aws

用户指南

Amazon DataZone

Amazon DataZone: 用户指南

Table of Contents

什么是亚马逊 DataZone？

Amazon DataZone 是一项数据管理服务，可让您更快、更轻松地对存储在本地和第三方来源的数据进行分类 AWS、发现、共享和管理。借助 Amazon DataZone，监督组织数据资产的管理员可以使用精细的控制来管理和控制对数据的访问。这些控件有助于确保在适当级别的权限和上下文下进行访问。Amazon DataZone 让工程师、数据科学家、产品经理、分析师和业务用户可以轻松地在整个组织中共享和访问数据，这样他们就可以发现、使用和协作以获得数据驱动的见解。

亚马逊通过集成数据管理服务，包括亚马逊 Redshift、Amazon Athena、Amazon、 QuickSight Glue、Lak AWS e Formation、本地来源、第三方来源 AWS 等， DataZone 帮助您直接向最终用户交付数据并简化架构。

主题

我能用 Amazon 做 DataZone什么？

借助 Amazon DataZone，您可以执行以下操作：

- 跨组织边界管理数据访问。借助 Amazon DataZone，您可以根据贵组织的安全法规，帮助确保正确的用户出于正确的目的访问正确的数据，而不必依赖个人证书。您还可以提供数据资产使用情况的透明度，并通过受管控的工作流程批准数据订阅。您还可以通过使用情况审计功能监控项目间的数据资产。
- 通过共享的数据和工具连接数据工作者，以获得业务见解。借助 Amazon DataZone，您可以通过跨团队的无缝协作以及提供对数据和分析工具的自助访问来提高业务团队的效率。您可以使用商业术语来搜索、共享和访问存储在 AWS本地或第三方提供商处的分类数据。此外，您还可以使用亚马逊 DataZone 企业术语表进一步了解您想要使用的数据。
- 利用机器学习自动发现和编目数据。借助 Amazon DataZone，您可以减少手动将数据属性输入业务数据目录所花费的时间。数据目录中更丰富的数据还可以改善搜索体验。

Amazon 如何 DataZone 支持其他服务并与其他 AWS 服务集成？

Amazon DataZone 支持与其他 AWS 服务的三种集成：

- 生产者数据源-您可以根据存储在 AWS Glue 数据 DataZone 目录和 Amazon Redshift 表和视图中的数据将数据资产发布到亚马逊目录。您也可以手动将对象从亚马逊简单存储服务 (S3) Simple Storage Service 发布到亚马逊 DataZone 目录。
- 消费者工具-您可以使用亚马逊 Athena 或 Amazon Redshift 查询编辑器来访问和分析您的数据资产。
- 访问控制和配送——亚马逊 DataZone 支持授予对 AWS Lake Formation 托管 AWS Glue 表格以及亚马逊 Redshift 表格和视图的访问权限。对于所有其他数据资产，亚马逊会向亚马逊 DataZone 发布与您的操作相关的标准事件（例如，批准订阅请求） EventBridge。您可以使用这些标准事件与其他 AWS 服务或第三方解决方案集成，以实现自定义集成。

我怎样才能访问亚马逊 DataZone？

您可以通过以下任何 DataZone 一种方式访问 Amazon：

- 亚马逊 DataZone 控制台

  您可以使用亚马逊 DataZone 管理控制台来访问和配置您的亚马逊 DataZone 域名、蓝图和用户。欲了解更多信息，请参阅 https://console.aws.amazon.com/datazone。亚马逊 DataZone 管理控制台还用于创建亚马逊 DataZone 数据门户。
- 亚马逊 DataZone 数据门户

  Amazon DataZone 数据门户是一个基于浏览器的网络应用程序，您可以在其中以自助方式对数据进行分类、发现、管理、共享和分析。数据门户可以通过 AWS IAM Identity Center（ AWS SSO 的继任者）使用身份提供商提供的证书或您的 IAM 凭证对您进行身份验证。你可以通过访问亚马逊 DataZone 控制台来获取数据门户网址，网址为 https://console.aws.amazon.com/datazone。
- 亚马逊 DataZone HTTPS API

  您可以使用亚马逊 DataZone HTTPS API DataZone 以编程方式访问亚马逊，它允许您直接向服务发出 HTTPS 请求。有关更多信息，请参阅 Amazon DataZone API 参考。

Amazon DataZone 术语和概念

在开始使用 Amazon 时 DataZone，了解其关键概念、术语和组成部分非常重要。

主题

亚马逊 DataZone 组件

Amazon DataZone 包括以下四个主要组成部分：

- 业务数据目录-您可以使用此组件根据业务背景对整个组织的数据进行分类，从而使组织中的每个人都能快速查找和理解数据。
- 发布和订阅工作流程-您可以使用这些自动化工作流程以自助方式保护生产者和消费者之间的数据，并确保组织中的每个人都能出于正确目的访问正确的数据。
- 项目和环境
  - Amazon DataZone 项目中包含基于业务用例的人员分组、资产（数据）和工具，用于简化对分析的访问。 AWS 项目提供了项目成员可以协作、交换数据和共享资产的区域。默认情况下，项目配置为只有明确添加到项目中的人员才能访问项目中的数据和分析工具。项目管理根据项目政策生产的资产的所有权，供数据使用者访问。
  - 在 Amazon DataZone 项目中，环境是由零个或多个已配置的资源（例如 Amazon S3 存储桶、AWS Glue 数据库或 Amazon Athena 工作组）组成的集合，一组给定的 IAM 委托人（例如，具有贡献者权限的用户）可以对其进行操作。
- 数据门户（ AWS 管理控制台外）-这是一个基于浏览器的 Web 应用程序，不同的用户可以在其中以自助方式对数据进行编目、发现、管理、共享和分析。数据门户使用 IAM 证书或您的身份提供商提供的现有证书对用户进行 AWS IAM Identity Center身份验证。

什么是 Amazon DataZone 域名？

您可以使用 Amazon DataZone 域来组织您的资产、用户及其项目。通过将其他 AWS 账户与您的 Amazon DataZone 域名关联，您可以汇集您的数据源。然后，您可以使用元数据表单和词汇表将这些数据源中的资源发布到您的域名目录中，从而提高元数据的完整性和质量。您也可以搜索和浏览这些资产，以查看域中发布了哪些数据。此外，您可以加入项目与其他用户协作，订阅资产，并使用项目环境访问分析工具，包括亚马逊 Athena 和 Amazon Redshift。无论是为企业创建单个 Amazon DataZone 域名，还是为不同的业务部门创建多个 Amazon 域名，Amazon DataZone 域名都能让您灵活地反映组织结构的数据和分析需求。 DataZone

Amazon 的 DataZone 项目和环境是什么？

Amazon 通过创建基于用例的团队、工具和数据分组， DataZone 使团队和分析用户能够在项目上进行协作。

- 在亚马逊中 DataZone，项目使一组用户能够就各种业务用例进行协作，这些用例涉及发布、发现、订阅和使用亚马逊 DataZone 目录中的数据。项目成员使用 Amazon DataZone 目录中的资产，并使用一个或多个分析工作流程生成新资产。项目支持数据门户中的以下活动：
  - 项目所有者可以添加具有所有者和参与者权限的成员
  - 项目成员可以是 SSO 用户、SSO 群组和 IAM 用户
  - 项目成员可以申请订阅数据目录中的资产

    项目获得订阅许可
- 在 Amazon DataZone 项目中，环境是由零个或多个已配置的资源（例如 Amazon S3、 AWS Glue 数据库或 Amazon Athena 工作组）组成的集合，其中有一组可以操作这些资源的 IAM 委托人。环境是通过使用环境配置文件创建的，环境配置文件是预先配置的资源集和蓝图，为创建环境提供了可重复使用的模板。环境配置文件定义设置，例如部署环境的 AWS 账户 或区域。

什么是亚马逊 DataZone 蓝图？

用于创建环境的蓝图定义了环境所属项目的成员在处理亚马逊目录中的资产时可以使用哪些 AWS 工具和服务（例如， AWS Glue 或 Ama DataZone zon Redshift）。

在当前版本的 Amazon 中 DataZone，支持以下默认蓝图：

蓝图名称	描述	创建的资源
数据湖蓝图	使 Amazon DataZone 项目成员能够在环境中启动数据湖生成器和使用者服务。 作为消费者，它使亚马逊 DataZone 项目成员能够直接在Amazon Athena和其他支持 Lake Formation的查询引擎中访问Lake Formation管理的资产的 “只读” 副本。 作为制作者，它使亚马逊 DataZone 项目成员能够使用 Amazon Athena 创建新的 LakeFormation托管表并将其发布到亚马逊目录中。 DataZone	使用户能够使用 Amazon Athena 创建和查询 Lake Formation 表。Amazon Athena 工作组 AWS Glue 、具有 “只读” Lake Formation 权限的数据库、“只读” 的 IAM 权限以及对由项目管理的 Amazon S3 的访问权限。 AWS Glue 具有 “创建” 和 “授予” Lake Formation 权限的数据库、“读取” 和 “写入” IAM 权限、带标签的 AWS Glue ETL（提取、转换和加载）。
数据仓库蓝图	作为消费者，该蓝图使亚马逊 DataZone 项目成员能够连接到自己的Amazon Redshift集群，以查询远程数据存储以及创建和存储新的数据集。 作为制作者，该蓝图使亚马逊 DataZone 项目成员能够连接到自己的 Amazon Redshift 集群，以查询远程数据存储、创建新数据集并将其发布到亚马逊 DataZone 目录。	访问亚马逊 Redshift 查询编辑器，“读取” 亚马逊 DataZone 目录中订阅的数据源，能够在配置的 Amazon Redshift 集群中创建本地资产。访问 Amazon Redshift 查询编辑器，“读取” 亚马逊 DataZone 目录中已订阅的数据源，能够从已配置的 Amazon Redshift 集群创建和发布资产。
亚马逊 Sagemaker 蓝图	该蓝图可帮助数据生产者和消费者无缝切换 SageMaker 到 Amazon，在机器学习 (ML) 项目上进行协作，同时对数据和机器学习资产实施访问管理。借助 Amazon DataZone	您可以创建一个可以在亚马逊中搜索、订阅和发布数据和机器学习资产的亚马逊 SageMaker 域名 DataZone。还可以按照配置订阅和发布

蓝图名称	描述	创建的资源
	和 Amazon 之间新的内置集成 SageMaker，数据使用者和创建者可以简化基础设施设置中的机器学习管理，协作开展业务计划，并轻松管理数据和机器学习资产。	AWS Glue 数据库和湖泊形成。

除了内置的蓝图外，您还可以启用自定义 AWS 服务蓝图，这样您就可以将 Amazon 配置 DataZone 为使用您自己已在组织中设置的现有 IAM 角色和 AWS 服务。有关更多信息，请参阅 在 Amazon 中 AWS 使用定制服务蓝图 DataZone。

Amazon DataZone 库存和发布工作流程是什么？

创建项目清单资产

要使用亚马逊对您的数据 DataZone 进行分类，您必须先将您的数据（资产）作为项目库存带到亚马逊 DataZone。为项目创建清单，使只有该项目的成员才能发现这些资产。除非明确发布，否则并非所有域名用户都可以在搜索/浏览中使用项目清单资产。在当前版本的 Amazon 中 DataZone，您可以通过以下方式向项目库存添加资产：

- 通过数据门户或使用 Amazon DataZone API 创建和运行数据源。在当前版本的亚马逊中 DataZone，你可以为 AWS Glue 和 Amazon Redshift 创建和运行数据源。通过创建和运行 AWS Glue 或 Amazon Redshift 数据源，您可以在选定的项目清单中创建资产，并将其技术元数据从源数据库表或数据仓库中作为库存导入到亚马逊。 DataZone
- 使用 API，您可以根据可用的系统资产类型（AWS Glue、Amazon Redshift、Amazon S3 对象）或自定义资产类型创建资产。
  - 使用 Amazon DataZone API 在项目清单中创建自定义资产类型。自定义资产类型可以包括机器学习模型、仪表板、本地表格等。
  - 使用 Amazon DataZone API 根据这些自定义资产类型创建资产。
- 使用 Amazon DataZone 数据门户手动为 S3 对象创建资产。

整@@ 理项目清单资产-创建项目清单后，数据所有者可以通过添加或更新企业名称（资产和架构）、描述（资产和架构）、自述、词汇表（资产和架构）和元数据表单，使用所需的业务元数据整理库存资

产。您可以通过数据门户网站或使用 Amazon DataZone API 来执行此操作。对资产的每次编辑都会创建一个新的库存版本。

将项目库存资产发布到 Amazon DataZone 目录

使用 Amazon DataZone 对您的数据进行分类的下一步是让域名用户可以发现您项目的库存资产。您可以通过将库存资产发布到 Amazon DataZone 目录来做到这一点。只有最新版本的库存资产可以发布到目录中，发现目录中只有最新发布的版本处于活动状态。如果库存资产在发布到亚马逊 DataZone 目录后进行了更新，则必须再次明确发布该库存资产，以使最新版本出现在发现目录中。在当前版本的 Amazon 中 DataZone，您可以通过以下方式将项目库存资产发布到亚马逊 DataZone 目录中：

- 通过数据门户或使用亚马逊 DataZone API 将您的项目库存资产手动发布到亚马逊 DataZone 目录。
- 在创建或编辑数据源时，启用可选的 “将您的 AWS Glue 资产发布到目录” 或 “将您的 Amazon Redshift 资产发布到目录” 设置，以便在计划或自动数据源运行期间使用。启用此设置后，数据源运行会将资产添加到项目的库存中，然后还会将库存资产发布到 Amazon DataZone 目录。请注意，如果您直接发布，则资产可能没有任何业务元数据，所有域名用户都可以直接发现这些资产。您可以通过数据门户或使用 Amazon DataZone API 在数据源上使用此设置。

Amazon DataZone 订阅和配送流程是什么？

将您的资产发布到亚马逊 DataZone 目录后，您的域名用户就可以发现这些资产，请求和访问这些资产，并继续使用亚马逊 DataZone 来管理、共享和分析这些资产。

用户通过代表项目订阅资产来请求访问该资产。创建订阅请求后，资产的所有者会收到通知，可以查看订阅请求并决定是要批准还是拒绝订阅请求。如果订阅请求获得数据所有者的批准，则订阅项目将被授予对该资产的访问权限。

订阅申请获得批准后，亚马逊将 DataZone 开始订阅配送工作流程，通过在 La AWS ke Formation 或 Amazon Redshift 中创建必要的授权，自动将资产添加到项目内的所有适用环境中。这样，订阅的项目成员就可以在其环境中使用其中一个查询工具（Amazon Athena 或 Amazon Redshift 查询编辑器）来查询资产。

亚马逊 DataZone 只能针对托管资产（包括 AWS Glue 表格和 Amazon Redshift 表格和视图）触发此自动配送逻辑。对于所有其他资产类型（非托管资产），亚马逊 DataZone 无法自动触发配送，而是在 Amazon Eventbridge中发布事件，并在事件负载中包含所有必要的详细信息，以便您可以在亚马逊之外创建必要的补助金。 DataZone亚马逊 DataZone 还提供了 `updateSubscriptionStatus` API，允许您在亚马逊以外的地方完成订阅后更新订阅状态， DataZone 以便亚马逊 DataZone 可以通知项目成员他们可以开始使用该资产。

Amazon 的用户角色 DataZone

以下是 Amazon DataZone 用户的主要角色：

- 负责将 Amazon 设置 DataZone 为其组织分析平台的域管理员。

  在亚马逊环境中 DataZone，域管理员 DataZone 在 AWS 账户中安装亚马逊，创建亚马逊 DataZone 域名，并配置 AWS 账户关联和身份提供者与亚马逊 DataZone 域的关联。域管理员还使用其他 AWS 服务控制台，例如 AWS 组织和服务目录，来配置 Amazon DataZone。

- 作为 Amazon DataZone （资产发布者和订阅者）执行分析和机器学习任务的主要用户的数据用户。

  数据用户包括数据分析工作者、数据科学家以及生产和使用数据资产的系统用户。在亚马逊环境中 DataZone，数据用户创建和加入项目和环境，使用预先配置的分析或机器学习工具订阅和使用数据资产，并将输出数据资产发布回亚马逊 DataZone 域名目录以与其他人共享。

- 构建自定义基础设施模板并将 Amazon DataZone 与内部目录或生产系统集成的系统开发人员。

  在亚马逊环境中 DataZone，系统开发人员以环境提供者的身份构建环境蓝图（基础设施模板）或基础架构即代码 CI/CD 管道、用于跨环境推广数据资产的数据管道、用于与内部目录集成的目录同步和订阅赠款配送适配器，或者根据需要在 Amazon DataZone API 与内部用户界面或生产系统之间进行集成。

- 数据治理官员，他们拥有组织安全、隐私和其他合规政策的定义和风险，并确保其组织 DataZone 中对亚马逊的使用符合这些定义。

亚马逊 DataZone 术语

域

Amazon DataZone 域名是将您的资产、用户及其项目连接在一起的组织实体。借助 Amazon DataZone 域名，您可以灵活地反映组织结构的数据和分析需求，无论是为企业创建单个 Amazon DataZone 域还是为不同的业务部门或团队创建多个数据区；域名。

关联账户

将您的 AWS 账户与亚马逊 DataZone 域名关联后，您可以将这些 AWS 账户中的数据发布到亚马逊 DataZone 目录中，并创建亚马逊 DataZone 项目来处理多个 AWS 账户中的数据。账户关联请求只能在拥有 Amazon DataZone 域名的 AWS 账户中发起。只有被邀请账户的管理员用户才能接受 AWS 账户关联请求。 AWS 账户与亚马逊 DataZone 域名关联后，您就可以将该账户中的数

据源（例如 AWS Glue 目录和 Amazon Redshift）注册到该域名。关联还使 AWS 账户能够创建 Amazon DataZone 项目和环境。

AWS 账户 可以与一个或多个 Amazon DataZone 域名相关联。

数据来源

在 Amazon 中 DataZone，您可以使用数据源将来自源数据库或数据仓库的资产（数据）的技术元数据导入亚马逊 DataZone。在当前版本的亚马逊中 DataZone，你可以为 AWS Glue 和 Amazon Redshift 创建和运行数据源。通过创建数据源，您可以在亚马逊 DataZone 与数据源（AWS Glue Data Catalog 或 Amazon Redshift Warehouse）之间建立连接，从而使您能够读取技术元数据，包括表名称、列名和数据类型。通过创建数据源，您还可以启动初始数据源运行，在 Amazon 中创建新资产或更新现有资产 DataZone。在创建数据源时或成功创建数据源之后，您还可以选择为数据源运行指定计划。

数据源运行

在亚马逊中 DataZone，数据源运行是亚马逊 DataZone 执行的一项任务，目的是在项目清单中创建资产，也可以选择将项目库存资产发布到亚马逊 DataZone 目录。数据源运行可以是自动运行（在最初创建数据源时启动）、计划运行或手动运行。数据选择标准使您能够微调要提取到项目清单或 Amazon 目录中的现有和未来数据集，以及这些库存或 DataZone目录资产的元数据更新频率。

订阅目标

在 Amazon 中 DataZone，订阅目标允许您访问在项目中订阅的数据。订阅目标指定了位置（例如，数据库或架构）和所需的权限（例如，IAM 角色），亚马逊 DataZone 可以使用这些权限与源数据建立连接并创建必要的授权，以便亚马逊 DataZone 项目的成员可以开始查询他们订阅的数据。

订阅请求

在亚马逊 DataZone，订阅请求是亚马逊 DataZone 项目必须遵循的流程才能获得对特定资产的访问权限。订阅请求可以获得批准、拒绝、撤销或批准。

资产

在 Amazon DataZone 中，资产是呈现单个物理数据对象（例如，表、仪表板、文件）或虚拟数据对象（例如视图）的实体。

Asset type

资产类型定义了资产在 Amazon DataZone 目录中的呈现方式。资产类型定义特定类型资产的架构。创建资产时，将根据其资产类型（默认为最新版本）定义的架构对其进行验证。当资产更新发

生时，Amazon DataZone 会创建一个新的资产版本，并允许亚马逊 DataZone 用户对所有资产版本进行操作。

商业词汇表

在亚马逊中 DataZone，业务词汇表是可能与资产相关的商业术语的集合。业务词汇表有助于确保组织在执行各种数据分析任务时使用相同的术语和定义。

可以将业务词汇表中的术语添加到资产和列中，以便在搜索过程中对这些属性进行分类或增强对这些属性的识别。可以选择词汇表作为元数据表单中与资产关联的字段的值类型。当选择特定术语作为资产元数据表单字段的值时，用户可以搜索业务词汇表术语并找到关联的资产。

元数据表单类型

元数据表单类型是一种模板，用于定义在将资产创建为库存或在 Amazon DataZone 域中发布时收集和保存的元数据。元数据表单类型可以与数据资产相关联。元数据表单类型可帮助域管理员定义该域所需的元数据表单，例如合规性信息、监管信息或分类。它使域管理员能够为其资产自定义其他元数据。Amazon DataZone 有系统元数据表单类型，例如 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、和。 suggestion-form-type

元数据表单

在亚马逊中 DataZone，元数据表单定义了在将资产创建为库存或在亚马逊 DataZone 域中发布时收集和保存的元数据。元数据表单定义由域管理员在目录域中创建。元数据表单定义由一个或多个字段定义组成，支持布尔值、日期、十进制、整数、字符串和业务词汇表字段值数据类型。

域管理员通过将元数据表单添加到其网域中，将元数据表单应用于其网域中的资产。然后，资源发布者在元数据表单中提供任何可选和必填的字段值。

项目

在亚马逊中 DataZone，项目允许一组用户就各种业务用例进行协作，这些用例涉及在项目清单中创建资产，从而使所有项目成员都能发现这些资产，然后发布、发现、订阅和使用亚马逊 DataZone 目录中的资产。项目成员使用 Amazon DataZone 目录中的资产，并使用一个或多个分析工作流程生成新资产。项目成员可以是所有者或贡献者。项目所有者可以添加或移除其他用户作为所有者或参与者，也可以修改或删除项目。对贡献者的其他限制可以通过政策来定义。当用户创建项目时，他们将成为该项目的第一个所有者。

环境

环境是已配置资源的集合（例如，Amazon S3 存储桶、 AWS Glue 数据库或 Amazon Athena 工作组），具有一组给定的 IAM 委托人（具有分配的贡献者权限），他们可以对这些资源进行操作。

每个环境还可能有用户主体，他们有权通过订阅和履行访问资源和访问数据。环境旨在存储指向 AWS 服务、外部 IDE 和控制台的可操作链接。项目成员可以通过环境中配置的深度链接访问诸如 Amazon Athena 控制台等服务。可以进一步将项目中的 SSO 用户和 IAM 用户范围缩小到使用/访问特定的环境。

环境概况

在 Amazon 中 DataZone，环境配置文件是您可以用来创建环境的模板。环境配置文件是使用蓝图创建的。

使用环境配置文件，域管理员可以用预先配置的参数封装蓝图，然后数据工作者可以通过选择现有环境配置文件并为新环境指定名称来快速创建任意数量的新环境。这使数据工作者能够高效地管理其项目和环境，同时确保他们满足域管理员实施的数据治理策略。

蓝图

用于创建环境的蓝图定义了环境所属项目的成员在处理亚马逊目录中的资产时可以使用哪些 AWS 工具和服务（例如， AWS Glue 或 Ama DataZone zon Redshift）。

在当前版本的 Amazon DataZone 中，支持以下蓝图：

- 数据湖蓝图
- 数据仓库蓝图
- 亚马逊 Sagemaker 蓝图
- 自定义 AWS 服务蓝图

用户配置文件

用户个人资料代表 Amazon DataZone 用户。Amazon DataZone 支持 IAM 角色和 SSO 身份，以便出于不同的目的与亚马逊 DataZone 管理控制台和数据门户进行交互。域管理员使用 IAM 角色在 Amazon DataZone 管理控制台中执行与域相关的初始管理工作，包括创建新的 Amazon DataZone 域、配置元数据表单类型和实施策略。数据工作者通过 Identity Center 使用他们的 SSO 企业身份登录亚马逊 DataZone 数据门户并访问他们拥有成员资格的项目。

群组简介

群组资料代表一组 Amazon DataZone 用户。群组可以手动创建，也可以映射到企业客户的 Active Directory 群组。在 Amazon 中 DataZone，群组有两个用途。首先，一个小组可以映射到组织结构图中的用户团队，从而在有新员工加入或离开团队时减少 Amazon DataZone 项目负责人的管理工作。其次，企业管理员使用 Active Directory 群组来管理和更新用户状态，因此亚马逊 DataZone 域管理员可以使用这些群组成员资格来实施亚马逊 DataZone 域名政策。

域管理员

在亚马逊中 DataZone，创建亚马逊 DataZone 域名的 IAM 委托人是该域的默认域管理员。Amazon 中的域管理员为域 DataZone 执行关键功能，包括创建域、分配其他域管理员、添加数据源和订阅目标、创建项目和环境以及分配项目所有者。

出版商

在亚马逊 DataZone，出版商将资产发布到亚马逊 DataZone 目录中，并且可以编辑他们发布的资产的元数据。如果获得此权限，出版商可以批准或拒绝其在 Amazon DataZone 目录中发布的资产的订阅请求。

订阅者

在亚马逊中 DataZone，订阅者是一个想要查找、访问和使用亚马逊 DataZone 目录中的资产的亚马逊 DataZone 项目。

AWS 账户 owner

在亚马逊中 DataZone， AWS 账户 所有者在其中创建角色、策略和权限 AWS 账户 ，使这些角色和权限 AWS 账户 能够与亚马逊 DataZone 域名关联。

Amazon 有哪些新内容 DataZone？

本节 DataZone 按发布日期介绍Amazon的新功能和改进。

主题

2024

亚马逊 DataZone 推出数据血统功能

于 2024 年 6 月 27 日发布

Amazon DataZone 推出数据沿袭预览版，帮助客户可视化来自 OpenLineage支持系统的系统或 API 的世系事件，并跟踪数据从源头到消费的移动。使用与亚马逊 DataZone OpenLineage兼容的 API，域管理员和数据创建者可以捕获和存储超出亚马逊可用范围的谱系事件 DataZone，包括 Amazon S3、G AWS lue 和其他服务中的转换。此外，Amazon DataZone 版本与每个事件保持一致，使用户能够在任何时间点可视化血统或比较资产或任务历史的转换。这种历史沿袭可以更深入地了解数据是如何演变的，这对于故障排除、审计和验证数据资产的完整性至关重要。有关更多信息，请参阅Amazon 中的数据谱系 DataZone（预览版）

亚马逊 DataZone 推出定制 AWS 服务蓝图

于 2024 年 6 月 17 日发布

借助定制 AWS 服务蓝图，如果您拥有包括 IAM 角色、数据湖、数据网格、Amazon S3 存储桶和 Amazon Redshift 集群在内的现有 AWS 资源，您现在可以使用自己的自定义 IAM 角色指定对这些现有资源的权限，这样您的亚马逊 DataZone 用户就可以利用发布和订阅来共享和管理这些资源。借助定制 AWS 服务蓝图，Amazon DataZone 管理员可以使用自己的自定义角色配置 AWS 服务环境。他们可以为这些 AWS 服务环境配置操作链接，从而提供对其任何现有 AWS 资源的联合访问权限。他们还可以在这些自定义 AWS 服务环境中配置订阅目标和数据源。管理员可以在自己的 Amazon DataZone 域账户中或他们想要发布、订阅、发现或管理数据的任何关联账户中设置 AWS 服务环境。有关更多信息，请参阅 在 Amazon 中 AWS 使用定制服务蓝图 DataZone。

数据源创建流程的增强

于 2024 年 10 月 6 日发布

Amazon DataZone 对数据源创建流程进行了增强，以简化数据生产者的访问管理。通过这些更新，当数据创建者创建用于发布其 AWS Glue 和 Amazon Redshift 资产的数据源时，亚马逊会向项目成员 DataZone 授予只读权限。创建 AWS Glue 数据源时，Amazon DataZone 会自动向用于创建数据源的环境的 IAM 角色授予 “只读” 权限，允许访问相关 AWS Glue 数据库中的所有表。同样，对于亚马逊 Redshift 数据源，亚马逊 DataZone 授予对数据源中使用的亚马逊 Redshift 架构中所有表的 “只读” 访问权限。有关更多信息，请参阅 为创建并运行 Amazon DataZone 数据源 AWS Glue Data Catalog 和 为亚马逊 Redshift 创建并运行亚马逊 DataZone 数据源。

亚马逊 DataZone 启动与亚马逊的整合 SageMaker

于 2024 年 6 月 5 日发布

亚马逊 DataZone 推出与亚马逊的集成， SageMaker以帮助数据生产者和消费者无缝切换 SageMaker 到亚马逊，在机器学习 (ML) 项目上进行协作，同时对数据和机器学习资产实施访问管理。借助 Amazon DataZone 和 Amazon 之间新的内置集成 SageMaker，数据使用者和创建者可以简化基础设施设置中的机器学习管理，协作开展业务计划，并轻松管理数据和机器学习资产。有关更多信息，请参阅 使用 Amazon DataZone 内置蓝图 和 使用关联账户发布和使用数据。

亚马逊 DataZone 推出与 L AWS ake Formation 混合访问模式的集成

于 2024 年 3 月 4 日发布

亚马逊推 DataZone 出了与 AWS Lake Formation混合访问模式的集成。这种集成使您能够轻松地通过亚马逊发布和共享您的 AWS Glue 表 DataZone，而无需先在 AWS Lake Formation 中注册它们。首先，管理员在 Amazon DataZone 控制台中启用`DefaultDataLake`蓝图下的数据位置注册设置。然后，当数据使用者订阅通过 IAM 权限管理的 AWS Glue 表时，亚马逊 DataZone 首先以混合模式注册该表的 Amazon S3 位置，然后通过 La AWS ke Formation 管理该表的权限，向数据使用者授予访问权限。这样可以确保使用新授予的 La AWS ke Formation 权限继续存在表上的 IAM 权限，而不会中断任何现有工作流程。有关更多信息，请参阅 亚马逊与 AWS Lake Formation 混合模式 DataZone 集成 。

亚马逊 DataZone 推出与 Glue 数据 AWS 质量的集成

于 2024 年 3 月 4 日发布

亚马逊 DataZone 推出与 AWS Glue 数据质量的集成，并提供 API 来集成来自第三方数据质量解决方案的数据质量指标。新的集成使您能够将Glue AWS 数据质量分数自动发布到亚马逊 DataZone 业务数据目录中。Amazon DataZone API 可用于从第三方来源获取质量指标。发布后，数据使用者可以轻松

搜索数据资产，查看精细的质量指标，识别失败的检查和规则，从而为业务决策提供支持。有关更多信息，请参阅 Amazon 的数据质量 DataZone。

Amazon 中描述的 AI 推荐正式发布版 DataZone

于 2024 年 3 月 27 日发布

Amazon DataZone 宣布正式发布基于人工智能的新生成功能，通过丰富业务数据目录来改善数据发现、数据理解和数据使用。只需单击一下，数据生成者就可以生成全面的业务数据描述和上下文，突出显示有影响力的专栏，并提供有关分析用例的建议。此次发布增加了对API的支持，数据生产者可以使用这些API以编程方式生成资产描述。有关更多信息，请参阅 使用机器学习和生成式 AI。

