aws

Guía del usuario

Amazon DataZone

Amazon DataZone: Guía del usuario

Table of Contents

¿Qué es Amazon DataZone?

Amazon DataZone es un servicio de administración de datos que te permite catalogar, descubrir, compartir y gestionar los datos almacenados en AWS fuentes locales y de terceros de forma más rápida y sencilla. Con Amazon DataZone, los administradores que supervisan los activos de datos de la organización pueden gestionar y controlar el acceso a los datos mediante controles detallados. Estos controles ayudan a garantizar el acceso con el nivel adecuado de privilegios y contexto. Amazon DataZone facilita a los ingenieros, científicos de datos, gerentes de productos, analistas y usuarios empresariales el acceso a los datos y el acceso a ellos en toda la organización para que puedan descubrir, usar y colaborar para obtener información basada en datos.

Amazon le DataZone ayuda a entregar los datos directamente a los usuarios finales y simplifica su arquitectura mediante la integración de servicios de gestión de datos, incluidos Amazon Redshift, Amazon Athena QuickSight, Amazon, Glue AWS , Lake AWS Formation, fuentes locales, fuentes de terceros y más.

Temas

¿Qué puedo hacer con Amazon DataZone?

Con Amazon DataZone, puedes hacer lo siguiente:

- Controle el acceso a los datos más allá de los límites organizacionales. Con Amazon DataZone, puedes ayudar a garantizar que el usuario correcto acceda a los datos correctos con el propósito correcto, de acuerdo con las normas de seguridad de tu organización, sin depender de credenciales individuales. También puedes ofrecer transparencia sobre el uso de los activos de datos y aprobar las suscripciones de datos con un flujo de trabajo regulado. También puede supervisar los activos de datos en todos los proyectos mediante las funciones de auditoría de uso.
- Conecte a los trabajadores de datos a través de datos y herramientas compartidos para obtener información empresarial. Con Amazon DataZone, puedes aumentar la eficiencia del equipo empresarial colaborando sin problemas entre los equipos y proporcionando acceso de autoservicio a las herramientas de datos y análisis. Puedes usar términos empresariales para buscar, compartir

y acceder a los datos catalogados almacenados en AWS, de forma local o con proveedores externos. Además, puedes obtener más información sobre los datos que quieres usar utilizando los glosarios DataZone empresariales de Amazon.

- Automatice el descubrimiento y la catalogación de datos con el aprendizaje automático. Con Amazon DataZone, puede reducir el tiempo dedicado a la introducción manual de los atributos de datos en el catálogo de datos empresariales. Los datos más detallados del catálogo de datos también mejoran la experiencia de búsqueda.

¿Cómo DataZone apoya Amazon otros AWS servicios y se integra con ellos?

Amazon DataZone admite tres tipos de integraciones con otros AWS servicios:

- Fuentes de datos de productores: puede publicar activos de datos en el DataZone catálogo de Amazon a partir de los datos almacenados en las tablas y vistas de AWS Glue Data Catalog y Amazon Redshift. También puede publicar objetos manualmente desde Amazon Simple Storage Service (S3) en el catálogo de Amazon DataZone .
- Herramientas para consumidores: puede utilizar los editores de consultas de Amazon Athena o Amazon Redshift para acceder a sus activos de datos y analizarlos.
- Control de acceso y gestión logística: Amazon DataZone apoya la concesión de acceso a las tablas AWS Glue gestionadas por AWS Lake Formation y a las tablas y vistas de Amazon Redshift. Para todos los demás activos de datos, Amazon DataZone publica los eventos estándar relacionados con tus acciones (por ejemplo, la aprobación de una solicitud de suscripción) en Amazon EventBridge. Puedes usar estos eventos estándar para integrarlos con otros AWS servicios o soluciones de terceros para realizar integraciones personalizadas.

¿Cómo puedo acceder a Amazon DataZone?

Puedes acceder a Amazon DataZone de cualquiera de las siguientes maneras:

- DataZone Consola Amazon

  Puedes usar la consola de DataZone administración de Amazon para acceder a tus DataZone dominios, blueprints y usuarios de Amazon y configurarlos. Para obtener más información, consulte https://console.aws.amazon.com/datazone. La consola DataZone de administración de Amazon también se utiliza para crear el portal de DataZone datos de Amazon.

- Portal de DataZone datos de Amazon

  El portal de DataZone datos de Amazon es una aplicación web basada en un navegador en la que puede catalogar, descubrir, gobernar, compartir y analizar datos de forma autoservicio. El portal de datos puede autenticarlo con las credenciales de su proveedor de identidad a través del Centro de Identidad de AWS IAM (sucesor del AWS SSO) o con sus credenciales de IAM. Puede obtener la URL del portal de datos accediendo a la DataZone consola de Amazon en https://console.aws.amazon.com/datazone.

- API DataZone HTTPS de Amazon

  Puedes acceder a Amazon mediante DataZone programación mediante la API DataZone HTTPS de Amazon, que te permite enviar solicitudes HTTPS directamente al servicio. Para obtener más información, consulta la referencia de la DataZone API de Amazon.

DataZone Terminología y conceptos de Amazon

Al empezar con Amazon DataZone, es importante que comprenda sus conceptos, terminología y componentes clave.

Temas

DataZone Componentes de Amazon

Amazon DataZone incluye los cuatro componentes principales siguientes:

- Catálogo de datos empresariales: puede utilizar este componente para catalogar los datos de su organización en función del contexto empresarial y, de este modo, permitir que todos los miembros de la organización encuentren y comprendan los datos rápidamente.
- Publique y suscriba flujos de trabajo: puede utilizar estos flujos de trabajo automatizados para proteger los datos entre productores y consumidores de forma autónoma y garantizar que todos los miembros de su organización tengan acceso a los datos correctos para el propósito correcto.
- Proyectos y entornos
  - En Amazon, DataZone los proyectos son agrupaciones de personas, activos (datos) y herramientas basadas en casos de uso empresarial que se utilizan para simplificar el acceso a los análisis. AWS Los proyectos proporcionan áreas en las que los miembros del proyecto pueden colaborar, intercambiar datos y compartir activos. De forma predeterminada, los proyectos están configurados para que solo aquellos que se agreguen explícitamente al proyecto puedan acceder a los datos y las herramientas de análisis que contienen. Los proyectos gestionan la propiedad de los activos producidos de acuerdo con las políticas del proyecto a los que pueden acceder los consumidores de datos.

    - En DataZone los proyectos de Amazon, los entornos son conjuntos de cero o más recursos configurados (por ejemplo, un bucket de Amazon S3, una AWS Glue base de datos o un grupo de trabajo de Amazon Athena) en los que puede operar un conjunto determinado de principios de IAM (por ejemplo, usuarios con permisos de colaborador).
- Portal de datos (fuera de la consola de AWS administración): se trata de una aplicación web basada en un navegador a la que diferentes usuarios pueden ir a catalogar, descubrir, gobernar, compartir y analizar datos de forma autoservicio. El portal de datos autentica a los usuarios con credenciales de IAM o con las credenciales existentes de su proveedor de identidad. AWS IAM Identity Center

¿Qué son los DataZone dominios de Amazon?

Puedes usar DataZone los dominios de Amazon para organizar tus activos, usuarios y sus proyectos. Al asociar AWS cuentas adicionales a tus DataZone dominios de Amazon, puedes agrupar tus fuentes de datos. A continuación, puede publicar activos de estas fuentes de datos en el catálogo de su dominio, con formularios de metadatos y glosarios que mejoran la integridad y la calidad de los metadatos. También puedes buscar y explorar estos recursos para ver qué datos están publicados en el dominio. Además, puede unirse a proyectos para colaborar con otros usuarios, suscribirse a activos y utilizar entornos de proyectos para acceder a herramientas de análisis, como Amazon Athena y Amazon Redshift. DataZone Los dominios de Amazon le ofrecen la flexibilidad necesaria para reflejar las necesidades de datos y análisis de su estructura organizativa, ya sea que se trate de crear un único DataZone dominio de Amazon para su empresa o varios DataZone dominios de Amazon para diferentes unidades de negocio.

¿Qué son los DataZone proyectos y entornos de Amazon?

Amazon DataZone permite a los equipos y a los usuarios de análisis colaborar en proyectos mediante la creación de agrupaciones de equipos, herramientas y datos basadas en casos de uso.

- En Amazon DataZone, los proyectos permiten a un grupo de usuarios colaborar en varios casos de uso empresarial que implican publicar, descubrir, suscribirse y consumir datos del DataZone catálogo de Amazon. Los miembros del proyecto consumen activos del DataZone catálogo de Amazon y producen nuevos activos mediante uno o más flujos de trabajo analíticos. Los proyectos respaldan las siguientes actividades dentro del portal de datos:
    - Los propietarios de los proyectos pueden añadir miembros con permisos de propietario y colaborador

- Los miembros del proyecto pueden ser usuarios de SSO, grupos de SSO y usuarios de IAM
- Los miembros del proyecto pueden solicitar la suscripción a los activos del catálogo de datos

  Las aprobaciones de suscripción se proporcionan a los proyectos
- En un DataZone proyecto de Amazon, los entornos son conjuntos de cero o más recursos configurados (por ejemplo, Amazon S3, una AWS Glue base de datos o un grupo de trabajo de Amazon Athena), con un conjunto determinado de directores de IAM que pueden operar con esos recursos. Los entornos se crean mediante perfiles de entorno, que son conjuntos de recursos y planos preconfigurados que proporcionan plantillas reutilizables para crear entornos. Los perfiles de entorno definen ajustes como la región Cuenta de AWS o la región en la que se implementan los entornos.

¿Qué son los DataZone planos de Amazon?

El plano con el que se crea el entorno define qué AWS herramientas y servicios (por ejemplo, AWS Glue Amazon Redshift) pueden utilizar los miembros del proyecto al que pertenece el entorno cuando trabajan con los activos del catálogo de Amazon DataZone .

En la versión actual de Amazon DataZone, se admiten los siguientes blueprints predeterminados:

Nombre del plano	Descripción	Recursos creados
Plano de Data Lake	Permite a los miembros del DataZone proyecto Amazon lanzar servicios para productor es y consumidores de Data Lake en el entorno. Como consumidor, permite a los miembros del DataZone proyecto de Amazon acceder a una copia de «solo lectura» de los activos gestionados por Lake Formation directamente en Amazon Athena y en otros motores de consulta compatibl es con Lake Formation.	Ofrece a los usuarios la posibilidad de crear y consultar tablas de Lake Formation con Amazon Athena. Grupo de trabajo de Amazon Athena, AWS Glue base de datos con permisos de «solo lectura» de Lake Formation, permisos de IAM de «solo lectura» y acceso a Amazon S3 administrado por el proyecto. AWS Glue base de datos con permisos de «creación» y «concesión» de

Nombre del plano	Descripción	Recursos creados
	Como productor, permite a los miembros DataZone del proyecto de Amazon crear nuevas tablas LakeForma tion gestionadas con Amazon Athena y publicarlas en el catálogo de Amazon DataZone.	Lake Formation, permisos de IAM de «lectura» y «escritur a», AWS Glue ETL (extracci ón, transformación y carga) con etiquetado.
Plano de almacén de datos	Como consumidores, este plan permite a los miembros DataZone del proyecto de Amazon conectarse a sus propios clústeres de Amazon Redshift para consultar almacenes de datos remotos y crear y almacenar nuevos conjuntos de datos. Como productores, este plan permite a los miembros DataZone del proyecto de Amazon conectarse a sus propios clústeres de Amazon Redshift para consultar almacenes de datos remotos, crear nuevos conjuntos de datos y publicarlos en el catálogo de Amazon. DataZone	Acceso al editor de consultas de Amazon Redshift, acceso de «lectura» a las fuentes de datos suscritas desde el DataZone catálogo de Amazon y capacidad de crear activos locales en el clúster de Amazon Redshift configurado. Acceso al editor de consultas de Amazon Redshift, acceso de «lectura» a las fuentes de datos suscritas desde el DataZone catálogo de Amazon, posibilidad de crear y publicar activos desde el clúster de Amazon Redshift configurado.

Nombre del plano	Descripción	Recursos creados
Plano de Amazon SageMaker	Este plan ayuda a los productores y consumidores de datos a cambiarse sin problemas SageMaker a Amazon para colaborar en proyectos de aprendizaje automático (ML) y, al mismo tiempo, reforzar la gobernanza del acceso a los datos y los activos de aprendizaje automático. Con la nueva integración integrada entre Amazon DataZone y Amazon SageMaker, los consumidores y productores de datos pueden optimizar la gobernanza del aprendizaje automático en toda la configuración de la infraestructura, colaborar en iniciativas empresariales y gestionar fácilmente los datos y los activos de aprendizaje automático.	Puedes crear un SageMaker dominio de Amazon que pueda buscar, suscribirse y publicar datos y activos de aprendizaje automático en Amazon DataZone. También puede suscribirse y publicar en las bases de datos de AWS Glue y en la formación de lagos según esté configurado.

¿Qué son los flujos de trabajo de DataZone inventario y publicación de Amazon?

Creación de activos de inventario de proyectos

Para poder utilizar Amazon DataZone para catalogar tus datos, primero debes incluir tus datos (activos) como inventario de tu proyecto en Amazon DataZone. Al crear un inventario para un proyecto, solo los miembros de ese proyecto pueden descubrir los activos. Los activos del inventario

del proyecto no están disponibles para todos los usuarios del dominio al realizar búsquedas o búsquedas, a menos que se publiquen de forma explícita. En la versión actual de Amazon DataZone, puedes añadir activos al inventario del proyecto de las siguientes maneras:

- Cree y ejecute fuentes de datos a través del portal de datos o mediante las DataZone API de Amazon. En la versión actual de Amazon DataZone, puede crear y ejecutar fuentes de datos para AWS Glue y Amazon Redshift. Al crear y ejecutar fuentes de datos de AWS Glue o Amazon Redshift, crea activos en el inventario de un proyecto elegido e importa sus metadatos técnicos de las tablas de bases de datos de origen o los almacenes de datos como inventario a Amazon. DataZone
- Con las API, puede crear activos a partir de los tipos de activos del sistema disponibles (AWS Glue, Amazon Redshift, objetos de Amazon S3) o a partir de sus tipos de activos personalizados.
  - Crea tipos de activos personalizados en el inventario de un proyecto mediante las DataZone API de Amazon. Los tipos de activos personalizados pueden incluir modelos de aprendizaje automático, paneles, tablas locales, etc.
  - Cree activos a partir de estos tipos de activos personalizados mediante DataZone las API de Amazon.
- Cree activos manualmente para objetos de S3 mediante el portal de DataZone datos de Amazon.

Gestión de los activos del inventario del proyecto: tras crear el inventario de un proyecto, los propietarios de los datos pueden organizar sus activos de inventario con los metadatos empresariales necesarios añadiendo o actualizando los nombres de las empresas (activo y esquema), las descripciones (activos y esquemas), el formato léame, los términos del glosario (activos y esquemas) y los formularios de metadatos. Puede hacerlo a través del portal de datos o mediante las DataZone API de Amazon. Cada edición de su activo crea una nueva versión de inventario.

Publicar los activos del inventario del proyecto en el DataZone catálogo de Amazon

El siguiente paso para usar Amazon DataZone para catalogar tus datos es hacer que los usuarios del dominio puedan descubrir los activos de inventario de tu proyecto. Puedes hacerlo publicando los activos del inventario en el DataZone catálogo de Amazon. Solo se puede publicar en el catálogo la última versión del activo de inventario y solo la última versión publicada está activa en el catálogo de descubrimiento. Si un activo de inventario se actualiza después de publicarse en el DataZone catálogo de Amazon, debes volver a publicarlo de forma explícita para que la última versión esté

en el catálogo de descubrimiento. En la versión actual de Amazon DataZone, puedes publicar los activos de inventario de tus proyectos en el DataZone catálogo de Amazon de las siguientes maneras:

- Publica manualmente los activos del inventario de tu proyecto en el DataZone catálogo de Amazon a través del portal de datos o mediante las DataZone API de Amazon.
- Como parte de la creación o edición de fuentes de datos, active la configuración opcional Publicar sus activos de AWS Glue en el catálogo o Publicar sus activos de Amazon Redshift en el catálogo para utilizarla durante las ejecuciones programadas o automatizadas de la fuente de datos. Cuando esta configuración está habilitada, la ejecución de una fuente de datos añade activos al inventario de tu proyecto y, a continuación, también publica los activos del inventario en el DataZone catálogo de Amazon. Ten en cuenta que si publicas directamente, es posible que los activos no contengan metadatos empresariales y que todos los usuarios del dominio los puedan encontrar directamente. Puedes usar esta configuración en tus fuentes de datos a través del portal de datos o mediante las DataZone API de Amazon.

¿Qué son los flujos de trabajo DataZone de suscripción y gestión logística de Amazon?

Una vez que tus activos se publiquen en el DataZone catálogo de Amazon, los usuarios de tu dominio podrán descubrirlos, solicitarlos y acceder a ellos, y seguir utilizando Amazon DataZone para gestionarlos, compartirlos y analizarlos.

Los usuarios solicitan acceso a un activo suscribiéndose a ese activo en nombre de un proyecto. Una vez creada una solicitud de suscripción, los propietarios del activo reciben una notificación y pueden revisarla y decidir si desean aprobarla o rechazarla. Si el propietario de los datos aprueba la solicitud de suscripción, el proyecto suscriptor tiene acceso a ese activo.

Una vez aprobada una solicitud de suscripción, Amazon DataZone inicia un flujo de trabajo de gestión de suscripciones que añade automáticamente el activo a todos los entornos aplicables del proyecto mediante la creación de las subvenciones necesarias en AWS Lake Formation o Amazon Redshift. Esto permite a los miembros del proyecto suscritos consultar el activo mediante una de las herramientas de consulta (Amazon Athena o el editor de consultas Amazon Redshift) de sus entornos.

Amazon DataZone puede activar esta lógica de gestión logística automatizada solo para los activos gestionados (esto incluye las tablas AWS Glue y las tablas y vistas de Amazon

Redshift). Para todos los demás tipos de activos (activos no gestionados), Amazon no DataZone puede activar automáticamente la gestión logística, sino que publica un evento en Amazon Eventbridge con todos los detalles necesarios en la carga útil del evento para que puedas crear las subvenciones necesarias fuera de Amazon. DataZone Amazon DataZone también proporciona la `updateSubscriptionStatus` API que te permite actualizar el estado de la suscripción una vez gestionada fuera de Amazon DataZone para que Amazon DataZone pueda notificar a los miembros del proyecto que pueden empezar a consumir el activo.

Las personas usuarias de Amazon DataZone

Los siguientes son los principales DataZone usuarios de Amazon:

- Administradores de dominio propietarios de la configuración de Amazon DataZone como plataforma de análisis de su organización.

  En el contexto de Amazon DataZone, los administradores de dominios instalan Amazon DataZone en AWS las cuentas, crean DataZone dominios de Amazon y configuran las asociaciones de AWS cuentas y las asociaciones de proveedores de identidad con los DataZone dominios de Amazon. Los administradores de dominio también utilizan otras consolas de AWS servicio, como AWS Organization y Service Catalog, para configurar Amazon DataZone.
- Usuarios de datos que son los principales usuarios de Amazon DataZone (editores de activos y suscriptores) para sus tareas de análisis y aprendizaje automático.

  Los usuarios de datos incluyen trabajadores de análisis de datos, científicos de datos y usuarios de sistemas que producen y consumen activos de datos. En el contexto de Amazon DataZone, los usuarios de datos crean proyectos y entornos y se unen a ellos, se suscriben y consumen activos de datos con herramientas de análisis o aprendizaje automático preconfiguradas y publican los activos de datos de salida en el catálogo de DataZone dominios de Amazon para compartirlos con otros.
- Desarrolladores de sistemas que crean plantillas de infraestructura personalizadas e integran Amazon DataZone con catálogos internos o sistemas de producción.

  En el contexto de Amazon DataZone, los desarrolladores de sistemas crean planos de entorno (plantillas de infraestructura) o canalizaciones de CI/CD de Infrastructure-As-Code como proveedor de entornos, canalizaciones de datos para promover los activos de datos en todos los entornos, adaptadores de sincronización de catálogos y cumplimiento de suscripciones para integrarlos con los catálogos internos o integraciones entre las API de Amazon DataZone y las interfaces de usuario internas o los sistemas de producción, si es necesario.

- Funcionarios de gobierno de datos que son dueños de las definiciones y los riesgos de las políticas de seguridad, privacidad y otras políticas de cumplimiento de la organización y que se aseguran de que el uso de Amazon DataZone en sus organizaciones cumpla con estas definiciones.

DataZone Terminología de Amazon

Dominio

Un DataZone dominio de Amazon es la entidad organizadora que conecta tus activos, usuarios y sus proyectos. Con DataZone los dominios de Amazon, tiene la flexibilidad de reflejar las necesidades de datos y análisis de su estructura organizativa, ya sea que se trate de crear un único DataZone dominio de Amazon para su empresa o varias zonas de datos; dominios para diferentes unidades de negocio o equipos.

Cuenta asociada

Al asociar tus AWS cuentas a DataZone los dominios de Amazon, podrás publicar datos de estas AWS cuentas en el DataZone catálogo de Amazon y crear DataZone proyectos de Amazon para trabajar con tus datos en varias AWS cuentas. Las solicitudes de asociación de cuentas solo se pueden iniciar en AWS cuentas que posean un DataZone dominio de Amazon. Las solicitudes de asociación de cuentas solo las pueden aceptar los usuarios administrativos de las AWS cuentas invitadas. Una vez que una AWS cuenta esté asociada a un DataZone dominio de Amazon, podrá registrar sus fuentes de datos, como el catálogo de AWS Glue y Amazon Redshift de esta cuenta, en este dominio. Al estar asociada, una AWS cuenta también puede crear DataZone proyectos y entornos de Amazon.

Se Cuenta de AWS puede asociar a uno o más DataZone dominios de Amazon.

Origen de datos

En Amazon DataZone, puede utilizar las fuentes de datos para importar metadatos técnicos de los activos (datos) de las bases de datos o almacenes de datos de origen a Amazon DataZone. En la versión actual de Amazon DataZone, puede crear y ejecutar fuentes de datos para AWS Glue y Amazon Redshift. Al crear una fuente de datos, establece una conexión entre Amazon DataZone y la fuente (AWS Glue Data Catalog o Amazon Redshift Warehouse) que le permite leer los metadatos técnicos, incluidos los nombres de las tablas, los nombres de las columnas y los tipos de datos. Al crear una fuente de datos, también se inicia la ejecución inicial de la fuente de datos que crea activos nuevos o actualiza los existentes en Amazon DataZone. Al crear una

fuente de datos o después de que la fuente de datos se haya creado correctamente, también tiene la opción de especificar un cronograma para la ejecución de la fuente de datos.

Fuente de datos: ejecutar

En Amazon DataZone, la ejecución de una fuente de datos es una tarea que Amazon DataZone realiza para crear activos en los inventarios de los proyectos y también, opcionalmente, para publicar los activos del inventario del proyecto en el DataZone catálogo de Amazon. La ejecución de las fuentes de datos puede ser automática (se inicia cuando se crea inicialmente una fuente de datos), programada o manual. Los criterios de selección de datos te permiten ajustar los conjuntos de datos actuales y futuros que se incorporarán a los inventarios de los proyectos o al DataZone catálogo de Amazon, así como la frecuencia de las actualizaciones de los metadatos de esos activos de inventario o catálogo.

Objetivo de suscripción

En Amazon DataZone, los objetivos de suscripción te permiten acceder a los datos a los que te has suscrito en tus proyectos. Un destino de suscripción especifica la ubicación (por ejemplo, una base de datos o un esquema) y los permisos necesarios (por ejemplo, una función de IAM) que Amazon DataZone puede utilizar para establecer una conexión con los datos de origen y crear las concesiones necesarias para que los miembros del DataZone proyecto de Amazon puedan empezar a consultar los datos a los que se han suscrito.

Solicitud de suscripción

En Amazon DataZone, una solicitud de suscripción es un proceso que debe seguir un DataZone proyecto de Amazon para poder acceder a un activo específico. Las solicitudes de suscripción se pueden aprobar, rechazar, revocar o conceder.

activo

En Amazon DataZone, un activo es una entidad que presenta un único objeto de datos físico (por ejemplo, una tabla, un panel o un archivo) o un objeto de datos virtual (por ejemplo, una vista).

Asset type (Tipo de activo)

Los tipos de activos definen cómo se representan los activos en el DataZone catálogo de Amazon. Un tipo de activo define el esquema de un tipo de activo específico. Cuando se crean los activos, se validan con el esquema definido por su tipo de activo (de forma predeterminada, la última versión). Cuando se produce una actualización de activos, Amazon DataZone crea una nueva versión de activos y permite a DataZone los usuarios de Amazon operar con todas las versiones de activos.

Glosario empresarial

En Amazon DataZone, un glosario empresarial es un conjunto de términos empresariales que pueden estar asociados a los activos. Un glosario empresarial ayuda a garantizar que se utilicen los mismos términos y definiciones en toda la organización en sus distintas tareas de análisis de datos.

Los términos de un glosario empresarial se pueden añadir a los activos y columnas para clasificar o mejorar la identificación de esos atributos durante la búsqueda. El glosario se puede seleccionar como el tipo de valor de un campo en un formulario de metadatos que esté asociado a un activo. Cuando se selecciona un término concreto como valor para el campo del formulario de metadatos de un activo, los usuarios pueden buscar el término del glosario empresarial y encontrar los activos asociados.

Tipo de formulario de metadatos

Un tipo de formulario de metadatos es una plantilla que define los metadatos que se recopilan y guardan cuando los activos se crean como inventario o se publican en un DataZone dominio de Amazon. Los tipos de formularios de metadatos se pueden asociar a un activo de datos. Los tipos de formularios de metadatos ayudan a los administradores de dominios a definir los formularios de metadatos necesarios para ese dominio, como la información de conformidad, la información reglamentaria o las clasificaciones. Permite a los administradores de dominios personalizar metadatos adicionales para sus activos. Amazon DataZone tiene tipos de formularios de metadatos del sistema como asset-common-details-form -type, column-business-metadata-form -type glue-table-form-type, glue-view-form-type,, redshift-table-form-type redshift-view-form-type, s3- object-collection-form-type subscription-terms-form-type, y. suggestion-form-type

Formulario de metadatos

En Amazon DataZone, los formularios de metadatos definen los metadatos que se recopilan y guardan cuando los activos se crean como inventario o se publican en un DataZone dominio de Amazon. Un administrador de dominios crea las definiciones de los formularios de metadatos en el dominio del catálogo. La definición de un formulario de metadatos se compone de una o más definiciones de campo y admite los tipos de datos booleanos, de fecha, decimales, enteros, de cadena y de valores de campo del glosario empresarial.

Un administrador de dominio aplica un formulario de metadatos a los activos de su dominio añadiendo el formulario de metadatos a su dominio. A continuación, los editores de activos proporcionan los valores de campo opcionales y obligatorios en el formulario de metadatos.

Proyecto

En Amazon DataZone, los proyectos permiten a un grupo de usuarios colaborar en varios casos de uso empresarial que implican la creación de activos en los inventarios de los proyectos y, por lo tanto, hacer que todos los miembros del proyecto puedan descubrirlos y, a continuación, publicar, descubrir, suscribirse y consumir los activos del catálogo de Amazon. DataZone Los miembros del proyecto consumen activos del DataZone catálogo de Amazon y producen nuevos activos mediante uno o más flujos de trabajo analíticos. Los miembros del proyecto pueden ser propietarios o colaboradores. Los propietarios de los proyectos pueden añadir o eliminar a otros usuarios como propietarios o colaboradores y pueden modificar o eliminar proyectos. Se pueden definir otras restricciones para los colaboradores mediante políticas. Cuando un usuario crea un proyecto, se convierte en el primer propietario de ese proyecto.

Entorno

Un entorno es un conjunto de recursos configurados (por ejemplo, un bucket de Amazon S3, una AWS Glue base de datos o un grupo de trabajo de Amazon Athena), con un conjunto determinado de directores de IAM (con permisos de colaborador asignados) que pueden operar con esos recursos. Cada entorno también puede tener usuarios principales que estén autorizados a acceder a los recursos y a los datos mediante suscripción y gestión logística. Los entornos están diseñados para almacenar enlaces procesables a AWS servicios, consolas e IDE externos. Los miembros del proyecto pueden acceder a servicios como la consola Amazon Athena y más a través de enlaces profundos configurados dentro de un entorno. Se puede restringir aún más el uso de los usuarios de SSO y los usuarios de IAM del proyecto para utilizar entornos específicos o acceder a ellos.

Perfil del entorno

En Amazon DataZone, un perfil de entorno es una plantilla que se puede utilizar para crear entornos. Los perfiles de entorno se crean mediante planos.

Con los perfiles de entorno, los administradores de dominio pueden incluir los planos con parámetros preconfigurados y, a continuación, los trabajadores de datos pueden crear rápidamente cualquier número de entornos nuevos seleccionando los perfiles de entorno existentes y especificando los nombres de los nuevos entornos. Esto permite a los trabajadores de datos administrar sus proyectos y entornos de manera eficiente y, al mismo tiempo, garantizar que cumplen con las políticas de gobierno de datos aplicadas por los administradores de sus dominios.

Esquema

El plano con el que se crea el entorno define qué AWS herramientas y servicios (por ejemplo, AWS Glue Amazon Redshift) pueden utilizar los miembros del proyecto al que pertenece el entorno cuando trabajan con los activos del catálogo de Amazon DataZone .

En la versión actual de Amazon DataZone se admiten los siguientes blueprints predeterminados:

- Plano de lago de datos
- Plano de almacén de datos
- Plano de Amazon SageMaker

Perfil de usuario

Un perfil de usuario representa a DataZone los usuarios de Amazon. Amazon DataZone admite funciones de IAM e identidades de SSO para interactuar con la consola de DataZone administración de Amazon y el portal de datos con distintos fines. Los administradores de dominios utilizan las funciones de IAM para realizar el trabajo administrativo inicial relacionado con el dominio en Amazon DataZone Management Console, incluida la creación de nuevos DataZone dominios de Amazon, la configuración de los tipos de formularios de metadatos y la implementación de políticas. Los trabajadores de datos utilizan sus identidades corporativas de SSO a través de Identity Center para iniciar sesión en el Amazon DataZone Data Portal y acceder a los proyectos en los que tienen membresías.

Perfil del grupo

Los perfiles de grupo representan grupos de DataZone usuarios de Amazon. Los grupos pueden crearse manualmente o asignarse a grupos de clientes empresariales de Active Directory. En Amazon DataZone, los grupos tienen dos propósitos. En primer lugar, un grupo puede asignarse a un equipo de usuarios del organigrama y, por lo tanto, reducir el trabajo administrativo del propietario de un DataZone proyecto de Amazon cuando hay nuevos empleados que se unen o abandonan un equipo. En segundo lugar, los administradores corporativos utilizan los grupos de Active Directory para gestionar y actualizar los estados de los usuarios, por lo que los administradores de DataZone dominios de Amazon pueden utilizar estas pertenencias a grupos para implementar las políticas de DataZone dominio de Amazon.

Administrador de dominios

En Amazon DataZone, el principal de IAM que crea un DataZone dominio de Amazon es el administrador de dominio predeterminado de ese dominio. Los administradores de dominios de Amazon DataZone realizan funciones clave para el dominio, como la creación de dominios, la

asignación de otros administradores de dominio, la adición de fuentes de datos y destinos de suscripción, la creación de proyectos y entornos y la asignación de propietarios de proyectos.

Publicador

En Amazon DataZone, los editores publican activos en el DataZone catálogo de Amazon y pueden editar los metadatos de los activos que publican. Si se les concede esta autorización, los editores pueden aprobar o rechazar las solicitudes de suscripción a los contenidos que publicaron en el DataZone catálogo de Amazon.

Suscriptor

En Amazon DataZone, un suscriptor es un DataZone proyecto de Amazon que quiere encontrar activos del DataZone catálogo de Amazon, acceder a ellos y consumirlos.

Cuenta de AWS owner

En Amazon DataZone, Cuenta de AWS los propietarios crean funciones, políticas y permisos en sus dominios Cuentas de AWS que permiten asociarlos Cuentas de AWS a los DataZone dominios de Amazon.

¿Qué hay de nuevo en Amazon DataZone?

En esta sección se describen las nuevas funciones y mejoras de Amazon DataZone por fecha de lanzamiento.

Temas

2024

Amazon DataZone lanza la integración con Amazon SageMaker

Publicado el 05/06/2024

Amazon DataZone lanza la integración con Amazon SageMaker para ayudar a los productores de datos y a los consumidores a cambiarse sin problemas SageMaker a Amazon para colaborar en proyectos de aprendizaje automático (ML) y, al mismo tiempo, reforzar la gobernanza del acceso a los datos y los activos de aprendizaje automático. Con la nueva integración integrada entre Amazon DataZone y Amazon SageMaker, los consumidores y productores de datos pueden optimizar la gobernanza del aprendizaje automático en toda la configuración de la infraestructura, colaborar en iniciativas empresariales y gestionar fácilmente los datos y los activos de aprendizaje automático. Para obtener más información, consulte Trabajar con los planos DataZone integrados de Amazon y Trabajar con cuentas asociadas para publicar y consumir datos.

Amazon DataZone lanza la integración con el modo de acceso híbrido de AWS Lake Formation

Lanzado el 4 de marzo de 2024

Amazon DataZone ha introducido una integración con el modo de acceso híbrido de AWS Lake Formation. Esta integración te permite publicar y compartir fácilmente tus tablas de AWS Glue a través de Amazon DataZone, sin necesidad de registrarlas primero en AWS Lake Formation. Para empezar, los administradores habilitan la configuración de registro de ubicación de datos en el `DefaultDataLake` blueprint de la DataZone consola de Amazon. A continuación, cuando un consumidor de datos se suscribe a una tabla de AWS Glue gestionada mediante permisos de IAM, Amazon DataZone primero registra las ubicaciones de Amazon S3 de esta tabla en modo híbrido y, a

continuación, concede acceso al consumidor de datos gestionando los permisos de la tabla mediante AWS Lake Formation. Esto garantiza que los permisos de IAM disponibles sigan existiendo con los permisos de AWS Lake Formation recientemente otorgados, sin interrumpir ningún flujo de trabajo existente. Para obtener más información, consulte DataZone Integración de Amazon con el modo híbrido de AWS Lake Formation .

Amazon DataZone lanza la integración con AWS Glue Data Quality

Publicado el 4 de marzo de 2024

Amazon DataZone lanza la integración con AWS Glue Data Quality y ofrece API para integrar métricas de calidad de datos de soluciones de calidad de datos de terceros. La nueva integración te permite publicar automáticamente las puntuaciones de calidad de los datos de AWS Glue en el catálogo de datos DataZone empresariales de Amazon. DataZone Las API de Amazon se pueden utilizar para incorporar métricas de calidad de fuentes de terceros. Una vez publicados, los consumidores de datos pueden buscar fácilmente los activos de datos, ver métricas de calidad detalladas e identificar las comprobaciones y normas fallidas, lo que facilita la toma de decisiones empresariales. Para obtener más información, consulte Calidad de los datos en Amazon DataZone.

Publicación de disponibilidad general de las recomendaciones de IA para las descripciones en Amazon DataZone

Publicada el 27/03/2024

Amazon DataZone anunció el lanzamiento de disponibilidad general de la nueva capacidad generativa basada en IA para mejorar el descubrimiento, la comprensión y el uso de datos mediante el enriquecimiento del catálogo de datos empresariales. Con un solo clic, los productores de datos pueden generar descripciones y contextos completos de los datos empresariales, destacar las columnas más impactantes e incluir recomendaciones sobre casos de uso analíticos. El lanzamiento añade compatibilidad con las API que los productores de datos pueden utilizar para generar descripciones de los activos mediante programación. Para obtener más información, consulte Uso del aprendizaje automático y la IA generativa.

Amazon DataZone presenta mejoras en la integración de Amazon Redshift

Lanzado el 21 de marzo de 2024

Amazon DataZone ha introducido varias mejoras en su integración con Amazon Redshift, lo que simplifica el proceso de publicación y suscripción a las tablas y vistas de Amazon Redshift. Estas

actualizaciones optimizan la experiencia tanto para los productores como para los consumidores de datos, ya que les permiten crear rápidamente entornos de almacenamiento de datos utilizando credenciales preconfiguradas y parámetros de conexión proporcionados por sus DataZone administradores de Amazon. Además, estas mejoras otorgan a los administradores un mayor control sobre quién puede usar los recursos de sus AWS cuentas y clústeres de Amazon Redshift, y con qué propósito.

- Configuración del blueprint: una vez que active el `DefaultDataWarehouseBlueprint` blueprint, podrá controlar qué proyectos pueden utilizar el `DefaultDataWarehouseBlueprint` blueprint de su cuenta para crear perfiles de entorno asignando la gestión de los proyectos al blueprint activado. También puede crear conjuntos de parámetros adicionales `DefaultDataWarehouseBlueprint` proporcionando parámetros como el clúster, la base de datos y un secreto. AWS También puedes crear AWS secretos desde la DataZone consola de Amazon.
- Perfil de entorno: al crear un perfil de entorno, puede elegir entre proporcionar sus propios parámetros de Amazon Redshift o utilizar uno de los conjuntos de parámetros de la configuración del blueprint. Si decide utilizar el conjunto de parámetros creado en la configuración del blueprint, el AWS secreto solo requiere una `AmazonDataZoneDomain` etiqueta (la `AmazonDataZoneProject` etiqueta solo es necesaria si decide proporcionar sus propios conjuntos de parámetros en el perfil del entorno). En el perfil del entorno, puede especificar una lista de proyectos autorizados. Solo los proyectos autorizados pueden usar este perfil de entorno para crear entornos de almacén de datos. También puede especificar qué datos pueden publicar los proyectos autorizados. Actualmente, puede elegir una de las siguientes opciones: 1) Publicar desde cualquier esquema, 2) Publicar desde el esquema de entorno predeterminado, 3) No permitir la publicación.
- Entorno: los productores o consumidores de datos ahora pueden seleccionar un perfil de entorno para crear entornos, sin necesidad de proporcionar sus propios parámetros de Amazon Redshift, incluidos AWS Secret, clúster, grupo de trabajo y base de datos. Estos parámetros se transfieren al entorno desde el perfil del entorno. Junto con la creación del entorno, Amazon DataZone ahora también crea un esquema predeterminado para el entorno. Los miembros del proyecto tienen acceso de lectura y escritura a este esquema y pueden publicar fácilmente cualquier tabla creada en este esquema en el catálogo ejecutando la fuente de datos predeterminada creada como parte de la creación del entorno. Los parámetros de Amazon Redshift que se utilizan para crear el entorno también se pueden utilizar para crear nuevas fuentes de datos (en lugar de que el productor de datos proporcione sus propios parámetros en la creación de la fuente de datos).

AWS Cloud Formation Support para Amazon DataZone

Lanzado el 18/01/2024

Los usuarios de Amazon ahora DataZone pueden aprovechar AWS CloudFormation para modelar y gestionar de forma eficaz un conjunto de DataZone recursos de Amazon. Este enfoque facilita el aprovisionamiento coherente de los recursos y, al mismo tiempo, permite la gestión del ciclo de vida mediante la infraestructura como prácticas de código. Con las plantillas personalizadas, puede definir con precisión los recursos necesarios y sus interdependencias. Para obtener más información, consulta la referencia del tipo DataZone de recurso de Amazon.

Agregue a los directores de IAM directamente como miembros de los proyectos de Amazon DataZone

Lanzado el 5 de enero de 2024

Ahora puedes añadir directores de IAM como miembros del proyecto, incluso si esos directores de IAM aún no han iniciado sesión en Amazon DataZone (requisito previo). Después de que un administrador de dominio o un administrador de TI añada `iam:GetUser` y `iam:GetRole` a la función de ejecución del dominio, los propietarios del proyecto pueden añadir a los directores de IAM como miembros simplemente proporcionando el nombre de recurso de Amazon (ARN) de la función de IAM o del usuario de IAM. El director de IAM aún debe tener los permisos de IAM necesarios para acceder a Amazon DataZone y estos se pueden configurar en la consola de IAM. Para obtener más información, consulte Agrega miembros a un proyecto.

Support para tipos de activos personalizados desde el portal de datos

Lanzado el 05/01/2024

La compatibilidad con activos personalizados permite DataZone a Amazon catalogar los activos a través del portal de datos para datos no estructurados, incluidos paneles, consultas y modelos, lo que facilita la adición de activos personalizados directamente en el portal de datos junto con el soporte de API disponible anteriormente. La capacidad de crear, actualizar y publicar activos personalizados en Amazon te permite compartir DataZone, buscar y suscribirte a cualquier tipo de activo y crear un flujo de trabajo empresarial que proporcione el control de esos activos. Para obtener más información, consulte Cree tipos de activos personalizados.

2023

Eliminar dominio

Publicado el 27 de diciembre de 2023

Esta es una función que le permite eliminar sus dominios más fácilmente. Ahora puede continuar con la eliminación del dominio incluso si no está vacío (ya que contiene proyectos, entornos, activos, fuentes de datos, etc.). Para obtener más información, consulte Eliminar dominios.

Modo híbrido

Lanzado el 22/12/2023

Amazon DataZone ha añadido soporte para el modo híbrido AWS Lake Formation. Con este soporte, si publicas una tabla AWS Glue en Amazon DataZone con su ubicación AWS S3 registrada en Lake Formation en modo híbrido, Amazon DataZone trata esta tabla como un activo gestionado y puede gestionar las subvenciones de suscripción a esta tabla. Antes del lanzamiento de esta función, Amazon DataZone trataba esta tabla como un activo no gestionado, es decir, Amazon no DataZone podía conceder suscripciones a esta tabla. Para obtener más información, consulte Configurar los permisos de Lake Formation para Amazon DataZone.

Conformidad con HIPAA

Publicado el 14 de diciembre de 2023

Amazon ahora DataZone cumple con la Ley de Portabilidad y Responsabilidad de los Seguros de Salud de los Estados Unidos de 1996 (HIPAA). Para ver la lista de AWS servicios que cumplen con la HIPAA, consulte https://aws.amazon.com/compliance//. hipaa-eligible-services-reference

Recomendaciones de IA para descripciones en Amazon DataZone (versión preliminar)

Publicado el 28 de noviembre de 2023

AWS anuncia la versión preliminar de una nueva capacidad generativa basada en IA en Amazon DataZone para mejorar el descubrimiento, la comprensión y el uso de datos mediante el enriquecimiento del catálogo de datos empresariales. Con un solo clic, los productores de datos pueden generar descripciones y contextos completos de los datos empresariales, destacar columnas

impactantes e incluir recomendaciones sobre casos de uso analíticos. Con las recomendaciones de IA para las descripciones en Amazon DataZone, los consumidores de datos pueden identificar las tablas y columnas de datos necesarias para el análisis, lo que mejora la capacidad de descubrimiento de los datos y reduce las back-and-forth comunicaciones con los productores de datos. La versión preliminar está disponible en DataZone los dominios de Amazon aprovisionados en las siguientes AWS regiones: EE.UU. Este (Norte de Virginia) y EE.UU. Oeste (Oregón). Para obtener más información, consulte Uso del aprendizaje automático y la IA generativa.

DefaultDataLake mejora del plano

Publicado el 20/11/2023

Amazon DataZone ha añadido una mejora al DefaultDataLake plan que te proporciona un mejor control sobre quién puede publicar qué datos de tu AWS cuenta. Hay dos cambios clave que se introdujeron con el lanzamiento de esta función.

- En la consola, una vez que active el DefaultDataLake blueprint, podrá controlar qué proyectos pueden utilizar el DefaultDataLake blueprint de su cuenta para crear perfiles de entorno asignando la gestión de proyectos al blueprint activado.
- El segundo cambio se produce en el portal. Si crea un perfil de entorno mediante el DefaultDataLake esquema, también puede seleccionar los proyectos autorizados que pueden usar el perfil de entorno para crear entornos. De forma predeterminada, todos los proyectos pueden usar el perfil de entorno del lago de datos, pero puede restringir el perfil de entorno a proyectos específicos y también controlar qué datos se pueden publicar utilizando los entornos creados con el perfil.

Para obtener más información, consulte Cree un perfil de entorno.

Configuración

Para configurar Amazon DataZone, debes tener una AWS cuenta y configurar las políticas y permisos de IAM necesarios para Amazon DataZone.

Una vez que hayas configurado tus DataZone permisos de Amazon, se recomienda que completes los pasos de la sección Primeros pasos, que te guiarán por la creación del DataZone dominio de Amazon, la obtención de la URL del portal de datos y los DataZone flujos de trabajo básicos de Amazon para productores y consumidores de datos.

Temas

Regístrate para obtener una AWS cuenta

Si no tiene una AWS cuenta, complete los siguientes pasos para crear una.

Si tienes una AWS organización, crea una cuenta:

1. Inicie sesión en la consola AWS de administración y abra la consola de Organizations en https://console.aws.amazon.com/organizations/.
2. En el panel de navegación, selecciona AWS cuentas.
3. Selecciona Añadir una AWS cuenta.
4. Selecciona Crear una AWS cuenta y proporciona los detalles solicitados. Selecciona Crear AWS cuenta.

Para crear una AWS cuenta

1. Abra https://portal.aws.amazon.com/billing/signup
2. Siga las instrucciones que se le indiquen.

Parte del procedimiento de registro consiste en recibir una llamada telefónica e indicar un código de verificación en el teclado del teléfono.

Al abrir una AWS cuenta, se crea un usuario raíz de la AWS cuenta. El usuario raíz tiene acceso a todos los AWS servicios y recursos de la cuenta. Como práctica recomendada de seguridad, asigne acceso administrativo a un usuario administrativo y utilice únicamente el usuario raíz para realizar tareas que requieran acceso de usuario raíz.

Configure los permisos de IAM necesarios para usar la consola de DataZone administración de Amazon

Cualquier usuario, grupo o rol que quiera usar la consola DataZone de administración de Amazon debe tener los permisos necesarios.

Temas

- Adjunta políticas obligatorias y opcionales a un usuario, grupo o rol para el acceso a la DataZone consola de Amazon
- Cree una política personalizada para los permisos de IAM para permitir la creación simplificada de roles en la consola de DataZone servicio de Amazon
- Crea una política personalizada de permisos para gestionar una cuenta asociada a un DataZone dominio de Amazon
- (Opcional) Cree una política personalizada para los permisos del Centro de AWS Identidad a fin de habilitar el inicio de sesión único (SSO) en su dominio
- (Opcional) Cree una política personalizada para los permisos del Centro de AWS Identidad para añadir y eliminar el acceso de usuarios y grupos de SSO a su dominio de Amazon DataZone .
- (Opcional) Añade tu principal de IAM como usuario clave para crear tu DataZone dominio de Amazon con una clave gestionada por el cliente de AWS Key Management Service (KMS)

Adjunta políticas obligatorias y opcionales a un usuario, grupo o rol para el acceso a la DataZone consola de Amazon

Complete el siguiente procedimiento para adjuntar las políticas personalizadas obligatorias y opcionales a un usuario, grupo o rol. Para obtener más información, consulte AWS políticas gestionadas para Amazon DataZone.

1. Inicie sesión en la consola AWS de administración y abra la consola de IAM en https://console.aws.amazon.com/iam/.
2. En el panel de navegación, seleccione Políticas.
3. Elija las siguientes políticas para asociarlas a su usuario, grupo o rol.

   - En la lista de políticas, active la casilla de verificación situada junto a AmazonDataZoneFullAccess. Puede utilizar el menú Filter y el cuadro de búsqueda para filtrar la lista de políticas. Para obtener más información, consulte AWS política gestionada: AmazonDataZoneFullAccess.
   - (Opcional) Cree una política personalizada para los permisos de IAM para permitir la creación simplificada de roles en la consola de DataZone servicio de Amazon.
   - (Opcional) Cree una política personalizada para los permisos del Centro de AWS Identidad a fin de habilitar el inicio de sesión único (SSO) en su dominio.
   - (Opcional) Cree una política personalizada para los permisos del Centro de AWS Identidad para añadir y eliminar el acceso de usuarios y grupos de SSO a su dominio de Amazon DataZone .
4. Elija Acciones y, a continuación, elija Adjuntar.
5. Elija el usuario, el grupo o el rol al que quiere adjuntar la política. Puede utilizar el menú Filter (Filtro) y el cuadro de búsqueda para filtrar la lista entidades principales. Después de elegir el usuario, el grupo o el rol, elija Adjuntar política.

Cree una política personalizada para los permisos de IAM para permitir la creación simplificada de roles en la consola de DataZone servicio de Amazon

Complete el siguiente procedimiento para crear una política en línea personalizada que le permita disponer de los permisos necesarios para que Amazon DataZone pueda crear las funciones necesarias en la consola AWS de administración en su nombre.

1. Inicie sesión en la consola AWS de administración y abra la consola de IAM en https://console.aws.amazon.com/iam/.
2. En el panel de navegación, elija Usuarios o Grupos de usuarios.
3. En la lista, seleccione el nombre del usuario o del grupo en el que integrará una política.

4. Elija la pestaña Permissions (Permisos) y, si es necesario, expanda la sección Permissions Policies (Políticas de permisos).
5. Seleccione el enlace Añadir permisos y Crear política en línea.
6. En la pantalla Crear política, en la sección del editor de políticas, selecciona JSON.

   Cree un documento de política con las siguientes declaraciones de JSON y, a continuación, seleccione Siguiente.

```
{
    "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. En la pantalla Revisar la política, introduce un nombre para la política. Cuando esté satisfecho con la política, seleccione Create policy (Crear política). Asegúrese de que no aparece ningún error en un cuadro rojo en la parte superior de la pantalla. Corrija todos los errores notificados.

Crea una política personalizada de permisos para gestionar una cuenta asociada a un DataZone dominio de Amazon

Complete el siguiente procedimiento para crear una política integrada personalizada que le permita disponer de los permisos necesarios en una AWS cuenta asociada para publicar, aceptar y rechazar los recursos compartidos de un dominio y, a continuación, habilitar, configurar y deshabilitar los esquemas de entorno en la cuenta asociada. Para habilitar la creación de roles simplificada de Amazon DataZone Service Console opcional disponible durante la configuración del blueprint, también Cree una política personalizada para los permisos de IAM para permitir la creación simplificada de roles en la consola de DataZone servicio de Amazon debe hacerlo.

1. Inicie sesión en la consola AWS de administración y abra la consola de IAM en https://console.aws.amazon.com/iam/.
2. En el panel de navegación, elija Usuarios o Grupos de usuarios.
3. En la lista, seleccione el nombre del usuario o del grupo en el que integrará una política.
4. Elija la pestaña Permissions (Permisos) y, si es necesario, expanda la sección Permissions Policies (Políticas de permisos).
5. Seleccione el enlace Añadir permisos y Crear política en línea.
6. En la pantalla Crear política, en la sección del editor de políticas, selecciona JSON. Cree un documento de política con las siguientes declaraciones de JSON y, a continuación, seleccione Siguiente.

```
{
    "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. En la pantalla Revisar la política, introduce un nombre para la política. Cuando esté satisfecho con la política, seleccione Create policy (Crear política). Asegúrese de que no aparece ningún error en un cuadro rojo en la parte superior de la pantalla. Corrija todos los errores notificados.

(Opcional) Cree una política personalizada para los permisos del Centro de AWS Identidad a fin de habilitar el inicio de sesión único (SSO) en su dominio

Complete el siguiente procedimiento para crear una política en línea personalizada con los permisos necesarios para habilitar el inicio de sesión único (SSO) mediante el Centro de AWS identidades de IAM en Amazon. DataZone

1. Inicie sesión en la consola de AWS administración y abra la consola de IAM en https://console.aws.amazon.com/iam/.
2. En el panel de navegación, elija Usuarios o Grupos de usuarios.
3. En la lista, seleccione el nombre del usuario o del grupo en el que integrará una política.
4. Elija la pestaña Permissions (Permisos) y, si es necesario, expanda la sección Permissions Policies (Políticas de permisos).
5. Seleccione Añadir permisos y Crear una política en línea.
6. En la pantalla Crear política, en la sección Editor de políticas, selecciona JSON.

   Cree un documento de política con las siguientes declaraciones de JSON y, a continuación, seleccione Siguiente.

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

7. En la pantalla Revisar la política, introduce un nombre para la política. Cuando esté satisfecho con la política, seleccione Create policy (Crear política). Asegúrese de que no aparece ningún error en un cuadro rojo en la parte superior de la pantalla. Corrija todos los errores notificados.

(Opcional) Cree una política personalizada para los permisos del Centro de AWS Identidad para añadir y eliminar el acceso de usuarios y grupos de SSO a su dominio de Amazon DataZone .

Complete el siguiente procedimiento para crear una política en línea personalizada que le permita disponer de los permisos necesarios para añadir y eliminar el acceso de usuarios y grupos de SSO a su dominio de Amazon. DataZone

1. Inicie sesión en la consola de AWS administración y abra la consola de IAM en https://console.aws.amazon.com/iam/.
2. En el panel de navegación, elija Usuarios o Grupos de usuarios.
3. En la lista, seleccione el nombre del usuario o del grupo en el que integrará una política.
4. Elija la pestaña Permissions (Permisos) y, si es necesario, expanda la sección Permissions Policies (Políticas de permisos).
5. Seleccione Añadir permisos y Crear una política en línea.
6. En la pantalla Crear política, en la sección Editor de políticas, selecciona JSON.

   Cree un documento de política con las siguientes declaraciones de JSON y, a continuación, seleccione Siguiente.

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

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

7. En la pantalla Revisar la política, introduce un nombre para la política. Cuando esté satisfecho con la política, seleccione Create policy (Crear política). Asegúrese de que no aparece ningún error en un cuadro rojo en la parte superior de la pantalla. Corrija todos los errores notificados.

(Opcional) Añade tu principal de IAM como usuario clave para crear tu DataZone dominio de Amazon con una clave gestionada por el cliente de AWS Key Management Service (KMS)

Antes de que puedas crear tu DataZone dominio de Amazon de forma opcional con una clave gestionada por el cliente (CMK) del Servicio de gestión de AWS claves (KMS), completa el siguiente procedimiento para convertir a tu principal de IAM en usuario de tu clave de KMS.

1. Inicie sesión en la consola de AWS administración y abra la consola KMS en https://console.aws.amazon.com/kms/.
2. Si desea ver las claves de la cuenta que usted crea y administra, en el panel de navegación, elija Customer managed keys (Claves administradas por el cliente).
3. En la lista de claves KMS, elija el alias o ID de clave de la clave KMS que desea examinar.
4. Para añadir o eliminar usuarios clave y permitir o impedir que AWS cuentas externas utilicen la clave KMS, utilice los controles de la sección Usuarios clave de la página. Los usuarios de claves pueden usar la clave KMS en operaciones criptográficas, como cifrar, descifrar, volver a cifrar y generar claves de datos.

Configure los permisos de IAM necesarios para usar el portal de DataZone datos de Amazon

Cualquier usuario, grupo o rol que quiera utilizar el portal de DataZone datos o el catálogo de Amazon debe tener los permisos necesarios.

Temas

- Adjunte la política requerida a un usuario, grupo o rol para acceder al portal de DataZone datos de Amazon
- Adjunta la política requerida a un usuario, grupo o rol para acceder al DataZone catálogo de Amazon
- Adjunta una política opcional a un usuario, grupo o rol para el acceso al portal de DataZone datos o al catálogo de Amazon si tu dominio está cifrado con una clave gestionada por el cliente del Servicio de administración de AWS claves (KMS)

Adjunte la política requerida a un usuario, grupo o rol para acceder al portal de DataZone datos de Amazon

Puede acceder al portal de DataZone datos de Amazon mediante sus AWS credenciales o sus credenciales de inicio de sesión único (SSO). Siga las instrucciones de la sección siguiente para configurar los permisos necesarios para acceder al portal de datos con sus credenciales. AWS Para obtener más información sobre el uso de Amazon DataZone con el inicio de sesión único, consulteConfiguración del centro de identidad de AWS IAM para Amazon DataZone.

> **Note**
>
> Solo los directores de IAM de la AWS cuenta de tu dominio pueden acceder al portal de datos del dominio. Los directores de IAM de otras AWS cuentas no pueden acceder al portal de datos del dominio.

