine Amazon	1 million
Glossaires	Le nombre maximum de glossaires commerciaux que vous pouvez créer dans un domaine	1 000
Termes du glossaire commercial	Le nombre maximum de termes du glossaire commercial que vous pouvez créer dans un domaine	10 000
Environnements d'un domaine	Le nombre maximum d'environnements dans un DataZone domaine Amazon	500

Historique du document pour le guide de DataZone l'utilisateur Amazon

Le tableau suivant décrit les versions de documentation pour Amazon DataZone.

Modification	Description	Date
AmazonDataZoneSageMakerProvisioning - nouvelle politique	La nouvelle politique appelée AmazonDataZoneSageMakerProvisioningaccorde à Amazon DataZone les autorisations nécessaires pour interagir avec Amazon SageMaker. Pour plus d'informations, consultez les DataZone mises à jour des politiques AWS gérées par Amazon.	30 avril 2024
AmazonDataZoneSageMakerEnvironmentRolePermissionsBoundary - nouvelle limite d'autorisations	Nouvelle limite d'autorisations appelée AmazonDataZoneSageMakerEnvironmentRolePermissionsBoundary. Lorsque vous créez un SageMaker environnement Amazon via le portail de DataZone données Amazon, Amazon DataZone applique cette limite d'autorisations aux rôles IAM produits lors de la création de l'environnement. La limite des autorisations limite l'étendue des rôles créés par Amazon DataZone et de tous les rôles que vous ajoutez. Pour plus d'informa	30 avril 2024

	tions, consultez les DataZone mises à jour des politiques AWS gérées par Amazon.	
AmazonDataZoneSageMakerAccess - nouvelle politique	Une nouvelle politique appelée AmazonDataZoneSageMakerAccessaccorde à Amazon DataZone les autorisations requises pour accorder aux utilisateurs l'accès à diverses ressources de l' SageMakerenvironnement Amazon. Pour plus d'informations, consultez les DataZone mises à jour des politiques AWS gérées par Amazon.	30 avril 2024
AmazonDataZoneFullAccess - mise à jour de la politique	Une mise à jour de la AmazonDataZoneFullAccesspolitique qui ajoute un accès à l'`DescribeSecurityGroups` action pour améliorer la facilité d'utilisation pour les administrateurs de compte qui configurent des plans dans la console et des `GetPolicy` actions pour aider à récupérer des informations sur la politique gérée spécifiée. Pour plus d'informations, consultez les DataZone mises à jour des politiques AWS gérées par Amazon.	30 avril 2024

AmazonDataZoneS3Manage- - nouveau rôle <region>< domainId>	Nouveau rôle appelé AmazonDataZoneS3Ma nage-<region>, <domainId >utilisé lorsqu'Amazon DataZone appelle AWS Lake Formation pour enregistrer un emplacement Amazon Simple Storage Service (Amazon S3). AWS Lake Formation assume ce rôle lors de l'accès aux données à cet emplaceme nt. Pour plus d'informations, consultez les DataZone mises à jour des politiques AWS gérées par Amazon.	1er avril 2024
AmazonDataZoneGlue ManageAccessRolePolicy - Mise à jour de la politique	Mise à jour du AmazonDat aZoneGlueManageAcc essRolePolicypour permettre la prise en charge des autorisations permettant DataZone à Amazon d'activer les autorisations de publication et d'accès aux données. Pour plus d'informations, consultez les DataZone mises à jour des politiques AWS gérées par Amazon.	1er avril 2024

AmazonDataZoneDomainExecutionRolePolicy et AmazonDataZoneFullUserAccess - Mise à jour de la politique	Mise à jour du AmazonDataZoneDomainExecutionRolePolicyet AmazonDataZoneFullUserAccesspour permettre la prise en charge de l'`CancelMetadataGenerationRun` API. Pour plus d'informations, consultez les DataZone mises à jour des politiques AWS gérées par Amazon.	29 mars 2024
AmazonDataZoneFullAccess - Mise à jour de la politique	Mise à jour du `AmazonDataZoneFullAccess` pour permettre aux utilisateurs de choisir leurs secrets, leurs clusters, leurs VPC et leurs sous-réseaux dans la console de DataZone gestion Amazon plutôt que de les saisir dans une zone de texte. Pour plus d'informations, consultez les DataZone mises à jour des politiques AWS gérées par Amazon.	13 mars 2024