亚马逊 DataZone 推出亚马逊 Redshift 集成增强功能

于 2024 年 3 月 21 日发布

亚马逊对其亚马逊Redshift集成 DataZone 进行了多项增强，简化了发布和订阅亚马逊Redshift表格和视图的过程。这些更新简化了数据创建者和使用者的体验，使他们能够使用 Amazon DataZone 管理员提供的预配置凭证和连接参数快速创建数据仓库环境。此外，这些增强功能使管理员能够更好地控制谁可以使用其 AWS 账户和 Amazon Redshift 集群中的资源以及用于什么目的。

- 蓝图配置：启用`DefaultDataWarehouseBlueprint`蓝图后，您可以通过将管理项目分配给已启用的`DefaultDataWarehouseBlueprint`蓝图来控制哪些项目可以使用您账户中的蓝图来创建环境配置文件。您还可以`DefaultDataWarehouseBlueprint`通过提供诸如集群、数据库和 AWS 密钥之类的参数来创建参数集。您也可以从 Amazon DataZone 控制台中创建 AWS 密钥。
- 环境配置文件：创建环境配置文件时，您可以选择提供自己的 Amazon Redshift 参数或使用蓝图配置中的一个参数集。如果您选择使用在蓝图配置中创建的参数集，则 AWS 密钥只需要`AmazonDataZoneDomain`和`AmazonDataZoneProject`标签（只有当您选择在环境配置文件中提供自己的参数集时，才需要标记）。在环境配置文件中，您可以指定已授权项目的列表。只有经过授权的项目才能使用此环境配置文件来创建数据仓库环境。您还可以指定允许发布哪些数据已获授权的项目。目前，您可以选择以下选项之一：1) 从任何架构中发布，2) 从默认环境架构发布，3) 不允许发布。
- 环境：数据创建者或使用者现在可以选择环境配置文件来创建环境，而无需提供自己的 Amazon Redshift 参数，包括 AWS 密钥、集群、工作组和数据库。这些参数从环境配置文件移植到环境中。除了创建环境外，Amazon DataZone 现在还会为环境创建默认架构。项目成员对该架构具有读写权限，并且可以通过运行在创建环境时创建的默认数据源，轻松地将在此架构中创建的任何表发布到目录中。用于创建环境的 Amazon Redshift 参数也可用于创建新的数据源（而不是数据创建者在创建数据源时提供自己的参数）。

AWS Amazon 的 Cloud Formation DataZone

于 2024 年 1 月 18 日发布

现在，Amazon 的用户 DataZone 可以利用它 AWS CloudFormation 来有效地建模和管理一套亚马逊 DataZone 资源。这种方法有助于实现资源的一致配置，同时还可以通过基础架构即代码实践实现生命周期管理。使用自定义模板，您可以精确定义所需的资源及其相互依赖关系。有关更多信息，请参阅 Amazon DataZone 资源类型参考。

直接将 IAM 委托人添加为 Amazon DataZone 项目的成员

于 2024 年 5 月 1 日发布

现在，您可以将 IAM 委托人添加为项目成员，即使这些 IAM 委托人尚未登录 Amazon DataZone （之前的要求）。在域管理员或 IT 管理员`iam:GetRole`向域的域执行角色添加`iam:GetUser`和后，项目所有者只需提供 IAM 角色或 IAM 用户的亚马逊资源名称 (ARN) 即可将 IAM 委托人添加为成员。IAM 委托人仍然必须拥有访问 Amazon 所需的 IAM 权限 DataZone ，这些权限可以在 IAM 控制台中进行配置。有关更多信息，请参阅 向项目添加成员。

Support 支持来自数据门户的自定义资产类型

于 2024 年 5 月 1 日发布

对自定义资产的支持使Amazon DataZone 能够通过数据门户对非结构化数据（包括仪表板、查询和模型）的资产进行分类，从而使您可以更轻松地直接在数据门户中添加自定义资产以及之前提供的 API 支持。通过在 Amazon 中创建 DataZone、更新和发布自定义资产，您可以共享、查找、订阅任何类型的资产，并构建可管理这些资产的业务工作流程。有关更多信息，请参阅 创建自定义资产类型。

2023

删除域名

于 2023 年 12 月 27 日发布

这项功能使您能够更轻松地删除您的域名。现在，即使域名不为空，也可以继续删除（如包含项目、环境、资产、数据源等）。有关更多信息，请参阅 删除域名。

混合模式

2023 年 12 月 22 日发布

亚马逊 DataZone 增加了对La AWS ke Formation混合模式的支持。有了这种支持，如果您将 AWS Glue表发布到亚马逊 DataZone ，其 AWS S3位置在混合模式下注册在Lake Formation中，则亚马逊 DataZone 会将此表视为托管资产，并且可以管理该表的订阅授权。在此功能发布之前，亚马逊 DataZone 会将此表视为非托管资产，也就是说，亚马逊 DataZone 将无法授予对该表的订阅。有关更多信息，请参阅 为亚马逊配置 Lake Formation 权限 DataZone。

HIPAA 资格

于 2023 年 12 月 14 日发布

亚马逊 DataZone 现已符合《1996 年美国健康保险流通与责任法案》(HIPAA)。要查看符合 HIPAA 标准的 AWS 服务列表，请参阅 https://aws.amazon.com/compliance/ hipaa-eligible-services-reference/。

Amazon 中描述的 AI 建议 DataZone（预览版）

于 2023 年 11 月 28 日发布

AWS 宣布在 Amazon 中预览基于人工智能的新生成功能，该功能通过丰富业务数据目录 DataZone来改善数据发现、数据理解和数据使用。只需单击一下，数据生成者就可以生成全面的业务数据描述和上下文，突出显示有影响力的专栏，并提供有关分析用例的建议。借助 Amazon 中描述的人工智能建议 DataZone，数据使用者可以识别分析所需的数据表和列，从而提高数据可发现性并减少与数据生产者的 back-and-forth 通信。预览版适用于在以下 AWS 区域配置的 Amazon DataZone 域名：美国东部（弗吉尼亚北部）、美国西部（俄勒冈）。有关更多信息，请参阅 使用机器学习和生成式 AI。

DefaultDataLake 蓝图增强

于 2023 年 11 月 20 日发布

Amazon 为 DefaultDataLake 蓝图添加 DataZone 了一项增强功能，让您可以更好地控制谁可以从您的 AWS 账户发布哪些数据。此功能发布引入了两项关键更改。

- 在控制台中，启用 DefaultDataLake 蓝图后，您可以通过将管理项目分配给已启用的 DefaultDataLake 蓝图来控制哪些项目可以使用您账户中的蓝图来创建环境配置文件。
- 第二个变化是在门户网站中。如果您使用 DefaultDataLake 蓝图创建环境配置文件，则还可以选择允许使用该环境配置文件创建环境的授权项目。默认情况下，允许所有项目使用数据湖环境配置文件，但您可以将环境配置文件限制为特定项目，也可以控制使用使用该配置文件创建的环境可以发布哪些数据。

有关更多信息，请参阅 创建环境配置文件。

设置

要设置亚马逊 DataZone，您必须拥有一个 AWS 账户并为亚马逊设置所需的 IAM 策略和权限 DataZone。

设置亚马逊 DataZone 权限后，建议您完成 “入门” 部分中的步骤，该部分将引导您完成创建亚马逊 DataZone 域、获取数据门户 URL 以及数据创建者和数据使用者的基本亚马逊 DataZone 工作流程。

主题

注册一个 AWS 账号

如果您没有 AWS 帐户，请完成以下步骤来创建一个帐户。

如果你有 AWS 组织，请创建一个账户：

1. 登录 AWS 管理控制台并打开 Organizations 控制台，网址为 https://console.aws.amazon.com/organizations/。
2. 在导航窗格中，选择AWS 账户。
3. 选择添加 AWS 账户。
4. 选择创建 AWS 账户并提供所需的详细信息。选择创建 AWS 账户。

要注册一个 AWS 账户

1. 打开 https://portal.aws.amazon.com/billing/signup。
2. 按照屏幕上的说明进行操作。

   在注册时，将接到一通电话，要求使用电话键盘输入一个验证码。

   当你注册一个 AWS 账户时，会创建一个AWS 账户 root 用户。root 用户有权访问账户中的所有 AWS 服务和资源。作为安全最佳实践，请 为管理用户分配管理访问权限，并且只使用根用户执行需要根用户访问权限的任务。

配置使用亚马逊 DataZone 管理控制台所需的 IAM 权限

任何想要使用 Amazon DataZone 管理控制台的用户、群组或角色都必须具有所需的权限。

主题

将必需和可选策略附加到用户、群组或角色以访问 Amazon DataZone 控制台

完成以下过程，将必需和可选的自定义策略附加到用户、组或角色。有关更多信息，请参阅 AWS Amazon 的托管政策 DataZone。

1. 登录 AWS 管理控制台并打开 IAM 控制台，网址为 https://console.aws.amazon.com/iam/。
2. 在导航窗格中，选择策略。
3. 选择以下策略以附加到您的用户、群组或角色。
   - 在策略列表中，选中旁边的复选框AmazonDataZoneFullAccess。您可以使用 Filter 菜单和搜索框来筛选策略列表。有关更多信息，请参阅 AWS 托管策略：AmazonDataZoneFullAccess。
   - （可选）为 IAM 权限创建自定义策略，以简化亚马逊 DataZone 服务控制台的角色创建。
   - （可选）为 Ident AWS ity Center 权限创建自定义策略，为您的域启用单点登录 (SSO)。
   - （可选）为 AWS 身份中心权限创建自定义策略，以添加和移除 SSO 用户和 SSO 群组对您的 Ama DataZone zon 域的访问权限。
4. 选择 Actions（操作），然后选择 Attach（附加）。
5. 选择要将策略附加到的用户、组或角色。您可以使用 Filter（筛选条件）菜单和搜索框来筛选委托人实体列表。选择用户、组或角色后，选择附加策略。

为 IAM 权限创建自定义策略以启用 Amazon DataZone 服务控制台简化角色创建

完成以下步骤以创建自定义内联策略，以获得必要的权限，让 Amazon DataZone 代表您在 AWS 管理控制台中创建必要的角色。

1. 登录 AWS 管理控制台并打开 IAM 控制台，网址为 https://console.aws.amazon.com/iam/。
2. 在导航窗格中，选择用户或用户组。
3. 在列表中，请选择要在其中嵌入策略的用户或组的名称。
4. 选择 Permissions (权限) 选项卡，然后展开 Permissions policies (权限策略) 部分（如有必要）。
5. 选择添加权限和创建内联策略链接。
6. 在创建策略屏幕的策略编辑器部分中，选择 JSON。

   使用以下 JSON 语句创建策略文档，然后选择下一步。

```
{
    "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. 在查看策略屏幕上，输入策略的名称。如果您对该策略感到满意，请选择 Create policy (创建策略)。确保屏幕顶部的红框中没有显示错误。更正报告的任何错误。

为管理与 Amazon DataZone 域名关联的账户的权限创建自定义策略

完成以下过程以创建自定义内联策略，使关联 AWS 账户拥有列出、接受和拒绝域资源共享所需的权限，然后在关联账户中启用、配置和禁用环境蓝图。要在蓝图配置期间启用可选的 Amazon DataZone 服务控制台简化角色创建，您还必须这样做为 IAM 权限创建自定义策略以启用 Amazon DataZone 服务控制台简化角色创建 。

1. 登录 AWS 管理控制台并打开 IAM 控制台，网址为 https://console.aws.amazon.com/iam/。
2. 在导航窗格中，选择用户或用户组。
3. 在列表中，请选择要在其中嵌入策略的用户或组的名称。
4. 选择 Permissions (权限) 选项卡，然后展开 Permissions policies (权限策略) 部分（如有必要）。
5. 选择添加权限和创建内联策略链接。
6. 在创建策略屏幕的策略编辑器部分中，选择 JSON。使用以下 JSON 语句创建策略文档，然后选择下一步。

```
{
    "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. 在查看策略屏幕上，输入策略的名称。如果您对该策略感到满意，请选择 Create policy (创建策略)。确保屏幕顶部的红框中没有显示错误。更正报告的任何错误。

（可选）为 Ident AWS ity Center 权限创建自定义策略，为您的域启用单点登录 (SSO)

完成以下步骤以创建自定义内联策略，以获得必要的权限，以便使用亚马逊的 AWS IAM 身份中心启用单点登录 (SSO)。 DataZone

1. 登录 AWS 管理控制台并打开 IAM 控制台，网址为 https://console.aws.amazon.com/iam/。
2. 在导航窗格中，选择用户或用户组。

3. 在列表中，请选择要在其中嵌入策略的用户或组的名称。
4. 选择 Permissions (权限) 选项卡，然后展开 Permissions policies (权限策略) 部分（如有必要）。
5. 选择添加权限和创建内联策略。
6. 在创建策略屏幕的策略编辑器部分中，选择 JSON。

   使用以下 JSON 语句创建策略文档，然后选择下一步。

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

7. 在查看策略屏幕上，输入策略的名称。如果您对该策略感到满意，请选择 Create policy (创建策略)。确保屏幕顶部的红框中没有显示错误。更正报告的任何错误。

（可选）为 AWS 身份中心权限创建自定义策略，以添加和移除 SSO 用户和 SSO 群组对您的 Ama DataZone zon 域的访问权限。

完成以下步骤以创建自定义内联策略，以获得添加和删除 SSO 用户和 SSO 群组对您的 Ama DataZone zon 域的访问权限所需的权限。

1. 登录 AWS 管理控制台并打开 IAM 控制台，网址为 https://console.aws.amazon.com/iam/。
2. 在导航窗格中，选择用户或用户组。
3. 在列表中，请选择要在其中嵌入策略的用户或组的名称。
4. 选择 Permissions (权限) 选项卡，然后展开 Permissions policies (权限策略) 部分（如有必要）。
5. 选择添加权限和创建内联策略。

6. 在创建策略屏幕的策略编辑器部分中，选择 JSON。

   使用以下 JSON 语句创建策略文档，然后选择下一步。

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

7. 在查看策略屏幕上，输入策略的名称。如果您对该策略感到满意，请选择 Create policy (创建策略)。确保屏幕顶部的红框中没有显示错误。更正报告的任何错误。

（可选）将您的 IAM 委托人添加为密钥用户，使用密钥管理服务 (KMS) 中的 AWS 客户管理密钥创建您的 Amazon DataZone 域

在您可以选择使用密钥管理服务 (KMS) 中的客户托管密钥 (CMK) 创建 Amazon DataZone 域之前，请完成以下步骤，使您的 IAM 委托人成为您的 KMS 密钥的用户。 AWS

1. 登录 AWS 管理控制台并打开 KMS 控制台，网址为 https://console.aws.amazon.com/kms/。
2. 要查看您账户中自己所创建和管理的密钥，请在导航窗格中选择 Customer managed keys (客户托管密钥)。
3. 在 KMS 密钥列表中，选择要检查的 KMS 密钥的别名或密钥 ID。

4. 要添加或删除密钥用户，以及允许或禁止外部 AWS 账户使用 KMS 密钥，请使用页面密钥用户部分中的控件。密钥用户可以在加密操作（如加密、解密、重新加密和生成数据密钥）中使用 KMS 密钥。

配置使用亚马逊 DataZone 数据门户所需的 IAM 权限

任何想要使用Amazon DataZone 数据门户或目录的用户、群组或角色都必须具有所需的权限。

主题

将必需的策略附加到用户、群组或角色以访问亚马逊 DataZone 数据门户

您可以使用 AWS 凭证或单点登录 (SSO) 凭证访问亚马逊 DataZone 数据门户。按照以下部分中的说明设置使用您的 AWS 凭据访问数据门户所需的权限。有关将 Amazon DataZone 与 SSO 配合使用的更多信息，请参阅为亚马逊设置 AWS IAM 身份中心 DataZone。

> **Note**
>
> 只有您域名 AWS 账户中的 IAM 委托人才能访问该域的数据门户。来自其他 AWS 账户的 IAM 委托人无法访问该域的数据门户。

完成以下过程，将所需的策略附加到用户、组或角色。有关更多信息，请参阅 AWS Amazon 的托管政策 DataZone。

1. 登录 AWS 管理控制台并打开 IAM 控制台，网址为 https://console.aws.amazon.com/iam/。
2. 在导航窗格中，选择 “用户”、“用户组” 或 “角色”。
3. 在列表中，选择要在其中嵌入策略的用户、组或角色的名称。
4. 选择 Permissions (权限) 选项卡，然后展开 Permissions policies (权限策略) 部分（如有必要）。
5. 选择添加权限和创建内联策略链接。
6. 在创建策略屏幕的策略编辑器部分中，选择 JSON。使用以下 JSON 语句创建策略文档，然后选择下一步。

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

7. 在查看策略屏幕上，输入策略的名称。如果您对该策略感到满意，请选择 Create policy (创建策略)。确保屏幕顶部的红框中没有显示错误。更正报告的任何错误。

向用户、群组或角色附加访问亚马逊 DataZone 目录所需的策略

> **Note**
>
> 只有您域名 AWS 账户中的 IAM 委托人才能访问该域的目录。来自其他 AWS 账户的 IAM 委托人无法访问该域的目录。

您可以通过以下步骤授予您的 IAM 身份通过 API 和软件开发工具包访问您的 Amazon DataZone 域名目录的权限。如果您希望这些 IAM 身份也能访问 Amazon DataZone 数据门户，请另外按照上述步骤操作将必需的策略附加到用户、群组或角色以访问亚马逊 DataZone 数据门户。有关更多信息，请参阅 AWS Amazon 的托管政策 DataZone。

1. 登录 AWS 管理控制台并打开 IAM 控制台，网址为 https://console.aws.amazon.com/iam/。
2. 在导航窗格中，选择策略。
3. 在策略列表中，选择策略旁边的AmazonDataZoneFullUserAccess单选按钮。您可以使用 Filter 菜单和搜索框来筛选策略列表。有关更多信息，请参阅 AWS 托管策略：AmazonDataZoneFullUserAccess。

4. 选择 Actions（操作），然后选择 Attach（附加）。
5. 通过选中每个委托人旁边的复选框，选择要将策略附加到的用户、组或角色。您可以使用 Filter（筛选条件）菜单和搜索框来筛选委托人实体列表。选择用户、组或角色后，选择附加策略。

如果您的域名使用密钥管理服务 (KMS) 的客户管理密钥加密，则将可选策略附加到 AWS 用户、群组或角色以访问亚马逊 DataZone 数据门户或目录

如果您使用自己的 KMS 密钥创建用于数据加密的 Amazon DataZone 域，则还必须创建具有以下权限的内联策略并将其附加到您的 IAM 委托人，以便他们可以访问亚马逊 DataZone 数据门户或目录。

1. 登录 AWS 管理控制台并打开 IAM 控制台，网址为 https://console.aws.amazon.com/iam/。
2. 在导航窗格中，选择 “用户”、“用户组” 或 “角色”。
3. 在列表中，选择要在其中嵌入策略的用户、组或角色的名称。
4. 选择 Permissions (权限) 选项卡，然后展开 Permissions policies (权限策略) 部分（如有必要）。
5. 选择添加权限和创建内联策略链接。
6. 在创建策略屏幕的策略编辑器部分中，选择 JSON。使用以下 JSON 语句创建策略文档，然后选择下一步。

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

7. 在查看策略屏幕上，输入策略的名称。如果您对该策略感到满意，请选择 Create policy (创建策略)。确保屏幕顶部的红框中没有显示错误。更正报告的任何错误。

为亚马逊设置 AWS IAM 身份中心 DataZone

> **Note**
>
> AWS 必须在与您的 Amazon DataZone 域名相同的 AWS 区域启用身份中心。目前， AWS 身份中心只能在单个 AWS 区域启用。

您可以使用单点登录 (SSO) 凭证或 AWS 凭证访问亚马逊 DataZone 数据门户。按照本节中的说明为亚马逊设置 AWS IAM 身份中心 DataZone。有关 AWS 凭证使用 Amazon DataZone 的更多信息，请参阅配置使用亚马逊 DataZone 管理控制台所需的 IAM 权限。

如果您已经在要创建 Amazon DataZone 域的同一 AWS 区域启用并配置了 AWS IAM Identity Center（ AWS 单点登录的继任者），则可以跳过本节中的步骤。

完成以下步骤以启用 AWS IAM 身份中心（ AWS 单点登录的继任者）。

1. 要启用 AWS IAM Identity Center，您必须使用您的 Organizations 管理账户 AWS 的证书登录管理控制台。 AWS 使用 Organizations 成员账户的证书登录时，您无法启用 IAM Ident AWS ity Center。有关更多信息，请参阅《Org anizations 用户指南》中的创建和管理 AWS 组织。
2. 打开 AWS IAM Identity Center（ AWS 单点登录的继任者）控制台，然后使用顶部导航栏中的 AWS 区域选择器选择要在其中创建 Amazon DataZone 域的区域。
3. 请选择 启用。
4. 选择您的身份来源。

   默认情况下，您可以获得 IAM Identity Center 存储，以便快速轻松地管理用户。或者，您可以改为连接外部身份提供商。在此过程中，我们使用默认的 IAM 身份中心存储。

   有关更多信息，请参阅选择您的身份来源。
5. 在 IAM 身份中心导航窗格中，选择群组，然后选择创建群组。输入群组名称并选择创建。
6. 在 IAM 身份中心导航窗格中，选择用户。
7. 在添加用户屏幕上，输入所需信息，然后选择向用户发送包含密码设置说明的电子邮件。用户应该会收到一封关于后续设置步骤的电子邮件。
8. 选择 “下一步：群组”，选择所需的群组，然后选择 “添加用户”。用户应收到一封邀请他们使用 SSO 的电子邮件。在这封电子邮件中，他们需要选择接受邀请并设置密码。

创建亚马逊 DataZone 域名后，您可以启用亚马逊 AWS 身份中心并向您的 SSO 用户 DataZone 和 SSO 群组提供访问权限。有关更多信息，请参阅 启用 Amazon 的 IAM 身份中心 DataZone。

开始使用

本节中的信息可帮助您开始使用 Amazon DataZone。如果您不熟悉 Amazon DataZone，请先熟悉中介绍的概念和术语Amazon DataZone 术语和概念。

本入门部分将引导您完成以下 Amazon DataZone 快速入门工作流程：

主题

- 亚马逊 DataZone 快速入门 Glue AWS 数据
- 亚马逊使用亚马逊 DataZone Redshift 数据快速入门
- 使用示例脚本的 Amazon DataZone 快速入门

> **Important**
>
> 在开始这两个快速入门工作流程中的任何一个步骤之前，必须完成本指南的 “设置” 部分中描述的步骤。如果您使用的是全新的 AWS 账户，则必须配置使用亚马逊 DataZone 管理控制台所需的权限。如果您使用的 AWS 账户已有 AWS Glue 数据目录对象，则还必须为亚马逊配置 Lake Formation 权限 DataZone。

亚马逊 DataZone 快速入门 Glue AWS 数据

主题

- 第 1 步-创建 Amazon DataZone 域名和数据门户
- 第 2 步-创建发布项目
- 步骤 3-创建环境
- 第 4 步-生成数据以供发布
- 第 5 步-从 AWS Glue 收集元数据
- 第 6 步-整理并发布数据资产
- 步骤 7-创建用于数据分析的项目
- 步骤 8-创建数据分析环境
- 步骤 9-搜索数据目录并订阅数据
- 第 10 步-批准订阅请求

- 步骤 11-在 Amazon Athena 中创建查询并分析数据

第 1 步-创建 Amazon DataZone 域名和数据门户

本节介绍为此工作流程创建 Amazon DataZone 域和数据门户的步骤。

完成以下步骤以创建 Amazon DataZone 域名。有关 Amazon DataZone 域名的更多信息，请参阅Amazon DataZone 术语和概念。

1. 导航到亚马逊 DataZone 控制台 https://console.aws.amazon.com/datazone，登录，然后选择创建域名。

   > **Note**
   >
   > 如果您想在此工作流程中使用现有 Amazon DataZone 域名，请选择查看域名，然后选择要使用的域名，然后继续执行创建发布项目的第 2 步。

2. 在创建域名页面上，为以下字段提供值：

   - 名称-为您的域名指定一个名称。就此工作流程而言，您可以将此域名命名为 “营销”。
   - 描述-指定可选的域描述。
   - 数据加密-默认情况下，您的数据使用为您 AWS 拥有和管理的密钥进行加密。对于此用例，您可以保留默认的数据加密设置。

     有关使用客户托管密钥的更多信息，请参阅Amazon 的静态数据加密 DataZone。如果您使用自己的 KMS 密钥进行数据加密，则必须在默认值中包含以下语句AmazonDataZoneDomainExecutionRole。

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

```
  ]
}
```

- 服务访问权限-在默认情况下保持所选的 “使用默认角色” 选项不变。

> **Note**
>
> 如果您在此工作流程中使用现有 Amazon DataZone 域名，则可以选择 “使用现有服务角色” 选项，然后从下拉菜单中选择现有角色。

- 在 “快速设置” 下，选择 “设置此帐户以使用和发布数据”。此选项启用内置的 Amazon 数据湖和数据仓库 DataZone 蓝图，并为该账户配置所需的权限、资源、默认项目以及默认数据湖和数据仓库环境配置文件。有关 Amazon DataZone 蓝图的更多信息，请参阅Amazon DataZone 术语和概念。
- 保持 “权限详情” 下的其余字段不变。

> **Note**
>
> 如果您已有 Amazon DataZone 域名，则可以选择 “使用现有服务角色” 选项，然后从 Glue 管理访问角色、Redshift 管理访问角色和配置角色的下拉菜单中选择现有角色。

- 保持 “标签” 下的字段不变。
- 选择创建域。

3. 成功创建域后，选择此域，然后在该域的摘要页面上记下该域的数据门户 URL。您可以使用此 URL 访问您的 Amazon DataZone 数据门户，以完成此工作流程中的其余步骤。您也可以通过选择打开数据门户来导航到数据门户。

> **Note**
>
> 在当前版本的 Amazon 中 DataZone，一旦创建了域，就无法修改为数据门户生成的 URL。

域名创建可能需要几分钟才能完成。等待域的状态变为 “可用”，然后再继续下一步。

第 2 步-创建发布项目

本节介绍为此工作流程创建发布项目所需的步骤。

1. 完成上述第 1 步并创建域名后，您将看到 “欢迎来到亚马逊 DataZone！ 窗口。在此窗口中，选择创建项目。
2. 例如，为该工作流程指定项目名称，您可以为其命名 SalesDataPublishingProject，然后将其余字段保持不变，然后选择 “创建”。

步骤 3-创建环境

本节介绍为此工作流程创建环境所需的步骤。

1. 完成上述步骤 2 并创建项目后，您将看到 “您的项目已准备就绪” 窗口。在此窗口中，选择创建环境。
2. 在创建环境页面上，指定以下内容，然后选择创建环境。
3. 为以下各项指定值：
   - 名称-指定环境的名称。在本演练中，你可以调用它`Default data lake environment`。
   - 描述-为环境指定描述。
   - 环境配置文件-选择DataLakeProfile环境配置文件。这使您能够在此工作流程 DataZone 中使用亚马逊来处理亚马逊 S3、 AWS Glue Catalog 和 Amazon Athena 中的数据。
   - 在本演练中，请保持其余字段不变。
4. 选择创建环境。

第 4 步-生成数据以供发布

本节介绍生成要在此工作流程中发布的数据所需的步骤。

1. 完成上述第 3 步后，在`SalesDataPublishingProject`项目中，在右侧面板的 “分析工具” 下，选择 Amazon Athena。这将使用项目的凭据打开 Athena 查询编辑器进行身份验证。确保在 Amazon 环境下拉列表中选择了您的发布 DataZone 环境，并按照查询编辑器中的方式选择了`<environment_name>%_pub_db`数据库。
2. 在本演练中，您将使用 “按选择创建表” (CTAS) 查询脚本来创建要发布到 Amazon 的新表。 DataZone在查询编辑器中，执行此 CTAS 脚本来创建一个可以发布并可供搜索和订阅的`mkt_sls_table`表。

```
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
```

确保在左侧的 “表和视图” 部分成功创建 mkt_sls_ table 表。现在，您有了可以发布到 Amazon DataZone 目录中的数据资产。

第 5 步-从 AWS Glue 收集元数据

本节介绍为该工作流程从 AWS Glue 收集元数据的步骤。

1. 完成上述步骤 4 后，在 Amazon DataZone 数据门户中，选择`SalesDataPublishingProject`项目，然后选择 “数据” 选项卡，然后在左侧面板中选择 “数据源”。
2. 选择在环境创建过程中创建的源。
3. 选择 “操作” 下拉菜单旁边的 “运行”，然后选择 “刷新” 按钮。数据源运行完成后，资产将添加到 Amazon DataZone 库存中。

第 6 步-整理并发布数据资产

本节介绍在此工作流程中整理和发布数据资产的步骤。

1. 完成上述步骤 5 后，在 Amazon DataZone 数据门户中，选择您在上一步中创建的`SalesDataPublishingProject`项目，选择 “数据” 选项卡，在左侧面板中选择 “库存数据”，然后找到`mkt_sls_table`表格。
2. 打开`mkt_sls_table`资产的详细信息页面，查看自动生成的公司名称。选择 “自动生成的元数据” 图标可查看资源和列的自动生成的名称。您可以单独接受或拒绝每个名称，也可以选择 “全部接受”

以应用生成的名称。或者，您也可以将可用的元数据表单添加到您的资产中，并选择词汇表术语来对数据进行分类。

3. 选择 “发布资源” 以发布该mkt_sls_table资源。

步骤 7-创建用于数据分析的项目

本节介绍创建用于数据分析的项目的步骤。这是此工作流程中数据使用者步骤的开始。

1. 完成上述步骤 6 后，在 Amazon DataZone 数据门户中，从项目下拉菜单中选择创建项目。
2. 在创建项目页面上，指定项目名称，例如，您可以为此工作流程命名 MarketingDataAnalysisProject，然后将其余字段保持不变，然后选择创建。

步骤 8-创建数据分析环境

本节介绍创建数据分析环境的步骤。

1. 完成上述步骤 7 后，在 Amazon DataZone 数据门户中，选择MarketingDataAnalysisProject项目，然后选择环境选项卡，然后选择创建环境。
2. 在创建环境页面上，指定以下内容，然后选择创建环境。
   - 名称-指定环境的名称。在本演练中，你可以调用它Default data lake environment。
   - 描述-为环境指定描述。
   - 环境配置文件-选择内置DataLakeProfile环境配置文件。
   - 在本演练中，请保持其余字段不变。

步骤 9-搜索数据目录并订阅数据

本节介绍搜索数据目录和订阅数据的步骤。

1. 完成上述步骤 8 后，在亚马逊 DataZone 数据门户中，选择亚马逊 DataZone图标，然后在亚马逊 DataZone 搜索字段中，使用数据门户搜索栏中的关键词（例如 “目录” 或 “销售”）搜索数据资产。

   如有必要，应用筛选器或排序，找到产品销售数据资产后，即可选择它来打开该资产的详细信息页面。
2. 在目录销售数据资产的详细信息页面上，选择订阅。

3. 在 “订阅” 对话框中，从下拉列表中选择您的MarketingDataAnalysisProject消费者项目，然后指定订阅请求的原因，然后选择 “订阅”。

第 10 步-批准订阅请求

本节介绍批准订阅请求的步骤。

1. 完成上述步骤 9 后，在 Amazon DataZone 数据门户中，选择用于发布资产的SalesDataPublishingProject项目。
2. 选择数据选项卡，然后选择已发布的数据，然后选择传入请求。
3. 现在，您可以看到需要批准的新请求所在的行。选择 “查看请求”。提供批准理由，然后选择批准。