Complete el siguiente procedimiento para adjuntar la política requerida a un usuario, grupo o rol. Para obtener más información, consulte AWS políticas gestionadas para Amazon DataZone.

1. Inicie sesión en la consola AWS de administración y abra la consola de IAM en https://console.aws.amazon.com/iam/.
2. En el panel de navegación, seleccione Usuarios, Grupos de usuarios o Funciones.
3. En la lista, elija el nombre del usuario, grupo o rol en el que desee incrustar una política.
4. Elija la pestaña Permissions (Permisos) y, si es necesario, expanda la sección Permissions Policies (Políticas de permisos).
5. Seleccione el enlace Añadir permisos y Crear política en línea.

6. En la pantalla Crear política, en la sección del editor de políticas, selecciona JSON. Cree un documento de política con las siguientes declaraciones de JSON y, a continuación, seleccione Siguiente.

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

7. En la pantalla Revisar la política, introduce un nombre para la política. Cuando esté satisfecho con la política, seleccione Create policy (Crear política). Asegúrese de que no aparece ningún error en un cuadro rojo en la parte superior de la pantalla. Corrija todos los errores notificados.

Adjunta la política requerida a un usuario, grupo o rol para acceder al DataZone catálogo de Amazon

> **Note**
>
> Solo los directores de IAM de la AWS cuenta de tu dominio pueden acceder al catálogo del dominio. Los directores de IAM de otras AWS cuentas no pueden acceder al catálogo del dominio.

Puedes conceder a tus identidades de IAM el acceso al catálogo de tu DataZone dominio de Amazon mediante la API y el SDK mediante el siguiente procedimiento. Si desea que estas identidades de IAM también tengan acceso al portal de DataZone datos de Amazon, siga también el procedimiento anterior paraAdjunte la política requerida a un usuario, grupo o rol para acceder al portal de

DataZone datos de Amazon. Para obtener más información, consulte AWS políticas gestionadas para Amazon DataZone.

1. Inicie sesión en la consola AWS de administración y abra la consola de IAM en https://console.aws.amazon.com/iam/.
2. En el panel de navegación, seleccione Políticas.
3. En la lista de políticas, seleccione el botón de opción situado junto a la AmazonDataZoneFullUserAccesspolítica. Puede utilizar el menú Filter y el cuadro de búsqueda para filtrar la lista de políticas. Para obtener más información, consulte AWS política gestionada: AmazonDataZoneFullUserAccess.
4. Elija Acciones y, a continuación, elija Adjuntar.
5. Seleccione el usuario, grupo o rol al que desee asociar la política marcando la casilla de verificación situada junto a cada director. Puede utilizar el menú Filter (Filtro) y el cuadro de búsqueda para filtrar la lista entidades principales. Después de elegir el usuario, el grupo o el rol, elija Adjuntar política.

Adjunta una política opcional a un usuario, grupo o rol para el acceso al portal de DataZone datos o al catálogo de Amazon si tu dominio está cifrado con una clave gestionada por el cliente del Servicio de administración de AWS claves (KMS)

Si crea su DataZone dominio de Amazon con su propia clave KMS para el cifrado de datos, también debe crear una política en línea con los siguientes permisos y adjuntarla a sus directores de IAM para que puedan acceder al portal o catálogo de DataZone datos de Amazon.

1. Inicie sesión en la consola de AWS administración y abra la consola de IAM en https://console.aws.amazon.com/iam/.
2. En el panel de navegación, seleccione Usuarios, Grupos de usuarios o Funciones.
3. En la lista, elija el nombre del usuario, grupo o rol en el que desee incrustar una política.
4. Elija la pestaña Permissions (Permisos) y, si es necesario, expanda la sección Permissions Policies (Políticas de permisos).
5. Seleccione el enlace Añadir permisos y Crear política en línea.

6. En la pantalla Crear política, en la sección del editor de políticas, selecciona JSON. Cree un documento de política con las siguientes declaraciones de JSON y, a continuación, seleccione Siguiente.

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

7. En la pantalla Revisar la política, introduce un nombre para la política. Cuando esté satisfecho con la política, seleccione Create policy (Crear política). Asegúrese de que no aparece ningún error en un cuadro rojo en la parte superior de la pantalla. Corrija todos los errores notificados.

Configuración del centro de identidad de AWS IAM para Amazon DataZone

> **Note**
>
> AWS El Centro de identidad debe estar habilitado en la misma AWS región que tu DataZone dominio de Amazon. Actualmente, AWS Identity Center solo se puede habilitar en una sola AWS región.

Puede acceder al portal de DataZone datos de Amazon mediante sus credenciales o credenciales de inicio de sesión único (SSO). AWS Siga las instrucciones de esta sección para configurar el Centro de identidad de AWS IAM para Amazon DataZone. Para obtener más información sobre el uso de

Amazon DataZone con tus AWS credenciales, consultaConfigure los permisos de IAM necesarios para usar la consola de DataZone administración de Amazon.

Puedes saltarte los procedimientos de esta sección si ya tienes activado y configurado el AWS IAM Identity Center (sucesor del AWS Single Sign-On) en la misma AWS región en la que quieres crear tu dominio de Amazon. DataZone

Complete el siguiente procedimiento para habilitar el AWS IAM Identity Center (sucesor del inicio de sesión único). AWS

1. Para habilitar AWS IAM Identity Center, debe iniciar sesión en la consola de AWS administración con las credenciales de la cuenta de administración de su AWS organización. No puede activar el Centro de identidad de IAM si ha iniciado sesión con las credenciales de una cuenta de miembro de AWS Organizations. Para obtener más información, consulte Creación y administración de una organización en la Guía del AWS usuario de Organizations.
2. Abre la consola del AWS IAM Identity Center (sucesora del AWS Single Sign-On) y utiliza el selector de regiones de la barra de navegación superior para elegir la AWS región en la que quieres crear tu dominio de Amazon. DataZone
3. Seleccione Habilitar.
4. Elija su fuente de identidad.

   De forma predeterminada, dispondrá de un almacén en el centro de identidad de IAM para gestionar los usuarios de forma rápida y sencilla. Si lo prefiere, puede conectar un proveedor de identidad externo. En este procedimiento, utilizamos el almacén predeterminado del Centro de Identidad de IAM.

   Para obtener más información, consulte Elija su fuente de identidad.
5. En el panel de navegación del Centro de identidades de IAM, elija Grupos y elija Crear grupo. Introduzca el nombre del grupo y seleccione Crear.
6. En el panel de navegación del IAM Identity Center, seleccione Usuarios.
7. En la pantalla Añadir usuario, introduzca la información necesaria y seleccione Enviar un correo electrónico al usuario con las instrucciones de configuración de la contraseña. El usuario debería recibir un correo electrónico con los siguientes pasos de configuración.
8. Seleccione Siguiente: Grupos, elija el grupo que desee y elija Agregar usuario. Los usuarios deberían recibir un correo electrónico en el que se les invite a usar el inicio de sesión único. En este correo electrónico, deben elegir Aceptar la invitación y establecer la contraseña.

Tras crear tu DataZone dominio de Amazon, puedes habilitar AWS Identity Center for Amazon DataZone y proporcionar acceso a tus usuarios y grupos de SSO. Para obtener más información, consulte Habilitar el Centro de Identidad de IAM para Amazon DataZone.

Introducción

La información de esta sección te ayuda a empezar a utilizar Amazon DataZone. Si eres nuevo en Amazon DataZone, empieza por familiarizarte con los conceptos y la terminología que se presentan en DataZone Terminología y conceptos de Amazon.

En esta sección de introducción, se explican los siguientes flujos de trabajo de DataZone inicio rápido de Amazon:

Temas

- Guía de DataZone inicio rápido de Amazon con datos de AWS Glue
- Guía de DataZone inicio rápido de Amazon con los datos de Amazon Redshift
- Guía de DataZone inicio rápido de Amazon con scripts de muestra

> **Important**
>
> Antes de iniciar los pasos de cualquiera de estos flujos de trabajo de inicio rápido, debe completar los procedimientos descritos en la sección Configuración de esta guía. Si utilizas una AWS cuenta completamente nueva, debes configurar los permisos necesarios para usar la consola de DataZone administración de Amazon. Si utilizas una AWS cuenta que tiene objetos del AWS Glue Data Catalog existentes, también debes configurar los permisos de Lake Formation para Amazon DataZone.

Guía de DataZone inicio rápido de Amazon con datos de AWS Glue

Temas

- Paso 1: Crea el portal de DataZone dominios y datos de Amazon
- Paso 2: Crea el proyecto de publicación
- Paso 3: Crea el entorno
- Paso 4: Producir datos para su publicación
- Paso 5: Recopila metadatos de AWS Glue
- Paso 6: Seleccione y publique el activo de datos

- Paso 7: Cree el proyecto para el análisis de datos
- Paso 8: Crear un entorno para el análisis de datos
- Paso 9: busque en el catálogo de datos y suscríbase a los datos
- Paso 10: Aprueba la solicitud de suscripción
- Paso 11: Cree una consulta y analice los datos en Amazon Athena

Paso 1: Crea el portal de DataZone dominios y datos de Amazon

En esta sección se describen los pasos para crear un DataZone dominio de Amazon y un portal de datos para este flujo de trabajo.

Complete el siguiente procedimiento para crear un DataZone dominio de Amazon. Para obtener más información sobre DataZone los dominios de Amazon, consulte DataZone Terminología y conceptos de Amazon.

1. Ve a la DataZone consola de Amazon en https://console.aws.amazon.com/datazone, inicia sesión y, a continuación, selecciona Crear dominio.

   > **Note**
   >
   > Si quieres usar un DataZone dominio de Amazon existente para este flujo de trabajo, selecciona Ver dominios, elige el dominio que quieres usar y, a continuación, continúa con el paso 2 de creación de un proyecto de publicación.

2. En la página Crear dominio, proporciona valores para los siguientes campos:

   - Nombre: especifique un nombre para su dominio. A los efectos de este flujo de trabajo, puede denominar a este dominio Marketing.
   - Descripción: especifique una descripción de dominio opcional.
   - Cifrado de datos: sus datos se cifran de forma predeterminada con una clave que le AWS pertenece y administra por usted. Para este caso de uso, puede dejar la configuración de cifrado de datos predeterminada.

     Para obtener más información sobre el uso de claves administradas por el cliente, consulteEl cifrado de datos en reposo para Amazon DataZone. Si utiliza su propia clave KMS para el cifrado de datos, debe incluir la siguiente declaración en la configuración predeterminadaAmazonDataZoneDomainExecutionRole.

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

- Acceso al servicio: deje sin cambios la opción seleccionada de forma predeterminada Usar un rol predeterminado.

> **Note**
>
> Si utilizas un DataZone dominio de Amazon existente para este flujo de trabajo, puedes elegir la opción Usar un rol de servicio existente y, a continuación, elegir un rol existente en el menú desplegable.

- En Configuración rápida, selecciona Configurar esta cuenta para el consumo y la publicación de datos. Esta opción habilita los DataZone planos integrados en Amazon de Data Lake y Data Warehouse, y configura los permisos, los recursos, un proyecto predeterminado y los perfiles de entorno de data lake y data warehouse necesarios para esta cuenta. Para obtener más información sobre los DataZone blueprints de Amazon, consulte DataZone Terminología y conceptos de Amazon.
- Mantenga sin cambios el resto de los campos de la sección Detalles de permisos.

> **Note**
>
> Si ya tienes un DataZone dominio de Amazon, puedes elegir la opción Usar un rol de servicio existente y, a continuación, elegir un rol existente en el menú desplegable para el rol Glue Manage Access, el rol Redshift Manage Access y el rol Provisioning.

- Mantenga los campos debajo de las etiquetas sin cambios.
- Seleccione Create domain (Crear un dominio).

3. Una vez que el dominio se haya creado correctamente, selecciónelo y, en la página de resumen del dominio, anote la URL del portal de datos correspondiente a este dominio. Puedes usar esta URL para acceder a tu portal de DataZone datos de Amazon y completar el resto de los pasos de este flujo de trabajo. También puede navegar al portal de datos seleccionando Portal de datos abiertos.

> **Note**
>
> En la versión actual de Amazon DataZone, una vez creado el dominio, la URL generada para el portal de datos no se puede modificar.

La creación del dominio puede tardar varios minutos en completarse. Espere a que el dominio tenga el estado Disponible antes de continuar con el siguiente paso.

Paso 2: Crea el proyecto de publicación

En esta sección se describen los pasos necesarios para crear el proyecto de publicación para este flujo de trabajo.

1. Cuando hayas completado el paso 1 anterior y hayas creado un dominio, verás el mensaje ¡Bienvenido a Amazon DataZone! ventana. En esta ventana, selecciona Crear proyecto.
2. Especifique el nombre del proyecto, por ejemplo, para este flujo de trabajo, puede asignarle un nombre SalesDataPublishingProject, dejar el resto de los campos sin cambios y, a continuación, elegir Crear.

Paso 3: Crea el entorno

En esta sección se describen los pasos necesarios para crear un entorno para este flujo de trabajo.

1. Cuando complete el paso 2 anterior y cree su proyecto, verá la ventana Su proyecto está listo para usarse. En esta ventana, selecciona Crear entorno.
2. En la página Crear entorno, especifique lo siguiente y, a continuación, seleccione Crear entorno.
3. Especifique valores para lo siguiente:

- Nombre: especifique el nombre del entorno. Para este tutorial, puede llamarlo. `Default data lake environment`
- Descripción: especifique una descripción para el entorno.
- Perfil de entorno: elija el perfil de DataLakeProfileentorno. Esto le permite utilizar Amazon DataZone en este flujo de trabajo para trabajar con datos en Amazon S3, AWS Glue Catalog y Amazon Athena.
- Para este tutorial, mantenga el resto de los campos sin cambios.

4. Seleccione Crear entorno.

Paso 4: Producir datos para su publicación

En esta sección se describen los pasos necesarios para producir datos para su publicación en este flujo de trabajo.

1. Cuando complete el paso 3 anterior, en su `SalesDataPublishingProject` proyecto, en el panel de la derecha, en Herramientas de análisis, elija Amazon Athena. Esto abre el editor de consultas de Athena con las credenciales de su proyecto para la autenticación. Asegúrese de que su entorno de publicación esté seleccionado en el menú desplegable del DataZone entorno de Amazon y de que la `<environment_name>%_pub_db` base de datos esté seleccionada como en el editor de consultas.
2. En este tutorial, utilizará el script de consulta Create Table as Select (CTAS) para crear una tabla nueva que desee publicar en Amazon. DataZone En su editor de consultas, ejecute este script de CTAS para crear una `mkt_sls_table` tabla que pueda publicar y poner a disposición para su búsqueda y suscripción.

```
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
```

Asegúrese de que la tabla mkt_sls_table se ha creado correctamente en la sección Tablas y vistas de la parte izquierda. Ahora tienes un activo de datos que se puede publicar en el DataZone catálogo de Amazon.

Paso 5: Recopila metadatos de AWS Glue

En esta sección se describe el paso de recopilar metadatos de AWS Glue para este flujo de trabajo.

1. Una vez que hayas completado el paso 4 anterior, en el portal de DataZone datos de Amazon, elige el `SalesDataPublishingProject` proyecto, luego elige la pestaña Datos y, a continuación, elige Fuentes de datos en el panel de la izquierda.
2. Elija la fuente que se creó como parte del proceso de creación del entorno.
3. Selecciona Ejecutar junto al menú desplegable Acción y, a continuación, selecciona el botón de actualización. Una vez finalizada la ejecución de la fuente de datos, los activos se añaden al DataZone inventario de Amazon.

Paso 6: Seleccione y publique el activo de datos

En esta sección se describen los pasos para conservar y publicar el activo de datos en este flujo de trabajo.

1. Una vez que hayas completado el paso 5 anterior, en el portal de DataZone datos de Amazon, elige el `SalesDataPublishingProject` proyecto que creaste en el paso anterior, elige la pestaña Datos de inventario en el panel de la izquierda y localiza la `mkt_sls_table` tabla.
2. Abre la página de detalles del `mkt_sls_table` activo para ver los nombres comerciales generados automáticamente. Seleccione el icono de metadatos generados automáticamente para ver los nombres generados automáticamente para los activos y las columnas. Puede aceptar o rechazar cada nombre de forma individual o seleccionar Aceptar todos para aplicar los nombres generados. Si lo desea, también puede añadir el formulario de metadatos disponible a su activo y seleccionar los términos del glosario para clasificar los datos.
3. Elija Publicar recurso para publicar el `mkt_sls_table` recurso.

Paso 7: Cree el proyecto para el análisis de datos

En esta sección se describen los pasos para crear el proyecto para el análisis de datos. Este es el comienzo de los pasos de consumo de datos de este flujo de trabajo.

1. Cuando hayas completado el paso 6 anterior, en el portal de DataZone datos de Amazon, selecciona Crear proyecto en el menú desplegable Proyecto.
2. En la página Crear proyecto, especifique el nombre del proyecto, por ejemplo, para este flujo de trabajo, puede asignarle un nombre MarketingDataAnalysisProject, dejar el resto de los campos sin cambios y, a continuación, seleccionar Crear.

Paso 8: Crear un entorno para el análisis de datos

En esta sección se describen los pasos para crear un entorno para el análisis de datos.

1. Una vez que haya completado el paso 7 anterior, en el portal de DataZone datos de Amazon, elija el `MarketingDataAnalysisProject` proyecto, elija la pestaña Entornos y, por último, elija Crear entorno.
2. En la página Crear entorno, especifique lo siguiente y, a continuación, seleccione Crear entorno.
   - Nombre: especifique el nombre del entorno. Para este tutorial, puede llamarlo. `Default data lake environment`
   - Descripción: especifique una descripción para el entorno.
   - Perfil de entorno: elija el perfil de DataLakeProfileentorno integrado.
   - Para este tutorial, mantenga el resto de los campos sin cambios.

Paso 9: busque en el catálogo de datos y suscríbase a los datos

En esta sección se describen los pasos para buscar en el catálogo de datos y suscribirse a los datos.

1. Una vez que complete el paso 8 anterior, en el portal de DataZone datos de Amazon, elija el DataZone icono de Amazon y, en el campo DataZone Búsqueda de Amazon, busque activos de datos mediante palabras clave (por ejemplo, «catálogo» o «ventas») en la barra de búsqueda del portal de datos.

   Si es necesario, aplique filtros o clasifíquelos y, una vez que encuentre el activo de datos de ventas de productos, podrá seleccionarlo para abrir la página de detalles del activo.

2. En la página de detalles del activo de datos de ventas por catálogo, seleccione Suscribirse.
3. En el cuadro de diálogo Suscribirse, elija su proyecto de MarketingDataAnalysisProjectconsumidor en el menú desplegable, especifique el motivo de su solicitud de suscripción y, a continuación, elija Suscribirse.

Paso 10: Aprueba la solicitud de suscripción

En esta sección se describen los pasos para aprobar la solicitud de suscripción.

1. Una vez que complete el paso 9 anterior, en el portal de DataZone datos de Amazon, elija el SalesDataPublishingProjectproyecto con el que publicó su activo.
2. Selecciona la pestaña Datos, luego Datos publicados y, a continuación, selecciona Solicitudes entrantes.
3. Ahora puedes ver la fila de la nueva solicitud que necesita aprobación. Selecciona Ver solicitud. Indique el motivo de la aprobación y elija Aprobar.

Paso 11: Cree una consulta y analice los datos en Amazon Athena

Ahora que has publicado correctamente un activo en el DataZone catálogo de Amazon y te has suscrito a él, puedes analizarlo.

1. En el portal de DataZone datos de Amazon, elige tu proyecto de MarketingDataAnalysisProjectconsumidor y, a continuación, en el panel de la derecha, en Herramientas de análisis, selecciona el enlace Consulta de datos con Amazon Athena. Esto abre el editor de consultas de Amazon Athena con las credenciales de su proyecto para la autenticación. Elija el entorno de MarketingDataAnalysisProjectconsumo en el menú desplegable Amazon DataZone Environment del editor de consultas y, a continuación, elija el de su proyecto en el menú desplegable `<environment_name>%sub_db` de la base de datos.
2. Ahora puede ejecutar consultas en la tabla suscrita. Puede elegir la tabla en Tablas y vistas y, a continuación, elegir Vista previa para que la declaración seleccionada aparezca en la pantalla del editor. Ejecute la consulta para ver los resultados.

Guía de DataZone inicio rápido de Amazon con los datos de Amazon Redshift

Temas

Paso 1: Crea el portal de DataZone dominios y datos de Amazon

Complete el siguiente procedimiento para crear un DataZone dominio de Amazon. Para obtener más información sobre DataZone los dominios de Amazon, consulte DataZone Terminología y conceptos de Amazon.

1. Ve a la DataZone consola de Amazon en https://console.aws.amazon.com/datazone, inicia sesión y, a continuación, selecciona Crear dominio.

   > **Note**
   >
   > Si quieres usar un DataZone dominio de Amazon existente para este flujo de trabajo, selecciona Ver dominios, elige el dominio que quieres usar y, a continuación, continúa con el paso 2 de creación de un proyecto de publicación.

2. En la página Crear dominio, proporciona valores para los siguientes campos:

   - Nombre: especifique un nombre para su dominio. A los efectos de este flujo de trabajo, puede llamar a este dominio`Marketing`.

- Descripción: especifique una descripción de dominio opcional.
- Cifrado de datos: sus datos se cifran de forma predeterminada con una clave que le AWS pertenece y administra por usted. Para este tutorial, puede dejar la configuración de cifrado de datos predeterminada.

  Para obtener más información sobre el uso de claves administradas por el cliente, consulteEl cifrado de datos en reposo para Amazon DataZone. Si utiliza su propia clave KMS para el cifrado de datos, debe incluir la siguiente declaración en la configuración predeterminadaAmazonDataZoneDomainExecutionRole.

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

- Acceso al servicio: elija la opción Usar un rol de servicio personalizado y, a continuación, elija AmazonDataZoneDomainExecutionRoleuno en el menú desplegable.
- En Configuración rápida, selecciona Configurar esta cuenta para el consumo y la publicación de datos. Esta opción habilita los DataZone planos integrados de Amazon para Data Lake y Data Warehouse, y configura los permisos y recursos necesarios para completar el resto de los pasos de este flujo de trabajo. Para obtener más información sobre los DataZone blueprints de Amazon, consulte DataZone Terminología y conceptos de Amazon.
- Mantén el resto de los campos de los detalles de los permisos y las etiquetas sin cambios y, a continuación, selecciona Crear dominio.

3. Una vez que el dominio se haya creado correctamente, elija este dominio y, en la página de resumen del dominio, anote la URL del portal de datos correspondiente a este dominio. Puedes usar esta URL para acceder a tu portal de DataZone datos de Amazon y completar el resto de los pasos de este flujo de trabajo.

> **Note**
>
> En la versión actual de Amazon DataZone, una vez creado el dominio, la URL generada para el portal de datos no se puede modificar.

La creación del dominio puede tardar varios minutos en completarse. Espere a que el dominio tenga el estado Disponible antes de continuar con el siguiente paso.

Paso 2: Crea el proyecto de publicación

En la siguiente sección se describen los pasos para crear el proyecto de publicación en este flujo de trabajo.

1. Cuando complete el paso 1, vaya al portal de DataZone datos de Amazon mediante la URL del portal de datos e inicie sesión con sus credenciales de inicio de sesión único (SSO) o AWS de IAM.
2. Elija Crear proyecto, especifique el nombre del proyecto, por ejemplo, para este flujo de trabajo, puede asignarle un nombre SalesDataPublishingProject, dejar el resto de los campos sin cambios y, a continuación, elegir Crear.

Paso 3: Crea el entorno

En la siguiente sección se describen los pasos para crear un entorno en este flujo de trabajo.

1. Cuando complete el paso 2, en el portal de DataZone datos de Amazon, elija el `SalesDataPublishingProject` proyecto que creó en el paso anterior, elija la pestaña Entornos y, por último, elija Crear entorno.
2. En la página Crear entorno, especifique lo siguiente y, a continuación, elija Crear entorno.
   - Nombre: especifique el nombre del entorno. Para este tutorial, puede llamarlo. `Default data warehouse environment`
   - Descripción: especifique una descripción para el entorno.
   - Perfil de entorno: elija el perfil de DataWarehouseProfileentorno.
   - Proporcione el nombre del clúster de Amazon Redshift, el nombre de la base de datos y el ARN secreto del clúster de Amazon Redshift en el que se almacenan los datos.

> **Note**
>
> Asegúrese de que su secreto en AWS Secrets Manager incluya las siguientes etiquetas (clave/valor):
>
> - Para el clúster de Amazon Redshift, datazone.rs.cluster: <cluster_name:database name>
>
> Para el grupo de trabajo Amazon Redshift Serverless: datazone.rs.workgroup: <workgroup_name:database_name>
> - AmazonDataZoneProject: <projectID>
> - AmazonDataZoneDomain: <domainID>
>
> Para obtener más información, consulte Almacenamiento de credenciales de bases de datos en AWS Secrets Manager.
>
> El usuario de la base de datos que proporcione en AWS Secrets Manager debe tener permisos de superusuario.

Paso 4: Producir datos para su publicación

En la siguiente sección se describen los pasos para producir datos para publicarlos en este flujo de trabajo.

1. Cuando complete el paso 3, en el portal de DataZone datos de Amazon, elija el `SalesDataPublishingProject` proyecto y, a continuación, en el panel de la derecha, en Herramientas de análisis, elija Amazon Redshift. Esto abre el editor de consultas de Amazon Redshift con las credenciales del proyecto para la autenticación.
2. En este tutorial, utilizará el script de consulta Create Table as Select (CTAS) para crear una tabla nueva que desee publicar en Amazon. DataZone En su editor de consultas, ejecute este script de CTAS para crear una `mkt_sls_table` tabla que pueda publicar y poner a disposición para su búsqueda y suscripción.

```
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
```

Asegúrese de que la tabla mkt_sls_table se ha creado correctamente. Ahora tienes un activo de datos que se puede publicar en el DataZone catálogo de Amazon.

Paso 5: Reunir metadatos de Amazon Redshift

En la siguiente sección se describen los pasos para recopilar metadatos de Amazon Redshift.

1. Una vez que complete el paso 4, en el portal de DataZone datos de Amazon, elija el `SalesDataPublishingProject` proyecto, luego elija la pestaña Datos y, por último, elija Fuentes de datos.
2. Elija la fuente que se creó como parte del proceso de creación del entorno.
3. Selecciona Ejecutar junto al menú desplegable Acción y, a continuación, selecciona el botón de actualización. Una vez finalizada la ejecución de la fuente de datos, los activos se añaden al DataZone inventario de Amazon.

Paso 6: Seleccione y publique el activo de datos

En la siguiente sección se describen los pasos para conservar y publicar el activo de datos en este flujo de trabajo.

1. Cuando hayas completado el paso 5, en el portal de DataZone datos de Amazon, selecciona el `SalesDataPublishingProject` proyecto y, a continuación, selecciona la pestaña Datos, selecciona Datos de inventario y localiza la `mkt_sls_table` tabla.
2. Abre la página de detalles del `mkt_sls_table` activo para ver los nombres comerciales generados automáticamente. Seleccione el icono de metadatos generados automáticamente para ver los nombres generados automáticamente para los activos y las columnas. Puede aceptar o rechazar cada nombre de forma individual o seleccionar Aceptar todos para aplicar los

nombres generados. Si lo desea, también puede añadir el formulario de metadatos disponible a su activo y seleccionar los términos del glosario para clasificar los datos.

3. Elija Publicar para publicar el `mkt_sls_table` recurso.

Paso 7: Cree el proyecto para el análisis de datos

En la siguiente sección se describen los pasos para crear el proyecto para el análisis de datos en este flujo de trabajo.

1. Una vez que complete el paso 6, en el portal de DataZone datos de Amazon, elija Crear proyecto.
2. En la página Crear proyecto, especifique el nombre del proyecto, por ejemplo, para este flujo de trabajo, puede asignarle un nombre MarketingDataAnalysisProject, dejar el resto de los campos sin cambios y, por último, elegir Crear.

Paso 8: Crear un entorno para el análisis de datos

En la siguiente sección se describen los pasos para crear un entorno para el análisis de datos en este flujo de trabajo.

1. Cuando complete el paso 7, en el portal de DataZone datos de Amazon, elija el `MarketingDataAnalysisProject` proyecto que creó en el paso anterior, elija la pestaña Entornos y, a continuación, elija Agregar entorno.
2. En la página Crear entorno, especifique lo siguiente y, a continuación, elija Crear entorno.

   - Nombre: especifique el nombre del entorno. Para este tutorial, puede llamarlo. `Default data warehouse environment`
   - Descripción: especifique una descripción para el entorno.
   - Perfil de entorno: elija DataWarehouseProfileel perfil de entorno.
   - Proporcione el nombre del clúster de Amazon Redshift, el nombre de la base de datos y el ARN secreto del clúster de Amazon Redshift en el que se almacenan los datos.

   > **Note**
   >
   > Asegúrese de que su secreto en AWS Secrets Manager incluya las siguientes etiquetas (clave/valor):

- Para el clúster de Amazon Redshift, datazone.rs.cluster: <cluster_name:database name>

  Para el grupo de trabajo Amazon Redshift Serverless: datazone.rs.workgroup: <workgroup_name:database_name>
- AmazonDataZoneProject: <projectID>
- AmazonDataZoneDomain: <domainID>

Para obtener más información, consulte Almacenamiento de credenciales de bases de datos en AWS Secrets Manager.

El usuario de la base de datos que proporcione en AWS Secrets Manager debe tener permisos de superusuario.

- Para este tutorial, mantenga el resto de los campos sin cambios.

Paso 9: busque en el catálogo de datos y suscríbase a los datos

En la siguiente sección se describen los pasos para buscar en el catálogo de datos y suscribirse a los datos.

1. Cuando complete el paso 8, en el portal de DataZone datos de Amazon, busque activos de datos mediante palabras clave (p. ej., «catálogo» o «ventas») en la barra de búsqueda del portal de datos.

   Si es necesario, aplique filtros o clasifique y, una vez que encuentre el activo de datos de ventas de productos, podrá seleccionarlo para abrir la página de detalles del activo.
2. En la página de detalles del activo de datos de ventas de productos, selecciona Suscribirse.
3. En el cuadro de diálogo, elige tu proyecto de consumidor en el menú desplegable, indica el motivo de la solicitud de acceso y, a continuación, selecciona Suscribirse.

Paso 10: Aprueba la solicitud de suscripción

En la siguiente sección se describen los pasos para aprobar la solicitud de suscripción en este flujo de trabajo.

1. Una vez que complete el paso 9, en el portal de DataZone datos de Amazon, elija el SalesDataPublishingProjectproyecto con el que publicó su activo.

2. Selecciona la pestaña Datos, luego Datos publicados y, por último, Solicitudes entrantes.
3. Selecciona el enlace para ver la solicitud y, a continuación, selecciona Aprobar.

Paso 11: Cree una consulta y analice los datos en Amazon Redshift

Ahora que has publicado correctamente un activo en el DataZone catálogo de Amazon y te has suscrito a él, puedes analizarlo.

1. En el panel derecho del portal de DataZone datos de Amazon, haz clic en el enlace Amazon Redshift. Esto abre el editor de consultas de Amazon Redshift con la credencial del proyecto para la autenticación.
2. Ahora puede ejecutar una consulta (sentencia de selección) en la tabla suscrita. Puede hacer clic en la tabla (three-vertical-dots opción) y elegir la vista previa para que la declaración seleccionada aparezca en la pantalla del editor. Ejecute la consulta para ver los resultados.

Guía de DataZone inicio rápido de Amazon con scripts de muestra

En la siguiente sección se describen ejemplos de scripts que invocan varias DataZone API de Amazon que puede utilizar para realizar las siguientes tareas:

Temas

- Crea un portal de datos y DataZone dominios de Amazon
- Cree un proyecto de publicación
- Cree un perfil de entorno
- Creación de un entorno
- Recopila metadatos de AWS Glue
- Seleccione y publique un activo de datos
- Busque en el catálogo de datos y suscríbase a los datos
- Otros ejemplos de scripts útiles

Crea un portal de datos y DataZone dominios de Amazon

Puedes usar el siguiente script de ejemplo para crear un DataZone dominio de Amazon. Para obtener más información sobre DataZone los dominios de Amazon, consulte DataZone Terminología y conceptos de 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",
    )
```

Cree un proyecto de publicación

Puedes usar el siguiente script de ejemplo para crear un proyecto de publicación en Amazon DataZone.

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

Cree un perfil de entorno

Puede utilizar los siguientes scripts de ejemplo para crear un perfil de entorno en Amazon DataZone.

Este ejemplo de carga útil se utiliza cuando se invoca la `CreateEnvironmentProfile` API:

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

Este script de ejemplo invoca la `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
```

Esta es la carga útil de salida de muestra una vez que se invoca la `CreateEnvironmentProfile` API:

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

```
                ]
            }
        ]
    }
}
```

Creación de un entorno

Puede utilizar el siguiente script de ejemplo para crear un entorno en 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
```

Recopila metadatos de AWS Glue

Puedes usar este script de ejemplo para recopilar metadatos de AWS Glue. Este script se ejecuta según un cronograma estándar. Puede recuperar los parámetros del script de muestra y hacerlos globales. Obtenga el ID del proyecto, el entorno y el dominio mediante funciones estándar. La fuente de datos de AWS Glue se crea y ejecuta a una hora estándar que se puede actualizar en la sección cron del 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"
    }
}
```

Seleccione y publique un activo de datos

Puede utilizar los siguientes scripts de ejemplo para seleccionar y publicar activos de datos en Amazon DataZone.

Puede usar el siguiente script para crear tipos de formulario personalizados:

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

```
        },
        owningProjectIdentifier = projectId,
        status = "ENABLED"
    )
```

Puede utilizar el siguiente script de ejemplo para crear tipos de activos personalizados:

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

Puede utilizar el siguiente script de ejemplo para crear activos personalizados:

```
def create_custom_asset(domainId, projectId):
    return dzclient.create_asset(
        domainIdentifier = domainId,
        name = 'custom asset',
        description = "custom asset",
        owningProjectIdentifier = projectId,
        typeIdentifier = "userCustomAssetType",
        formsInput = [
            {
                "formName": "UserCustomForm",
                "typeIdentifier": "customForm",
                "content": "{\"simple\":\"sample-catalogId\"}"
            }
        ]
    )
```

Puede utilizar el siguiente script de ejemplo para crear un glosario:

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

Puede utilizar el siguiente script de ejemplo para crear un término en el glosario:

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

Puede utilizar el siguiente script de ejemplo para crear un activo mediante un tipo de activo definido por el sistema:

```
def create_asset(domainId, projectId):
    return dzclient.create_asset(
        domainIdentifier = domainId,
        name = 'sample asset name',
        description = "this is a glue table asset",
        owningProjectIdentifier = projectId,
        typeIdentifier = "amazon.datazone.GlueTableAssetType",
        formsInput = [
            {
                "formName": "GlueTableForm",
                "content": "{\"catalogId\":\"sample-catalogId\",\"columns\":
[{\"columnDescription\":\"sample-columnDescription\",\"columnName\":\"sample-
```

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

Puede utilizar el siguiente script de ejemplo para crear una revisión de activos y adjuntar un término al glosario:

```
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:>"]
    )
```

Puede utilizar el siguiente script de ejemplo para publicar un activo:

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

Busque en el catálogo de datos y suscríbase a los datos

Puede utilizar los siguientes scripts de ejemplo para buscar en el catálogo de datos y suscribirse a los datos:

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

Puedes usar el siguiente script de ejemplo para obtener el ID de listado del activo:

```
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']
```

Puedes usar los siguientes scripts de ejemplo para crear una solicitud de suscripción con el ID del anuncio:

```
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."
    )
```

Con `create_subscription_response` lo anterior, obtén la suscripción y `subscription_request_id`, a continuación, acéptala o aprueba mediante el siguiente script de ejemplo:

```
subscription_request_id = create_subscription_response["id"]

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

Otros ejemplos de scripts útiles

Puedes usar los siguientes scripts de ejemplo para completar varias tareas mientras trabajas con tus datos en Amazon DataZone.

Usa el siguiente script de ejemplo para enumerar los DataZone dominios de Amazon existentes:

```
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
```

Usa el siguiente script de ejemplo para enumerar los DataZone proyectos de Amazon existentes:

```
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
```

Usa el siguiente script de ejemplo para enumerar los formularios de DataZone metadatos de Amazon existentes:

```
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
```

Administrar DataZone los dominios de Amazon y el acceso de los usuarios

Temas

Crea dominios

> **Note**
>
> Si utilizas Amazon DataZone con AWS Identity Center para proporcionar acceso a los usuarios y grupos de SSO, actualmente tu DataZone dominio de Amazon debe estar en la misma AWS región que tu instancia de AWS Identity Center.

Amazon DataZone, un dominio es una entidad organizadora para conectar sus activos, usuarios y sus proyectos. Para obtener más información, consulte DataZone Terminología y conceptos de Amazon.

Para crear un DataZone dominio de Amazon, debes asumir una función de IAM en la cuenta con permisos administrativos. Configure los permisos de IAM necesarios para usar la consola de DataZone administración de Amazonpara obtener los permisos mínimos necesarios para crear un dominio.

Amazon necesita funciones de IAM adicionales DataZone para realizar acciones en nombre de los usuarios del dominio con una configuración predeterminada. Puede crear estas funciones de IAM por adelantado o hacer que Amazon las DataZone cree por usted. Si quieres que Amazon DataZone cree estas funciones de IAM por ti durante el proceso de creación del dominio, debes asumir una

función de IAM con permisos de creación de funciones. Consulte Cree una política personalizada para los permisos de IAM para permitir la creación simplificada de roles en la consola de DataZone servicio de Amazon . En función de tus opciones de creación de dominios, Amazon DataZone creará hasta cuatro nuevas funciones de IAM para ti: AmazonDataZoneDomainExecutionRole, AmazonDataZoneGlueManageAccessRoleAmazonDataZoneRedshiftManageAccessRole, y AmazonDataZoneProvisioningRole.

Complete el siguiente procedimiento para crear un DataZone dominio de Amazon.

1. Ve a la DataZone consola de Amazon en https://console.aws.amazon.com/datazone y utiliza el selector de regiones de la barra de navegación superior para elegir la AWS región correspondiente.
2. Selecciona Crear dominio y proporciona valores para los siguientes campos:

   - Nombre: especifique un nombre descriptivo para el dominio. Una vez creado el dominio, este nombre no se puede cambiar.
   - Descripción: (opcional) especifique una descripción de dominio.
   - Cifrado de datos: el Servicio de administración de AWS claves (KMS) cifra tu DataZone dominio de Amazon, tus metadatos y tus datos de informes con una clave específica de tu Amazon DataZone. Usa este campo para especificar si quieres usar una AWS clave propia o elegir una clave de AWS KMS diferente.

     Para obtener más información sobre el uso de claves administradas por el cliente, consulteEl cifrado de datos en reposo para Amazon DataZone. Si utiliza su propia clave KMS para el cifrado de datos, debe incluir la siguiente declaración en la configuración predeterminadaAmazonDataZoneDomainExecutionRole.

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

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

- Acceso al servicio: elige si deseas que Amazon DataZone cree y use uno nuevo DomainExecutionRolepara ti o elige un rol de IAM existente.
- Configuración rápida: (opcional) marca esta casilla para empezar más rápido haciendo que Amazon DataZone configure tu cuenta para el consumo y la publicación de datos. Amazon DataZone creará tres funciones de IAM para aprovisionar, administrar y administrar el acceso a los recursos de AWS Glue y Amazon Redshift, creará un nuevo bucket de Amazon S3, creará un DataZone proyecto administrativo de Amazon y creará perfiles de entorno para los planos predeterminados del lago de datos y el almacén de datos.
- Etiquetas: (opcional) especifique las AWS etiquetas (pares de clave y valor) para el dominio.
- Una vez que el dominio se haya creado correctamente, tu navegador debería actualizarse para mostrar la página de detalles del nuevo DataZone dominio de Amazon.

Edita los dominios

En Amazon DataZone, un dominio es una entidad organizadora que conecta tus activos, usuarios y sus proyectos. Para obtener más información, consulte DataZone Terminología y conceptos de Amazon.

Tras crear un DataZone dominio de Amazon, podrás editarlo posteriormente para: cambiar la descripción, activar el Centro de Identidad de IAM y añadir, editar o eliminar las claves de etiquetas y sus valores. Para editar un DataZone dominio de Amazon, debes asumir una función de IAM en la cuenta con permisos administrativos. Configure los permisos de IAM necesarios para usar la consola de DataZone administración de Amazonpara obtener los permisos mínimos necesarios para editar un dominio.

Para editar un dominio, siga estos pasos:

1. Inicie sesión en la consola AWS de administración y abra la DataZone consola de Amazon en https://console.aws.amazon.com/datazone.
2. Selecciona Ver dominios y elige el nombre del dominio de la lista. El nombre es un hipervínculo.

3. En la página de detalles del dominio, selecciona Editar.
4.
   - Edita la descripción.
   - Establezca la configuración del Centro de identidad de IAM. Obtenga más información sobre estos ajustes enConfiguración del centro de identidad de AWS IAM para Amazon DataZone.
   - Agrega, edita o elimina las claves de etiqueta y sus valores.
5. Una vez que hayas realizado las modificaciones, selecciona Actualizar dominio.

Eliminar dominios

En Amazon DataZone, un dominio es una entidad organizadora que conecta tus activos, usuarios y sus proyectos. Para obtener más información, consulte DataZone Terminología y conceptos de Amazon.

El acto de eliminar un dominio es definitivo. La eliminación elimina irrevocablemente todas las DataZone entidades de Amazon, incluidas las fuentes de datos, los proyectos, los entornos, los activos, los glosarios y los formularios de metadatos. La eliminación no elimina DataZone AWS los recursos ajenos a Amazon que Amazon DataZone pueda haberle ayudado a crear, como las funciones de IAM, los buckets de S3, las bases de datos de AWS Glue y las subvenciones de suscripción a través de Redshift o LakeFormation Redshift. Si ya no necesita estos recursos, elimínelos en el servicio correspondiente. AWS

Para evitar que alguien elimine un dominio de forma malintencionada, la eliminación de un dominio requiere permisos administrativos de IAM para Amazon DataZone, que puedes configurar con IAM. Para evitar que alguien elimine un dominio accidentalmente, para eliminar un dominio se requiere una palabra de confirmación (en la DataZone consola de Amazon).

Para eliminar un dominio, sigue estos pasos:

1. Inicie sesión en la consola AWS de administración y abra la DataZone consola de Amazon en https://console.aws.amazon.com/datazone.
2. Selecciona Ver dominios y elige el nombre del dominio de la lista. El nombre es un hipervínculo.
3. Seleccione Eliminar y revise las advertencias informativas.
4. Escribe el texto solicitado para confirmar que entiendes estas advertencias. Elija Eliminar.

> **Important**
>
> Eliminar tu dominio es una acción irrevocable que no puedes deshacer ni tú ni tú. AWS

> **Note**
>
> Cuando tú o los usuarios de tu dominio creáis un entorno en un proyecto, Amazon DataZone crea AWS recursos en vuestro dominio o en las cuentas asociadas para proporcionaros funcionalidad a vosotros y a los usuarios de vuestro dominio. A continuación, se muestra la lista de AWS recursos que Amazon DataZone puede crear para proyectos en tu dominio, junto con el nombre predeterminado. Al eliminar un dominio, no se elimina ninguno de estos AWS recursos de tus AWS cuentas.
>
> - <environmentId>Funciones de IAM: datazone_usr_.
> - <environmentName>Bases de datos Glue: (1) <environmentName>_pub_db-*, (2) _sub_db-*. Si ya existía una base de datos con este nombre, Amazon DataZone añadirá el ID del entorno.
> - <environmentName>Grupos de trabajo de Athena: -*. Si ya existía un grupo de trabajo con este nombre, Amazon DataZone añadirá el ID del entorno.
> - CloudWatch grupo de registro: datazone_ <environmentId>

Habilitar el Centro de Identidad de IAM para Amazon DataZone

> **Note**
>
> Para completar este procedimiento, debes tener activado el Centro de identidad de AWS IAM en la misma AWS región que tu DataZone dominio de Amazon.

Puedes proporcionar a los usuarios y grupos de SSO acceso a tu portal de DataZone datos de Amazon mediante AWS IAM Identity Center. Una vez completadoConfiguración del centro de identidad de AWS IAM para Amazon DataZone, puedes permitir que tus usuarios y grupos de SSO accedan a tu portal de datos de DataZone dominios de Amazon.

Para habilitar el uso del Centro de Identidad de AWS IAM con tu DataZone dominio de Amazon, debes asumir una función de IAM en la cuenta con permisos administrativos. Configure los permisos de IAM necesarios para usar la consola de DataZone administración de Amazony Cree una política personalizada para los permisos de IAM para permitir la creación simplificada de roles en la consola de DataZone servicio de Amazon obtener los permisos mínimos necesarios para habilitar el IAM Identity Center para su uso con Amazon DataZone.

Complete el siguiente procedimiento para habilitar el Centro de identidades de AWS IAM para Amazon DataZone.

1. Inicie sesión en la consola AWS de administración y abra la DataZone consola en https://console.aws.amazon.com/datazone.
2. Seleccione Ver dominios y elija el nombre del dominio de la lista. El nombre es un hipervínculo.
3. En la página de detalles del dominio, selecciona Editar.
   - Seleccione la casilla Habilitar usuarios en el Centro de identidades de IAM.
   - Elija entre los dos modos de asignación de usuarios. Una vez que tu dominio se actualice con tu selección, no podrás cambiarlo más adelante.
     - Con la asignación de usuarios implícita, cualquier usuario que se añada al directorio del centro de identidad de IAM puede acceder a su dominio de Amazon DataZone .
     - Con la asignación explícita de usuarios, añadirá usuarios o grupos específicos de su directorio de IAM Identity Center para proporcionarles acceso a su DataZone dominio de Amazon. Añadirás y eliminarás estos usuarios y grupos más adelante en Amazon DataZone Console.
4. Una vez que esté satisfecho con su selección, elija Actualizar dominio.

Desactivar el centro de identidad de IAM para Amazon DataZone

Al deshabilitar el Centro de identidad de AWS IAM para un DataZone dominio de Amazon, se eliminará el acceso de todos los usuarios de SSO.

> **Note**
>
> La desactivación del Centro de Identidad de IAM no detendrá la facturación a los usuarios del SSO. Para dejar de facturar a los usuarios de SSO, debes desactivarlos en tu dominio. La

facturación continúa hasta el final del mes en el que se desactiva un usuario. Para desactivar usuarios, consulte. Administra los usuarios en la DataZone consola de Amazon

Puedes proporcionar a los usuarios y grupos de SSO acceso a tu portal de DataZone datos de Amazon mediante AWS IAM Identity Center. Si ha activado AWS IAM Identity Center para Amazon DataZone, más adelante podrá deshabilitar el acceso para todos los usuarios.

Para inhabilitar el Centro de identidad de AWS IAM para su uso con tu DataZone dominio de Amazon, debes asumir una función de IAM en la cuenta con permisos administrativos. Configure los permisos de IAM necesarios para usar la consola de DataZone administración de Amazony Cree una política personalizada para los permisos de IAM para permitir la creación simplificada de roles en la consola de DataZone servicio de Amazon obtener los permisos mínimos necesarios para inhabilitar el uso del Centro de Identidad de IAM con Amazon DataZone.

Complete el siguiente procedimiento para deshabilitar el Centro de identidades de AWS IAM para Amazon DataZone.

1. Inicie sesión en la consola AWS de administración y abra la DataZone consola en https://console.aws.amazon.com/datazone.
2. Seleccione Ver dominios y elija el nombre del dominio de la lista. El nombre es un hipervínculo.
3. <regionName><accountId><domainName>Copia el nombre de recurso de Amazon (ARN) de tu dominio, que comienza por arn:aws:datazone: ::domain/.
4. Abra la consola del IAM Identity Center en https://console.aws.amazon.com/singlesignon/.
5. Elija Aplicaciones.
6. Elija el dominio para el que desee deshabilitar el Centro de identidades de AWS IAM, lo que impedirá el acceso al portal de datos del dominio para todos los usuarios de SSO. Puede utilizar el menú Filtro y el cuadro de búsqueda para filtrar la lista de aplicaciones.
7. En el menú Acciones, selecciona Desactivar.
8. Los usuarios de SSO perderán el acceso al DataZone dominio de Amazon.
9. Para volver a activar el Centro de Identidad de AWS IAM para el DataZone dominio de Amazon, selecciona el dominio para el que quieres volver a activar el Centro de Identidad de AWS IAM y, en el menú Acciones, selecciona Activar.

Administra los usuarios en la DataZone consola de Amazon

Sus usuarios pueden acceder al portal de DataZone datos de Amazon mediante sus AWS credenciales o credenciales de inicio de sesión único (SSO). Para gestionar los usuarios de un DataZone dominio de Amazon en la DataZone consola de Amazon, debes asumir una función de IAM en la cuenta con permisos administrativos. Configure los permisos de IAM necesarios para usar la consola de DataZone administración de Amazonpara obtener los permisos mínimos necesarios para gestionar los usuarios en la DataZone consola de Amazon.

Temas

- Gestione las funciones y los usuarios de IAM
- Administre los usuarios de SSO
- Administra los grupos de SSO

Gestione las funciones y los usuarios de IAM

Los roles y usuarios de IAM se crean mediante AWS Identity and Access Management (IAM) (Identity and Access Management, IAM) y acceden a tus DataZone dominios de Amazon mediante los permisos que se les asignan mediante políticas. Para obtener más información, consulte Configure los permisos de IAM necesarios para usar el portal de DataZone datos de Amazon. Puedes ver la lista de funciones y usuarios de IAM que han activado su suscripción a un DataZone dominio de Amazon, han desactivado su acceso y lo han activado si lo habían desactivado anteriormente.

1. Inicie sesión en la consola AWS de administración y abra la DataZone consola en https://console.aws.amazon.com/datazone.
2. Seleccione Ver dominios y elija el nombre del dominio de la lista. El nombre es un hipervínculo.
3. En la página de detalles del dominio, selecciona Administración de usuarios.
4. Para el tipo de usuario, seleccione Usuarios de IAM para ver la lista actual de usuarios y funciones de IAM activados y desactivados.

    - La columna Nombre muestra el nombre del usuario o rol de IAM.
    - La columna Estado muestra el estado actual del usuario o rol de IAM en el dominio.
        - Activado significa que el usuario o rol de IAM ha llamado a una API, ha emitido un comando (mediante la interfaz de línea de comandos) o ha accedido al DataZone portal de Amazon de tu dominio, y se te está facturando la suscripción del usuario.

- Desactivado significa que el usuario o rol de IAM tiene bloqueado el acceso a tu dominio de Amazon DataZone .

5. Para desactivar un usuario o rol de IAM que esté activado actualmente, marca la casilla situada junto al usuario y selecciona Desactivar en el menú Acciones. El usuario perderá el acceso al DataZone dominio de Amazon. La facturación del usuario finalizará al final del mes natural actual.
6. Para activar un usuario o rol de IAM que esté actualmente desactivado, marca la casilla situada junto al usuario y selecciona Activar en el menú Acciones. El usuario tendrá acceso al DataZone dominio de Amazon si el usuario o rol de IAM tiene los permisos adecuados. La facturación para el usuario se reanudará.

Administre los usuarios de SSO

Los usuarios de SSO se crean o sincronizan con su proveedor de identidades en el Centro de identidades de AWS IAM. Para obtener más información, consulte Configuración del centro de identidad de AWS IAM para Amazon DataZone y Habilitar el Centro de Identidad de IAM para Amazon DataZone para habilitar y configurar AWS IAM Identity Center para Amazon DataZone. Puede ver la lista de usuarios de SSO asignados al dominio, añadir usuarios de SSO y eliminar usuarios de SSO.

1. Inicie sesión en la consola AWS de administración y abra la DataZone consola en https://console.aws.amazon.com/datazone.
2. Seleccione Ver dominios y elija el nombre del dominio de la lista. El nombre es un hipervínculo.
3. En la página de detalles del dominio, desplázate hacia abajo y selecciona Administración de usuarios.
4. Para el tipo de usuario, selecciona Usuarios de SSO para ver la lista actual de usuarios de SSO.

   - La columna Nombre muestra el nombre del usuario del SSO.
   - La columna Estado muestra el estado actual del usuario de SSO en el dominio.
     - Asignado significa que el usuario del SSO se ha asignado explícitamente al dominio. Como resultado, el usuario tiene acceso a Amazon DataZone. Este estado solo se usa cuando el modo de proveedor de identidad de tu dominio está configurado para una asignación explícita.

- Activado significa que el usuario de SSO ha accedido al DataZone portal de Amazon del dominio y se te está facturando la suscripción del usuario. La activación se produce automáticamente.
- Desactivado significa que el acceso del usuario de SSO está bloqueado al portal de datos del dominio. La facturación del usuario finalizó al final del mes en el que se desactivó su acceso.
- Eliminado significa que el usuario del SSO estaba previamente asignado al dominio, pero se eliminó antes de que accediera.

5. Para añadir usuarios de SSO, selecciona Añadir y Añadir usuarios. Esta opción no está disponible si el dominio está configurado con una asignación de usuarios implícita, lo que significa que todos los usuarios del grupo de identidades tienen acceso al DataZone dominio de Amazon.

   - En la página Añadir usuarios, busca los alias de los usuarios que quieres añadir. Aparecerá una lista debajo del cuadro de búsqueda con posibles coincidencias.
   - Elige el usuario que quieres añadir. Su alias aparecerá como un chip debajo del cuadro de búsqueda.
   - Cuando estés satisfecho con la lista de usuarios que quieres añadir, selecciona Añadir usuario (s).
   - Los usuarios se asignan al DataZone dominio de Amazon con el estado Asignado.
   - Cuando el usuario acceda por primera vez al portal de datos del dominio, el estado cambiará automáticamente a Activado y se empezará a facturar la suscripción del usuario.

6. Para eliminar un usuario de SSO asignado, selecciónalo y selecciona Desactivar en el menú de acciones. Como resultado, el usuario perderá el acceso al DataZone dominio de Amazon. El estado del usuario aparecerá como Eliminado. Esta opción no está disponible si el dominio está configurado con una asignación de usuarios implícita.
7. Para desactivar un usuario de SSO activado, selecciónelo y elija Desactivar en el menú de acciones. Como resultado, el acceso del usuario al DataZone dominio de Amazon se perderá y se bloqueará. La facturación de la suscripción del usuario continuará hasta fin de mes. El estado del usuario aparecerá como Desactivado.
8. Para activar un usuario de SSO desactivado, selecciónelo y elija Activar en el menú Acciones. Como resultado, el usuario recuperará el acceso al DataZone dominio de Amazon. La facturación comenzará inmediatamente. El del usuario aparecerá como Activado.

Administra los grupos de SSO

Los grupos de SSO se crean o sincronizan con su proveedor de identidades en el Centro de identidades de AWS IAM. Para obtener más información, consulte Configuración del centro de identidad de AWS IAM para Amazon DataZone y Habilitar el Centro de Identidad de IAM para Amazon DataZone para habilitar y configurar AWS IAM Identity Center para Amazon DataZone. Puede ver la lista de grupos de SSO asignados al dominio, añadir grupos de SSO y eliminar grupos de SSO.

1. Inicie sesión en la consola AWS de administración y abra la DataZone consola en https://console.aws.amazon.com/datazone.
2. Seleccione Ver dominios y elija el nombre del dominio de la lista. El nombre es un hipervínculo.
3. En la página de detalles del dominio, desplázate hacia abajo y selecciona Administración de usuarios.
4. Para el tipo de usuario, selecciona Grupos de SSO para ver la lista actual de grupos de SSO.
   - La columna Nombre muestra el nombre del grupo de SSO.
   - La columna Estado muestra el estado actual del grupo de SSO en el dominio.
     - Asignado significa que el grupo de SSO se ha asignado explícitamente al dominio. Como resultado, todos los usuarios del grupo tienen acceso al portal de datos del dominio (a menos que el usuario esté desactivado).
     - No asignado significa que el grupo de SSO se ha eliminado del dominio. Los usuarios del grupo no tienen acceso al portal de datos del dominio al pertenecer a este grupo.
5. Para añadir grupos de SSO, seleccione Añadir y Añadir grupos. Esta opción no está disponible si el dominio está configurado con una asignación de usuarios implícita, lo que significa que todos los usuarios del grupo de identidades tienen acceso al DataZone dominio de Amazon, independientemente de si pertenecen al grupo.
   - En la página Añadir grupos, busque los alias de los grupos que desee añadir. Aparecerá una lista debajo del cuadro de búsqueda con posibles coincidencias.
   - Elige el grupo que quieres añadir. Su alias aparecerá como un chip debajo del cuadro de búsqueda.
   - Cuando esté satisfecho con la lista de grupos que desea añadir, seleccione Añadir grupo (s).
   - Los grupos se asignan al DataZone dominio de Amazon con el estado Asignado.

- Cuando un miembro del grupo acceda al portal de datos del dominio, el estado cambiará automáticamente a Activado y se te empezará a facturar la suscripción del usuario.

6. Para eliminar un grupo de SSO asignado, selecciónalo y elige Cancelar asignación en el menú Acciones. Como resultado, el grupo perderá el acceso al DataZone dominio de Amazon. El estado del grupo aparecerá como No asignado. Los usuarios que hayan accedido a Amazon a DataZone través de su pertenencia a este grupo perderán el acceso. Esta opción no está disponible si el dominio está configurado para una asignación de usuarios implícita. Para dejar de facturar a los usuarios a los que se les quita el acceso al anular la asignación de su grupo, tendrá que seleccionar y desactivar manualmente sus perfiles de usuario.

Administrar los permisos de los usuarios en el portal DataZone de datos de Amazon

En la versión actual de Amazon DataZone, el mecanismo de autorización predeterminado permite a todos los usuarios autenticados (IAM y SSO) de los DataZone dominios de Amazon crear proyectos, crear entidades dentro de los proyectos y realizar búsquedas. Los miembros del proyecto deben seguir respetando los permisos que se les han otorgado según las funciones que hayan designado como propietarios o colaboradores del proyecto.

Trabajar con los planos DataZone integrados de Amazon

Un plano con el que se crea un entorno define qué herramientas y servicios pueden utilizar los miembros del proyecto al que pertenece el entorno cuando trabajan con los activos del DataZone catálogo de Amazon. En la versión actual de Amazon DataZone, hay los siguientes planos integrados:

- Plano de lago de datos
- Plano de almacén de datos
- SageMaker Plano de Amazon

Temas

Habilita los blueprints integrados en la AWS cuenta propietaria del dominio de Amazon DataZone

Un plano con el que se crea un entorno define qué herramientas y servicios pueden utilizar los miembros del proyecto al que pertenece el entorno cuando trabajan con los activos del DataZone catálogo de Amazon.

En la versión actual de Amazon DataZone, hay varios planos integrados: el plano del lago de datos, el plano del almacén de datos y el plano de Amazon. SageMaker

- El plano del lago de datos contiene la definición para lanzar y configurar un conjunto de servicios (AWS Glue, AWS Lake Formation, Amazon Athena) para publicar y utilizar los activos del lago de datos en el catálogo de Amazon DataZone .
- El plano de almacén de datos contiene la definición para lanzar y configurar un conjunto de servicios (Amazon Redshift) para publicar y utilizar los activos de Amazon Redshift en el catálogo de Amazon. DataZone
- El SageMaker blueprint de Amazon contiene la definición para lanzar y configurar un conjunto de servicios (Amazon SageMaker Studio) para publicar y utilizar SageMaker los activos de Amazon en el DataZone catálogo de Amazon.

Para obtener más información, consulte DataZone Terminología y conceptos de Amazon.

Al crear un DataZone dominio de Amazon, tiene la opción de elegir la configuración rápida, que habilita automáticamente el lago de datos predeterminado y los planos integrados del almacén de datos predeterminado como parte del proceso de creación del dominio. La configuración rápida también crea perfiles de entorno predeterminados y entornos predeterminados para usted mediante estos esquemas integrados.

Si no eliges la configuración rápida como parte de la creación de tu DataZone dominio de Amazon, puedes usar el siguiente procedimiento para habilitar los blueprints integrados disponibles en la AWS cuenta que aloja este DataZone dominio de Amazon. Debe habilitar estos esquemas integrados antes de poder usarlos para crear perfiles de entorno y entornos en este dominio.

Para habilitar los blueprints integrados en un DataZone dominio de Amazon a través de la consola DataZone de administración de Amazon, debes asumir una función de IAM en la cuenta con permisos administrativos. Configure los permisos de IAM necesarios para usar la consola de DataZone administración de Amazonpara obtener los permisos mínimos.

Habilita los blueprints integrados en un dominio de Amazon DataZone

1. Ve a la DataZone consola de Amazon en https://console.aws.amazon.com/datazone e inicia sesión con las credenciales de tu cuenta.
2. Selecciona Ver dominios y elige el dominio en el que quieres habilitar uno o más blueprints integrados.
3. En la página de detalles del dominio, vaya a la pestaña Blueprints.
4. En la lista de planos, selecciona el plano DefaultDataLakeo DefaultDataWarehouseel SageMaker plano de Amazon.
5. En la página de detalles del plano elegido, selecciona Activar en esta cuenta.
6. En la página de permisos y recursos, especifique lo siguiente:

    - Si estás habilitando el DefaultDataLakeblueprint, para la función Glue Manage Access, especifica una función de servicio nueva o existente que DataZone autorice a Amazon a ingerir y gestionar el acceso a las tablas de AWS Glue and AWS Lake Formation.
    - Si está habilitando el DefaultDataWarehouseblueprint, para la función Administrar acceso de Redshift, especifique una función de servicio nueva o existente que autorice a DataZone Amazon a ingerir y administrar el acceso a datos compartidos, tablas y vistas en Amazon Redshift.

- Si está habilitando el SageMaker blueprint de Amazon, en la función SageMaker Administrar acceso, especifique una función de servicio nueva o existente que conceda DataZone permisos a Amazon para publicar SageMaker datos de Amazon en el catálogo. También otorga DataZone permisos a Amazon para conceder o revocar el acceso a los activos SageMaker publicados por Amazon en el catálogo.

  > **Important**
  >
  > Al activar el SageMaker blueprint de Amazon, Amazon DataZone comprueba si las siguientes funciones de IAM para Amazon DataZone existen en la cuenta corriente y la región. Si estos roles no existen, Amazon los crea DataZone automáticamente.
  >
  > - AmazonDataZoneGlueAccess- <region>- <domainId>
  > - AmazonDataZoneRedshiftAccess- <region>- <domainId>

- En la función de aprovisionamiento, especifique una función de servicio nueva o existente que DataZone autorice a Amazon a crear y configurar los recursos del entorno utilizando AWS CloudFormation la cuenta y la región del entorno.
- Si está habilitando el SageMaker blueprint de Amazon, para el bucket de Amazon S3 para la fuente de datos SageMaker -Glue, especifique un bucket de Amazon S3 que vayan a utilizar todos los SageMaker entornos de la AWS cuenta. El prefijo de bucket que especifique debe ser uno de los siguientes:
  - amazon-datazone*
  - datazone-sagemaker*
  - sagemaker-datazone*
  - DataZone-Sagemaker*
  - Sagemaker- * DataZone
  - DataZone-SageMaker*
  - SageMaker-DataZone*

7. Seleccione Activar blueprint.

Una vez que haya activado los planos elegidos, podrá controlar qué proyectos pueden utilizarlos en su cuenta para crear perfiles de entorno. Para ello, puede asignar la gestión de proyectos a la configuración del blueprint.

Especifique la gestión de proyectos en los blueprints habilitados

1. Ve a la DataZone consola de Amazon en https://console.aws.amazon.com/datazone e inicia sesión con las credenciales de tu cuenta.
2. Selecciona Ver dominios y, a continuación, elige el dominio en el que quieres añadir los proyectos de gestión para los planos elegidos.
3. Selecciona la pestaña Planos y, a continuación, elige el plano con el que quieres trabajar.
4. De forma predeterminada, todos los proyectos del dominio pueden usar los DefaultDataLake SageMaker blueprints o o Amazon de la cuenta para crear perfiles de entorno. DefaultDataWareshouse Sin embargo, puede restringirlo asignando la gestión de proyectos a los blueprints. Para añadir proyectos de gestión, elija Seleccionar proyecto de gestión y, a continuación, elija los proyectos que desee añadir como proyectos de gestión en el menú desplegable y, a continuación, seleccione Seleccionar proyectos de gestión.

Una vez que habilites el DefaultDataWarehouse blueprint en tu AWS cuenta, podrás añadir conjuntos de parámetros a la configuración del blueprint. Un conjunto de parámetros es un grupo de claves y valores necesarios para que Amazon DataZone establezca una conexión con el clúster de Amazon Redshift y que se utiliza para crear entornos de almacenamiento de datos. Estos parámetros incluyen el nombre del clúster de Amazon Redshift, la base de datos y el AWS secreto que contiene las credenciales del clúster.

Añadir conjuntos de parámetros al blueprint DefaultDataWarehouse

1. Ve a la DataZone consola de Amazon en https://console.aws.amazon.com/datazone e inicia sesión con las credenciales de tu cuenta.
2. Selecciona Ver dominios y, a continuación, elige el dominio en el que quieres añadir el conjunto de parámetros.
3. Seleccione la pestaña Planos y, a continuación, elija el DefaultDataWareshouse esquema para abrir la página de detalles del esquema.
4. En la pestaña Conjuntos de parámetros de la página de detalles del plano, elija Crear conjunto de parámetros.
   - Proporcione un nombre para el conjunto de parámetros.
   - Si lo desea, proporcione una descripción del conjunto de parámetros.
   - Seleccione una región
   - Seleccione un clúster de Amazon Redshift o Amazon Redshift Serverless.

- Seleccione el ARN AWS secreto que contiene las credenciales del clúster de Amazon Redshift seleccionado o del grupo de trabajo Amazon Redshift Serverless. El AWS secreto debe estar etiquetado con la `AmazonDataZoneDomain : [Domain_ID]` etiqueta para que pueda usarse dentro de un conjunto de parámetros.
  - Si no tienes un AWS secreto existente, también puedes crear uno nuevo seleccionando Crear nuevo AWS secreto. Esto abre un cuadro de diálogo en el que puede proporcionar el nombre del secreto, el nombre de usuario y la contraseña. Cuando eliges Create New AWS Secret, Amazon DataZone crea un nuevo secreto en el servicio AWS Secrets Manager y se asegura de que el secreto esté etiquetado con el dominio en el que intentas crear el conjunto de parámetros.
- Si eligió un clúster de Amazon Redshift en el paso anterior, ahora elija un clúster del menú desplegable. Si eligió el grupo de trabajo Amazon Redshift en el paso anterior, ahora elija un grupo de trabajo del menú desplegable.
- Introduzca el nombre de la base de datos del clúster de Amazon Redshift o del grupo de trabajo Amazon Redshift Serverless seleccionado.
- Elija Crear conjunto de parámetros.

Una vez que habilites el SageMaker blueprint de Amazon en tu AWS cuenta, podrás añadir conjuntos de parámetros a la configuración del blueprint. Un conjunto de parámetros es un grupo de claves y valores necesarios para DataZone que Amazon establezca una conexión con tu Amazon SageMaker y que se utiliza para crear entornos de SageMaker.

Añadir conjuntos de parámetros al SageMaker blueprint de Amazon

1. Ve a la DataZone consola de Amazon en https://console.aws.amazon.com/datazone e inicia sesión con las credenciales de tu cuenta.
2. Selecciona Ver dominios y, a continuación, elige el dominio que contiene el blueprint activado al que quieres añadir el conjunto de parámetros.
3. Selecciona la pestaña Blueprints y, a continuación, elige el SageMaker blueprint de Amazon para abrir la página de detalles del blueprint.
4. En la pestaña Conjuntos de parámetros de la página de detalles del blueprint, selecciona Crear conjunto de parámetros y, a continuación, especifica lo siguiente:
   - Proporcione un nombre para el conjunto de parámetros.
   - Si lo desea, proporcione una descripción del conjunto de parámetros.

- Especifica el tipo de autenticación SageMaker del dominio de Amazon. Puede elegir entre IAM o IAM Identity Center (SSO).
- Especifique una región. AWS
- Especifique una clave AWS KMS para el cifrado de datos. Puede elegir una clave existente o crear una nueva clave.
- En Parámetros del entorno, especifique lo siguiente:
  - ID de VPC: el ID que utilizas para la VPC del entorno de Amazon. SageMaker Puede especificar una VPC existente o crear una nueva.
  - Subredes: uno o más ID para un rango de direcciones IP para recursos específicos dentro de su VPC.
  - Acceso a la red: elija solo VPC o solo Internet público.
  - Grupo de seguridad: el grupo de seguridad que se debe usar al configurar la VPC y las subredes.
- En Parámetros de la fuente de datos, elija una de las siguientes opciones:
  - AWS Glue únicamente
  - AWS Glue + Amazon Redshift Serverless. Si elige esta opción, especifique lo siguiente:
    - Especifique el AWS ARN secreto que contiene las credenciales del clúster de Amazon Redshift seleccionado. El AWS secreto debe estar etiquetado con la `AmazonDataZoneDomain : [Domain_ID]` etiqueta para que pueda usarse dentro de un conjunto de parámetros.

      Si no tienes un AWS secreto existente, también puedes crear uno nuevo seleccionando Crear nuevo AWS secreto. Esto abre un cuadro de diálogo en el que puede proporcionar el nombre del secreto, el nombre de usuario y la contraseña. Cuando eliges Create New AWS Secret, Amazon DataZone crea un nuevo secreto en el servicio AWS Secrets Manager y se asegura de que el secreto esté etiquetado con el dominio en el que intentas crear el conjunto de parámetros.
    - Especifique el grupo de trabajo de Amazon Redshift que desee utilizar al crear entornos.
    - Especifique el nombre de la base de datos (dentro del grupo de trabajo que ha elegido) que desea usar al crear entornos.
  - AWS Solo Glue + Amazon Redshift Cluster
    - Especifique el AWS ARN secreto que contiene las credenciales del clúster de Amazon Redshift seleccionado. El AWS secreto debe estar etiquetado con la

`AmazonDataZoneDomain : [Domain_ID]` etiqueta para que pueda usarse dentro de un conjunto de parámetros.

Si no tienes un AWS secreto existente, también puedes crear uno nuevo seleccionando Crear nuevo AWS secreto. Esto abre un cuadro de diálogo en el que puede proporcionar el nombre del secreto, el nombre de usuario y la contraseña. Cuando eliges Create New AWS Secret, Amazon DataZone crea un nuevo secreto en el servicio AWS Secrets Manager y se asegura de que el secreto esté etiquetado con el dominio en el que intentas crear el conjunto de parámetros.

- Especifique el clúster de Amazon Redshift que desee utilizar al crear entornos.
- Especifique el nombre de la base de datos (dentro del clúster que ha elegido) que desea usar al crear entornos.

5. Elija Crear conjunto de parámetros.

Añade Amazon SageMaker como servicio de confianza en la AWS cuenta propietaria del DataZone dominio de Amazon

Si has activado el SageMaker blueprint de Amazon, también debes añadirlo SageMaker como uno de los servicios de confianza de Amazon DataZone. Para ello, complete el siguiente procedimiento:

1. Ve a la DataZone consola de Amazon en https://console.aws.amazon.com/datazone e inicia sesión con las credenciales de tu cuenta.
2. Selecciona Ver dominios y, a continuación, elige el dominio que contiene el SageMaker blueprint activado.
3. Elige los servicios de confianza, Amazon y SageMaker, por último, Activar.

Trabajar con cuentas asociadas para publicar y consumir datos

Al asociar tus AWS cuentas a tu DataZone dominio de Amazon, los usuarios del dominio pueden publicar y consumir datos de estas AWS cuentas. Hay tres pasos para configurar una asociación de cuentas.

- En primer lugar, comparte el dominio con la AWS cuenta deseada solicitando la asociación. Amazon DataZone usa AWS Resource Access Manager (RAM) si la AWS cuenta es diferente de la AWS cuenta del dominio. Solo el DataZone dominio de Amazon puede iniciar una asociación de cuentas.
- En segundo lugar, haz que el propietario de la cuenta acepte la solicitud de asociación.
- En tercer lugar, pida al propietario de la cuenta que habilite los planos de entorno deseados. Al habilitar un blueprint, el propietario de la cuenta proporciona a los usuarios del dominio las funciones de IAM y las configuraciones de recursos necesarias para crear y acceder a los recursos de su cuenta, como las bases de datos de AWS Glue y los clústeres de Amazon Redshift.

Temas

Solicite la asociación con otras cuentas AWS

> **Note**
>
> Al enviar una solicitud de asociación a otra AWS cuenta, compartes tu dominio con la otra AWS cuenta con AWS Resource Access Manager (RAM). Asegúrese de comprobar la precisión del identificador de cuenta que ha introducido.

Para solicitar la asociación con otras AWS cuentas de la DataZone consola de Amazon para un DataZone dominio de Amazon, debes asumir una función de IAM en la cuenta con permisos administrativos. Configure los permisos de IAM necesarios para usar la consola de DataZone administración de Amazonpara obtener los permisos mínimos necesarios para solicitar la asociación de una cuenta.

Complete el siguiente procedimiento para solicitar la asociación con otras AWS cuentas.

1. Inicie sesión en la consola AWS de administración y abra la consola DataZone de administración de Amazon en https://console.aws.amazon.com/datazone.
2. Selecciona Ver dominios y elige el nombre del dominio de la lista. El nombre es un hipervínculo.
3. Desplázate hacia abajo hasta la pestaña Cuentas asociadas y selecciona Solicitar asociación.
4. Introduce los ID de las cuentas que deseas solicitar la asociación. Cuando esté satisfecho con la lista de identificadores de cuentas, elija Solicitar asociación.
5. Amazon DataZone crea un recurso compartido en AWS Resource Access Manager en nombre de tu cuenta, con los ID de cuenta introducidos como principales.
6. Debe notificar al propietario de las otras AWS cuentas para que acepte su solicitud. Las invitaciones vencen después de siete (7) días.

Proporcione acceso a la cuenta a su clave KMS administrada por el cliente

Los DataZone dominios de Amazon y sus metadatos se cifran (de forma predeterminada) mediante una clave mantenida por AWS u (opcionalmente) una clave gestionada por el cliente del Servicio de gestión de AWS claves (KMS) que usted posea y que proporcione durante la creación del dominio. Si tu dominio está cifrado con una clave gestionada por el cliente, sigue el procedimiento que se indica a continuación para conceder permiso a la cuenta asociada para usar la clave KMS.

1. Inicie sesión en la consola AWS de administración y abra la consola KMS en https://console.aws.amazon.com/kms/.
2. Si desea ver las claves de la cuenta que usted crea y administra, en el panel de navegación, elija Customer managed keys (Claves administradas por el cliente).
3. Si desea ver las claves de la cuenta que usted crea y administra, en el panel de navegación, elija Customer managed keys (Claves administradas por el cliente).
4. En la lista de claves KMS, elija el alias o ID de clave de la clave KMS que desea examinar.
5. Para permitir o impedir que AWS las cuentas externas usen la clave KMS, utilice los controles de la sección Otras AWS cuentas de la página. Los directores de IAM de estas cuentas (con

los permisos de KMS adecuados) pueden usar la clave de KMS en operaciones criptográficas, como cifrar, descifrar, volver a cifrar y generar claves de datos.

Acepte una solicitud de asociación de cuentas de un DataZone dominio de Amazon y active un plan de entorno

Para aceptar la asociación en la consola DataZone de administración de Amazon con un DataZone dominio de Amazon, debes asumir una función de IAM en la cuenta con permisos administrativos. Configure los permisos de IAM necesarios para usar la consola de DataZone administración de Amazonpara obtener los permisos mínimos.

Completa lo siguiente para aceptar la asociación con un DataZone dominio de Amazon.

1. Inicie sesión en la consola AWS de administración y abra la consola DataZone de administración de Amazon en https://console.aws.amazon.com/datazone.
2. Selecciona Ver solicitudes y selecciona el dominio de la lista. Debe solicitarse el estado de la invitación. Selecciona Revisar solicitud.
3. Elija si desea habilitar los esquemas predeterminados del entorno del lago de datos o del entorno de almacén de datos; para ello, no seleccione ninguna de las casillas, o ambas. Puede hacerlo más adelante.

   - El plan del entorno del lago de datos permite a los usuarios del dominio crear y administrar recursos de AWS Glue, Amazon S3 y Amazon Athena para publicarlos y consumirlos desde un lago de datos.
   - El esquema del entorno de almacén de datos permite a los usuarios del dominio crear y administrar recursos de Amazon Redshift para publicarlos y consumirlos desde un almacén de datos.
4. Si elige seleccionar uno o ambos esquemas de entorno predeterminados, configure los siguientes permisos y recursos.

   - La función Gestionar el acceso (IAM) proporciona permisos a Amazon DataZone para permitir a los usuarios del dominio ingerir y gestionar el acceso a las tablas, como AWS Glue y Amazon Redshift. Puede elegir que Amazon DataZone cree y utilice un nuevo rol de IAM, o puede elegir uno de los roles de IAM existentes.
   - La función IAM de aprovisionamiento proporciona permisos DataZone a Amazon para que los usuarios del dominio puedan crear y configurar recursos del entorno, como las bases de datos

de AWS Glue. Puede elegir que Amazon DataZone cree y utilice un nuevo rol de IAM, o puede elegir uno de los roles de IAM existentes.

- El depósito de Amazon S3 para Data Lake es el depósito o la ruta que DataZone utilizará Amazon cuando los usuarios del dominio almacenen datos de data lake. Puedes usar el bucket predeterminado seleccionado por Amazon DataZone o elegir tu propia ruta de Amazon S3 existente introduciendo su cadena de ruta. Si seleccionas tu propia ruta de Amazon S3, tendrás que actualizar las políticas de IAM para conceder a Amazon DataZone los permisos necesarios para usarla.

5. Cuando esté satisfecho con sus configuraciones, elija Aceptar y configurar la asociación.

Rechazar una solicitud de asociación de cuentas de un DataZone dominio de Amazon

Para rechazar una solicitud de asociación en la consola de DataZone administración de Amazon desde un DataZone dominio de Amazon, debes asumir una función de IAM en la cuenta con permisos administrativos. Configure los permisos de IAM necesarios para usar la consola de DataZone administración de Amazonpara obtener los permisos mínimos.

Completa lo siguiente para rechazar una solicitud de asociación de un DataZone dominio de Amazon.

1. Inicie sesión en la consola AWS de administración y abra la consola DataZone de administración de Amazon en https://console.aws.amazon.com/datazone.
2. Selecciona Ver solicitudes y selecciona el dominio de la lista. Debe solicitarse el estado de la invitación. Elija Rechazar asociación. Confirme su elección seleccionando Rechazar asociación.

Habilite un esquema de entorno en una cuenta asociada AWS

Para habilitar un blueprint de entorno en la consola DataZone de administración de Amazon, debe asumir una función de IAM en la cuenta con permisos administrativos. Configure los permisos de IAM necesarios para usar la consola de DataZone administración de Amazonpara obtener los permisos mínimos.

Complete lo siguiente para habilitar un blueprint en un dominio asociado.

1. Inicie sesión en la consola AWS de administración y abra la consola DataZone de administración de Amazon en https://console.aws.amazon.com/datazone.
2. Abre el panel de navegación izquierdo y selecciona Dominios asociados.
3. Elija el dominio para el que quiere habilitar un esquema de entorno.
4. En la lista de planos, selecciona el plano DefaultDataLakeo DefaultDataWarehouseel SageMaker plano de Amazon.
5. En la página de detalles del plano elegido, selecciona Activar en esta cuenta.
6. En la página de permisos y recursos, especifique lo siguiente:

   - Si estás habilitando el DefaultDataLakeblueprint, para la función Glue Manage Access, especifica una función de servicio nueva o existente que DataZone autorice a Amazon a ingerir y gestionar el acceso a las tablas de AWS Glue and AWS Lake Formation.
   - Si está habilitando el DefaultDataWarehouseblueprint, para la función Administrar acceso de Redshift, especifique una función de servicio nueva o existente que autorice a DataZone Amazon a ingerir y administrar el acceso a datos compartidos, tablas y vistas en Amazon Redshift.
   - Si está habilitando el SageMaker blueprint de Amazon, en la función SageMaker Administrar acceso, especifique una función de servicio nueva o existente que conceda DataZone permisos a Amazon para publicar SageMaker datos de Amazon en el catálogo. También otorga DataZone permisos a Amazon para conceder o revocar el acceso a los activos SageMaker publicados por Amazon en el catálogo.

     > **Important**
     >
     > Al activar el SageMaker blueprint de Amazon, Amazon DataZone comprueba si las siguientes funciones de IAM para Amazon DataZone existen en la cuenta corriente y la región. Si estos roles no existen, Amazon los crea DataZone automáticamente.
     >
     > - AmazonDataZoneGlueAccess- <region>- <domainId>
     > - AmazonDataZoneRedshiftAccess- <region>- <domainId>

   - En la función de aprovisionamiento, especifique una función de servicio nueva o existente que DataZone autorice a Amazon a crear y configurar los recursos del entorno utilizando AWS CloudFormation la cuenta y la región del entorno.
   - Si está habilitando el SageMaker blueprint de Amazon, para el bucket de Amazon S3 para la fuente de datos SageMaker -Glue, especifique un bucket de Amazon S3 que vayan a utilizar

todos los SageMaker entornos de la AWS cuenta. El prefijo de bucket que especifique debe ser uno de los siguientes:

- amazon-datazone*
- datazone-sagemaker*
- sagemaker-datazone*
- DataZone-Sagemaker*
- Sagemaker- * DataZone
- DataZone-SageMaker*
- SageMaker-DataZone*

7. Seleccione Activar blueprint.

Una vez que haya activado los planos elegidos, podrá controlar qué proyectos pueden utilizarlos en su cuenta para crear perfiles de entorno. Para ello, puede asignar la gestión de proyectos a la configuración del blueprint.

Especifique la gestión de proyectos en modo activado DefaultDataLake o blueprint DefaultDataWarehouse

1. Ve a la DataZone consola de Amazon en https://console.aws.amazon.com/datazone e inicia sesión con las credenciales de tu cuenta.
2. Abre el panel de navegación izquierdo y selecciona Dominios asociados y, a continuación, elige el dominio al que quieres añadir proyectos de gestión.
3. Seleccione la pestaña Planos y, a continuación, elija un DefaultDataLake DefaultDataWareshouse plano.
4. De forma predeterminada, todos los proyectos del dominio pueden usar el DefaultDataWareshouse plano DefaultDataLake o plano de la cuenta para crear perfiles de entorno. Sin embargo, puede restringirlo asignando los proyectos de gestión al blueprint. Para añadir proyectos de gestión, elija Seleccionar proyecto de gestión y, a continuación, elija los proyectos que desee añadir como proyectos de gestión en el menú desplegable y, a continuación, seleccione Seleccionar proyectos de gestión.

Una vez que habilites el DefaultDataWarehouse blueprint en tu AWS cuenta, podrás añadir conjuntos de parámetros a la configuración del blueprint. Un conjunto de parámetros es un grupo de claves y valores necesarios para que Amazon DataZone establezca una conexión con el clúster de Amazon

Redshift y que se utiliza para crear entornos de almacenamiento de datos. Estos parámetros incluyen el nombre del clúster de Amazon Redshift, la base de datos y el AWS secreto que contiene las credenciales del clúster.

Añadir conjuntos de parámetros al blueprint DefaultDataWarehouse

1. Ve a la DataZone consola de Amazon en https://console.aws.amazon.com/datazone e inicia sesión con las credenciales de tu cuenta.
2. Abre el panel de navegación izquierdo y selecciona Dominios asociados y, a continuación, elige el dominio al que quieres añadir los conjuntos de parámetros.
3. Seleccione la pestaña Planos y, a continuación, elija el DefaultDataWareshouse esquema para abrir la página de detalles del esquema.
4. En la pestaña Conjuntos de parámetros de la página de detalles del plano, elija Crear conjunto de parámetros.
   - Proporcione un nombre para el conjunto de parámetros.
   - Si lo desea, proporcione una descripción del conjunto de parámetros.
   - Seleccione una región
   - Seleccione un clúster de Amazon Redshift o Amazon Redshift Serverless.
   - Seleccione el ARN AWS secreto que contiene las credenciales del clúster de Amazon Redshift seleccionado o del grupo de trabajo Amazon Redshift Serverless. El AWS secreto debe estar etiquetado con la `AmazonDataZoneDomain : [Domain_ID]` etiqueta para que pueda usarse dentro de un conjunto de parámetros.
     - Si no tienes un AWS secreto existente, también puedes crear uno nuevo seleccionando Crear nuevo AWS secreto. Esto abre un cuadro de diálogo en el que puede proporcionar el nombre del secreto, el nombre de usuario y la contraseña. Cuando eliges Create New AWS Secret, Amazon DataZone crea un nuevo secreto en el servicio AWS Secrets Manager y se asegura de que el secreto esté etiquetado con el dominio en el que intentas crear el conjunto de parámetros.
   - Seleccione un clúster de Amazon Redshift o un grupo de trabajo Amazon Redshift Serverless.
   - Introduzca el nombre de la base de datos del clúster de Amazon Redshift o del grupo de trabajo Amazon Redshift Serverless seleccionado.
   - Elija Crear conjunto de parámetros.

Una vez que habilites el SageMaker blueprint de Amazon en tu AWS cuenta, podrás añadir conjuntos de parámetros a la configuración del blueprint. Un conjunto de parámetros es un grupo de claves y valores necesarios para DataZone que Amazon establezca una conexión con tu Amazon SageMaker y que se utiliza para crear entornos de SageMaker.

Añadir conjuntos de parámetros al SageMaker blueprint de Amazon

1. Ve a la DataZone consola de Amazon en https://console.aws.amazon.com/datazone e inicia sesión con las credenciales de tu cuenta.
2. Selecciona Ver dominios y, a continuación, elige el dominio que contiene el blueprint activado al que quieres añadir el conjunto de parámetros.
3. Selecciona la pestaña Blueprints y, a continuación, elige el SageMaker blueprint de Amazon para abrir la página de detalles del blueprint.
4. En la pestaña Conjuntos de parámetros de la página de detalles del plano, selecciona Crear conjunto de parámetros y, a continuación, especifica lo siguiente:
   - Proporcione un nombre para el conjunto de parámetros.
   - Si lo desea, proporcione una descripción del conjunto de parámetros.
   - Especifique el tipo de autenticación SageMaker del dominio de Amazon. Puede elegir entre IAM o IAM Identity Center (SSO).
   - Especifique una región. AWS
   - Especifique una clave AWS KMS para el cifrado de datos. Puede elegir una clave existente o crear una nueva clave.
   - En Parámetros del entorno, especifique lo siguiente:
     - ID de VPC: el ID que utilizas para la VPC del entorno de Amazon. SageMaker Puede especificar una VPC existente o crear una nueva.
     - Subredes: uno o más ID para un rango de direcciones IP para recursos específicos dentro de su VPC.
     - Acceso a la red: elija solo VPC o solo Internet público.
     - Grupo de seguridad: el grupo de seguridad que se debe usar al configurar la VPC y las subredes.
   - En Parámetros de la fuente de datos, elija una de las siguientes opciones:
     - AWS Glue únicamente
     - AWS Glue + Amazon Redshift Serverless. Si elige esta opción, especifique lo siguiente:

- Especifique el AWS ARN secreto que contiene las credenciales del clúster de Amazon Redshift seleccionado. El AWS secreto debe estar etiquetado con la `AmazonDataZoneDomain : [Domain_ID]` etiqueta para que pueda usarse dentro de un conjunto de parámetros.

  Si no tienes un AWS secreto existente, también puedes crear uno nuevo seleccionando Crear nuevo AWS secreto. Esto abre un cuadro de diálogo en el que puede proporcionar el nombre del secreto, el nombre de usuario y la contraseña. Cuando eliges Create New AWS Secret, Amazon DataZone crea un nuevo secreto en el servicio AWS Secrets Manager y se asegura de que el secreto esté etiquetado con el dominio en el que intentas crear el conjunto de parámetros.
- Especifique el grupo de trabajo de Amazon Redshift que desee utilizar al crear entornos.
- Especifique el nombre de la base de datos (dentro del grupo de trabajo que ha elegido) que desea usar al crear entornos.

- AWS Solo Glue + Amazon Redshift Cluster
  - Especifique el AWS ARN secreto que contiene las credenciales del clúster de Amazon Redshift seleccionado. El AWS secreto debe estar etiquetado con la `AmazonDataZoneDomain : [Domain_ID]` etiqueta para que pueda usarse dentro de un conjunto de parámetros.

    Si no tienes un AWS secreto existente, también puedes crear uno nuevo seleccionando Crear nuevo AWS secreto. Esto abre un cuadro de diálogo en el que puede proporcionar el nombre del secreto, el nombre de usuario y la contraseña. Cuando eliges Create New AWS Secret, Amazon DataZone crea un nuevo secreto en el servicio AWS Secrets Manager y se asegura de que el secreto esté etiquetado con el dominio en el que intentas crear el conjunto de parámetros.
  - Especifique el clúster de Amazon Redshift que desee utilizar al crear entornos.
  - Especifique el nombre de la base de datos (dentro del clúster que ha elegido) que desea usar al crear entornos.

5. Elija Crear conjunto de parámetros.

Añade Amazon SageMaker como servicio de confianza en la AWS cuenta asociada

Si has activado el SageMaker blueprint de Amazon, también debes añadirlo SageMaker como uno de los servicios de confianza de Amazon DataZone. Para ello, complete el siguiente procedimiento:

1. Ve a la DataZone consola de Amazon en https://console.aws.amazon.com/datazone e inicia sesión con las credenciales de tu cuenta.
2. Selecciona Ver dominios y, a continuación, elige el dominio que contiene el SageMaker blueprint activado.
3. Elige los servicios de confianza, Amazon y SageMaker, por último, Activar.

Eliminar una cuenta asociada

Para eliminar una AWS cuenta asociada en la consola DataZone de administración de Amazon, debes asumir una función de IAM en la cuenta con permisos administrativos. Configure los permisos de IAM necesarios para usar la consola de DataZone administración de Amazonpara obtener los permisos mínimos.

Complete el siguiente procedimiento para eliminar una cuenta asociada de su dominio.

1. Inicie sesión en la consola AWS de administración y abra la consola DataZone de administración de Amazon en https://console.aws.amazon.com/datazone.
2. Selecciona Ver dominios y elige el nombre del dominio de la lista. El nombre es un hipervínculo.
3. Desplázate hacia abajo hasta la pestaña Cuentas asociadas. Elige el ID de cuenta de la AWS cuenta que deseas eliminar.
4. Elija Desasociar. Confirma tu elección introduciendo disociar en el campo y seleccionando Desasociar.
5. La cuenta ahora se ha eliminado de tu dominio y los usuarios del dominio no pueden utilizarla para publicar y consumir datos.

Trabajar con el catálogo de DataZone datos de Amazon

Puedes usar el catálogo de datos DataZone empresariales de Amazon para catalogar los datos de toda tu organización con el contexto empresarial y permitir así que todos los miembros de tu organización encuentren y entiendan los datos rápidamente. Para obtener más información, consulte DataZone Terminología y conceptos de Amazon.

Temas

Crea, edita o elimina un glosario empresarial

En Amazon DataZone, un glosario empresarial es un conjunto de términos empresariales (palabras) que pueden estar asociados a activos (datos). Proporciona los vocabularios adecuados con una lista de términos empresariales y sus definiciones para que los usuarios empresariales puedan utilizar las mismas definiciones en toda la organización a la hora de analizar los datos. Los glosarios empresariales se crean en el dominio del catálogo y se pueden aplicar a los activos y columnas para ayudar a comprender las características clave de esos activos o columnas. Se pueden aplicar uno o más términos del glosario. Un glosario empresarial puede ser una lista plana de términos en la que cualquier término del glosario empresarial puede asociarse a una sublista de otros términos. Para obtener más información, consulte DataZone Terminología y conceptos de Amazon. Para crear, editar o eliminar un glosario en tu DataZone dominio de Amazon, debes ser miembro del proyecto propietario y tener los permisos adecuados para ese dominio.

Para crear un glosario, sigue estos pasos:

1. Navegue al portal de DataZone datos de Amazon mediante la URL del portal de datos e inicie sesión con su SSO o sus AWS credenciales. Si eres DataZone administrador de Amazon, puedes obtener la URL del portal de datos accediendo a la DataZone consola de Amazon en https://console.aws.amazon.com/datazone en la AWS cuenta en la que se creó el DataZone dominio de Amazon.
2. Navega hasta el menú Catálogo en la barra de navegación superior, junto a Buscar.

3. En el Amazon DataZone Data Portal, selecciona Glosarios y, a continuación, selecciona Crear glosario.
4. Especifique un nombre, una descripción y un propietario para el glosario y, a continuación, elija Crear glosario.
5. Activa el nuevo glosario pulsando la opción Activado.
6. En la página de detalles del glosario, puede seleccionar Crear un archivo readme para añadir información adicional sobre este glosario.

Para activar o desactivar un glosario empresarial, sigue estos pasos:

1. Navegue al portal de DataZone datos de Amazon mediante la URL del portal de datos e inicie sesión con su SSO o sus AWS credenciales. Si eres DataZone administrador de Amazon, puedes obtener la URL del portal de datos accediendo a la DataZone consola de Amazon en https://console.aws.amazon.com/datazone en la AWS cuenta en la que se creó el DataZone dominio de Amazon.
2. Navega hasta el menú Catálogo en la barra de navegación superior, junto a Buscar.
3. En el Amazon DataZone Data Portal, selecciona Glosarios y localiza el glosario empresarial que deseas activar o desactivar.
4. En la página de detalles del glosario, localice la opción Activar/Desactivar y utilícela para activar o desactivar el glosario seleccionado.

> **Note**
>
> Al deshabilitar un glosario, también se deshabilitan todos los términos que contiene.

Para editar un glosario empresarial, siga estos pasos:

1. Navegue al portal de DataZone datos de Amazon mediante la URL del portal de datos e inicie sesión con su SSO o sus AWS credenciales. Si eres DataZone administrador de Amazon, puedes obtener la URL del portal de datos accediendo a la DataZone consola de Amazon en https://console.aws.amazon.com/datazone en la AWS cuenta en la que se creó el DataZone dominio de Amazon.
2. Navega hasta el menú Catálogo en la barra de navegación superior, junto a Buscar.
3. En el Amazon DataZone Data Portal, selecciona Glosarios y localiza el glosario empresarial que deseas editar.

4. En la página de detalles del glosario, expanda Acciones y, a continuación, elija Editar para editar el glosario.
5. Actualice el nombre y la descripción y, a continuación, seleccione Guardar.

Para eliminar un glosario empresarial, sigue estos pasos:

1. Navegue al portal de DataZone datos de Amazon mediante la URL del portal de datos e inicie sesión con su SSO o sus AWS credenciales. Si eres DataZone administrador de Amazon, puedes obtener la URL del portal de datos accediendo a la DataZone consola de Amazon en https://console.aws.amazon.com/datazone en la AWS cuenta en la que se creó el DataZone dominio de Amazon.
2. Navega hasta el menú Catálogo en la barra de navegación superior, junto a Buscar.
3. En el Amazon DataZone Data Portal, selecciona Glosarios y localiza el glosario empresarial que deseas eliminar.
4. En la página de detalles del glosario, expanda Acciones y, a continuación, elija Eliminar para eliminar el glosario.

> **Note**
>
> Debe eliminar todos los términos existentes en el glosario para poder eliminarlo.

5. Confirme la eliminación del glosario seleccionando Eliminar.

Cree, edite o elimine un término de un glosario

En Amazon DataZone, un glosario empresarial es un conjunto de términos empresariales que pueden estar asociados a activos (datos). Para obtener más información, consulte DataZone Terminología y conceptos de Amazon. Para crear, editar o eliminar términos de un glosario en tu DataZone dominio de Amazon, debes ser miembro del proyecto propietario con los permisos adecuados para ese dominio.

En Amazon DataZone, los términos del glosario empresarial pueden tener descripciones detalladas. Para establecer el contexto de un término concreto, puedes especificar las relaciones entre los términos. Al definir una relación para un término, se añade automáticamente a la definición del término relacionado. Los términos relaciones del glosario disponibles en Amazon DataZone incluyen lo siguiente:

- Es un tipo de: indica que el término actual es un tipo del término identificado. Indica que el término identificado es el padre del término actual.
- Tiene tipos: indica que el término actual es un término genérico para el término o los términos específicos indicados. Esta relación puede denotar términos secundarios del término genérico.

Para crear un término nuevo, complete los siguientes pasos:

1. Navegue al portal de DataZone datos de Amazon mediante la URL del portal de datos e inicie sesión con su SSO o sus AWS credenciales. Si eres DataZone administrador de Amazon, puedes obtener la URL del portal de datos accediendo a la DataZone consola de Amazon en https://console.aws.amazon.com/datazone en la AWS cuenta en la que se creó el DataZone dominio de Amazon.
2. Navega hasta el menú Catálogo en la barra de navegación superior, junto a Buscar.
3. En el Amazon DataZone Data Portal, elija Glosarios y, a continuación, elija el glosario en el que desee crear el nuevo término.
4. Especifique un nombre, una descripción y un propietario para el término y, a continuación, elija Crear término.
5. Activa el nuevo término pulsando el botón Activado.
6. Para añadir Léame, vaya a la página de detalles del término y, a continuación, seleccione Crear archivo readme para añadir información adicional sobre este glosario.
7. Para añadir relaciones, vaya a la página de detalles del término, seleccione la sección Relaciones temporales y, a continuación, seleccione Añadir términos al glosario. En el cuadro de diálogo, elija la relación y los términos que desee relacionar y, a continuación, elija Cerrar para añadir un término al tipo de relación correspondiente. Esta relación también se añade a todos los términos que haya relacionado.

Para editar un término de un glosario, siga estos pasos:

1. Navegue al portal de DataZone datos de Amazon mediante la URL del portal de datos e inicie sesión con su SSO o sus AWS credenciales. Si eres DataZone administrador de Amazon, puedes obtener la URL del portal de datos accediendo a la DataZone consola de Amazon en https://console.aws.amazon.com/datazone en la AWS cuenta en la que se creó el DataZone dominio de Amazon.
2. Navega hasta el menú Catálogo en la barra de navegación superior, junto a Buscar.

3. En el Amazon DataZone Data Portal, elija Glosarios, localice el glosario que contiene el término que quiere editar y, a continuación, selecciónelo.
4. En la página de detalles del término, expanda Acciones y, a continuación, seleccione Editar para editar el término.
5. Actualice el nombre y la descripción y, a continuación, seleccione Guardar.

Para eliminar un término de un glosario, siga estos pasos:

1. Navegue al portal de DataZone datos de Amazon mediante la URL del portal de datos e inicie sesión con su SSO o sus AWS credenciales. Si eres DataZone administrador de Amazon, puedes obtener la URL del portal de datos accediendo a la DataZone consola de Amazon en https://console.aws.amazon.com/datazone en la AWS cuenta en la que se creó el DataZone dominio de Amazon.
2. Navega hasta el menú Catálogo en la barra de navegación superior, junto a Buscar.
3. En el Amazon DataZone Data Portal, selecciona Glosarios, localiza el glosario que contiene el término que deseas eliminar y, a continuación, selecciónalo.
4. En la página de detalles del glosario, expanda Acciones y, a continuación, seleccione Eliminar para eliminar el término.
5. Confirme la eliminación del término seleccionando Eliminar.

Cree, edite o elimine formularios de metadatos

En Amazon DataZone, los formularios de metadatos son formularios sencillos para añadir un contexto empresarial adicional a los metadatos de los activos del catálogo. Sirve como un mecanismo ampliable para que los propietarios de los datos enriquezcan el activo con información que pueda ayudar a los usuarios a buscar y encontrar esos datos. Los formularios de metadatos también pueden servir como mecanismo para garantizar la coherencia de todos los activos que se publican en el DataZone catálogo de Amazon.

La definición de un formulario de metadatos se compone de una o más definiciones de campo y admite los tipos de datos booleanos, de fecha, decimales, enteros, de cadena y de valores de campo del glosario empresarial. Para obtener más información, consulte DataZone Terminología y conceptos de Amazon. Para crear, editar o eliminar formularios de metadatos en tu DataZone dominio de Amazon, debes ser miembro del proyecto propietario y tener las credenciales adecuadas.

Para crear un formulario de metadatos, sigue estos pasos:

1. Navegue al portal de DataZone datos de Amazon mediante la URL del portal de datos e inicie sesión con su SSO o sus AWS credenciales. Si eres DataZone administrador de Amazon, puedes obtener la URL del portal de datos accediendo a la DataZone consola de Amazon en https://console.aws.amazon.com/datazone en la AWS cuenta en la que se creó el DataZone dominio de Amazon.
2. Navega hasta el menú Catálogo en la barra de navegación superior, junto a Buscar.
3. En el Amazon DataZone Data Portal, selecciona Formularios de metadatos y, a continuación, selecciona Crear formulario.
4. Especifique el nombre, la descripción y el propietario del formulario de metadatos y, a continuación, seleccione Crear formulario.

Para editar un formulario de metadatos, complete los siguientes pasos:

1. Navegue al portal de DataZone datos de Amazon mediante la URL del portal de datos e inicie sesión con su SSO o sus AWS credenciales. Si eres DataZone administrador de Amazon, puedes obtener la URL del portal de datos accediendo a la DataZone consola de Amazon en https://console.aws.amazon.com/datazone en la AWS cuenta en la que se creó el DataZone dominio de Amazon.
2. Navega hasta el menú Catálogo en la barra de navegación superior, junto a Buscar.
3. En el Amazon DataZone Data Portal, elija Formularios de metadatos y, a continuación, localice el formulario de metadatos que desee editar.
4. En la página de detalles del formulario de metadatos, expanda Acciones y, a continuación, seleccione Editar.
5. Actualice los campos de nombre, descripción y propietario y, a continuación, seleccione Actualizar formulario.

Para eliminar un formulario de metadatos, siga estos pasos:

> **Note**
>
> Antes de poder eliminar un formulario de metadatos, debe eliminarlo de todos los tipos de activos o activos a los que se aplique.

1. Navegue al portal de DataZone datos de Amazon mediante la URL del portal de datos e inicie sesión con su SSO o sus AWS credenciales. Si eres DataZone administrador de Amazon, puedes obtener la URL del portal de datos accediendo a la DataZone consola de Amazon en https://console.aws.amazon.com/datazone en la AWS cuenta en la que se creó el DataZone dominio de Amazon.
2. Navega hasta el menú Catálogo en la barra de navegación superior, junto a Buscar.
3. En el Amazon DataZone Data Portal, elija Formularios de metadatos y, a continuación, localice el formulario de metadatos que desee eliminar.
4. Si el formulario de metadatos que desea eliminar está activado, desactívelo pulsando la opción Activado.
5. En la página de detalles del formulario de metadatos, expanda Acciones y, a continuación, elija Eliminar.
6. Confirme la eliminación seleccionando Eliminar.

Cree, edite o elimine campos en los formularios de metadatos

En Amazon DataZone, los formularios de metadatos son formularios sencillos para añadir un contexto empresarial adicional a los metadatos de los activos del catálogo. Sirve como un mecanismo ampliable para que los propietarios de los datos enriquezcan el activo con información que pueda ayudar a los usuarios a buscar y encontrar esos datos. Los formularios de metadatos también pueden servir como mecanismo para garantizar la coherencia de todos los activos que se publican en el DataZone catálogo de Amazon.

La definición de un formulario de metadatos se compone de una o más definiciones de campo y admite los tipos de datos booleanos, de fecha, decimales, enteros, de cadena y de valores de campo del glosario empresarial. Para obtener más información, consulte DataZone Terminología y conceptos de Amazon. Para crear, editar o eliminar campos en los formularios de metadatos de tu DataZone dominio de Amazon, debes ser miembro del proyecto propietario y tener las credenciales correctas.

Para crear un campo en un formulario de metadatos, sigue estos pasos:

1. Navegue al portal de DataZone datos de Amazon mediante la URL del portal de datos e inicie sesión con su SSO o sus AWS credenciales. Si eres DataZone administrador de Amazon, puedes obtener la URL del portal de datos accediendo a la DataZone consola de Amazon en

https://console.aws.amazon.com/datazone en la AWS cuenta en la que se creó el DataZone dominio de Amazon.

2. Navega hasta el menú Catálogo en la barra de navegación superior, junto a Buscar.
3. En el Amazon DataZone Data Portal, elija Formularios de metadatos y, a continuación, elija el formulario de metadatos en el que desee crear los campos.
4. En la página de detalles del formulario, selecciona Crear campo.
5. Especifique el nombre, la descripción y el tipo del campo y si se trata de un campo obligatorio y, a continuación, elija Crear campo.

Para editar un campo en un formulario de metadatos, siga estos pasos:

1. Navegue al portal de DataZone datos de Amazon mediante la URL del portal de datos e inicie sesión con su SSO o sus AWS credenciales. Si eres DataZone administrador de Amazon, puedes obtener la URL del portal de datos accediendo a la DataZone consola de Amazon en https://console.aws.amazon.com/datazone en la AWS cuenta en la que se creó el DataZone dominio de Amazon.
2. Navega hasta el menú Catálogo en la barra de navegación superior, junto a Buscar.
3. En el Amazon DataZone Data Portal, elija Formularios de metadatos y, a continuación, elija el formulario de metadatos en el que desee editar los campos.
4. En la página de detalles del formulario, elija el campo que desee editar, expanda Acciones y elija Editar.
5. Actualice el nombre, la descripción y el tipo del campo y si se trata de un campo obligatorio y, a continuación, seleccione Actualizar campo.

Para eliminar un campo de un formulario de metadatos, siga estos pasos:

1. Navegue al portal de DataZone datos de Amazon mediante la URL del portal de datos e inicie sesión con su SSO o sus AWS credenciales. Si eres DataZone administrador de Amazon, puedes obtener la URL del portal de datos accediendo a la DataZone consola de Amazon en https://console.aws.amazon.com/datazone en la AWS cuenta en la que se creó el DataZone dominio de Amazon.
2. Navega hasta el menú Catálogo en la barra de navegación superior, junto a Buscar.
3. En el Amazon DataZone Data Portal, elija Formularios de metadatos y, a continuación, elija el formulario de metadatos en el que desee eliminar los campos.

4. En la página de detalles del formulario, elija el campo que desee eliminar, expanda Acciones y elija Eliminar.
5. Confirme la eliminación seleccionando Eliminar.

Trabajar con proyectos y entornos en Amazon DataZone

En Amazon DataZone, los proyectos permiten a un grupo de usuarios colaborar en varios casos de uso empresarial que implican publicar, descubrir, suscribirse y consumir activos de datos del DataZone catálogo de Amazon. A cada DataZone proyecto de Amazon se le aplica un conjunto de controles de acceso para que solo las personas, grupos y roles autorizados puedan acceder al proyecto y a los activos de datos a los que está suscrito este proyecto, y pueden usar solo las herramientas definidas por los permisos del proyecto. Los proyectos actúan como un principal de identidad que recibe concesiones de acceso a los recursos subyacentes, lo que permite DataZone a Amazon operar dentro de la infraestructura de una organización sin depender de las credenciales de los usuarios individuales. Para obtener más información, consulte DataZone Terminología y conceptos de Amazon.

Temas

Cree un perfil de entorno

En Amazon DataZone, un perfil de entorno es una plantilla que se puede utilizar para crear entornos. El objetivo de un perfil de entorno es simplificar la creación de entornos mediante la incorporación de información de ubicación, como la AWS cuenta y la región, en los perfiles. Para obtener más información, consulte DataZone Terminología y conceptos de Amazon. Para crear perfiles de

entorno en un DataZone dominio de Amazon, debes pertenecer a un DataZone proyecto de Amazon. Todos los perfiles de entorno son propiedad de los proyectos y todos los usuarios autorizados, de cualquier proyecto, pueden utilizarlos para crear nuevos entornos.

Para crear un perfil de entorno

1. Navegue al portal de DataZone datos de Amazon mediante la URL del portal de datos e inicie sesión con su SSO o sus AWS credenciales. Si eres DataZone administrador de Amazon, puedes obtener la URL del portal de datos accediendo a la DataZone consola de Amazon en https://console.aws.amazon.com/datazone en la AWS cuenta en la que se creó el DataZone dominio de Amazon.
2. En el portal de datos, elija Examinar proyectos y seleccione el proyecto en el que desee crear el perfil de entorno.
3. Vaya a la pestaña Entornos del proyecto y, a continuación, elija Crear perfil de entorno.
4. Configure los siguientes campos:

   - Nombre: el nombre de su perfil de entorno.
   - Descripción: (opcional) una descripción del perfil de su entorno.
   - Proyecto propietario: el proyecto en el que se está creando el perfil se selecciona de forma predeterminada en este campo.
   - Plano: el esquema para el que se crea este perfil. Puedes elegir uno de los DataZone planos predeterminados de Amazon (Data Lake o Data Warehouse).

     Si especificó el plano del almacén de datos, haga lo siguiente:

     - Proporcione un conjunto de parámetros. Para seleccionar un conjunto de parámetros existente, elija la opción Elegir un conjunto de parámetros. Si desea introducir sus propios parámetros, elija Introducir los míos.
     - Si decide seleccionar un parámetro existente, haga lo siguiente:
       - Seleccione una AWS cuenta en el menú desplegable.
       - Seleccione un conjunto de parámetros del menú desplegable.
     - Si decide introducir sus propios parámetros, haga lo siguiente:
       - Proporcione los AWS parámetros seleccionando la AWS cuenta y la región en el menú desplegable.
       - Proporcione los parámetros de Redshift Data Warehouse:
         - Seleccione un clúster de Amazon Redshift o Amazon Redshift Serverless

- Introduzca el ARN AWS secreto que contiene las credenciales del clúster de Amazon Redshift o del grupo de trabajo Amazon Redshift Serverless seleccionado. El AWS secreto debe estar etiquetado con el ID de dominio y el ID del proyecto en el que va a crear el perfil de entorno.
  - `AmazonDataZoneDomain: [Domain_ID]`
  - `AmazonDataZoneProject: [Project_ID]`
- Introduzca el nombre del clúster de Amazon Redshift o del grupo de trabajo Amazon Redshift Serverless.
- Introduzca el nombre de la base de datos del clúster de Amazon Redshift o del grupo de trabajo Amazon Redshift Serverless seleccionado.

- En la sección Proyectos autorizados, especifique los proyectos que pueden usar el perfil de entorno para crear entornos. De forma predeterminada, todos los proyectos del dominio pueden usar los perfiles de entorno de la cuenta para crear entornos. Para mantener esta configuración predeterminada, selecciona Todos los proyectos. Sin embargo, puede restringirlo asignando proyectos autorizados al entorno. Para ello, seleccione Solo proyectos autorizados y, a continuación, especifique los proyectos que pueden utilizar este perfil de proyecto para crear entornos.
- En la sección Publicación, elija una de las siguientes opciones:
  - Publicar desde cualquier esquema: si elige esta opción, los entornos creados con este perfil de entorno se pueden usar para publicar desde cualquier esquema de la base de datos seleccionada en los parámetros de Redshift proporcionados anteriormente. Los usuarios del entorno creado con estos perfiles de entorno también pueden proporcionar sus propios parámetros de Amazon Redshift para publicarlos desde cualquier esquema de la AWS cuenta y la región seleccionadas en el perfil del entorno.
  - Publicar solo desde el esquema de entorno predeterminado: si elige esta opción, los entornos creados con ella se pueden usar para publicar solo desde el esquema predeterminado creado por Amazon DataZone para ese entorno. Los usuarios del entorno creado con los perfiles de este entorno no pueden proporcionar sus propios parámetros de Amazon Redshift.
  - No permita la publicación: si elige esta opción, los entornos creados con este perfil de entorno solo se pueden usar para la suscripción y el consumo de datos. Los entornos no se pueden utilizar para publicar ningún dato en absoluto.

Si especificó el esquema de Data Lake, haga lo siguiente:

- En la sección de parámetros de la AWS cuenta, especifique el número de AWS cuenta y la región de la AWS cuenta en la que se crearán los posibles entornos.
- En la sección Proyectos autorizados, especifique los proyectos que pueden usar el perfil de entorno con el perfil de entorno de Data Lake integrado para crear entornos. De forma predeterminada, todos los proyectos del dominio pueden usar el esquema del lago de datos de la cuenta para crear perfiles de entorno. Para mantener esta configuración predeterminada, selecciona Todos los proyectos. Sin embargo, puede restringirlo asignando proyectos al blueprint. Para ello, seleccione Solo proyectos autorizados y, a continuación, especifique los proyectos que pueden utilizar este perfil de proyecto para crear entornos.
- En la sección Bases de datos, elija Cualquier base de datos para permitir la publicación desde cualquier base de datos de la AWS cuenta y la región en la que se creó el entorno o elija Solo la base de datos predeterminada para permitir la publicación únicamente desde la base de datos de publicación predeterminada que se crea con el entorno.

5. Seleccione Crear perfil de entorno.

Edite un perfil de entorno

En Amazon DataZone, un perfil de entorno es una plantilla que se puede utilizar para crear entornos. Para obtener más información, consulte DataZone Terminología y conceptos de Amazon. Para editar los perfiles de un entorno existente en un DataZone dominio de Amazon, debe pertenecer a un DataZone proyecto de Amazon.

Para editar un perfil de entorno

1. Ve a la URL del portal de DataZone datos de Amazon e inicia sesión con el inicio de sesión único (SSO) o con tus credenciales. AWS Si eres DataZone administrador de Amazon, puedes ir a la DataZone consola de Amazon en https://console.aws.amazon.com/datazone e iniciar sesión con el Cuenta de AWS lugar donde se creó el dominio y, a continuación, elegir Open data portal.
2. En el portal de datos, selecciona Explorar proyectos y selecciona el proyecto en el que quieres editar el perfil del entorno.
3. Vaya a la pestaña Entornos del proyecto, elija Perfiles de entorno y, a continuación, elija el perfil de entorno que desee editar.

   Si está editando un perfil de entorno de almacén de datos, solo puede editar el nombre y la descripción de un perfil de entorno existente.

Si está editando un perfil de entorno de Data Lake, puede editar el nombre y la descripción del perfil y también puede editar los proyectos que están autorizados a usar este perfil para crear entornos y puede editar bases de datos. Para editar estos ajustes, haga lo siguiente:

- En la sección Proyectos autorizados, especifique los proyectos que pueden usar el perfil de entorno con el perfil de entorno de Data Lake integrado para crear entornos. De forma predeterminada, todos los proyectos del dominio pueden usar el esquema del lago de datos de la cuenta para crear perfiles de entorno. Para mantener esta configuración predeterminada, selecciona Todos los proyectos. Sin embargo, puede restringirlo asignando proyectos al blueprint. Para ello, seleccione Solo proyectos autorizados y, a continuación, especifique los proyectos que pueden utilizar este perfil de proyecto para crear entornos.
- En la sección Bases de datos, elija Cualquier base de datos para permitir la publicación desde cualquier base de datos de la AWS cuenta y la región en la que se creó el entorno o elija Solo la base de datos predeterminada para permitir la publicación únicamente desde la base de datos de publicación predeterminada que se crea con el entorno.

Cuando complete las modificaciones, elija Editar perfil de entorno.

Elimine un perfil de entorno

En Amazon DataZone, un perfil de entorno es una plantilla que se puede utilizar para crear entornos. El objetivo de un perfil de entorno es simplificar la creación de entornos mediante la incorporación de información de ubicación, como la AWS cuenta y la región, en los perfiles. Para obtener más información, consulte DataZone Terminología y conceptos de Amazon. Para eliminar perfiles de entorno en un DataZone dominio de Amazon, debe pertenecer a un DataZone proyecto de Amazon.

> **Note**
>
> Al eliminar un perfil de entorno, no podrá crear más entornos con este perfil.

Para eliminar un perfil de entorno

1. Ve a la URL del portal de DataZone datos de Amazon e inicia sesión con el inicio de sesión único (SSO) o con tus credenciales. AWS Si eres DataZone administrador de Amazon, puedes ir

a la DataZone consola de Amazon en https://console.aws.amazon.com/datazone e iniciar sesión con el Cuenta de AWS lugar donde se creó el dominio y, a continuación, elegir Open data portal.

2. En el portal de datos, selecciona Explorar proyectos y selecciona el proyecto en el que quieres eliminar el perfil del entorno.
3. Vaya a la pestaña Entornos del proyecto, elija Perfiles de entorno y, a continuación, elija el perfil de entorno que desee eliminar.
4. Seleccione el perfil de entorno que desee eliminar y, a continuación, elija Acciones, Eliminar y confirme la eliminación.

Creación de un nuevo entorno

En los DataZone proyectos de Amazon, los entornos son conjuntos de recursos configurados (por ejemplo, un bucket de Amazon S3, una base de datos de AWS Glue o un grupo de trabajo de Amazon Athena), con un conjunto determinado de principios de IAM (roles de usuario del entorno) con permisos de propietario o colaborador asignados que pueden operar con esos recursos. Para obtener más información, consulte DataZone Terminología y conceptos de Amazon.

Cualquier DataZone usuario de Amazon con los permisos necesarios para acceder al portal de datos puede crear un DataZone entorno de Amazon dentro de un proyecto.

Para crear un entorno nuevo, complete los siguientes pasos.

1. Ve a la URL del portal de DataZone datos de Amazon e inicia sesión con el inicio de sesión único (SSO) o con tus credenciales. AWS Si eres DataZone administrador de Amazon, puedes ir a la DataZone consola de Amazon en https://console.aws.amazon.com/datazone e iniciar sesión con el Cuenta de AWS lugar donde se creó el dominio y, a continuación, elegir Open data portal.
2. Selecciona Explorar todos los proyectos y selecciona el proyecto en el que quieres crear un nuevo entorno.
3. Elija Crear entorno, especifique los valores para los siguientes campos y, a continuación, elija Crear entorno:

   - Nombre: el nombre del entorno
   - Descripción: descripción del entorno
   - Perfil de entorno: elija un perfil de entorno existente o cree uno nuevo. Un perfil de entorno es una plantilla que se puede utilizar para crear entornos. Para obtener más información, consulte DataZone Terminología y conceptos de Amazon.

Una vez que haya seleccionado el perfil de entorno, en la sección Parámetros, especifique los valores de los campos que forman parte de este perfil de entorno.

Edite un entorno

En DataZone los proyectos de Amazon, los entornos son conjuntos de recursos configurados (por ejemplo, un bucket de Amazon S3, una base de datos de AWS Glue o un grupo de trabajo de Amazon Athena), con un conjunto determinado de directores de IAM (con permisos de colaborador asignados) que pueden operar con esos recursos. Para obtener más información, consulte DataZone Terminología y conceptos de Amazon.

Cualquier DataZone usuario de Amazon con los permisos necesarios para acceder al portal de datos puede editar un DataZone entorno de Amazon dentro de un proyecto.

Para editar un entorno existente, complete los siguientes pasos.

1. Ve a la URL del portal de DataZone datos de Amazon e inicia sesión con el inicio de sesión único (SSO) o con tus credenciales. AWS Si eres DataZone administrador de Amazon, puedes ir a la DataZone consola de Amazon en https://console.aws.amazon.com/datazone e iniciar sesión con el Cuenta de AWS lugar donde se creó el dominio y, a continuación, elegir Open data portal.
2. Selecciona Buscar proyectos en el panel de navegación superior y selecciona el proyecto que contiene el entorno que deseas editar.
3. Localice el entorno y selecciónelo para abrir su página de detalles. A continuación, expanda Acciones y elija Editar entorno.
4. Modifique el nombre y la descripción del entorno y, a continuación, seleccione Guardar cambios.

Eliminación de un entorno

En DataZone los proyectos de Amazon, los entornos son conjuntos de recursos configurados (por ejemplo, un bucket de Amazon S3, una base de datos de AWS Glue o un grupo de trabajo de Amazon Athena), con un conjunto determinado de directores de IAM (con permisos de colaborador asignados) que pueden operar con esos recursos. Para obtener más información, consulte DataZone Terminología y conceptos de Amazon.

Cualquier DataZone usuario de Amazon con los permisos necesarios para acceder al portal de datos puede eliminar un DataZone entorno de Amazon dentro de un proyecto.

Para eliminar un entorno existente, complete los siguientes pasos.

1. Ve a la URL del portal de DataZone datos de Amazon e inicia sesión con el inicio de sesión único (SSO) o con tus credenciales. AWS Si eres DataZone administrador de Amazon, puedes ir a la DataZone consola de Amazon en https://console.aws.amazon.com/datazone e iniciar sesión con el Cuenta de AWS lugar donde se creó el dominio y, a continuación, elegir Open data portal.
2. Selecciona Buscar proyecto en el panel de navegación superior y selecciona el proyecto que contiene el entorno que deseas eliminar.
3. Busque y elija el entorno para abrir su página de detalles, luego expanda Acciones y elija Eliminar entorno.
4. En la ventana emergente Eliminar entorno, confirme la eliminación escribiendo `Delete` en el campo y, a continuación, seleccione Eliminar entorno.

   Puede eliminar correctamente un entorno solo después de que se hayan eliminado todas las entidades que dependen de este entorno. Para eliminar un entorno, primero debe eliminar todas sus fuentes de datos y destinos de suscripción asociados.

Crear un nuevo proyecto de

En Amazon DataZone, los proyectos permiten a un grupo de usuarios colaborar en varios casos de uso empresarial que implican publicar, descubrir, suscribirse y consumir activos de datos del DataZone catálogo de Amazon. Para obtener más información, consulte DataZone Terminología y conceptos de Amazon.

Cualquier DataZone usuario de Amazon con los permisos necesarios para acceder al portal de datos puede crear un DataZone proyecto de Amazon.

Para crear un nuevo proyecto, complete los siguientes pasos.

1. Ve a la URL del portal de DataZone datos de Amazon e inicia sesión con el inicio de sesión único (SSO) o con tus credenciales. AWS Si eres DataZone administrador de Amazon, puedes ir a la DataZone consola de Amazon en https://console.aws.amazon.com/datazone e iniciar sesión con el Cuenta de AWS lugar donde se creó el dominio y, a continuación, elegir Open data portal.
2. En el portal de DataZone datos de Amazon, selecciona Create Project.
3. Especifique los valores para los siguientes campos y, a continuación, elija Crear proyecto:

   - Nombre: el nombre del proyecto.

- Descripción: descripción del proyecto.

Editar proyecto

En Amazon DataZone, los proyectos permiten a un grupo de usuarios colaborar en varios casos de uso empresarial que implican publicar, descubrir, suscribirse y consumir activos de datos del DataZone catálogo de Amazon. Para obtener más información, consulte DataZone Terminología y conceptos de Amazon. Para editar un DataZone proyecto de Amazon, debes ser el propietario de ese proyecto o el administrador del dominio que contiene este proyecto.

Para editar un proyecto existente, sigue estos pasos.

1. Ve a la URL del portal de DataZone datos de Amazon e inicia sesión con el inicio de sesión único (SSO) o con tus credenciales. AWS Si eres DataZone administrador de Amazon, puedes ir a la DataZone consola de Amazon en https://console.aws.amazon.com/datazone e iniciar sesión con el Cuenta de AWS lugar donde se creó el dominio y, a continuación, elegir Open data portal.
2. Selecciona Buscar proyectos.
3. Elige el proyecto que deseas editar. Si no lo ve fácilmente en la lista de proyectos, puede buscarlo especificando el nombre del proyecto en el campo Buscar proyecto.
4. Expanda Acciones y elija Editar proyecto.
5. Actualice el nombre y la descripción del proyecto y, a continuación, seleccione Guardar.

Eliminar proyecto

En Amazon DataZone, los proyectos permiten a un grupo de usuarios colaborar en varios casos de uso empresarial que implican publicar, descubrir, suscribirse o consumir activos de datos del DataZone catálogo de Amazon. Para obtener más información, consulte DataZone Terminología y conceptos de Amazon.

El acto de eliminar un proyecto es definitivo. La eliminación elimina de forma irrevocable el contenido del proyecto, incluidas las fuentes de datos, los entornos, los activos, los glosarios y los formularios de metadatos. Amazon DataZone revoca las subvenciones que Amazon DataZone ha otorgado a los activos gestionados a través de Lake Formation y Amazon Redshift. Al eliminar un proyecto, no se eliminan DataZone AWS los recursos ajenos a Amazon que Amazon te DataZone haya ayudado a crear. Si ya no necesitas estos AWS recursos, elimínalos en sus respectivos AWS servicios y cuentas.

Para eliminar un DataZone proyecto de Amazon, debes ser el propietario del proyecto.

Para eliminar un proyecto existente, sigue estos pasos.

1. Ve a la URL del portal de DataZone datos de Amazon e inicia sesión con el inicio de sesión único (SSO) o con tus credenciales. AWS Un director de IAM puede ir a la DataZone consola de Amazon en https://console.aws.amazon.com/datazone e iniciar sesión con el Cuenta de AWS lugar donde se creó el dominio y, a continuación, elegir Open data portal.
2. Selecciona Explorar proyectos en el panel de navegación superior.
3. Elija el proyecto que desee eliminar. Si no lo ve en la lista de proyectos, puede buscarlo especificando el nombre del proyecto en el campo Buscar proyecto.
4. Expanda Acciones y elija Eliminar proyecto.

   Revisa las advertencias informativas sobre el posible impacto de eliminar el proyecto.
5. Si aceptas las advertencias, escribe el texto de confirmación y selecciona Eliminar.

> **Important**
>
> Eliminar un proyecto es una acción irrevocable que no puedes deshacer ni tú ni tú. AWS

> **Note**
>
> Cuando tú o los usuarios de tu dominio creáis un entorno en un proyecto, Amazon DataZone crea AWS recursos en vuestro dominio o en las cuentas asociadas para proporcionaros funcionalidad a vosotros y a los usuarios de vuestro dominio. A continuación se muestra la lista de AWS recursos que Amazon DataZone puede crear para un proyecto, junto con el nombre predeterminado. Al eliminar un proyecto, no se elimina ninguno de estos AWS recursos de tus AWS cuentas.
>
> - <environmentId>Funciones de IAM: datazone_usr_.
> - <environmentName>Bases de datos Glue: (1) <environmentName>_pub_db-*, (2) _sub_db-*. Si ya existía una base de datos con este nombre, Amazon DataZone añadirá el ID del entorno.
> - <environmentName>Grupos de trabajo de Athena: -*. Si ya existía un grupo de trabajo con este nombre, Amazon DataZone añadirá el ID del entorno.

- CloudWatch grupo de registro: datazone_ <environmentId>

Salir del proyecto

En Amazon DataZone, los proyectos permiten a un grupo de usuarios colaborar en varios casos de uso empresarial que implican publicar, descubrir, suscribirse y consumir activos de datos del DataZone catálogo de Amazon. Para obtener más información, consulte DataZone Terminología y conceptos de Amazon.

Para dejar un proyecto existente, sigue estos pasos.

1. Ve a la URL del portal de DataZone datos de Amazon e inicia sesión con el inicio de sesión único (SSO) o con tus credenciales. AWS Si eres DataZone administrador de Amazon, puedes ir a la DataZone consola de Amazon en https://console.aws.amazon.com/datazone e iniciar sesión con el Cuenta de AWS lugar donde se creó el dominio y, a continuación, elegir Open data portal.
2. Selecciona Seleccionar proyecto en el panel de navegación superior y selecciona el proyecto.
3. Elija el proyecto del que quiere salir. Si no lo ve fácilmente en la lista de proyectos, puede buscarlo especificando el nombre del proyecto en el campo Buscar proyecto.
4. Expanda Acciones y elija Salir del proyecto.

Agrega miembros a un proyecto

En Amazon DataZone, los proyectos permiten a un grupo de usuarios colaborar en varios casos de uso empresarial que implican publicar, descubrir, suscribirse y consumir activos de datos del DataZone catálogo de Amazon. Para obtener más información, consulte DataZone Terminología y conceptos de Amazon.

Debes ser propietario o colaborador de un proyecto para añadir miembros a un proyecto. Puede añadir grupos de SSO, usuarios de SSO o directores de IAM (roles o usuarios) como miembros del proyecto.

Para añadir miembros a un proyecto existente, sigue estos pasos.

1. Ve a la URL del portal de DataZone datos de Amazon e inicia sesión con el inicio de sesión único (SSO) o con tus credenciales. AWS Si eres DataZone administrador de Amazon, puedes ir

a la DataZone consola de Amazon en https://console.aws.amazon.com/datazone e iniciar sesión con el Cuenta de AWS lugar donde se creó el dominio y, a continuación, elegir Open data portal.

2. Selecciona Seleccionar proyecto en el panel de navegación superior y selecciona el proyecto.
3. Elija el proyecto al que desee añadir miembros. Si no lo ve fácilmente en la lista de proyectos, puede buscarlo especificando el nombre del proyecto en el campo Buscar proyecto.
4. En la página de detalles del proyecto, seleccione la pestaña Miembros y el nodo Elija todos los miembros.
5. En la pestaña Miembros del proyecto, selecciona Añadir miembros.
6. En la ventana emergente Añadir miembros al proyecto, especifique los usuarios que desee añadir y especifique su función en el proyecto (propietario o colaborador) y, a continuación, seleccione Añadir miembros.

> **Note**
>
> Puedes añadir un director de IAM como miembro del proyecto si ese director ya tiene un perfil de DataZone usuario de Amazon en el dominio. Amazon crea DataZone automáticamente un perfil de usuario para un principal de IAM cuando interactúa correctamente con el dominio a través del portal, la API o la CLI. No puede crear un perfil de usuario para un principal de IAM. Para añadir a los directores de IAM como miembros del proyecto en el caso de que el principal de IAM no tenga un perfil de DataZone usuario de Amazon existente en el dominio, pídale a su administrador que añada los dos permisos de IAM siguientes a los de su dominio AmazonDataZoneDomainExecutionRoleen la consola de IAM: y. `iam:GetUser` `iam:GetRole` Por separado, para realizar acciones en el dominio, el titular de IAM debe tener los permisos de IAM correspondientes a dichas acciones.

Eliminar miembros de un proyecto

En Amazon DataZone, los proyectos permiten a un grupo de usuarios colaborar en varios casos de uso empresarial que implican publicar, descubrir, suscribirse y consumir activos de datos del DataZone catálogo de Amazon. Para obtener más información, consulte DataZone Terminología y conceptos de Amazon. Debes ser el propietario de un proyecto para poder eliminar miembros de un proyecto.

Para eliminar miembros de un proyecto que ya está en marcha, sigue estos pasos.

1. Navegue al portal de DataZone datos de Amazon mediante la URL del portal de datos e inicie sesión con su SSO o sus AWS credenciales. Si eres DataZone administrador de Amazon, puedes obtener la URL del portal de datos accediendo a la DataZone consola de Amazon en https://console.aws.amazon.com/datazone en la AWS cuenta en la que se creó el DataZone dominio de Amazon.
2. Selecciona Seleccionar proyecto en el panel de navegación superior y selecciona el proyecto.
3. Elija el proyecto del que desee eliminar miembros. Si no lo ve fácilmente en la lista de proyectos, puede buscarlo especificando el nombre del proyecto en el campo Buscar proyecto.
4. En la página de detalles del proyecto, seleccione la pestaña Miembros y el nodo Elija todos los miembros.
5. En la pestaña Miembros del proyecto, elija los miembros que desee eliminar del proyecto y, a continuación, elija Eliminar.
6. En la ventana emergente Eliminar miembros, confirma la eliminación seleccionando Eliminar miembros.

Creación de inventario y publicación de datos en Amazon DataZone

En esta sección se describen las tareas y los procedimientos que deseas realizar para crear un inventario de tus datos en Amazon DataZone y publicarlos en Amazon DataZone.

Para poder utilizar Amazon DataZone para catalogar tus datos, primero debes incluir tus datos (activos) como inventario de tu proyecto en Amazon DataZone. Al crear un inventario para un proyecto en particular, solo los miembros de ese proyecto pueden descubrir los activos. Los activos del inventario del proyecto no están disponibles para todos los usuarios del dominio al realizar búsquedas o búsquedas, a menos que se publiquen de forma explícita. Tras crear el inventario de un proyecto, los propietarios de los datos pueden seleccionar sus activos de inventario con los metadatos empresariales necesarios añadiendo o actualizando los nombres de las empresas (activo y esquema), las descripciones (activo y esquema), el formato léame, los términos del glosario (activo y esquema) y los formularios de metadatos.

El siguiente paso para usar Amazon DataZone para catalogar tus datos es hacer que los usuarios del dominio puedan descubrir los activos de inventario de tu proyecto. Puedes hacerlo publicando los activos del inventario en el DataZone catálogo de Amazon. Solo se puede publicar en el catálogo la última versión del activo de inventario y solo la última versión publicada está activa en el catálogo de descubrimiento. Si un activo de inventario se actualiza después de publicarse en el DataZone catálogo de Amazon, debes volver a publicarlo de forma explícita para que la última versión esté en el catálogo de descubrimiento.

Temas

- Eliminar un DataZone activo de Amazon
- Iniciar manualmente la ejecución de una fuente de datos en Amazon DataZone
- Revisiones de activos en Amazon DataZone
- Calidad de los datos en Amazon DataZone
- Uso del aprendizaje automático y la IA generativa

Configurar los permisos de Lake Formation para Amazon DataZone

Al crear un entorno con el blueprint (DefaultDataLake) del lago de datos integrado, se añade una base de datos AWS Glue en Amazon DataZone como parte del proceso de creación de este entorno. Si desea publicar recursos de esta base de datos de AWS Glue, no necesita permisos adicionales.

Sin embargo, si quieres publicar activos y suscribirte a activos de una base de datos de AWS Glue que existe fuera de tu DataZone entorno de Amazon, debes proporcionar explícitamente a Amazon DataZone los permisos para acceder a las tablas de esta base de datos de AWS Glue externa. Para ello, debe completar los siguientes ajustes en AWS Lake Formation y adjuntar los permisos de Lake Formation necesarios aAmazonDataZoneGlueAccess- <region>- <domainId>.

- Configure la ubicación de Amazon S3 para su lago de datos en AWS Lake Formation con el modo de permiso de Lake Formation o el modo de acceso híbrido. Para obtener más información, consulte https://docs.aws.amazon.com/lake-formation/latest/dg/ register-data-lake .html.
- Elimine el `IAMAllowedPrincipals` permiso de las tablas de Amazon Lake Formation para las que Amazon DataZone gestiona los permisos. Para obtener más información, consulte https://docs.aws.amazon.com/lake-formation/latest/dg/ upgrade-glue-lake-formation -background.html.
- Adjunte los siguientes permisos de AWS Lake Formation aAmazonDataZoneGlueAccess- <region>- <domainId>:
  - `Describe`y `Describe grantable` permisos en la base de datos en la que se encuentran las tablas
  - `Describe`,`Select`,`Describe Grantable`, `Select Grantable` permisos en todas las tablas de la base de datos anterior DataZone a las que desee administrar el acceso en su nombre.

> **Note**
>
> Amazon DataZone admite el modo AWS Lake Formation Hybrid. El modo híbrido de Lake Formation le permite empezar a gestionar los permisos de sus bases de datos y tablas de AWS Glue a través de Lake Formation, sin dejar de mantener los permisos de IAM existentes en estas tablas y bases de datos. Para obtener más información, consulte DataZone Integración de Amazon con el modo híbrido de AWS Lake Formation .

Para obtener más información, consulte Solución de problemas de permisos de AWS Lake Formation para Amazon DataZone.

DataZone Integración de Amazon con el modo híbrido de AWS Lake Formation

Amazon DataZone está integrado con el modo híbrido AWS Lake Formation. Esta integración te permite publicar y compartir fácilmente tus tablas de AWS Glue a través de Amazon DataZone sin necesidad de registrarlas primero en AWS Lake Formation. El modo híbrido te permite empezar a gestionar los permisos de tus tablas de AWS Glue a través de AWS Lake Formation y, al mismo tiempo, conservar los permisos de IAM existentes en estas tablas.

Para empezar, puedes activar la configuración de registro de ubicación de datos en el DefaultDataLakeblueprint de la consola de DataZone administración de Amazon.

Habilite la integración con el modo híbrido de AWS Lake Formation

1. Ve a la DataZone consola de Amazon en https://console.aws.amazon.com/datazone e inicia sesión con las credenciales de tu cuenta.
2. Elija Ver dominios y elija el dominio en el que desee habilitar la integración con el modo híbrido de AWS Lake Formation.
3. En la página de detalles del dominio, vaya a la pestaña Blueprints.
4. En la lista de esquemas, elija el DefaultDataLakeesquema.
5. Asegúrese de que el DefaultDataLake esquema esté activado. Si no está activado, sigue los pasos que se indican Habilita los blueprints integrados en la AWS cuenta propietaria del dominio de Amazon DataZone para activarlo en tu AWS cuenta.
6. En la página de DefaultDataLake detalles, abre la pestaña Aprovisionamiento y selecciona el botón Editar en la esquina superior derecha de la página.

7. En Registro de ubicaciones de datos, active la casilla para habilitar el registro de ubicaciones de datos.
8. Para la función de administración de ubicaciones de datos, puede crear una nueva función de IAM o seleccionar una función de IAM existente. Amazon DataZone utiliza esta función para gestionar el acceso de lectura y escritura a los depósitos de Amazon S3 elegidos para Data Lake mediante el modo de acceso híbrido AWS Lake Formation. Para obtener más información, consulte AmazonDataZone<region>S3 Manage- - <domainId>.
9. Si lo desea, puede optar por excluir determinadas ubicaciones de Amazon S3 si no desea que Amazon DataZone las registre automáticamente en modo híbrido. Para ello, complete los siguientes pasos:
   - Pulse el botón de alternancia para excluir ubicaciones específicas de Amazon S3.
   - Proporcione el URI del bucket de Amazon S3 que desea excluir.
   - Para añadir depósitos adicionales, selecciona Añadir ubicación de S3.

     > **Note**
     >
     > Amazon DataZone solo permite excluir una ubicación raíz de S3. Cualquier ubicación de S3 que se encuentre dentro de la ruta de una ubicación raíz de S3 se excluirá automáticamente del registro.

   - Elija Guardar cambios.

Una vez que haya habilitado la configuración de registro de ubicaciones de datos en su AWS cuenta, cuando un consumidor de datos se suscriba a una tabla de AWS Glue gestionada mediante permisos de IAM, Amazon DataZone registrará primero las ubicaciones de Amazon S3 de esta tabla en modo híbrido y, a continuación, concederá acceso al consumidor de datos gestionando los permisos de la tabla a través de AWS Lake Formation. Esto garantiza que los permisos de IAM disponibles sigan existiendo con los permisos de AWS Lake Formation recién otorgados, sin interrumpir ningún flujo de trabajo existente.

Cómo gestionar las ubicaciones cifradas de Amazon S3 al habilitar la integración del modo híbrido de AWS Lake Formation en Amazon DataZone

Si utiliza una ubicación de Amazon S3 cifrada con una clave de KMS gestionada o AWS gestionada por el cliente, la función AmazonDataZoneS3Manage debe tener el permiso para cifrar y descifrar

datos con la clave de KMS, o la política de claves de KMS debe conceder permisos sobre la clave de la función.

Si su ubicación de Amazon S3 está cifrada con una clave AWS gestionada, añada la siguiente política en línea al AmazonDataZoneDataLocationManagementrol:

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

Si su ubicación de Amazon S3 está cifrada con una clave gestionada por el cliente, haga lo siguiente:

1. Abra la consola de AWS KMS en https://console.aws.amazon.com/kms e inicie sesión como usuario administrativo de AWS Identity and Access Management (IAM) o como usuario que puede modificar la política de claves de la clave de KMS utilizada para cifrar la ubicación.
2. En el panel de navegación, elija Claves administradas por el cliente y, a continuación, el nombre de la clave de KMS deseada.
3. En la página de detalles de la clave KMS, elija la pestaña Política de claves y, a continuación, siga una de las instrucciones siguientes para añadir su rol personalizado o el rol vinculado al servicio de Lake Formation como usuario de la clave KMS:

   - Si aparece la vista predeterminada (con las secciones Administradores de claves, Eliminación de claves, Usuarios clave y Otras AWS cuentas), en la sección Usuarios clave, agregue la AmazonDataZoneDataLocationManagementfunción.

- Si aparece la política clave (JSON), edítela para añadir una AmazonDataZoneDataLocationManagementfunción al objeto «Permitir el uso de la clave», como se muestra en el siguiente ejemplo