AmazonDataZoneDomainExecutionRolePolicy - Mise à jour de la politique	Mise à jour du AmazonDataZoneDomainExecutionRolePolicypour permettre la prise en charge de l' ListEnvironmentBlueprintConfigurationSummaries API requise pour créer des profils d'environnement en identifiant quels plans sont activés dans quel compte et dans quelle région. Pour plus d'informations, consultez les DataZone mises à jour des politiques AWS gérées par Amazon.	1 février 2024
AmazonDataZoneGlueManageAccessRolePolicy - Mise à jour de la politique	Mise à jour du AmazonDataZoneGlueManageAccessRolePolicypour permettre la prise en charge du mode hybride AWS Lake Formation . Pour plus d'informations, consultez les DataZone mises à jour des politiques AWS gérées par Amazon.	14 décembre 2023

AmazonDataZoneFullUserAccess et AmazonDataZoneDomainExecutionRolePolicy - Mises à jour des politiques	Amazon a DataZone mis à jour les politiques AmazonDataZoneFullUserAccesset les AmazonDataZoneDomainExecutionRolePolicypolitiques afin de prendre en charge la fonctionnalité de description des données basée sur l'IA générative d'Amazon. DataZone Pour plus d'informations, consultez les DataZone mises à jour des politiques AWS gérées par Amazon.	28 novembre 2023
AmazonDataZoneEnvironmentRolePermissionsBoundary - Mise à jour de la politique	Amazon DataZone a mis à jour la politique AmazonDataZoneEnvironmentRolePermissionsBoundarygérée qui consiste en une `athena:GetQueryResultsStream` autorisation supplémentaire limitée à la `ResourceTag` condition . Pour plus d'informations, consultez les DataZone mises à jour des politiques AWS gérées par Amazon.	17 novembre 2023

AmazonDataZoneRedshiftManageAccessRolePolicy - Mise à jour de la politique	Amazon a DataZone mis à jour la AmazonDataZoneRedshiftManageAccessRolePolicypolitique en supprimant la vérification de l'identifiant de l'organisation pour `redshift:AssociateDataShareConsumer` cette action. Cela vous permet de partager les ressources entre les AWS organisations. Pour plus d'informations, consultez les DataZone mises à jour des politiques AWS gérées par Amazon.	16 novembre 2023
AmazonDataZoneFullUserAccess - Mise à jour de la politique	Amazon a DataZone mis à jour la AmazonDataZoneFullUserAccesspolitique qui accorde un accès complet à Amazon DataZone, mais elle n'autorise pas la gestion des domaines, des utilisateurs ou des comptes associés. Pour plus d'informations, consultez les DataZone mises à jour des politiques AWS gérées par Amazon.	2 octobre 2023
AmazonDataZonePreviewConsoleFullAccess - politique déconseillée	Amazon DataZone a déconseillé le AmazonDataZonePreviewConsoleFullAccess. Pour plus d'informations, consultez les DataZone mises à jour des politiques gérées par Amazon. AWS	29 septembre 2023

AmazonDataZonePortalFullAccessPolicy - politique déconseillée	Amazon DataZone a déconseillé le AmazonDataZonePortalFullAccessPolicy. Pour plus d'informations, consultez les DataZone mises à jour des politiques gérées par Amazon. AWS	29 septembre 2023
AmazonDataZoneDomainExecutionRolePolicy - Nouvelle politique	Amazon DataZone a ajouté une nouvelle politique appelée AmazonDataZoneDomainExecutionRolePolicy. Il s'agit de la politique par défaut pour le rôle DataZone `AmazonDataZoneDomainExecutionRole` de service Amazon. Ce rôle est utilisé par Amazon DataZone pour cataloguer, découvrir, gérer, partager et analyser les données du DataZone domaine Amazon. Vous pouvez joindre la `AmazonDataZoneDomainExecutionRolePolicy` politique à votre`AmazonDataZoneDomainExecutionRole` . Pour plus d'informations, consultez les DataZone mises à jour des politiques AWS gérées par Amazon.	25 septembre 2023