步骤 11-在 Amazon Athena 中创建查询并分析数据

现在，您已成功将资产发布到 Amazon DataZone 目录并订阅了该资产，您可以对其进行分析。

1. 在亚马逊 DataZone 数据门户中，选择您的MarketingDataAnalysisProject消费者项目，然后从右侧面板的 “分析工具” 下，选择 Amazon Athena 的 “查询数据” 链接。这将使用项目的身份验证凭证打开 Amazon Athena 查询编辑器。从查询编辑器的 Amazon Environment 下拉列表中选择使用MarketingDataAnalysisProject者 DataZone 环境，然后`<environment_name>%sub_db`从数据库下拉列表中选择您的项目。
2. 现在，您可以对已订阅的表运行查询。您可以从 “表和视图” 中选择表格，然后选择 “预览”，在编辑器屏幕上显示 select 语句。运行查询以查看结果。

亚马逊使用亚马逊 DataZone Redshift 数据快速入门

主题

- 步骤 8-创建数据分析环境
- 步骤 9-搜索数据目录并订阅数据
- 第 10 步-批准订阅请求
- 第 11 步-在 Amazon Redshift 中创建查询并分析数据

第 1 步-创建 Amazon DataZone 域名和数据门户

完成以下步骤以创建 Amazon DataZone 域名。有关 Amazon DataZone 域名的更多信息，请参阅Amazon DataZone 术语和概念。

1. 导航到亚马逊 DataZone 控制台 https://console.aws.amazon.com/datazone，登录，然后选择创建域名。

   > **Note**
   >
   > 如果您想在此工作流程中使用现有 Amazon DataZone 域名，请选择查看域名，然后选择要使用的域名，然后继续执行创建发布项目的第 2 步。

2. 在创建域名页面上，为以下字段提供值：

   - 名称-为您的域名指定一个名称。出于此工作流程的目的，您可以调用此域`Marketing`。
   - 描述-指定可选的域描述。
   - 数据加密-默认情况下，您的数据使用为您 AWS 拥有和管理的密钥进行加密。在本演练中，您可以保留默认的数据加密设置。

     有关使用客户托管密钥的更多信息，请参阅Amazon 的静态数据加密 DataZone。如果您使用自己的 KMS 密钥进行数据加密，则必须在默认值中包含以下语句AmazonDataZoneDomainExecutionRole。

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

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

- 服务访问权限-选择 “使用自定义服务角色” 选项，然后AmazonDataZoneDomainExecutionRole从下拉菜单中选择。
- 在 “快速设置” 下，选择 “设置此帐户以使用和发布数据”。此选项启用内置的 Amazon 数据湖和数据仓库 DataZone 蓝图，并配置完成此工作流程中其余步骤所需的权限和资源。有关 Amazon DataZone 蓝图的更多信息，请参阅Amazon DataZone 术语和概念。
- 保持权限详细信息和标签下的其余字段不变，然后选择创建域。

3. 成功创建域后，选择此域，然后在该域的摘要页面上记下该域的数据门户 URL。您可以使用此 URL 访问您的 Amazon DataZone 数据门户，以完成此工作流程中的其余步骤。

> **Note**
>
> 在当前版本的 Amazon 中 DataZone，一旦创建了域，就无法修改为数据门户生成的 URL。

域名创建可能需要几分钟才能完成。等待域的状态变为 “可用”，然后再继续下一步。

第 2 步-创建发布项目

以下部分介绍在此工作流程中创建发布项目的步骤。

1. 完成步骤 1 后，使用数据门户 URL 导航至 Amazon DataZone 数据门户，然后使用单点登录 (SSO) 或 AWS IAM 凭证登录。
2. 选择 “创建项目”，指定项目名称，例如，为该工作流程指定项目名称 SalesDataPublishingProject，然后将其余字段保持不变，然后选择 “创建”。

步骤 3-创建环境

以下部分介绍在此工作流程中创建环境的步骤。

1. 完成步骤 2 后，在 Amazon DataZone 数据门户中，选择您在上一步中创建的`SalesDataPublishingProject`项目，然后选择环境选项卡，然后选择创建环境。

2. 在创建环境页面上，指定以下内容，然后选择创建环境。

   - 名称-指定环境的名称。在本演练中，你可以调用它`Default data warehouse environment`。
   - 描述-为环境指定描述。
   - 环境配置文件-选择DataWarehouseProfile环境配置文件。
   - 提供您的 Amazon Redshift 集群的名称、数据库名称以及存储数据的亚马逊 Redshift 集群的秘密 ARN。

   > **Note**
   >
   > 确保你在 Secrets Manager 中的 AWS 密钥包含以下标签（键/值）：
   >
   > - 对于亚马逊 Redshift 集群——datazone.rs.cluster：<cluster_name:database name>
   >
   >   对于 Amazon Redshift 无服务器工作组——datazone.rs.workgroup：<workgroup_name:database_name>
   > - AmazonDataZoneProject: <projectID>
   > - AmazonDataZoneDomain: <domainID>
   >
   > 有关更多信息，请参阅在 S AWS ecrets Manager 中存储数据库凭据。
   > 您在 S AWS ecrets Manager 中提供的数据库用户必须具有超级用户权限。

第 4 步-生成数据以供发布

以下部分介绍在此工作流程中生成要发布的数据的步骤。

1. 完成步骤 3 后，在亚马逊 DataZone 数据门户中，选择`SalesDataPublishingProject`项目，然后在右侧面板的 “分析工具” 下，选择 Amazon Redshift。这将使用项目的身份验证凭证打开 Amazon Redshift 查询编辑器。
2. 在本演练中，您将使用 “按选择创建表” (CTAS) 查询脚本来创建要发布到 Amazon 的新表。 DataZone在查询编辑器中，执行此 CTAS 脚本来创建一个可以发布并可供搜索和订阅的`mkt_sls_table`表。

```
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
```

确保成功创建 mkt_sls_table 表。现在，您有了可以发布到 Amazon DataZone 目录中的数据资产。

第 5 步——从亚马逊 Redshift 收集元数据

以下部分介绍从亚马逊 Redshift 收集元数据的步骤。

1. 完成步骤 4 后，在 Amazon DataZone 数据门户中，选择SalesDataPublishingProject项目，然后选择 “数据” 选项卡，然后选择 “数据源”。
2. 选择在环境创建过程中创建的源。
3. 选择 “操作” 下拉菜单旁边的 “运行”，然后选择 “刷新” 按钮。数据源运行完成后，资产将添加到 Amazon DataZone 库存中。

第 6 步-整理并发布数据资产

以下部分介绍了在此工作流程中策划和发布数据资产的步骤。

1. 完成第 5 步后，在 Amazon DataZone 数据门户中，选择SalesDataPublishingProject项目，然后选择数据选项卡，选择库存数据，然后找到mkt_sls_table表格。
2. 打开mkt_sls_table资产的详细信息页面，查看自动生成的公司名称。选择 “自动生成的元数据” 图标可查看资源和列的自动生成的名称。您可以单独接受或拒绝每个名称，也可以选择 “全部接受” 以应用生成的名称。或者，您也可以将可用的元数据表单添加到您的资产中，并选择词汇表术语来对数据进行分类。

3. 选择 “发布” 以发布mkt_sls_table资源。

步骤 7-创建用于数据分析的项目

以下部分介绍在此工作流程中创建用于数据分析的项目的步骤。

1. 完成步骤 6 后，在 Amazon DataZone 数据门户中，选择创建项目。
2. 在 “创建项目” 页面中，指定项目名称，例如，为该工作流程命名 MarketingDataAnalysisProject，然后将其余字段保持不变，然后选择 “创建”。

步骤 8-创建数据分析环境

以下部分介绍在此工作流程中创建用于数据分析的环境的步骤。

1. 完成步骤 7 后，在 Amazon DataZone 数据门户中，选择您在上一步中创建的MarketingDataAnalysisProject项目，然后选择环境选项卡，然后选择添加环境。
2. 在创建环境页面上，指定以下内容，然后选择创建环境。
   - 名称-指定环境的名称。在本演练中，你可以调用它Default data warehouse environment。
   - 描述-为环境指定描述。
   - 环境配置文件-选择DataWarehouseProfile环境配置文件。
   - 提供您的 Amazon Redshift 集群的名称、数据库名称以及存储数据的亚马逊 Redshift 集群的秘密 ARN。

> **Note**
>
> 确保你在 Secrets Manager 中的 AWS 密钥包含以下标签（键/值）：
>
> - 对于亚马逊 Redshift 集群——datazone.rs.cluster：<cluster_name:database name>
>
> 对于 Amazon Redshift 无服务器工作组——datazone.rs.workgroup：<workgroup_name:database_name>
> - AmazonDataZoneProject: <projectID>
> - AmazonDataZoneDomain: <domainID>
>
> 有关更多信息，请参阅在 S AWS ecrets Manager 中存储数据库凭据。

您在 S AWS ecrets Manager 中提供的数据库用户必须具有超级用户权限。

- 在本演练中，请保持其余字段不变。

步骤 9-搜索数据目录并订阅数据

以下部分介绍搜索数据目录和订阅数据的步骤。

1. 完成步骤 8 后，在亚马逊 DataZone 数据门户中，使用数据门户搜索栏中的关键词（例如 “目录” 或 “销售”）搜索数据资产。

   如有必要，应用筛选器或排序，找到产品销售数据资产后，即可选择它来打开该资产的详细信息页面。
2. 在产品销售数据资产的详细信息页面上，选择订阅。
3. 在对话框中，从下拉列表中选择您的消费者项目，提供访问请求的原因，然后选择订阅。

第 10 步-批准订阅请求

以下部分介绍在此工作流程中批准订阅请求的步骤。

1. 完成步骤 9 后，在 Amazon DataZone 数据门户中，选择用于发布资产的SalesDataPublishingProject项目。
2. 依次选择数据选项卡、已发布数据和传入请求。
3. 选择查看请求链接，然后选择批准。

第 11 步-在 Amazon Redshift 中创建查询并分析数据

现在，您已成功将资产发布到 Amazon DataZone 目录并订阅了该资产，您可以对其进行分析。

1. 在亚马逊 DataZone 数据门户网站的右侧面板上，单击 Amazon Redshift 链接。这将使用项目的身份验证凭证打开 Amazon Redshift 查询编辑器。
2. 现在，您可以对已订阅的表运行查询（select 语句）。您可以单击表格（three-vertical-dots 选项），然后选择预览以在编辑器屏幕上显示选择语句。执行查询以查看结果。

使用示例脚本的 Amazon DataZone 快速入门

以下部分介绍了调用各种 Amazon DataZone API 的示例脚本，您可以使用这些脚本来完成以下任务：

主题

创建 Amazon DataZone 域名和数据门户

您可以使用以下示例脚本创建 Amazon DataZone 域名。有关 Amazon DataZone 域名的更多信息，请参阅Amazon DataZone 术语和概念。

```
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",
    )
```

创建发布项目

您可以使用以下示例脚本在 Amazon 中创建发布项目 DataZone。

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

创建环境配置文件

您可以使用以下示例脚本在 Amazon 中创建环境配置文件 DataZone。

调用 `CreateEnvironmentProfile` API 时使用以下示例负载：

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

此示例脚本调用 API：CreateEnvironmentProfile

```
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
```

这是调用 CreateEnvironmentProfile API 后的输出负载示例：

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

创建环境

您可以使用以下示例脚本在 Amazon 中创建环境 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
```

从 AWS Glue 收集元数据

您可以使用此示例脚本从 AWS Glue 收集元数据。此脚本按标准计划运行。您可以从示例脚本中检索参数并将其设为全局参数。使用标准函数获取项目、环境和域 ID。 AWS Glue 数据源是在标准时间创建和运行的，可以在脚本的 cron 部分进行更新。

```
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"
    }
}
```

整理和发布数据资产

您可以使用以下示例脚本在 Amazon DataZone 中整理和发布数据资产。

您可以使用以下脚本来创建自定义表单类型：

```
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"
    )
```

您可以使用以下示例脚本来创建自定义资产类型：

```
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,
    )
```

您可以使用以下示例脚本来创建自定义资产：

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

您可以使用以下示例脚本来创建词汇表：

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

您可以使用以下示例脚本来创建词汇表术语：

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

您可以使用以下示例脚本使用系统定义的资产类型创建资产：

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

您可以使用以下示例脚本来创建资源修订版并附加词汇表术语：

```
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:>"]
    )
```

您可以使用以下示例脚本来发布资源：

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

搜索数据目录并订阅数据

您可以使用以下示例脚本来搜索数据目录和订阅数据：

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

您可以使用以下示例脚本来获取资产的清单 ID：

```
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']
```

您可以使用以下示例脚本使用清单 ID 创建订阅请求：

```
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."
    )
```

使用create_subscription_response上述方法，获取订阅 subscription_request_id，然后使用以下示例脚本接受/批准订阅：

```
subscription_request_id = create_subscription_response["id"]

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

其他有用的示例脚本

在 Amazon 中处理数据时，您可以使用以下示例脚本来完成各种任务 DataZone。

使用以下示例脚本列出现有的 Amazon DataZone 域名：

```
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
```

使用以下示例脚本列出现有的 Amazon DataZone 项目：

```
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
```

使用以下示例脚本列出现有的 Amazon DataZone 元数据表单：

```
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
```

管理 Amazon DataZone 域名和用户访问权限

主题

创建域名

> **Note**
>
> 如果您使用 DataZone 带 AWS 身份中心的 Amazon 来向 SSO 用户和群组提供访问权限，则当前您的亚马逊 DataZone 域必须与您的 AWS 身份中心实例位于同一 AWS 区域。

Amazon DataZone，域名是一个组织实体，用于连接您的资产、用户及其项目。有关更多信息，请参阅 Amazon DataZone 术语和概念。

要创建 Amazon DataZone 域名，您必须在账户中扮演具有管理权限的 IAM 角色。 配置使用亚马逊 DataZone 管理控制台所需的 IAM 权限以获得创建域所需的最低权限。

Amazon 需要其他 IAM 角色 DataZone 才能代表具有默认配置的域用户执行操作。您可以提前创建这些 IAM 角色，也可以让 Amazon 为您 DataZone 创建它们。如果您希望 Amazon DataZone 在域名创建过程中为您创建这些 IAM 角色，那么要创建域，您必须担任具有角色创建权限的 IAM 角色。请参阅 为 IAM 权限创建自定义策略以启用 Amazon DataZone 服务控制台简化角色创建 。根据您的域名创建选择，Amazon DataZone 将为您创建最多四个新的 IAM 角色：AmazonDataZoneDomainExecutionRoleAmazonDataZoneGlueManageAccessRole、AmazonDataZone和AmazonDataZoneProvisioningRole。

完成以下步骤以创建 Amazon DataZone 域名。

1. 通过 https://console.aws.amazon.com/datazone 导航到亚马逊 DataZone 控制台，然后使用顶部导航栏中的区域选择器选择相应的 AWS 区域。
2. 选择创建属性域并为以下字段提供值：

   - 名称-为域名指定一个友好名称。一旦创建了域，就无法更改此名称。
   - 描述-（可选）指定域描述。
   - 数据加密-您的亚马逊 DataZone 域名、元数据和报告数据由 AWS 密钥管理服务 (KMS) 使用您的亚马逊特有的密钥进行加密 DataZone。使用此字段指定是要使用 AWS 自有密钥还是选择其他 AWS KMS 密钥。

     有关使用客户托管密钥的更多信息，请参阅Amazon 的静态数据加密 DataZone。
     如果您使用自己的 KMS 密钥进行数据加密，则必须在默认值中包含以下语句AmazonDataZoneDomainExecutionRole。

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

   - 服务访问权限-选择是让 Amazon DomainExecutionRole为您 DataZone 创建和使用新的 IAM 角色，还是选择现有的 IAM 角色。
   - 快速设置-（可选）勾选此复选框，让亚马逊为您的账户 DataZone 设置数据消耗和发布功能，从而更快地开始使用。亚马逊 DataZone 将创建三个 IAM 角色用于配置、接收和管理对 GI AWS ue 和 Amazon Redshift 资源的访问权限，创建一个新的 Amazon S3 存储桶，创建管理 DataZone 亚马逊项目，以及为数据湖和数据仓库默认蓝图创建环境配置文件。

- 标签-（可选）为域指定 AWS 标签（键和值对）。
- 成功创建域名后，您的浏览器应刷新以显示您的新 Amazon DataZone 域名的详情页面。

编辑域名

在 Amazon 中 DataZone，域名是一个组织实体，用于连接您的资产、用户及其项目。有关更多信息，请参阅 Amazon DataZone 术语和概念。

创建 Amazon DataZone 域后，您可以稍后编辑该域名以：更改描述、启用 IAM Identity Center 以及添加、编辑或删除标签密钥及其值。要编辑 Amazon DataZone 域名，您必须在账户中扮演具有管理权限的 IAM 角色。 配置使用亚马逊 DataZone 管理控制台所需的 IAM 权限以获得编辑域所需的最低权限。

要编辑域名，请完成以下步骤：

1. 登录 AWS 管理控制台并打开亚马逊 DataZone 控制台，网址为 https://console.aws.amazon.com/datazone。
2. 选择查看域名，然后从列表中选择域名。该名称是一个超链接。
3. 在域名的详细信息页面上，选择编辑。
4.
   - 编辑描述。
   - 设置 I AM 身份中心设置。要详细了解这些设置，请参阅为亚马逊设置 AWS IAM 身份中心 DataZone。
   - 添加、编辑或移除标签键及其值。
5. 编辑完毕后，选择更新域名。

删除域名

在 Amazon 中 DataZone，域名是一个组织实体，用于连接您的资产、用户及其项目。有关更多信息，请参阅 Amazon DataZone 术语和概念。

删除域名的行为是最终的。删除操作将不可撤销地删除每个 Amazon DataZone 实体，包括数据源、项目、环境、资产、术语表和元数据表单。删除不会删除亚马逊 DataZone 可能帮助您创建的非亚马逊 DataZone AWS 资源，例如 IAM 角色、S3 存储桶、G AWS lue 数据库以及通过或 LakeFormation Redshift 授予的订阅授权。如果您不再需要这些资源，请在相应的 AWS 服务中将其删除。

为防止他人恶意删除域名，删除域名需要亚马逊的 IAM 管理权限 DataZone，您可以使用 IAM 进行配置。为防止他人意外删除域名，删除域名需要输入确认词（在 Amazon DataZone 控制台中）。

要删除域名，请完成以下步骤：

1. 登录 AWS 管理控制台并打开亚马逊 DataZone 控制台，网址为 https://console.aws.amazon.com/datazone。
2. 选择查看域名，然后从列表中选择域名。该名称是一个超链接。
3. 选择 “删除” 并查看信息性警告。
4. 键入请求的文本，以确认您已理解这些警告。选择删除。

> **Important**
>
> 删除您的域名是一项不可撤销的操作，您或您都无法撤消。 AWS

> **Note**
>
> 当您或您的域用户在项目中创建环境时，Amazon DataZone 会在您的域名或关联账户中创建 AWS 资源，为您和您的域用户提供功能。以下是 Amazon DataZone 可能为您域中的项目创建的 AWS 资源列表以及默认名称。删除域名并不会删除您 AWS 账户中的任何此类 AWS 资源。
>
> - <environmentId>IAM 角色：datazone_usr_。
> - <environmentName>Glue 数据库：(1) <environmentName>_pub_db-*，(2) _sub_db-*。如果已经存在同名数据库，Amazon DataZone 将添加环境 ID。
> - <environmentName>Athena 工作组：-*。如果已经存在同名工作组，Amazon DataZone 将添加环境 ID。
> - CloudWatch 日志组：datazone_ <environmentId>

启用 Amazon 的 IAM 身份中心 DataZone

> **Note**
>
> 要完成此过程，您必须在与您的 Amazon DataZone 域相同的 AWS 区域启用 IA AWS M 身份中心。

您可以使用 AWS IAM 身份中心为 SSO 用户和群组提供访问您的 Amazon DataZone 数据门户的权限。完成后为亚马逊设置 AWS IAM 身份中心 DataZone，您可以允许您的 SSO 用户和群组访问您的 Amazon DataZone 域名数据门户。

要使您的 Amazon DataZone 域名能够使用 IA AWS M 身份中心，您必须在账户中扮演具有管理权限的 IAM 角色。 配置使用亚马逊 DataZone 管理控制台所需的 IAM 权限并为 IAM 权限创建自定义策略以启用 Amazon DataZone 服务控制台简化角色创建 获得启用 IAM 身份中心以便在 Amazon 上使用所需的最低权限 DataZone。

完成以下步骤以启用 Amazon AWS 的 IAM 身份中心 DataZone。

1. 登录 AWS 管理控制台并打开控制 DataZone 台，网址为 https://console.aws.amazon.com/datazone。
2. 选择查看域名，然后从列表中选择域名。该名称是一个超链接。
3. 在域名的详情页面上，选择编辑。
   - 选中 “在 IAM 身份中心启用用户” 复选框。
   - 在两种用户分配模式之间进行选择。一旦根据您的选择更新了您的域名，以后就无法对其进行更改。
     - 通过隐式用户分配，任何添加到您的 IAM 身份中心目录的用户都可以访问您的 Amazon DataZone 域。
     - 使用显式用户分配，您将从 IAM Identity Center 目录中添加特定用户或群组，为他们提供访问您的 Amazon DataZone 域的权限。稍后，您将在 Amazon DataZone 控制台中添加和删除这些用户和群组。
4. 对您的选择感到满意后，选择更新域名。

禁用 Amazon 的 IAM 身份中心 DataZone

禁用 AWS Amazon DataZone 域名的 IAM 身份中心将取消所有 SSO 用户的访问权限。

> **Note**
>
> 禁用 IAM 身份中心不会停止向 SSO 用户计费。要停止向 SSO 用户计费，您必须在您的域中停用他们。计费将持续到用户停用的月底。要停用用户，请参阅在 Amazon DataZone 控制台中管理用户。

您可以使用 AWS IAM 身份中心为 SSO 用户和群组提供访问您的 Amazon DataZone 数据门户的权限。如果您已启用适用于 Amazon AWS 的 IAM Identity Center DataZone，则可以稍后禁用所有用户的访问权限。

要禁用用于您的 Amazon DataZone 域的 IA AWS M 身份中心，您必须在账户中扮演具有管理权限的 IAM 角色。 配置使用亚马逊 DataZone 管理控制台所需的 IAM 权限并为 IAM 权限创建自定义策略以启用 Amazon DataZone 服务控制台简化角色创建 获得禁用 IAM 身份中心在 Amazon 上使用所需的最低权限 DataZone。

完成以下步骤以禁用 Amazon AWS 的 IAM 身份中心 DataZone。

1. 登录 AWS 管理控制台并打开控制 DataZone 台，网址为 https://console.aws.amazon.com/datazone。
2. 选择查看域名，然后从列表中选择域名。该名称是一个超链接。
3. <regionName><accountId><domainName>复制您的域名的亚马逊资源名称 (ARN)，该名称以 arn: aws: datazone::: domain/ 开头。
4. 打开 IAM 身份中心控制台，网址为 https://console.aws.amazon.com/singlesignon/。
5. 选择应用程序。
6. 选择您要禁用 AWS IAM Identity Center 的域，这将取消所有 SSO 用户对该域数据门户的访问权限。您可以使用 “筛选” 菜单和搜索框来筛选应用程序列表。
7. 从 “操作” 菜单中选择 “禁用”。
8. SSO 用户将无法访问 Amazon DataZone 域名。
9. 要为 Amazon DataZone 域重新启用 AWS IAM 身份中心，请选择要为其重新启用 AWS IAM 身份中心的域，然后从 “操作” 菜单中选择 “启用”。

在 Amazon DataZone 控制台中管理用户

您的用户可以使用其 AWS 凭证或单点登录 (SSO) 凭证访问亚马逊 DataZone 数据门户。要在亚马逊 DataZone控制台中管理亚马逊 DataZone 域的用户，您必须在账户中扮演具有管理权限的 IAM 角色。配置使用亚马逊 DataZone 管理控制台所需的 IAM 权限以获得在 Amazon DataZone 控制台中管理用户所需的最低权限。

主题

- 管理 IAM 角色和用户
- 管理 SSO 用户

- 管理 SSO 群组

管理 IAM 角色和用户

IAM 角色和用户使用 AWS 身份和访问管理 (IAM) 创建，并通过策略附加的权限访问您的 DataZone 亚马逊域名。有关更多信息，请参阅 配置使用亚马逊 DataZone 数据门户所需的 IAM 权限。在当前版本的 Amazon 中 DataZone，来自亚马逊 DataZone 域名所有者账户的管理员可以为自己账户中的用户或关联账户中的用户创建 IAM 用户个人资料。亚马逊 DataZone 域名所有者账户的管理员也可以将现有用户的状态设置为 “已分配” 或 “未分配”（如已分配或未分配以使用亚马逊 DataZone），或者激活或停用任何现有用户。

1. 登录 AWS 管理控制台并打开控制 DataZone 台，网址为 https://console.aws.amazon.com/datazone。
2. 选择查看域名，然后从列表中选择域名。该名称是一个超链接。
3. 在域的详细信息页面上，选择用户管理。
4. 要在 Amazon DataZone 域名所有者账户或关联账户中添加用户 IAM 用户，请选择添加，然后选择添加 IAM 用户。
5. 在添加用户页面上，选择当前账户或关联账户，使用查找并添加用户或角色字段查找要添加的用户，然后选择添加用户。
6. 要查看现有 IAM 用户的状态，请在用户管理页面的用户类型下拉菜单中选择 IAM 用户。
   - “名称” 列显示 IAM 用户或角色的 ARN。
   - 状态列显示域中 IAM 用户或角色的当前状态。
     - 已指定 IAM 用户已被分配使用亚马逊 DataZone。
     - “未分配” 表示已取消指定 IAM 用户使用亚马逊。 DataZone
     - 已激活意味着 IAM 用户或角色已调用 API、发出命令（通过命令行界面）或访问了您域名的 Amazon DataZone 门户，并且您需要为该用户的订阅付费。
     - 停用意味着 IAM 用户或角色被禁止访问您的 Amazon DataZone 域。
7. 要停用当前已激活的 IAM 用户或角色，请选中该用户旁边的复选框，然后从 “操作” 菜单中选择 “停用”。用户将失去对 Amazon DataZone 域的访问权限。用户的账单将在当前日历月末结束。
8. 要激活当前已停用的 IAM 用户或角色，请选中该用户旁边的复选框，然后从 “操作” 菜单中选择 “激活”。如果 IAM 用户或角色具有适当的权限，则该用户将获得对 Amazon DataZone 域的访问权限。将重新开始为用户计费。

管理 SSO 用户

SSO 用户是在 AWS IAM Identity Center 中创建的，或者与您的身份提供商同步。有关更多信息，请参阅为亚马逊设置 AWS IAM 身份中心 DataZone和启用 Amazon 的 IAM 身份中心 DataZone以启用和配置适用于 Amazon 的 AWS IAM 身份中心 DataZone。您可以查看分配给该域的 SSO 用户列表、添加 SSO 用户和删除 SSO 用户。

1. 登录 AWS 管理控制台并打开控制 DataZone 台，网址为 https://console.aws.amazon.com/datazone。
2. 选择查看域名，然后从列表中选择域名。该名称是一个超链接。
3. 在域的详细信息页面上，向下滚动并选择用户管理。
4. 对于用户类型，选择 SSO 用户以查看当前的 SSO 用户列表。
   - “名称” 列显示 SSO 用户的姓名。
   - 状态列显示域中 SSO 用户的当前状态。
     - 已分配表示已将 SSO 用户明确分配给该域。因此，用户可以访问亚马逊 DataZone。仅当您的域名的身份提供商模式设置为显式分配时，才会使用此状态。
     - 已激活表示 SSO 用户已访问该域的 Amazon DataZone 门户，并且您需要为该用户的订阅付费。激活会自动发生。
     - 停用意味着 SSO 用户对域名数据门户的访问被阻止。该用户的账单于其访问权限被停用的当月月底结束。
     - 已移除意味着 SSO 用户之前已被分配到该域，但在他们访问之前就被移除了。
5. 通过选择添加和添加用户来添加 SSO 用户。如果域名设置为隐式用户分配，则此选项不可用，这意味着身份池中的所有用户都可以访问该Amazon DataZone 域。
   - 在添加用户页面上，搜索要添加的用户的别名。搜索框下方将出现一个包含潜在匹配项的列表。
   - 选择要添加的用户。他们的别名将作为筹码出现在搜索框下方。
   - 如果您对要添加的用户列表感到满意，请选择添加用户。
   - 用户被分配到状态为 “已分配” 的 Amazon DataZone 域。
   - 当用户首次访问域的数据门户时，状态将自动更改为 “已激活”，并开始向您收取用户的订阅费用。
6. 选择已分配的 SSO 用户并从 “操作” 菜单中选择 “禁用”，即可移除该用户。因此，用户将失去对 Amazon DataZone 域的访问权限。用户的状态将显示为 “已移除”。如果将域设置为隐式用户分配，则此选项不可用。

7. 通过选择已激活的 SSO 用户并从 “操作” 菜单中选择 “停用” 来停用该用户。因此，用户对 Amazon DataZone 域的访问权限将丢失并被阻止。用户的订阅费用将持续到月底。用户的状态将显示为 “已停用”。
8. 通过选择已停用的 SSO 用户并从 “操作” 菜单中选择 “激活” 来激活该用户。因此，用户将重新获得对 Amazon DataZone 域的访问权限。计费将立即开始。用户将显示为 “已激活”。

管理 SSO 群组

SSO 组是在 AWS IAM 身份中心中创建的，或者与您的身份提供商同步。有关更多信息，请参阅为亚马逊设置 AWS IAM 身份中心 DataZone和启用 Amazon 的 IAM 身份中心 DataZone以启用和配置适用于 Amazon 的 AWS IAM 身份中心 DataZone。您可以查看分配给该域的 SSO 组列表、添加 SSO 组和删除 SSO 组。

1. 登录 AWS 管理控制台并打开控制 DataZone 台，网址为 https://console.aws.amazon.com/datazone。
2. 选择查看域名，然后从列表中选择域名。该名称是一个超链接。
3. 在域的详细信息页面上，向下滚动并选择用户管理。
4. 对于用户类型，选择 SSO 群组以查看当前的 SSO 群组列表。
   - “名称” 列显示 SSO 组的名称。
   - 状态列显示域中 SSO 组的当前状态。
     - 已分配表示已将 SSO 组明确分配给该域。因此，群组中的所有用户都可以访问该域的数据门户（除非用户已停用）。
     - 未分配意味着 SSO 组已从域中删除。群组中的用户无法通过其在该群组中的成员身份访问该域的数据门户。
5. 通过选择添加和添加群组来添加 SSO 群组。如果域名设置为隐式用户分配，则此选项不可用，这意味着无论群组成员资格如何，身份池中的所有用户都可以访问Amazon DataZone 域。
   - 在添加群组页面上，搜索要添加的群组的别名。搜索框下方将出现一个包含潜在匹配项的列表。
   - 选择要添加的群组。他们的别名将作为筹码出现在搜索框下方。
   - 如果您对要添加的群组列表感到满意，请选择添加群组。
   - 这些群组被分配到状态为 “已分配” 的 Amazon DataZone 域。
   - 当群组成员访问域的数据门户时，状态将自动更改为 “已激活”，并开始向您收取该用户的订阅费用。