```
...
        {
            "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 clave de KMS o la ubicación de Amazon S3 no se encuentran en la misma AWS cuenta que el catálogo de datos, siga las instrucciones que se indican en Registrar una ubicación de Amazon S3 cifrada en todas AWS las cuentas.

Cree tipos de activos personalizados

En Amazon DataZone, los activos representan tipos específicos de recursos de datos, como tablas de bases de datos, paneles o modelos de aprendizaje automático. Para proporcionar coherencia

y estandarización a la hora de describir los activos del catálogo, un DataZone dominio de Amazon debe tener un conjunto de tipos de activos que definan cómo se representan los activos en el catálogo. Un tipo de activo define el esquema de un tipo específico de activo. Un tipo de activo tiene un conjunto de tipos de formularios de metadatos obligatorios y opcionales con nombre (por ejemplo, GovForm o GovernanceFormType). Los tipos de activos en Amazon DataZone están versionados. Cuando se crean los activos, se validan según el esquema definido por su tipo de activo (normalmente, la última versión) y, si se especifica una estructura no válida, se produce un error en la creación del activo.

Tipos de activos del sistema: DataZone Amazon suministra tipos de activos del sistema propiedad del servicio (incluidos GlueTableAssetType GlueViewAssetType, RedshiftTableAssetType RedshiftViewAssetType, y S3ObjectCollectionAssetType) y tipos de formularios del sistema (incluidos DataSourceReferenceFormType AssetCommonDetailsFormType, y SubscriptionTermsFormType). Los tipos de activos del sistema no se pueden editar.

Tipos de activos personalizados: para crear tipos de activos personalizados, se empieza por crear los tipos de formulario de metadatos y los glosarios necesarios para utilizarlos en los tipos de formulario. A continuación, puede crear tipos de activos personalizados especificando el nombre, la descripción y los formularios de metadatos asociados, que pueden ser obligatorios u opcionales.

En el caso de los tipos de activos con datos estructurados, para representar el esquema de columnas en el portal de datos, puede utilizarlos `RelationalTableFormType` para añadir los metadatos técnicos a las columnas (incluidos los nombres de las columnas, las descripciones y los tipos de datos) y `ColumnBusinessMetadataForm` para añadir las descripciones comerciales de las columnas, incluidos los nombres comerciales, los términos del glosario y los pares de valores clave personalizados.

Para crear un tipo de activo personalizado a través del portal de datos, siga estos pasos:

1. Ve a la URL del portal de DataZone datos de Amazon e inicia sesión con el inicio de sesión único (SSO) o con tus credenciales. AWS Si eres DataZone administrador de Amazon, puedes ir a la DataZone consola de Amazon en https://console.aws.amazon.com/datazone e iniciar sesión con el Cuenta de AWS lugar donde se creó el dominio y, a continuación, elegir Open data portal.
2. Selecciona Seleccionar proyecto en el panel de navegación superior y selecciona el proyecto en el que quieres crear un tipo de activo personalizado.
3. Navegue hasta la pestaña Datos del proyecto.
4. Selecciona Tipos de activos en el panel de navegación izquierdo y, a continuación, selecciona Crear tipo de activo.

5. Especifique lo siguiente y, a continuación, elija Crear.

   - Nombre: el nombre del tipo de activo personalizado
   - Descripción: descripción del tipo de activo personalizado.
   - Elija Agregar formularios de metadatos para agregar formularios de metadatos a este tipo de activo personalizado.

6. Una vez creado el tipo de activo personalizado, puede usarlo para crear activos.

Para crear un tipo de activo personalizado mediante las API, complete los siguientes pasos:

1. Cree un tipo de formulario de metadatos invocando la acción de la `CreateFormType` API.

   El siguiente es un SageMaker ejemplo de 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. A continuación, puedes crear un tipo de activo invocando la acción de la `CreateAssetType` API. Puedes crear tipos de activos solo a través de DataZone las API de Amazon utilizando los

tipos de formulario del sistema disponibles (`SubscriptionTermsFormType`en el siguiente ejemplo) o tus tipos de formulario personalizados. En el caso de los tipos de formulario del sistema, el nombre del tipo debe empezar por`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,
        },
    },
)
```

El siguiente es un ejemplo de creación de un tipo de activo para datos estructurados:

```
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. Y ahora, puede crear un activo con los tipos de activos personalizados que creó en los pasos anteriores.

```
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}"
        }
        ]
)
```

Y en este ejemplo, está creando un activo de datos estructurados:

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

Cree y ejecute una fuente DataZone de datos de Amazon para AWS Glue Data Catalog

En Amazon DataZone, puedes crear una fuente de AWS Glue Data Catalog datos desde la que importar metadatos técnicos de tablas de bases de datos AWS Glue. Para añadir una fuente de datos para la AWS Glue Data Catalog, la base de datos de origen debe existir ya en AWS Glue.

Cuando creas y ejecutas una fuente de AWS Glue datos, añades activos de la AWS Glue base de datos de origen al inventario de tu DataZone proyecto de Amazon. Puede ejecutar sus fuentes de AWS Glue datos según un cronograma establecido o bajo demanda para crear o actualizar los metadatos técnicos de sus activos. Durante la ejecución de la fuente de datos, si lo desea, puede optar por publicar sus activos en el DataZone catálogo de Amazon y, de este modo, hacer que todos los usuarios del dominio puedan descubrirlos. También puedes publicar los activos del inventario de tu proyecto después de editar sus metadatos empresariales. Los usuarios del dominio pueden buscar y descubrir tus activos publicados y solicitar suscripciones a estos activos.

Para añadir una fuente AWS Glue de datos

1. Ve a la URL del portal de DataZone datos de Amazon e inicia sesión con el inicio de sesión único (SSO) o con tus credenciales. AWS Si eres DataZone administrador de Amazon, puedes ir a la DataZone consola de Amazon en https://console.aws.amazon.com/datazone e iniciar sesión con el Cuenta de AWS lugar donde se creó el dominio y, a continuación, elegir Open data portal.
2. Selecciona Seleccionar proyecto en el panel de navegación superior y selecciona el proyecto al que quieres añadir la fuente de datos.
3. Navegue hasta la pestaña Datos del proyecto.
4. Selecciona Fuentes de datos en el panel de navegación izquierdo y, a continuación, selecciona Crear fuente de datos.
5. Configure los siguientes campos:

   - Nombre: el nombre de la fuente de datos.
   - Descripción: descripción de la fuente de datos.
6. En Tipo de fuente de datos, elija AWS Glue.
7. En Seleccione un entorno, especifique un entorno en el que publicar las AWS Glue tablas.
8. En Selección de datos, proporcione una AWS Glue base de datos e introduzca los criterios de selección de la tabla. Por ejemplo, si selecciona Incluir e introducir`*corporate`, la base de datos incluirá todas las tablas de origen que terminen con la palabra`corporate`.

   Puede elegir una AWS Glue base de datos en el menú desplegable o escribir un nombre para la base de datos. El menú desplegable incluye dos bases de datos: la base de datos de publicación y la base de datos de suscripciones del entorno. Si desea extraer activos de una base de datos que no ha sido creada por el entorno, debe escribir el nombre de la base de datos en lugar de seleccionarla en el menú desplegable.

   Puede añadir varias reglas de inclusión y exclusión para las tablas de una sola base de datos. También puede agregar varias bases de datos mediante el botón Agregar otra base de datos.

9. En Calidad de los datos, puede optar por habilitar la calidad de los datos para esta fuente de datos. Si lo haces, Amazon DataZone importará tu salida de calidad de datos de AWS Glue existente a tu DataZone catálogo de Amazon. De forma predeterminada, Amazon DataZone importa de AWS Glue los últimos 100 informes de calidad existentes sin fecha de caducidad.

   Las métricas de calidad de los datos de Amazon te DataZone ayudan a entender la integridad y precisión de tus fuentes de datos. Amazon DataZone extrae estas métricas de calidad de

datos de AWS Glue para proporcionar contexto en un momento dado, por ejemplo, durante una búsqueda en un catálogo de datos empresariales. Los usuarios de datos pueden ver cómo cambian las métricas de calidad de los datos a lo largo del tiempo para sus activos suscritos. Los productores de datos pueden asimilar las puntuaciones de calidad de los datos de AWS Glue según un cronograma. El catálogo de datos DataZone empresariales de Amazon también puede mostrar métricas de calidad de datos de sistemas de terceros a través de API de calidad de datos. Para obtener más información, consulte Calidad de los datos en Amazon DataZone.

10. Elija Siguiente.
11. En la configuración de publicación, elija si los activos se pueden detectar inmediatamente en el catálogo de datos empresariales. Si solo los agrega al inventario, puede elegir las condiciones de suscripción más adelante y publicarlos en el catálogo de datos empresariales. Para obtener más información, consulte the section called “Gestione las fuentes de datos existentes”.
12. Para la generación automática de nombres comerciales, elija si desea generar automáticamente los metadatos de los activos a medida que se importan de la fuente.
13. (Opcional) En el caso de los formularios de metadatos, añade formularios para definir los metadatos que se recopilan y guardan al importar los activos a Amazon DataZone. Para obtener más información, consulte the section called “Cree, edite o elimine formularios de metadatos”.
14. En Preferencia de ejecución, elija cuándo ejecutar la fuente de datos.
    - Ejecutar según una programación: especifique las fechas y la hora para ejecutar la fuente de datos.
    - Ejecutar bajo demanda: puede iniciar manualmente la ejecución de la fuente de datos.
15. Elija Siguiente.
16. Revise la configuración de la fuente de datos y seleccione Crear.

Creación y ejecución de una fuente de DataZone datos de Amazon para Amazon Redshift

En Amazon DataZone, puede crear una fuente de datos de Amazon Redshift para importar metadatos técnicos de tablas y vistas de bases de datos desde el almacén de datos de Amazon Redshift. Para añadir una fuente de DataZone datos de Amazon para Amazon Redshift, el almacén de datos de origen debe existir ya en Amazon Redshift.

Cuando crea y ejecuta una fuente de datos de Amazon Redshift, añade activos del almacén de datos de Amazon Redshift de origen al inventario de su proyecto de DataZone Amazon. Puede ejecutar

sus fuentes de datos de Amazon Redshift según un cronograma establecido o a pedido para crear o actualizar los metadatos técnicos de sus activos. Durante la ejecución de la fuente de datos, si lo desea, puede optar por publicar los activos de inventario de su proyecto en el DataZone catálogo de Amazon y, de este modo, hacer que todos los usuarios del dominio puedan descubrirlos. También puedes publicar tus activos de inventario después de editar sus metadatos empresariales. Los usuarios del dominio pueden buscar y descubrir tus activos publicados y solicitar suscripciones a estos activos.

Para añadir una fuente de datos de Amazon Redshift

1. Ve a la URL del portal de DataZone datos de Amazon e inicia sesión con el inicio de sesión único (SSO) o con tus credenciales. AWS Si eres DataZone administrador de Amazon, puedes ir a la DataZone consola de Amazon en https://console.aws.amazon.com/datazone e iniciar sesión con el Cuenta de AWS lugar donde se creó el dominio y, a continuación, elegir Open data portal.
2. Selecciona Seleccionar proyecto en el panel de navegación superior y selecciona el proyecto al que quieres añadir la fuente de datos.
3. Navegue hasta la pestaña Datos del proyecto.
4. Selecciona Fuentes de datos en el panel de navegación izquierdo y, a continuación, selecciona Crear fuente de datos.
5. Configure los siguientes campos:
   - Nombre: el nombre de la fuente de datos.
   - Descripción: descripción de la fuente de datos.
6. En Tipo de fuente de datos, elija Amazon Redshift.
7. En Seleccione un entorno, especifique un entorno en el que publicar las tablas de Amazon Redshift.
8. Según el entorno que seleccione, Amazon DataZone aplicará automáticamente las credenciales de Amazon Redshift y otros parámetros directamente desde el entorno o le dará la opción de elegir los suyos propios.
   - Si ha seleccionado un entorno que solo permite publicar desde el esquema de Amazon Redshift predeterminado del entorno, Amazon DataZone aplicará automáticamente las credenciales de Amazon Redshift y otros parámetros, como el nombre del clúster o grupo de trabajo de Amazon Redshift, el secreto AWS , el nombre de la base de datos y el nombre del esquema. No puede editar estos parámetros que se rellenan automáticamente.

- Si selecciona un entorno que no permite publicar ningún dato, no podrá continuar con la creación de la fuente de datos.
- Si selecciona un entorno que permita publicar datos de cualquier esquema, verá la opción de usar las credenciales y otros parámetros de Amazon Redshift del entorno o de introducir sus propias credenciales/parámetros.

9. Si decide usar sus propias credenciales para crear la fuente de datos, proporcione los siguientes detalles:

   - En Proporcionar credenciales de Amazon Redshift, elija si desea utilizar un clúster de Amazon Redshift aprovisionado o un espacio de trabajo sin servidor de Amazon Redshift como fuente de datos.
   - Según lo que haya seleccionado en el paso anterior, elija su clúster o espacio de trabajo de Amazon Redshift en el menú desplegable y, a continuación, elija el secreto en AWS Secrets Manager que desee usar para la autenticación. Puede elegir un secreto existente o crear uno nuevo.
   - Para que el secreto existente aparezca en el menú desplegable, asegúrate de que tu secreto en AWS Secrets Manager incluya las siguientes etiquetas (clave/valor):
     - AmazonDataZoneProject: <projectID>
     - AmazonDataZoneDomain: <domainID>

     Si decides crear un secreto nuevo, el secreto se etiqueta automáticamente con las etiquetas a las que se ha hecho referencia anteriormente y no es necesario realizar ningún paso adicional. Para obtener más información, consulte Almacenar las credenciales de la base de datos en AWS Secrets Manager.

     Los usuarios de Amazon Redshift que utilicen el AWS secreto proporcionado para crear la fuente de datos deben tener `SELECT` permisos en las tablas que se van a publicar. Si quieres que Amazon DataZone también gestione las suscripciones (acceso) en tu nombre, los usuarios de la base de datos que figuran en el AWS secreto también deben tener los siguientes permisos:
     - `CREATE DATASHARE`
     - `ALTER DATASHARE`
     - `DROP DATASHARE`

10. En Selección de datos, proporcione una base de datos y un esquema de Amazon Redshift e introduzca los criterios de selección de la tabla o vista. Por ejemplo, si elige Incluir e

introducir`*corporate`, el activo incluirá todas las tablas de origen que terminen con la palabra`corporate`.

Puede añadir varias reglas de inclusión para las tablas de una única base de datos. También puede agregar varias bases de datos mediante el botón Agregar otra base de datos.

11. Elija Siguiente.
12. En la configuración de publicación, elija si los activos se pueden detectar inmediatamente en el catálogo de datos. Si solo los agrega al inventario, puede elegir las condiciones de suscripción más adelante y publicarlos en el catálogo de datos empresariales. Para obtener más información, consulte the section called “Gestione las fuentes de datos existentes”.
13. Para la generación automática de nombres comerciales, elija si desea generar automáticamente los metadatos de los activos a medida que se publican y actualizan desde la fuente.
14. (Opcional) En el caso de los formularios de metadatos, añade formularios para definir los metadatos que se recopilan y guardan al importar los activos a Amazon DataZone. Para obtener más información, consulte the section called “Cree, edite o elimine formularios de metadatos”.
15. En Preferencia de ejecución, elija cuándo ejecutar la fuente de datos.
    - Ejecutar según una programación: especifique las fechas y la hora para ejecutar la fuente de datos.
    - Ejecutar bajo demanda: puede iniciar manualmente la ejecución de la fuente de datos.
16. Elija Siguiente.
17. Revise la configuración de la fuente de datos y seleccione Crear.

Gestiona las fuentes de DataZone datos de Amazon existentes

Tras crear una fuente de DataZone datos de Amazon, puede modificarla en cualquier momento para cambiar los detalles de la fuente o los criterios de selección de datos. Cuando ya no necesite una fuente de datos, puede eliminarla.

Para completar estos pasos, debe tener adjunta la política AmazonDataZoneFullAccess AWS administrada. Para obtener más información, consulte the section called “AWS políticas gestionadas”.

Temas

Edite una fuente de datos

Puede editar una fuente de DataZone datos de Amazon para modificar su configuración de selección de datos, lo que incluye añadir, eliminar o cambiar los criterios de selección de la tabla. También puede añadir y eliminar bases de datos. No puede cambiar el tipo de fuente de datos ni el entorno en el que se publica una fuente de datos.

Para editar un origen de datos, realice el siguiente procedimiento:

1. Ve a la URL del portal de DataZone datos de Amazon e inicia sesión con el inicio de sesión único (SSO) o con tus credenciales. AWS Si eres DataZone administrador de Amazon, puedes ir a la DataZone consola de Amazon en https://console.aws.amazon.com/datazone e iniciar sesión con el Cuenta de AWS lugar donde se creó el dominio y, a continuación, elegir Open data portal.
2. Selecciona Seleccionar proyecto en el panel de navegación superior y selecciona el proyecto al que pertenece la fuente de datos.
3. Navegue hasta la pestaña Datos del proyecto.
4. Elija Fuentes de datos en el panel de navegación izquierdo y, a continuación, elija la fuente de datos que desee modificar.
5. Vaya a la pestaña de definición de fuente de datos y elija Editar.
6. Realice los cambios que desee en la definición de la fuente de datos. Puede actualizar los detalles de la fuente de datos y realizar cambios en los criterios de selección de datos.
7. Cuando termine de realizar los cambios, seleccione Guardar.

Eliminar un origen de datos

Cuando ya no necesite una fuente de DataZone datos de Amazon, puede eliminarla permanentemente. Tras eliminar una fuente de datos, todos los activos que se originaron en esa fuente de datos seguirán estando disponibles en el catálogo y los usuarios podrán seguir suscribiéndose a ellos. Sin embargo, los activos dejarán de recibir actualizaciones de la fuente. Le recomendamos que primero mueva los activos dependientes a una fuente de datos diferente antes de eliminarlos.

> **Note**
>
> Debes eliminar todos los cumplimientos de la fuente de datos para poder eliminarla. Para obtener más información, consulte Detectar, suscribirse y consumir datos en Amazon DataZone.

Eliminación de un origen de datos

1. En la pestaña Datos del proyecto, selecciona Fuentes de datos en el panel de navegación izquierdo.
2. Elija la fuente de datos que desee eliminar.
3. Seleccione Acciones, elimine la fuente de datos y confirme la eliminación.

Publica activos en el DataZone catálogo de Amazon desde el inventario del proyecto

Puedes publicar DataZone los activos de Amazon y sus metadatos de los inventarios de proyectos en el DataZone catálogo de Amazon. Solo puedes publicar la versión más reciente de un activo en el catálogo.

Tenga en cuenta lo siguiente al publicar activos en el catálogo:

- Para publicar un activo en el catálogo, debe ser el propietario o el colaborador de ese proyecto.
- En el caso de los activos de Amazon Redshift, asegúrese de que los clústeres de Amazon Redshift asociados a los clústeres de publicadores y suscriptores cumplan todos los requisitos para el intercambio de datos de Amazon Redshift para que Amazon pueda gestionar el acceso DataZone a las tablas y vistas de Redshift. Consulte Conceptos de uso compartido de datos para Amazon Redshift.
- Amazon DataZone solo admite la gestión del acceso a los activos publicados desde Amazon Redshift AWS Glue Data Catalog y Amazon Redshift. Para todos los demás activos, como los objetos de Amazon S3, Amazon DataZone no gestiona el acceso de los suscriptores aprobados. Si se suscribe a estos activos no gestionados, se le notificará con el siguiente mensaje:

```
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.
```

Publica un activo

Si no eligió hacer que los activos se pudieran detectar inmediatamente en el catálogo de datos al crear una fuente de datos, lleve a cabo los siguientes pasos para publicarlos más adelante.

Para publicar un activo

1. Ve a la URL del portal de DataZone datos de Amazon e inicia sesión con el inicio de sesión único (SSO) o con tus credenciales. AWS Si eres DataZone administrador de Amazon, puedes ir a la DataZone consola de Amazon en https://console.aws.amazon.com/datazone e iniciar sesión con el Cuenta de AWS lugar donde se creó el dominio y, a continuación, elegir Open data portal.
2. Selecciona Seleccionar proyecto en el panel de navegación superior y selecciona el proyecto al que pertenece el activo.
3. Navegue hasta la pestaña Datos del proyecto.
4. Selecciona Datos de inventario en el panel de navegación izquierdo y, a continuación, selecciona el activo que deseas publicar.

   > **Note**
   >
   > De forma predeterminada, todos los activos requieren la aprobación de la suscripción, lo que significa que el propietario de los datos debe aprobar todas las solicitudes de suscripción al activo. Si desea cambiar esta configuración antes de publicar el activo, abra los detalles del activo y seleccione Editar junto a la aprobación de la suscripción. Puede cambiar esta configuración más adelante modificando y volviendo a publicar el activo.

5. Seleccione Publicar recurso. El activo se publica directamente en el catálogo.

   Si realiza cambios en el activo, como modificar sus requisitos de aprobación, puede elegir Volver a publicar para publicar las actualizaciones en el catálogo.

Gestione el inventario y gestione los activos

Para poder utilizar Amazon DataZone para catalogar tus datos, primero debes incluir tus datos (activos) como inventario de tu proyecto en Amazon DataZone. Al crear un inventario para un proyecto en particular, solo los miembros de ese proyecto pueden descubrir los activos.

Una vez creados los activos en el inventario del proyecto, se pueden conservar sus metadatos. Por ejemplo, puedes editar el nombre o la descripción del activo o leerme. Cada edición del activo crea una nueva versión del activo. Puede utilizar la pestaña Historial de la página de detalles del activo para ver todas las versiones del activo.

Puede editar la sección Léeme y añadir descripciones detalladas para el activo. La sección Léame permite rebajas, lo que te permite dar el formato necesario a tus descripciones y describir la información clave sobre un activo a los consumidores.

Los términos del glosario se pueden añadir a nivel de activo rellenando los formularios disponibles.

Para organizar el esquema, puede revisar las columnas, agregar nombres comerciales, descripciones y agregar términos de glosario a nivel de columna.

Si la generación automática de metadatos está habilitada al crear la fuente de datos, los nombres comerciales de los activos y las columnas están disponibles para revisarlos y aceptarlos o rechazarlos individualmente o todos a la vez.

También puede editar las condiciones de la suscripción para especificar si se requiere o no la aprobación del activo.

Los formularios de metadatos de Amazon le DataZone permiten ampliar el modelo de metadatos de un activo de datos añadiendo atributos personalizados (por ejemplo, región de ventas, año de venta y trimestre de ventas). Los formularios de metadatos que se adjuntan a un tipo de activo se aplican a todos los activos creados a partir de ese tipo de activo. También puede agregar formularios de metadatos adicionales a activos individuales como parte de la fuente de datos que se ejecuta o después de crearla. Para crear nuevos formularios, consultethe section called “Cree, edite o elimine formularios de metadatos”.

Para actualizar los metadatos de un activo, debe ser el propietario o el colaborador del proyecto al que pertenece el activo.

Para actualizar los metadatos de un activo

1. Ve a la URL del portal de DataZone datos de Amazon e inicia sesión con el inicio de sesión único (SSO) o con tus credenciales. AWS Si eres DataZone administrador de Amazon, puedes ir a la DataZone consola de Amazon en https://console.aws.amazon.com/datazone e iniciar sesión con el Cuenta de AWS lugar donde se creó el dominio y, a continuación, elegir Open data portal.
2. Selecciona Seleccionar proyecto en el panel de navegación superior y selecciona el proyecto que contiene el activo cuyos metadatos deseas actualizar.
3. Navegue hasta la pestaña Datos del proyecto.
4. Selecciona Datos de inventario en el panel de navegación izquierdo y, a continuación, elige el nombre del activo cuyos metadatos deseas actualizar.
5. En la página de detalles del activo, en Formularios de metadatos, selecciona Editar y edita los formularios existentes según sea necesario. También puede adjuntar formularios de metadatos adicionales al activo. Para obtener más información, consulte the section called “Adjunte formularios de metadatos adicionales a los activos”.
6. Cuando haya terminado de realizar las actualizaciones, elija Guardar formulario.

   Al guardar el formulario, Amazon DataZone genera una nueva versión de inventario del activo. Para publicar la versión actualizada en el catálogo, selecciona Volver a publicar el activo.

Adjunte formularios de metadatos adicionales a los activos

De forma predeterminada, los formularios de metadatos adjuntos a un dominio se adjuntan a todos los activos publicados en ese dominio. Los publicadores de datos pueden asociar formularios de metadatos adicionales a activos individuales para proporcionar un contexto adicional.

Para adjuntar formularios de metadatos adicionales a un activo

1. Ve a la URL del portal de DataZone datos de Amazon e inicia sesión con el inicio de sesión único (SSO) o con tus credenciales. AWS Si eres DataZone administrador de Amazon, puedes ir a la DataZone consola de Amazon en https://console.aws.amazon.com/datazone e iniciar sesión con el Cuenta de AWS lugar donde se creó el dominio y, a continuación, elegir Open data portal.
2. Selecciona Seleccionar proyecto en el panel de navegación superior y selecciona el proyecto que contiene el activo cuyos metadatos quieres añadir.
3. Navegue hasta la pestaña Datos del proyecto.

4. Selecciona Datos de inventario en el panel de navegación izquierdo y, a continuación, elige el nombre del activo cuyos metadatos quieres añadir.
5. En la página de detalles del activo, en Formularios de metadatos, selecciona Añadir formularios.
6. Seleccione los formularios que desee añadir al activo y, a continuación, elija Añadir formularios.
7. Introduzca valores para cada uno de los campos de metadatos y, a continuación, seleccione Guardar formulario.

   Al guardar el formulario, Amazon DataZone genera una nueva versión de inventario del activo. Para publicar la versión actualizada en el catálogo, selecciona Volver a publicar el activo.

Publique el activo en el catálogo después de la conservación

Una vez satisfecho con la conservación de los activos, el propietario de los datos puede publicar una versión del activo en el DataZone catálogo de Amazon y, de este modo, hacer que todos los usuarios del dominio puedan descubrirla. El activo muestra la versión de inventario y la versión publicada. En el catálogo de descubrimiento, solo aparece la última versión publicada. Si los metadatos se actualizan después de la publicación, habrá una nueva versión de inventario disponible para su publicación en el catálogo.

Cree un activo manualmente

En Amazon DataZone, un activo es una entidad que presenta un único objeto de datos físico (por ejemplo, una tabla, un panel o un archivo) o un objeto de datos virtual (por ejemplo, una vista). Para obtener más información, consulte DataZone Terminología y conceptos de Amazon. La publicación manual de un activo es una operación que se realiza una sola vez. No se especifica un programa de ejecución para el activo, por lo que no se actualiza automáticamente si su origen cambia.

Para crear manualmente un activo a través de un proyecto, debe ser el propietario o el colaborador de ese proyecto.

Para crear un activo manualmente

1. Ve a la URL del portal de DataZone datos de Amazon e inicia sesión con el inicio de sesión único (SSO) o con tus credenciales. AWS Si eres DataZone administrador de Amazon, puedes ir a la DataZone consola de Amazon en https://console.aws.amazon.com/datazone e iniciar sesión con el Cuenta de AWS lugar donde se creó el dominio y, a continuación, elegir Open data portal.

2. Selecciona Seleccionar proyecto en el panel de navegación superior y selecciona el proyecto en el que quieres crear el activo.
3. Navegue hasta la pestaña Datos del proyecto.
4. Selecciona Fuentes de datos en el panel de navegación izquierdo y, a continuación, selecciona Crear activo de datos.
5. Para ver los detalles del activo, configure los siguientes ajustes:

   - Tipo de activo: el tipo de activo.
   - Nombre: el nombre del activo.
   - Descripción: descripción del activo.
6. Para la ubicación de S3, introduzca el nombre de recurso de Amazon (ARN) del bucket de S3 de origen.