AmazonDataZoneCrossAccountAdmin - Nouvelle politique	Amazon DataZone a ajouté une nouvelle politique appelée AmazonDataZoneCrossAccountAdminqui permet aux utilisateurs de travailler avec Amazon DataZone et ses comptes associés. Pour plus d'informations, consultez les DataZone mises à jour des politiques AWS gérées par Amazon.	19 septembre 2023
AmazonDataZoneRedshiftManageAccessRolePolicy - Nouvelle politique	Amazon DataZone a ajouté une nouvelle politique appelée AmazonDataZoneRedshiftManageAccessRolePolicyqui accorde des autorisations permettant DataZone à Amazon d'activer les autorisations de publication et d'accès aux données. Pour plus d'informations, consultez les DataZone mises à jour des politiques AWS gérées par Amazon.	12 septembre 2023

AmazonDataZoneRedshiftGlueProvisioningPolicy - Nouvelle politique	Amazon DataZone a ajouté une nouvelle politique appelée AmazonDataZoneRedshiftGlueProvisioningPolicyqui accorde à Amazon DataZone les autorisations nécessaires pour interagir avec les sources de données prises en charge. Pour plus d'informations, consultez les DataZone mises à jour des politiques AWS gérées par Amazon.	12 septembre 2023
AmazonDataZoneGlueManageAccessRolePolicy - Nouvelle politique	Amazon DataZone a ajouté une nouvelle politique qui AmazonDataZoneGlueManageAccessRolePolicyaccorde à Amazon l' DataZoneautorisation de publier les données AWS Glue dans le catalogue. Cela donne également à Amazon l' DataZoneautorisation d'accorder ou de révoquer l'accès aux ressources publiées par AWS Glue dans le catalogue. Pour plus d'informations, consultez les DataZone mises à jour des politiques AWS gérées par Amazon.	12 septembre 2023

AmazonDataZoneFull UserAccess - Nouvelle politique	Amazon DataZone a ajouté une nouvelle politique appelée AmazonDataZoneFull UserAccessqui accorde un accès complet à Amazon DataZone via le portail de données. Pour plus d'informations, consultez les DataZone mises à jour des politiques AWS gérées par Amazon.	12 septembre 2023
AmazonDataZoneFullAccess - Nouvelle politique	Amazon DataZone a ajouté une nouvelle politique appelée AmazonDataZoneFull Accessqui fournit un accès complet à Amazon DataZone via la console AWS de gestion. Pour plus d'informations, consultez les DataZone mises à jour des politiques AWS gérées par Amazon.	12 septembre 2023
AmazonDataZoneEnvironmentRolePermissionsBoundary - Nouvelle politique	Amazon DataZone a ajouté une nouvelle politique appelée AmazonDataZoneEnvironmentRolePermissionsBoundaryqui limite le principal IAM provisionné auquel il est attaché. Pour plus d'informations, consultez les DataZone mises à jour des politiques AWS gérées par Amazon.	12 septembre 2023

Mise à jour des politiques gérées	Mises à jour de la politique AmazonDataZonePrev iewConsoleFullAccess gérée. Pour plus d'informations, consultez les DataZone mises à jour des politiques AWS gérées par Amazon.	13 juin 2023
Mise à jour des politiques gérées	Mises à jour de la politique AmazonDataZoneProj ectDeploymentPermi ssionsBoundary gérée. Pour plus d'informations, consultez les DataZone mises à jour des politiques AWS gérées par Amazon.	3 avril 2023
???	Première publication du guide de l'utilisateur Amazon DataZone (version prélimina ire).	29 mars 2023

Les traductions sont fournies par des outils de traduction automatique. En cas de conflit entre le contenu d'une traduction et celui de la version originale en anglais, la version anglaise prévaudra.