6. 选择已分配的 SSO 群组，然后从 “操作” 菜单中选择 “取消分配”，即可移除该群组。因此，该群组将无法访问 Amazon DataZone 域名。群组的状态将显示为 “未分配”。 DataZone 通过该群组的成员资格获得Amazon访问权限的用户将失去访问权限。如果将域设置为隐式用户分配，则此选项不可用。要停止为因取消分配群组而被删除访问权限的用户计费，接下来您需要手动选择并停用他们的用户个人资料。

在 Amazon DataZone 数据门户中管理用户权限

在当前版本的 Amazon 中 DataZone，默认授权机制允许亚马逊 DataZone 域的所有经过身份验证的用户（IAM 和 SSO）创建项目、在项目中创建实体和进行搜索。项目成员仍必须遵守根据其指定的项目所有者或项目参与者角色赋予他们的权限。

使用 Amazon DataZone 内置蓝图

用于创建环境的蓝图定义了环境所属项目的成员在处理 Amazon DataZone 目录中的资产时可以使用的工具和服务。在当前版本的 Amazon 中 DataZone，有以下内置蓝图：

- 数据湖蓝图
- 数据仓库蓝图
- 亚马逊 SageMaker 蓝图

主题

在拥有 Amazon DataZone 域 AWS 名的账户中启用内置蓝图

用于创建环境的蓝图定义了环境所属项目的成员在处理 Amazon DataZone 目录中的资产时可以使用的工具和服务。

在当前版本的 Amazon 中 DataZone，有几个内置蓝图：数据湖蓝图、数据仓库蓝图和亚马逊 SageMaker 蓝图。

- 数据湖蓝图包含启动和配置一组服务（AWS Glue、 AWS Lake Formation、Amazon Athena）以发布和使用亚马逊目录中的数据湖资产的定义。 DataZone
- 数据仓库蓝图包含启动和配置一组服务（Amazon Redshift）的定义，以发布和使用亚马逊目录中的亚马逊 Redshift 资产。 DataZone
- 亚马逊 SageMaker 蓝图包含启动和配置一组服务（Amazon SageMaker Studio）以发布和使用亚马逊 DataZone 目录中的亚马逊 SageMaker 资产的定义。

有关更多信息，请参阅 Amazon DataZone 术语和概念。

创建 Amazon DataZone 域时，您可以选择在域创建过程中自动启用默认数据湖和默认数据仓库内置蓝图的快速设置。快速设置还可以使用这些内置蓝图为您创建默认环境配置文件和默认环境。

如果您在创建亚马逊 DataZone 域名时未选择快速设置，则可以使用以下步骤在存放此亚马逊 DataZone 域名的 AWS 账户中启用可用的内置蓝图。必须先启用这些内置蓝图，然后才能使用它们在此域中创建环境配置文件和环境。

要通过亚马逊 DataZone 管理控制台在亚马逊 DataZone 域中启用内置蓝图，您必须在账户中扮演具有管理权限的 IAM 角色。 配置使用亚马逊 DataZone 管理控制台所需的 IAM 权限以获得最低权限。

在 Amazon DataZone 域中启用内置蓝图

1. 通过 https://console.aws.amazon.com/datazone 导航到亚马逊 DataZone 控制台，然后使用您的账户凭证登录。
2. 选择 “查看域”，然后选择要在其中启用一个或多个内置蓝图的域。
3. 在域名详细信息页面上，导航至蓝图选项卡。
4. 从蓝图列表中，选择、DefaultDataLake或 Amazon SageMaker 蓝图。DefaultDataWarehouse
5. 在所选蓝图的详细信息页面上，选择在此账户中启用。
6. 在 “权限和资源” 页面上，指定以下内容：

   - 如果您要启用DefaultDataLake蓝图，请为 Glue 管理访问权限角色指定一个新的或现有的服务角色，该角色 DataZone 授予亚马逊收录和管理对 G AWS lue 和 La AWS ke Formation 中表的访问权限的授权。
   - 如果您要启用DefaultDataWarehouse蓝图，请为 Redshift 管理访问权限角色指定一个新的或现有的服务角色，该角色 DataZone 授权亚马逊获取和管理对 Amazon Redshift 中的数据共享、表和视图的访问权限。
   - 如果您要启用亚马逊 SageMaker蓝图，请为SageMaker 管理访问角色指定一个新的或现有的服务角色，以授予亚马逊向目录发布亚马逊 SageMaker 数据的 DataZone权限。它还授予亚马逊授予访问 DataZone 权限或撤销对亚马逊在目录中 SageMaker 发布的资产的访问权限的权限。

     > **Important**
     >
     > 在您启用亚马逊 SageMaker蓝图时，亚马逊 DataZone 会检查当前账户和地区中是否 DataZone 存在以下 Amazon 的 IAM 角色。如果这些角色不存在，Amazon DataZone 会自动创建它们。
     >
     > - AmazonDataZoneGlueAccess-<region>-<domainId>
     > - AmazonDataZoneRedshiftAccess-<region>-<domainId>

   - 对于配置角色，请指定一个新的或现有的服务角色，该角色 DataZone 授予 Amazon 在环境账户和区域 AWS CloudFormation 中使用创建和配置环境资源的授权。
   - 如果您要为 SageMaker-Glu e 数据源的 Amazon S3 存储桶启用亚马逊 SageMaker蓝图，请指定 AWS 账户中所有 SageMaker 环境都要使用的 Amazon S3 存储桶。您指定的存储桶前缀必须是以下之一：

- 亚马逊数据区*
- datazone-sagemaker*
- sagemaker-datazone*
- DataZone-Sagemaker*
- Sagemaker-* DataZone
- DataZone-SageMaker*
- SageMaker-DataZone*

7. 选择启用蓝图。

启用所选蓝图后，您可以控制哪些项目可以使用您账户中的蓝图来创建环境配置文件。您可以通过将管理项目分配给蓝图的配置来实现此目的。

指定在已启用的蓝图上管理项目

1. 通过 https://console.aws.amazon.com/datazone 导航到亚马逊 DataZone 控制台，然后使用您的账户凭证登录。
2. 选择 “查看域”，然后选择要为所选蓝图添加管理项目的域。
3. 选择蓝图选项卡，然后选择要使用的蓝图。
4. 默认情况下，域内的所有项目都可以使用账户中的 DefaultDataLake 或或 DefaultDataWareshouse Amazon SageMaker 蓝图来创建环境配置文件。但是，您可以通过将管理项目分配给蓝图来限制这一点。要添加管理项目，请选择选择管理项目，然后从下拉菜单中选择要添加为管理项目的项目，然后选择选择管理项目。

在 AWS 账户中启用 DefaultDataWarehouse 蓝图后，您可以向蓝图配置中添加参数集。参数集是一组键和值，是亚马逊 DataZone 与您的 Amazon Redshift 集群建立连接所必需的，用于创建数据仓库环境。这些参数包括您的 Amazon Redshift 集群的名称、数据库以及保存集群凭证的 AWS 密钥。

向 DefaultDataWarehouse 蓝图添加参数集

1. 通过 https://console.aws.amazon.com/datazone 导航到亚马逊 DataZone 控制台，然后使用您的账户凭证登录。
2. 选择 “查看域”，然后选择要添加参数集的域。
3. 选择蓝图选项卡，然后选择 DefaultDataWareshouse 蓝图以打开蓝图详细信息页面。
4. 在蓝图详细信息页面的参数集选项卡下，选择创建参数集。

- 为参数集提供一个名称。
- （可选）提供参数集的描述。
- 选择一个区域
- 选择 Amazon Redshift 集群或亚马逊 Redshift Serverless。
- 选择保存所选 Amazon Redshift 集群或 Amazon Redshift 无服务器工作组凭证的 AWS 秘密 ARN。 AWS 密钥必须用`AmazonDataZoneDomain : [Domain_ID]`标签进行标记，才有资格在参数集中使用。
  - 如果您没有现有 AWS 密钥，也可以通过选择 “创建新密钥” 来创建新 AWS 密钥。这将打开一个对话框，您可以在其中提供密钥的名称、用户名和密码。选择 “创建新 AWS 密钥” 后，Amazon 将在 Secr AWS ets Manager 服务中 DataZone创建一个新密钥，并确保该密钥使用您尝试创建参数集的域进行标记。
- 如果您在上述步骤中选择了 Amazon Redshift 集群，那么现在请从下拉列表中选择一个集群。如果您在上述步骤中选择了 Amazon Redshift 工作组，那么现在请从下拉列表中选择一个工作组。
- 输入所选 Amazon Redshift 集群或 Amazon Redshift Serverless 工作组中的数据库名称。
- 选择 “创建参数集”。

在您的 AWS 账户中启用 Amazon SageMaker 蓝图后，您可以向蓝图配置中添加参数集。参数集是一组键和值，是亚马逊与您的亚马逊 DataZone SageMaker 建立连接所必需的，用于创建 sagemaker 环境。

向 Amazon SageMaker 蓝图添加参数集

1. 通过 https://console.aws.amazon.com/datazone 导航到亚马逊 DataZone 控制台，然后使用您的账户凭证登录。
2. 选择 View domains，然后选择包含要添加参数集的已启用蓝图的域。
3. 选择蓝图选项卡，然后选择 Amazon SageMaker 蓝图以打开蓝图的详细信息页面。
4. 在蓝图详细信息页面的参数集选项卡下，选择创建参数集，然后指定以下内容：
   - 为参数集提供一个名称。
   - （可选）为参数集提供描述。
   - 指定 Amazon SageMaker 域名身份验证类型。您可以选择 IAM 或 IAM 身份中心 (SSO)。
   - 指定 AWS 区域。

- 为数据加密指定 AWS KMS 密钥。您可以选择现有密钥或创建新密钥。
- 在 “环境参数” 下，指定以下内容：
  - VPC ID-您用于亚马逊 SageMaker 环境的 VPC 的 ID。您可以指定现有 VPC 或创建新 VPC。
  - 子网-您的 VPC 中特定资源的一系列 IP 地址的一个或多个 ID。
  - 网络访问-选择 “仅限 VPC” 或 “仅限公共互联网”。
  - 安全组-配置 VPC 和子网时使用的安全组。
- 在 “数据源参数” 下，选择以下选项之一：
  - AWS 仅限 Glue
  - AWS Glue + Amazon Redshift Serverless。如果选择此选项，请指定以下内容：
    - 指定保存所选 Amazon Redshift 集群凭证的 AWS 秘密 ARN。 AWS 密钥必须用`AmazonDataZoneDomain : [Domain_ID]`标签进行标记，才有资格在参数集中使用。

      如果您没有现有 AWS 密钥，也可以通过选择 “创建新密钥” 来创建新 AWS 密钥。这将打开一个对话框，您可以在其中提供密钥的名称、用户名和密码。选择 “创建新 AWS 密钥” 后，Amazon 将在 Secr AWS ets Manager 服务中 DataZone 创建一个新密钥，并确保该密钥使用您尝试创建参数集的域进行标记。
    - 指定要在创建环境时使用的 Amazon Redshift 工作组。
    - 指定要在创建环境时使用的数据库（在您选择的工作组中）的名称。
  - AWS 仅限 Glue + 亚马逊 Redshift 集群
    - 指定保存所选 Amazon Redshift 集群凭证的 AWS 秘密 ARN。 AWS 密钥必须用`AmazonDataZoneDomain : [Domain_ID]`标签进行标记，才有资格在参数集中使用。

      如果您没有现有 AWS 密钥，也可以通过选择 “创建新密钥” 来创建新 AWS 密钥。这将打开一个对话框，您可以在其中提供密钥的名称、用户名和密码。选择 “创建新 AWS 密钥” 后，Amazon 将在 Secr AWS ets Manager 服务中 DataZone 创建一个新密钥，并确保该密钥使用您尝试创建参数集的域进行标记。
    - 指定要在创建环境时使用的 Amazon Redshift 集群。
    - 指定要在创建环境时使用的数据库（在您选择的集群中）的名称。

5. 选择 “创建参数集”。

将亚马逊 SageMaker 作为可信服务添加到拥有亚马逊 DataZone 域名的 AWS 账户中

如果您启用了亚马逊 SageMaker 蓝图，则还必须将其添加 SageMaker 为亚马逊内部的可信服务之一 DataZone。为此，请完成以下步骤：

1. 通过 https://console.aws.amazon.com/datazone 导航到亚马逊 DataZone 控制台，然后使用您的账户凭证登录。
2. 选择 “查看域”，然后选择包含已启用 SageMaker 蓝图的域。
3. 选择 “可信服务”，然后选择 Amazon SageMaker，然后选择 “启用”。

在 Amazon 中 AWS 使用定制服务蓝图 DataZone

在亚马逊中 DataZone，自定义 AWS 服务蓝图允许您通过 DataZone 将亚马逊配置为使用您自己已在组织中设置的现有 AWS 身份和访问管理 (IAM) 角色和 AWS 服务，从而优化资源使用和成本。

用于创建 Amazon DataZone 环境的蓝图定义了该环境所属项目的成员在处理 Amazon DataZone 目录中的资产时可以使用哪些工具和服务。在当前版本的 Amazon 中 DataZone，有以下内置蓝图：

- 数据湖蓝图
- 数据仓库蓝图
- 亚马逊 SageMaker 蓝图

借助 Amazon DataZone 定制 AWS 服务蓝图，您可以创建针对您当前在组织中使用的任何 AWS 服务进行定制的环境和项目。借助自定义蓝图，您可以将 Amazon 纳入现有的数据管道 DataZone 中，方法是将其配置为使用现有的 IAM 角色来增强对基础设施设置的监管，并就业务计划进行协作。

主题

启用自定义 AWS 服务蓝图

完成以下步骤以在您的域中启用自定义 AWS 服务蓝图。

1. 登录 AWS 管理控制台并打开亚马逊 DataZone 管理控制台，网址为 https://console.aws.amazon.com/datazone。
2. 选择 “查看域”，然后选择要在其中启用自定义 AWS 服务蓝图的域。
3. 选择 “蓝图” 选项卡，然后从可用蓝图列表中选择AWS 服务 bluepint，然后选择 “启用”。

使用自定义 AWS 服务蓝图创建环境

完成以下过程，使用自定义 AWS 服务蓝图创建环境。

1. 登录 AWS 管理控制台并打开亚马逊 DataZone 管理控制台，网址为 https://console.aws.amazon.com/datazone。
2. 选择 “查看域”，然后选择启用自定义 AWS 服务蓝图的域。
3. 选择 “蓝图” 选项卡，然后选择已启用的AWS 服务 bluepint，然后选择 “创建环境”。
4. 在创建环境页面上，指定以下内容，然后选择创建环境：

   - 名称-指定环境的名称。
   - 描述-指定环境的描述。
   - 项目-为环境指定新的或现有的拥有项目。项目使一群用户能够发现、发布、订阅和使用 Amazon 中的资产 DataZone。该环境将可供指定项目的所有成员使用。所有环境都归其用户有权访问该环境的项目所有。
   - 环境角色-指定一个现有 IAM 角色，该角色将授予亚马逊在此环境中 DataZone 访问您的现有 AWS 服务和资源（例如 Amazon S3 和 AWS Glue）的权限。

     > **Note**
     >
     > Amazon DataZone 不会为您配置此角色。您必须拥有一个现有 IAM 角色，该角色具有您想要在此环境中启用的现有 AWS 服务和资源的权限。
     > 确保此 IAM 角色具有所需的最低权限，换句话说，将范围缩小为仅提供您要在此环境中启用的 AWS 服务和资源的访问权限。

   - AWS region-指定要在其中创建此环境的 AWS 区域。

在自定义 AWS 服务环境中创建操作

完成以下步骤以在自定义 AWS 服务环境中创建操作。通过在自定义 AWS 服务环境中创建操作，您可以将指向 Amazon DataZone 数据门户的深度链接添加到该环境中可用的分析工具。

1. 登录 AWS 管理控制台并打开亚马逊 DataZone 管理控制台，网址为 https://console.aws.amazon.com/datazone。
2. 选择 “查看域”，然后选择启用自定义 AWS 服务蓝图的域。

3. 选择 Bluep rints 选项卡，然后选择已启用的AWS 服务 bluepint，然后选择要在其中添加操作的 AWS 服务环境。
4. 在 AWS 控制台链接页面上，从 “热门链接” 或 “自定义 AWS 链接” 部分中选择 AWS 链接（操作），以启用通过 DataZone 亚马逊数据门户指向您的 Amazon S3 存储桶、Amazon Athena AWS 工作组、Glue 任务或该环境中 AWS 任何其他自定义控制台资源的深度链接。
5. 如果您使用此环境的 “摘要” 部分中的数据门户链接在数据门户中导航到此环境，则可以在分析工具部分下看到您添加的深层链接。

将项目成员添加到自定义 AWS 服务环境

完成以下步骤，将项目成员添加到 AWS 服务环境。

1. 登录 AWS 管理控制台并打开亚马逊 DataZone 管理控制台，网址为 https://console.aws.amazon.com/datazone。
2. 选择 “项目” 选项卡，然后在 AWS 服务环境中选择要向其中添加成员的项目。
3. 选择添加，然后在添加成员页面上查找并添加来自 IAM 用户、SSO 用户或 SSO 群组的成员。指定分配的项目角色为 “所有者” 或 “参与者”。完成查找和添加成员后，选择添加成员。

在 AWS 服务环境中配置数据源

完成以下步骤，在 AWS 服务环境中配置数据源。

1. 登录 AWS 管理控制台并打开亚马逊 DataZone 管理控制台，网址为 https://console.aws.amazon.com/datazone。
2. 选择蓝图选项卡，然后选择自定义 AWS 服务蓝图。
3. 在 “已创建的环境” 下，选择要在其中配置数据源的 AWS 服务环境。
4. 选择 “数据源” 选项卡，选择 “添加”，指定以下内容，然后选择 “添加”。
   - 名称-数据源名称。
   - 资源 ——选择 AWS Glue 或 Amazon Redshift。
     - 对于 AWS Glue，请指定资源数据库。
     - 对于 Amazon Redshift，选择集群或无服务器，然后指定 Redshift 凭证，包括新的或现有的 AWS 密钥、创建环境时要使用的集群或无服务器工作组、创建环境时要使用的数据库以及指定数据库中的架构。

- 权限-指定一个管理访问角色，该角色将授权亚马逊 DataZone 提取和管理对 La AWS ke Formation 中表的访问权限（适用于 G AWS lue），或者授予亚马逊采集和管理对亚马逊 DataZone Redshift 中表的访问权限的授权。
- 用于数据消费-在亚马逊中 DataZone，项目成员可以通过订阅目标 DataZone使用数据，亚马逊使用订阅目标来访问您在项目中订阅的数据。指定是否也将此数据源添加为订阅目标。

在 AWS 服务环境中配置订阅目标

完成以下步骤，在 AWS 服务环境中配置订阅目标。

1. 登录 AWS 管理控制台并打开亚马逊 DataZone 管理控制台，网址为 https://console.aws.amazon.com/datazone。
2. 选择蓝图选项卡，然后选择 AWS 服务蓝图。
3. 在 “已创建的环境” 下，选择要在其中配置订阅目标的 AWS 服务环境。
4. 选择 “订阅目标” 选项卡，选择 “添加”，指定以下内容，然后选择 “添加”。

   - 名称-订阅目标名称。
   - 资源 ——选择 AWS Glue 或 Amazon Redshift。
     - 对于 AWS Glue，请指定资源数据库。
     - 对于 Amazon Redshift，选择集群或无服务器，然后指定 Redshift 凭证，包括新的或现有的 AWS 密钥、创建环境时要使用的集群或无服务器工作组、创建环境时要使用的数据库以及指定数据库中的架构。
   - 权限-指定一个管理访问角色，该角色将授权亚马逊 DataZone 提取和管理对 La AWS ke Formation 中表的访问权限（适用于 G AWS lue），或者授予亚马逊采集和管理对亚马逊 DataZone Redshift 中表的访问权限的授权。
   - 用于数据消费-在 Amazon 中 DataZone，您可以通过允许提取元数据的数据源将数据发布到数据目录中。指定是否也将此订阅目标添加为数据源。

使用关联账户发布和使用数据

将您的 AWS 账户与您的 Amazon DataZone 域名关联后，域用户就可以发布和使用这些 AWS 账户中的数据。设置账户关联有三个步骤。

- 首先，通过请求关联将域名与所需 AWS 账户共享。如果账户与域名 AWS 账户不同，亚马逊将 DataZone 使用 AWS 资源访问管理器 (RAM)。 AWS 账户关联只能由 Amazon DataZone 域名发起。
- 其次，让账户所有者接受关联请求。
- 第三，让账户所有者启用所需的环境蓝图。通过启用蓝图，账户所有者为网域中的用户提供在其账户中创建和访问资源（例如 AWS Glue 数据库和 Amazon Redshift 集群）所需的 IAM 角色和资源配置。

主题

请求与其他 AWS 账户关联

> **Note**
>
> 通过向其他 AWS 账户发送关联请求，您就是在使用 Resource Acc AWS ess Manager (RAM) 与其他 AWS 账户共享您的域。请务必检查您输入的账户 ID 的准确性。

要在亚马逊 DataZone 控制台中请求与其他 AWS 账户关联亚马逊 DataZone 域名，您必须在该账户中扮演具有管理权限的 IAM 角色。 配置使用亚马逊 DataZone 管理控制台所需的 IAM 权限以获得申请账户关联所需的最低权限。

完成以下步骤以请求与其他 AWS 账户关联。

1. 登录 AWS 管理控制台并打开亚马逊 DataZone 管理控制台，网址为 https://console.aws.amazon.com/datazone。
2. 选择查看域名，然后从列表中选择域名。该名称是一个超链接。
3. 向下滚动到 “关联账户” 选项卡，然后选择 “请求关联”。
4. 输入您要请求关联的账户的 ID。如果您对账户 ID 列表感到满意，请选择请求关联。
5. 在 RAM 策略下，指定账户关联的 RAM 策略。您可以选择`AWSRAMPermissionDataZonePortalReadWrite`哪个账户将允许关联账户执行 Amazon DataZone API 并访问数据门户`AWSRAMPermissionDataZoneDefault`，也可以选择允许关联账户仅执行 Amazon DataZone API 而不提供数据门户访问权限。 DataZone 然后，亚马逊代表您的账户在 Resource Access Manager 中创建 AWS 资源共享，并将输入的账户 ID 作为委托人。
6. 您必须通知其他 AWS 账户的所有者接受您的请求。邀请将在七 (7) 天后过期。

提供对您的客户管理的 KMS 密钥的账户访问权限

Amazon DataZone 域及其元数据是加密的，要么是（默认情况下）使用由您持有的密钥进行加密 AWS，或者（可选）使用您在域创建期间拥有并提供的 AWS 密钥管理服务 (KMS) 中的客户管理密钥。如果您的域使用客户管理的密钥加密，请按照以下步骤向关联账户授予使用 KMS 密钥的权限。

1. 登录 AWS 管理控制台并打开 KMS 控制台，网址为 https://console.aws.amazon.com/kms/。
2. 要查看您账户中自己所创建和管理的密钥，请在导航窗格中选择 Customer managed keys (客户托管密钥)。
3. 要查看您账户中自己所创建和管理的密钥，请在导航窗格中选择 Customer managed keys (客户托管密钥)。
4. 在 KMS 密钥列表中，选择要检查的 KMS 密钥的别名或密钥 ID。
5. 要允许或禁止外部 AWS 账户使用 KMS 密钥，请使用页面其他 AWS 账户部分中的控件。这些账户中的 IAM 委托人（本身具有适当的 KMS 权限）可以在加密操作中使用 KMS 密钥，例如加密、解密、重新加密和生成数据密钥。

接受来自 Amazon DataZone 域的账户关联请求并启用环境蓝图

要在亚马逊 DataZone 管理控制台中接受与亚马逊 DataZone 域的关联，您必须在账户中扮演具有管理权限的 IAM 角色。 配置使用亚马逊 DataZone 管理控制台所需的 IAM 权限以获得最低权限。

完成以下操作以接受与 Amazon DataZone 域名的关联。

1. 登录 AWS 管理控制台并打开亚马逊 DataZone 管理控制台，网址为 https://console.aws.amazon.com/datazone。
2. 选择 “查看请求”，然后从列表中选择邀请域。邀请状态应为 “已请求”。选择 “查看请求”。
3. 选择是否启用默认数据湖和/或数据仓库环境蓝图，方法是选择两者都选中或其中一个复选框。你可以稍后再做。
   - 数据湖环境蓝图使域用户能够创建和管理 AWS Glue、Amazon S3 和 Amazon Athena 资源，以便从数据湖发布和使用。
   - 数据仓库环境蓝图使域用户能够创建和管理 Amazon Redshift 资源，以便从数据仓库中发布和使用。
4. 如果您选择选择一个或两个默认环境蓝图，请配置以下权限和资源。
   - 管理访问权限 IAM 角色向亚马逊提供权限，使域用户 DataZone能够提取和管理对表（例如 G AWS lue 和 Amazon Redshift）的访问权限。您可以选择让 Amazon DataZone 创建和使用新的 IAM 角色，也可以从现有 IAM 角色列表中进行选择。
   - 配置 IAM 角色向 A mazon 提供权限 DataZone，使域用户能够创建和配置环境资源，例如 AWS Glue 数据库。您可以选择让 Amazon DataZone 创建和使用新的 IAM 角色，也可以从现有 IAM 角色列表中进行选择。
   - 用于数据湖的 Amazon S3 存储桶是域用户存储数据湖数据时亚马逊 DataZone 将使用的存储桶或路径。您可以使用亚马逊选择的默认存储桶， DataZone 也可以通过输入其路径字符串来选择自己的现有 Amazon S3 路径。如果您选择自己的 Amazon S3 路径，则需要更新 IAM 策略以向亚马逊 DataZone 提供使用该路径的权限。
5. 如果您对配置感到满意，请选择接受并配置关联。

拒绝来自亚马逊 DataZone 域名的账户关联请求

要在亚马逊 DataZone 管理控制台中拒绝来自亚马逊 DataZone域的关联请求，您必须在该账户中扮演具有管理权限的 IAM 角色。 配置使用亚马逊 DataZone 管理控制台所需的 IAM 权限以获得最低权限。

完成以下操作，拒绝来自亚马逊 DataZone 域的关联请求。

1. 登录 AWS 管理控制台并打开亚马逊 DataZone 管理控制台，网址为 https://console.aws.amazon.com/datazone。
2. 选择 “查看请求”，然后从列表中选择邀请域。邀请状态应为 “已请求”。选择 “拒绝关联”。选择 “拒绝关联”，确认您的选择。

在关联 AWS 账户中启用环境蓝图

要在 Amazon DataZone 管理控制台中启用环境蓝图，您必须在账户中扮演具有管理权限的 IAM 角色。 配置使用亚马逊 DataZone 管理控制台所需的 IAM 权限以获得最低权限。

完成以下操作以在关联域中启用蓝图。

1. 登录 AWS 管理控制台并打开亚马逊 DataZone 管理控制台，网址为 https://console.aws.amazon.com/datazone。
2. 打开左侧导航面板并选择关联域名。
3. 选择要为其启用环境蓝图的域。
4. 从蓝图列表中，选择DefaultDataLake或DefaultDataWarehouse SageMaker、Amazon 或定制 AWS 服务蓝图。

   > **Note**
   >
   > 如果要启用自定义 AWS 服务蓝图，则无需指定管理访问角色。自定义 AWS 服务 bluerpint 的权限和授权机制是在您使用此蓝图创建环境时处理的。有关更多信息，请参阅使用自定义 AWS 服务蓝图创建环境。

5. 在所选蓝图的详细信息页面上，选择在此账户中启用。
6. 在 “权限和资源” 页面上，指定以下内容：

   - 如果您要启用DefaultDataLake蓝图，请为 Glue 管理访问权限角色指定一个新的或现有的服务角色，该角色 DataZone 授予亚马逊收录和管理对 G AWS lue 和 La AWS ke Formation 中表的访问权限的授权。
   - 如果您要启用DefaultDataWarehouse蓝图，请为 Redshift 管理访问权限角色指定一个新的或现有的服务角色，该角色 DataZone 授权亚马逊获取和管理对 Amazon Redshift 中的数据共享、表和视图的访问权限。
   - 如果您要启用亚马逊 SageMaker蓝图，请为SageMaker 管理访问角色指定一个新的或现有的服务角色，以授予亚马逊向目录发布亚马逊 SageMaker 数据的 DataZone 权限。它还授予亚马逊授予访问 DataZone 权限或撤销对亚马逊在目录中 SageMaker 发布的资产的访问权限的权限。

> **Important**
>
> 在您启用亚马逊 SageMaker蓝图时，亚马逊 DataZone 会检查当前账户和地区中是否 DataZone 存在以下 Amazon 的 IAM 角色。如果这些角色不存在，Amazon DataZone 会自动创建它们。
>
> - AmazonDataZoneGlueAccess-<region>-<domainId>
> - AmazonDataZoneRedshiftAccess-<region>-<domainId>

- 对于配置角色，请指定一个新的或现有的服务角色，该角色 DataZone 授予 Amazon 在环境账户和区域 AWS CloudFormation 中使用创建和配置环境资源的授权。
- 如果您要为 SageMaker-Glu e 数据源的 Amazon S3 存储桶启用亚马逊 SageMaker蓝图，请指定 AWS 账户中所有 SageMaker 环境都要使用的 Amazon S3 存储桶。您指定的存储桶前缀必须是以下之一：
  - 亚马逊数据区*
  - datazone-sagemaker*
  - sagemaker-datazone*
  - DataZone-Sagemaker*
  - Sagemaker-* DataZone
  - DataZone-SageMaker*
  - SageMaker-DataZone*

7. 选择启用蓝图。

启用所选蓝图后，您可以控制哪些项目可以使用您账户中的蓝图来创建环境配置文件。您可以通过将管理项目分配给蓝图的配置来实现此目的。

指定在已启用 DefaultDataLake 或 DefaultDataWarehouse 蓝图上管理项目

1. 通过 https://console.aws.amazon.com/datazone 导航到亚马逊 DataZone 控制台，然后使用您的账户凭证登录。
2. 打开左侧导航面板并选择 “关联域”，然后选择要在其中添加管理项目的域。
3. 选择蓝图选项卡，然后选择 DefaultDataLake 或 DefaultDataWareshouse 蓝图。
4. 默认情况下，域内的所有项目都可以使用账户中的 DefaultDataLake 或 DefaultDataWareshouse 蓝图来创建环境配置文件。但是，您可以通过将管理项目分配给蓝图来限制这一点。要添加管理项

目，请选择选择管理项目，然后从下拉菜单中选择要添加为管理项目的项目，然后选择选择管理项目。

在 AWS 账户中启用 DefaultDataWarehouse 蓝图后，您可以向蓝图配置中添加参数集。参数集是一组键和值，是亚马逊 DataZone 与您的 Amazon Redshift 集群建立连接所必需的，用于创建数据仓库环境。这些参数包括您的 Amazon Redshift 集群的名称、数据库以及保存集群凭证的 AWS 密钥。