   Si lo desea, introduzca un punto de acceso S3. Para obtener más información, consulte Administración del acceso a datos con puntos de acceso de Amazon S3.
7. En la configuración de publicación, elija si los activos se pueden detectar inmediatamente en el catálogo. Si solo los agrega al inventario, puede elegir las condiciones de suscripción más adelante para publicarlos en el catálogo.
8. Seleccione Crear.

   Una vez creado el activo, se publicará directamente como activo en el catálogo o se almacenará en el inventario hasta que decidas publicarlo.

Anular la publicación de un activo del catálogo de Amazon DataZone

Al anular la publicación de un DataZone recurso de Amazon del catálogo, deja de aparecer en los resultados de búsqueda globales. Los nuevos usuarios no podrán encontrar ni suscribirse a la lista de activos del catálogo, pero todas las suscripciones existentes seguirán siendo las mismas.

Para anular la publicación de un activo, debe ser el propietario o el colaborador del proyecto al que pertenece el activo:

Para anular la publicación de un activo

1. Ve a la URL del portal de DataZone datos de Amazon e inicia sesión con el inicio de sesión único (SSO) o con tus credenciales. AWS Si eres DataZone administrador de Amazon, puedes ir a la DataZone consola de Amazon en https://console.aws.amazon.com/datazone e iniciar sesión con el Cuenta de AWS lugar donde se creó el dominio y, a continuación, elegir Open data portal.
2. Selecciona Seleccionar proyecto en el panel de navegación superior y selecciona el proyecto al que pertenece el activo.
3. Navegue hasta la pestaña Datos del proyecto.
4. Seleccione Datos publicados en el panel de navegación izquierdo.
5. Localice el activo en la lista de activos publicados y, a continuación, seleccione Anular la publicación.

   El activo se elimina del catálogo. Puede volver a publicar el activo en cualquier momento seleccionando Publicar.

Eliminar un DataZone activo de Amazon

Cuando ya no necesites un activo en Amazon DataZone, puedes eliminarlo permanentemente. Eliminar un recurso no es lo mismo que anular la publicación de un activo del catálogo. Puede eliminar un activo y su listado relacionado en el catálogo para que no aparezca en ningún resultado de búsqueda. Para eliminar el listado de activos, primero debes revocar todas sus suscripciones.

Para eliminar un activo, debe ser el propietario o el colaborador del proyecto al que pertenece el activo:

> **Note**
>
> Para eliminar un listado de activos, primero debe revocar todas las suscripciones existentes al activo. No puedes eliminar un listado de activos que ya tenga suscriptores.

Para eliminar un activo

1. Ve a la URL del portal de DataZone datos de Amazon e inicia sesión con el inicio de sesión único (SSO) o con tus credenciales. AWS Si eres DataZone administrador de Amazon, puedes ir

a la DataZone consola de Amazon en https://console.aws.amazon.com/datazone e iniciar sesión con el Cuenta de AWS lugar donde se creó el dominio y, a continuación, elegir Open data portal.

2. Selecciona Seleccionar proyecto en el panel de navegación superior y selecciona el proyecto que contiene el activo que deseas eliminar.
3. Navegue hasta la pestaña Datos del proyecto.
4. Selecciona Datos publicados en el panel de navegación izquierdo y, a continuación, busca y elige el activo que deseas eliminar. Esto abre la página de detalles del activo.
5. Seleccione Acciones, Eliminar y confirme la eliminación.

   Una vez que se elimina el recurso, deja de estar disponible para su visualización y los usuarios no pueden suscribirse a él.

Iniciar manualmente la ejecución de una fuente de datos en Amazon DataZone

Cuando ejecutas una fuente de datos, Amazon DataZone extrae todos los metadatos nuevos o modificados de la fuente y actualiza los activos asociados en el inventario. Cuando agregas una fuente de datos a Amazon DataZone, especificas la preferencia de ejecución de la fuente, que define si la fuente se ejecuta según una programación o bajo demanda. Si la fuente se ejecuta bajo demanda, debe iniciar una fuente de datos que se ejecute manualmente.

Incluso si la fuente se ejecuta según una programación, puede ejecutarla manualmente en cualquier momento. Tras añadir metadatos empresariales a los activos, puedes seleccionarlos y publicarlos en el DataZone catálogo de Amazon para que todos los usuarios del dominio puedan descubrirlos. Los demás usuarios del dominio solo pueden buscar los activos publicados.

Para ejecutar una fuente de datos manualmente

1. Ve a la URL del portal de DataZone datos de Amazon e inicia sesión con el inicio de sesión único (SSO) o con tus credenciales. AWS Si eres DataZone administrador de Amazon, puedes ir a la DataZone consola de Amazon en https://console.aws.amazon.com/datazone e iniciar sesión con el Cuenta de AWS lugar donde se creó el dominio y, a continuación, elegir Open data portal.
2. Selecciona Seleccionar proyecto en el panel de navegación superior y selecciona el proyecto al que pertenece la fuente de datos.
3. Navegue hasta la pestaña Datos del proyecto.

4. Elija Fuentes de datos en el panel de navegación izquierdo y, a continuación, busque y elija la fuente de datos que desee ejecutar. Esto abre la página de detalles de la fuente de datos.
5. Elija Ejecutar bajo demanda.

   El estado de la fuente de datos cambia a `Running` cuando Amazon DataZone actualiza los metadatos de los activos con los datos más recientes de la fuente. Puede supervisar el estado de la ejecución en la pestaña Ejecuciones de la fuente de datos.

Revisiones de activos en Amazon DataZone

Amazon DataZone incrementa la revisión de un activo cuando editas sus metadatos comerciales o técnicos. Estas modificaciones incluyen la modificación del nombre del activo, la descripción, los términos del glosario, los nombres de las columnas, los formularios de metadatos y los valores de los campos del formulario de metadatos. Estos cambios pueden ser el resultado de ediciones manuales, de la ejecución de tareas en la fuente de datos o de operaciones de la API. Amazon genera DataZone automáticamente una nueva revisión del activo cada vez que realizas una modificación en el activo.

Tras actualizar un activo y generar una nueva revisión, debes publicar la nueva revisión en el catálogo para que se actualice y esté disponible para los suscriptores. Para obtener más información, consulte the section called “Publica los activos del inventario del proyecto en el catálogo”. Solo puede publicar la versión más reciente de un activo en el catálogo.

Para ver las revisiones anteriores de un activo

1. Ve a la URL del portal de DataZone datos de Amazon e inicia sesión con el inicio de sesión único (SSO) o con tus credenciales. AWS Si eres DataZone administrador de Amazon, puedes ir a la DataZone consola de Amazon en https://console.aws.amazon.com/datazone e iniciar sesión con el Cuenta de AWS lugar donde se creó el dominio y, a continuación, elegir Open data portal.
2. Selecciona Seleccionar proyecto en el panel de navegación superior y selecciona el proyecto que contiene el activo.
3. Vaya a la pestaña Datos del proyecto y, a continuación, busque y elija el activo. Esto abre la página de detalles del activo.
4. Navegue a la pestaña Historial, que muestra una lista de las revisiones anteriores del activo.

Calidad de los datos en Amazon DataZone

Las métricas de calidad de los datos de Amazon te DataZone ayudan a entender las diferentes métricas de calidad, como la integridad, la puntualidad y la precisión de tus fuentes de datos. Amazon DataZone se integra con AWS Glue Data Quality y ofrece API para integrar métricas de calidad de datos de soluciones de calidad de datos de terceros. Los usuarios de datos pueden ver cómo las métricas de calidad de los datos cambian a lo largo del tiempo para sus activos suscritos. Para crear y ejecutar las reglas de calidad de los datos, puede utilizar la herramienta de calidad de datos que prefiera, como AWS Glue Data Quality. Con las métricas de calidad de los datos de Amazon DataZone, los consumidores de datos pueden visualizar las puntuaciones de calidad de los datos de los activos y las columnas, lo que ayuda a generar confianza en los datos que utilizan para tomar decisiones.

Requisitos previos y cambios en las funciones de IAM

Si utilizas las políticas AWS gestionadas DataZone de Amazon, no hay pasos de configuración adicionales y estas políticas gestionadas se actualizan automáticamente para garantizar la calidad de los datos. Si utilizas tus propias políticas para las funciones que otorgan a Amazon DataZone los permisos necesarios para interoperar con los servicios compatibles, debes actualizar las políticas adjuntas a estas funciones para permitir la lectura de la información sobre la calidad de los datos de AWS Glue en el AWS política gestionada: AmazonDataZoneGlueManageAccessRolePolicy y habilitar el soporte para las API de series temporales en el AWS política gestionada: AmazonDataZoneDomainExecutionRolePolicy y en elAWS política gestionada: AmazonDataZoneFullUserAccess.

Habilitar la calidad de los datos para los activos de AWS Glue

Amazon DataZone extrae las métricas de calidad de los datos de AWS Glue para proporcionar contexto durante un momento determinado, por ejemplo, durante una búsqueda en un catálogo de datos empresariales. Los usuarios de datos pueden ver cómo cambian las métricas de calidad de los datos a lo largo del tiempo para sus activos suscritos. Los productores de datos pueden asimilar las puntuaciones de calidad de los datos de AWS Glue según un cronograma. El catálogo de datos DataZone empresariales de Amazon también puede mostrar métricas de calidad de datos de sistemas de terceros a través de API de calidad de datos. Para obtener más información, consulte AWS Glue Data Quality y Introducción a AWS Glue Data Quality para el catálogo de datos.

Puedes habilitar las métricas de calidad de los datos para tus DataZone activos de Amazon de las siguientes maneras:

- Utilice el portal de datos o DataZone las API de Amazon para mejorar la calidad de los datos de su fuente de datos de AWS Glue a través del portal de DataZone datos de Amazon, ya sea al crear una nueva fuente de datos de AWS Glue o al editar la existente.

  Para obtener más información sobre cómo habilitar la calidad de los datos para una fuente de datos a través del portal, consulte Cree y ejecute una fuente DataZone de datos de Amazon para AWS Glue Data Catalog yGestiona las fuentes de DataZone datos de Amazon existentes.

  > **Note**
  >
  > Puede usar el portal de datos para habilitar la calidad de los datos solo para sus activos de inventario de AWS Glue. En esta versión de Amazon, no se admite la DataZone habilitación de la calidad de los datos para activos de Amazon Redshift o de tipos personalizados a través del portal de datos.

  También puede utilizar las API para mejorar la calidad de los datos de sus fuentes de datos nuevas o existentes. Para ello, invoca CreateDataSourceo UpdateDataSourcey establece el `autoImportDataQualityResult` parámetro en «Verdadero».

  Una vez habilitada la calidad de los datos, puede ejecutar la fuente de datos a pedido o según lo programado. Cada ejecución puede generar hasta 100 métricas por activo. No es necesario crear formularios ni añadir métricas manualmente cuando se utiliza la fuente de datos para garantizar la calidad de los datos. Cuando se publica el activo, las actualizaciones realizadas en el formulario de calidad de los datos (hasta 30 puntos de datos por regla histórica) se reflejan en el anuncio para los consumidores. Posteriormente, cada nueva incorporación de métricas al activo se añade automáticamente al anuncio. No es necesario volver a publicar el activo para que las puntuaciones más recientes estén disponibles para los consumidores.

Habilitar la calidad de los datos para los tipos de activos personalizados

Puede usar las DataZone API de Amazon para habilitar la calidad de los datos para cualquiera de sus activos de tipo personalizado. Para más información, consulte los siguientes temas:

- PostTimeSeriesDataPoints
- ListTimeSeriesDataPoints
- GetTimeSeriesDataPoint

- DeleteTimeSeriesDataPoints

Los siguientes pasos proporcionan un ejemplo del uso de las API o la CLI para importar métricas de terceros para sus activos en Amazon DataZone:

1. Invoca la `PostTimeSeriesDataPoints` API de la siguiente manera:

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

con la siguiente carga útil:

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

```
 0.28\",\n \"details\" : {\n \"STATISTIC_NAME\" : \"Completeness\",\n \"COLUMN_NAME
\" : \"AnnualRevenue\"\n },\n \"status\" : \"PASS\"\n }, {\n \"description
\" : \"StandardDeviation \\\"AnnualRevenue\\\" between 1658483123.39 and
 1833060294.28\",\n \"details\" : {\n \"STATISTIC_NAME\" : \"StandardDeviation
\",\n \"COLUMN_NAME\" : \"AnnualRevenue\"\n },\n \"status\" : \"PASS\"\n }, {\n
 \"description\" : \"ColumnValues \\\"AnnualRevenue\\\" between 29999999 and
 5600000001\",\n \"details\" : {\n \"STATISTIC_NAME\" : \"Minimum,Maximum\",\n
 \"COLUMN_NAME\" : \"AnnualRevenue,AnnualRevenue\"\n },\n \"status\" : \"PASS
\"\n } ],\n \"passingPercentage\" : 1.0\n}",
"formName": "GREAT_EXPECTATION_NEW",
"typeIdentifier": "amazon.datazone.DataQualityResultFormType",
"timestamp": 1608969556
}
]
}
```

2. Invoca la `DeleteTimeSeriesDataPoints` API de la siguiente manera:

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

Uso del aprendizaje automático y la IA generativa

> **Note**
>
> Desarrollado por Amazon Bedrock: AWS implementa la detección automática de abusos. Como las recomendaciones de IA para la funcionalidad de descripciones de Amazon DataZone se basan en Amazon Bedrock, los usuarios heredan los controles implementados en Amazon Bedrock para garantizar la protección, la seguridad y el uso responsable de la IA.

En la versión actual de Amazon DataZone, puedes usar la funcionalidad de recomendaciones de IA para descripciones a fin de automatizar el descubrimiento y la catalogación de datos. Support for generative AI and machine learning en Amazon DataZone crea descripciones para activos y

columnas. Puedes usar estas descripciones para añadir un contexto empresarial a tus datos y recomendar el análisis de los conjuntos de datos, lo que puede ayudar a impulsar los resultados de descubrimiento de datos.

Con la tecnología de los grandes modelos lingüísticos de Amazon Bedrock, las recomendaciones de IA para las descripciones de activos de datos en Amazon le DataZone ayudan a garantizar que sus datos sean comprensibles y fáciles de descubrir. Las recomendaciones de la IA también sugieren las aplicaciones analíticas más pertinentes para los conjuntos de datos. Al reducir las tareas de documentación manual y asesorar sobre el uso adecuado de los datos, las descripciones generadas automáticamente pueden ayudarlo a mejorar la confiabilidad de sus datos y minimizar la omisión de datos valiosos para acelerar la toma de decisiones informadas.

> **Important**
>
> En la DataZone versión actual de Amazon, la función de recomendaciones de IA para las descripciones solo se admite en las siguientes regiones:
>
> - Este de EE. UU. (Norte de Virginia)
> - Oeste de EE. UU. (Oregón)
> - Europa (Fráncfort)
> - Asia-Pacífico (Tokio)

El siguiente procedimiento describe cómo generar recomendaciones de IA para las descripciones en Amazon DataZone:

1. Ve a la URL del portal de DataZone datos de Amazon e inicia sesión con el inicio de sesión único (SSO) o con tus credenciales. AWS Si eres DataZone administrador de Amazon, dirígete a la DataZone consola de Amazon en https://console.aws.amazon.com/datazone, inicia sesión con el Cuenta de AWS lugar donde se creó el dominio y, a continuación, selecciona Open data portal.
2. En el panel de navegación superior, selecciona Seleccionar proyecto y, a continuación, elige el proyecto que contiene el activo para el que quieres generar recomendaciones de IA para su descripción.
3. Ve a la pestaña Datos del proyecto.
4. En el panel de navegación izquierdo, selecciona Datos de inventario y, a continuación, elige el nombre del activo para el que quieres generar recomendaciones de IA para su descripción.

5. En la página de detalles del activo, en la pestaña de metadatos empresariales, selecciona Generar descripciones.
6. Una vez generadas las descripciones, puede editarlas, aceptarlas o rechazarlas. Aparecen iconos verdes junto a cada descripción de metadatos generada automáticamente para el activo de datos. En la pestaña Metadatos empresariales, puede elegir el icono verde situado junto al resumen generado automáticamente y, a continuación, elegir Editar, Aceptar o Rechazar para abordar la descripción generada. También puede seleccionar Aceptar todas o Rechazar todas las opciones que aparecen en la parte superior de la página cuando se selecciona la pestaña Metadatos empresariales y, de este modo, realizar la acción seleccionada en todas las descripciones generadas automáticamente.

   También puede elegir la pestaña Esquema y, a continuación, abordar las descripciones generadas automáticamente de forma individual. Para ello, seleccione el icono verde para las descripciones de una columna cada vez y, a continuación, elija Aceptar o Rechazar. En la pestaña Esquema, también puede seleccionar Aceptar todas o Rechazar todas y, de este modo, realizar la acción seleccionada en todas las descripciones generadas automáticamente.
7. Para publicar el activo en el catálogo con las descripciones generadas, seleccione Publicar activo y, a continuación, confirme esta acción pulsando de nuevo Publicar activo en la ventana emergente Publicar activo.

> **Note**
>
> Si no acepta o rechaza las descripciones generadas para un activo y, a continuación, publica este activo, estos metadatos generados automáticamente y no revisados no se incluyen en el activo de datos publicado.

Detectar, suscribirse y consumir datos en Amazon DataZone

En Amazon DataZone, una vez que se publica un activo en un dominio, los suscriptores pueden descubrirlo y solicitar una suscripción a ese activo. El proceso de suscripción comienza cuando el suscriptor busca y navega por el catálogo para encontrar el activo que busca. Desde el DataZone portal de Amazon, eligen suscribirse al activo enviando una solicitud de suscripción que incluye la justificación y el motivo de la solicitud. A continuación, el aprobador de la suscripción, tal como se define en el acuerdo de publicación, revisa la solicitud de acceso. Puede aprobar o rechazar la solicitud.

Una vez concedida la suscripción, se inicia un proceso de gestión logística para facilitar el acceso del suscriptor al activo. Existen dos modos principales de control de acceso y gestión logística de los activos: los de los activos DataZone gestionados por Amazon y los de los activos que no gestiona Amazon DataZone.

- Activos gestionados: Amazon DataZone puede gestionar la gestión logística y los permisos de los activos gestionados, como AWS Glue tablas y vistas de Amazon Redshift.
- Activos no gestionados: Amazon DataZone publica eventos estándar relacionados con tus acciones (por ejemplo, la aprobación de una solicitud de suscripción) en Amazon EventBridge. Puedes usar estos eventos estándar para integrarlos con otros AWS servicios o soluciones de terceros para realizar integraciones personalizadas.

Temas

Descubriendo datos

En las siguientes tareas se describen varias formas de descubrir datos en Amazon DataZone.

Temas

Busque y visualice los activos en el catálogo

Amazon DataZone ofrece una forma simplificada de buscar datos. Cualquier DataZone usuario de Amazon con permisos para acceder al portal de datos puede buscar activos en el DataZone catálogo de Amazon y ver los nombres de los activos y los metadatos que se les han asignado. Puedes ver más de cerca un activo examinando su página de detalles.

> **Note**
>
> Para ver los datos reales que contiene un activo, primero debe suscribirse al activo y solicitar que se apruebe su solicitud de suscripción y se le conceda el acceso. Para obtener más información, consulte Suscribirse a los datos.

Para buscar activos en el catálogo

1. Ve a la URL del portal de DataZone datos de Amazon e inicia sesión con el inicio de sesión único (SSO) o con tus credenciales. AWS Si eres DataZone administrador de Amazon, puedes ir a la DataZone consola de Amazon en https://console.aws.amazon.com/datazone e iniciar sesión con el Cuenta de AWS lugar donde se creó el dominio y, a continuación, elegir Open data portal.
2. Puedes escribir el nombre del activo que estás buscando en la barra de búsqueda de la página de inicio del portal de datos.
3. Para explorar los espacios de nombres, elija Catálogo en la parte superior derecha de la página para abrir el catálogo. El catálogo ofrece una experiencia de búsqueda multifacética para encontrar activos mediante la búsqueda en función de criterios como el propietario de los datos y los términos del glosario.
4. Introduzca el término de búsqueda en uno de los cuadros de búsqueda. Tras realizar una búsqueda, puede aplicar varios filtros para restringir los resultados. Los filtros incluyen el tipo de activo, la cuenta de origen y la cuenta a la que Región de AWS pertenece el activo.
5. Para ver los detalles de un activo específico, selecciónelo para abrir su página de detalles. La página de detalles incluye la siguiente información:

   - El nombre del activo, la fuente de datos (AWS Glue Amazon Redshift o Amazon S3), el tipo (tabla, vista u objeto de S3), el número de columnas y el tamaño.
   - Una descripción del activo.
   - La revisión actual publicada del activo, el propietario, si es necesaria la aprobación de las suscripciones, el nombre y el historial de actualizaciones.

- Una pestaña de descripción general que incluye términos del glosario y formularios de metadatos.
- Una pestaña de esquema que muestra el esquema del activo, incluidos los nombres de las columnas comerciales y técnicas, los tipos de datos y las descripciones comerciales de las columnas. La pestaña de esquema solo está visible para las tablas y vistas (no para los objetos de Amazon S3).
- Una pestaña de suscripciones que incluye una lista de suscriptores del dominio.
- Una pestaña de historial que incluye una lista de las revisiones anteriores del activo.

Suscribirse a los datos

Las siguientes tareas proporcionan detalles sobre la suscripción a activos en Amazon DataZone.

Temas

Solicita la suscripción a los activos

Amazon DataZone le permite encontrar, acceder y consumir los activos del DataZone catálogo de Amazon. Cuando encuentres un activo en el catálogo al que quieras acceder, tendrás que suscribirte al activo, lo que generará una solicitud de suscripción. A continuación, un aprobador podrá aprobar o solicitar tu solicitud.

Debe ser miembro de un proyecto para poder solicitar la suscripción a un activo de ese proyecto.

Para suscribirse a un activo

1. Ve a la URL del portal de DataZone datos de Amazon e inicia sesión con el inicio de sesión único (SSO) o con tus credenciales. AWS Si eres DataZone administrador de Amazon, puedes ir

a la DataZone consola de Amazon en https://console.aws.amazon.com/datazone e iniciar sesión con el Cuenta de AWS lugar donde se creó el dominio y, a continuación, elegir Open data portal.

2. Usa la barra de búsqueda para buscar y elegir el activo al que deseas suscribirte y, a continuación, selecciona Suscribirse.
3. En la ventana emergente Suscríbete, proporciona la siguiente información:
   - El proyecto al que desea suscribir al activo.
   - Una breve justificación de su solicitud de suscripción.
4. Elija Suscribirse.

   Recibirás una notificación en el portal de datos cuando el editor apruebe tu solicitud.

Para ver el estado de la solicitud de suscripción, busque y elija el proyecto con el que se suscribió al activo. Vaya a la pestaña Datos del proyecto y, a continuación, seleccione Datos solicitados en el panel de navegación izquierdo. En esta página se enumeran los activos a los que el proyecto ha solicitado acceso. Puede filtrar la lista por el estado de la solicitud.

Apruebe o rechace una solicitud de suscripción

Amazon DataZone le permite encontrar, acceder y consumir los activos del DataZone catálogo de Amazon. Cuando encuentres un activo en el catálogo al que quieras acceder, debes suscribirte al activo, lo que crea una solicitud de suscripción. A continuación, un aprobador podrá aprobar o rechazar la solicitud.

Debe ser miembro del proyecto propietario (el proyecto que publicó el activo) para aprobar o rechazar una solicitud de suscripción.

Para aprobar o rechazar una solicitud de suscripción

1. Ve a la URL del portal de DataZone datos de Amazon e inicia sesión con el inicio de sesión único (SSO) o con tus credenciales. AWS Si eres DataZone administrador de Amazon, puedes ir a la DataZone consola de Amazon en https://console.aws.amazon.com/datazone e iniciar sesión con el Cuenta de AWS lugar donde se creó el dominio y, a continuación, elegir Open data portal.
2. En el portal de datos, selecciona Explorar lista de proyectos y selecciona el proyecto que contiene el activo con la solicitud de suscripción.
3. Vaya a la pestaña Datos y, a continuación, seleccione Solicitudes entrantes en el panel de navegación izquierdo.

4. Busca la solicitud y selecciona Ver solicitud. Puedes filtrar por pendiente para ver solo las solicitudes que aún están abiertas.
5. Revisa la solicitud de suscripción y el motivo del acceso, y decide si la apruebas o la rechazas.
6. (Opcional) Escribe una respuesta que explique el motivo por el que aceptas o rechazas la solicitud.
7. Selecciona Aprobar o Rechazar.

Como propietario del proyecto, puedes revocar la suscripción en cualquier momento. Para obtener más información, consulte the section called “Revocar una suscripción existente”.

Para ver todas las solicitudes de suscripción, consulteTrabajar con DataZone eventos y notificaciones de Amazon.

Revocar una suscripción existente

Amazon DataZone le permite encontrar, acceder y consumir los activos del DataZone catálogo de Amazon. Cuando encuentres un activo en el catálogo al que quieras acceder, tendrás que suscribirte al activo, lo que generará una solicitud de suscripción. A continuación, un aprobador podrá aprobar o solicitar tu solicitud. Es posible que tengas que revocar una suscripción después de haberla aprobado, ya sea porque la aprobación fue un error o porque el suscriptor ya no necesita acceder al activo.

Debe ser miembro del proyecto propietario (el proyecto que publicó el activo) para revocar una suscripción.

Para revocar una suscripción

1. Ve a la URL del portal de DataZone datos de Amazon e inicia sesión con el inicio de sesión único (SSO) o con tus credenciales. AWS Si eres DataZone administrador de Amazon, puedes ir a la DataZone consola de Amazon en https://console.aws.amazon.com/datazone e iniciar sesión con el Cuenta de AWS lugar donde se creó el dominio y, a continuación, elegir Open data portal.
2. Selecciona Seleccionar proyecto en el panel de navegación superior y selecciona el proyecto que contiene la suscripción que quieres revocar.
3. Ve a la pestaña Datos y, a continuación, selecciona Solicitudes entrantes en el panel de navegación izquierdo.
4. Busca la suscripción que deseas revocar y selecciona Ver suscripción.

5. (Opcional) Active la casilla de verificación para permitir que el suscriptor mantenga el activo en los objetivos de suscripción del proyecto. Un objetivo de suscripción es una referencia a un conjunto de recursos en los que los datos suscritos pueden estar disponibles en un entorno.

   Si desea revocar el acceso al activo desde el destino de la suscripción más adelante, debe hacerlo en. AWS Lake Formation
6. Selecciona Revocar la suscripción.

No puedes volver a aprobar una suscripción después de haberla revocado. El suscriptor debe volver a suscribirse al activo para que tú lo apruebes.

Cancelar una solicitud de suscripción

Amazon DataZone le permite encontrar, acceder y consumir los activos del DataZone catálogo de Amazon. Cuando encuentres un activo en el catálogo al que quieras acceder, tendrás que suscribirte al activo, lo que generará una solicitud de suscripción. A continuación, un aprobador podrá aprobar o solicitar tu solicitud. Es posible que tengas que cancelar una solicitud de suscripción pendiente, ya sea porque la has enviado por error o porque ya no necesitas el acceso de lectura al recurso.

Para cancelar una solicitud de suscripción, debe ser propietario del proyecto o colaborador.

Para cancelar una solicitud de suscripción

1. Ve a la URL del portal de DataZone datos de Amazon e inicia sesión con el inicio de sesión único (SSO) o con tus credenciales. AWS Si eres DataZone administrador de Amazon, puedes ir a la DataZone consola de Amazon en https://console.aws.amazon.com/datazone e iniciar sesión con el Cuenta de AWS lugar donde se creó el dominio y, a continuación, elegir Open data portal.
2. Selecciona Seleccionar proyecto en el panel de navegación superior y selecciona el proyecto que contiene la solicitud de suscripción.
3. Vaya a la pestaña Datos del proyecto y, a continuación, seleccione Datos solicitados en el panel de navegación izquierdo. En esta página se enumeran los activos a los que el proyecto ha solicitado acceso.
4. Filtre por solicitado para ver solo las solicitudes que aún están pendientes. Busca la solicitud y selecciona Ver solicitud.
5. Revisa la solicitud de suscripción y selecciona Cancelar solicitud.

Si desea volver a suscribirse al activo (o a otro activo), consultethe section called “Solicita la suscripción a los activos”.

Darse de baja de un activo

Amazon DataZone le permite encontrar, acceder y consumir los activos del DataZone catálogo de Amazon. Cuando encuentres un activo en el catálogo al que quieras acceder, tendrás que suscribirte al activo, lo que generará una solicitud de suscripción. A continuación, un aprobador podrá aprobar o solicitar tu solicitud. Es posible que tengas que darte de baja de un recurso, ya sea porque te suscribiste por error y te aprobaron, o porque ya no necesitas el acceso de lectura al activo.

Debe ser miembro de un proyecto para darse de baja de uno de sus activos.

Para cancelar la suscripción a un activo

1. Ve a la URL del portal de DataZone datos de Amazon e inicia sesión con el inicio de sesión único (SSO) o con tus credenciales. AWS Si eres DataZone administrador de Amazon, puedes ir a la DataZone consola de Amazon en https://console.aws.amazon.com/datazone e iniciar sesión con el Cuenta de AWS lugar donde se creó el dominio y, a continuación, elegir Open data portal.
2. Selecciona Seleccionar proyecto en el panel de navegación superior y selecciona el proyecto que contiene el activo del que quieres darte de baja.
3. Vaya a la pestaña Datos del proyecto y, a continuación, seleccione Datos solicitados en el panel de navegación izquierdo. En esta página se enumeran los activos a los que el proyecto ha solicitado acceso.
4. Filtre por aprobados para ver solo las solicitudes que se han aprobado. Busca la solicitud y selecciona Ver suscripción.
5. Revisa la suscripción y selecciona Cancelar suscripción.

Si desea volver a suscribirse al activo (o a otro activo), consultethe section called “Solicita la suscripción a los activos”.

Uso de las funciones de IAM existentes para gestionar las suscripciones de Amazon DataZone

En la versión actual, Amazon le DataZone ayuda a utilizar sus funciones de IAM actuales para acceder a los datos. Para lograrlo, puedes crear un objetivo de suscripción en el DataZone entorno

de Amazon que utilices para gestionar tu suscripción. Para crear un objetivo de suscripción para un entorno en una de las AWS cuentas asociadas, puedes seguir los siguientes pasos:

Paso 1: Asegúrese de que su DataZone dominio de Amazon utilice la versión 2 o superior de la política de RAM

1. Ve a la página Compartido por mí: Recursos compartidos en la consola AWS RAM.
2. Dado que los recursos de AWS RAM se comparten en AWS regiones específicas, selecciona la AWS región correspondiente en la lista desplegable situada en la esquina superior derecha de la consola.
3. Selecciona el recurso compartido correspondiente a tu DataZone dominio de Amazon y, a continuación, selecciona Modificar. Puede identificar el recurso compartido de RAM del DataZone dominio de Amazon mediante el nombre o el ID del dominio, ya que el recurso compartido de RAM se crea con el nombre:`DataZone-<domain-name>-<domain-id>`.
4. Seleccione Siguiente para continuar con el siguiente paso, en el que podrá comprobar la versión de la política de RAM y modificarla.
5. Asegúrese de que la versión de la política de RAM sea la versión 2 o superior. Si no es así, usa el menú desplegable para seleccionar la versión 2 o superior.
6. Selecciona Saltar al paso 4: Revisar y actualizar.
7. Selecciona Actualizar recurso compartido.

Paso 2: Cree un objetivo de suscripción a partir de una cuenta asociada

- En la versión actual, Amazon DataZone admite la creación de objetivos de suscripción únicamente mediante API. A continuación, se muestran algunos ejemplos de la carga útil que puede utilizar para crear un objetivo de suscripción para gestionar las suscripciones a sus tablas o vistas de AWS Glue y Amazon Redshift. Para obtener más información, consulte. CreateSubscriptionTarget

  Ejemplo de objetivo de suscripción para 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"
}
```

Ejemplo de objetivo de suscripción para 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

- El EnvironmentIdentifier que utilice en la llamada a la API anterior debe estar en la misma cuenta asociada desde la que realiza la llamada a la API. De lo contrario, la llamada a la API no se realizará correctamente.
- La función de IAM (ARN) que utilizas en «AuthorizedPrincipals» es la función a la que DataZone Amazon concederá acceso una vez que se añada un activo suscrito al objetivo de la suscripción. Estos directores autorizados deben pertenecer a la misma cuenta que el entorno en el que se está creando el objetivo de la suscripción.

- El valor del campo del proveedor debe ser «Amazon DataZone» para DataZone que Amazon pueda completar la gestión logística de la suscripción.
- El nombre de la base de datos proporcionado ya subscriptionTargetConfig debería existir en la cuenta en la que se está creando el destino. Amazon no DataZone creará esta base de datos. Asegúrese también de que la función de administración de acceso tenga el permiso CREATE TABLE en esta base de datos.
- Asegúrese también de que las funciones (la función de IAM para AWS Glue y la función de base de datos para Amazon Redshift) que se proporcionan como entidades principales autorizadas ya existan en la cuenta del entorno. En el caso de los destinos de suscripción a Amazon Redshift, se requieren actualizaciones adicionales para que la función que se asuma al conectarse al clúster. Esta función debe tener una RedshiftDbRoles etiqueta adjunta a la función. El valor de la etiqueta puede ser una lista separada por comas. El valor debe ser la función de base de datos que se proporcionó como principal autorizado al crear el destino de la suscripción.

Paso 3: Suscríbase a una tabla nueva y complete la suscripción al nuevo objetivo

- Una vez que hayas creado el objetivo de suscripción, puedes suscribirte a una nueva tabla y Amazon lo DataZone cumplirá con el objetivo anterior. Para obtener más información, consulte Suscribirse a los datos.

Otorgar acceso a los datos

Las siguientes tareas proporcionan detalles sobre la concesión de acceso a las suscripciones aprobadas a los activos de Amazon DataZone.

En Amazon DataZone, los aprobadores de suscripciones gestionan las solicitudes de suscripción y las suscripciones aprobadas o concedidas para el acceso de lectura a los activos. El aprobador de la suscripción de un activo viene determinado por el acuerdo de publicación con el que se publicó este activo en el DataZone catálogo de Amazon.

Temas

Conceda acceso a los activos gestionados AWS Glue Data Catalog

> **Note**
>
> No se admite la administración del acceso a AWS Glue Data Catalog los activos mediante el método AWS Lake Formation LF-TBAC.
> No se admite el uso compartido de AWS Glue Data Catalog activos entre regiones.

Una vez que se aprueba una solicitud de suscripción a AWS Glue Data Catalog los activos gestionados, Amazon añade DataZone automáticamente estos activos a todos los entornos de lagos de datos existentes en el proyecto. DataZone A continuación, Amazon concede y gestiona el acceso a las AWS Glue Data Catalog tablas aprobadas en tu nombre a través de AWS Lake Formation. En el caso del proyecto de suscriptor, los activos que se conceden aparecen AWS Glue Data Catalog como recursos en tu cuenta. A continuación, puede utilizar Amazon Athena para consultar las tablas.

> **Note**
>
> Si se agrega un nuevo entorno de lago de datos al proyecto después de que los AWS Glue Data Catalog activos suscritos se hayan agregado automáticamente a los entornos de lago de datos existentes, tendrá que agregar manualmente estos AWS Glue Data Catalog activos suscritos a este nuevo entorno de lago de datos. Para ello, selecciona la opción Añadir subvención en la pestaña Datos de la página de resumen del proyecto en el portal de DataZone datos de Amazon.

Para DataZone que Amazon pueda conceder acceso a las tablas del catálogo de datos de AWS Glue, se deben cumplir las siguientes condiciones.

- La mesa AWS Glue debe estar gestionada por Lake Formation, ya que Amazon DataZone concede el acceso gestionando los permisos de Lake Formation.
- La función Administrar acceso al entorno del lago de datos utilizada para publicar la tabla del catálogo de datos de AWS Glue debe tener los siguientes permisos de Lake Formation:
  - `DESCRIBE`y `DESCRIBE GRANTABLE` permisos en la base de datos de AWS Glue que contiene la tabla publicada.
  - `DESCRIBE`,`SELECT`,`DESCRIBE GRANTABLE`, `SELECT GRANTABLE` permisos en Lake Formation en la propia tabla publicada.

Para obtener más información, consulte Concesión y revocación de permisos sobre los recursos del catálogo en la Guía para AWS Lake Formation desarrolladores.

Conceder acceso a los activos gestionados de Amazon Redshift

Cuando se aprueba una suscripción a una tabla o vista de Amazon Redshift, Amazon DataZone puede añadir automáticamente el activo suscrito a todos los entornos de almacenamiento de datos del proyecto, de modo que los miembros del proyecto puedan consultar los datos mediante el enlace del editor de consultas de Amazon Redshift dentro de sus entornos. Bajo el capó DataZone, Amazon crea las concesiones y los datos compartidos necesarios entre la fuente y el destino de la suscripción.

El proceso de concesión del acceso varía según la ubicación de la base de datos de origen (editor) y de la base de datos de destino (suscriptor).

- El mismo clúster, la misma base de datos: si los datos deben compartirse dentro de la misma base de datos, Amazon DataZone concede los permisos directamente en la tabla de origen.
- Mismo clúster, base de datos diferente: si los datos deben compartirse entre dos bases de datos del mismo clúster, Amazon DataZone crea una vista en la base de datos de destino y se conceden permisos en la vista creada.
- Clúster diferente de la misma cuenta: Amazon DataZone crea un recurso compartido de datos entre el clúster de origen y el de destino y crea una vista en la parte superior de la tabla compartida. Los permisos se conceden en la vista.
- Entre cuentas: igual que en el caso anterior, pero se requiere un paso adicional para autorizar el intercambio de datos entre cuentas por parte del clúster de productores y otro paso para asociar el intercambio de datos por parte del clúster de consumidores.

> **Note**
>
> Si se agrega un nuevo entorno de almacenamiento de datos al proyecto después de que los activos de Amazon Redshift suscritos se hayan agregado automáticamente a los entornos de almacenamiento de datos existentes, tendrá que agregar manualmente estos activos de Amazon Redshift suscritos a este nuevo entorno de almacenamiento de datos. Para ello, selecciona la opción Añadir subvención en la pestaña Datos de la página de resumen del proyecto en el portal de DataZone datos de Amazon.

Asegúrese de que los clústeres de Amazon Redshift que publica y se suscribe cumplen todos los requisitos de los datos compartidos de Amazon Redshift. Para obtener más información, consulte la Guía para desarrolladores de Amazon Redshift.

> **Note**
>
> Amazon DataZone admite la concesión automática de suscripciones a los activos de Amazon Redshift Cluster y Amazon Redshift Serverless.
> No se admite el intercambio de datos entre regiones mediante Amazon Redshift.

> **Note**
>
> En la versión actual, Amazon solo DataZone puede gestionar el acceso a las tablas y vistas de Amazon Redshift si los clústeres o grupos de trabajo de Amazon Redshift de origen y destino se encuentran en las cuentas que pertenecen a AWS la misma organización. AWS

Conceda acceso a los activos no gestionados para las suscripciones aprobadas

Amazon DataZone permite a los usuarios publicar cualquier tipo de activo en el catálogo de datos empresariales. Para algunos de estos activos, Amazon DataZone puede gestionar automáticamente las concesiones de acceso. Estos activos se denominan activos gestionados e incluyen tablas del catálogo de datos de AWS Glue gestionado por Lake Formation y tablas y vistas de Amazon Redshift. Todos los demás activos a los que Amazon no DataZone puede conceder suscripciones automáticamente se denominan no gestionados.

Amazon te DataZone proporciona una ruta para gestionar las concesiones de acceso a tus activos no gestionados. Cuando el propietario de los datos aprueba una suscripción a un activo del catálogo de datos empresariales, Amazon DataZone publica un evento en Amazon EventBridge en tu cuenta junto con toda la información necesaria en la carga útil que te permite crear las concesiones de acceso entre el origen y el destino. Cuando recibas este evento, puedes activar un controlador personalizado que puede usar la información del evento para crear las concesiones o permisos necesarios. Una vez que hayas concedido el acceso, puedes informar y actualizar el estado de la suscripción en Amazon DataZone para que notifique a los usuarios que se suscribieron al activo

que pueden empezar a consumirlo. Para obtener más información, consulte Trabajar con DataZone eventos y notificaciones de Amazon.

Consumir datos

Las siguientes tareas proporcionan detalles sobre el consumo de datos a los que te has suscrito en Amazon DataZone.

Temas

- Consulte datos en Amazon Athena o Amazon Redshift

Consulte datos en Amazon Athena o Amazon Redshift

En Amazon DataZone, una vez que un suscriptor tiene acceso a un activo del catálogo, puede consumirlo (consultarlo y analizarlo) con Amazon Athena o el editor de consultas Amazon Redshift v2. Debe ser propietario o colaborador del proyecto para completar esta tarea. Según los planos habilitados en el proyecto, Amazon DataZone proporciona enlaces a Amazon Athena o al editor de consultas Amazon Redshift v2 en el panel lateral derecho de la página del proyecto en el portal de datos.

1. Ve a la URL del portal de DataZone datos de Amazon e inicia sesión con el inicio de sesión único (SSO) o con tus credenciales. AWS Si eres DataZone administrador de Amazon, puedes ir a la DataZone consola de Amazon en https://console.aws.amazon.com/datazone e iniciar sesión con el Cuenta de AWS lugar donde se creó el dominio y, a continuación, elegir Open data portal.
2. En el portal de DataZone datos de Amazon, elija Examinar lista de proyectos y, a continuación, busque y elija el proyecto en el que tiene los datos que desea analizar.
3. Si el blueprint de Data Lake está activado en este proyecto, aparecerá un enlace a Amazon Athena en el panel lateral derecho de la página de inicio del proyecto.

   Si el esquema del almacén de datos está activado en este proyecto, aparecerá un enlace al editor de consultas en el panel lateral derecho de la página de inicio del proyecto.

   > **Note**
   >
   > Los planos se definen en el perfil de entorno con el que se crea un proyecto.

Temas

- Consulte datos con Amazon Athena
- Consulte datos con Amazon Redshift

Consulte datos con Amazon Athena

Elija el enlace Amazon Athena para abrir el editor de consultas de Amazon Athena en una nueva pestaña del navegador con las credenciales del proyecto para la autenticación. El DataZone proyecto de Amazon con el que estás trabajando se selecciona automáticamente como grupo de trabajo actual en el editor de consultas.

En el editor de consultas de Amazon Athena, escriba y ejecute sus consultas. Algunas de las tareas más comunes incluyen:

- Consulte y analice sus activos suscritos
- Crea tablas nuevas
- Cree una tabla a partir de los resultados de una consulta (CTAS) desde un bucket de S3 externo

Consulte y analice sus activos suscritos

Si Amazon no concede automáticamente el acceso a los activos a los que está suscrito tu proyecto DataZone, debes estar autorizado a acceder a los datos subyacentes. Para obtener más información sobre cómo conceder acceso a estos activos, consulteConceda acceso a los activos no gestionados para las suscripciones aprobadas.

Si Amazon concede automáticamente el acceso a los activos a los que está suscrito su proyecto DataZone, puede ejecutar consultas SQL en las tablas y ver los resultados en Amazon Athena. Para obtener más información sobre el uso de SQL en Amazon Athena, consulte la referencia de SQL para Athena.

Cuando navega hasta el editor de consultas de Amazon Athena después de elegir el enlace de Amazon Athena en el panel lateral derecho de la página de inicio del proyecto, aparece un menú desplegable de proyectos en la esquina superior derecha del editor de consultas de Amazon Athena y se selecciona automáticamente el contexto del proyecto.

Puede ver las siguientes bases de datos en el menú desplegable Base de datos:

- Una base de datos de publicación (*{environmentname}*_pub_db). El objetivo de esta base de datos es proporcionarte un entorno en el que puedas generar nuevos datos en el contexto de tu proyecto y luego poder publicarlos en el DataZone catálogo de Amazon. Los propietarios y colaboradores del proyecto tienen acceso de lectura y escritura a esta base de datos. Los espectadores del proyecto solo tienen acceso de lectura a esta base de datos.
- Una base de datos de suscripciones (*{environmentname}*_sub_db). El objetivo de esta base de datos es compartir contigo los datos a los que te has suscrito como miembro del proyecto en el DataZone catálogo de Amazon y permitirte consultarlos.

Crea tablas nuevas

Si se ha conectado a un bucket de S3 externo, puede utilizar Amazon Athena para consultar y analizar los activos de un bucket de Amazon S3 externo. En este escenario, Amazon DataZone no tiene permisos para conceder acceso directamente a los datos subyacentes del bucket externo de Amazon S3, y los datos externos de Amazon S3 creados fuera del proyecto no se gestionan automáticamente en Lake Formation y Amazon no puede gestionarlos DataZone. Una alternativa es copiar los datos del bucket de Amazon S3 externo a una nueva tabla dentro del bucket de Amazon S3 del proyecto mediante una `CREATE TABLE` declaración en Amazon Athena. Cuando ejecuta una `CREATE TABLE` consulta en Amazon Athena, registra la tabla con. AWS Glue Data Catalog

Para especificar la ruta a los datos en Amazon S3, utilice la propiedad `LOCATION`, como se muestra en el ejemplo siguiente:

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

Para obtener más información, consulte Ubicación de la tabla en Amazon S3.

Cree una tabla a partir de los resultados de una consulta (CTAS) desde un bucket de S3 externo

Al suscribirse a un activo, el acceso a los datos subyacentes es de solo lectura. Puede usar Amazon Athena para crear una copia de la tabla. En Amazon Athena, `A CREATE TABLE AS SELECT`

(CTAS) query crea una nueva tabla en Amazon Athena a partir de los resultados de SELECT una declaración de otra consulta. Para obtener información sobre la sintaxis de las CTAS, consulte CREATE TABLE AS.

En el siguiente ejemplo se crea una tabla copiando todas las columnas de una tabla:

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

En la siguiente variante del ejemplo anterior, la instrucción SELECT incluye también una cláusula WHERE. En este caso, la consulta solo selecciona las filas de la tabla que satisfacen la cláusula WHERE:

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

En el siguiente ejemplo se crea una nueva consulta que se ejecuta en un conjunto de columnas de otra tabla:

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

Esta variante del mismo ejemplo crea una nueva tabla a partir de columnas específicas de varias tablas:

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

Estas tablas recién creadas ahora forman parte de la AWS Glue base de datos de tus proyectos y otras personas pueden descubrirlas y compartirlas con otros DataZone proyectos de Amazon publicando los datos como un activo en el catálogo de Amazon DataZone.

Consulte datos con Amazon Redshift

En el portal de DataZone datos de Amazon, abra un entorno que utilice el modelo de almacén de datos. Elija el enlace Amazon Redshift en el panel derecho de la página del entorno. Se abrirá un cuadro de diálogo de confirmación con los detalles necesarios que le ayudarán a establecer una conexión con el clúster de Amazon Redshift o el grupo de trabajo Amazon Redshift Serverless de su entorno en el editor de consultas de Amazon Redshift v2.0. Una vez que haya identificado los detalles necesarios para establecer la conexión, pulse el botón Abrir Amazon Redshift. Esto abre el editor de consultas Amazon Redshift v2.0 en una nueva pestaña del navegador con las credenciales temporales del entorno de Amazon. DataZone

En el editor de consultas, siga los pasos que se indican a continuación en función de si su entorno utiliza un grupo de trabajo Amazon Redshift Serverless o un clúster de Amazon Redshift.

Para un grupo de trabajo sin servidor de Amazon Redshift

1. En el editor de consultas, identifique el grupo de trabajo Amazon Redshift Serverless de su DataZone entorno de Amazon, haga clic con el botón derecho en él y elija Create a connection.
2. Elija Usuario federado para la autenticación.
3. Proporcione el nombre de la base de datos del DataZone entorno de Amazon.
4. Seleccione Crear conexión.

Para un clúster de Amazon Redshift:

1. En el editor de consultas, identifique el clúster Amazon Redshift de su DataZone entorno de Amazon, haga clic con el botón derecho en él y elija Create a connection.
2. Seleccione Credenciales temporales con su identidad de IAM para la autenticación.
3. Si el método de autenticación anterior no está disponible, abra la configuración de la cuenta pulsando el botón con forma de engranaje situado en la esquina inferior izquierda, seleccione Autenticar con credenciales de IAM y guarde. Se trata de una configuración one-time-only.
4. Proporcione el nombre de la base de datos del DataZone entorno de Amazon para crear la conexión.
5. Seleccione Crear conexión.

Ahora puede empezar a realizar consultas en las tablas y vistas del clúster de Amazon Redshift o del grupo de trabajo Amazon Redshift Serverless configurado para su entorno de Amazon. DataZone

Todas las tablas o vistas de Amazon Redshift a las que se haya suscrito están vinculadas al clúster de Amazon Redshift o al grupo de trabajo Amazon Redshift Serverless configurado para el entorno. Puede suscribirse a las tablas y vistas, así como publicar las tablas y vistas nuevas que cree en el clúster o la base de datos de su entorno.

Por ejemplo, tomemos un escenario en el que un entorno está vinculado a un clúster de Amazon Redshift llamado `redshift-cluster-1` y a una base de datos llamada `dev` en ese clúster. Con el portal de DataZone datos de Amazon, puede consultar las tablas y vistas que se añaden a su entorno. En la `Analytics tools` sección del panel lateral derecho del portal de datos, puede elegir el enlace Amazon Redshift para este entorno, que abre el editor de consultas. A continuación, puede hacer clic con el botón derecho en el `redshift-cluster-1` clúster y crear una conexión con credenciales temporales con su identidad de IAM. Una vez establecida la conexión, podrá ver todas las tablas y vistas a las que tiene acceso su entorno en la base de datos de desarrollo.

Trabajar con DataZone eventos y notificaciones de Amazon

Amazon lo DataZone mantiene informado de las actividades importantes de su portal de datos, como las solicitudes de suscripción, las actualizaciones, los comentarios y los eventos del sistema. Amazon te DataZone proporciona esta información mediante la entrega de los mensajes en la bandeja de entrada específica del portal de datos o a través del bus EventBridge predeterminado de Amazon.

Temas

Cómo trabajar con los eventos a través de la bandeja de entrada específica del portal de DataZone datos de Amazon

Amazon DataZone proporciona una bandeja de entrada específica en el portal de datos donde puedes ver tus mensajes y tomar medidas al respecto. Los mensajes recientes también aparecen en la página de inicio, la página del proyecto y la página del catálogo. Por ejemplo, si un usuario solicita acceso a un activo de datos, los propietarios del proyecto de publicación y los contribuyentes de ese activo ven la solicitud en el portal de datos y, una vez que se realiza una acción, los miembros del proyecto suscriptor relacionado con esta solicitud ven la notificación en el portal de datos. Hay dos tipos de mensajes:

- Tareas: estos mensajes informan al destinatario de que es necesario realizar alguna acción en algún lugar. Tienen un campo de estado opcional que puedes usar para realizar el seguimiento.
- Eventos: estos mensajes son informativos y no tienen ningún estado asignado. Los eventos proporcionan un registro de auditoría de las actualizaciones recientes.

En Amazon DataZone, los mensajes se generan para los siguientes tipos de eventos:

Categoría de evento	Nombre de evento	Descripción del evento	Tipo de evento
Suscripción	Se ha creado una solicitud de suscripción	El evento se genera cuando se crea una solicitud de suscripción	Tarea
Suscripción	Solicitud de suscripción aceptada	El evento se genera cuando se acepta una solicitud de suscripción	Evento
Suscripción	Solicitud de suscripción rechazada	El evento se genera cuando se rechaza una solicitud de suscripción	Evento
Suscripción	Se ha eliminado la solicitud de suscripción	El evento se genera cuando se elimina una solicitud de suscripción	Evento
Proyecto	La creación del proyecto se realizó correctamente	El evento se genera cuando la creación del proyecto se realiza correctamente	Evento
Pertenencia al proyecto	La adición de miembros del proyecto se realizó correctamente	El evento se genera cuando se agrega un nuevo miembro a un proyecto	Evento
Pertenencia al proyecto	La eliminación del miembro del proyecto se realizó correctamente	El evento se genera cuando se elimina un miembro de un proyecto	Evento

Categoría de evento	Nombre de evento	Descripción del evento	Tipo de evento
Pertenencia al proyecto	El cambio de rol del miembro del proyecto se realizó correctam ente	Se genera un evento, se cambia el rol de un miembro en el proyecto	Evento
Entorno	Se inició el despliegue del entorno	El evento se genera cuando se inicia la implementación de un entorno	Evento
Entorno	Se completó el despliegue del entorno	El evento se genera cuando la implementación de un entorno se completa correctamente	Evento
Entorno	Falló la implement ación del entorno	El evento se genera cuando se produce un error en la implement ación de un entorno	Evento
Entorno	Se inicia un flujo de trabajo personalizado de implementación del entorno	El evento se genera cuando se inicia un entorno con un flujo de trabajo personali zado	Evento
Activo de datos	Activo agregado al inventario	El evento se genera cuando se agrega un nuevo activo de datos al inventario, es decir, se agrega al catálogo en estado de borrador	Evento

Categoría de evento	Nombre de evento	Descripción del evento	Tipo de evento
Activo de datos	Activo publicado	El evento se genera cuando se publica un nuevo activo de datos, es decir, está disponible para su suscripción	Evento
Activo de datos	El esquema de activos ha cambiado	El evento se genera cuando el esquema de un activo ha cambiado desde el trabajo de ingestión anterior	Evento
Suscripción	Suscripción creada	El evento se genera cuando alguien solicita suscribirse a un activo de datos	Tarea
Suscripción	Suscripción aprobada	El evento se genera cuando el propietario o el colaborador del proyecto de publicación aprueba una suscripción	Evento
Suscripción	Suscripción rechazada	El evento se genera cuando el propietario o el colaborador del proyecto publicador rechaza una suscripción	Evento

Categoría de evento	Nombre de evento	Descripción del evento	Tipo de evento
Suscripción	Se ha eliminado la suscripción	El evento se genera cuando el suscriptor cancela una suscripción	Evento
Suscripción	Se solicita una concesión de suscripción	El evento se genera cuando alguien solicita acceso a un activo	Evento
Suscripción	Concesión de suscripción completada	El evento se genera cuando el propietario o colaborador del proyecto publicador concede acceso al activo a una suscripción	Evento
Suscripción	Falló la concesión de la suscripción	El evento se genera cuando se produce un error en la concesión de una suscripción	Evento
Suscripción	Se solicita la revocación de la subvención de suscripción	El evento se genera cuando el propietario o el colaborador del proyecto publicador inicia una concesión de suscripción revocada	Evento

Categoría de evento	Nombre de evento	Descripción del evento	Tipo de evento
Suscripción	Se ha completad o la revocación de la subvención de suscripción	El evento se genera cuando se completa la revocación de una subvención de suscripción	Evento
Suscripción	Falló la revocación de la concesión de la suscripción	El evento se genera cuando se produce un error en la revocación de una concesión de suscripción	Evento
Generación automatiz ada de nombres comerciales	El nombre de la empresa se generó correctamente	El evento se genera cuando el trabajo generado automátic amente por el nombre de la empresa se completa correctam ente	Evento
Generación automátic a de nombres comerciales	Error al generar el nombre de la empresa	El evento se genera cuando se produce un error en el trabajo generado automátic amente por el nombre de la empresa	Evento
Se ejecutó la fuente de datos	Fuente de datos creada	El evento se genera cuando se crea una nueva fuente de datos	Evento
La fuente de datos se ejecutó	Fuente de datos actualizada	El evento se genera cuando se actualiza una fuente de datos existente	Evento

Categoría de evento	Nombre de evento	Descripción del evento	Tipo de evento
Se ejecutó la fuente de datos	Se activó la ejecución de la fuente de	El evento se genera cuando se inicia la ejecución de una fuente de datos	Evento
Ejecución de la fuente de datos	La fuente de datos se ejecutó correctamente	El evento se genera cuando la ejecución de una fuente de datos se ejecuta correctamente	Evento
Ejecución de la fuente de datos	Falló la ejecución de la fuente de datos	El evento se genera cuando se produce un error al ejecutar una fuente de datos	Evento

Para ver las tareas en la bandeja de entrada del portal de datos, complete los siguientes pasos:

1. Navegue al portal de DataZone datos de Amazon mediante la URL del portal de datos e inicie sesión con su SSO o sus AWS credenciales. Si eres DataZone administrador de Amazon, puedes obtener la URL del portal de datos accediendo a la DataZone consola de Amazon en https://console.aws.amazon.com/datazone en la AWS cuenta en la que se creó el DataZone dominio de Amazon.
2. En el portal de datos, para ver una ventana emergente con el conjunto de tareas recientes, selecciona el icono de campana situado junto a la barra de búsqueda.
3. Seleccione Ver todo para ver todas las tareas. Puede cambiar las vistas y ver todos los eventos seleccionando la pestaña Eventos.
4. Puede filtrar la búsqueda por el asunto del evento, el estado activo o inactivo o el intervalo de fechas.
5. Elija una tarea individual para ir a la ubicación en la que puede responder a la tarea.

Para ver los eventos en la bandeja de entrada de su portal de datos, complete los siguientes pasos:

1. Navegue al portal de DataZone datos de Amazon mediante la URL del portal de datos e inicie sesión con su SSO o sus AWS credenciales. Si es DataZone administrador de Amazon, puede obtener la URL del portal de datos accediendo a la DataZone consola de Amazon en https://console.aws.amazon.com/datazone en la AWS cuenta en la que se creó el dominio DataZone raíz de Amazon.
2. En el portal de datos, para ver la ventana emergente del conjunto de eventos recientes, selecciona el icono de campana situado junto a la barra de búsqueda.
3. Seleccione Ver todo para ver todos los eventos. Puede cambiar las vistas y ver todas las tareas seleccionando la pestaña Tareas.
4. Filtra la búsqueda por tema o rango de fechas del evento.
5. Elige un evento individual para ir a la ubicación en la que puedes ver los detalles de ese evento.

Trabajar con eventos a través del bus EventBridge predeterminado de Amazon

Además de enviar mensajes a tu bandeja de entrada específica en el portal de datos, DataZone también envía estos mensajes a tu bus de eventos EventBridge predeterminado de Amazon en la misma AWS cuenta en la que está alojado tu dominio DataZone raíz de Amazon. Esto permite la automatización basada en eventos, como la gestión de suscripciones o las integraciones personalizadas con otras herramientas. Puedes crear reglas que coincidan con EventBridge los eventos entrantes de Amazon y enviarlos a Amazon EventBridge Targets para su procesamiento. Una sola regla puede enviar un evento a varios destinos, que luego pueden ejecutarse en paralelo.

Este es un ejemplo de evento:

```
{
  "version": "0",
  "id": "bd3d6239-2877-f464-0572-b1d76760e085",
  "detail-type": "Subscription Request Created",
  "source": "aws.datazone",
  "account": "111111111111",
  "time": "2023-11-13T17:57:00Z",
  "region": "us-east-1",
  "resources": [],
  "detail": {
    "version": "655",
```

```
    "metadata": {
      "domain": "dzd_bc8e1ez8r2a6xz",
      "user": "44f864b8-50a1-70cc-736f-c1f763934ab7",
      "id": "5jbc0lie0sr99j",
      "version": "1",
      "typeName": "SubscriptionRequestEntityType",
      "owningProjectId": "6oy92hwk937pgn",
      "awsAccountId": "111111111111",
      "clientToken": "e781b7b5-78c5-4608-961e-3792a6c3ff0d"
    },
    "data": {
      "autoApproved": true,
      "requesterId": "44f864b8-50a1-70cc-736f-c1f763934ab7",
      "status": "PENDING",
      "subscribedListings": [
        {
          "id": "ayzstznnx4dxyf",
          "ownerProjectId": "5a3se66qm88947",
          "version": "12"
        }
      ],
      "subscribedPrincipals": [
        {
          "id": "6oy92hwk937pgn",
          "type": "PROJECT"
        }
      ]
    }
  }
}
```


La lista completa de tipos de detalles admitidos por Amazon DataZone incluye:

- Solicitud de suscripción creada
- Solicitud de suscripción aceptada
- Solicitud de suscripción rechazada
- Solicitud de suscripción eliminada
- Se ha solicitado una subvención de suscripción
- Concesión de suscripción completada
- Falló la concesión de la suscripción

- Se solicitó la revocación de la concesión de la suscripción
- Se ha completado la revocación de la subvención de suscripción
- Falló la revocación de la concesión de la suscripción
- Activo agregado al inventario
- Activo agregado al catálogo
- El esquema de activos ha cambiado
- Cambio de estado de la fuente de datos
- Fuente de datos creada
- Fuente de datos actualizada
- Se activa la ejecución de la fuente de datos
- La ejecución de la fuente de datos fue correcta
- Falló la ejecución de la fuente de datos
- La creación del dominio se realizó correctamente
- No se pudo crear el dominio
- La eliminación del dominio se realizó correctamente
- No se pudo eliminar el dominio
- Se inició el despliegue del entorno
- Se completó el despliegue del entorno
- Falló la implementación del entorno
- Se inició la eliminación del entorno
- Se completó la eliminación del entorno
- Falló la eliminación del entorno
- La creación del proyecto se realizó correctamente
- La adición de miembros del proyecto se realizó correctamente
- La eliminación del miembro del proyecto se realizó correctamente
- El cambio de rol del miembro del proyecto se realizó correctamente
- Implementación del entorno: se inició el flujo de trabajo
- La generación del nombre de la empresa tuvo éxito
- No se pudo generar el nombre de la empresa

Para obtener más información, consulta Amazon EventBridge.

Seguridad en Amazon DataZone

La seguridad en la nube AWS es la máxima prioridad. Como AWS cliente, usted se beneficia de los centros de datos y las arquitecturas de red diseñados para cumplir con los requisitos de las organizaciones más sensibles a la seguridad.

La seguridad es una responsabilidad compartida entre AWS usted y usted. El modelo de responsabilidad compartida la describe como seguridad de la nube y seguridad en la nube:

- Seguridad de la nube: AWS es responsable de proteger la infraestructura que ejecuta AWS los servicios en la Nube de AWS. AWS también le proporciona servicios que puede utilizar de forma segura. Los auditores externos prueban y verifican periódicamente la eficacia de nuestra seguridad como parte de los AWS programas de de . Para obtener más información sobre los programas de conformidad que se aplican a Amazon DataZone, consulta AWS Servicios en el ámbito de aplicación por programa de conformidad AWS .
- Seguridad en la nube: tu responsabilidad viene determinada por el AWS servicio que utilices. Usted también es responsable de otros factores, incluida la confidencialidad de los datos, los requisitos de la empresa y la legislación y los reglamentos aplicables.

Esta documentación te ayuda a entender cómo aplicar el modelo de responsabilidad compartida cuando utilizas Amazon DataZone. En los temas siguientes, se muestra cómo configurar Amazon DataZone para que cumpla con sus objetivos de seguridad y conformidad. También aprenderás a usar otros AWS servicios que te ayudan a monitorear y proteger tus DataZone recursos de Amazon.

Temas

Protección de datos en Amazon DataZone

El AWS modelo de se aplica a protección de datos en Amazon DataZone. Como se describe en este modelo, AWS es responsable de proteger la infraestructura global en la que se ejecutan todos los Nube de AWS. Usted es responsable de mantener el control sobre el contenido alojado en esta infraestructura. Usted también es responsable de las tareas de administración y configuración de seguridad para los Servicios de AWS que utiliza. Para obtener más información sobre la privacidad de los datos, consulte las Preguntas frecuentes sobre la privacidad de datos. Para obtener información sobre la protección de datos en Europa, consulte la publicación de blog sobre el Modelo de responsabilidad compartida de AWS y GDPR en el Blog de seguridad de AWS .

Con fines de protección de datos, le recomendamos que proteja Cuenta de AWS las credenciales y configure los usuarios individuales con AWS IAM Identity Center o AWS Identity and Access Management (IAM). De esta manera, solo se otorgan a cada usuario los permisos necesarios para cumplir sus obligaciones laborales. También recomendamos proteger sus datos de la siguiente manera:

- Utilice la autenticación multifactor (MFA) en cada cuenta.
- Utilice SSL/TLS para comunicarse con los recursos. AWS Se recomienda el uso de TLS 1.2 y recomendamos TLS 1.3.
- Configure la API y el registro de actividad de los usuarios con. AWS CloudTrail
- Utilice soluciones de AWS cifrado, junto con todos los controles de seguridad predeterminados Servicios de AWS.
- Utilice servicios de seguridad administrados avanzados, como Amazon Macie, que lo ayuden a detectar y proteger los datos confidenciales almacenados en Amazon S3.
- Si necesita módulos criptográficos validados por FIPS 140-2 para acceder a AWS través de una interfaz de línea de comandos o una API, utilice un punto final FIPS. Para obtener más información sobre los puntos de conexión de FIPS disponibles, consulte Estándar de procesamiento de la información federal (FIPS) 140-2.

Se recomienda encarecidamente no introducir nunca información confidencial o sensible, como, por ejemplo, direcciones de correo electrónico de clientes, en etiquetas o campos de formato libre, tales como el campo Nombre. Esto incluye cuando trabajas con Amazon DataZone u otros Servicios de AWS usuarios mediante la consola, la API o AWS los SDK. AWS CLI Cualquier dato que ingrese en etiquetas o campos de formato libre utilizados para nombres se puede emplear para los registros de facturación o diagnóstico. Si proporciona una URL a un servidor externo,

recomendamos encarecidamente que no incluya información de credenciales en la URL a fin de validar la solicitud para ese servidor.

Cifrado de datos

Al conceder permisos, tú decides quién obtiene qué permisos y qué DataZone recursos de Amazon. Habilite las acciones específicas que desea permitir en dichos recursos. Por lo tanto, debe conceder únicamente los permisos obligatorios para realizar una tarea. La implementación del acceso con privilegios mínimos es esencial a la hora de reducir los riesgos de seguridad y el impacto que podrían causar los errores o los intentos malintencionados.

Cifrado en reposo

Amazon DataZone cifra todos sus datos de forma predeterminada con una AWS clave del Servicio de administración de claves (AWS KMS) que AWS posee y administra por usted. También puede cifrar los datos almacenados en el DataZone catálogo de Amazon mediante claves que administra con AWS KMS.

Cuando creas un dominio en Amazon DataZone, puedes proporcionar la configuración de cifrado marcando la casilla de verificación situada junto a Personalizar la configuración de cifrado (avanzada) en Cifrado de datos y proporcionando una clave de KMS.

Cifrado en tránsito

Amazon DataZone utiliza Transport Layer Security (TLS) y el cifrado del lado del cliente para el cifrado en tránsito. La comunicación con Amazon siempre DataZone se realiza a través de HTTPS, por lo que tus datos siempre están cifrados en tránsito.

Privacidad del tráfico entre redes

Para proteger las conexiones entre cuentas, Amazon DataZone utiliza funciones de servicio y funciones de IAM para conectarse de forma segura a las cuentas de los clientes y ejecutar operaciones en nombre del cliente.

Temas

- El cifrado de datos en reposo para Amazon DataZone
- Uso de puntos de enlace de VPC de interfaz para Amazon DataZone

El cifrado de datos en reposo para Amazon DataZone

El cifrado de los datos en reposo de forma predeterminada ayuda a reducir la sobrecarga operativa y la complejidad que implica la protección de los datos confidenciales. Al mismo tiempo, le permite crear aplicaciones seguras que cumplen con los estrictos requisitos normativos y de conformidad con el cifrado.

Amazon DataZone utiliza claves AWS propias por defecto para cifrar automáticamente los datos en reposo. No puedes ver, gestionar ni auditar el uso de las claves AWS propias. Para obtener más información, consulta las claves AWS propias.

Si bien no puedes deshabilitar esta capa de cifrado ni seleccionar un tipo de cifrado alternativo, puedes añadir una segunda capa de cifrado sobre las claves de cifrado que ya AWS poseas si eliges una clave gestionada por el cliente al crear tus dominios de Amazon DataZone . Amazon DataZone admite el uso de claves simétricas administradas por el cliente que puedes crear, poseer y administrar para añadir una segunda capa de cifrado sobre el cifrado que ya AWS tienes. Como tienes el control total de esta capa de cifrado, en ella puedes realizar las siguientes tareas:

- Establezca y mantenga políticas clave
- Establezca y mantenga las políticas y subvenciones de IAM
- Habilite y deshabilite las políticas clave
- Rote el material criptográfico clave
- Agregue etiquetas
- Cree alias clave
- Programa la eliminación de claves

Para obtener más información, consulte Claves administradas por el cliente.

> **Note**
>
> Amazon habilita DataZone automáticamente el cifrado en reposo mediante claves AWS propias para proteger los datos de los clientes sin coste alguno.
> AWS Se aplican cargos de KMS por el uso de claves administradas por el cliente. Para obtener más información sobre los precios, consulte los precios de los servicios de administración de AWS claves.

Cómo DataZone utiliza Amazon las subvenciones en AWS KMS

Amazon DataZone requiere tres concesiones para usar tu clave gestionada por el cliente. Cuando creas un DataZone dominio de Amazon cifrado con una clave gestionada por el cliente, Amazon DataZone crea subvenciones y subsubvenciones en tu nombre mediante el envío de CreateGrantsolicitudes a AWS KMS. Las concesiones en AWS KMS se utilizan para dar a Amazon DataZone acceso a una clave de KMS de tu cuenta. Amazon DataZone crea las siguientes concesiones para usar tu clave gestionada por el cliente en las siguientes operaciones internas:

Una subvención para cifrar los datos en reposo para las siguientes operaciones:

- Envía DescribeKeysolicitudes a AWS KMS para comprobar que el identificador de clave de KMS simétrico gestionado por el cliente introducido al crear una colección de DataZone dominios de Amazon es válido.
- Envíelo GenerateDataKeyrequestsa AWS KMS para generar claves de datos cifradas por su clave administrada por el cliente.
- Envíe las solicitudes de descifrado a AWS KMS para descifrar las claves de datos cifradas, de modo que puedan usarse para cifrar sus datos.
- RetireGrantpara retirar la concesión cuando se elimine el dominio.

Dos subvenciones para la búsqueda y el descubrimiento de sus datos:

- Beca 2:
  - DescribeKey
  - GenerateDataKey
  - Cifrar, descifrar, ReEncrypt
  - CreateGrantpara crear subvenciones familiares para los AWS servicios utilizados internamente por. DataZone
  - RetireGrant
- Beca 3:
  - GenerateDataKey
  - Decrypt
  - RetireGrant

Puede revocar el acceso a la concesión o eliminar el acceso del servicio a la clave administrada por el cliente en cualquier momento. Si lo haces, Amazon DataZone no podrá acceder a ninguno de los datos cifrados por la clave gestionada por el cliente, lo que afectará a las operaciones que dependen de esos datos. Por ejemplo, si intentas obtener detalles de un activo de datos a los que Amazon no DataZone puede acceder, la operación devolverá un `AccessDeniedException` error.

Crear una clave administrada por el cliente

Puede crear una clave simétrica gestionada por el cliente mediante la consola AWS de administración o las API de AWS KMS.

Para crear una clave simétrica gestionada por el cliente, siga los pasos para crear una clave simétrica gestionada por el cliente que se indican en la Guía para desarrolladores del servicio de gestión de AWS claves.

Política clave: las políticas clave controlan el acceso a la clave gestionada por el cliente. Cada clave administrada por el cliente debe tener exactamente una política de clave, que contiene instrucciones que determinan quién puede usar la clave y cómo puede utilizarla. Cuando crea la clave administrada por el cliente, puede especificar una política de clave. Para obtener más información, consulte Administrar el acceso a las claves administradas por el cliente en la Guía AWS para desarrolladores del Servicio de administración de claves.

Para usar tu clave gestionada por el cliente con tus DataZone recursos de Amazon, la política de claves debe permitir las siguientes operaciones de API:

- kms: CreateGrant — añade una concesión a una clave gestionada por el cliente. Otorga acceso de control a una clave de KMS específica, que permite el acceso a las operaciones de subvención que Amazon DataZone requiere. Para obtener más información sobre el uso de las subvenciones, consulte la Guía para desarrolladores del servicio de administración de AWS claves.
- kms: DescribeKey — proporciona los detalles de la clave gestionada por el cliente DataZone para que Amazon pueda validar la clave.
- kms: GenerateDataKey — devuelve una clave de datos simétrica única para usarla fuera de AWS KMS.
- KMS:Decrypt: descifra el texto cifrado mediante una clave KMS.

Los siguientes son ejemplos de declaraciones de política que puedes añadir para 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 política de rechazo de KMS no se aplica a los recursos a los que se accede a través del portal de DataZone datos de Amazon.

Para obtener más información sobre cómo especificar los permisos en una política, consulte la Guía para desarrolladores del servicio de administración de AWS claves.

Para obtener más información sobre la solución de problemas de acceso a las claves, consulte la Guía AWS para desarrolladores del Servicio de administración de claves.

Especificar una clave gestionada por el cliente para Amazon DataZone

Contexto DataZone de cifrado de Amazon

Un contexto de cifrado es un conjunto opcional de pares clave-valor que pueden contener información contextual adicional sobre los datos.

AWS KMS utiliza el contexto de cifrado como datos autenticados adicionales para respaldar el cifrado autenticado. Al incluir un contexto de cifrado en una solicitud de cifrado de datos, AWS KMS vincula el contexto de cifrado a los datos cifrados. Para descifrar los datos, debe incluir el mismo contexto de cifrado en la solicitud.

Amazon DataZone utiliza el siguiente contexto de cifrado:

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

Uso del contexto de cifrado para la supervisión: cuando utilizas una clave simétrica gestionada por el cliente para cifrar Amazon DataZone, también puedes utilizar el contexto de cifrado en los registros y registros de auditoría para identificar cómo se utiliza la clave gestionada por el cliente. El contexto de cifrado también aparece en los registros generados por AWS CloudTrail Amazon CloudWatch Logs.

Utilizar el contexto de cifrado para controlar el acceso a la clave gestionada por el cliente: puede utilizar el contexto de cifrado en las políticas de claves y en las políticas de IAM como condiciones para controlar el acceso a la clave simétrica gestionada por el cliente. Puede usar también una restricción de contexto de cifrado en una concesión.

Amazon DataZone utiliza una restricción de contexto de cifrado en las concesiones para controlar el acceso a la clave gestionada por el cliente en tu cuenta o región. La restricción de concesión requiere que las operaciones que permite la concesión utilicen el contexto de cifrado especificado.

Los siguientes son ejemplos de declaraciones de política clave para conceder acceso a una clave administrada por el cliente para un contexto de cifrado específico. La condición de esta declaración de política exige que las concesiones tengan una restricción de contexto de cifrado que especifique el contexto de cifrado.

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

Supervisión de tus claves de cifrado para Amazon DataZone

Cuando utilizas una clave gestionada por el cliente de AWS KMS con tus DataZone recursos de Amazon, puedes utilizarla AWS CloudTrailpara realizar un seguimiento de las solicitudes que Amazon DataZone envía a AWS KMS. Los siguientes ejemplos son AWS CloudTrail eventos para `CreateGrant` `GenerateDataKeyDecrypt`, y `DescribeKey` para supervisar las operaciones de KMS solicitadas por Amazon DataZone para acceder a los datos cifrados por la clave gestionada por el cliente. Cuando utilizas una clave gestionada por el cliente de AWS KMS para cifrar tu DataZone dominio de Amazon, Amazon DataZone envía una `CreateGrant` solicitud en tu nombre para acceder a la clave de KMS de tu AWS cuenta. Las subvenciones que Amazon DataZone crea son específicas del recurso asociado a la clave gestionada por el cliente de AWS KMS. Además, Amazon DataZone utiliza la `RetireGrant` operación para eliminar una concesión cuando eliminas un dominio. El siguiente evento de ejemplo registra la operación `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"
}
```

Creación de entornos de Data Lake que incluyan catálogos de AWS Glue cifrados

En casos de uso avanzado, cuando trabajas con un catálogo de AWS Glue cifrado, debes conceder acceso al DataZone servicio de Amazon para usar tu clave de KMS gestionada por el cliente. Para ello, actualiza tu política de KMS personalizada y añade una etiqueta a la clave. Para conceder acceso al DataZone servicio de Amazon para trabajar con los datos de un catálogo de AWS Glue cifrado, sigue estos pasos:

- Añade la siguiente política a tu clave KMS personalizada. Para obtener más información, consulte Cambiar una política de claves.

```
{
  "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*"
    }
```

```
  }
}
```

- Añada la siguiente etiqueta a su clave KMS personalizada. Para obtener más información, consulte Uso de etiquetas para controlar el acceso a las claves de KMS.

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

Uso de puntos de enlace de VPC de interfaz para Amazon DataZone

Si utiliza Amazon Virtual Private Cloud (Amazon VPC) para alojar sus AWS recursos, puede establecer una conexión entre su Amazon VPC y Amazon. DataZone Puedes usar esta conexión con Amazon DataZone sin tener que cruzar la red pública de Internet.

Amazon VPC le permite lanzar AWS recursos en una red virtual personalizada. Puede utilizar una VPC para controlar la configuración de red, como el intervalo de direcciones IP, las subredes, las tablas de enrutamiento y las puertas de enlace de red. Para obtener más información sobre VPC, consulte la Guía del usuario de Amazon VPC.

Para conectar su VPC de Amazon a Amazon DataZone, primero debe definir un punto de enlace de VPC de interfaz, que le permita conectar su VPC a otros servicios. AWS El punto de conexión ofrece conectividad escalable de confianza sin necesidad de utilizar una gateway de Internet, una instancia de conversión de las direcciones de red (NAT) o una conexión de VPN. Para obtener más información y pasos detallados sobre cómo crear un punto de enlace de VPC, consulte Interface VPC Endpoints () en la Guía AWS PrivateLink del usuario de Amazon VPC.

> **Important**
>
> En la VPC, una política de punto final es una política basada en recursos que se puede adjuntar a un punto final de VPC para controlar qué entidades principales pueden usar el punto final para AWS acceder a un servicio. AWS
> En la versión actual de Amazon DataZone, no se admite el uso de políticas de puntos de conexión para establecer y utilizar conexiones entre tu VPC de Amazon y Amazon. DataZone

La administración de DataZone acceso de Amazon se basa en la configuración de la RAM y en las principales políticas de IAM que se definen a nivel de servicio.

Autorización en Amazon DataZone

DataZoneLa interfaz de Amazon consta de una consola de administración interna AWS y una aplicación web externa (portal de datos).

AWS Los administradores pueden usar la consola de DataZone administración de Amazon para top-level-resource las API, incluida la creación y administración de dominios, las asociaciones de AWS cuentas para estos dominios y las fuentes de datos para las que desee delegar la administración del acceso a Amazon DataZone. Puede utilizar la consola de DataZone administración de Amazon para gestionar todas las funciones y la configuración de IAM necesarias para delegar el control de la gestión de acceso al DataZone servicio de Amazon para sus AWS cuentas configuradas de forma explícita. El portal de DataZone datos de Amazon es una aplicación de centro de AWS identidad propia para usuarios de SSO. Si está habilitada, los directores de IAM autorizados también pueden utilizar la consola para federarse en el portal de datos en lugar de utilizar una identidad de SSO.

El portal DataZone de datos de Amazon está diseñado para que lo utilicen principalmente los usuarios autenticados del AWS IAM Identity Center para administrar el acceso a los datos y realizar tareas de publicación, descubrimiento, suscripción y análisis de datos.

Autorización en la DataZone consola de Amazon

El modelo de autorización de DataZone la consola de Amazon utiliza la autorización de IAM. Los administradores utilizan la consola principalmente para la configuración. Amazon DataZone utiliza el concepto de una AWS cuenta de administrador de dominio y AWS cuentas de miembros, y todas estas cuentas utilizan la consola para crear relaciones de confianza y, al mismo tiempo, respetar los límites de AWS la organización.

Autorización en el DataZone portal Amazon

El modelo de autorización del portal de DataZone datos de Amazon es una ACL jerárquica con arquetipos de roles estáticos (perfiles) que incluyen administradores y espectadores. Por ejemplo, los usuarios pueden tener un perfil de administrador o usuario. A nivel de dominio, pueden tener una designación de usuario de dominio como propietario de los datos. A nivel de proyecto, un usuario puede ser propietario o colaborador. Estos perfiles se pueden configurar de dos tipos: usuarios

y grupos. A continuación, estos perfiles se asocian a dominios y proyectos, y el estado de estos permisos se almacena en una tabla de asociaciones.

Dentro de este modelo de autorización, Amazon DataZone permite a los usuarios gestionar los permisos de usuarios y grupos. Los usuarios administran la membresía de los proyectos, solicitan la membresía a los proyectos y aprueban las membresías. Los usuarios publican datos, definen los aprobadores de suscripciones de datos, se suscriben a los datos y aprueban las suscripciones.

Los usuarios realizan análisis de datos en proyectos específicos cuando su cliente del portal de datos solicita las credenciales de sesión de IAM que Amazon DataZone genera en función del perfil efectivo del usuario en el contexto específico del proyecto. Esta sesión se basa tanto en los permisos del usuario como en los recursos del proyecto específico. Luego, los usuarios acceden a Athena o Redshift para consultar los datos relevantes y todo el trabajo de IAM subyacente queda completamente abstraído.

DataZone Perfiles y funciones de Amazon

Una vez que se autentica un usuario, el contexto autenticado se asigna a un ID de perfil de usuario. Este perfil de usuario puede tener varias asociaciones diferentes (propietario del proyecto, administrador del dominio, etc.) que se utilizan para autorizar a los usuarios. Cada asociación (por ejemplo, el propietario del proyecto, el administrador del dominio, etc.) tiene permisos para realizar determinadas actividades en función del contexto. Por ejemplo, un usuario que tiene una asociación de administradores de dominio puede crear dominios adicionales, asignar otros administradores de dominio al dominio y crear plantillas de proyectos dentro de su dominio. El propietario de un proyecto puede añadir o eliminar miembros del proyecto, crear acuerdos de publicación con un dominio y publicar activos en un dominio.

Control del acceso a los DataZone recursos de Amazon mediante IAM

Necesita AWS Identity and Access Management (IAM) para completar las siguientes tareas relacionadas con la seguridad:

- Cree usuarios y grupos en su. Cuenta de AWS
- Asigne credenciales de seguridad únicas a cada usuario de su Cuenta de AWS.
- Controle los permisos de cada usuario para realizar tareas con AWS los recursos.
- Permite que los usuarios de otro Cuenta de AWS usuario compartan tus AWS recursos.

- Cree funciones para usted Cuenta de AWS y defina los usuarios o servicios que pueden asumirlas.
- Utilice las identidades existentes de su empresa a fin de conceder permisos para realizar tareas utilizando AWS los recursos

Para obtener más información sobre IAM, consulte lo siguiente:

- AWS Identity and Access Management (IAM)
- Introducción
- Guía del usuario de IAM

En las siguientes secciones se describen las políticas y los permisos necesarios para configurar Amazon DataZone y sus componentes, como los dominios (incluido el dominio), las cuentas asociadas, los proyectos y las fuentes de datos. Para obtener más información, consulte DataZone Terminología y conceptos de Amazon.

Contenido

AWS políticas gestionadas para Amazon DataZone

Una política AWS gestionada es una política independiente creada y administrada por AWS. AWS Las políticas administradas están diseñadas para proporcionar permisos para muchos casos de uso comunes, de modo que pueda empezar a asignar permisos a usuarios, grupos y funciones.

Ten en cuenta que es posible que las políticas AWS administradas no otorguen permisos con privilegios mínimos para tus casos de uso específicos, ya que están disponibles para que los usen todos los AWS clientes. Se recomienda definir políticas administradas por el cliente específicas para sus casos de uso a fin de reducir aún más los permisos.

No puedes cambiar los permisos definidos en AWS las políticas administradas. Si AWS actualiza los permisos definidos en una política AWS administrada, la actualización afecta a todas las identidades

principales (usuarios, grupos y roles) a las que está asociada la política. AWS es más probable que actualice una política AWS administrada cuando Servicio de AWS se lance una nueva o cuando estén disponibles nuevas operaciones de API para los servicios existentes.

Para obtener más información, consulte Políticas administradas de AWS en la Guía del usuario de IAM.

Contenido

AWS política gestionada: AmazonDataZoneFullAccess

Puede adjuntar la política `AmazonDataZoneFullAccess` a las identidades de IAM.

Esta política proporciona acceso completo a Amazon DataZone a través de AWS Management Console.

Detalles de los permisos

Esta política incluye los permisos siguientes:

- `datazone`— otorga a los directores acceso completo a Amazon a DataZone través del AWS Management Console.
- `kms`— Permite a los directores enumerar los alias y describir las claves.

- `s3`— Permite a los directores elegir depósitos S3 existentes o crear nuevos para almacenar los datos de Amazon DataZone .
- `ram`— Permite a los directores compartir DataZone dominios de Amazon entre Cuentas de AWS sí.
- `iam`— Permite a los directores enumerar y transferir funciones y obtener políticas.
- `sso`— Permite a los directores obtener las regiones en las que AWS IAM Identity Center está habilitada.

```
{
  "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_*"
        }
      }
    }
  ]
}
```

Consideraciones y limitaciones políticas

Hay ciertas funcionalidades que la `AmazonDataZoneFullAccess` política no cubre.

- Si crea un DataZone dominio de Amazon con su propia AWS KMS clave, debe tener los permisos necesarios `kms:CreateGrant` para que la creación del dominio se realice correctamente y `kms:Decrypt` para que esa clave pueda invocar otras DataZone API de Amazon`kms:GenerateDataKey`, como `listDataSources` y`createDataSource`. Además, debe tener los permisos para`kms:CreateGrant`, `kms:Decrypt``kms:GenerateDataKey`, y estar `kms:DescribeKey` en la política de recursos de esa clave.

  Si utilizas la clave KMS predeterminada que es propiedad del servicio, no es obligatoria.

  Para obtener más información, consulte AWS Key Management Service.

- Si quieres usar las funcionalidades de creación y actualización de roles en la DataZone consola de Amazon, debes tener privilegios de administrador o tener los permisos de IAM necesarios para crear roles de IAM y crear o actualizar políticas. Los permisos necesarios incluyen`iam:CreateRole`,, y `iam:CreatePolicy` los permisos. `iam:CreatePolicyVersion` `iam:DeletePolicyVersion` `iam:AttachRolePolicy`
- Si creas un dominio nuevo en Amazon DataZone con el inicio de sesión de AWS IAM Identity Center los usuarios activado, o si lo activas para un dominio existente en Amazon DataZone, debes tener permisos para lo siguiente: `sso:CreateManagedApplicationInstance` `sso:DeleteManagedApplicationInstance`, y `sso:PutApplicationAssignmentConfiguration`.
- Para aceptar una solicitud de asociación de AWS cuentas en Amazon DataZone, debes tener el `ram:AcceptResourceShareInvitation` permiso.

AWS política gestionada: AmazonDataZoneFullUserAccess

Esta política otorga acceso total a Amazon DataZone, pero no permite la administración de dominios, usuarios o cuentas asociadas.

Detalles de los permisos

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Sid": "AmazonDataZoneUserOperations",
      "Effect": "Allow",
      "Action": [
        "datazone:GetDomain",
        "datazone:CreateFormType",
        "datazone:GetFormType",
        "datazone:GetIamPortalLoginUrl",
        "datazone:SearchUserProfiles",
        "datazone:SearchGroupProfiles",
        "datazone:GetUserProfile",
        "datazone:GetGroupProfile",
        "datazone:ListGroupsForUser",
        "datazone:DeleteFormType",
        "datazone:CreateAssetType",
        "datazone:GetAssetType",
```

```
        "datazone:DeleteAssetType",
        "datazone:CreateGlossary",
        "datazone:GetGlossary",
        "datazone:DeleteGlossary",
        "datazone:UpdateGlossary",
        "datazone:CreateGlossaryTerm",
        "datazone:GetGlossaryTerm",
        "datazone:DeleteGlossaryTerm",
        "datazone:UpdateGlossaryTerm",
        "datazone:CreateAsset",
        "datazone:GetAsset",
        "datazone:DeleteAsset",
        "datazone:CreateAssetRevision",
        "datazone:ListAssetRevisions",
        "datazone:AcceptPredictions",
        "datazone:RejectPredictions",
        "datazone:Search",
        "datazone:SearchTypes",
        "datazone:CreateListingChangeSet",
        "datazone:DeleteListing",
        "datazone:SearchListings",
        "datazone:GetListing",
        "datazone:CreateDataSource",
        "datazone:GetDataSource",
        "datazone:DeleteDataSource",
        "datazone:UpdateDataSource",
        "datazone:ListDataSources",
        "datazone:StartDataSourceRun",
        "datazone:GetDataSourceRun",
        "datazone:ListDataSourceRuns",
        "datazone:ListDataSourceRunActivities",
        "datazone:ListEnvironmentBlueprintConfigurations",
        "datazone:CreateEnvironmentBlueprint",
        "datazone:GetEnvironmentBlueprint",
        "datazone:DeleteEnvironmentBlueprint",
        "datazone:UpdateEnvironmentBlueprint",
        "datazone:ListEnvironmentBlueprints",
        "datazone:CreateProject",
        "datazone:UpdateProject",
        "datazone:GetProject",
        "datazone:DeleteProject",
        "datazone:ListProjects",
        "datazone:CreateProjectMembership",
        "datazone:DeleteProjectMembership",
```

```
        "datazone:ListProjectMemberships",
        "datazone:CreateEnvironmentProfile",
        "datazone:GetEnvironmentProfile",
        "datazone:UpdateEnvironmentProfile",
        "datazone:DeleteEnvironmentProfile",
        "datazone:ListEnvironmentProfiles",
        "datazone:CreateEnvironment",
        "datazone:GetEnvironment",
        "datazone:DeleteEnvironment",
        "datazone:UpdateEnvironment",
        "datazone:UpdateEnvironmentDeploymentStatus",
        "datazone:ListEnvironments",
        "datazone:ListAccountEnvironments",
        "datazone:GetEnvironmentActionLink",
        "datazone:GetEnvironmentCredentials",
        "datazone:GetSubscriptionTarget",
        "datazone:DeleteSubscriptionTarget",
        "datazone:ListSubscriptionTargets",
        "datazone:CreateSubscriptionRequest",
        "datazone:AcceptSubscriptionRequest",
        "datazone:UpdateSubscriptionRequest",
        "datazone:ListWarehouseMetadata",
        "datazone:RejectSubscriptionRequest",
        "datazone:GetSubscriptionRequestDetails",
        "datazone:ListSubscriptionRequests",
        "datazone:DeleteSubscriptionRequest",
        "datazone:GetSubscription",
        "datazone:CancelSubscription",
        "datazone:GetSubscriptionEligibility",
        "datazone:ListSubscriptions",
        "datazone:RevokeSubscription",
        "datazone:CreateSubscriptionGrant",
        "datazone:DeleteSubscriptionGrant",
        "datazone:GetSubscriptionGrant",
        "datazone:ListSubscriptionGrants",
        "datazone:UpdateSubscriptionGrantStatus",
        "datazone:ListNotifications",
        "datazone:StartMetadataGenerationRun",
        "datazone:GetMetadataGenerationRun",
        "datazone:CancelMetadataGenerationRun",
        "datazone:ListMetadataGenerationRuns"
      ],
      "Resource": "*"
    },
```

```
    {
      "Sid": "RAMResourceShareOperations",
      "Effect": "Allow",
      "Action": "ram:GetResourceShareAssociations",
      "Resource": "*"
    }
  ]
}
```

AWS política gestionada: AmazonDataZoneCustomEnvironmentDeploymentPolicy

Puede utilizar esta política para actualizar la configuración de los entornos que se crean mediante esquemas personalizados. Esta política también se puede utilizar para crear objetivos de DataZone suscripción y fuentes de datos de Amazon.

Detalles de los permisos

```
{
 "Version": "2012-10-17",
 "Statement": [
  {
   "Sid": "AmazonDataZoneCustomEnvironment",
   "Effect": "Allow",
   "Action": [
    "datazone:ListAssociatedAccounts",
    "datazone:GetAccountAssociation",
    "datazone:GetEnvironment",
    "datazone:GetEnvironmentProfile",
    "datazone:GetEnvironmentBlueprint",
    "datazone:GetProject",
    "datazone:UpdateEnvironmentConfiguration",
    "datazone:UpdateEnvironmentDeploymentStatus",
    "datazone:CreateSubscriptionTarget",
    "datazone:CreateDataSource"
   ],
   "Resource": "*"
  }
 ]
}
```

AWS política gestionada: AmazonDataZoneEnvironmentRolePermissionsBoundary

> **Note**
>
> Esta política es un límite de permisos. Un límite de permisos establece los permisos máximos que una política basada en la identidad puede conceder a una entidad de IAM. No debes usar ni adjuntar las políticas de límites de DataZone permisos de Amazon por tu cuenta. Las políticas de límites de DataZone permisos de Amazon solo deben adjuntarse a las funciones DataZone gestionadas por Amazon. Para obtener más información sobre los límites de los permisos, consulte los límites de los permisos para las entidades de IAM en la Guía del usuario de IAM.

Cuando crea un entorno a través del portal de DataZone datos de Amazon, Amazon DataZone aplica este límite de permisos a las funciones de IAM que se generan durante la creación del entorno. El límite de permisos limita el alcance de las funciones que Amazon DataZone crea y de las funciones que añadas.

Amazon DataZone utiliza la política `AmazonDataZoneEnvironmentRolePermissionsBoundary` gestionada para limitar el principal de IAM aprovisionado al que está asociada. Los directores pueden adoptar la forma de las funciones de usuario que Amazon DataZone puede asumir en nombre de los usuarios empresariales interactivos o de los servicios analíticos (por ejemplo) y AWS Glue, a continuación, llevar a cabo acciones para procesar datos, como leer y escribir desde Amazon S3 o ejecutarlos. Rastreador de AWS Glue

La `AmazonDataZoneEnvironmentRolePermissionsBoundary` política concede a Amazon acceso de lectura y escritura DataZone a servicios como AWS Glue Amazon S3 AWS Lake Formation, Amazon Redshift y Amazon Athena. La política también otorga permisos de lectura y escritura a algunos recursos de infraestructura necesarios para usar estos servicios, como las interfaces y AWS KMS claves de red.

Amazon DataZone aplica la política `AmazonDataZoneEnvironmentRolePermissionsBoundary` AWS gestionada como límite de permisos para todos los roles del DataZone entorno de Amazon (propietario y colaborador). Este límite de permisos restringe estas funciones para permitir el acceso únicamente a los recursos y acciones necesarios para un entorno.

El límite incluye las siguientes declaraciones de JSON:

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Sid": "CreateGlueConnection",
      "Effect": "Allow",
      "Action": [
        "ec2:CreateTags",
        "ec2:DeleteTags"
      ],
      "Resource": [
        "arn:aws:ec2:*:*:network-interface/*"
      ],
      "Condition": {
        "ForAllValues:StringEquals": {
          "aws:TagKeys": [
            "aws-glue-service-resource"
          ]
        }
      }
    },
    {
      "Sid": "GlueOperations",
      "Effect": "Allow",
      "Action": [
        "glue:*DataQuality*",
        "glue:BatchCreatePartition",
        "glue:BatchDeleteConnection",
        "glue:BatchDeletePartition",
        "glue:BatchDeleteTable",
        "glue:BatchDeleteTableVersion",
        "glue:BatchGetJobs",
        "glue:BatchGetWorkflows",
        "glue:BatchStopJobRun",
        "glue:BatchUpdatePartition",
        "glue:CreateBlueprint",
        "glue:CreateConnection",
        "glue:CreateCrawler",
        "glue:CreateDatabase",
        "glue:CreateJob",
        "glue:CreatePartition",
        "glue:CreatePartitionIndex",
        "glue:CreateTable",
        "glue:CreateWorkflow",
```

```
        "glue:DeleteBlueprint",
        "glue:DeleteColumnStatisticsForPartition",
        "glue:DeleteColumnStatisticsForTable",
        "glue:DeleteConnection",
        "glue:DeleteCrawler",
        "glue:DeleteJob",
        "glue:DeletePartition",
        "glue:DeletePartitionIndex",
        "glue:DeleteTable",
        "glue:DeleteTableVersion",
        "glue:DeleteWorkflow",
        "glue:GetColumnStatisticsForPartition",
        "glue:GetColumnStatisticsForTable",
        "glue:GetConnection",
        "glue:GetDatabase",
        "glue:GetDatabases",
        "glue:GetTable",
        "glue:GetTables",
        "glue:GetPartition",
        "glue:GetPartitions",
        "glue:ListSchemas",
        "glue:ListJobs",
        "glue:NotifyEvent",
        "glue:PutWorkflowRunProperties",
        "glue:ResetJobBookmark",
        "glue:ResumeWorkflowRun",
        "glue:SearchTables",
        "glue:StartBlueprintRun",
        "glue:StartCrawler",
        "glue:StartCrawlerSchedule",
        "glue:StartJobRun",
        "glue:StartWorkflowRun",
        "glue:StopCrawler",
        "glue:StopCrawlerSchedule",
        "glue:StopWorkflowRun",
        "glue:UpdateBlueprint",
        "glue:UpdateColumnStatisticsForPartition",
        "glue:UpdateColumnStatisticsForTable",
        "glue:UpdateConnection",
        "glue:UpdateCrawler",
        "glue:UpdateCrawlerSchedule",
        "glue:UpdateDatabase",
        "glue:UpdateJob",
        "glue:UpdatePartition",
```

```
        "glue:UpdateTable",
        "glue:UpdateWorkflow"
      ],
      "Resource": "*",
      "Condition": {
        "Null": {
          "aws:ResourceTag/AmazonDataZoneEnvironment": "false"
        }
      }
    },
    {
      "Sid": "PassRole",
      "Effect": "Allow",
      "Action": [
        "iam:PassRole"
      ],
      "Resource": [
        "arn:aws:iam::*:role/datazone*"
      ],
      "Condition": {
        "StringEquals": {
          "iam:PassedToService": "glue.amazonaws.com"
        }
      }
    },
    {
      "Sid": "SameAccountKmsOperations",
      "Effect": "Allow",
      "Action": [
        "kms:DescribeKey",
        "kms:Decrypt",
        "kms:ListKeys"
      ],
      "Resource": "*",
      "Condition": {
        "StringNotEquals": {
          "aws:ResourceAccount": "${aws:PrincipalAccount}"
        }
      }
    },
    {
      "Sid": "KmsOperationsWithResourceTag",
      "Effect": "Allow",
      "Action": [
```

```
        "kms:DescribeKey",
        "kms:Decrypt",
        "kms:ListKeys",
        "kms:Encrypt",
        "kms:GenerateDataKey",
        "kms:Verify",
        "kms:Sign"
      ],
      "Resource": "*",
      "Condition": {
        "Null": {
          "aws:ResourceTag/AmazonDataZoneEnvironment": "false"
        }
      }
    },
    {
      "Sid": "AnalyticsOperations",
      "Effect": "Allow",
      "Action": [
        "datazone:*",
        "sqlworkbench:*"
      ],
      "Resource": "*"
    },
    {
      "Sid": "QueryOperations",
      "Effect": "Allow",
      "Action": [
        "athena:BatchGetNamedQuery",
        "athena:BatchGetPreparedStatement",
        "athena:BatchGetQueryExecution",
        "athena:CreateNamedQuery",
        "athena:CreateNotebook",
        "athena:CreatePreparedStatement",
        "athena:CreatePresignedNotebookUrl",
        "athena:DeleteNamedQuery",
        "athena:DeleteNotebook",
        "athena:DeletePreparedStatement",
        "athena:ExportNotebook",
        "athena:GetDatabase",
        "athena:GetDataCatalog",
        "athena:GetNamedQuery",
        "athena:GetPreparedStatement",
        "athena:GetQueryExecution",
```

```
        "athena:GetQueryResults",
        "athena:GetQueryRuntimeStatistics",
        "athena:GetTableMetadata",
        "athena:GetWorkGroup",
        "athena:ImportNotebook",
        "athena:ListDatabases",
        "athena:ListDataCatalogs",
        "athena:ListEngineVersions",
        "athena:ListNamedQueries",
        "athena:ListPreparedStatements",
        "athena:ListQueryExecutions",
        "athena:ListTableMetadata",
        "athena:ListTagsForResource",
        "athena:ListWorkGroups",
        "athena:StartCalculationExecution",
        "athena:StartQueryExecution",
        "athena:StartSession",
        "athena:StopCalculationExecution",
        "athena:StopQueryExecution",
        "athena:TerminateSession",
        "athena:UpdateNamedQuery",
        "athena:UpdateNotebook",
        "athena:UpdateNotebookMetadata",
        "athena:UpdatePreparedStatement",
        "ec2:CreateNetworkInterface",
        "ec2:DeleteNetworkInterface",
        "ec2:Describe*",
        "glue:BatchCreatePartition",
        "glue:BatchDeletePartition",
        "glue:BatchDeleteTable",
        "glue:BatchDeleteTableVersion",
        "glue:BatchGetJobs",
        "glue:BatchGetPartition",
        "glue:BatchGetWorkflows",
        "glue:BatchUpdatePartition",
        "glue:CreateBlueprint",
        "glue:CreateConnection",
        "glue:CreateCrawler",
        "glue:CreateDatabase",
        "glue:CreateJob",
        "glue:CreatePartition",
        "glue:CreatePartitionIndex",
        "glue:CreateTable",
        "glue:CreateWorkflow",
```

```
        "glue:DeleteColumnStatisticsForPartition",
        "glue:DeleteColumnStatisticsForTable",
        "glue:DeletePartition",
        "glue:DeletePartitionIndex",
        "glue:DeleteTable",
        "glue:DeleteTableVersion",
        "glue:GetColumnStatisticsForPartition",
        "glue:GetColumnStatisticsForTable",
        "glue:GetConnection",
        "glue:GetDatabase",
        "glue:GetDatabases",
        "glue:GetTable",
        "glue:GetTables",
        "glue:GetPartition",
        "glue:GetPartitions",
        "glue:ListSchemas",
        "glue:ListJobs",
        "glue:NotifyEvent",
        "glue:SearchTables",
        "glue:UpdateColumnStatisticsForPartition",
        "glue:UpdateColumnStatisticsForTable",
        "glue:UpdateDatabase",
        "glue:UpdatePartition",
        "glue:UpdateTable",
        "iam:GetRole",
        "iam:GetRolePolicy",
        "iam:ListGroups",
        "iam:ListRolePolicies",
        "iam:ListRoles",
        "iam:ListUsers",
        "logs:DescribeLogGroups",
        "logs:DescribeLogStreams",
        "logs:DescribeMetricFilters",
        "logs:DescribeQueries",
        "logs:DescribeQueryDefinitions",
        "logs:DescribeMetricFilters",
        "logs:StartQuery",
        "logs:StopQuery",
        "logs:GetLogEvents",
        "logs:GetLogGroupFields",
        "logs:GetQueryResults",
        "logs:GetLogRecord",
        "logs:PutLogEvents",
        "logs:CreateLogStream",
```

```
        "logs:FilterLogEvents",
        "lakeformation:GetDataAccess",
        "lakeformation:GetDataLakeSettings",
        "lakeformation:GetResourceLFTags",
        "lakeformation:ListPermissions",
        "redshift-data:ListTables",
        "redshift-data:DescribeTable",
        "redshift-data:ListSchemas",
        "redshift-data:ListDatabases",
        "redshift-data:ExecuteStatement",
        "redshift-data:GetStatementResult",
        "redshift-data:DescribeStatement",
        "redshift:CreateClusterUser",
        "redshift:DescribeClusters",
        "redshift:DescribeDataShares",
        "redshift:GetClusterCredentials",
        "redshift:GetClusterCredentialsWithIAM",
        "redshift:JoinGroup",
        "redshift-serverless:ListNamespaces",
        "redshift-serverless:ListWorkgroups",
        "redshift-serverless:GetNamespace",
        "redshift-serverless:GetWorkgroup",
        "redshift-serverless:GetCredentials",
        "secretsmanager:ListSecrets",
        "tag:GetResources"
      ],
      "Resource": "*"
    },
    {
      "Sid": "QueryOperationsWithResourceTag",
      "Effect": "Allow",
      "Action": [
        "athena:GetQueryResultsStream"
      ],
      "Resource": "*",
      "Condition": {
        "Null": {
          "aws:ResourceTag/AmazonDataZoneEnvironment": "false"
        }
      }
    },
    {
      "Sid": "SecretsManagerOperationsWithTagKeys",
      "Effect": "Allow",
```

```
      "Action": [
        "secretsmanager:CreateSecret",
        "secretsmanager:TagResource"
      ],
      "Resource": "arn:aws:secretsmanager:*:*:secret:AmazonDataZone-*",
      "Condition": {
        "StringLike": {
          "aws:ResourceTag/AmazonDataZoneDomain": "*",
          "aws:ResourceTag/AmazonDataZoneProject": "*"
        },
        "Null": {
          "aws:TagKeys": "false"
        },
        "ForAllValues:StringEquals": {
          "aws:TagKeys": [
            "AmazonDataZoneDomain",
            "AmazonDataZoneProject"
          ]
        }
      }
    },
    {
      "Sid": "DataZoneS3Buckets",
      "Effect": "Allow",
      "Action": [
        "s3:AbortMultipartUpload",
        "s3:DeleteObject",
        "s3:DeleteObjectVersion",
        "s3:GetObject",
        "s3:PutObject",
        "s3:PutObjectRetention",
        "s3:ReplicateObject",
        "s3:RestoreObject"
      ],
      "Resource": [
        "arn:aws:s3:::*/datazone/*"
      ]
    },
    {
      "Sid": "DataZoneS3BucketLocation",
      "Effect": "Allow",
      "Action": [
        "s3:GetBucketLocation"
      ],
```

```
      "Resource": "*"
    },
    {
      "Sid": "ListDataZoneS3Bucket",
      "Effect": "Allow",
      "Action": [
        "s3:ListBucket"
      ],
      "Resource": [
        "*"
      ],
      "Condition": {
        "StringLike": {
          "s3:prefix": [
            "*/datazone/*",
            "datazone/*"
          ]
        }
      }
    },
    {
      "Sid": "NotDeniedOperations",
      "Effect": "Deny",
      "NotAction": [
        "datazone:*",
        "sqlworkbench:*",
        "athena:BatchGetNamedQuery",
        "athena:BatchGetPreparedStatement",
        "athena:BatchGetQueryExecution",
        "athena:CreateNamedQuery",
        "athena:CreateNotebook",
        "athena:CreatePreparedStatement",
        "athena:CreatePresignedNotebookUrl",
        "athena:DeleteNamedQuery",
        "athena:DeleteNotebook",
        "athena:DeletePreparedStatement",
        "athena:ExportNotebook",
        "athena:GetDatabase",
        "athena:GetDataCatalog",
        "athena:GetNamedQuery",
        "athena:GetPreparedStatement",
        "athena:GetQueryExecution",
        "athena:GetQueryResults",
        "athena:GetQueryResultsStream",
```

```
        "athena:GetQueryRuntimeStatistics",
        "athena:GetTableMetadata",
        "athena:GetWorkGroup",
        "athena:ImportNotebook",
        "athena:ListDatabases",
        "athena:ListDataCatalogs",
        "athena:ListEngineVersions",
        "athena:ListNamedQueries",
        "athena:ListPreparedStatements",
        "athena:ListQueryExecutions",
        "athena:ListTableMetadata",
        "athena:ListTagsForResource",
        "athena:ListWorkGroups",
        "athena:StartCalculationExecution",
        "athena:StartQueryExecution",
        "athena:StartSession",
        "athena:StopCalculationExecution",
        "athena:StopQueryExecution",
        "athena:TerminateSession",
        "athena:UpdateNamedQuery",
        "athena:UpdateNotebook",
        "athena:UpdateNotebookMetadata",
        "athena:UpdatePreparedStatement",
        "ec2:CreateNetworkInterface",
        "ec2:CreateTags",
        "ec2:DeleteNetworkInterface",
        "ec2:DeleteTags",
        "ec2:Describe*",
        "glue:*DataQuality*",
        "glue:BatchCreatePartition",
        "glue:BatchDeleteConnection",
        "glue:BatchDeletePartition",
        "glue:BatchDeleteTable",
        "glue:BatchDeleteTableVersion",
        "glue:BatchGetJobs",
        "glue:BatchGetPartition",
        "glue:BatchGetWorkflows",
        "glue:BatchStopJobRun",
        "glue:BatchUpdatePartition",
        "glue:CreateBlueprint",
        "glue:CreateConnection",
        "glue:CreateCrawler",
        "glue:CreateDatabase",
        "glue:CreateJob",
```

```
        "glue:CreatePartition",
        "glue:CreatePartitionIndex",
        "glue:CreateTable",
        "glue:CreateWorkflow",
        "glue:DeleteBlueprint",
        "glue:DeleteColumnStatisticsForPartition",
        "glue:DeleteColumnStatisticsForTable",
        "glue:DeleteConnection",
        "glue:DeleteCrawler",
        "glue:DeleteJob",
        "glue:DeletePartition",
        "glue:DeletePartitionIndex",
        "glue:DeleteTable",
        "glue:DeleteTableVersion",
        "glue:DeleteWorkflow",
        "glue:GetColumnStatisticsForPartition",
        "glue:GetColumnStatisticsForTable",
        "glue:GetConnection",
        "glue:GetDatabase",
        "glue:GetDatabases",
        "glue:GetTable",
        "glue:GetTables",
        "glue:GetPartition",
        "glue:GetPartitions",
        "glue:ListSchemas",
        "glue:ListJobs",
        "glue:NotifyEvent",
        "glue:PutWorkflowRunProperties",
        "glue:ResetJobBookmark",
        "glue:ResumeWorkflowRun",
        "glue:SearchTables",
        "glue:StartBlueprintRun",
        "glue:StartCrawler",
        "glue:StartCrawlerSchedule",
        "glue:StartJobRun",
        "glue:StartWorkflowRun",
        "glue:StopCrawler",
        "glue:StopCrawlerSchedule",
        "glue:StopWorkflowRun",
        "glue:UpdateBlueprint",
        "glue:UpdateColumnStatisticsForPartition",
        "glue:UpdateColumnStatisticsForTable",
        "glue:UpdateConnection",
        "glue:UpdateCrawler",
```

```
        "glue:UpdateCrawlerSchedule",
        "glue:UpdateDatabase",
        "glue:UpdateJob",
        "glue:UpdatePartition",
        "glue:UpdateTable",
        "glue:UpdateWorkflow",
        "iam:GetRole",
        "iam:GetRolePolicy",
        "iam:List*",
        "iam:PassRole",
        "kms:DescribeKey",
        "kms:Decrypt",
        "kms:Encrypt",
        "kms:GenerateDataKey",
        "kms:ListKeys",
        "kms:Verify",
        "kms:Sign",
        "logs:DescribeLogGroups",
        "logs:DescribeLogStreams",
        "logs:DescribeMetricFilters",
        "logs:DescribeQueries",
        "logs:DescribeQueryDefinitions",
        "logs:StartQuery",
        "logs:StopQuery",
        "logs:GetLogEvents",
        "logs:GetLogGroupFields",
        "logs:GetQueryResults",
        "logs:GetLogRecord",
        "logs:PutLogEvents",
        "logs:CreateLogStream",
        "logs:FilterLogEvents",
        "lakeformation:GetDataAccess",
        "lakeformation:GetDataLakeSettings",
        "lakeformation:GetResourceLFTags",
        "lakeformation:ListPermissions",
        "redshift-data:ListTables",
        "redshift-data:DescribeTable",
        "redshift-data:ListSchemas",
        "redshift-data:ListDatabases",
        "redshift-data:ExecuteStatement",
        "redshift-data:GetStatementResult",
        "redshift-data:DescribeStatement",
        "redshift:CreateClusterUser",
        "redshift:DescribeClusters",
```

```
        "redshift:DescribeDataShares",
        "redshift:GetClusterCredentials",
        "redshift:GetClusterCredentialsWithIAM",
        "redshift:JoinGroup",
        "redshift-serverless:ListNamespaces",
        "redshift-serverless:ListWorkgroups",
        "redshift-serverless:GetNamespace",
        "redshift-serverless:GetWorkgroup",
        "redshift-serverless:GetCredentials",
        "s3:AbortMultipartUpload",
        "s3:DeleteObject",
        "s3:DeleteObjectVersion",
        "s3:GetObject",
        "s3:GetBucketLocation",
        "s3:ListBucket",
        "s3:PutObject",
        "s3:PutObjectRetention",
        "s3:ReplicateObject",
        "s3:RestoreObject",
        "secretsmanager:CreateSecret",
        "secretsmanager:ListSecrets",
        "secretsmanager:TagResource",
        "tag:GetResources"
      ],
      "Resource": [
        "*"
      ]
    }
  ]
}
```

AWS política gestionada: AmazonDataZoneRedshiftGlueProvisioningPolicy

La AmazonDataZoneRedshiftGlueProvisioningPolicy política concede a Amazon DataZone los permisos necesarios para interoperar con AWS Glue y Amazon Redshift.