向 DefaultDataWarehouse蓝图添加参数集

1. 通过 https://console.aws.amazon.com/datazone 导航到亚马逊 DataZone 控制台，然后使用您的账户凭证登录。
2. 打开左侧导航面板并选择 “关联域”，然后选择要在其中添加参数集的域。
3. 选择蓝图选项卡，然后选择 DefaultDataWareshouse 蓝图以打开蓝图详细信息页面。
4. 在蓝图详细信息页面的参数集选项卡下，选择创建参数集。
   - 为参数集提供一个名称。
   - （可选）提供参数集的描述。
   - 选择一个区域
   - 选择 Amazon Redshift 集群或亚马逊 Redshift Serverless。
   - 选择保存所选 Amazon Redshift 集群或 Amazon Redshift 无服务器工作组凭证的 AWS 秘密 ARN。 AWS 密钥必须用`AmazonDataZoneDomain : [Domain_ID]`标签进行标记，才有资格在参数集中使用。
     - 如果您没有现有 AWS 密钥，也可以通过选择 “创建新密钥” 来创建新 AWS 密钥。这将打开一个对话框，您可以在其中提供密钥的名称、用户名和密码。选择 “创建新 AWS 密钥” 后，Amazon 将在 Secr AWS ets Manager 服务中 DataZone 创建一个新密钥，并确保该密钥使用您尝试创建参数集的域进行标记。
   - 选择 Amazon Redshift 集群或亚马逊 Redshift 无服务器工作组。
   - 输入所选 Amazon Redshift 集群或 Amazon Redshift Serverless 工作组中的数据库名称。
   - 选择 “创建参数集”。

在您的 AWS 账户中启用 Amazon SageMaker 蓝图后，您可以向蓝图配置中添加参数集。参数集是一组键和值，是亚马逊与您的亚马逊 DataZone SageMaker 建立连接所必需的，用于创建 sagemaker 环境。

向 Amazon SageMaker 蓝图添加参数集

1. 通过 https://console.aws.amazon.com/datazone 导航到亚马逊 DataZone 控制台，然后使用您的账户凭证登录。
2. 选择 View domains，然后选择包含要添加参数集的已启用蓝图的域。
3. 选择蓝图选项卡，然后选择 Amazon SageMaker 蓝图以打开蓝图的详细信息页面。
4. 在蓝图详细信息页面的参数集选项卡下，选择创建参数集，然后指定以下内容：
   - 为参数集提供一个名称。
   - （可选）为参数集提供描述。
   - 指定 Amazon SageMaker 域名身份验证类型。您可以选择 IAM 或 IAM 身份中心 (SSO)。
   - 指定 AWS 区域。
   - 为数据加密指定 AWS KMS 密钥。您可以选择现有密钥或创建新密钥。
   - 在 “环境参数” 下，指定以下内容：
     - VPC ID-您用于亚马逊 SageMaker环境的 VPC 的 ID。您可以指定现有 VPC 或创建新 VPC。
     - 子网-您的 VPC 中特定资源的一系列 IP 地址的一个或多个 ID。
     - 网络访问-选择 “仅限 VPC” 或 “仅限公共互联网”。
     - 安全组-配置 VPC 和子网时使用的安全组。
   - 在 “数据源参数” 下，选择以下选项之一：
     - AWS 仅限 Glue
     - AWS Glue + Amazon Redshift Serverless。如果选择此选项，请指定以下内容：
       - 指定保存所选 Amazon Redshift 集群凭证的 AWS 秘密 ARN。 AWS 密钥必须用`AmazonDataZoneDomain : [Domain_ID]`标签进行标记，才有资格在参数集中使用。

         如果您没有现有 AWS 密钥，也可以通过选择 “创建新密钥” 来创建新 AWS 密钥。这将打开一个对话框，您可以在其中提供密钥的名称、用户名和密码。选择 “创建新 AWS 密钥” 后，Amazon 将在 Secr AWS ets Manager 服务中 DataZone 创建一个新密钥，并确保该密钥使用您尝试创建参数集的域进行标记。
       - 指定要在创建环境时使用的 Amazon Redshift 工作组。
       - 指定要在创建环境时使用的数据库（在您选择的工作组中）的名称。
     - AWS 仅限 Glue + 亚马逊 Redshift 集群

- 指定保存所选 Amazon Redshift 集群凭证的 AWS 秘密 ARN。 AWS 密钥必须用`AmazonDataZoneDomain : [Domain_ID]`标签进行标记，才有资格在参数集中使用。

  如果您没有现有 AWS 密钥，也可以通过选择 “创建新密钥” 来创建新 AWS 密钥。这将打开一个对话框，您可以在其中提供密钥的名称、用户名和密码。选择 “创建新 AWS 密钥” 后，Amazon 将在 Secr AWS ets Manager 服务中 DataZone 创建一个新密钥，并确保该密钥使用您尝试创建参数集的域进行标记。
- 指定要在创建环境时使用的 Amazon Redshift 集群。
- 指定要在创建环境时使用的数据库（在您选择的集群中）的名称。

5. 选择 “创建参数集”。

在关联 AWS 账户中 SageMaker 将 Amazon 添加为可信服务

如果您启用了亚马逊 SageMaker 蓝图，则还必须将其添加 SageMaker 为亚马逊内部的可信服务之一 DataZone。为此，请完成以下步骤：

1. 通过 https://console.aws.amazon.com/datazone 导航到亚马逊 DataZone 控制台，然后使用您的账户凭证登录。
2. 选择查看域，然后选择包含已启用 SageMaker 蓝图的域。
3. 选择 “可信服务”，然后选择 Amazon SageMaker，然后选择 “启用”。

移除关联账户

要在 Amazon DataZone 管理控制台中删除关联 AWS 账户，您必须在该账户中扮演具有管理权限的 IAM 角色。 配置使用亚马逊 DataZone 管理控制台所需的 IAM 权限以获得最低权限。

完成以下步骤，从您的域中移除关联账户。

1. 登录 AWS 管理控制台并打开亚马逊 DataZone 管理控制台，网址为 https://console.aws.amazon.com/datazone。
2. 选择 “查看域名”，然后从列表中选择域名。该名称是一个超链接。
3. 向下滚动到 “关联账户” 选项卡。为要删除的 AWS 账户选择账户 ID。
4. 选择取消关联。在字段中输入 “取消关联”，然后选择 “取消关联”，确认您的选择。
5. 该账户现已从您的网域中移除，该域的用户无法使用该账户来发布和使用数据。

使用 Amazon DataZone 数据目录

您可以使用 Amazon B DataZone usiness 数据目录根据业务背景对整个组织的数据进行分类，从而使组织中的每个人都能快速查找和理解数据。有关更多信息，请参阅 Amazon DataZone 术语和概念。

主题

创建、编辑或删除业务词汇表

在亚马逊中 DataZone，业务词汇表是可能与资产（数据）相关的商业术语（单词）的集合。它为业务用户提供了相应的词汇表，其中包含业务术语及其定义的列表，以确保在分析数据时，整个组织使用相同的定义。业务词汇表是在目录域中创建的，可以应用于资产和列，以帮助理解该资产或列的关键特征。可以应用一个或多个词汇表术语。业务词汇表可以是术语的平面列表，其中业务词汇表中的任何术语都可以与其他术语的子列表相关联。有关更多信息，请参阅 Amazon DataZone 术语和概念。要在您的 Amazon DataZone 域中创建、编辑或删除词汇表，您必须是拥有该域名的相应权限的拥有项目的成员。

要创建词汇表，请完成以下步骤：

1. 使用 DataZone 数据门户 URL 导航至 Amazon 数据门户，然后使用您的 SSO 或 AWS 凭证登录。如果您是亚马逊 DataZone 管理员，则可以通过使用创建亚马逊 DataZone 域名的 AWS 账户访问亚马逊 DataZone 控制台 https://console.aws.amazon.com/datazone 来获取数据门户网址。
2. 导航到顶部导航栏中 “搜索” 旁边的 “目录” 菜单。
3. 在 Amazon DataZone 数据门户中，选择 “词汇表”，然后选择 “创建词汇表”。
4. 为词汇表指定名称、描述和所有者，然后选择 “创建词汇表”。
5. 通过选择 “启用” 开关来启用新的词汇表。
6. 在词汇表的详细信息页面上，您可以选择 “创建自述文件” 来添加有关此词汇表的其他信息。

要禁用或启用业务词汇表，请完成以下步骤：

1. 使用 DataZone 数据门户 URL 导航至 Amazon 数据门户，然后使用您的 SSO 或 AWS 凭证登录。如果您是亚马逊 DataZone 管理员，则可以通过使用创建亚马逊 DataZone 域名的 AWS 账户访问亚马逊 DataZone 控制台 https://console.aws.amazon.com/datazone 来获取数据门户网址。
2. 导航到顶部导航栏中 “搜索” 旁边的 “目录” 菜单。
3. 在 Amazon DataZone 数据门户中，选择术语表，然后找到要禁用/启用的业务词汇表。
4. 在词汇表详情页面上，找到 “启用/禁用” 开关，然后使用它来启用或禁用所选词汇表。

> **Note**
>
> 禁用词汇表也会禁用其中包含的所有术语。

要编辑业务词汇表，请完成以下步骤：

1. 使用 DataZone 数据门户 URL 导航至 Amazon 数据门户，然后使用您的 SSO 或 AWS 凭证登录。如果您是亚马逊 DataZone 管理员，则可以通过使用创建亚马逊 DataZone 域名的 AWS 账户访问亚马逊 DataZone 控制台 https://console.aws.amazon.com/datazone 来获取数据门户网址。
2. 导航到顶部导航栏中 “搜索” 旁边的 “目录” 菜单。
3. 在 Amazon DataZone 数据门户中，选择 “术语表”，然后找到要编辑的业务词汇表。
4. 在词汇表详细信息页面上，展开操作，然后选择编辑以编辑词汇表。
5. 更新名称和描述，然后选择 “保存”。

要删除业务词汇表，请完成以下步骤：

1. 使用 DataZone 数据门户 URL 导航至 Amazon 数据门户，然后使用您的 SSO 或 AWS 凭证登录。如果您是亚马逊 DataZone 管理员，则可以通过使用创建亚马逊 DataZone 域名的 AWS 账户访问亚马逊 DataZone 控制台 https://console.aws.amazon.com/datazone 来获取数据门户网址。
2. 导航到顶部导航栏中 “搜索” 旁边的 “目录” 菜单。
3. 在 Amazon DataZone 数据门户中，选择 “术语表”，然后找到要删除的业务词汇表。
4. 在词汇表详细信息页面上，展开操作，然后选择删除以删除词汇表。

> **Note**
>
> 必须先删除词汇表中的所有现有术语，然后才能删除词汇表。

5. 选择 “删除”，确认删除词汇表。

创建、编辑或删除词汇表中的术语

在亚马逊中 DataZone，业务词汇表是可能与资产（数据）相关的商业术语的集合。有关更多信息，请参阅 Amazon DataZone 术语和概念。要创建、编辑或删除您的 Amazon DataZone 域名词汇表中的术语，您必须是拥有该域名的相应权限的拥有项目的成员。

在 Amazon 中 DataZone，商业词汇表术语可以有近似的描述。要设置特定术语的上下文，可以指定术语之间的关系。当您为术语定义关系时，它会自动添加到相关术语的定义中。Amazon 中提供的词汇表术语关系 DataZone 包括以下内容：

- 类型为-表示当前术语是已识别术语的一种类型。表示已识别的术语是当前术语的父项。
- Has Types-表示当前术语是指明的一个或多个特定术语的通用术语。这种关系可以表示通用术语的子项。

要创建新学期，请完成以下步骤：

1. 使用 DataZone 数据门户 URL 导航至 Amazon 数据门户，然后使用您的 SSO 或 AWS 凭证登录。如果您是亚马逊 DataZone 管理员，则可以通过使用创建亚马逊 DataZone 域名的 AWS 账户访问亚马逊 DataZone 控制台 https://console.aws.amazon.com/datazone 来获取数据门户网址。
2. 导航到顶部导航栏中 “搜索” 旁边的 “目录” 菜单。
3. 在 Amazon DataZone 数据门户中，选择 “词汇表”，然后选择要在其中创建新术语的词汇表。
4. 为术语指定名称、描述和所有者，然后选择创建术语。
5. 通过选择 “启用” 开关启用新学期。
6. 要添加自述文件，请导航到术语详细信息页面，然后您可以选择 “创建自述文件” 来添加有关此词汇表的其他信息。
7. 要添加关系，请导航至术语详细信息页面，选择 “术语关系” 部分，然后选择 “添加词汇表术语”。在对话框中，选择要关联的关系和术语，然后选择 “关闭”，将术语添加到相应的关系类型中。这种关系还会添加到您创建的所有相关术语中。

要编辑词汇表中的术语，请完成以下步骤：

1. 使用 DataZone 数据门户 URL 导航至 Amazon 数据门户，然后使用您的 SSO 或 AWS 凭证登录。如果您是亚马逊 DataZone 管理员，则可以通过使用创建亚马逊 DataZone 域名的 AWS 账户访问亚马逊 DataZone 控制台 https://console.aws.amazon.com/datazone 来获取数据门户网址。

2. 导航到顶部导航栏中 “搜索” 旁边的 “目录” 菜单。
3. 在 Amazon DataZone 数据门户中，选择 “词汇表”，找到包含您要编辑的术语的词汇表，然后选择该术语。
4. 在学期详细信息页面上，展开 “操作”，然后选择 “编辑” 以编辑该术语。
5. 更新名称和描述，然后选择 “保存”。

要删除词汇表中的术语，请完成以下步骤：

1. 使用 DataZone 数据门户 URL 导航至 Amazon 数据门户，然后使用您的 SSO 或 AWS 凭证登录。如果您是亚马逊 DataZone 管理员，则可以通过使用创建亚马逊 DataZone 域名的 AWS 账户访问亚马逊 DataZone 控制台 https://console.aws.amazon.com/datazone 来获取数据门户网址。
2. 导航到顶部导航栏中 “搜索” 旁边的 “目录” 菜单。
3. 在亚马逊 DataZone 数据门户中，选择词汇表，找到包含您要删除的术语的词汇表，然后选择该术语。
4. 在词汇表详细信息页面上，展开操作，然后选择删除以删除该术语。
5. 选择 “删除”，确认删除该术语。

创建、编辑或删除元数据表单

在 Amazon 中 DataZone，元数据表单是一种简单的表单，用于为目录中的资产元数据补充额外的业务背景。它为数据所有者提供了一种可扩展的机制，通过信息来丰富资产，这些信息可以在数据用户搜索和查找数据时为他们提供帮助。元数据表单还可以作为一种机制，确保发布到 Amazon DataZone 目录的所有资产保持一致。

元数据表单定义由一个或多个字段定义组成，支持布尔值、日期、十进制、整数、字符串和业务词汇表字段值数据类型。有关更多信息，请参阅 Amazon DataZone 术语和概念。要在您的 Amazon DataZone 域中创建、编辑或删除元数据表单，您必须是拥有相应证书的拥有项目的成员。

要创建元数据表单，请完成以下步骤：

1. 使用 DataZone 数据门户 URL 导航至 Amazon 数据门户，然后使用您的 SSO 或 AWS 凭证登录。如果您是亚马逊 DataZone 管理员，则可以通过使用创建亚马逊 DataZone 域名的 AWS 账户访问亚马逊 DataZone 控制台 https://console.aws.amazon.com/datazone 来获取数据门户网址。
2. 导航到顶部导航栏中 “搜索” 旁边的 “目录” 菜单。
3. 在 Amazon DataZone 数据门户中，选择元数据表单，然后选择创建表单。

4. 指定元数据表单的名称、描述、所有者，然后选择创建表单。

要编辑元数据表单，请完成以下步骤：

1. 使用 DataZone 数据门户 URL 导航至 Amazon 数据门户，然后使用您的 SSO 或 AWS 凭证登录。如果您是亚马逊 DataZone 管理员，则可以通过使用创建亚马逊 DataZone 域名的 AWS 账户访问亚马逊 DataZone 控制台 https://console.aws.amazon.com/datazone 来获取数据门户网址。
2. 导航到顶部导航栏中 “搜索” 旁边的 “目录” 菜单。
3. 在 Amazon DataZone 数据门户中，选择元数据表单，然后找到要编辑的元数据表单。
4. 在元数据表单的详细信息页面上，展开操作，然后选择编辑。
5. 更新姓名、描述、所有者字段，然后选择更新表单。

要删除元数据表单，请完成以下步骤：

> **Note**
>
> 在删除元数据表单之前，必须将其从应用该表单的所有资产类型或资源中移除。

1. 使用 DataZone 数据门户 URL 导航至 Amazon 数据门户，然后使用您的 SSO 或 AWS 凭证登录。如果您是亚马逊 DataZone 管理员，则可以通过使用创建亚马逊 DataZone 域名的 AWS 账户访问亚马逊 DataZone 控制台 https://console.aws.amazon.com/datazone 来获取数据门户网址。
2. 导航到顶部导航栏中 “搜索” 旁边的 “目录” 菜单。
3. 在 Amazon DataZone 数据门户中，选择元数据表单，然后找到要删除的元数据表单。
4. 如果您要删除的元数据表单已启用，请通过选择 “启用” 开关来禁用该元数据表单。
5. 在元数据表单的详细信息页面上，展开操作，然后选择删除。
6. 选择 “删除” 以确认删除。

创建、编辑或删除元数据表单中的字段

在 Amazon 中 DataZone，元数据表单是一种简单的表单，用于为目录中的资产元数据补充额外的业务背景。它为数据所有者提供了一种可扩展的机制，通过信息来丰富资产，这些信息可以在数据用户搜索和查找数据时为他们提供帮助。元数据表单还可以作为一种机制，确保发布到 Amazon DataZone 目录的所有资产保持一致。

元数据表单定义由一个或多个字段定义组成，支持布尔值、日期、十进制、整数、字符串和业务词汇表字段值数据类型。有关更多信息，请参阅 Amazon DataZone 术语和概念。要在您的 Amazon DataZone 域中创建、编辑或删除元数据表单中的字段，您必须是拥有相应证书的拥有项目的成员。

要在元数据表单中创建字段，请完成以下步骤：

1. 使用 DataZone 数据门户 URL 导航至 Amazon 数据门户，然后使用您的 SSO 或 AWS 凭证登录。如果您是亚马逊 DataZone 管理员，则可以通过使用创建亚马逊 DataZone 域名的 AWS 账户访问亚马逊 DataZone 控制台 https://console.aws.amazon.com/datazone 来获取数据门户网址。
2. 导航到顶部导航栏中 “搜索” 旁边的 “目录” 菜单。
3. 在 Amazon DataZone 数据门户中，选择元数据表单，然后选择要在其中创建字段的元数据表单。
4. 在表单的详细信息页面上，选择创建字段。
5. 指定字段名称、描述、类型以及是否为必填字段，然后选择创建字段。

要编辑元数据表单中的字段，请完成以下步骤：

1. 使用 DataZone 数据门户 URL 导航至 Amazon 数据门户，然后使用您的 SSO 或 AWS 凭证登录。如果您是亚马逊 DataZone 管理员，则可以通过使用创建亚马逊 DataZone 域名的 AWS 账户访问亚马逊 DataZone 控制台 https://console.aws.amazon.com/datazone 来获取数据门户网址。
2. 导航到顶部导航栏中 “搜索” 旁边的 “目录” 菜单。
3. 在 Amazon DataZone 数据门户中，选择元数据表单，然后选择要在其中编辑字段的元数据表单。
4. 在表单的详细信息页面上，选择要编辑的字段，然后展开 “操作”，然后选择 “编辑”。
5. 更新字段名称、描述、类型以及此字段是否为必填字段，然后选择更新字段。

要删除元数据表单中的字段，请完成以下步骤：

1. 使用 DataZone 数据门户 URL 导航至 Amazon 数据门户，然后使用您的 SSO 或 AWS 凭证登录。如果您是亚马逊 DataZone 管理员，则可以通过使用创建亚马逊 DataZone 域名的 AWS 账户访问亚马逊 DataZone 控制台 https://console.aws.amazon.com/datazone 来获取数据门户网址。
2. 导航到顶部导航栏中 “搜索” 旁边的 “目录” 菜单。
3. 在 Amazon DataZone 数据门户中，选择元数据表单，然后选择要删除字段的元数据表单。
4. 在表单的详细信息页面上，选择要删除的字段，然后展开 “操作”，然后选择 “删除”。
5. 选择 “删除” 以确认删除。

在 Amazon 中处理项目和环境 DataZone

在亚马逊中 DataZone，项目使一组用户能够就各种业务用例进行协作，这些用例涉及发布、发现、订阅和使用亚马逊 DataZone 目录中的数据资产。每个 Amazon DataZone 项目都应用了一组访问控制，因此只有获得授权的个人、团体和角色才能访问该项目和该项目订阅的数据资产，并且只能使用由项目权限定义的工具。项目充当身份主体，接收对底层资源的访问授权，从而使 Amazon DataZone 能够在组织的基础设施内运营，而无需依赖个人用户的证书。有关更多信息，请参阅 Amazon DataZone 术语和概念。

主题

创建环境配置文件

在 Amazon 中 DataZone，环境配置文件是您可以用来创建环境的模板。环境配置文件的目的是通过在配置文件中嵌入放置信息（例如 AWS 账户和区域）来简化环境创建。有关更多信息，请参阅 Amazon DataZone 术语和概念。要在亚马逊 DataZone域中创建环境配置文件，您必须属于亚马逊 DataZone 项目。所有环境配置文件均归项目所有，任何项目的所有授权用户均可使用这些配置文件来创建新环境。

创建环境配置文件

1. 使用 DataZone 数据门户 URL 导航至 Amazon 数据门户，然后使用您的 SSO 或 AWS 凭证登录。如果您是亚马逊 DataZone 管理员，则可以通过使用创建亚马逊 DataZone 域名的 AWS 账户访问亚马逊 DataZone 控制台 https://console.aws.amazon.com/datazone 来获取数据门户网址。
2. 在数据门户中，选择浏览项目，然后选择要在其中创建环境配置文件的项目。
3. 导航到项目内的 “环境” 选项卡，然后选择 “创建环境配置文件”。
4. 配置以下字段：

   - 名称-您的环境配置文件的名称。
   - 描述-（可选）对您的环境配置文件的描述。
   - 所有者项目-默认情况下，在此字段中选择要创建配置文件的项目。
   - 蓝图-为其创建此配置文件的蓝图。您可以选择一个默认的 Amazon DataZone 蓝图（数据湖或数据仓库）。

     如果您指定了数据仓库蓝图，请执行以下操作：

     - 提供参数集。要选择现有参数集，请选择 “选择参数集” 选项。如果要输入自己的参数，请选择 “输入我自己的参数”。
     - 如果您选择选择现有参数，请执行以下操作：
       - 从下拉列表中选择一个 AWS 账户。
       - 从下拉列表中选择一个参数集。
     - 如果您选择输入自己的参数，请执行以下操作：
       - 通过从下拉列表中选择 “ AWS 账户和区域” 来提供 AWS 参数。
       - 提供 Redshift 数据仓库参数：
         - 选择亚马逊 Redshift 集群或亚马逊 Redshift Serverless
         - 输入保存所选 Amazon Redshift 集群或 Amazon Redshift Serverless 工作组凭证的 AWS 秘密 ARN。必须使用在其中创建环境配置文件的域 ID 和项目 ID 来标记 AWS 密钥。
           - `AmazonDataZoneDomain: [Domain_ID]`
           - `AmazonDataZoneProject: [Project_ID]`
         - 输入 Amazon Redshift 集群或亚马逊 Redshift Serverless 工作组的名称。
         - 输入所选 Amazon Redshift 集群或 Amazon Redshift Serverless 工作组中的数据库名称。

- 在 “已授权的项目” 部分中，指定可以使用环境配置文件创建环境的项目。默认情况下，域内的所有项目都可以使用账户中的环境配置文件来创建环境。要保留此默认设置，请选择 “所有项目”。但是，您可以通过将已授权的项目分配给环境来限制这一点。为此，请选择 “仅限授权项目”，然后指定可以使用此项目配置文件创建环境的项目。
- 在 “发布” 部分中，选择以下选项之一：
  - 从任何架构发布：如果选择此选项，则使用此环境配置文件创建的环境可用于从上面提供的 Redshift 参数中选择的数据库中的任何架构进行发布。使用此环境配置文件创建的环境的用户也可以提供自己的 Amazon Redshift 参数，以便从环境配置文件中选择的 AWS 账户和区域内的任何架构进行发布。
  - 仅从默认环境架构发布：如果您选择此选项，则使用此选项创建的环境只能用于从 Amazon DataZone 为该环境创建的默认架构进行发布。使用此环境配置文件创建的环境的用户无法提供他们自己的 Amazon Redshift 参数。
  - 不允许发布：如果选择此选项，则使用此环境配置文件创建的环境只能用于订阅和使用数据。环境根本不能用于发布任何数据。

如果您指定了数据湖蓝图，请执行以下操作：

- 在AWS 账户参数部分，指定 AWS 账号和将在其中创建潜在环境的 AWS 账户区域。
- 在 “已授权项目” 部分中，指定哪些项目可以使用环境配置文件和内置 Data Lake 环境配置文件来创建环境。默认情况下，域内的所有项目都可以使用账户中的数据湖蓝图来创建环境配置文件。要保留此默认设置，请选择 “所有项目”。但是，您可以通过将项目分配给蓝图来限制这一点。为此，请选择 “仅限授权项目”，然后指定可以使用此项目配置文件创建环境的项目。
- 在 “数据库” 部分中，选择 “任何数据库” 以允许从创建环境的 AWS 帐户和区域内的任何数据库进行发布，或者选择 “仅默认数据库” 以仅允许从使用该环境创建的默认发布数据库进行发布。

5. 选择 “创建环境配置文件”。

编辑环境配置文件

在 Amazon 中 DataZone，环境配置文件是您可以用来创建环境的模板。有关更多信息，请参阅 Amazon DataZone 术语和概念。要编辑亚马逊 DataZone 域中的现有环境配置文件，您必须属于亚马逊 DataZone 项目。

编辑环境配置文件

1. 导航至 Amazon DataZone 数据门户 URL，然后使用单点登录 (SSO) 或凭证登录 AWS 。如果您是亚马逊 DataZone 管理员，则可以通过 https://console.aws.amazon.com/datazone 导航到亚马逊 DataZone 控制台，使用域名创建 AWS 账户 地登录，然后选择打开数据门户。
2. 在数据门户中，选择浏览项目，然后选择要在其中编辑环境配置文件的项目。
3. 导航到项目中的环境选项卡，然后选择环境配置文件，然后选择要编辑的环境配置文件。

   如果您正在编辑 Data Warehouse 环境配置文件，则只能编辑现有环境配置文件的名称和描述。

   如果您正在编辑 Data Lake 环境配置文件，则可以编辑配置文件的名称和描述，也可以编辑有权使用此配置文件创建环境的项目，也可以编辑数据库。要编辑这些设置，请执行以下操作：

   - 在“已授权项目”部分中，指定哪些项目可以使用环境配置文件和内置 Data Lake 环境配置文件来创建环境。默认情况下，域内的所有项目都可以使用账户中的数据湖蓝图来创建环境配置文件。要保留此默认设置，请选择“所有项目”。但是，您可以通过将项目分配给蓝图来限制这一点。为此，请选择“仅限授权项目”，然后指定可以使用此项目配置文件创建环境的项目。
   - 在“数据库”部分中，选择“任何数据库”以允许从创建环境的 AWS 帐户和区域内的任何数据库进行发布，或者选择“仅默认数据库”以仅允许从使用该环境创建的默认发布数据库进行发布。

   完成编辑后，选择编辑环境配置文件。

删除环境配置文件

在 Amazon 中 DataZone，环境配置文件是您可以用来创建环境的模板。环境配置文件的目的是通过在配置文件中嵌入放置信息（例如 AWS 账户和区域）来简化环境创建。有关更多信息，请参阅 Amazon DataZone 术语和概念。要删除亚马逊 DataZone域中的环境配置文件，您必须属于亚马逊 DataZone 项目。

> **Note**
>
> 删除环境配置文件后，您将无法再使用此配置文件创建任何环境。

删除环境配置文件

1. 导航至 Amazon DataZone 数据门户 URL，然后使用单点登录 (SSO) 或凭证登录 AWS 。如果您是亚马逊 DataZone 管理员，则可以通过 https://console.aws.amazon.com/datazone 导航到亚马逊 DataZone 控制台，使用域名创建 AWS 账户 地登录，然后选择打开数据门户。
2. 在数据门户中，选择浏览项目，然后选择要删除环境配置文件的项目。
3. 导航到项目中的环境选项卡，然后选择环境配置文件，然后选择要删除的环境配置文件。
4. 选择要删除的环境配置文件，然后选择操作、删除并确认删除。

创建新环境

在 Amazon DataZone 项目中，环境是已配置资源的集合（例如，Amazon S3 存储桶、 AWS Glue 数据库或 Amazon Athena 工作组），具有一组给定的 IAM 委托人（环境用户角色），分配了可以对这些资源进行操作的所有者或贡献者权限。有关更多信息，请参阅 Amazon DataZone 术语和概念。

任何具有访问数据门户所需权限的亚马逊 DataZone 用户都可以在项目中创建亚马逊 DataZone 环境。

要创建新环境，请完成以下步骤。

1. 导航至 Amazon DataZone 数据门户 URL，然后使用单点登录 (SSO) 或凭证登录 AWS 。如果您是亚马逊 DataZone 管理员，则可以通过 https://console.aws.amazon.com/datazone 导航到亚马逊 DataZone 控制台，使用域名创建 AWS 账户 地登录，然后选择打开数据门户。
2. 选择 “浏览所有项目”，然后选择要在其中创建新环境的项目。
3. 选择创建环境，为以下字段指定值，然后选择创建环境：

   - 名称-环境名称
   - 描述-对环境的描述
   - 环境配置文件-选择现有的环境配置文件或创建新的环境配置文件。环境配置文件是可用于创建环境的模板。有关更多信息，请参阅 Amazon DataZone 术语和概念。

     选择环境配置文件后，在 “参数” 部分下，为该环境配置文件中的字段指定值。

编辑环境

在 Amazon DataZone 项目中，环境是已配置资源的集合（例如，Amazon S3 存储桶、 AWS Glue 数据库或 Amazon Athena 工作组），其中的一组给定的 IAM 委托人（具有分配的贡献者权限）可以对这些资源进行操作。有关更多信息，请参阅 Amazon DataZone 术语和概念。

任何具有访问数据门户所需权限的亚马逊 DataZone 用户都可以在项目中编辑亚马逊 DataZone 环境。

要编辑现有环境，请完成以下步骤。

1. 导航至 Amazon DataZone 数据门户 URL，然后使用单点登录 (SSO) 或凭证登录 AWS 。如果您是亚马逊 DataZone 管理员，则可以通过 https://console.aws.amazon.com/datazone 导航到亚马逊 DataZone 控制台，使用域名创建 AWS 账户 地登录，然后选择打开数据门户。
2. 从顶部导航窗格中选择 “浏览项目”，然后选择包含要编辑的环境的项目。
3. 找到并选择要打开其详细信息页面的环境。然后展开操作并选择编辑环境。
4. 编辑环境的名称和描述，然后选择保存更改。

删除环境

在 Amazon DataZone 项目中，环境是已配置资源的集合（例如，Amazon S3 存储桶、 AWS Glue 数据库或 Amazon Athena 工作组），其中的一组给定的 IAM 委托人（具有分配的贡献者权限）可以对这些资源进行操作。有关更多信息，请参阅 Amazon DataZone 术语和概念。