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

```
  {
   "Sid": "AmazonDataZonePermissionsToCreateEnvironmentRole",
   "Effect": "Allow",
   "Action": [
    "iam:CreateRole",
    "iam:DetachRolePolicy",
    "iam:DeleteRolePolicy",
    "iam:AttachRolePolicy",
    "iam:PutRolePolicy"
   ],
   "Resource": "arn:aws:iam::*:role/datazone*",
   "Condition": {
    "StringEquals": {
     "iam:PermissionsBoundary": "arn:aws:iam::aws:policy/
AmazonDataZoneEnvironmentRolePermissionsBoundary",
     "aws:CalledViaFirst": [
      "cloudformation.amazonaws.com"
     ]
    }
   }
  },
  {
   "Sid": "IamPassRolePermissions",
   "Effect": "Allow",
   "Action": [
    "iam:PassRole"
   ],
   "Resource": [
    "arn:aws:iam::*:role/datazone*"
   ],
   "Condition": {
    "StringEquals": {
     "iam:PassedToService": [
      "glue.amazonaws.com",
      "lakeformation.amazonaws.com"
     ],
     "aws:CalledViaFirst": [
      "cloudformation.amazonaws.com"
     ]
    }
   }
  },
  {
   "Sid": "AmazonDataZonePermissionsToManageCreatedEnvironmentRole",
```

```
    "Effect": "Allow",
    "Action": [
     "iam:DeleteRole",
     "iam:GetRole"
    ],
    "Resource": "arn:aws:iam::*:role/datazone*",
    "Condition": {
     "StringEquals": {
      "aws:CalledViaFirst": [
       "cloudformation.amazonaws.com"
      ]
     }
    }
   },
   {
    "Sid": "AmazonDataZoneCFStackCreationForEnvironments",
    "Effect": "Allow",
    "Action": [
     "cloudformation:CreateStack",
     "cloudformation:TagResource"
    ],
    "Resource": [
     "arn:aws:cloudformation:*:*:stack/DataZone*"
    ],
    "Condition": {
     "ForAnyValue:StringLike": {
      "aws:TagKeys": "AmazonDataZoneEnvironment"
     },
     "Null": {
      "aws:ResourceTag/AmazonDataZoneEnvironment": "false"
     }
    }
   },
   {
    "Sid": "AmazonDataZoneCFStackManagementForEnvironments",
    "Effect": "Allow",
    "Action": [
     "cloudformation:DeleteStack",
     "cloudformation:DescribeStacks",
     "cloudformation:DescribeStackEvents"
    ],
    "Resource": [
     "arn:aws:cloudformation:*:*:stack/DataZone*"
    ]
```

```
  },
  {
   "Sid": "AmazonDataZoneEnvironmentParameterValidation",
   "Effect": "Allow",
   "Action": [
    "lakeformation:GetDataLakeSettings",
    "lakeformation:PutDataLakeSettings",
    "lakeformation:RevokePermissions",
    "lakeformation:ListPermissions",
    "glue:CreateDatabase",
    "glue:GetDatabase",
    "athena:GetWorkGroup",
    "logs:DescribeLogGroups",
    "redshift-serverless:GetNamespace",
    "redshift-serverless:GetWorkgroup",
    "redshift:DescribeClusters",
    "secretsmanager:ListSecrets"
   ],
   "Resource": "*"
  },
  {
   "Sid": "AmazonDataZoneEnvironmentLakeFormationPermissions",
   "Effect": "Allow",
   "Action": [
    "lakeformation:RegisterResource",
    "lakeformation:DeregisterResource",
    "lakeformation:GrantPermissions",
    "lakeformation:ListResources"
   ],
   "Resource": "*",
   "Condition": {
    "StringEquals": {
     "aws:CalledViaFirst": [
      "cloudformation.amazonaws.com"
     ]
    }
   }
  },
  {
   "Sid": "AmazonDataZoneEnvironmentGlueDeletePermissions",
   "Effect": "Allow",
   "Action": [
    "glue:DeleteDatabase"
   ],
```

```
    "Resource": "*",
    "Condition": {
     "StringEquals": {
      "aws:CalledViaFirst": [
       "cloudformation.amazonaws.com"
      ]
     }
    }
   },
   {
    "Sid": "AmazonDataZoneEnvironmentAthenaDeletePermissions",
    "Effect": "Allow",
    "Action": [
     "athena:DeleteWorkGroup"
    ],
    "Resource": "*",
    "Condition": {
     "StringEquals": {
      "aws:CalledViaFirst": [
       "cloudformation.amazonaws.com"
      ]
     }
    }
   },
   {
    "Sid": "AmazonDataZoneEnvironmentAthenaResourceCreation",
    "Effect": "Allow",
    "Action": [
     "athena:CreateWorkGroup",
     "athena:TagResource",
     "iam:TagRole",
     "iam:TagPolicy",
     "logs:TagLogGroup"
    ],
    "Resource": "*",
    "Condition": {
     "ForAnyValue:StringLike": {
      "aws:TagKeys": "AmazonDataZoneEnvironment"
     },
     "Null": {
      "aws:ResourceTag/AmazonDataZoneEnvironment": "false"
     },
     "StringEquals": {
      "aws:CalledViaFirst": [
```

```
      "cloudformation.amazonaws.com"
     ]
    }
   }
  },
  {
   "Sid": "AmazonDataZoneEnvironmentLogGroupCreation",
   "Effect": "Allow",
   "Action": [
    "logs:CreateLogGroup",
    "logs:DeleteLogGroup"
   ],
   "Resource": "arn:aws:logs:*:*:log-group:datazone-*",
   "Condition": {
    "ForAnyValue:StringLike": {
     "aws:TagKeys": "AmazonDataZoneEnvironment"
    },
    "Null": {
     "aws:ResourceTag/AmazonDataZoneEnvironment": "false"
    },
    "StringEquals": {
     "aws:CalledViaFirst": [
      "cloudformation.amazonaws.com"
     ]
    }
   }
  },
  {
   "Sid": "AmazonDataZoneEnvironmentLogGroupManagement",
   "Action": [
    "logs:PutRetentionPolicy"
   ],
   "Resource": "arn:aws:logs:*:*:log-group:datazone-*",
   "Effect": "Allow",
   "Condition": {
    "StringEquals": {
     "aws:CalledViaFirst": [
      "cloudformation.amazonaws.com"
     ]
    }
   }
  },
  {
   "Sid": "AmazonDataZoneEnvironmentIAMPolicyManagement",
```

```
    "Effect": "Allow",
    "Action": [
     "iam:DeletePolicy",
     "iam:CreatePolicy",
     "iam:GetPolicy",
     "iam:ListPolicyVersions"
    ],
    "Resource": [
     "arn:aws:iam::*:policy/datazone*"
    ],
    "Condition": {
     "StringEquals": {
      "aws:CalledViaFirst": [
       "cloudformation.amazonaws.com"
      ]
     }
    }
   },
   {
    "Sid": "AmazonDataZoneEnvironmentS3ValidationPermissions",
    "Effect": "Allow",
    "Action": [
     "s3:ListAllMyBuckets",
     "s3:ListBucket"
    ],
    "Resource": "arn:aws:s3:::*"
   },
   {
    "Sid": "AmazonDataZoneEnvironmentKMSDecryptPermissions",
    "Effect": "Allow",
    "Action": [
     "kms:GenerateDataKey",
     "kms:Decrypt"
    ],
    "Resource": "*",
    "Condition": {
     "Null": {
      "aws:ResourceTag/AmazonDataZoneEnvironment": "false"
     }
    }
   },
   {
    "Sid": "PermissionsToTagAmazonDataZoneEnvironmentGlueResources",
    "Effect": "Allow",
```

```
    "Action": [
     "glue:TagResource"
    ],
    "Resource": "*",
    "Condition": {
     "ForAnyValue:StringLike": {
      "aws:TagKeys": "AmazonDataZoneEnvironment"
     },
     "Null": {
      "aws:RequestTag/AmazonDataZoneEnvironment": "false"
     }
    }
   },
   {
    "Sid": "PermissionsToGetAmazonDataZoneEnvironmentBlueprintTemplates",
    "Effect": "Allow",
    "Action": "s3:GetObject",
    "Resource": "*",
    "Condition": {
     "StringNotEquals": {
      "aws:ResourceAccount": "${aws:PrincipalAccount}"
     },
     "StringEquals": {
      "aws:CalledViaFirst": [
       "cloudformation.amazonaws.com"
      ]
     }
    }
   },
   {
    "Sid": "RedshiftDataPermissions",
    "Effect": "Allow",
    "Action": [
     "redshift-data:ListSchemas",
     "redshift-data:ExecuteStatement"
    ],
    "Resource": [
     "arn:aws:redshift-serverless:*:*:workgroup/*",
     "arn:aws:redshift:*:*:cluster:*"
    ]
   },
   {
    "Sid": "DescribeStatementPermissions",
    "Effect": "Allow",
```

```
    "Action": [
     "redshift-data:DescribeStatement"
    ],
    "Resource": "*"
   },
   {
    "Sid": "GetSecretValuePermissions",
    "Effect": "Allow",
    "Action": [
     "secretsmanager:GetSecretValue"
    ],
    "Resource": "*",
    "Condition": {
     "StringLike": {
      "secretsmanager:ResourceTag/AmazonDataZoneDomain": "dzd*"
     }
    }
   }
  ]
}
```

AWS política gestionada: AmazonDataZoneGlueManageAccessRolePolicy

Esta política otorga a Amazon DataZone permisos para publicar datos de AWS Glue en el catálogo. También otorga a Amazon DataZone permisos para conceder o revocar el acceso a los activos publicados por AWS Glue en el catálogo.

```
{
 "Version": "2012-10-17",
 "Statement": [
  {
   "Sid": "GlueDataQualityPermissions",
   "Effect": "Allow",
   "Action": [
    "glue:ListDataQualityResults",
    "glue:GetDataQualityResult"
   ],
   "Resource": "arn:aws:glue:*:*:dataQualityRuleset/*",
   "Condition": {
```

```
    "StringEquals": {
     "aws:ResourceAccount": "${aws:PrincipalAccount}"
    }
   }
  },
  {
   "Sid": "GlueTableDatabasePermissions",
   "Effect": "Allow",
   "Action": [
    "glue:CreateTable",
    "glue:DeleteTable",
    "glue:GetDatabases",
    "glue:GetTables"
   ],
   "Resource": [
    "arn:aws:glue:*:*:catalog",
    "arn:aws:glue:*:*:database/*",
    "arn:aws:glue:*:*:table/*"
   ],
   "Condition": {
    "StringEquals": {
     "aws:ResourceAccount": "${aws:PrincipalAccount}"
    }
   }
  },
  {
   "Sid": "LakeformationResourceSharingPermissions",
   "Effect": "Allow",
   "Action": [
    "lakeformation:BatchGrantPermissions",
    "lakeformation:BatchRevokePermissions",
    "lakeformation:CreateLakeFormationOptIn",
    "lakeformation:DeleteLakeFormationOptIn",
    "lakeformation:GrantPermissions",
    "lakeformation:GetResourceLFTags",
    "lakeformation:ListLakeFormationOptIns",
    "lakeformation:ListPermissions",
    "lakeformation:RegisterResource",
    "lakeformation:RevokePermissions",
    "glue:GetDatabase",
    "glue:GetTable",
    "organizations:DescribeOrganization",
    "ram:GetResourceShareInvitations",
    "ram:ListResources"
```

```
    ],
    "Resource": "*"
   },
   {
    "Sid": "CrossAccountRAMResourceSharingPermissions",
    "Effect": "Allow",
    "Action": [
     "glue:DeleteResourcePolicy",
     "glue:PutResourcePolicy"
    ],
    "Resource": [
     "arn:aws:glue:*:*:catalog",
     "arn:aws:glue:*:*:database/*",
     "arn:aws:glue:*:*:table/*"
    ],
    "Condition": {
     "ForAnyValue:StringEquals": {
      "aws:CalledVia": [
       "ram.amazonaws.com"
      ]
     }
    }
   },
   {
    "Sid": "CrossAccountLakeFormationResourceSharingPermissions",
    "Effect": "Allow",
    "Action": [
     "ram:CreateResourceShare"
    ],
    "Resource": "*",
    "Condition": {
     "StringEqualsIfExists": {
      "ram:RequestedResourceType": [
       "glue:Table",
       "glue:Database",
       "glue:Catalog"
      ]
     },
     "ForAnyValue:StringEquals": {
      "aws:CalledVia": [
       "lakeformation.amazonaws.com"
      ]
     }
    }
```

```
  },
  {
   "Sid": "CrossAccountRAMResourceShareInvitationPermission",
   "Effect": "Allow",
   "Action": [
    "ram:AcceptResourceShareInvitation"
   ],
   "Resource": "arn:aws:ram:*:*:resource-share-invitation/*"
  },
  {
   "Sid": "CrossAccountRAMResourceSharingViaLakeFormationPermissions",
   "Effect": "Allow",
   "Action": [
    "ram:AssociateResourceShare",
    "ram:DeleteResourceShare",
    "ram:DisassociateResourceShare",
    "ram:GetResourceShares",
    "ram:ListResourceSharePermissions",
    "ram:UpdateResourceShare"
   ],
   "Resource": "*",
   "Condition": {
    "StringLike": {
     "ram:ResourceShareName": [
      "LakeFormation*"
     ]
    },
    "ForAnyValue:StringEquals": {
     "aws:CalledVia": [
      "lakeformation.amazonaws.com"
     ]
    }
   }
  },
  {
   "Sid": "CrossAccountRAMResourceSharingViaLakeFormationHybrid",
   "Effect": "Allow",
   "Action": "ram:AssociateResourceSharePermission",
   "Resource": "*",
   "Condition": {
    "StringLike": {
     "ram:PermissionArn": "arn:aws:ram::aws:permission/AWSRAMLFEnabled*"
    },
    "ForAnyValue:StringEquals": {
```

```
      "aws:CalledVia": [
       "lakeformation.amazonaws.com"
      ]
     }
    }
   },
   {
    "Sid": "KMSDecryptPermission",
    "Effect": "Allow",
    "Action": [
     "kms:Decrypt"
    ],
    "Resource": "*",
    "Condition": {
     "StringEquals": {
      "aws:ResourceTag/datazone:projectId": "proj-all"
     }
    }
   },
   {
    "Sid": "GetRoleForDataZone",
    "Effect": "Allow",
    "Action": [
     "iam:GetRole"
    ],
    "Resource": [
     "arn:aws:iam::*:role/AmazonDataZone*",
     "arn:aws:iam::*:role/service-role/AmazonDataZone*"
    ]
   },
   {
    "Sid": "PassRoleForDataLocationRegistration",
    "Effect": "Allow",
    "Action": [
     "iam:PassRole"
    ],
    "Resource": [
     "arn:aws:iam::*:role/AmazonDataZone*",
     "arn:aws:iam::*:role/service-role/AmazonDataZone*"
    ],
    "Condition": {
     "StringEquals": {
      "iam:PassedToService": [
       "lakeformation.amazonaws.com"
```

```
     ]
    }
   }
  }
 ]
}
```

AWS política gestionada: AmazonDataZoneRedshiftManageAccessRolePolicy

Esta política otorga a Amazon DataZone permisos para publicar datos de Amazon Redshift en el catálogo. También otorga DataZone permisos a Amazon para conceder o revocar el acceso a los activos publicados en el catálogo de Amazon Redshift o Amazon Redshift Serverless.

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

Política administrada de AWS : AmazonDataZoneCrossAccountAdmin

Puede adjuntar la AmazonDataZoneCrossAccountAdmin política a sus identidades de IAM.

Esta política permite a los usuarios trabajar con las cuentas DataZone asociadas a Amazon.

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Action": [
                "ram:UpdateResourceShare",
                "ram:DeleteResourceShare",
                "ram:AssociateResourceShare",
                "ram:DisassociateResourceShare",
                "ram:GetResourceShares"
            ],
            "Resource": "*",
            "Condition": {
                "StringLike": {
                    "ram:ResourceShareName": [
                        "DataZone*"
```

```
                    ]
                }
            }
        },
        {
            "Effect": "Allow",
            "Action": [
                "datazone:PutEnvironmentBlueprintConfiguration",
                "datazone:GetEnvironmentBlueprintConfiguration",
                "datazone:DeleteEnvironmentBlueprintConfiguration",
                "datazone:ListEnvironmentBlueprintConfigurations",
                "datazone:ListDomains",
                "datazone:GetDomain",
                "datazone:GetEnvironmentBlueprint",
                "datazone:ListEnvironmentBlueprints",
                "datazone:ListEnvironments",
                "datazone:GetEnvironment",
                "ram:AcceptResourceShareInvitation",
                "ram:RejectResourceShareInvitation",
                "ram:Get*",
                "ram:List*"
            ],
            "Resource": "*"
        }
    ]
}
```

AWS política gestionada: AmazonDataZoneDomainExecutionRolePolicy

Esta es la política predeterminada para el rol de DataZone `DomainExecutionRole` servicio de Amazon. Amazon utiliza esta función DataZone para catalogar, descubrir, gobernar, compartir y analizar datos en el DataZone dominio de Amazon.

Puede adjuntar la AmazonDataZoneDomainExecutionRolePolicy política a su`AmazonDataZoneDomainExecutionRole`.

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

```
      "Effect": "Allow",
      "Action": [
        "datazone:AcceptPredictions",
        "datazone:AcceptSubscriptionRequest",
        "datazone:CancelSubscription",
        "datazone:CreateAsset",
        "datazone:CreateAssetRevision",
        "datazone:CreateAssetType",
        "datazone:CreateDataSource",
        "datazone:CreateEnvironment",
        "datazone:CreateEnvironmentBlueprint",
        "datazone:CreateEnvironmentProfile",
        "datazone:CreateFormType",
        "datazone:CreateGlossary",
        "datazone:CreateGlossaryTerm",
        "datazone:CreateListingChangeSet",
        "datazone:CreateProject",
        "datazone:CreateProjectMembership",
        "datazone:CreateSubscriptionGrant",
        "datazone:CreateSubscriptionRequest",
        "datazone:DeleteAsset",
        "datazone:DeleteAssetType",
        "datazone:DeleteDataSource",
        "datazone:DeleteEnvironment",
        "datazone:DeleteEnvironmentBlueprint",
        "datazone:DeleteEnvironmentProfile",
        "datazone:DeleteFormType",
        "datazone:DeleteGlossary",
        "datazone:DeleteGlossaryTerm",
        "datazone:DeleteListing",
        "datazone:DeleteProject",
        "datazone:DeleteProjectMembership",
        "datazone:DeleteSubscriptionGrant",
        "datazone:DeleteSubscriptionRequest",
        "datazone:DeleteSubscriptionTarget",
        "datazone:GetAsset",
        "datazone:GetAssetType",
        "datazone:GetDataSource",
        "datazone:GetDataSourceRun",
        "datazone:GetDomain",
        "datazone:GetEnvironment",
        "datazone:GetEnvironmentActionLink",
        "datazone:GetEnvironmentBlueprint",
        "datazone:GetEnvironmentCredentials",
```

```
        "datazone:GetEnvironmentProfile",
        "datazone:GetFormType",
        "datazone:GetGlossary",
        "datazone:GetGlossaryTerm",
        "datazone:GetGroupProfile",
        "datazone:GetListing",
        "datazone:GetProject",
        "datazone:GetSubscription",
        "datazone:GetSubscriptionEligibility",
        "datazone:GetSubscriptionGrant",
        "datazone:GetSubscriptionRequestDetails",
        "datazone:GetSubscriptionTarget",
        "datazone:GetUserProfile",
        "datazone:ListAccountEnvironments",
        "datazone:ListAssetRevisions",
        "datazone:ListDataSourceRunActivities",
        "datazone:ListDataSourceRuns",
        "datazone:ListDataSources",
        "datazone:ListEnvironmentBlueprintConfigurations",
        "datazone:ListEnvironmentBlueprintConfigurationSummaries",
        "datazone:ListEnvironmentBlueprints",
        "datazone:ListEnvironmentProfiles",
        "datazone:ListEnvironments",
        "datazone:ListGroupsForUser",
        "datazone:ListNotifications",
        "datazone:ListProjectMemberships",
        "datazone:ListProjects",
        "datazone:ListSubscriptionGrants",
        "datazone:ListSubscriptionRequests",
        "datazone:ListSubscriptionTargets",
        "datazone:ListSubscriptions",
        "datazone:ListWarehouseMetadata",
        "datazone:RejectPredictions",
        "datazone:RejectSubscriptionRequest",
        "datazone:RevokeSubscription",
        "datazone:Search",
        "datazone:SearchGroupProfiles",
        "datazone:SearchListings",
        "datazone:SearchTypes",
        "datazone:SearchUserProfiles",
        "datazone:StartDataSourceRun",
        "datazone:UpdateDataSource",
        "datazone:UpdateEnvironment",
        "datazone:UpdateEnvironmentBlueprint",
```

```
        "datazone:UpdateEnvironmentDeploymentStatus",
        "datazone:UpdateEnvironmentProfile",
        "datazone:UpdateGlossary",
        "datazone:UpdateGlossaryTerm",
        "datazone:UpdateProject",
        "datazone:UpdateSubscriptionGrantStatus",
        "datazone:UpdateSubscriptionRequest",
        "datazone:StartMetadataGenerationRun",
        "datazone:GetMetadataGenerationRun",
        "datazone:CancelMetadataGenerationRun",
        "datazone:ListMetadataGenerationRuns"
      ],
      "Resource": "*"
    },
    {
      "Sid": "RAMResourceShareStatement",
      "Effect": "Allow",
      "Action": "ram:GetResourceShareAssociations",
      "Resource": "*"
    }
  ]
}
```

AWS política gestionada: AmazonDataZoneSageMakerProvisioning

La AmazonDataZoneSageMakerProvisioning política otorga a Amazon DataZone los permisos necesarios para interoperar con Amazon SageMaker.

```
{
 "Version": "2012-10-17",
 "Statement": [
  {
   "Sid": "CreateSageMakerStudio",
   "Effect": "Allow",
   "Action": [
    "sagemaker:CreateDomain"
   ],
   "Resource": [
    "*"
   ],
   "Condition": {
    "StringEquals": {
```

```
      "aws:CalledViaFirst": [
       "cloudformation.amazonaws.com"
      ]
     },
     "ForAnyValue:StringEquals": {
      "aws:TagKeys": [
       "AmazonDataZoneEnvironment"
      ]
     },
     "Null": {
      "aws:TagKeys": "false",
      "aws:ResourceTag/AmazonDataZoneEnvironment": "false",
      "aws:RequestTag/AmazonDataZoneEnvironment": "false"
     }
    }
   },
   {
    "Sid": "DeleteSageMakerStudio",
    "Effect": "Allow",
    "Action": [
     "sagemaker:DeleteDomain"
    ],
    "Resource": [
     "*"
    ],
    "Condition": {
     "StringEquals": {
      "aws:CalledViaFirst": [
       "cloudformation.amazonaws.com"
      ]
     },
     "ForAnyValue:StringLike": {
      "aws:TagKeys": [
       "AmazonDataZoneEnvironment"
      ]
     },
     "Null": {
      "aws:TagKeys": "false",
      "aws:ResourceTag/AmazonDataZoneEnvironment": "false"
     }
    }
   },
   {
    "Sid": "AmazonDataZoneEnvironmentSageMakerDescribePermissions",
```

```
    "Effect": "Allow",
    "Action": [
     "sagemaker:DescribeDomain"
    ],
    "Resource": "*",
    "Condition": {
     "StringEquals": {
      "aws:CalledViaFirst": [
       "cloudformation.amazonaws.com"
      ]
     }
    }
   },
   {
    "Sid": "IamPassRolePermissions",
    "Effect": "Allow",
    "Action": [
     "iam:PassRole"
    ],
    "Resource": [
     "arn:aws:iam::*:role/sm-provisioning/datazone_usr*"
    ],
    "Condition": {
     "StringEquals": {
      "iam:PassedToService": [
       "glue.amazonaws.com",
       "lakeformation.amazonaws.com",
       "sagemaker.amazonaws.com"
      ],
      "aws:CalledViaFirst": [
       "cloudformation.amazonaws.com"
      ]
     }
    }
   },
   {
    "Sid": "AmazonDataZonePermissionsToCreateEnvironmentRole",
    "Effect": "Allow",
    "Action": [
     "iam:CreateRole",
     "iam:DetachRolePolicy",
     "iam:DeleteRolePolicy",
     "iam:AttachRolePolicy",
     "iam:PutRolePolicy"
```

```
    ],
    "Resource": [
     "arn:aws:iam::*:role/sm-provisioning/datazone_usr*"
    ],
    "Condition": {
     "StringEquals": {
      "aws:CalledViaFirst": [
       "cloudformation.amazonaws.com"
      ],
      "iam:PermissionsBoundary": "arn:aws:iam::aws:policy/
AmazonDataZoneSageMakerEnvironmentRolePermissionsBoundary"
     }
    }
   },
   {
    "Sid": "AmazonDataZonePermissionsToManageEnvironmentRole",
    "Effect": "Allow",
    "Action": [
     "iam:GetRole",
     "iam:GetRolePolicy",
     "iam:DeleteRole"
    ],
    "Resource": [
     "arn:aws:iam::*:role/sm-provisioning/datazone_usr*"
    ],
    "Condition": {
     "StringEquals": {
      "aws:CalledViaFirst": [
       "cloudformation.amazonaws.com"
      ]
     }
    }
   },
   {
    "Sid": "AmazonDataZonePermissionsToCreateSageMakerServiceRole",
    "Effect": "Allow",
    "Action": [
     "iam:CreateServiceLinkedRole"
    ],
    "Resource": [
     "arn:aws:iam::*:role/aws-service-role/sagemaker.amazonaws.com/
AWSServiceRoleForAmazonSageMakerNotebooks"
    ],
    "Condition": {
```

```
    "StringEquals": {
     "aws:CalledViaFirst": [
      "cloudformation.amazonaws.com"
     ]
    }
   }
  },
  {
   "Sid": "AmazonDataZoneEnvironmentParameterValidation",
   "Effect": "Allow",
   "Action": [
    "ec2:DescribeVpcs",
    "ec2:DescribeSubnets",
    "sagemaker:ListDomains"
   ],
   "Resource": "*"
  },
  {
   "Sid": "AmazonDataZoneEnvironmentKMSKeyValidation",
   "Effect": "Allow",
   "Action": [
    "kms:DescribeKey"
   ],
   "Resource": "arn:aws:kms:*:*:key/*",
   "Condition": {
    "Null": {
     "aws:ResourceTag/AmazonDataZoneEnvironment": "false"
    }
   }
  },
  {
   "Sid": "AmazonDataZoneEnvironmentGluePermissions",
   "Effect": "Allow",
   "Action": [
    "glue:CreateConnection",
    "glue:DeleteConnection"
   ],
   "Resource": [
    "arn:aws:glue:*:*:connection/dz-sm-athena-glue-connection-*",
    "arn:aws:glue:*:*:connection/dz-sm-redshift-cluster-connection-*",
    "arn:aws:glue:*:*:connection/dz-sm-redshift-serverless-connection-*",
    "arn:aws:glue:*:*:catalog"
   ],
   "Condition": {
```

```
    "StringEquals": {
     "aws:CalledViaFirst": [
      "cloudformation.amazonaws.com"
     ]
    }
   }
  }
 ]
}
```

AWS política gestionada: AmazonDataZoneSageMakerAccess

Esta política otorga a Amazon DataZone permisos para publicar SageMaker los activos de Amazon en el catálogo. También otorga DataZone permisos a Amazon para conceder o revocar el acceso a los activos SageMaker publicados por Amazon en el catálogo.

Esta política incluye permisos para hacer lo siguiente:

- cloudtrail: recupera información sobre CloudTrail los senderos.
- cloudwatch: recupera las alarmas actuales CloudWatch .
- registros: recupera los filtros de métricas para los CloudWatch registros.
- sns: recupera la lista de suscripciones a un tema de SNS.
- config: recupera información sobre los grabadores de configuración, los recursos y las reglas de AWS configuración. También permite que el rol vinculado al servicio cree y elimine reglas de AWS Config y ejecute evaluaciones en función de las reglas.
- iam: obtiene y genera informes de credenciales para las cuentas.
- organizaciones: recuperan la información de la cuenta y la unidad organizativa (OU) de una organización.
- securityhub: recupera información sobre cómo se configuran el servicio, los estándares y los controles del Security Hub.
- etiqueta: recupera información sobre las etiquetas de recursos.

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

```
    "Sid": "AmazonSageMakerReadPermission",
    "Effect": "Allow",
    "Action": [
     "sagemaker:DescribeFeatureGroup",
     "sagemaker:ListModelPackages",
     "sagemaker:DescribeModelPackage",
     "sagemaker:DescribeModelPackageGroup",
     "sagemaker:DescribeAlgorithm",
     "sagemaker:ListTags",
     "sagemaker:DescribeDomain",
     "sagemaker:GetModelPackageGroupPolicy",
     "sagemaker:Search"
    ],
    "Resource": "*"
   },
   {
    "Sid": "AmazonSageMakerTaggingPermission",
    "Effect": "Allow",
    "Action": [
     "sagemaker:AddTags",
     "sagemaker:DeleteTags"
    ],
    "Resource": "*",
    "Condition": {
     "ForAnyValue:StringLike": {
      "aws:TagKeys": [
       "sagemaker:shared-with:*"
      ]
     }
    }
   },
   {
    "Sid": "AmazonSageMakerModelPackageGroupPolicyPermission",
    "Effect": "Allow",
    "Action": [
     "sagemaker:PutModelPackageGroupPolicy",
     "sagemaker:DeleteModelPackageGroupPolicy"
    ],
    "Resource": [
     "arn:*:sagemaker:*:*:model-package-group/*"
    ]
   },
   {
    "Sid": "AmazonSageMakerRAMPermission",
```

```
    "Effect": "Allow",
    "Action": [
     "ram:GetResourceShares",
     "ram:GetResourceShareInvitations",
     "ram:GetResourceShareAssociations"
    ],
    "Resource": "*"
   },
   {
    "Sid": "AmazonSageMakerRAMResourcePolicyPermission",
    "Effect": "Allow",
    "Action": [
     "sagemaker:PutResourcePolicy",
     "sagemaker:GetResourcePolicy",
     "sagemaker:DeleteResourcePolicy"
    ],
    "Resource": [
     "arn:*:sagemaker:*:*:feature-group/*"
    ]
   },
   {
    "Sid": "AmazonSageMakerRAMTagResourceSharePermission",
    "Effect": "Allow",
    "Action": [
     "ram:TagResource"
    ],
    "Resource": "arn:*:ram:*:*:resource-share/*",
    "Condition": {
     "Null": {
      "aws:RequestTag/AwsDataZoneDomainId": "false"
     }
    }
   },
   {
    "Sid": "AmazonSageMakerRAMDeleteResourceSharePermission",
    "Effect": "Allow",
    "Action": [
     "ram:DeleteResourceShare"
    ],
    "Resource": "arn:*:ram:*:*:resource-share/*",
    "Condition": {
     "Null": {
      "aws:ResourceTag/AwsDataZoneDomainId": "false"
     }
```

```
    }
   },
   {
    "Sid": "AmazonSageMakerRAMCreateResourceSharePermission",
    "Effect": "Allow",
    "Action": [
     "ram:CreateResourceShare"
    ],
    "Resource": "*",
    "Condition": {
     "StringLikeIfExists": {
      "ram:RequestedResourceType": [
       "sagemaker:*"
      ]
     },
     "Null": {
      "aws:RequestTag/AwsDataZoneDomainId": "false"
     }
    }
   },
   {
    "Sid": "AmazonSageMakerS3BucketPolicyPermission",
    "Effect": "Allow",
    "Action": [
     "s3:DeleteBucketPolicy",
     "s3:PutBucketPolicy",
     "s3:GetBucketPolicy"
    ],
    "Resource": [
     "arn:aws:s3:::sagemaker-datazone*",
     "arn:aws:s3:::SageMaker-DataZone*",
     "arn:aws:s3:::datazone-sagemaker*",
     "arn:aws:s3:::DataZone-SageMaker*",
     "arn:aws:s3:::amazon-datazone*"
    ]
   },
   {
    "Sid": "AmazonSageMakerS3Permission",
    "Effect": "Allow",
    "Action": [
     "s3:GetObject",
     "s3:ListBucket"
    ],
    "Resource": [
```

```
    "arn:aws:s3:::sagemaker-datazone*",
    "arn:aws:s3:::SageMaker-DataZone*",
    "arn:aws:s3:::datazone-sagemaker*",
    "arn:aws:s3:::DataZone-SageMaker*",
    "arn:aws:s3:::amazon-datazone*"
   ]
  },
  {
   "Sid": "AmazonSageMakerECRPermission",
   "Effect": "Allow",
   "Action": [
    "ecr:GetRepositoryPolicy",
    "ecr:SetRepositoryPolicy",
    "ecr:DeleteRepositoryPolicy"
   ],
   "Resource": "*",
   "Condition": {
    "Null": {
     "aws:ResourceTag/AmazonDataZoneEnvironment": "false"
    }
   }
  },
  {
   "Sid": "AmazonSageMakerKMSReadPermission",
   "Effect": "Allow",
   "Action": [
    "kms:DescribeKey"
   ],
   "Resource": "*",
   "Condition": {
    "ForAnyValue:StringEquals": {
     "aws:TagKeys": [
      "AmazonDataZoneEnvironment"
     ]
    }
   }
  },
  {
   "Sid": "AmazonSageMakerKMSGrantPermission",
   "Effect": "Allow",
   "Action": [
    "kms:CreateGrant"
   ],
   "Resource": "*",
```

```
    "Condition": {
     "ForAnyValue:StringEquals": {
      "aws:TagKeys": [
       "AmazonDataZoneEnvironment"
      ]
     },
     "ForAllValues:StringEquals": {
      "kms:GrantOperations": [
       "Decrypt"
      ]
     }
    }
   }
  ]
}
```

AWS política gestionada: AmazonDataZoneSageMakerEnvironmentRolePermissionsBoundary

> **Note**
>
> Esta política es un límite de permisos. Un límite de permisos establece los permisos máximos que una política basada en la identidad puede conceder a una entidad de IAM. No debes usar ni adjuntar las políticas de límites de DataZone permisos de Amazon por tu cuenta. Las políticas de límites de DataZone permisos de Amazon solo deben adjuntarse a las funciones DataZone gestionadas por Amazon. Para obtener más información sobre los límites de los permisos, consulte los límites de los permisos para las entidades de IAM en la Guía del usuario de IAM.

Cuando crea un SageMaker entorno de Amazon a través del portal de DataZone datos de Amazon, Amazon DataZone aplica este límite de permisos a las funciones de IAM que se generan durante la creación del entorno. El límite de permisos limita el alcance de las funciones que Amazon DataZone crea y de las funciones que añadas.

Amazon DataZone utiliza la política `AmazonDataZoneSageMakerEnvironmentRolePermissionsBoundary` gestionada para limitar el principal de IAM aprovisionado al que está asociada. Los directores pueden adoptar la forma de las funciones de usuario que Amazon DataZone puede asumir en nombre de los

usuarios empresariales interactivos o de los servicios analíticos (por ejemplo) y AWS SageMaker, a continuación, realizar acciones para procesar datos como leer y escribir desde Amazon S3 o Amazon Redshift o ejecutar AWS Glue Crawler.

La `AmazonDataZoneSageMakerEnvironmentRolePermissionsBoundary` política otorga a Amazon acceso de lectura y escritura DataZone a servicios como Amazon SageMaker, AWS Glue, Amazon S3, AWS Lake Formation, Amazon Redshift y Amazon Athena. La política también otorga permisos de lectura y escritura a algunos recursos de infraestructura necesarios para usar estos servicios, como las interfaces de red, los repositorios de Amazon ECR y las claves de AWS KMS. También da acceso a SageMaker aplicaciones de Amazon como Amazon SageMaker Canvas.

Amazon DataZone aplica la política `AmazonDataZoneSageMakerEnvironmentRolePermissionsBoundary` gestionada como límite de permisos para todos los roles del DataZone entorno de Amazon (propietario y colaborador). Este límite de permisos restringe estas funciones para permitir el acceso únicamente a los recursos y acciones necesarios para un entorno.

```
       {
"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 actualiza las políticas AWS gestionadas

Consulta los detalles sobre las actualizaciones de las políticas AWS gestionadas de Amazon DataZone desde que este servicio comenzó a realizar el seguimiento de estos cambios. Para recibir alertas automáticas sobre los cambios en esta página, suscríbete a la fuente RSS de la página del historial de DataZone documentos de Amazon.

Cambio	Descripción	Fecha
AmazonDataZoneSage MakerEnvironmentRo lePermissionsBoundary - nuevo límite de permisos	Se ha denominado un nuevo límite de permisos AmazonDataZoneSage MakerEnvironmentRo lePermissionsBoundary. Cuando crea un SageMaker entorno de Amazon a través	30 de abril de 2024

Cambio	Descripción	Fecha
	del portal de DataZone datos de Amazon, Amazon DataZone aplica este límite de permisos a las funciones de IAM que se generan durante la creación del entorno. El límite de permisos limita el alcance de las funciones que Amazon DataZone crea y de las funciones que añadas.	
AmazonDataZoneSage MakerAccess - nueva política	La nueva política llamada AmazonDataZoneSage MakerAccessotorga DataZone permisos a Amazon para publicar SageMaker los activos de Amazon en el catálogo. También otorga DataZone permisos a Amazon para conceder o revocar el acceso a los activos SageMaker publicados por Amazon en el catálogo.	30 de abril de 2024

Cambio	Descripción	Fecha
AmazonDataZoneFullAccess - actualización de la política	Una actualización de la AmazonDataZoneFull Accesspolítica que añade acceso a las `DescribeS ecurityGroups` acciones para mejorar la usabilidad de los administradores de cuentas que configuran los planes en la consola y a las `GetPolicy` acciones que ayudan a recuperar informaci ón sobre la política gestionada especificada.	30 de abril de 2024
AmazonDataZoneSage MakerProvisioning - nueva política	La nueva política denominad a AmazonDataZoneSage MakerProvisioningconcede a Amazon DataZone los permisos necesarios para interoperar con Amazon SageMaker.	30 de abril de 2024
AmazonDataZoneS3Manage- <region>- - <domainId>- nuevo rol	Nueva función denominad a AmazonDataZoneS3Ma nage-, <region><domainId> que se utiliza cuando Amazon DataZone llama a AWS Lake Formation para registrar una ubicación del Amazon Simple Storage Service (Amazon S3). AWS Lake Formation asume esta función al acceder a los datos de esa ubicación.	1 de abril de 2024

Cambio	Descripción	Fecha
AmazonDataZoneGlue ManageAccessRolePolicy - Actualización de la política	Se actualizó AmazonDat aZoneGlueManageAcc essRolePolicypara habilitar la compatibilidad con los permisos que permiten DataZone a Amazon habilitar la publicación y las concesion es de acceso a los datos.	1 de abril de 2024
AmazonDataZoneDoma inExecutionRolePolicy y AmazonDataZoneFull UserAccess - Actualización de la política	Se actualizó el AmazonDat aZoneDomainExecuti onRolePolicyy AmazonDat aZoneFullUserAccesspara habilitar la compatibilidad con la `CancelMetadataGene rationRun` API.	29 de marzo de 2024
AmazonDataZoneFullAccess - Actualización de la política	Se actualizó `AmazonDat aZoneFullAccess` para permitir a los usuarios elegir sus secretos, clústeres, vpc y subredes en la consola de DataZone administración de Amazon en lugar de escribirl os en un cuadro de texto.	13 de marzo de 2024

Cambio	Descripción	Fecha
AmazonDataZoneDomainExecutionRolePolicy - Actualización de la política	Se actualizó AmazonDataZoneDomainExecutionRolePolicypara permitir la compatibilidad con la `ListEnvironmentBlueprintConfigurationSummaries` API necesaria para crear perfiles de entorno, identificando qué blueprints están habilitados en cada cuenta y región.	1 de febrero de 2024
AmazonDataZoneGlueManageAccessRolePolicy - Actualización de la política	Se actualizó AmazonDataZoneGlueManageAccessRolePolicypara habilitar la compatibilidad con el modo híbrido AWS Lake Formation.	14 de diciembre de 2023
AmazonDataZoneFullUserAccess y AmazonDataZoneDomainExecutionRolePolicy - Actualizaciones de la política	Se actualizaron las políticas AmazonDataZoneFullUserAccessy las AmazonDataZoneDomainExecutionRolePolicypolíticas para admitir la funcionalidad generativa de descripciones de datos basada en IA en Amazon. DataZone	28 de noviembre de 2023

Cambio	Descripción	Fecha
AmazonDataZoneEnvironmentRolePermissionsBoundary - Actualización de la política	Amazon DataZone ha realizado una actualización de la política AmazonDataZoneEnvironmentRolePermissionsBoundarygestionada que consiste en un `athena:GetQueryResultsStream` permiso adicional con el alcance de la `ResourceTag` condición.	17 de noviembre de 2023
AmazonDataZoneRedshiftManageAccessRolePolicy - Actualización de la política	Amazon la DataZone actualizó AmazonDataZoneRedshiftManageAccessRolePolicyeliminando la verificación del ID de la organización para la `redshift:AssociateDataShareConsumer` acción. Esto le permite compartir recursos entre AWS organizaciones.	16 de noviembre de 2023
AmazonDataZoneFullUserAccess - Actualización de la política	Amazon DataZone actualizó la AmazonDataZoneFullUserAccesspolítica que otorga acceso total a Amazon DataZone, pero no permite la administración de dominios, usuarios o cuentas asociadas.	2 de octubre de 2023
AmazonDataZonePortalFullAccessPolicy - política obsoleta	Amazon DataZone dejó en desuso el AmazonDataZonePortalFullAccessPolicy.	29 de septiembre de 2023

Cambio	Descripción	Fecha
AmazonDataZonePrev iewConsoleFullAccess - política obsoleta	Amazon DataZone dejó en desuso el AmazonDat aZonePreviewConsol eFullAccess.	29 de septiembre de 2023
AmazonDataZoneDoma inExecutionRolePolicy - Nueva política	Amazon DataZone agregó una nueva política llamada AmazonDataZoneDoma inExecutionRolePolicy. Esta es la política predeterm inada para el rol de DataZone `AmazonDataZoneDoma inExecutionRole` servicio de Amazon. Amazon utiliza esta función DataZone para catalogar, descubrir, gobernar, compartir y analizar datos en el DataZone dominio de Amazon. Puede adjuntar la `AmazonDat aZoneDomainExecuti onRolePolicy` política a su`AmazonDataZoneDoma inExecutionRole` .	25 de septiembre de 2023
AmazonDataZoneCros sAccountAdmin - Nueva política	Amazon DataZone agregó una nueva política llamada AmazonDataZoneCros sAccountAdminque permite a los usuarios trabajar con Amazon DataZone y sus cuentas asociadas.	19 de septiembre de 2023

Cambio	Descripción	Fecha
AmazonDataZoneFull UserAccess - Nueva política	Amazon DataZone agregó una nueva política llamada AmazonDataZoneFull UserAccessque otorga acceso total a Amazon DataZone, pero no permite la administr ación de dominios, usuarios o cuentas asociadas.	12 de septiembre de 2023
AmazonDataZoneReds hiftManageAccessRolePolicy - Nueva política	Amazon DataZone agregó una nueva política llamada AmazonDataZoneReds hiftManageAccessRo lePolicyque otorga permisos para permitir que Amazon habilite DataZone la publicaci ón y las concesiones de acceso a los datos.	12 de septiembre de 2023
AmazonDataZoneGlue ManageAccessRolePolicy - Nueva política	Amazon DataZone agregó una nueva política llamada AmazonDataZoneGlue ManageAccessRolePolicyque otorga DataZone permisos a Amazon para publicar datos de AWS Glue en el catálogo. También otorga a Amazon DataZone permisos para conceder o revocar el acceso a los activos publicados por AWS Glue en el catálogo.	12 de septiembre de 2023

Cambio	Descripción	Fecha
AmazonDataZoneReds hiftGlueProvisioningPolicy - Nueva política	Amazon DataZone agregó una nueva política llamada AmazonDataZoneReds hiftGlueProvisioningPolicyque otorga a Amazon DataZone los permisos necesarios para interoperar con las fuentes de datos compatibles.	12 de septiembre de 2023
AmazonDataZoneEnvi ronmentRolePermiss ionsBoundary - Nueva política	Amazon DataZone agregó una nueva política llamada AmazonDataZoneEnvi ronmentRolePermiss ionsBoundaryque limita el principal de IAM aprovisionado al que está asociado.	12 de septiembre de 2023
AmazonDataZoneFullAccess - Nueva política	Amazon DataZone agregó una nueva política llamada AmazonDataZoneFull Accessque proporciona acceso total a Amazon a DataZone través de la consola AWS de administración.	12 de septiembre de 2023
Actualización de la política administrada	Actualizaciones de la política AmazonDataZonePrev iewConsoleFullAcce ssgestionada que consiste en `iam:GetPolicy` permisos adicionales.	13 de junio de 2023

Cambio	Descripción	Fecha
Amazon DataZone comenzó a rastrear los cambios	Amazon DataZone comenzó a realizar un seguimiento de los cambios en sus políticas AWS gestionadas.	20 de marzo de 2023

Funciones de IAM para Amazon DataZone

Temas

AmazonDataZoneProvisioningRole-<domainAccountId>

El `AmazonDataZoneProvisioningRole-<domainAccountId>` tiene lo `AmazonDataZoneRedshiftGlueProvisioningPolicy` adjunto. Esta función otorga a Amazon DataZone los permisos necesarios para interoperar con AWS Glue y Amazon Redshift.

El valor predeterminado `AmazonDataZoneProvisioningRole-<domainAccountId>` incluye la siguiente política de confianza:

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

```
      "Action": "sts:AssumeRole",
      "Condition": {
        "StringEquals": {
            "aws:SourceAccount": "{{domain_account}}"
        }
      }
    }
  ]
}
```

AmazonDataZoneDomainExecutionRole

AmazonDataZoneDomainExecutionRoleTiene la política AWS gestionada AmazonDataZoneDomainExecutionRolePolicyadjunta. Amazon DataZone crea este rol para ti en tu nombre. Para determinadas acciones del portal de datos, Amazon DataZone asume esta función en la cuenta en la que se creó la función y comprueba que esta función está autorizada para realizar la acción.

El AmazonDataZoneDomainExecutionRolerol es obligatorio en el Cuenta de AWS que se aloja tu DataZone dominio de Amazon. Este rol se crea automáticamente cuando creas tu DataZone dominio de Amazon.

El AmazonDataZoneDomainExecutionRolerol predeterminado tiene la siguiente política de confianza.

```
{
    "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>

El `AmazonDataZoneGlueAccess-<region>-<domainId>` papel tiene algo que `AmazonDataZoneGlueManageAccessRolePolicy` ver. Esta función otorga a Amazon DataZone permisos para publicar datos de AWS Glue en el catálogo. También otorga a Amazon DataZone permisos para conceder o revocar el acceso a los activos publicados por AWS Glue en el catálogo.

El `AmazonDataZoneGlueAccess-<region>-<domainId>` rol predeterminado incluye la siguiente política de confianza:

```
{
  "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>

El `AmazonDataZoneRedshiftAccess-<region>-<domainId>` papel tiene algo que `AmazonDataZoneRedshiftManageAccessRolePolicy` ver. Esta función otorga a Amazon DataZone permisos para publicar datos de Amazon Redshift en el catálogo. También otorga DataZone permisos a Amazon para conceder o revocar el acceso a los activos publicados en el catálogo de Amazon Redshift o Amazon Redshift Serverless.

El `AmazonDataZoneRedshiftAccess-<region>-<domainId>` rol predeterminado incluye la siguiente política de permisos en línea:

```
{
   "Version":"2012-10-17",
   "Statement":[
      {
         "Sid": "RedshiftSecretStatement",
         "Effect":"Allow",
         "Action":"secretsmanager:GetSecretValue",
         "Resource":"*",
         "Condition":{
            "StringEquals":{
               "secretsmanager:ResourceTag/AmazonDataZoneDomain":"{{domainId}}"
            }
         }
      }
   ]
}
```

El valor predeterminado `AmazonDataZoneRedshiftManageAccessRole<timestamp>` incluye la siguiente política de confianza:

```
{
  "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>

El AmazonDataZone S3Manage- <region>- <domainId>se utiliza cuando Amazon DataZone llama a AWS Lake Formation para registrar una ubicación del Amazon Simple Storage Service (Amazon S3). AWS Lake Formation asume esta función al acceder a los datos de esa ubicación. Para obtener más información, consulte los requisitos de las funciones utilizadas para registrar ubicaciones.

Este rol tiene adjunta la siguiente política de permisos en línea.

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

El AmazonDataZone S3Manage- <region>- <domainId>tiene adjunta la siguiente política de confianza:

```
{
    "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>

El `AmazonDataZoneSageMakerManageAccessRole` rol tiene las `AmazonDataZoneSageMakerAccessAmazonDataZoneRedshiftManageAccessRolePolicy`, las y las `AmazonDataZoneGlueManageAccessRolePolicy` adjuntas. Este rol otorga a Amazon DataZone permisos para publicar y administrar suscripciones para activos de data lake, data warehouse y Amazon Sagemaker.

El `AmazonDataZoneSageMakerManageAccessRole` rol tiene la siguiente política en línea adjunta:

```
{
   "Version":"2012-10-17",
   "Statement":[
      {
         "Sid": "RedshiftSecretStatement",
         "Effect":"Allow",
         "Action":"secretsmanager:GetSecretValue",
         "Resource":"*",
         "Condition":{
            "StringEquals":{
               "secretsmanager:ResourceTag/AmazonDataZoneDomain":"{{domainId}}"
            }
         }
      }
   ]
}
```

El `AmazonDataZoneSageMakerManageAccessRole` rol tiene la siguiente política de confianza adjunta:

```
{
  "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>

El `AmazonDataZoneSageMakerProvisioningRole` rol tiene la `AmazonDataZoneSageMakerProvisioning` y la `AmazonDataZoneRedshiftGlueProvisioningPolicy` adjunta. Esta función otorga a Amazon DataZone los permisos necesarios para interoperar con AWS Glue, Amazon Redshift y Amazon Sagemaker.

El `AmazonDataZoneSageMakerProvisioningRole` rol incluye la siguiente política en línea:

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Sid": "SageMakerStudioTagOnCreate",
            "Effect": "Allow",
            "Action": [
                "sagemaker:AddTags"
            ],
            "Resource": "arn:aws:sagemaker:*:{{AccountId}}:*/*",
            "Condition": {
                "Null": {
                    "sagemaker:TaggingAction": "false"
                }
```

```
            }
        }
    ]
}
```

El `AmazonDataZoneSageMakerProvisioningRole` rol tiene la siguiente política de confianza adjunta:

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Sid": "DataZoneTrustPolicyStatement",
      "Effect": "Allow",
      "Principal": {
        "Service": "datazone.amazonaws.com"
      },
      "Action": "sts:AssumeRole",
      "Condition": {
        "StringEquals": {
            "aws:SourceAccount": "{{domain_account}}"
        }
      }
    }
  ]
}
```

Funciones basadas en la identidad

Las políticas basadas en identidad son documentos de políticas de permisos JSON que puede asociar a una identidad, como un usuario de IAM, un grupo de usuarios o un rol. Estas políticas controlan qué acciones pueden realizar los usuarios y los roles, en qué recursos y en qué condiciones. Para obtener más información sobre cómo crear una política basada en identidad, consulte Creación de políticas de IAM en la Guía del usuario de IAM.

Con las políticas basadas en identidades de IAM, puede especificar las acciones y los recursos permitidos o denegados, así como las condiciones en las que se permiten o deniegan las acciones. No es posible especificar la entidad principal en una política basada en identidad porque se aplica

al usuario o rol al que está adjunto. Para más información sobre los elementos que puede utilizar en una política de JSON, consulte Referencia de los elementos de las políticas de JSON de IAM en la Guía del usuario de IAM.

Al crear un DataZone proyecto de Amazon, en el portal, se crean tres funciones de IAM para este proyecto, una para cada tipo de función de miembro del proyecto: propietario y colaborador. Los permisos asociados a cada rol dependen del rol del proyecto, y las políticas de permisos asociadas dependen de las capacidades con las que se implemente el proyecto.

Para DataZone que Amazon gestione los permisos y comparta activos con los proyectos de los suscriptores, los roles de usuario del proyecto de suscriptor se añaden automáticamente como administrador del lago de datos AWS Lake Formation en el Cuenta de AWS que se publican los activos.

Puedes ver la mayoría de las up-to-date versiones del rol en la consola de administración de AWS IAM o revisar los permisos de los distintos roles en la siguiente tabla.

Permisos de propietario del proyecto

Tipo de entorno	Permisos de IAM
Lago de datos predeterminado	Esta es la combinación de las capacidades Essential, Data Lake Producer y Data Lake Consumer.

Essential	<pre>{
	  "Version": "2012-10-17",
	  "Statement": [
	  {
	  "Effect": "Allow",
	  "Action": [
	  "s3:List*",
	  "s3:Get*",
	  "s3:Describe*",
	  "s3:DeleteObjectVersion",
	  "s3:RestoreObject",</pre>

Tipo de entorno	Permisos de IAM	

```
        "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"
    },
    {
      "Action":
 ["kms:ListKeys",
 "kms:ListAliases"],
      "Resource": "*",
```

Tipo de entorno	Permisos de IAM
	"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" }, { "Effect": "Allow", "Action": [

Tipo de entorno	Permisos de IAM	

```
        "s3:Get*",
        "s3:List*",
        "kms:List*",
        "kms:Get*",
        "kms:Desc
ribe*",
        "kms:Decrypt"
      ],
      "Resource": "*",
      "Condition": {
        "StringNo
tEquals": {
          "aws:Reso
urceAccount":
 "project-account-id"
        }
      }
    }
  ]
}
```

Tipo de entorno	Permisos de IAM
Productor 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:DeleteColumn

Tipo de entorno	Permisos de IAM	

```
StatisticsForParti
tion",

 "glue:DeleteColumn
StatisticsForTable",

 "glue:DeletePartit
ionIndex",

 "glue:UpdateColumn
StatisticsForParti
tion",

 "glue:UpdateColumn
StatisticsForTable",

 "glue:BatchDeleteT
ableVersion",

 "glue:BatchDeleteT
able",

 "glue:CreatePartit
ion",

 "glue:DeletePartit
ion",

 "glue:UpdatePartit
ion"
            ],
            "Resource":
 [

 "arn:aws:glue:regi
on:account:database/
dbName",

 "arn:aws:glue:regi
on:account:catalog",

 "arn:aws:glue:regi
```

Tipo de entorno	Permisos de IAM	

```
on:account:table/d
bName/*"
            ]
        },
        {
            "Sid":
 "VisualEditor0",
            "Effect":
 "Allow",
            "Action": [

 "glue:SearchTables",

 "glue:NotifyEvent",

 "glue:StartBluepri
ntRun",

 "glue:PutWorkflowR
unProperties",

 "glue:StopCrawler",

 "glue:DeleteJob",

 "glue:DeleteWorkfl
ow",

 "glue:UpdateCrawler",

 "glue:DeleteBluepr
int",

 "glue:UpdateWorkfl
ow",

 "glue:StartCrawler",

 "glue:ResetJobBook
mark",

 "glue:UpdateJob",
```

Tipo de entorno	Permisos de IAM	

```
 "glue:StartWorkflo
wRun",

 "glue:StopCrawlerS
chedule",

 "glue:ResumeWorkfl
owRun",

 "glue:List*",

 "glue:DeleteCrawler",

 "glue:UpdateBluepr
int",

 "glue:BatchStopJob
Run",

 "glue:StopWorkflow
Run",

 "glue:BatchGet*",

 "glue:UpdateCrawle
rSchedule",

 "glue:DeleteConnec
tion",

 "glue:UpdateConnec
tion",

 "glue:Get*",

 "glue:BatchDeleteC
onnection",

 "glue:StartCrawler
Schedule",
```

Tipo de entorno	Permisos de IAM	

```
 "glue:StartJobRun",

 "glue:CreateWorkfl
ow",

 "glue:PublishDataQ
uality",

 "glue:*DataQuality*"
           ],
           "Resource":
 "*",
           "Conditio
n": {

 "ForAnyValue:Strin
gEquals": {

 "aws:ResourceTag/n
oah-analytics:proj
ectId": "projectId"
               }
           }
       },
       {
           "Sid":
 "CreateGlueResourc
es",
           "Effect":
 "Allow",
           "Action": [

 "glue:CreateBluepr
int",

 "glue:CreateJob",

 "glue:CreateConnec
tion",

 "glue:CreateCrawler",
```

Tipo de entorno	Permisos de IAM

```
 "glue:CreateDataQu
alityRuleset"
            ],
            "Resource":
 "*"
        },
        {
            "Sid":
 "VisualEditor0",
            "Effect":
 "Allow",
            "Action": [

 "iam:ListRoles",

 "iam:ListUsers",

 "iam:ListGroups",

 "iam:ListRolePolic
ies",

 "iam:GetRole",

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

Tipo de entorno	Permisos de IAM
Consumidor 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",

Tipo de entorno	Permisos de IAM	

```
        "athena:E
xportNotebook",
        "athena:S
topQueryExecution",
        "athena:S
tartCalculationExe
cution",
        "athena:S
tartSession",
        "athena:C
reatePresignedNote
bookUrl",
        "athena:C
reateNotebook",
        "athena:I
mportNotebook"
      ],
      "Resource": [
        "arn:aws:
athena:region:acco
unt-id:workgroup/w
orkGroupName",
        "arn:aws:
athena:region:acco
unt-id:datacatalog/
AwsDataCatalog"
      ]
    },
    {
      "Effect": "Allow",
      "Action": [
        "athena:L
istWorkGroups",
        "athena:L
istDataCatalogs",
        "athena:List*"
      ],
      "Resource": ["*"]
    },
    {
      "Effect": "Allow",
      "Action": [
```

Tipo de entorno	Permisos de IAM	

```
        "glue:Bat
chGet*",
        "glue:Get*",
        "glue:Sea
rchTables",
        "glue:List*"
      ],
      "Resource": [
        "arn:aws:
glue:region:account-
id:database/dbName",
        "arn:aws:
glue:region:account-
id:catalog",
        "arn:aws:
glue:region:account-
id:table/dbName/*"
      ]
    }
  ]
}
```

Tipo de entorno	Permisos de IAM

Productor de almacenes de datos	{
	  "Version": "2012-10-17",
	  "Statement": [
	    {
	      "Effect": "Allow",
	      "Action": [
	        "redshift:GetClusterCredentials",
	        "redshift:JoinGroup",
	        "redshift:CreateClusterUser",
	        "redshift:DescribeClusters"
	      ],
	      "Resource": "arn:aws:redshift:region:account:cluster:producerRedshiftCluster"
	    },
	    {
	      "Effect": "Allow",
	      "Action": [
	        "redshift-data:DescribeStatement",
	        "redshift-data:ExecuteStatement"
	      ],
	      "Resource": "arn:aws:redshift:region:account:cluster:producerRedshiftCluster"
	    }
	  ]
	}

Tipo de entorno	Permisos de IAM	

Tipo de entorno	Permisos de IAM

Consumidor de almacenes de datos	{
	  "Version": "2012-10-17",
	  "Statement": [
	  {
	  "Effect": "Allow",
	  "Action": [
	  "redshift:GetClusterCredentials",
	  "redshift:JoinGroup",
	  "redshift:CreateClusterUser",
	  "redshift:DescribeClusters"
	  ],
	  "Resource": [
	  "arn:aws:redshift:region:account:dbuser:cluster-identifier/dbUser",
	  "arn:aws:redshift:region:account:dbgroup:cluster-identifier/project_owner@projectName",
	  "arn:aws:redshift:region:account:dbname:cluster-identifier/*"
	  ],
	  "Condition": {
	  "ForAnyValue:StringEquals": {
	  "aws:PrincipalTag/RedshiftDbUser": "dbUser"
	  }

Tipo de entorno	Permisos de IAM	
	`}, { "Sid": "VisualEditor2", "Effect": "Allow", "Action": [ "redshift-data:DescribeStatement", "redshift-data:ExecuteStatement" ], "Resource": "arn:aws:redshift:region:account-id:cluster:cluster-identifier" } ] }`	

Tipo de entorno	Permisos de IAM

Editor de consultas de Amazon Redshift v2	{
	  "Version": "2012-10-17",
	  "Statement": [
	    {
	      "Action": "redshift:DescribeClusters",
	      "Effect": "Allow",
	      "Resource": "arn:aws:redshift:region:account-id:cluster:*",
	      "Sid": "RedshiftPermissions"
	    },
	    {
	      "Action": "tag:GetResources",
	      "Condition": {
	        "StringEquals": { "aws:CalledViaLast": "sqlworkbench.amazonaws.com" }
	      },
	      "Effect": "Allow",
	      "Resource": "*",
	      "Sid": "ResourceGroupsTaggingPermissions"
	    },
	    {
	      "Action": [
	        "sqlworkbench:DriverExecute",
	        "sqlworkbench:GenerateSession",

Tipo de entorno	Permisos de IAM	

```
        "sqlworkb
ench:ListConnectio
ns",
        "sqlworkb
ench:ListDatabases",
        "sqlworkb
ench:ListFiles",
        "sqlworkb
ench:ListNotebooks",
        "sqlworkb
ench:ListQueryExec
utionHistory",
        "sqlworkb
ench:ListRedshiftC
lusters",
        "sqlworkb
ench:ListSampleDat
abases",
        "sqlworkb
ench:ListTabs",
        "sqlworkb
ench:ListTaggedRes
ources"
      ],
      "Effect": "Allow",
      "Resource": "*",
      "Sid": "AmazonRe
dshiftQueryEditorV
2PermissionsPart1"
    },
    {
      "Action":
 "sqlworkbench:*",
      "Effect": "Allow",
      "Resource": [
        "arn:aws:
sqlworkbench:regio
n:account-id:query/
*",
        "arn:aws:
sqlworkbench:regio
```

Tipo de entorno	Permisos de 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" }] }

Permisos de colaborador del proyecto

Tipo de entorno	Permisos de IAM
Lago de datos predeterminado	Esta es la combinación de las capacidades Essential, Data Lake Producer y Data Lake Consumer.
Essential	{ "Version": "2012-10- 17", "Statement": [{ "Effect": "Allow",

Tipo de entorno	Permisos de IAM	

```
      "Action": [
        "s3:List*",
        "s3:Get*",
        "s3:Describe*",
        "s3:Delet
eObjectVersion",
        "s3:Resto
reObject",
        "s3:Repli
cateObject",
        "s3:PutObject",
        "s3:Abort
MultipartUpload",
        "s3:PutOb
jectRetention",
        "s3:Delet
eObject"
      ],
      "Resource":
 ["s3BucketArn",
 "s3BucketArn/*"]
    },
    { "Action":
 ["s3:List*"],
 "Resource": "*",
 "Effect": "Allow" },
    {
      "Action": [
        "kms:List*",
        "kms:Get*",
        "kms:Desc
ribe*",
        "kms:Decrypt",
        "kms:Encrypt",
        "kms:ReEn
crypt*",
        "kms:Verify",
        "kms:Sign",
        "kms:Gene
rateDataKey"
      ],
```

Tipo de entorno	Permisos de IAM	

```
      "Resource":
 "keyArn",
      "Effect": "Allow"
    },
    {
      "Action":
 ["kms:ListKeys",
 "kms:ListAliases"],
      "Resource": "*",
      "Effect": "Allow"
    },
    {
      "Action": [
        "ec2:Desc
ribeSecurityGroups",
        "ec2:Desc
ribeSecurityGroupR
ules",
        "ec2:Desc
ribeTags"
      ],
      "Resource": "*",
      "Effect": "Allow"
    },
    {
      "Action": [
        "logs:Des
cribe*",
        "logs:Sta
rtQuery",
        "logs:Sto
pQuery",
        "logs:Get*",
        "logs:List*",
        "logs:Put
LogEvents",
        "logs:Cre
ateLogStream",
        "logs:Fil
terLogEvents"
      ],
```

Tipo de entorno	Permisos de IAM
	"Resource": "arn:aws:logs:region:account-id:log-group:log-group-name:*", "Effect": "Allow" }, { "Effect": "Allow", "Action": ["s3:Get*", "s3:List*", "kms:List*", "kms:Get*", "kms:Describe*", "kms:Decrypt"], "Resource": "*", "Condition": { "StringNotEquals": { "aws:ResourceAccount": "project-account-id" } } }] }

Tipo de entorno	Permisos de IAM

Productor de Data Lake	{
	  "Version": "2012-10-17",
	  "Statement": [
	  {
	  "Effect": "Allow",
	  "Action": [
	  "glue:BatchGet*",
	  "glue:Get*",
	  "glue:SearchTables",
	  "glue:List*",
	  "glue:BatchCreatePartition",
	  "glue:CreatePartitionIndex",
	  "glue:CreateTable",
	  "glue:BatchUpdatePartition",
	  "glue:BatchDeletePartition",
	  "glue:UpdateTable",
	  "glue:DeleteTableVersion",
	  "glue:DeleteTable",
	  "glue:DeleteColumnStatisticsForPartition",
	  "glue:DeleteColumnStatisticsForTable",
	  "glue:DeletePartitionIndex",
	  "glue:UpdateColumnStatisticsForPartition",

Tipo de entorno	Permisos de IAM	

```
        "glue:Upd
ateColumnStatistic
sForTable",
        "glue:Bat
chDeleteTableVersi
on",
        "glue:Bat
chDeleteTable",
        "glue:Cre
atePartition",
        "glue:Del
etePartition",
        "glue:Upd
atePartition"
      ],
      "Resource": [
        "arn:aws:
glue:region:accoun
t:database/dbName",
        "arn:aws:
glue:region:accoun
t:catalog",
        "arn:aws:
glue:region:accoun
t:table/dbName/*"
      ]
    },
    {
      "Sid": "VisualEd
itor0",
      "Effect": "Allow",
      "Action": [
        "glue:Sea
rchTables",
        "glue:Not
ifyEvent",
        "glue:Sta
rtBlueprintRun",
        "glue:Put
WorkflowRunPropert
ies",
```

Tipo de entorno	Permisos de IAM	

```
        "glue:Sto
pCrawler",
        "glue:Del
eteJob",
        "glue:Del
eteWorkflow",
        "glue:Upd
ateCrawler",
        "glue:Del
eteBlueprint",
        "glue:Upd
ateWorkflow",
        "glue:Sta
rtCrawler",
        "glue:Res
etJobBookmark",
        "glue:Upd
ateJob",
        "glue:Sta
rtWorkflowRun",
        "glue:Sto
pCrawlerSchedule",
        "glue:Res
umeWorkflowRun",
        "glue:List*",
        "glue:Del
eteCrawler",
        "glue:Upd
ateBlueprint",
        "glue:Bat
chStopJobRun",
        "glue:Sto
pWorkflowRun",
        "glue:Bat
chGet*",
        "glue:Upd
ateCrawlerSchedule",
        "glue:Del
eteConnection",
        "glue:Upd
ateConnection",
        "glue:Get*",
```

Tipo de entorno	Permisos de IAM	

```
        "glue:Bat
chDeleteConnection",
        "glue:Sta
rtCrawlerSchedule",
        "glue:Sta
rtJobRun",
        "glue:Cre
ateWorkflow",
        "glue:Pub
lishDataQuality",
        "glue:*Da
taQuality*"
      ],
      "Resource": "*",
      "Condition": {
        "ForAnyVa
lue:StringEquals": {
          "aws:Reso
urceTag/noah-analy
tics:projectId":
 "projectId"
        }
      }
    },
    {
      "Sid": "CreateGl
ueResources",
      "Effect": "Allow",
      "Action": [
        "glue:Cre
ateBlueprint",
        "glue:Cre
ateJob",
        "glue:Cre
ateConnection",
        "glue:Cre
ateCrawler",
        "glue:Cre
ateDataQualityRule
set"
      ],
      "Resource": "*"
```

Tipo de entorno	Permisos de IAM	

```
    },
    {
      "Sid": "VisualEd
itor0",
      "Effect": "Allow",
      "Action": [
        "iam:List
Roles",
        "iam:List
Users",
        "iam:List
Groups",
        "iam:List
RolePolicies",
        "iam:GetRole",
        "iam:GetR
olePolicy"
      ],
      "Resource": "*"
    }
  ]
}
```

Tipo de entorno	Permisos de IAM

Consumidor 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",

Tipo de entorno	Permisos de IAM

```
        "athena:E
xportNotebook",
        "athena:S
topQueryExecution",
        "athena:S
tartCalculationExe
cution",
        "athena:S
tartSession",
        "athena:C
reatePresignedNote
bookUrl",
        "athena:C
reateNotebook",
        "athena:I
mportNotebook"
      ],
      "Resource": [
        "arn:aws:
athena:region:acco
unt-id:workgroup/w
orkGroupName",
        "arn:aws:
athena:region:acco
unt-id:datacatalog/
AwsDataCatalog"
      ]
    },
    {
      "Effect": "Allow",
      "Action": [
        "athena:L
istWorkGroups",
        "athena:L
istDataCatalogs",
        "athena:List*"
      ],
      "Resource": ["*"]
    },
    {
      "Effect": "Allow",
      "Action": [
```

Tipo de entorno	Permisos de IAM	

```
        "glue:Bat
chGet*",
        "glue:Get*",
        "glue:Sea
rchTables",
        "glue:List*"
      ],
      "Resource": [
        "arn:aws:
glue:region:account-
id:database/dbName",
        "arn:aws:
glue:region:account-
id:catalog",
        "arn:aws:
glue:region:account-
id:table/dbName/*"
      ]
    }
  ]
}
```

Tipo de entorno	Permisos de IAM

Productor de almacenes de datos	{
	  "Version": "2012-10-17",
	  "Statement": [
	    {
	      "Effect": "Allow",
	      "Action": [
	        "redshift:GetClusterCredentials",
	        "redshift:JoinGroup",
	        "redshift:CreateClusterUser",
	        "redshift:DescribeClusters"
	      ],
	      "Resource": "arn:aws:redshift:region:account:cluster:producerRedshiftCluster"
	    },
	    {
	      "Effect": "Allow",
	      "Action": [
	        "redshift-data:DescribeStatement",
	        "redshift-data:ExecuteStatement"
	      ],
	      "Resource": "arn:aws:redshift:region:account:cluster:producerRedshiftCluster"
	    }
	  ]
	}

Tipo de entorno	Permisos de IAM	

Tipo de entorno	Permisos de IAM

Consumidor de almacenes de datos	{
	  "Version": "2012-10-17",
	  "Statement": [
	  {
	  "Effect": "Allow",
	  "Action": [
	  "redshift:GetClusterCredentials",
	  "redshift:JoinGroup",
	  "redshift:CreateClusterUser",
	  "redshift:DescribeClusters"
	  ],
	  "Resource": [
	  "arn:aws:redshift:region:account:dbuser:cluster-identifier/dbUser",
	  "arn:aws:redshift:region:account:dbgroup:cluster-identifier/project_owner@projectName",
	  "arn:aws:redshift:region:account:dbname:cluster-identifier/*"
	  ],
	  "Condition": {
	  "ForAnyValue:StringEquals": {
	  "aws:PrincipalTag/RedshiftDbUser": "dbUser"
	  }

Tipo de entorno	Permisos de IAM	
	`}, { "Sid": "VisualEditor2", "Effect": "Allow", "Action": [ "redshift-data:DescribeStatement", "redshift-data:ExecuteStatement" ], "Resource": "arn:aws:redshift:region:account-id:cluster:cluster-identifier" } ] }`	

Tipo de entorno	Permisos de IAM

Editor de consultas de Amazon Redshift v2	{
	  "Version": "2012-10-17",
	  "Statement": [
	    {
	      "Action": "redshift:DescribeClusters",
	      "Effect": "Allow",
	      "Resource": "arn:aws:redshift:region:account-id:cluster:*",
	      "Sid": "RedshiftPermissions"
	    },
	    {
	      "Action": "tag:GetResources",
	      "Condition": {
	        "StringEquals": { "aws:CalledViaLast": "sqlworkbench.amazonaws.com" }
	      },
	      "Effect": "Allow",
	      "Resource": "*",
	      "Sid": "ResourceGroupsTaggingPermissions"
	    },
	    {
	      "Action": [
	        "sqlworkbench:DriverExecute",
	        "sqlworkbench:GenerateSession",

Tipo de entorno	Permisos de IAM	

```
        "sqlworkb
ench:ListConnectio
ns",
        "sqlworkb
ench:ListDatabases",
        "sqlworkb
ench:ListFiles",
        "sqlworkb
ench:ListNotebooks",
        "sqlworkb
ench:ListQueryExec
utionHistory",
        "sqlworkb
ench:ListRedshiftC
lusters",
        "sqlworkb
ench:ListSampleDat
abases",
        "sqlworkb
ench:ListTabs",
        "sqlworkb
ench:ListTaggedRes
ources"
      ],
      "Effect": "Allow",
      "Resource": "*",
      "Sid": "AmazonRe
dshiftQueryEditorV
2PermissionsPart1"
    },
    {
      "Action":
 "sqlworkbench:*",
      "Effect": "Allow",
      "Resource": [
        "arn:aws:
sqlworkbench:regio
n:account-id:query/
*",
        "arn:aws:
sqlworkbench:regio
```

Tipo de entorno	Permisos de 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"
    }
  ]
}
```

Credenciales temporales

Algunos AWS servicios no funcionan cuando inicias sesión con credenciales temporales. Para obtener información adicional, incluidos AWS los servicios que funcionan con credenciales temporales, consulte AWS los servicios que funcionan con IAM en la Guía del usuario de IAM.

Utiliza credenciales temporales si inicia sesión en ellas AWS Management Console mediante cualquier método excepto un nombre de usuario y una contraseña. Por ejemplo, cuando accedes AWS mediante el enlace de inicio de sesión único (SSO) de tu empresa, ese proceso crea automáticamente credenciales temporales. También crea credenciales temporales de forma automática cuando inicia sesión en la consola como usuario y luego cambia de rol. Para más información sobre el cambio de roles, consulte Cambio a un rol (consola) en la Guía del usuario de IAM.

Puedes crear credenciales temporales manualmente mediante la AWS CLI API o. AWS A continuación, puede utilizar esas credenciales temporales para acceder AWS. AWS recomienda generar credenciales temporales de forma dinámica en lugar de utilizar claves de acceso a largo plazo. Para más información, consulte Credenciales de seguridad temporales en IAM.

Permisos de entidades principales

Cuando utilizas un usuario o un rol de IAM para realizar acciones en AWSél, se te considera director. Las políticas conceden permisos a una entidad principal. Cuando utiliza algunos servicios, es posible que realice una acción que desencadene otra acción en un servicio diferente. En este caso, debe tener permisos para realizar ambas acciones. Para ver si una acción requiere acciones dependientes adicionales en una política, consulte Acciones, recursos y claves de condición para obtener AWS información básica sobre la documentación en la Referencia de autorización de servicios.

Validación de conformidad para Amazon DataZone

Para saber si uno Servicio de AWS está dentro del ámbito de aplicación de programas de cumplimiento específicos, consulte Servicios de AWS Alcance por programa de cumplimiento Servicios de AWS de cumplimiento y elija el programa de cumplimiento que le interese. Para obtener información general, consulte Programas de AWS cumplimiento > Programas AWS .

Puede descargar informes de auditoría de terceros utilizando AWS Artifact. Para obtener más información, consulte Descarga de informes en AWS Artifact .

Su responsabilidad de cumplimiento al Servicios de AWS utilizarlos viene determinada por la confidencialidad de sus datos, los objetivos de cumplimiento de su empresa y las leyes y reglamentos aplicables. AWS proporciona los siguientes recursos para ayudar con el cumplimiento:

- Guías de inicio rápido sobre seguridad y cumplimiento: estas guías de implementación analizan las consideraciones arquitectónicas y proporcionan los pasos para implementar entornos básicos centrados en AWS la seguridad y el cumplimiento.
- Diseño de arquitectura para garantizar la seguridad y el cumplimiento de la HIPAA en Amazon Web Services: en este documento técnico se describe cómo pueden utilizar AWS las empresas para crear aplicaciones aptas para la HIPAA.

> **Note**
>
> No Servicios de AWS todas cumplen con los requisitos de la HIPAA. Para más información, consulte la Referencia de servicios compatibles con HIPAA.

- AWS Recursos de de cumplimiento: esta colección de libros de trabajo y guías puede aplicarse a su industria y ubicación.
- AWS Guías de cumplimiento para clientes: comprenda el modelo de responsabilidad compartida desde la perspectiva del cumplimiento. Las guías resumen las mejores prácticas para garantizar la seguridad Servicios de AWS y orientan los controles de seguridad en varios marcos (incluidos el Instituto Nacional de Estándares y Tecnología (NIST), el Consejo de Normas de Seguridad del Sector de Tarjetas de Pago (PCI) y la Organización Internacional de Normalización (ISO)).
- Evaluación de los recursos con reglas en la guía para AWS Config desarrolladores: el AWS Config servicio evalúa en qué medida las configuraciones de los recursos cumplen con las prácticas internas, las directrices del sector y las normas.
- AWS Security Hub— Esto Servicio de AWS proporciona una visión completa del estado de su seguridad interior AWS. Security Hub utiliza controles de seguridad para evaluar sus recursos de AWS y comprobar su cumplimiento con los estándares y las prácticas recomendadas del sector de la seguridad. Para obtener una lista de los servicios y controles compatibles, consulte la Referencia de controles de Security Hub.
- Amazon GuardDuty: Servicio de AWS detecta posibles amenazas para sus cargas de trabajo Cuentas de AWS, contenedores y datos mediante la supervisión de su entorno para detectar actividades sospechosas y maliciosas. GuardDuty puede ayudarlo a cumplir con varios requisitos de conformidad, como el PCI DSS, al cumplir con los requisitos de detección de intrusiones exigidos por ciertos marcos de cumplimiento.
- AWS Audit Manager— Esto le Servicio de AWS ayuda a auditar continuamente su AWS uso para simplificar la gestión del riesgo y el cumplimiento de las normativas y los estándares del sector.

Mejores prácticas de seguridad para Amazon DataZone

Amazon DataZone proporciona una serie de características de seguridad que debes tener en cuenta a la hora de desarrollar e implementar tus propias políticas de seguridad. Las siguientes prácticas recomendadas son directrices generales y no constituyen una solución de seguridad completa. Puesto que es posible que estas prácticas recomendadas no sean adecuadas o suficientes para el entorno, considérelas como consideraciones útiles en lugar de como normas.

Implementación del acceso a los privilegios mínimos

Al conceder permisos, tú decides quién obtiene qué permisos y qué DataZone recursos de Amazon. Habilite las acciones específicas que desea permitir en dichos recursos. Por lo tanto, debe conceder únicamente los permisos obligatorios para realizar una tarea. La implementación del acceso con privilegios mínimos es esencial a la hora de reducir los riesgos de seguridad y el impacto que podrían causar los errores o los intentos malintencionados.

Uso de roles de IAM

Las aplicaciones de productores y clientes deben tener credenciales válidas para acceder a DataZone los recursos de Amazon. No debe almacenar AWS las credenciales directamente en una aplicación cliente o en un bucket de Amazon S3. Estas son las credenciales a largo plazo que no rotan automáticamente y que podrían tener un impacto empresarial significativo si se comprometen.

En su lugar, deberías usar un rol de IAM para gestionar las credenciales temporales de tus aplicaciones de productor y cliente para acceder a DataZone los recursos de Amazon. Al utilizar un rol, no tiene que utilizar credenciales a largo plazo (como un nombre de usuario y una contraseña o claves de acceso) para acceder a otros recursos.

Para obtener más información, consulte los siguientes temas de la guía del usuario de IAM:

- Roles de IAM
- Situaciones habituales con los roles: usuarios, aplicaciones y servicios

Implementación del cifrado en el servidor en recursos dependientes

Los datos en reposo y los datos en tránsito se pueden cifrar en Amazon DataZone.

Se usa CloudTrail para monitorear las llamadas a la API

Amazon DataZone está integrado con AWS CloudTrail un servicio que proporciona un registro de las acciones realizadas por un usuario, un rol o un AWS servicio en Amazon DataZone.

Con la información recopilada por CloudTrail, puedes determinar la solicitud que se realizó a Amazon DataZone, la dirección IP desde la que se realizó la solicitud, quién la hizo, cuándo se realizó y detalles adicionales.

Resiliencia en Amazon DataZone

La infraestructura AWS global se basa en distintas zonas Regiones de AWS de disponibilidad. Regiones de AWS proporcionan varias zonas de disponibilidad aisladas y separadas físicamente, que están conectadas mediante redes de baja latencia, alto rendimiento y alta redundancia. Con las zonas de disponibilidad, puede diseñar y utilizar aplicaciones y bases de datos que realizan una conmutación por error automática entre las zonas sin interrupciones. Las zonas de disponibilidad tienen una mayor disponibilidad, tolerancia a errores y escalabilidad que las infraestructuras tradicionales de uno o varios centros de datos.

Para obtener más información sobre las zonas de disponibilidad Regiones de AWS y las zonas de disponibilidad, consulte Infraestructura global.AWS

Además de la infraestructura AWS global, Amazon DataZone ofrece varias funciones que ayudan a respaldar sus necesidades de respaldo y resiliencia de datos.

Temas

Resiliencia de fuentes de datos

Durante un evento de DataZone disponibilidad en Amazon, los `DataSource` trabajos se volverán a intentar de forma periódica durante un máximo de 24 horas. Si un trabajo falla debido a un error de configuración, se emitirá un `DataSourceRunFailed` evento. Si el DataZone dominio de Amazon

está configurado con una clave KMS y AmazonDataZoneDomainExecutionRole pierde el acceso a esta clave durante la ejecución de un trabajo, la ejecución finalizará en ese `INACCESSIBLE` estado. Una vez que se restablezca el acceso al KMS, el trabajo debe actualizarse manualmente para activar la transición a un estado utilizable.

Resiliencia de activos

En Amazon DataZone, los activos están versionados. Si es necesario revertir una versión de un activo, puedes crear una nueva versión con el contenido de la última versión estable. Se puede publicar una versión de activo. No se puede editar una versión publicada de un activo, excepto publicando una versión nueva. Se puede suscribir a un activo publicado (también conocido como listado). Para evitar nuevas suscripciones a un activo, se puede anular su publicación. La anulación de la publicación de un activo no afecta a las suscripciones existentes. Al eliminar un recurso, se eliminarán todas las versiones no publicadas del activo. Las versiones publicadas del activo se deben eliminar por separado. La versión publicada de un recurso solo se puede eliminar si no hay suscripciones.

El tipo de activo y los metadatos forman resiliencia

En Amazon DataZone, los tipos de activos y los tipos de formularios de metadatos están versionados. Un tipo de activo no se puede eliminar si un activo lo está utilizando. No se puede eliminar un tipo de formulario de metadatos si lo está utilizando un tipo de activo o un activo. Si no quieres que se utilice un metadata-form-type contenido específico para la selección, puedes deshabilitarlo, lo que no afectará a los archivos a los que ya está adjunto.

Glosario: resiliencia

En Amazon DataZone, los glosarios y los términos del glosario no se pueden eliminar si están en uso. Si no quieres que se utilice un glosario o término de glosario específico para la selección, puedes desactivarlos para que no afecten a los que ya están adjuntos.

Capacidad de recuperación de búsquedas globales

En Amazon DataZone, los activos publicados (también conocidos como listados) se pueden encontrar mediante una búsqueda global. La publicación de un activo se puede anular anulando la publicación del activo. La anulación de la publicación de un activo no afecta a las suscripciones existentes. Un activo publicado se puede revertir a una versión concreta del activo volviendo a publicar esa versión. Esto no afectará a las suscripciones existentes.

Resistencia de las suscripciones

En Amazon DataZone, SubscriptionGrant Fulfillment intentará retirarlos dos veces antes de fallar. Si se produce un error, debes eliminarlo manualmente para volver a intentarlo. Si Amazon DataZone no puede revocar los permisos de una suscripción, es posible que no se pueda eliminar la suscripción. Se debe corregir el error subyacente o se puede utilizar la `retainPermissions` marca en la operación de la `DeleteSubscriptionGrant` API para forzar la eliminación de la concesión de Amazon DataZone sin revocar los permisos.

Si el DataZone dominio de Amazon está configurado con una clave KMS y `AmazonDataZoneDomainExecutionRole` pierde el acceso a esta clave durante el `SubscriptionGrant` flujo de trabajo, se marca la concesión`INACCESSIBLE`. Una vez que se restablezca el acceso al KMS, las `INACCESSIBLE` concesiones se deben eliminar y volver a crear.

Resiliencia ambiental

Si el DataZone dominio de Amazon está configurado con una clave KMS y `AmazonDataZoneDomainExecutionRole` pierde el acceso a esta clave durante el flujo de trabajo del entorno, se marcará el entorno`INACCESSIBLE`. Una vez que se restablezca el acceso al KMS, se debe eliminar y volver a crear el `INACCESSIBLE` entorno. Al crear el entorno, se intentará retirarlos dos veces antes de que se produzca un error. Si se produce un error, se debe eliminar manualmente para volver a intentarlo. Si el flujo de trabajo del entorno falla, el entorno entrará en un estado fallido. En este punto, solo se puede eliminar y volver a crear.

Plano ambiental: resiliencia

En Amazon DataZone, un blueprint de entorno no se puede eliminar si hay algún perfil de entorno subyacente.

Resiliencia del proyecto

En Amazon DataZone, no se puede eliminar un proyecto si hay algún entorno contenido.

Resiliencia de RAM

Para obtener información sobre la resiliencia de la RAM, consulte https://docs.aws.amazon.com/ram/latest/userguide/ security-disaster-recovery-resiliency .html.

Capacidad de gestión de perfiles de usuario

Para obtener información sobre la resiliencia de los perfiles de usuario, consulte AWS Identity Center.

Resiliencia del dominio

En Amazon DataZone, no se puede eliminar un dominio si contiene proyectos o fuentes de datos.

Seguridad de infraestructuras en Amazon DataZone

Como servicio gestionado, Amazon DataZone está protegido por la seguridad de la red AWS global. Para obtener información sobre los servicios AWS de seguridad y cómo se AWS protege la infraestructura, consulte Seguridad AWS en la nube. Para diseñar su AWS entorno utilizando las mejores prácticas de seguridad de la infraestructura, consulte Protección de infraestructuras en un marco de buena AWS arquitectura basado en el pilar de la seguridad.

Utilizas las llamadas a la API AWS publicadas para acceder a Amazon DataZone a través de la red. Los clientes deben admitir lo siguiente:

- Seguridad de la capa de transporte (TLS). Exigimos TLS 1.2 y recomendamos TLS 1.3.
- Conjuntos de cifrado con confidencialidad directa total (PFS) como DHE (Ephemeral Diffie-Hellman) o ECDHE (Elliptic Curve Ephemeral Diffie-Hellman). La mayoría de los sistemas modernos como Java 7 y posteriores son compatibles con estos modos.

Además, las solicitudes deben estar firmadas mediante un ID de clave de acceso y una clave de acceso secreta que esté asociada a una entidad de seguridad de IAM principal. También puede utilizar AWS Security Token Service (AWS STS) para generar credenciales de seguridad temporales para firmar solicitudes.

Prevención policial confusa entre servicios en Amazon DataZone

El problema de la sustitución confusa es un problema de seguridad en el que una entidad que no tiene permiso para realizar una acción puede obligar a una entidad con más privilegios a realizar la acción. En AWS, la suplantación de identidad entre servicios puede provocar el confuso problema de un diputado. La suplantación entre servicios puede producirse cuando un servicio (el servicio que lleva a cabo las llamadas) llama a otro servicio (el servicio al que se llama). El servicio que lleva a

cabo las llamadas se puede manipular para utilizar sus permisos a fin de actuar en función de los recursos de otro cliente de una manera en la que no debe tener permiso para acceder. Para evitarlo, AWS proporciona herramientas que le ayudan a proteger los datos de todos los servicios cuyos directores de servicio tengan acceso a los recursos de su cuenta.

Recomendamos utilizar la clave de contexto aws: SourceAccount global condition en las políticas de recursos para limitar los permisos que Amazon DataZone concede a otro servicio al recurso. Utilice aws: SourceAccount si quiere permitir que cualquier recurso de esa cuenta se asocie al uso entre servicios.

Análisis de configuración y vulnerabilidad para Amazon DataZone

AWS se encarga de tareas de seguridad básicas, como la aplicación de parches al sistema operativo (SO) huésped y a las bases de datos, la configuración del firewall y la recuperación ante desastres. Estos procedimientos han sido revisados y certificados por los terceros pertinentes. Para obtener más información, consulte el modelo de responsabilidad AWS compartida.

Dominios para añadir a tu lista de permitidos

Para que el portal de DataZone datos de Amazon acceda al DataZone servicio de Amazon, debe añadir los siguientes dominios a la lista de dominios permitidos de la red desde la que el portal de datos intenta acceder al servicio.

- `*.api.aws`
- `*.on.aws`

Supervisión de Amazon DataZone

La supervisión es una parte importante del mantenimiento de la fiabilidad, la disponibilidad y el rendimiento de Amazon DataZone y sus demás AWS soluciones. AWS proporciona las siguientes herramientas de supervisión para vigilar Amazon DataZone, informar cuando algo va mal y tomar medidas automáticas cuando sea necesario:

- Amazon CloudWatch monitorea tus AWS recursos y las aplicaciones en las que AWS ejecutas en tiempo real. Puede recopilar métricas y realizar un seguimiento de las métricas, crear paneles personalizados y definir alarmas que le advierten o que toman medidas cuando una métrica determinada alcanza el umbral que se especifique. Por ejemplo, puede CloudWatch hacer un seguimiento del uso de la CPU u otras métricas de sus instancias de Amazon EC2 y lanzar automáticamente nuevas instancias cuando sea necesario. Para obtener más información, consulta la Guía del CloudWatch usuario de Amazon.
- Amazon CloudWatch Logs le permite supervisar, almacenar y acceder a sus archivos de registro desde instancias de Amazon EC2 y otras fuentes. CloudTrail CloudWatch Los registros pueden monitorear la información de los archivos de registro y notificarle cuando se alcancen ciertos umbrales. También se pueden archivar los datos del registro en un almacenamiento de larga duración. Para obtener más información, consulta la Guía del usuario CloudWatch de Amazon Logs.
- Amazon se EventBridge puede utilizar para automatizar sus AWS servicios y responder automáticamente a los eventos del sistema, como los problemas de disponibilidad de las aplicaciones o los cambios de recursos. Los eventos de AWS los servicios se entregan EventBridge prácticamente en tiempo real. Puede crear reglas sencillas para indicar qué eventos le resultan de interés, así como qué acciones automatizadas se van a realizar cuando un evento cumple una de las reglas. Para obtener más información, consulta la Guía EventBridge del usuario de Amazon.
- AWS CloudTrailcaptura las llamadas a la API y los eventos relacionados realizados por su AWS cuenta o en su nombre y entrega los archivos de registro a un bucket de Amazon S3 que especifique. Puede identificar qué usuarios y cuentas llamaron AWS, la dirección IP de origen desde la que se realizaron las llamadas y cuándo se produjeron. Para obtener más información, consulte la Guía del usuario de AWS CloudTrail.

Supervisión de Amazon DataZone con Amazon CloudWatch

Puedes monitorizar el DataZone uso de Amazon CloudWatch, que recopila datos sin procesar y los procesa para convertirlos en métricas legibles prácticamente en tiempo real. Estas estadísticas se mantienen durante 15 meses, de forma que pueda obtener acceso a información histórica y disponer de una mejor perspectiva sobre el desempeño de su aplicación web o servicio. También puede establecer alarmas que vigilen determinados umbrales y enviar notificaciones o realizar acciones cuando se cumplan dichos umbrales. Para obtener más información, consulta la Guía del CloudWatch usuario de Amazon.

El portal de DataZone datos de Amazon utiliza las API del plano de DataZone datos de Amazon con autenticación y autorización JWT. Amazon DataZone asume el rol de servicio DataZone predeterminado de Amazon y registra todas las llamadas a la DataZone API de Amazon realizadas a través del portal de DataZone datos de Amazon en un grupo de registros denominado DataZoneDataPortalAPI CallLogs.

Supervisión de DataZone los eventos de Amazon en Amazon EventBridge

Puede monitorizar DataZone los eventos de Amazon en EventBridge, lo que proporciona un flujo de datos en tiempo real desde sus propias aplicaciones, aplicaciones software-as-a-service (SaaS) y AWS servicios. EventBridgedirige esos datos a objetivos como AWS Lambda Amazon Simple Notification Service. Estos eventos son los mismos que aparecen en Amazon CloudWatch Events, que ofrece una transmisión casi en tiempo real de los eventos del sistema que describen los cambios en AWS los recursos.

Para obtener más información, consulte Trabajar con eventos a través del bus EventBridge predeterminado de Amazon.

Registro de llamadas a DataZone la API de Amazon mediante AWS CloudTrail

Amazon DataZone está integrado con AWS CloudTrail un servicio que proporciona un registro de las acciones realizadas por un usuario, un rol o un AWS servicio en Amazon DataZone. CloudTrail captura todas las llamadas a la API de Amazon DataZone como eventos. Las llamadas capturadas incluyen llamadas desde la DataZone consola de Amazon y llamadas en código a las operaciones

de la DataZone API de Amazon. Si crea una ruta, puede habilitar la entrega continua de CloudTrail eventos a un bucket de Amazon S3, incluidos los eventos de Amazon DataZone. Si no configura una ruta, podrá ver los eventos más recientes en la CloudTrail consola, en el historial de eventos. Con la información recopilada por CloudTrail, puedes determinar la solicitud que se realizó a Amazon DataZone, la dirección IP desde la que se realizó la solicitud, quién la hizo, cuándo se realizó y detalles adicionales.

Para obtener más información CloudTrail, consulta la Guía AWS CloudTrail del usuario.

DataZone Información de Amazon en CloudTrail

CloudTrail está habilitada en tu cuenta Cuenta de AWS al crear la cuenta. Cuando se produce una actividad en la consola DataZone de administración de Amazon, esa actividad se registra en un CloudTrail evento junto con otros eventos de AWS servicio en el historial de eventos. Puede ver, buscar y descargar los eventos recientes en su Cuenta de AWS. Para obtener más información, consulte Visualización de eventos con el historial de CloudTrail eventos.

Para tener un registro continuo de tus eventos Cuenta de AWS, incluidos los de Amazon DataZone, crea una ruta. Un rastro permite CloudTrail entregar archivos de registro a un bucket de Amazon S3. De forma predeterminada, cuando se crea un registro de seguimiento en la consola, el registro de seguimiento se aplica a todas las Regiones de AWS. La ruta registra los eventos de todas las regiones de la AWS partición y envía los archivos de registro al bucket de Amazon S3 que especifique. Además, puede configurar otros AWS servicios para analizar más a fondo los datos de eventos recopilados en los CloudTrail registros y actuar en función de ellos. Para más información, consulte los siguientes temas:

- Introducción a la creación de registros de seguimiento
- CloudTrail servicios e integraciones compatibles
- Configuración de las notificaciones de Amazon SNS para CloudTrail
- Recibir archivos de CloudTrail registro de varias regiones y recibir archivos de CloudTrail registro de varias cuentas

Todas DataZone las acciones de Amazon las registra CloudTrail.

Solución de problemas de Amazon DataZone

Si te encuentras con problemas de acceso denegado o dificultades similares al trabajar con Amazon, DataZone consulta los temas de esta sección.

Solución de problemas de permisos de AWS Lake Formation para Amazon DataZone

Esta sección contiene instrucciones de solución de problemas que puedan surgir cuandoConfigurar los permisos de Lake Formation para Amazon DataZone:

Mensaje de error en el portal de datos	Resolución
No se puede asumir la función de acceso a los datos.	Este error aparece cuando Amazon DataZone no puede asumir AmazonDataZoneGlue DataAccessRoleque utilizaste para habilitar lo DefaultDataLakeBlueprinten tu cuenta. Para solucionar el problema, ve a la consola de AWS IAM de la cuenta en la que se encuentra tu activo de datos y asegúrate de que AmazonDataZoneGlueDataAcces sRoletiene la relación de confianza adecuada con el director de DataZone servicio de Amazon. Para obtener más información, consulte AmazonDataZoneGlueAccess-<region>- <domainId>.
La función de acceso a los datos no tiene los permisos necesarios para leer los metadatos del activo al que intenta suscribirse.	Este error aparece cuando Amazon asume DataZone correctamente el AmazonDat aZoneGlueDataAccessRolerol, pero el rol no tiene los permisos necesarios. Para soluciona r el problema, vaya a la consola de AWS IAM de la cuenta en la que se encuentra su activo de datos y asegúrese de que el rol lo tenga AmazonDataZoneGlueManageAccessRolePo licyasociado. Para obtener más informaci

Mensaje de error en el portal de datos	Resolución
	ón, consulte AmazonDataZoneGlueAccess-<region>- <domainId>.
El activo es un enlace a un recurso. Amazon DataZone no admite suscripciones a enlaces de recursos.	Este error aparece cuando el recurso que estás intentando publicar en Amazon DataZone es un enlace de recursos a una tabla de AWS Glue.

Mensaje de error en el portal de datos	Resolución
AWS Lake Formation no administra el activo.	Este error indica que los permisos de AWS Lake Formation no se aplican al activo que desea publicar. Esto puede ocurrir en los siguientes casos. • La ubicación del activo en Amazon S3 no está registrada en AWS Lake Formation. Para solucionar el problema, inicie sesión en la consola de AWS Lake Formation en la cuenta en la que se encuentra la tabla y registre la ubicación de Amazon S3 en modo AWS Lake Formation o modo híbrido. Para obtener más información, consulte Registro de una ubicación de Amazon S3. Hay varios escenarios que requieren modificaciones adicionales. Estos incluyen depósitos de AmazonS3 cifrados o un depósito de S3 multicuenta y una configuración de AWS Glue Catalog. En esos casos, puede ser necesario modificar la configuración de KMS o S3. Para obtener más informaci ón, consulte Registro de una ubicación de Amazon S3. • La ubicación de Amazon S3 está registrad a en el modo AWS Lake Formation, pero AllowedPrincipal se añade IAM a los permisos de la tabla. Para solucionar el problema, puede eliminar el IAM AllowedPr incipal de los permisos de la tabla o registrar la ubicación S3 en modo híbrido. Para obtener más información, consulte Acerca de la actualización al modelo de permisos de Lake Formation. Si tu ubicación de S3 está cifrada o la ubicación de S3 está en una cuenta diferente a la de tu tabla de AWS

Mensaje de error en el portal de datos	Resolución
	Glue, sigue las instrucciones de Registrar una ubicación cifrada de Amazon S3.
El rol de acceso a datos no tiene los permisos de Lake Formation necesarios para conceder acceso a este activo.	Este error indica que el elemento AmazonDataZoneGlueDataAccessRoleque estás utilizando para habilitar el DefaultDataLakeBlueprintcontenido en tu cuenta no tiene los permisos necesarios para DataZone que Amazon gestione los permisos del activo publicado. Puede resolver el problema añadiendo al AmazonDataZoneGlueDataAccessRolecomo administrador de AWS Lake Formation o concediendo los siguientes permisos al activo que desee publicar. AmazonDataZoneGlueDataAccessRole • Describa y describa los permisos concedibles en la base de datos en la que se encuentra el activo • Describa, seleccione, describa los permisos concedibles y seleccione los permisos concedibles sobre todos los activos de la base de datos cuyo acceso desea que Amazon gestione en su nombre. DataZone

Cuotas para Amazon DataZone

Tu AWS cuenta tiene cuotas predeterminadas, anteriormente denominadas límites, para cada AWS servicio. A menos que se indique otra cosa, cada cuota es específica de la región.

Amazon DataZone tiene las siguientes cuotas y límites.

Recurso	Descripción	Valor
Tipos de activos de datos	El número máximo de tipos de activos de datos que se pueden crear en un DataZone dominio	1 000
Activos de datos	El número máximo de activos de datos que se pueden crear en un DataZone dominio de Amazon	1 millón
Glosarios	El número máximo de glosarios empresariales que puedes crear en un dominio	1 000
Términos del glosario empresarial	El número máximo de términos totales del glosario empresarial que puedes crear en un dominio	10000
Entornos de un dominio	El número máximo de entornos en un DataZone dominio de Amazon	500

Historial de documentos de la Guía del DataZone usuario de Amazon

En la siguiente tabla se describen las versiones de documentación de Amazon DataZone.

Cambio	Descripción	Fecha
AmazonDataZoneSageMakerProvisioning - nueva política	La nueva política denominada AmazonDataZoneSageMakerProvisioningconcede a Amazon DataZone los permisos necesarios para interoperar con Amazon SageMaker. Para obtener más información, consulta Amazon DataZone actualiza las políticas AWS gestionadas.	30 de abril de 2024
AmazonDataZoneSageMakerEnvironmentRolePermissionsBoundary - nuevo límite de permisos	Se ha denominado un nuevo límite de permisos AmazonDataZoneSageMakerEnvironmentRolePermissionsBoundary. Cuando crea un SageMaker entorno de Amazon a través del portal de DataZone datos de Amazon, Amazon DataZone aplica este límite de permisos a las funciones de IAM que se generan durante la creación del entorno. El límite de permisos limita el alcance de las funciones que Amazon DataZone crea y de las funciones que añadas. Para obtener más información,	30 de abril de 2024

	consulta Amazon DataZone actualiza las políticas AWS gestionadas.	
AmazonDataZoneSageMakerAccess - nueva política	La nueva política denominada AmazonDataZoneSageMakerAccessconcede a Amazon DataZone los permisos necesarios para conceder a los usuarios el acceso a varios recursos del SageMaker entorno de Amazon. Para obtener más información, consulta Amazon DataZone actualiza las políticas AWS gestionadas.	30 de abril de 2024
AmazonDataZoneFullAccess - actualización de la política	Una actualización de la AmazonDataZoneFull Accesspolítica que añade acceso a las `DescribeSecurityGroups` acciones para mejorar la usabilidad de los administradores de cuentas que configuran los planes en la consola y a las `GetPolicy` acciones que ayudan a recuperar información sobre la política gestionada especificada. Para obtener más información, consulta Amazon DataZone actualiza las políticas AWS gestionadas.	30 de abril de 2024

AmazonDataZoneS3Manage- - - - nueva función <region>< domainId>	Nueva función denominad a AmazonDataZoneS3Ma nage-, <region><domainId> que se utiliza cuando Amazon DataZone llama a AWS Lake Formation para registrar una ubicación del Amazon Simple Storage Service (Amazon S3). AWS Lake Formation asume esta función al acceder a los datos de esa ubicación. Para obtener más información, consulta Amazon DataZone actualiza las políticas AWS gestionadas.	1 de abril de 2024
AmazonDataZoneGlue ManageAccessRolePolicy - Actualización de la política	Se actualizó AmazonDat aZoneGlueManageAcc essRolePolicypara habilitar la compatibilidad con los permisos que permiten DataZone a Amazon habilitar la publicación y las concesion es de acceso a los datos. Para obtener más información, consulta Amazon DataZone actualiza las políticas AWS gestionadas.	1 de abril de 2024

AmazonDataZoneDomainExecutionRolePolicy y AmazonDataZoneFullUserAccess - Actualización de la política	Se actualizó el AmazonDataZoneDomainExecutionRolePolicyy AmazonDataZoneFullUserAccesspara habilitar la compatibilidad con la `CancelMetadataGenerationRun` API. Para obtener más información, consulta Amazon DataZone actualiza las políticas AWS gestionadas.	29 de marzo de 2024
AmazonDataZoneFullAccess - Actualización de la política	Se actualizó `AmazonDataZoneFullAccess` para permitir a los usuarios elegir sus secretos, clústeres, vpc y subredes en la consola de DataZone administración de Amazon en lugar de escribirlos en un cuadro de texto. Para obtener más información, consulta Amazon DataZone actualiza las políticas AWS gestionadas.	13 de marzo de 2024

AmazonDataZoneDomainExecutionRolePolicy - Actualización de la política	Se actualizó AmazonDataZoneDomainExecutionRolePolicypara permitir la compatibilidad con la ListEnvironmentBlueprintConfigurationSummaries API necesaria para crear perfiles de entorno, identificando qué blueprints están habilitados en cada cuenta y región. Para obtener más información, consulta Amazon DataZone actualiza las políticas AWS gestionadas.	1 de febrero de 2024
AmazonDataZoneGlueManageAccessRolePolicy - Actualización de la política	Se actualizó AmazonDataZoneGlueManageAccessRolePolicypara habilitar la compatibilidad con el modo híbrido AWS Lake Formation. Para obtener más información, consulta Amazon DataZone actualiza las políticas AWS gestionadas.	14 de diciembre de 2023

AmazonDataZoneFullUserAccess y AmazonDataZoneDomainExecutionRolePolicy - Actualizaciones de políticas	Amazon DataZone actualizó las políticas AmazonDataZoneFullUserAccessy las AmazonDataZoneDomainExecutionRolePolicypolíticas para admitir la función generativa de descripciones de datos impulsada por IA en Amazon. DataZone Para obtener más información, consulta Amazon DataZone actualiza las políticas AWS gestionadas.	28 de noviembre de 2023
AmazonDataZoneEnvironmentRolePermissionsBoundary - Actualización de la política	Amazon DataZone ha realizado una actualización de la política AmazonDataZoneEnvironmentRolePermissionsBoundarygestionada que consiste en un `athena:GetQueryResultsStream` permiso adicional con el alcance de la `ResourceTag` condición. Para obtener más información, consulta Amazon DataZone actualiza las políticas AWS gestionadas.	17 de noviembre de 2023

AmazonDataZoneRedshiftManageAccessRolePolicy - Actualización de la política	Amazon DataZone actualizó la AmazonDataZoneRedshiftManageAccessRolePolicypolítica al eliminar la verificación del ID de la organización para la `redshift:AssociateDataShareConsumer` acción. Esto le permite compartir recursos entre AWS organizaciones. Para obtener más información, consulta Amazon DataZone actualiza las políticas AWS gestionadas.	16 de noviembre de 2023
AmazonDataZoneFullUserAccess - Actualización de la política	Amazon DataZone ha actualizado la AmazonDataZoneFullUserAccesspolítica que concede acceso total a Amazon DataZone, pero no permite la gestión de dominios, usuarios o cuentas asociadas. Para obtener más información, consulta Amazon DataZone actualiza las políticas AWS gestionadas.	2 de octubre de 2023
AmazonDataZonePreviewConsoleFullAccess - política obsoleta	Amazon DataZone dejó en desuso AmazonDataZonePreviewConsoleFullAccessel. Para obtener más información, consulte Amazon DataZone updates to AWS managed policies.	29 de septiembre de 2023

AmazonDataZonePortalFullAccessPolicy - política obsoleta	Amazon DataZone dejó en desuso AmazonDataZonePortalFullAccessPolicyel. Para obtener más información, consulte Amazon DataZone updates to AWS managed policies.	29 de septiembre de 2023
AmazonDataZoneDomainExecutionRolePolicy - Nueva política	Amazon DataZone agregó una nueva política llamada AmazonDataZoneDomainExecutionRolePolicy. Esta es la política predeterminada para el rol de DataZone `AmazonDataZoneDomainExecutionRole` servicio de Amazon. Amazon utiliza esta función DataZone para catalogar, descubrir, gobernar, compartir y analizar datos en el DataZone dominio de Amazon. Puede adjuntar la `AmazonDataZoneDomainExecutionRolePolicy` política a su`AmazonDataZoneDomainExecutionRole` . Para obtener más información, consulta Amazon DataZone actualiza las políticas AWS gestionadas.	25 de septiembre de 2023

AmazonDataZoneCrossAccountAdmin - Nueva política	Amazon DataZone agregó una nueva política llamada AmazonDataZoneCrossAccountAdminque permite a los usuarios trabajar con Amazon DataZone y sus cuentas asociadas. Para obtener más información, consulta Amazon DataZone actualiza las políticas AWS gestionadas.	19 de septiembre de 2023
AmazonDataZoneRedshiftManageAccessRolePolicy - Nueva política	Amazon DataZone agregó una nueva política llamada AmazonDataZoneRedshiftManageAccessRolePolicyque otorga permisos para permitir que Amazon habilite DataZone la publicación y las concesiones de acceso a los datos. Para obtener más información, consulta Amazon DataZone actualiza las políticas AWS gestionadas.	12 de septiembre de 2023

AmazonDataZoneRedshiftGlueProvisioningPolicy - Nueva política	Amazon DataZone agregó una nueva política llamada AmazonDataZoneRedshiftGlueProvisioningPolicyque otorga a Amazon DataZone los permisos necesarios para interoperar con las fuentes de datos compatibles. Para obtener más información, consulta Amazon DataZone actualiza las políticas AWS gestionadas.	12 de septiembre de 2023
AmazonDataZoneGlueManageAccessRolePolicy - Nueva política	Amazon DataZone ha añadido una nueva política llamada AmazonDataZoneGlueManageAccessRolePolicyconceder DataZone permisos a Amazon para publicar datos de AWS Glue en el catálogo. También otorga a Amazon DataZone permisos para conceder o revocar el acceso a los activos publicados por AWS Glue en el catálogo. Para obtener más información, consulta Amazon DataZone actualiza las políticas AWS gestionadas.	12 de septiembre de 2023

AmazonDataZoneFull UserAccess - Nueva política	Amazon DataZone agregó una nueva política llamada AmazonDataZoneFull UserAccessque otorga acceso total a Amazon a DataZone través del portal de datos. Para obtener más información, consulta Amazon DataZone actualiza las políticas AWS gestionadas.	12 de septiembre de 2023
AmazonDataZoneFullAccess - Nueva política	Amazon DataZone agregó una nueva política llamada AmazonDataZoneFull Accessque proporciona acceso total a Amazon a DataZone través de la consola AWS de administración. Para obtener más información, consulta Amazon DataZone actualiza las políticas AWS gestionadas.	12 de septiembre de 2023
AmazonDataZoneEnvironmentRolePermissionsBoundary - Nueva política	Amazon DataZone agregó una nueva política llamada AmazonDataZoneEnvironmentRolePermissionsBoundaryque limita el principal de IAM aprovisionado al que está asociado. Para obtener más información, consulta Amazon DataZone actualiza las políticas AWS gestionadas.	12 de septiembre de 2023

Actualización gestionada de la política	Actualizaciones de la política AmazonDataZonePreviewConsoleFullAccess gestionada. Para obtener más información, consulta Amazon DataZone actualiza las políticas AWS gestionadas.	13 de junio de 2023
Actualización gestionada de la política	Actualizaciones de la política AmazonDataZoneProjectDeploymentPermissionsBoundary gestionada. Para obtener más información, consulta Amazon DataZone actualiza las políticas AWS gestionadas.	3 de abril de 2023
???	Versión inicial de la Guía del usuario de Amazon DataZone (versión preliminar).	29 de marzo de 2023

Las traducciones son generadas a través de traducción automática. En caso de conflicto entre la traducción y la version original de inglés, prevalecerá la version en inglés.