任何具有访问数据门户所需权限的亚马逊 DataZone 用户都可以在项目中删除亚马逊 DataZone 环境。

要删除现有环境，请完成以下步骤。

1. 导航至 Amazon DataZone 数据门户 URL，然后使用单点登录 (SSO) 或凭证登录 AWS 。如果您是亚马逊 DataZone 管理员，则可以通过 https://console.aws.amazon.com/datazone 导航到亚马逊 DataZone 控制台，使用域名创建 AWS 账户 地登录，然后选择打开数据门户。
2. 从顶部导航窗格中选择 “浏览项目”，然后选择包含要删除的环境的项目。
3. 找到并选择要打开其详细信息页面的环境，然后展开操作并选择删除环境。
4. 在 “删除环境” 弹出窗口中，通过在字段`Delete`中键入来确认删除，然后选择 “删除环境”。

   只有在删除所有依赖于该环境的实体之后，才能成功删除该环境。要删除环境，必须先删除其所有关联的数据源和订阅目标。

创建新 项目

在亚马逊中 DataZone，项目使一组用户能够就各种业务用例进行协作，这些用例涉及发布、发现、订阅和使用亚马逊 DataZone 目录中的数据资产。有关更多信息，请参阅 Amazon DataZone 术语和概念。

任何具有访问数据门户所需权限的亚马逊 DataZone 用户都可以创建亚马逊 DataZone 项目。

要创建新项目，请完成以下步骤。

1. 导航至 Amazon DataZone 数据门户 URL，然后使用单点登录 (SSO) 或凭证登录 AWS 。如果您是亚马逊 DataZone 管理员，则可以通过 https://console.aws.amazon.com/datazone 导航到亚马逊 DataZone 控制台，使用域名创建 AWS 账户 地登录，然后选择打开数据门户。
2. 在亚马逊 DataZone 数据门户中，选择创建项目。
3. 为以下字段指定值，然后选择 “创建项目”：
   - 名称-项目名称。
   - 描述-项目的描述。

编辑项目

在亚马逊中 DataZone，项目使一组用户能够就各种业务用例进行协作，这些用例涉及发布、发现、订阅和使用亚马逊 DataZone 目录中的数据资产。有关更多信息，请参阅 Amazon DataZone 术语和概念。要编辑 Amazon DataZone 项目，您必须是该项目的所有者或包含该项目的域名的域管理员。

要编辑现有项目，请完成以下步骤。

1. 导航至 Amazon DataZone 数据门户 URL，然后使用单点登录 (SSO) 或凭证登录 AWS 。如果您是亚马逊 DataZone 管理员，则可以通过 https://console.aws.amazon.com/datazone 导航到亚马逊 DataZone 控制台，使用域名创建 AWS 账户 地登录，然后选择打开数据门户。
2. 选择 “浏览项目”。
3. 选择要编辑的项目。如果您在项目列表中看不到它，则可以通过在 “查找项目” 字段中指定项目名称来进行搜索。
4. 展开 “操作”，然后选择 “编辑项目”。
5. 更新项目名称和描述，然后选择 “保存”。

删除项目

在亚马逊中 DataZone，项目使一组用户能够就各种业务用例进行协作，这些用例涉及发布、发现、订阅和/或使用亚马逊 DataZone 目录中的数据资产。有关更多信息，请参阅 Amazon DataZone 术语和概念。

删除项目的行为是最终的。删除将不可撤销地删除项目的内容，包括数据源、环境、资产、词汇表和元数据表单。亚马逊 DataZone 撤销 DataZone 了亚马逊通过Lake Formation和Amazon Redshift对托管资产发放的补助。删除项目不会删除亚马逊 DataZone 可能帮助您创建的非亚马逊 DataZone AWS 资源。如果您不再需要这些 AWS 资源，请在相应的 AWS 服务和帐户中将其删除。

要删除 Amazon DataZone 项目，您必须是该项目的所有者。

要删除现有项目，请完成以下步骤。

1. 导航至 Amazon DataZone 数据门户 URL，然后使用单点登录 (SSO) 或凭证登录 AWS 。IAM 委托人可以通过 https://console.aws.amazon.com/datazone 导航到亚马逊 DataZone控制台，使用域名创建 AWS 账户 地登录，然后选择打开数据门户。
2. 从顶部导航窗格中选择 “浏览项目”。
3. 选择要删除的项目。如果您在项目列表中看不到它，则可以通过在 “查找项目” 字段中指定项目名称来进行搜索。
4. 展开 “操作”，然后选择 “删除项目”。

   查看有关删除项目的潜在影响的信息警告。
5. 如果您接受警告，请键入确认文本，然后选择删除。

> **Important**
>
> 删除项目是一项不可撤销的操作，您或您都无法撤消。 AWS

> **Note**
>
> 当您或您的域用户在项目中创建环境时，Amazon DataZone 会在您的域名或关联账户中创建 AWS 资源，为您和您的域用户提供功能。以下是 Amazon DataZone 可能为项目创建的 AWS 资源列表以及默认名称。删除项目不会删除您 AWS 账户中的任何此类 AWS 资源。
>
> - <environmentId>IAM 角色：datazone_usr_。
> - <environmentName>Glue 数据库：(1) <environmentName>_pub_db-*，(2) _sub_db-*。如果已经存在同名数据库，Amazon DataZone 将添加环境 ID。
> - <environmentName>Athena 工作组：-*。如果已经存在同名工作组，Amazon DataZone 将添加环境 ID。

- CloudWatch 日志组：datazone_ <environmentId>

离开项目

在亚马逊中 DataZone，项目使一组用户能够就各种业务用例进行协作，这些用例涉及发布、发现、订阅和使用亚马逊 DataZone 目录中的数据资产。有关更多信息，请参阅 Amazon DataZone 术语和概念。

要退出现有项目，请完成以下步骤。

1. 导航至 Amazon DataZone 数据门户 URL，然后使用单点登录 (SSO) 或凭证登录 AWS 。如果您是亚马逊 DataZone 管理员，则可以通过 https://console.aws.amazon.com/datazone 导航到亚马逊 DataZone 控制台，使用域名创建 AWS 账户 地登录，然后选择打开数据门户。
2. 从顶部导航窗格中选择 “选择项目”，然后选择项目。
3. 选择您要离开的项目。如果您在项目列表中看不到它，则可以通过在 “查找项目” 字段中指定项目名称来进行搜索。
4. 展开 “操作”，然后选择 “离开项目”。

向项目添加成员

在亚马逊中 DataZone，项目使一组用户能够就各种业务用例进行协作，这些用例涉及发布、发现、订阅和使用亚马逊 DataZone 目录中的数据资产。有关更多信息，请参阅 Amazon DataZone 术语和概念。

要向项目添加成员，您必须是项目所有者或贡献者。您可以将 SSO 群组、SSO 用户或 IAM 委托人（角色或用户）添加为项目成员。

要向现有项目添加成员，请完成以下步骤。

1. 导航至 Amazon DataZone 数据门户 URL，然后使用单点登录 (SSO) 或凭证登录 AWS 。如果您是亚马逊 DataZone 管理员，则可以通过 https://console.aws.amazon.com/datazone 导航到亚马逊 DataZone 控制台，使用域名创建 AWS 账户 地登录，然后选择打开数据门户。
2. 从顶部导航窗格中选择 “选择项目”，然后选择项目。
3. 选择要向其添加成员的项目。如果您在项目列表中看不到它，则可以通过在 “查找项目” 字段中指定项目名称来进行搜索。

4. 在项目的详细信息页面上，选择 “成员” 选项卡，然后选择 “所有成员” 节点。
5. 在项目成员选项卡中，选择添加成员。
6. 在向项目添加成员弹出窗口中，指定要添加的用户并指定他们在项目中的角色（所有者或参与者），然后选择添加成员。

> **Note**
>
> 如果 IAM 委托人的域中已有 Amazon DataZone 用户资料，则可以将该委托人添加为项目成员。当亚马逊通过门户、API 或 CLI 成功与 IAM 委托人交互时，它 DataZone 会自动为该域名创建用户档案。您无法为 IAM 委托人创建用户个人资料。如果 IAM 委托人的域中没有现有 Amazon DataZone 用户资料，则要将 IAM 委托人添加为项目成员，请管理员在 IAM 控制台AmazonDataZoneDomainExecutionRole中为您的域添加以下两个 IAM 权限：`iam:GetUser`和`iam:GetRole`。另外，要在域中执行操作，IAM 委托人必须拥有相应的 IAM 权限才能执行此类操作。

从项目中移除成员

在亚马逊中 DataZone，项目使一组用户能够就各种业务用例进行协作，这些用例涉及发布、发现、订阅和使用亚马逊 DataZone 目录中的数据资产。有关更多信息，请参阅 Amazon DataZone 术语和概念。要从项目中移除成员，您必须是项目所有者。

要从现有项目中移除成员，请完成以下步骤。

1. 使用 DataZone 数据门户 URL 导航至 Amazon 数据门户，然后使用您的 SSO 或 AWS 凭证登录。如果您是亚马逊 DataZone 管理员，则可以通过使用创建亚马逊 DataZone 域名的 AWS 账户访问亚马逊 DataZone 控制台 https://console.aws.amazon.com/datazone 来获取数据门户网址。
2. 从顶部导航窗格中选择 “选择项目”，然后选择项目。
3. 选择要移除成员的项目。如果您在项目列表中看不到它，则可以通过在 “查找项目” 字段中指定项目名称来进行搜索。
4. 在项目的详细信息页面上，选择 “成员” 选项卡，然后选择 “所有成员” 节点。
5. 在项目 “成员” 选项卡中，选择要从项目中移除的成员，然后选择 “移除”。
6. 在 “移除成员” 弹出窗口中，选择 “移除成员” 以确认删除。

在 Amazon 中创建库存和发布数据 DataZone

本节介绍您要执行的任务和程序，以便在亚马逊上创建数据清单， DataZone 并在亚马逊上发布数据 DataZone。

要使用亚马逊对您的数据 DataZone 进行分类，您必须先将您的数据（资产）作为项目库存带到亚马逊 DataZone。为特定项目创建清单，则只有该项目的成员才能发现这些资产。除非明确发布，否则并非所有域名用户都可以在搜索/浏览中使用项目清单资产。创建项目清单后，数据所有者可以通过添加或更新企业名称（资产和架构）、描述（资产和架构）、自述、词汇表（资产和架构）和元数据表单，使用所需的业务元数据整理库存资产。

使用 Amazon DataZone 对您的数据进行分类的下一步是让域名用户可以发现您项目的库存资产。您可以通过将库存资产发布到 Amazon DataZone 目录来做到这一点。只有最新版本的库存资产可以发布到目录中，发现目录中只有最新发布的版本处于活动状态。如果库存资产在发布到亚马逊 DataZone 目录后进行了更新，则必须再次明确发布该库存资产，以使最新版本出现在发现目录中。

主题

为亚马逊配置 Lake Formation 权限 DataZone

当您使用内置的数据湖蓝图 (DefaultDataLake) 创建环境时，会在 Amazon DataZone 中添加一个 AWS Glue 数据库，这是该环境创建过程的一部分。如果要从此 AWS Glue 数据库发布资产，则无需其他权限。

但是，如果您想发布资产并订阅存在于亚马逊 DataZone 环境之外的 AWS Glue 数据库中的资产，则必须明确向亚马逊 DataZone 提供访问此外部 AWS Glue 数据库中表的权限。为此，你必须在 AWS Lake Formation 中完成以下设置，并将必要的 Lake Formation 权限附加到AmazonDataZoneGlueAccess-<region>-<domainId>。

- 使用 Lake Formation 权限模式或混合访问模式在 AWS Lake Formation 中为您的数据湖配置 Amazon S3 位置。欲了解更多信息，请参阅 https://docs.aws.amazon.com/lake-formation/latest/dg/register-data-lake .html。
- 从亚马逊 DataZone 处理`IAMAllowedPrincipals`权限的 Amazon Lake Formation 表中移除权限。欲了解更多信息，请参阅 https://docs.aws.amazon.com/lake-formation/latest/dg/ upgrade-glue-lake-formation-background.html。
- 将以下 AWS Lake Formation 权限附加到AmazonDataZoneGlueAccess-<region>-<domainId>：
  - `Describe`以及对存在表的数据库的`Describe grantable`权限
  - `Describe`、`SelectDescribe Grantable`、、以上数据库中您 DataZone 要代表您管理访问`Select Grantable`权限的所有表的权限。

> **Note**
>
> 亚马逊 DataZone 支持 AWS Lake Formation 混合模式。Lake For AWS mation 混合模式允许你开始通过 Lake Formation 管理你的 Glue 数据库和表的权限，同时继续保持对这些表和数据库的任何现有 IAM 权限。有关更多信息，请参阅亚马逊与 AWS Lake Formation 混合模式 DataZone 集成

有关更多信息，请参阅 对亚马逊 AWS Lake Formation 权限进行故障排除 DataZone。

亚马逊与 AWS Lake Formation 混合模式 DataZone 集成

亚马逊 DataZone 已与 La AWS ke Formation 混合模式集成。这种集成使您能够轻松地通过亚马逊发布和共享您的 AWS Glue 表， DataZone而无需先在 AWS Lake Formation 中注册它们。混合模式允许

您开始通过 AWS Lake For AWS mation 管理您的 Glue 表的权限，同时继续保持对这些表的任何现有 IAM 权限。

首先，您可以在 Amazon DataZone 管理控制台中启用DefaultDataLake蓝图下的数据位置注册设置。

启用与 AWS Lake Formation 混合模式的集成

1. 通过 https://console.aws.amazon.com/datazone 导航到亚马逊 DataZone 控制台，然后使用您的账户凭证登录。
2. 选择 “查看域”，然后选择要在其中启用与 AWS Lake Formation 混合模式集成的域。
3. 在域名详细信息页面上，导航至蓝图选项卡。
4. 从蓝图列表中选择DefaultDataLake蓝图。
5. 确保 DefaultDataLake 蓝图已启用。如果未启用，请按照中的步骤在您的 AWS 账户中在拥有 Amazon DataZone 域 AWS 名的账户中启用内置蓝图将其启用。
6. 在 DefaultDataLake 详细信息页面上，打开配置选项卡，然后选择页面右上角的编辑按钮。
7. 在 “数据位置注册” 下，选中复选框以启用数据位置注册。
8. 对于数据位置管理角色，您可以创建新的 IAM 角色或选择现有的 IAM 角色。亚马逊 DataZone 使用此角色通过 Lake Formation 混合访问模式管理对为数据湖选择的 Amazon S3 存储桶的读/写权限。 AWS 有关更多信息，请参阅 AmazonDataZone<region>S3Manage--<domainId>。
9. 或者，如果您不希望亚马逊在混合模式下自动注册某些 Amazon S3 地点 DataZone ，则可以选择将其排除在外。为此，请完成以下步骤：

   - 选择切换按钮以排除指定的 Amazon S3 地点。
   - 提供您要排除的 Amazon S3 存储桶的 URI。
   - 要添加其他存储桶，请选择添加 S3 位置。

   > **Note**
   >
   > Amazon DataZone 仅允许排除 S3 根位置。S3 根位置路径内的任何 S3 位置都将自动排除在注册范围之外。

   - 选择保存更改。

在 AWS 账户中启用数据位置注册设置后，当数据使用者订阅通过 IAM 权限管理的 AWS Glue 表时，亚马逊 DataZone 将首先以混合模式注册该表的 Amazon S3 位置，然后通过 La AWS ke Formation 管

理表的权限，向数据使用者授予访问权限。这样可以确保使用新授予的 La AWS ke Formation 权限继续存在表上的 IAM 权限，而不会中断任何现有工作流程。

在亚马逊启用 AWS Lake Formation 混合模式集成时如何处理加密的亚马逊 S3 位置 DataZone

如果您使用的是使用客户托 AWS 管或托管 KMS 密钥加密的 Amazon S3 位置，则 AmazonDataZoneS3Manag e 角色必须有权使用 KMS 密钥加密和解密数据，或者 KMS 密钥策略必须向该角色授予密钥使用权限。

如果您的 Amazon S3 位置使用 AWS 托管密钥加密，请向该AmazonDataZoneDataLocationManagement角色添加以下内联策略：

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

如果您的 Amazon S3 位置已使用客户托管密钥加密，请执行以下操作：

1. 打开 AWS KMS 控制台，网址为 https://console.aws.amazon.com/kms 并以 AWS 身份和访问管理 (IAM) 管理用户或可以修改用于加密位置的 KMS 密钥策略的用户身份登录。
2. 在导航窗格中，选择客户自主管理型密钥，然后选择所需的 KMS 密钥的名称。
3. 在 KMS 密钥详细信息页面上，选择密钥策略选项卡，然后执行以下任一操作将您的自定义角色或 Lake Formation 服务相关角色添加为 KMS 密钥用户：
   - 如果显示默认视图（包括 “密钥管理员”、“密钥删除”、“密钥用户” 和 “其他 AWS 账户” 部分），请在 “密钥用户” 部分下添加AmazonDataZoneDataLocationManagement角色。

- 如果显示密钥策略 (JSON)，请编辑策略以向 “允许使用密钥” 对象添加AmazonDataZoneDataLocationManagement角色，如以下示例所示

```
...
        {
            "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**
>
> 如果 KMS 密钥或 Amazon S3 位置与数据目录不在同一个 AWS 账户中，请按照跨 AWS 账户注册加密的 Amazon S3 位置中的说明进行操作。

创建自定义资产类型

在 Amazon 中 DataZone，资产代表特定类型的数据资源，例如数据库表、控制面板或机器学习模型。为了在描述目录资产时保持一致性和标准化，Amazon DataZone 域必须有一组资产类型来定义资产在目录中的表示方式。资产类型定义特定类型资产的架构。资产类型具有一组必填和可选的可命名元数据表单类型（例如 GovForm 或 GovernanceFormType）。Amazon 中的资产类型 DataZone 是版本化

的。创建资产时，将根据其资产类型（通常是最新版本）定义的架构对其进行验证，如果指定的结构无效，则资产创建将失败。

系统资产类型-Ama DataZone zon 预置服务拥有的系统资产类型（包括 GlueTableAssetType GlueViewAssetType RedshiftTableAssetType、 RedshiftViewAssetType、和 S3ObjectCollectionAssetType）和系统表单类型（包括 DataSourceReferenceFormType AssetCommonDetailsFormType、和 SubscriptionTermsFormType）。无法编辑系统资产类型。

自定义资产类型-要创建自定义资产类型，首先要创建表单类型所需的元数据表单类型和词汇表，以便在表单类型中使用。然后，您可以通过指定名称、描述和关联的元数据表单来创建自定义资产类型，这些表单可以是必需的，也可以是可选的。

对于包含结构化数据的资产类型，要表示数据门户中的列架构，您可以使用`RelationalTableFormType`向列中添加技术元数据（包括列名、描述和数据类型），并使用添加列的业务描述，包括公司名称、词汇表术语和自定义键值对。 `ColumnBusinessMetadataForm`

要通过数据门户创建自定义资产类型，请完成以下步骤：

1. 导航至 Amazon DataZone 数据门户 URL，然后使用单点登录 (SSO) 或凭证登录 AWS 。如果您是亚马逊 DataZone 管理员，则可以通过 https://console.aws.amazon.com/datazone 导航到亚马逊 DataZone 控制台，使用域名创建 AWS 账户 地登录，然后选择打开数据门户。
2. 从顶部导航窗格中选择 “选择项目”，然后选择要在其中创建自定义资产类型的项目。
3. 导航到项目的 “数据” 选项卡。
4. 从左侧导航窗格中选择资产类型，然后选择创建资产类型。
5. 指定以下内容，然后选择 “创建”。
   - 名称-自定义资产类型的名称
   - 描述-自定义资产类型的描述。
   - 选择 “添加元数据表单”，将元数据表单添加到此自定义资产类型。
6. 创建自定义资产类型后，您可以使用它来创建资产。

要通过 API 创建自定义资产类型，请完成以下步骤：

1. 通过调用 `CreateFormType` API 操作创建元数据表单类型。

   以下是 Amazon 的 SageMaker 示例：

```
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. 接下来，您可以通过调用 CreateAssetType API 操作来创建资产类型。您只能使用可用的系统表单类型（SubscriptionTermsFormType在以下示例中）或自定义表单类型通过 Amazon DataZone API 创建资产类型。对于系统表单类型，类型名称必须以开头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,
```

```
        },
    },
)
```

以下是为结构化数据创建资产类型的示例：

```
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. 现在，您可以使用在上述步骤中创建的自定义资产类型来创建资产。

```
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}"
        }
        ]
)
```

在此示例中，您正在创建结构化数据资产：

```
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": ".."
        },
        .....
```

```
        ]
)
```

为创建并运行 Amazon DataZone 数据源 AWS Glue Data Catalog

在 Amazon 中 DataZone，您可以创建 AWS Glue Data Catalog 数据源，以便从中导入数据库表的技术元数据 AWS Glue。要为添加数据源 AWS Glue Data Catalog，源数据库必须已存在于 AWS Glue。

创建和运行 AWS Glue 数据源时，会将源 AWS Glue 数据库中的资产添加到您的 Amazon DataZone 项目的库存中。您可以按设定的时间表或按需运行 AWS Glue 数据源，以创建或更新资产的技术元数据。在数据源运行期间，您可以选择将您的资产发布到 Amazon DataZone 目录，从而使所有域用户都能发现这些资产。您也可以在编辑项目清单资产的业务元数据后发布这些资产。域用户可以搜索和发现您发布的资产，并申请订阅这些资产。

添加 AWS Glue 数据源

1. 导航至 Amazon DataZone 数据门户 URL，然后使用单点登录 (SSO) 或凭证登录 AWS 。如果您是亚马逊 DataZone 管理员，则可以通过 https://console.aws.amazon.com/datazone 导航到亚马逊 DataZone 控制台，使用域名创建 AWS 账户 地登录，然后选择打开数据门户。
2. 从顶部导航窗格中选择 “选择项目”，然后选择要向其中添加数据源的项目。
3. 导航到项目的 “数据” 选项卡。
4. 从左侧导航窗格中选择数据源，然后选择创建数据源。
5. 配置以下字段：
   - 名称-数据源名称。
   - 描述-数据源描述。
6. 在 “数据源类型” 下，选择AWS Glue。
7. 在 “选择环境” 下，指定要在其中发布 AWS Glue 表的环境。
8. 在数据选择下，提供一个 AWS Glue 数据库并输入您的表选择标准。例如，如果您选择 Incl u de 并输入`*corporate`，则数据库将包括所有以该词结尾的源表`corporate`。

   您可以从下拉列表中选择一个 AWS Glue 数据库，也可以键入数据库名称。下拉列表包括两个数据库：发布数据库和环境的订阅数据库。如果要从不是由环境创建的数据库中提取资产，则必须键入数据库的名称，而不是从下拉列表中进行选择。

您可以为单个数据库中的表添加多个包含和排除规则。您也可以使用 “添加其他数据库” 按钮添加多个数据库。

9. 在 “数据质量” 下，您可以选择为此数据源启用数据质量。如果您这样做，亚马逊会将您现有的 AWS Glue 数据质量输出 DataZone导入您的亚马逊 DataZone目录中。默认情况下，亚马逊会从 AWS Glue DataZone 导入现有 100 份没有有效期的最新 100 份质量报告。

   Amazon 的数据质量指标 DataZone 可帮助您了解数据源的完整性和准确性。亚马逊从 AWS G DataZone lue 中提取这些数据质量指标，以便在某个时间点（例如在搜索业务数据目录期间）提供背景信息。数据用户可以看到其订阅资产的数据质量指标如何随着时间的推移而变化。数据生成者可以按计划获 AWS 取 Glue 数据质量分数。亚马逊 DataZone 企业数据目录还可以通过数据质量 API 显示来自第三方系统的数据质量指标。有关更多信息，请参阅Amazon 的数据质量 DataZone
10. 选择下一步。
11. 对于发布设置，选择是否可以在业务数据目录中立即发现资产。如果您只将它们添加到库存中，则可以稍后选择订阅条款并将其发布到业务数据目录中。有关更多信息，请参阅 the section called “管理现有数据源”。
12. 对于自动生成企业名称，请选择是否在从来源导入资产时自动生成元数据。
13. （可选）对于元数据表单，添加表单以定义在资产导入 Amazon 时收集和保存的元数据 DataZone。有关更多信息，请参阅 the section called “创建、编辑或删除元数据表单”。
14. 在 “运行” 首选项中，选择何时运行数据源。
    - 按计划运行-指定运行数据源的日期和时间。
    - 按需运行-您可以手动启动数据源运行。
15. 选择下一步。
16. 查看您的数据源配置并选择创建。

> **Note**
>
> 创建 AWS Glue 数据源时，亚马逊 DataZone 会为环境的 IAM 角色创建 Lake Formation “只读” 权限，该角色用于创建数据源，以访问数据源中使用的 G AWS lue 数据库中的所有表。您可以在环境详细信息页面的数据源下监控这些授权的状态。在向发布环境的 IAM 角色授予访问权限时，亚马逊会向 AWS Glue 数据库 DataZone 添加以下 AWS 标签：`DataZoneDiscoverable_${domainId}: true`

对于在 Amazon 当前版本之前创建的环境 DataZone，项目成员将无法在 Amazon Athena 中看到已授权的表。

为亚马逊 Redshift 创建并运行亚马逊 DataZone 数据源

在亚马逊中 DataZone，您可以创建亚马逊 Redshift 数据源，以便从亚马逊 Redshift 数据仓库中导入数据库表和视图的技术元数据。要为亚马逊 Redshift 添加亚马逊 DataZone 数据源，源数据仓库必须已经存在于亚马逊 Redshift 中。

创建和运行 Amazon Redshift 数据源时，您可以将源亚马逊 Redshift 数据仓库中的资产添加到您的 DataZone 亚马逊项目的库存中。您可以按设定的计划或按需运行 Amazon Redshift 数据源，以创建或更新资产的技术元数据。在数据源运行期间，您可以选择将项目库存资产发布到 Amazon DataZone 目录，从而使所有域用户都能发现这些资产。您也可以在编辑库存资产的业务元数据后发布这些资产。域用户可以搜索和发现您发布的资产，并申请订阅这些资产。

添加 Amazon Redshift 数据源

1. 导航至 Amazon DataZone 数据门户 URL，然后使用单点登录 (SSO) 或凭证登录 AWS 。如果您是亚马逊 DataZone 管理员，则可以通过 https://console.aws.amazon.com/datazone 导航到亚马逊 DataZone 控制台，使用域名创建 AWS 账户 地登录，然后选择打开数据门户。
2. 从顶部导航窗格中选择 “选择项目”，然后选择要向其中添加数据源的项目。
3. 导航到项目的 “数据” 选项卡。
4. 从左侧导航窗格中选择数据源，然后选择创建数据源。
5. 配置以下字段：
   - 名称-数据源名称。
   - 描述-数据源描述。
6. 在 “数据源类型” 下，选择 Amazon Redshift。
7. 在 “选择环境” 下，指定要在其中发布 Amazon Redshift 表的环境。
8. 根据您选择的环境，亚马逊 DataZone 将自动直接从环境中应用Amazon Redshift凭证和其他参数，或者允许您选择自己的凭证和其他参数。
   - 如果您选择的环境仅允许通过环境的默认 Amazon Redshift 架构进行发布，则亚马逊 DataZone 将自动应用亚马逊 Redshift 凭证和其他参数，包括亚马逊 Redshift 集群或工作组名称 AWS 、密钥、数据库名称和架构名称。您无法编辑这些自动填充的参数。
   - 如果您选择的环境不允许发布任何数据，则将无法继续创建数据源。

- 如果您选择的环境允许从任何架构发布数据，则可以选择使用该环境中的证书和其他 Amazon Redshift 参数，也可以输入自己的证书/参数。

9. 如果您选择使用自己的凭据来创建数据源，请提供以下详细信息：

   - 在 “提供亚马逊 Redshift 凭证” 下，选择是使用预配置的 Amazon Redshift 集群还是亚马逊 Redshift 无服务器工作空间作为数据源。
   - 根据您在上述步骤中的选择，从下拉菜单中选择您的 Amazon Redshift 集群或工作空间，然后在 Secr AWS ets Manager 中选择用于身份验证的密钥。您可以选择现有密钥或创建新密钥。
   - 为了使现有密钥显示在下拉列表中，请确保您在 Secrets Manager 中的 AWS 密钥包含以下标签（键/值）：
     - AmazonDataZoneProject: <projectID>
     - AmazonDataZoneDomain: <domainID>

     如果您选择创建新密钥，则系统会自动使用上面提及的标签对密钥进行标记，无需执行任何额外步骤。有关更多信息，请参阅中存储数据库凭据 AWS Secrets Manager。

     为创建数据源而提供的 AWS 密钥中的 Amazon Redshift 用户必须拥有要发布的表的SELECT权限。如果您希望 Amazon DataZone 同时代表您管理订阅（访问权限），则 AWS 密钥中的数据库用户还必须具有以下权限：
     - `CREATE DATASHARE`
     - `ALTER DATASHARE`
     - `DROP DATASHARE`

10. 在 “数据选择” 下，提供 Amazon Redshift 数据库、架构，然后输入您的表或视图选择标准。例如，如果您选择 Incl u de 并输入`*corporate`，则资产将包括所有以该词结尾的源表`corporate`。

    您可以为单个数据库中的表添加多个包含规则。您也可以使用 “添加其他数据库” 按钮添加多个数据库。

11. 选择下一步。
12. 对于发布设置，选择是否可以在数据目录中立即发现资产。如果您只将它们添加到库存中，则可以稍后选择订阅条款并将其发布到业务数据目录中。有关更多信息，请参阅 the section called “管理现有数据源”。
13. 对于自动生成企业名称，请选择是否在从源头发布和更新资产时自动生成元数据。
14. （可选）对于元数据表单，添加表单以定义在资产导入 Amazon 时收集和保存的元数据 DataZone。有关更多信息，请参阅 the section called “创建、编辑或删除元数据表单”。

15. 在 “运行” 首选项中，选择何时运行数据源。
    - 按计划运行-指定运行数据源的日期和时间。
    - 按需运行-您可以手动启动数据源运行。
16. 选择下一步。
17. 查看您的数据源配置并选择创建。

> **Note**
>
> 创建 Amazon Redshift 数据源时，亚马逊会 DataZone 授予对用于创建数据源的环境的 “只读” 访问权限，以访问数据源中使用的 Amazon Redshift 架构中的所有表。您可以在环境详细信息页面的数据源下监控这些授权的状态。
> 使用不同于创建环境的 Amazon Redshift 集群或无服务器工作组时，必须确保将以下 AWS 标签添加到集群或工作组。要使环境用户能够在 Amazon Redshift 查询编辑器 V2 中查看授权的数据库，这是必要的：`DataZoneDiscoverable_${domainId}: true`
> 对于在 Amazon 当前版本之前创建的环境 DataZone，项目成员将无法在 Amazon Redshift 中查看已授权的表。

管理现有的 Amazon DataZone 数据源

创建 Amazon DataZone 数据源后，您可以随时对其进行修改以更改源详细信息或数据选择标准。当您不再需要某个数据源时，可以将其删除。

要完成这些步骤，您必须附加AmazonDataZoneFullAccess AWS 托管策略。有关更多信息，请参阅 the section called “AWS 托管策略”。

主题

- 编辑数据源
- 删除数据源

编辑数据源

您可以编辑 Amazon DataZone 数据源以修改其数据选择设置，包括添加、删除或更改表选择标准。您也可以添加和移除数据库。您无法更改数据源类型或发布数据源的环境。

编辑数据来源

1. 导航至 Amazon DataZone 数据门户 URL，然后使用单点登录 (SSO) 或凭证登录 AWS 。如果您是亚马逊 DataZone管理员，则可以通过 https://console.aws.amazon.com/datazone 导航到亚马逊 DataZone 控制台，使用域名创建 AWS 账户 地登录，然后选择打开数据门户。
2. 从顶部导航窗格中选择 “选择项目”，然后选择数据源所属的项目。
3. 导航到项目的 “数据” 选项卡。
4. 从左侧导航窗格中选择 “数据源”，然后选择要修改的数据源。
5. 导航至 “数据源定义” 选项卡，然后选择 “编辑”。
6. 对数据源定义进行更改。您可以更新数据源详细信息并更改数据选择标准。
7. 完成更改后，选择 Save (保存)。

删除数据源

当您不再需要 Amazon DataZone 数据源时，可以将其永久删除。删除数据源后，源自该数据源的所有资产仍可在目录中使用，用户仍然可以订阅它们。但是，资源将停止接收来自来源的更新。我们建议您先将依赖资产移至其他数据源，然后再将其删除。

> **Note**
>
> 您必须先移除数据源上的所有发货，然后才能将其删除。有关更多信息，请参阅 在 Amazon 中发现、订阅和使用数据 DataZone。

删除数据来源

1. 在项目的 “数据” 选项卡上，从左侧导航窗格中选择 “数据源”。
2. 选择要删除的数据源。
3. 选择操作，删除数据源并确认删除。

将项目库存中的资产发布到 Amazon DataZone 目录

您可以将项目清单中的亚马逊 DataZone 资产及其元数据发布到亚马逊 DataZone 目录中。您只能将资源的最新版本发布到目录中。

将资源发布到目录时，请考虑以下事项：

- 要将资源发布到目录中，您必须是该项目的所有者或贡献者。
- 对于亚马逊 Redshift 资产，请确保与发布商和订阅者集群关联的亚马逊 Redshift 集群满足亚马逊 Redshift 数据共享的所有要求，以便亚马逊 DataZone 能够管理 Redshift 表和视图的访问权限。请参阅 Amazon Redshift 的数据共享概念。
- 亚马逊 DataZone 仅支持对从和亚马逊 Redshift 发布 AWS Glue Data Catalog 的资产进行访问管理。对于所有其他资产，例如 Amazon S3 对象，Amazon DataZone 不管理已批准订阅者的访问权限。如果您订阅了这些非托管资产，则会收到以下消息通知：

  ```
  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.
  ```

发布资产

如果您在创建数据源时没有选择让资产立即在数据目录中被发现，请执行以下步骤以便稍后将其发布。

发布资产

1. 导航至 Amazon DataZone 数据门户 URL，然后使用单点登录 (SSO) 或凭证登录 AWS 。如果您是亚马逊 DataZone管理员，则可以通过 https://console.aws.amazon.com/datazone 导航到亚马逊 DataZone 控制台，使用域名创建 AWS 账户 地登录，然后选择打开数据门户。
2. 从顶部导航窗格中选择 “选择项目”，然后选择资产所属的项目。
3. 导航到项目的 “数据” 选项卡。
4. 从左侧导航窗格中选择库存数据，然后选择要发布的资产。

   > **Note**
   >
   > 默认情况下，所有资产都需要订阅批准，这意味着数据所有者必须批准对该资产的所有订阅请求。如果您想在发布资源之前更改此设置，请打开资产详细信息并选择订阅批准旁边的编辑。您可以稍后通过修改和重新发布资源来更改此设置。

5. 选择 “发布资源”。资源将直接发布到目录中。

   如果您对资源进行了更改，例如修改其批准要求，则可以选择 “重新发布”，将更新发布到目录。

管理库存和整理资产

要使用亚马逊对您的数据 DataZone 进行分类，您必须先将您的数据（资产）作为项目库存带到亚马逊 DataZone。为特定项目创建清单，则只有该项目的成员才能发现这些资产。

一旦在项目清单中创建了资产，就可以对其元数据进行整理。例如，您可以编辑资产的名称、描述或阅读我的内容。对资源的每次编辑都会创建资源的新版本。您可以使用资产详细信息页面上的 “历史记录” 选项卡来查看所有资产版本。

您可以编辑 “自述” 部分，并为该资产添加丰富的描述。Read Me 部分支持 markdown，因此您可以根据需要设置描述的格式，并向消费者描述有关资产的关键信息。

通过填写可用表格，可以在资产层面添加词汇表术语。

要整理架构，您可以查看列，添加公司名称、描述，并在列级别添加词汇表术语。

如果在创建数据源时启用了自动元数据生成，则资产和列的企业名称可供单独或一次全部查看和接受或拒绝。

您也可以编辑订阅条款以指定是否需要批准该资产。

借 DataZone 助 Amazon 中的元数据表单，您可以通过添加自定义属性（例如，销售区域、销售年度和销售季度）来扩展数据资产的元数据模型。附加到某一资产类型的元数据表单将应用于根据该资产类型创建的所有资产。您还可以在数据源运行过程中或创建数据源之后，向单个资产添加其他元数据表单。有关创建新表单的信息，请参阅the section called “创建、编辑或删除元数据表单”。

要更新资产的元数据，您必须是该资产所属项目的所有者或贡献者。

更新资产的元数据

1. 导航至 Amazon DataZone 数据门户 URL，然后使用单点登录 (SSO) 或凭证登录 AWS 。如果您是亚马逊 DataZone 管理员，则可以通过 https://console.aws.amazon.com/datazone 导航到亚马逊 DataZone 控制台，使用域名创建 AWS 账户 地登录，然后选择打开数据门户。
2. 从顶部导航窗格中选择 Selec t project，然后选择包含要更新其元数据的资产的项目。
3. 导航到项目的 “数据” 选项卡。
4. 从左侧导航窗格中选择库存数据，然后选择要更新其元数据的资产的名称。
5. 在资产详细信息页面的元数据表单下，选择编辑并根据需要编辑现有表单。您还可以将其他元数据表单附加到资产。有关更多信息，请参阅 the section called “将其他元数据表单附加到资产”。
6. 完成更新后，选择 “保存表单”。

当您保存表单时，Amazon DataZone 会生成该资产的新库存版本。要将更新的版本发布到目录中，请选择 “重新发布资源”。

将其他元数据表单附加到资产

默认情况下，附加到某个域的元数据表单会附加到发布到该域的所有资产。数据发布者可以将其他元数据表单与单个资产关联起来，以提供更多背景信息。

将其他元数据表单附加到资产

1. 导航至 Amazon DataZone 数据门户 URL，然后使用单点登录 (SSO) 或凭证登录 AWS 。如果您是亚马逊 DataZone管理员，则可以通过 https://console.aws.amazon.com/datazone 导航到亚马逊 DataZone 控制台，使用域名创建 AWS 账户 地登录，然后选择打开数据门户。
2. 从顶部导航窗格中选择 Selec t project，然后选择包含要向其添加元数据的资产的项目。
3. 导航到项目的 “数据” 选项卡。
4. 从左侧导航窗格中选择库存数据，然后选择要向其添加元数据的资产的名称。
5. 在资产详细信息页面的元数据表单下，选择添加表单。
6. 选择要添加到资产中的表单，然后选择添加表单。
7. 为每个元数据字段输入值，然后选择保存表单。

   当您保存表单时，Amazon DataZone 会生成该资产的新库存版本。要将更新的版本发布到目录中，请选择 “重新发布资源”。

策划后将资源发布到目录

一旦对资产管理感到满意，数据所有者就可以将资产版本发布到 Amazon DataZone 目录中，从而使其可供所有域名用户发现。资产显示库存版本和已发布版本。在发现目录中，仅显示最新发布的版本。如果元数据在发布后更新，则新的库存版本将可供发布到目录中。

手动创建资产

在 Amazon DataZone 中，资产是呈现单个物理数据对象（例如表、控制面板、文件）或虚拟数据对象（例如视图）的实体。有关更多信息，请参阅 Amazon DataZone 术语和概念。手动发布资源是一次性操作。您没有为资源指定运行计划，因此如果其来源发生变化，它不会自动更新。

要通过项目手动创建资产，您必须是该项目的所有者或贡献者。

手动创建资产

1. 导航至 Amazon DataZone 数据门户 URL，然后使用单点登录 (SSO) 或凭证登录 AWS 。如果您是亚马逊 DataZone 管理员，则可以通过 https://console.aws.amazon.com/datazone 导航到亚马逊 DataZone 控制台，使用域名创建 AWS 账户 地登录，然后选择打开数据门户。
2. 从顶部导航窗格中选择 “选择项目”，然后选择要为其创建资源的项目。
3. 导航到项目的 “数据” 选项卡。
4. 从左侧导航窗格中选择数据源，然后选择创建数据资产。
5. 有关资产的详细信息，请配置以下设置：
   - 资产类型-资产的类型。
   - 名称-资产的名称。
   - 描述-对资产的描述。
6. 对于 S3 位置，请输入源 S3 存储桶的亚马逊资源名称 (ARN)。

   （可选）输入 S3 接入点。有关更多信息，请参阅使用 Amazon S3 接入点管理数据访问。
7. 对于发布设置，选择是否可以在目录中立即发现资源。如果您只将它们添加到库存中，则可以选择订阅条款将其发布到目录中。
8. 选择创建。

   资源创建后，要么将其作为活跃资产直接发布在目录中，要么存储在清单中，直到您决定发布为止。

从 Amazon DataZone 目录中取消发布资产

当您从目录中取消发布亚马逊 DataZone 资产时，该资产将不再出现在全球搜索结果中。新用户将无法在目录中找到或订阅资产清单，但所有现有订阅保持不变。

要取消发布资产，您必须是该资产所属项目的所有者或贡献者：

取消发布资源

1. 导航至 Amazon DataZone 数据门户 URL，然后使用单点登录 (SSO) 或凭证登录 AWS 。如果您是亚马逊 DataZone 管理员，则可以通过 https://console.aws.amazon.com/datazone 导航到亚马逊 DataZone 控制台，使用域名创建 AWS 账户 地登录，然后选择打开数据门户。
2. 从顶部导航窗格中选择 “选择项目”，然后选择资产所属的项目。

3. 导航到项目的 “数据” 选项卡。
4. 从左侧导航窗格中选择 “已发布的数据”。
5. 从已发布资源列表中找到该资源，然后选择 “取消发布”。

   该资产已从目录中移除。您可以随时通过选择 “发布” 来重新发布资源。

删除亚马逊 DataZone 资产

如果您不再需要 Amazon 中的某项资产 DataZone，则可以将其永久删除。删除资源与从目录中取消发布资源不同。您可以删除目录中的资产及其相关列表，使其在任何搜索结果中都不可见。要删除资产清单，必须先撤销其所有订阅。

要删除资产，您必须是该资产所属项目的所有者或贡献者：

> **Note**
>
> 要删除资产清单，必须先撤销对该资产的所有现有订阅。您无法删除已有订阅者的资产清单。

要删除资产

1. 导航至 Amazon DataZone 数据门户 URL，然后使用单点登录 (SSO) 或凭证登录 AWS 。如果您是亚马逊 DataZone 管理员，则可以通过 https://console.aws.amazon.com/datazone 导航到亚马逊 DataZone 控制台，使用域名创建 AWS 账户 地登录，然后选择打开数据门户。
2. 从顶部导航窗格中选择 “选择项目”，然后选择包含要删除的资产的项目。
3. 导航到项目的 “数据” 选项卡。
4. 从左侧导航窗格中选择 “已发布的数据”，然后找到并选择要删除的资产。这将打开资产详细信息页面。
5. 选择操作，删除并确认删除。

   资产一旦被删除，便无法再查看，用户也无法订阅该资源。

手动启动在 Amazon 中运行的数据源 DataZone

当您运行数据源时，Amazon 会从源中 DataZone 提取所有新的或修改过的元数据，并更新库存中的关联资产。向 Amazon 添加数据源时 DataZone，您需要指定该源的运行首选项，该首选项定义了数据源是按计划运行还是按需运行。如果您的源按需运行，则必须手动启动数据源的运行。

即使您的源代码按计划运行，您仍然可以随时手动运行。向资产添加业务元数据后，您可以选择资产并将其发布到 Amazon DataZone 目录，以便所有域名用户都能发现这些资产。其他网域用户只能搜索已发布的资源。

手动运行数据源

1. 导航至 Amazon DataZone 数据门户 URL，然后使用单点登录 (SSO) 或凭证登录 AWS 。如果您是亚马逊 DataZone 管理员，则可以通过 https://console.aws.amazon.com/datazone 导航到亚马逊 DataZone 控制台，使用域名创建 AWS 账户 地登录，然后选择打开数据门户。
2. 从顶部导航窗格中选择 “选择项目”，然后选择数据源所属的项目。
3. 导航到项目的 “数据” 选项卡。
4. 从左侧导航窗格中选择 “数据源”，然后找到并选择要运行的数据源。这将打开数据源详细信息页面。
5. 选择 “按需运行”。

   当 Amazon 使用源中的最新数据 DataZone 更新资产元数据时，数据源状态将更改`Running`为。您可以在 “数据源运行” 选项卡上监控运行状态。

Amazon 中的资产修订 DataZone

当您编辑资产的业务或技术元数据时，Amazon 会 DataZone 增加资产的修订量。这些编辑包括修改资产名称、描述、词汇表、列名、元数据表单和元数据表单字段值。这些更改可能源于手动编辑、数据源作业运行或 API 操作。每当您对资产进行编辑时，Amazon 都会 DataZone 自动生成新的资产修订。

更新资源并生成新修订版后，必须将新修订版发布到目录中，才能对其进行更新并可供订阅者使用。有关更多信息，请参阅 the section called “将资源从项目清单发布到目录”。您只能将资源的最新版本发布到目录中。

查看资产过去的修订版本

1. 导航至 Amazon DataZone 数据门户 URL，然后使用单点登录 (SSO) 或凭证登录 AWS 。如果您是亚马逊 DataZone 管理员，则可以通过 https://console.aws.amazon.com/datazone 导航到亚马逊 DataZone 控制台，使用域名创建 AWS 账户 地登录，然后选择打开数据门户。
2. 从顶部导航窗格中选择 “选择项目”，然后选择包含该资产的项目。
3. 导航到项目的 “数据” 选项卡，然后找到并选择资产。这将打开资产详细信息页面。
4. 导航到 “历史记录” 选项卡，该选项卡显示了该资产过去的修订列表。

Amazon 的数据质量 DataZone

Amazon 中的数据质量指标 DataZone 可帮助您了解不同的质量指标，例如数据源的完整性、及时性和准确性。Amazon DataZone 与 AWS Glue 数据质量集成，并提供 API 来集成来自第三方数据质量解决方案的数据质量指标。数据用户可以看到其订阅资产的数据质量指标如何随着时间的推移而变化。要编写和运行数据质量规则，您可以使用自己选择的数据质量工具，例如 AWS Glue 数据质量。借助 Amazon 中的数据质量指标 DataZone，数据使用者可以可视化资产和列的数据质量分数，从而帮助建立对他们用于决策的数据的信任。

先决条件和 IAM 角色变更

如果您使用的是Amazon DataZone 的 AWS 托管策略，则无需执行其他配置步骤，并且这些托管策略会自动更新以支持数据质量。如果您对角色使用自己的策略来授予 Amazon DataZone 与支持的服务互操作所需的权限，则必须更新附加到这些角色的策略，以支持读取中的 AWS Glue 数据质量信息，AWS 托管策略：AmazonDataZoneGlueManageAccessRolePolicy并启用对AWS 托管策略：AmazonDataZoneDomainExecutionRolePolicy和中的时间序列 API 的支持。AWS 托管策略：AmazonDataZoneFullUserAccess

为 AWS Glue 资产启用数据质量

亚马逊从 AWS G DataZone lue 中提取数据质量指标是为了提供某一时间点的背景信息，例如在搜索业务数据目录期间。数据用户可以看到其订阅资产的数据质量指标如何随着时间的推移而变化。数据生成者可以按计划获 AWS 取 Glue 数据质量分数。亚马逊 DataZone 企业数据目录还可以通过数据质量 API 显示来自第三方系统的数据质量指标。有关更多信息，请参阅 AWS Glue 数据质量和数据目录的 AWS Glue 数据质量入门。

您可以通过以下方式为您的 Amazon DataZone 资产启用数据质量指标：

- 在创建新的 AWS Glue 数据源或编辑现有 Glue 数据源时，使用数据门户或 Amazon DataZone API 通过亚马逊 DataZone 数据门户启用 AWS Glue 数据源的数据质量。

  有关通过门户为数据源启用数据质量的更多信息，请参阅为创建并运行 Amazon DataZone 数据源 AWS Glue Data Catalog和管理现有的 Amazon DataZone 数据源。

  > **Note**
  >
  > 您可以使用数据门户仅为 AWS Glue 库存资产启用数据质量。在此版本的 Amazon 中，不支持通过数据门户为 Amazon Redshift 或自定义类型资产 DataZone 启用数据质量。

您还可以使用 API 为新的或现有的数据源启用数据质量。为此，您可以调用CreateDataSource或UpdateDataSource并将autoImportDataQualityResult参数设置为“True”。

启用数据质量后，您可以按需或按计划运行数据源。每次运行最多可以为每项资产引入 100 个指标。使用数据源来提高数据质量时，无需手动创建表单或添加指标。资产发布后，对数据质量表单所做的更新（每条历史规则最多 30 个数据点）将反映在面向消费者的清单中。随后，资产中每增加一个新的指标，都会自动添加到列表中。无需重新发布该资产即可向消费者提供最新的分数。

为自定义资产类型启用数据质量

您可以使用 Amazon DataZone API 为您的任何自定义类型资产启用数据质量。有关更多信息，请参阅下列内容：

- PostTimeSeriesDataPoints
- ListTimeSeriesDataPoints
- GetTimeSeriesDataPoint
- DeleteTimeSeriesDataPoints

以下步骤提供了使用 API 或 CLI 在亚马逊中为您的资产导入第三方指标的示例 DataZone：

1. 按如下方式调用 PostTimeSeriesDataPoints API：

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

有效载荷如下：

```
"domainId": "dzd_5oo7xzoqltu8mf",
    "entityId": "4wyh64k2n8czaf",
    "entityType": "ASSET",
    "form": {
        "content": "{\n  \"evaluations\" : [ {\n    \"types\" : [ \"MaximumLength
\" ],\n    \"description\" : \"ColumnLength \\\"ShippingCountry\\\" <= 6\",\n
```

```
   \"details\" : { },\n    \"applicableFields\" : [ \"ShippingCountry\" ],\n
   \"status\" : \"PASS\"\n  }, {\n    \"types\" : [ \"MaximumLength\" ],\n
 \"description\" : \"ColumnLength \\\"ShippingState\\\" <= 2\",\n    \"details
\" : { },\n    \"applicableFields\" : [ \"ShippingState\" ],\n    \"status\" :
 \"PASS\"\n  }, {\n    \"types\" : [ \"MaximumLength\" ],\n    \"description
\" : \"ColumnLength \\\"ShippingCity\\\" <= 8\",\n    \"details\" : { },\n
 \"applicableFields\" : [ \"ShippingCity\" ],\n    \"status\" : \"PASS\"\n  },
 {\n    \"types\" : [ \"Completeness\" ],\n    \"description\" : \"Completeness \
\\"ShippingStreet\\\" >= 0.59\",\n    \"details\" : { },\n    \"applicableFields
\" : [ \"ShippingStreet\" ],\n    \"status\" : \"PASS\"\n  }, {\n    \"types\" :
 [ \"MaximumLength\" ],\n    \"description\" : \"ColumnLength \\\"ShippingStreet\\
\" <= 101\",\n    \"details\" : { },\n    \"applicableFields\" : [ \"ShippingStreet
\" ],\n    \"status\" : \"PASS\"\n  }, {\n    \"types\" : [ \"MaximumLength\" ],\n
    \"description\" : \"ColumnLength \\\"BillingCountry\\\" <= 6\",\n    \"details
\" : { },\n    \"applicableFields\" : [ \"BillingCountry\" ],\n    \"status\" :
 \"PASS\"\n  }, {\n    \"types\" : [ \"Completeness\" ],\n    \"description\" :
 \"Completeness \\\"biLlingcountry\\\" >= 0.5\",\n    \"details\" : {\n
 \"EVALUATION_MESSAGE\" : \"Value: 0.26666666666666666 does not meet the constraint
 requirement!\"\n    },\n    \"applicableFields\" : [ \"biLlingcountry\" ],\n
   \"status\" : \"FAIL\"\n  }, {\n    \"types\" : [ \"Completeness\" ],\n
 \"description\" : \"Completeness \\\"Billingstreet\\\" >= 0.5\",\n    \"details
\" : { },\n    \"applicableFields\" : [ \"Billingstreet\" ],\n    \"status\" :
 \"PASS\"\n  } ],\n  \"passingPercentage\" : 88.0,\n  \"evaluationsCount\" : 8\n}",
        "formName": "shortschemaruleset",
        "id": "athp9dyw75gzhj",
        "timestamp": 1.71700477757E9,
        "typeIdentifier": "amazon.datazone.DataQualityResultFormType",
        "typeRevision": "8"
    },
    "formName": "shortschemaruleset"
}
```

您可以通过调用以下GetFormType操作来获取此有效负载：

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

2. 按如下方式调用 DeleteTimeSeriesDataPoints API：

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

使用机器学习和生成式 AI

> **Note**
>
> 由 Amazon Bedrock 提供支持： AWS 实现自动滥用检测。由于亚马逊中关于描述功能的人工智能建议 DataZone 是建立在 Amazon Bedrock 之上的，因此用户继承了 Amazon Bedrock 中实施的控制措施，以强制执行安全、安保和负责任地使用人工智能。

在当前版本的 Amazon 中 DataZone，您可以使用 AI 推荐描述功能来自动发现和编目数据。Amazon 对生成式 AI 和机器学习的支持为资产和列 DataZone 创建了描述。您可以使用这些描述为数据添加业务背景并推荐数据集的分析，这有助于提高数据发现结果。

在 Amazon Bedrock 的大型语言模型的支持下，Amazon 中针对数据资产描述的人工智能建议可 DataZone 帮助您确保您的数据易于理解且易于发现。人工智能的建议还为数据集提供了最相关的分析应用程序。通过减少手动记录任务并就适当的数据使用提出建议，自动生成的描述可以帮助您增强数据的可信度，最大限度地减少对宝贵数据的忽视，从而加快做出明智的决策。

> **Important**
>
> 在当前的 Amazon DataZone 版本中，仅以下区域支持 AI 推荐描述功能：
>
> - 美国东部（弗吉尼亚州北部）
> - 美国西部（俄勒冈州）
> - 欧洲地区（法兰克福）
> - Asia Pacific (Tokyo)

以下过程介绍如何为亚马逊中的描述生成 AI 推荐 DataZone：

1. 导航到亚马逊 DataZone 数据门户 URL，然后使用单点登录 (SSO) 或您的 AWS 凭证登录。如果您是亚马逊 DataZone 管理员，请导航至亚马逊 DataZone 控制台 https://console.aws.amazon.com/datazone 并使用域名创建 AWS 账户 地登录，然后选择打开数据门户。
2. 在顶部导航窗格中，选择 Selec t project，然后选择包含要为其生成 AI 推荐以进行描述的资产的项目。
3. 导航到项目的 “数据” 选项卡。
4. 在左侧导航窗格中，选择库存数据，然后选择要为其生成 AI 推荐的资产名称，以供资产描述使用。
5. 在资产的详细信息页面的业务元数据选项卡中，选择生成描述。
6. 描述生成后，您可以编辑、接受或拒绝描述。每个自动生成的数据资产元数据描述旁边都显示绿色图标。在业务元数据选项卡中，您可以选择自动生成的摘要旁边的绿色图标，然后选择编辑、接受或拒绝来处理生成的描述。您也可以选择 “全部接受” 或 “全部拒绝” 选项，这些选项在选择业务元数据选项卡时显示在页面顶部，从而对所有自动生成的描述执行选定的操作。

   或者，您可以选择 “架构” 选项卡，然后通过一次为一列描述选择绿色图标，然后选择 “接受” 或 “拒绝” 来逐个处理自动生成的描述。在 “架构” 选项卡中，您也可以选择 “全部接受” 或 “全部拒绝”，从而对所有自动生成的描述执行所选操作。
7. 要将资源与生成的描述一起发布到目录中，请选择 “发布资源”，然后在 “发布资源” 弹出窗口中再次选择 “发布资源”，确认此操作。

> **Note**
>
> 如果您不接受或拒绝为某项资产生成的描述，然后发布该资产，则此未经审核的自动生成的元数据将不会包含在已发布的数据资产中。

Amazon 中的数据谱系 DataZone （预览版）

> **Important**
>
> 目前，Amazon 中的数据谱系功能 DataZone 处于预览版中。

Amazon 中的数据沿袭 DataZone 是一项 API 驱动的、 OpenLineage兼容的功能，可帮助您从 OpenLineage支持系统的系统或通过 API 捕获和可视化世系事件，从而跟踪数据来源、跟踪转换和查

看跨组织的数据消耗情况。它为您提供了对数据资产的总体视图，以查看资产的来源及其连接链。世系数据包括有关亚马逊 DataZone业务数据目录内活动的信息，包括有关编目资产、这些资产的订阅者以及使用 API 以编程方式捕获的业务数据目录之外发生的活动的信息。

使用与亚马逊 DataZone OpenLineage兼容的 API，域管理员和数据创建者可以捕获和存储超出亚马逊可用范围的世系事件 DataZone，包括 Amazon S3、G AWS lue 和其他服务中的转换。这为数据使用者提供了全面的视图，并帮助他们获得对资产来源的信心，而数据生产者则可以通过了解资产的使用情况来评估资产变化的影响。此外，Amazon DataZone 版本与每个事件保持一致，使用户能够在任何时间点可视化血统或比较资产或任务历史的转换。这种历史沿袭可以更深入地了解数据是如何演变的，这对于故障排除、审计和确保数据资产的完整性至关重要。

借助数据沿袭，您可以在 Amazon DataZone 中完成以下任务：

- 了解数据的来源：通过了解数据的来源、依赖关系和转换，您可以清楚地了解数据的来源、依赖关系和转换，从而增强人们对数据的信任。这种透明度有助于做出自信的数据驱动型决策。
- 了解数据管道变更的影响：当对数据管道进行更改时，可以使用世系来识别将受到影响的所有下游消费者。这有助于确保在不中断关键数据流的情况下进行更改。
- 确定数据质量问题的根本原因：如果在下游报告中检测到数据质量问题，则可以使用世系（尤其是列级谱系）来追溯数据（在列级别），以将问题追溯到其根源。这可以帮助数据工程师识别和修复问题。
- 改善数据治理和合规性：列级谱系可用于证明遵守数据治理和隐私法规。例如，列级谱系可用于显示敏感数据（例如 PII）的存储位置以及下游活动中的处理方式。

Amazon 中的血统节点类型 DataZone

在 Amazon 中 DataZone，数据谱系信息显示在代表表和视图的节点中。根据项目的上下文，例如在数据门户网站左上角选择的项目，制作者可以同时查看库存和已发布的资产，而消费者只能查看已发布的资产。首次在资产详细信息页面中打开世系选项卡时，编目数据集节点是通过谱系图的谱系节点向上游或下游导航的起点。

以下是 Amazon DataZone 支持的数据血统节点类型：

- 数据集节点-此节点类型包括有关特定数据资产的数据谱系信息。
  - 包含亚马逊 DataZone 目录中发布的 AWS Glue 或 Amazon Redshift 资产相关信息的数据集节点是自动生成的，节点中包含相应的 G AWS lue 或 Amazon Redshift 图标。
  - 包含未在 Amazon DataZone 目录中发布的资产信息的数据集节点由域管理员（制作者）手动创建，并由节点内的默认自定义资产图标表示。

- Job (run) 节点-此节点类型显示作业的详细信息，包括特定作业的最新运行情况和运行细节。此节点还会捕获任务的多次运行，可以在节点详细信息的 “历史记录” 选项卡中查看。您可以通过选择节点图标来查看节点的详细信息。

世系节点中的关键属性

世系节点中的sourceIdentifier属性表示数据集中发生的事件。世系节点sourceIdentifier的标识符是数据集的标识符（表/视图等）。它用于在血统节点上强制执行唯一性。例如，不能有两个血统节点具有相同的sourceIdentifier血统节点。以下是不同类型节点的sourceIdentifier值示例：

- 对于具有相应数据集类型的数据集节点：
  - 资产：amazone.datazone.asset/ <assetId>
  - 清单（已发布资产）：amazone.datazone.listing/ <listingId>
  - AWS <region><account-id><database>Glue table：arn: aws: glue:: table//<table-name>
  - <redshift/redshift-serverless> <region><account-id><table-type (table/view etc) ><clusterIdentifier/workgroupName> <database><schema>亚马逊 Redshift table/view：arn: aws::::: ::////<table-name>
  - 对于使用 open-lineage 运行事件导入的任何其他类型的数据集节点，将使用 <namespace><name>该节点的输入/输出数据集的/。sourceIdentifier
- 对于工作：
  - <jobs_namespace>对于使用 open-lineage 运行事件导入的作业节点，. <job_name>用作源标识符。
- 对于任务运行：
  - <jobs_namespace>对于使用 open-lineage 运行事件导入的作业运行节点，. <job_name>/ <run_id>用作源标识符。

对于使用 createAsset API 创建的资产，sourceIdentifier必须使用 createAssetRevision API 进行更新，才能将资产映射到上游资源。

可视化数据沿袭

Amazon DataZone 的资产详情页面以图形方式呈现数据谱系，便于直观呈现上游或下游的数据关系。资产详细信息页面提供以下功能来浏览图表：

- 列级谱系：如果在数据集节点中可用，则扩展列级谱系。如果源列信息可用，这将自动显示与上游或下游数据集节点的关系。
- 列搜索：当列数的默认显示为 10 时。如果列超过 10 个，则会激活分页以导航到其余列。要快速查看特定列，可以在仅列出搜索列的数据集节点上进行搜索。
- 仅查看数据集节点：如果要切换为仅查看数据集谱系节点并筛选出作业节点，则可以选择图表查看器左上角的打开视图控件图标，然后切换仅显示数据集节点选项。这将从图表中移除所有任务节点，并允许您仅浏览数据集节点。请注意，当开启仅视图数据集节点时，图表无法向上游或下游展开。
- 详细信息窗格：选中每个世系节点后，都会捕获并显示详细信息。
  - 数据集节点有一个详细信息窗格，用于显示在给定时间戳内为该节点捕获的所有详细信息。每个数据集节点都有 3 个选项卡，即：“世系信息”、“架构” 和 “历史记录” 选项卡。历史选项卡列出了为该节点捕获的血统事件的不同版本。从 API 捕获的所有详细信息均使用元数据表单或 JSON 查看器显示。
  - Job 节点有一个详细信息窗格，用于显示带有选项卡的作业详细信息，即：作业信息和历史记录。详细信息窗格还会捕获在作业运行过程中捕获的查询或表达式。“历史记录” 选项卡列出了为该作业捕获的不同版本的作业运行事件。从 API 捕获的所有详细信息均使用元数据表单或 JSON 查看器显示。
- 版本选项卡：Amazon DataZone 数据谱系中的所有世系节点都有版本控制。对于每个数据集节点或作业节点，版本都被捕获为历史记录，这使您能够在不同的版本之间导航，以确定随着时间的推移发生了哪些变化。每个版本都会在世系页面中打开一个新选项卡，以帮助比较或对比。

Amazon 中的数据沿袭授权 DataZone

写入权限-要将世系数据发布到 Amazon DataZone，您必须拥有一个 IAM 角色，其权限策略包括对 `PostLineageEvent` API 的`ALLOW`操作。此 IAM 授权发生在 API Gateway 层。

读取权限-有两个操作：`GetLineageNode`和`ListLineageNodeHistory`包含在`AmazonDataZoneDomainExecutionRolePolicy`托管策略中，因此 Amazon DataZone 域中的每个用户都可以调用这些操作来遍历数据谱系图。

Amazon 中的数据沿袭示例体验 DataZone

您可以使用数据沿袭示例体验来浏览和了解 Amazon 中的数据谱系 DataZone，包括在数据谱系图中遍历上游或下游、探索版本和列级谱系。

完成以下步骤，在 Amazon 中试用示例数据谱系体验： DataZone

1. 导航至 Amazon DataZone 数据门户 URL，然后使用单点登录 (SSO) 或凭证登录 AWS 。如果您是亚马逊 DataZone管理员，则可以通过 https://console.aws.amazon.com/datazone 导航到亚马逊 DataZone 控制台，使用域名创建 AWS 账户 地登录，然后选择打开数据门户。
2. 选择任何可用的数据资产以打开资产的详细信息页面。
3. 在资产的详细信息页面上，选择 “世系” 选项卡，然后选择 “预览”，然后选择 “尝试样本世系”。
4. 在数据谱系弹出窗口中，选择开始引导式数据谱系之旅。

   此时，将显示一个提供血统信息的所有空间的全屏选项卡。样本数据谱系图最初显示的是两端（上游和下游）都有一个深度为 1 的基本节点。您可以将图表扩展到上游或下游。列信息也可供您选择，并查看血统如何流经节点。

以编程方式使用 Amazon DataZone 数据谱系

要在 Amazon 中使用数据血统功能 DataZone，您可以调用以下 API：

- GetLineageNode
- ListLineageNodeHistory
- PostLineageEvent

在 Amazon 中发现、订阅和使用数据 DataZone

在 Amazon 中 DataZone，一旦资产发布到某个域名，订阅者就可以发现该资产并请求订阅该资产。订阅过程始于订阅者搜索并浏览目录以找到他们想要的资产。在亚马逊 DataZone门户网站上，他们选择通过提交包含申请理由和理由的订阅请求来订阅资产。然后，根据发布协议中的定义，订阅批准者会审查访问请求。他们可以批准或拒绝请求。

授予订阅后，将开始履行流程，以方便订阅者访问资产。有两种主要的资产访问控制和配送模式：亚马逊管理的资产和非亚马逊 DataZone管理的资产的访问控制和配送模式。 DataZone

- 托管资产 — 亚马逊 DataZone 可以管理托管资产的配送和权限，例如 AWS Glue 表格和 Amazon Redshift 表格和视图。
- 非托管资产 — 亚马逊向亚马逊 DataZone 发布与您的操作相关的标准事件（例如，批准订阅请求）。 EventBridge您可以使用这些标准事件与其他 AWS 服务或第三方解决方案集成，以实现自定义集成。

主题

发现数据

以下任务描述了在 Amazon 中发现数据的各种方法 DataZone。

主题

在目录中搜索和查看资产

Amazon DataZone 提供了一种简化的数据搜索方式。任何有权访问数据门户的亚马逊 DataZone 用户都可以在亚马逊 DataZone目录中搜索资产，并查看资产名称和分配给他们的元数据。您可以通过查看其详细信息页面来仔细查看资产。

> **Note**
>
> 要查看资产包含的实际数据，您必须先订阅该资产，并批准您的订阅请求并授予访问权限。有关更多信息，请参阅 订阅数据。

在目录中搜索资产

1. 导航至 Amazon DataZone 数据门户 URL，然后使用单点登录 (SSO) 或凭证登录 AWS 。如果您是亚马逊 DataZone管理员，则可以通过 https://console.aws.amazon.com/datazone 导航到亚马逊 DataZone 控制台，使用域名创建 AWS 账户 地登录，然后选择打开数据门户。
2. 您可以在数据门户主页的搜索栏中键入要查找的资产的名称。
3. 要浏览命名空间，请从页面右上角选择目录以打开目录。该目录提供了一种分面搜索体验，您可以通过搜索诸如数据所有者和词汇表术语之类的条件来查找资产。
4. 在其中一个搜索框中输入您的搜索词。运行搜索后，您可以应用各种筛选器来缩小结果范围。筛选条件包括资产类型、来源账户和资产 AWS 区域 所属账户。
5. 要查看特定资产的详细信息，请选择该资产以打开其详细信息页面。详细信息页面包含以下信息：
   - 资产名称、数据源（AWS Glue Amazon Redshift 或 Amazon S3）、类型（表、视图或 S3 对象）、列数和大小。
   - 对资产的描述。
   - 当前发布的资源修订版、所有者、订阅是否需要批准、命名空间和更新历史记录。
   - “概述” 选项卡，包括词汇表术语和元数据表单。
   - 一个 “架构” 选项卡，显示资产的架构，包括列的业务和技术列名称、数据类型和业务描述。架构选项卡仅对表和视图可见（Amazon S3 对象不可见）。
   - “订阅” 选项卡，其中包含该域的订阅者列表。
   - “历史记录” 选项卡，其中包含资产过去修订的列表。

订阅数据

以下任务提供了有关在 Amazon DataZone 中订阅资产的详细信息。

主题

- 申请订阅资产
- 批准或拒绝订阅请求

- 撤销现有订阅
- 取消订阅请求
- 取消订阅资产
- 使用现有 IAM 角色完成亚马逊 DataZone订阅

申请订阅资产

亚马逊 DataZone 允许您查找、访问和使用亚马逊 DataZone目录中的资产。当您在目录中找到要访问的资产时，需要订阅该资产，这将创建订阅请求。然后，批准者可以批准或请求您的请求。

您必须是项目成员才能申请订阅该项目中的资产。

订阅资产

1. 导航至 Amazon DataZone 数据门户 URL，然后使用单点登录 (SSO) 或凭证登录 AWS 。如果您是亚马逊 DataZone管理员，则可以通过 https://console.aws.amazon.com/datazone 导航到亚马逊 DataZone 控制台，使用域名创建 AWS 账户 地登录，然后选择打开数据门户。
2. 使用搜索栏搜索并选择要订阅的资产，然后选择 “订阅”。
3. 在 “订阅” 弹出窗口中，提供以下信息：
   - 您要订阅资产的项目。
   - 申请订阅的简短理由。
4. 选择订阅。

   当发布者批准您的请求时，您会在数据门户中收到通知。

要查看订阅请求的状态，请找到并选择您订阅该资产的项目。导航至项目的 “数据” 选项卡，然后从左侧导航窗格中选择 “请求的数据”。此页面列出了项目已请求访问的资产。您可以按请求状态筛选列表。

批准或拒绝订阅请求

亚马逊 DataZone 允许您查找、访问和使用亚马逊 DataZone目录中的资产。当您在目录中找到要访问的资产时，必须订阅该资产，这会创建订阅请求。然后，批准者可以批准或拒绝您的请求。

您必须是所属项目（发布资产的项目）的成员，才能批准或拒绝订阅请求。

批准或拒绝订阅请求

1. 导航至 Amazon DataZone 数据门户 URL，然后使用单点登录 (SSO) 或凭证登录 AWS 。如果您是亚马逊 DataZone管理员，则可以通过 https://console.aws.amazon.com/datazone 导航到亚马逊 DataZone 控制台，使用域名创建 AWS 账户 地登录，然后选择打开数据门户。
2. 在数据门户中，选择 “浏览项目列表”，然后选择包含订阅请求的资产的项目。
3. 导航至 “数据” 选项卡，然后从左侧导航窗格中选择 “传入请求”。
4. 找到请求并选择查看请求。您可以按 “待处理” 进行筛选，以仅查看仍处于打开状态的请求。
5. 查看订阅请求和访问原因，然后决定是批准还是拒绝。
6. （可选）输入回复，说明您接受或拒绝请求的原因。
7. 选择 “批准” 或 “拒绝”。

作为项目所有者，您可以随时撤销订阅。有关更多信息，请参阅 the section called “撤销现有订阅”。

要查看所有订阅请求，请参阅处理 Amazon DataZone 事件和通知。

撤销现有订阅

亚马逊 DataZone 允许您查找、访问和使用亚马逊 DataZone目录中的资产。当您在目录中找到要访问的资产时，需要订阅该资产，这将创建订阅请求。然后，批准者可以批准或请求您的请求。在批准订阅后，您可能需要撤销订阅，这要么是因为批准有误，要么是因为订阅者不再需要访问该资产。

您必须是所属项目（发布资产的项目）的成员才能撤销订阅。

撤销订阅

1. 导航至 Amazon DataZone 数据门户 URL，然后使用单点登录 (SSO) 或凭证登录 AWS 。如果您是亚马逊 DataZone管理员，则可以通过 https://console.aws.amazon.com/datazone 导航到亚马逊 DataZone 控制台，使用域名创建 AWS 账户 地登录，然后选择打开数据门户。
2. 从顶部导航窗格中选择 “选择项目”，然后选择包含要撤消的订阅的项目。
3. 导航至 “数据” 选项卡，然后从左侧导航窗格中选择 “传入请求”。
4. 找到您要撤销的订阅，然后选择查看订阅。
5. （可选）启用该复选框以允许订阅者将资产保留在项目的订阅目标中。订阅目标是对一组资源的引用，在这些资源中，订阅的数据可以在环境中使用。

   如果您想稍后撤消订阅目标对资产的访问权限，则必须在中 AWS Lake Formation执行此操作。
6. 选择 “撤消订阅”。

撤销订阅后，您无法重新批准该订阅。订阅者必须再次订阅该资产，您才能批准该资产。

取消订阅请求

亚马逊 DataZone 允许您查找、访问和使用亚马逊 DataZone目录中的资产。当您在目录中找到要访问的资产时，需要订阅该资产，这将创建订阅请求。然后，批准者可以批准或请求您的请求。您可能需要取消待处理的订阅请求，这可能是因为您错误地提交了该请求，或者因为您不再需要对该资产的读取权限。

要取消订阅请求，您必须是项目所有者或贡献者。

取消订阅请求

1. 导航至 Amazon DataZone 数据门户 URL，然后使用单点登录 (SSO) 或凭证登录 AWS 。如果您是亚马逊 DataZone管理员，则可以通过 https://console.aws.amazon.com/datazone 导航到亚马逊 DataZone 控制台，使用域名创建 AWS 账户 地登录，然后选择打开数据门户。
2. 从顶部导航窗格中选择 “选择项目”，然后选择包含订阅请求的项目。
3. 导航至项目的 “数据” 选项卡，然后从左侧导航窗格中选择 “请求的数据”。此页面列出了项目已请求访问的资产。
4. 按 “已请求” 筛选，仅查看仍处于待处理状态的请求。找到请求并选择查看请求。
5. 查看订阅请求并选择取消申请。

如果您想重新订阅该资产（或其他资产），请参阅the section called “申请订阅资产”。

取消订阅资产

亚马逊 DataZone 允许您查找、访问和使用亚马逊 DataZone目录中的资产。当您在目录中找到要访问的资产时，需要订阅该资产，这将创建订阅请求。然后，批准者可以批准或请求您的请求。您可能需要取消订阅某项资产，这要么是因为您错误订阅并获得了批准，要么是因为您不再需要对该资产的读取权限。

您必须是项目成员才能取消订阅其中一项资产。

取消订阅资产

1. 导航至 Amazon DataZone 数据门户 URL，然后使用单点登录 (SSO) 或凭证登录 AWS 。如果您是亚马逊 DataZone管理员，则可以通过 https://console.aws.amazon.com/datazone 导航到亚马逊 DataZone 控制台，使用域名创建 AWS 账户 地登录，然后选择打开数据门户。
2. 从顶部导航窗格中选择 “选择项目”，然后选择包含要取消订阅的资源的项目。

3. 导航至项目的 “数据” 选项卡，然后从左侧导航窗格中选择 “请求的数据”。此页面列出了项目已请求访问的资产。
4. 按 “已批准” 筛选，仅查看已批准的请求。找到请求并选择查看订阅。
5. 查看订阅并选择取消订阅。

如果您想重新订阅该资产（或其他资产），请参阅the section called “申请订阅资产”。

使用现有 IAM 角色完成亚马逊 DataZone订阅

在当前版本中，Amazon DataZone 支持您使用现有的 IAM 角色来访问数据。为此，您可以在 Amazon DataZone 环境中创建用于完成订阅的订阅目标。要在其中一个关联 AWS 账户中为环境创建订阅目标，可以使用以下步骤：

第 1 步：确保您的 Amazon DataZone 域名使用的是 RAM 策略的版本 2 或更高版本

1. 在 AWS RAM 控制台中导航到 “我共享：资源共享” 页面。
2. 由于 AWS RAM 资源共享存在于特定 AWS 区域中，因此请从控制台右上角的下拉列表中选择相应的 AWS 区域。
3. 选择与您的 Amazon DataZone 域名对应的资源共享，然后选择修改。您可以使用域名的名称或 ID 来识别 Amazon DataZone 域的 RAM 共享，因为创建的 RAM 共享名为:`DataZone-<domain-name>-<domain-id>`。
4. 选择 “下一步” 继续下一步，在此可以检查 RAM 策略的版本并对其进行修改。
5. 确保 RAM 策略的版本为版本 2 或更高版本。如果不是，请使用下拉列表选择版本 2 或更高版本。
6. 选择 “跳至步骤 4：查看和更新”。
7. 选择 “更新资源共享”。

步骤 2：通过关联账户创建订阅目标

- 在当前版本中，Amazon 仅 DataZone 支持使用 API 创建订阅目标。以下是一些有效负载示例，您可以用来创建订阅目标，以满足您的 AWS Glue 表格和 Amazon Redshift 表或视图的订阅。有关更多信息，请参阅CreateSubscriptionTarget。

  AWS Glue 的订阅目标示例

```
{
        "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"
}
```

亚马逊 Redshift 的订阅目标示例：

```
{
        "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

- 您在上述 API 调用中使用的 environmentIdentifier 应存在于您发出 API 调用的同一个关联账户中。否则，API 调用将无法成功。
- 您在 “AuthorizedPrincipals” 中使用的 IAM 角色 ARN 是在订阅资产添加到订阅目标后，亚马逊 DataZone 将向其授予访问权限的角色。这些授权委托人必须与创建订阅目标的环境属于同一个账户。

- 供应商字段的值必须为 “Amazon DataZone” DataZone ，亚马逊才能完成订阅配送。
- 中提供的数据库名称 subscriptionTargetConfig 应该已经存在于创建目标的账户中。亚马逊 DataZone 不会创建此数据库。还要确保管理访问角色对此数据库拥有 CREATE TABLE 权限。
- 此外，请确保作为授权委托人提供的角色（ AWS Glue 的 IAM 角色和 Amazon Redshift 的数据库角色）已存在于环境账户中。对于 Amazon Redshift 订阅目标，在连接到集群时需要对所担任的角色进行额外更新。此角色必须为该角色附加 RedshiftDbRoles 标签。标签的值可以是逗号分隔的列表。该值应是创建订阅目标时作为授权主体提供的数据库角色。

第 3 步：订阅新表格并完成对新目标的订阅

- 创建订阅目标后，您可以订阅新表，Amazon DataZone 会将其实现上述目标。有关更多信息，请参阅 订阅数据。

授予数据访问权限

以下任务详细介绍了如何向已批准的亚马逊资产订阅授予访问权限 DataZone。

在 Amazon 中 DataZone，订阅请求以及已批准或授予的资产读取权限订阅由订阅批准者管理。某项资产的订阅批准者由该资产发布到 Amazon DataZone 目录的发布协议确定。

主题

- 授予对托管 AWS Glue Data Catalog 资产的访问权限
- 授予对受管理的亚马逊 Redshift 资产的访问权限
- 为已批准的非托管资产的订阅授予访问权限

授予对托管 AWS Glue Data Catalog 资产的访问权限

> **Note**
>
> 不支持使用 AWS Lake Formation LF-TBAC 方法对 AWS Glue Data Catalog 资产进行访问管理。
> 不支持跨区域共享中的 AWS Glue Data Catalog 资产。

托管 AWS Glue Data Catalog 资产的订阅请求获得批准后，Amazon DataZone 会自动将这些资产添加到项目中的所有现有数据湖环境中。 DataZone 然后，Amazon 会代表您通过授予并管理对已批准 AWS Glue Data Catalog 表格的访问权限 AWS Lake Formation。对于订阅者项目，授予的资产将 AWS Glue Data Catalog 作为您账户中的资源显示在中。然后，您可以使用 Amazon Athena 来查询这些表。

> **Note**
>
> 如果在已订阅的 AWS Glue Data Catalog 资产自动添加到现有数据湖环境后向项目中添加了新的数据湖环境，则必须手动将这些订阅的 AWS Glue Data Catalog 资产添加到这个新的数据湖环境中。为此，您可以在 Amazon DataZone 数据门户中项目概述页面的 “数据” 选项卡中选择 “添加授权” 选项。

为了 DataZone 使亚马逊能够授予对 G AWS lue 数据目录表的访问权限，必须满足以下条件。

- Glue AWS 表必须由 Lake Formation 管理，因为亚马逊通过管理 Lake Formation 权限来 DataZone 授予访问权限。
- 用于发布 AWS Glue 数据目录表的数据湖环境的管理访问角色必须具有以下 Lake Formation 权限：
  - `DESCRIBE`以及对包含已发布表的 AWS Glue 数据库的`DESCRIBE GRANTABLE`权限。
  - `DESCRIBE`、、`SELECTDESCRIBE GRANTABLE`、Lake Formation 中对已发布表本身的`SELECT GRANTABLE`权限。

有关更多信息，请参阅《AWS Lake Formation 开发人员指南》中的授予和撤消目录资源的权限。

授予对受管理的亚马逊 Redshift 资产的访问权限

当对 Amazon Redshift 表或视图的订阅获得批准后，Amazon DataZone 可以自动将订阅的资产添加到项目内的所有数据仓库环境中，这样项目成员就可以在其环境中使用 Amazon Redshift 查询编辑器链接查询数据。在幕后 DataZone，Amazon在来源和订阅目标之间创建了必要的赠款和数据共享。

根据源数据库（发布者）和目标数据库（订阅服务器）所在的位置，授予访问权限的过程会有所不同。

- 同一个集群，同一个数据库-如果必须在同一个数据库中共享数据，Amazon 会直接 DataZone 授予对源表的权限。
- 同一个集群，不同的数据库-如果数据必须在同一个集群中的两个数据库之间共享，Amazon DataZone 将在目标数据库中创建一个视图并授予对已创建视图的权限。

- 同一账户不同的集群-Amazon DataZone 在源集群和目标集群之间创建数据共享，并在共享表的顶部创建视图。已授予对视图的权限。
- 跨账户-与上面相同，但需要额外的步骤才能在生产者集群端授权跨账户数据共享，还需要另外一个步骤才能关联消费者集群端的数据共享。

> **Note**
>
> 如果在已订阅的 Amazon Redshift 资产自动添加到现有数据仓库环境后向项目添加了新的数据仓库环境，则必须手动将这些订阅的 Amazon Redshift 资产添加到这个新的数据仓库环境中。为此，您可以在 Amazon DataZone 数据门户中项目概述页面的 “数据” 选项卡中选择 “添加授权” 选项。

确保您的发布和订阅亚马逊 Redshift 集群满足亚马逊 Redshift 数据共享的所有要求。有关更多信息，请参阅亚马逊 Redshift 开发者指南。

> **Note**
>
> 亚马逊 DataZone 支持自动授予对亚马逊 Redshift 集群和亚马逊 Redshift 无服务器资产的订阅。
> 不支持使用 Amazon Redshift 进行跨区域数据共享。

> **Note**
>
> 在当前版本中，只有源和目标 Ama DataZone zon Redshift 集群或工作组位于属于同一组织的账户中时，亚马逊才能管理对 Amazon Redshift 表和视图 AWS 的访问权限。 AWS

为已批准的非托管资产的订阅授予访问权限

Amazon DataZone 允许用户在业务数据目录中发布任何类型的资产。对于其中一些资产，Amazon DataZone 可以自动管理访问授权。这些资产称为托管资产，包括 Lake Formation 管理的 G AWS lue 数据目录表以及 Amazon Redshift 表和视图。Amazon DataZone 无法自动授予订阅权限的所有其他资产都称为非托管资产。

Amazon 为您 DataZone 提供了管理非托管资产访问权限的途径。当企业数据目录中某项资产的订阅获得数据所有者的批准后，亚马逊会在您的账户中 EventBridge 在亚马逊上 DataZone 发布一个事件，并在有效载荷中发布所有必要的信息，使您能够在来源和目标之间创建访问授权。当您收到此事件时，您可以触发一个自定义处理程序，该处理程序可以使用事件中的信息来创建必要的授权或权限。授予访问权限后，您可以在 Amazon 上报告和更新订阅状态， DataZone 这样它就可以通知订阅该资产的用户他们可以开始使用该资产。有关更多信息，请参阅 处理 Amazon DataZone 事件和通知。

消费数据

以下任务详细介绍了您在 Amazon DataZone 中订阅的数据的使用情况。

主题

- 在亚马逊 Athena 或亚马逊 Redshift 中查询数据

在亚马逊 Athena 或亚马逊 Redshift 中查询数据

在亚马逊中 DataZone，一旦订阅者可以访问目录中的资产，他们就可以使用 Amazon Athena 或 Amazon Redshift 查询编辑器 v2 使用该资产（查询和分析）。要完成此任务，您必须是项目所有者或贡献者。根据项目中启用的蓝图，亚马逊在数据门户项目页面的右侧窗格中 DataZone 提供指向亚马逊 Athena 和/或 Amazon Redshift 查询编辑器 v2 的链接。

1. 导航至 Amazon DataZone 数据门户 URL，然后使用单点登录 (SSO) 或凭证登录 AWS 。如果您是亚马逊 DataZone管理员，则可以通过 https://console.aws.amazon.com/datazone 导航到亚马逊 DataZone 控制台，使用域名创建 AWS 账户 地登录，然后选择打开数据门户。
2. 在 Amazon DataZone 数据门户中，选择 “浏览项目列表”，然后找到并选择要分析的数据所在的项目。
3. 如果在此项目上启用了数据湖蓝图，则项目主页的右侧面板中将显示指向 Amazon Athena 的链接。

   如果在此项目上启用了数据仓库蓝图，则该项目主页的右侧面板中将显示查询编辑器的链接。

   > **Note**
   >
   > 蓝图是在创建项目的环境配置文件中定义的。

主题

- 使用亚马逊 Athena 查询数据
- 使用 Amazon Redshift 查询数据

使用亚马逊 Athena 查询数据

选择 Amazon Athena 链接，使用项目的身份验证凭证在浏览器的新选项卡中打开 Amazon Athena 查询编辑器。在查询编辑器中，系统会自动选择您正在处理的 Amazon DataZone 项目作为当前工作组。

在 Amazon Athena 查询编辑器中，编写并运行您的查询。一些常见任务包括：

- 查询和分析您订阅的资产
- 创建新表
- 根据外部 S3 存储桶的查询结果 (CTAS) 创建表

查询和分析您订阅的资产

如果 Amazon 未自动授予您项目订阅的资产的访问权限 DataZone，则必须授权您访问基础数据。有关如何授予对这些资产的访问权限的更多信息，请参阅为已批准的非托管资产的订阅授予访问权限。

如果亚马逊自动授予您项目订阅的资产的访问权限 DataZone，则可以对表运行 SQL 查询并在 Amazon Athena 中查看结果。有关在 Amazon Athena 中使用 SQL 的更多信息，请参阅 Athena 的 SQL 参考资料。

当您在项目主页的右侧面板中选择亚马逊 Athena 链接后导航到 Amazon Athena 查询编辑器时，Amazon Athena 查询编辑器的右上角会显示一个项目下拉列表，并自动选择您的项目上下文。

您可以在 “数据库” 下拉列表中看到以下数据库：

- 发布数据库 (*{environmentname}*_pub_db)。该数据库的目的是为您提供一个环境，让您可以在项目背景下生成新数据，然后将这些数据发布到 Amazon DataZone 目录中。项目所有者和贡献者拥有对该数据库的读写权限。项目查看者只能对该数据库具有读取权限。
- 订阅数据库 (*{environmentname}*_sub_db)。该数据库的目的是与您共享您作为项目成员在 Amazon DataZone 目录中订阅的数据，并使您能够查询这些数据。

创建新表

如果您已连接到外部 S3 存储桶，则可以使用 Amazon Athena 查询和分析来自外部 Amazon S3 存储桶的资产。在这种情况下，亚马逊 DataZone 无权直接授予对外部 Amazon S3 存储桶中基础数据的

访问权限，并且在项目外部创建的外部 Amazon S3 数据不会在 Lake Formation 中自动管理，也无法由亚马逊管理 DataZone。另一种方法是使用 Amazon Athena 中的语句将数据从外部 Amazon S3 存储桶复制到项目的 Amazon S3 存储桶内的新CREATE TABLE表中。当你在 Amazon Athena 中运行CREATE TABLE查询时，你需要向注册表。 AWS Glue Data Catalog

要在 Amazon S3 中指定数据的路径，请使用 LOCATION 属性，如以下示例中所示：

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

有关更多信息，请参阅 Amazon S3 中的表格位置。

根据外部 S3 存储桶的查询结果 (CTAS) 创建表

当您订阅资产时，对基础数据的访问权限是只读的。您可以使用 Amazon Athena 来创建表格的副本。在 Amazon Athena 中A CREATE TABLE AS SELECT （CTAS），查询根据另一个查询的语句结果在 Amazon Athena 中创建一个新表。SELECT有关 CTAS 语法的信息，请参阅创建表为。

以下示例通过复制表的所有列来创建表：

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

在同一个示例的下列变化中，您的 SELECT 语句还包括 WHERE 子句。在这种情况下，查询将只从表中选择满足 WHERE 子句的行：

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

以下示例创建运行在其他表的一组列上的新查询：

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

同一个示例的此变化从多个表的特定列创建新表：

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

这些新创建的表现在已成为您项目 AWS Glue 数据库的一部分，通过将数据作为资产发布到亚马逊目录中，可以让其他人发现并与其他亚马逊 DataZone DataZone项目共享。

使用 Amazon Redshift 查询数据

在 Amazon DataZone 数据门户中，打开使用数据仓库蓝图的环境。在环境页面的右侧面板中选择 Amazon Redshift 链接。这将打开一个确认对话框，其中包含必要的详细信息，可帮助您在 Amazon Redshift 查询编辑器 v2.0 中与环境的 Amazon Redshift 集群或亚马逊 Redshift 无服务器工作组建立连接。确定建立连接所需的详细信息后，选择 “打开 Amazon Redshift” 按钮。这将使用亚马逊环境的临时凭证在浏览器的新选项卡中打开 Amazon Redshift 查询编辑器 v2.0。 DataZone

在查询编辑器中，根据您的环境使用的是 Amazon Redshift 无服务器工作组还是亚马逊 Redshift 集群，按照以下步骤进行操作。

适用于 Amazon Redshift 无服务器工作组

1. 在查询编辑器中，识别您的亚马逊 DataZone 环境的 Amazon Redshift Serverless 工作组，右键单击该工作组，然后选择创建连接。
2. 选择联合用户进行身份验证。
3. 提供 Amazon DataZone 环境数据库的名称。
4. 选择创建连接。

对于亚马逊 Redshift 集群：

1. 在查询编辑器中，识别您的亚马逊 DataZone 环境的 Amazon Redshift 集群，右键单击它并选择创建连接。
2. 选择使用您的 IAM 身份进行身份验证的临时证书。
3. 如果上述身份验证方法不可用，请通过选择左下角的齿轮按钮打开账户设置，选择使用 IAM 凭证进行身份验证并保存。这是一个 one-time-only设置。
4. 提供用于创建连接的 Amazon DataZone 环境数据库的名称。
5. 选择创建连接。

现在，您可以开始查询为亚马逊环境配置的 Amazon Redshift 集群或 Amazon Redshift 无服务器工作组中的表和视图。 DataZone

您订阅的任何 Amazon Redshift 表或视图都链接到为该环境配置的亚马逊 Redshift 集群或亚马逊 Redshift 无服务器工作组。您可以订阅表和视图，也可以发布您在环境的集群或数据库中创建的任何新表和视图。

例如，让我们举一个场景，其中一个环境链接到一个名为的 Amazon Redshift 集群，`redshift-cluster-1`而该集群`dev`中有一个名为的数据库。使用 Amazon DataZone 数据门户，您可以查询已添加到您的环境中的表和视图。在数据门户右侧窗格的`Analytics tools`部分下，您可以选择此环境的 Amazon Redshift 链接，这将打开查询编辑器。然后，您可以右键单击`redshift-cluster-1`集群，并使用您的 IAM 身份使用临时证书创建连接。建立连接后，您可以在开发数据库下看到您的环境可以访问的所有表和视图。

处理 Amazon DataZone 事件和通知

Amazon DataZone 会随时通知您数据门户中的重要活动，例如订阅请求、更新、评论和系统事件。亚马逊通过在数据门户的专用收件箱中或通过亚马逊 EventBridge 默认总线传送消息来向您 DataZone 提供这些信息。

主题

通过 Amazon DataZone 数据门户中的专用收件箱处理事件

Amazon在数据门户中 DataZone 提供了一个专用的收件箱，您可以在其中查看消息并对其采取行动。最近的消息还会出现在主页、项目页面和目录页面上。例如，如果用户请求访问某项数据资产，则该资产的发布项目的所有者和贡献者会在数据门户中看到该请求，并且在采取操作后，与该请求相关的订阅项目的项目成员将在数据门户中看到通知。有两种类型的消息：

- 任务-这些消息告知收件人需要在某个地方采取行动。它们有一个可选的状态字段，你可以用它来跟踪。
- 事件-这些消息仅供参考，没有分配状态。事件提供了最近更新的审计跟踪。

在 Amazon 中 DataZone，会为以下事件类型生成消息：

事件类别	事件名称	事件描述	事件类型
订阅	订阅请求已创建	创建订阅请求时生成事件	任务
订阅	订阅请求已接受	当订阅请求被接受时生成事件	事件
订阅	订阅请求被拒绝	订阅请求被拒绝时生成事件	事件
订阅	订阅请求已删除	删除订阅请求时会生成事件	事件

事件类别	事件名称	事件描述	事件类型
项目	项目创建成功	项目创建成功时生成事件	事件
项目成员资格	成功添加项目成员	向项目添加新成员时会生成事件	事件
项目成员资格	成功移除项目成员	将成员移至项目时生成事件	事件
项目成员资格	项目成员角色更改成功	事件已生成，成员在项目中的角色已更改	事件
环境	环境部署已开始	启动环境部署时会生成事件	事件
环境	环境部署已完成	环境部署成功完成时生成事件	事件
环境	环境部署失败	环境部署失败时会生成事件	事件
环境	环境部署自定义工作流程已启动	启动具有自定义工作流程的环境时会生成事件	事件
数据资产	资产已添加到库存	将新的数据资产添加到清单（即在草稿状态下添加到目录中）时生成事件	事件
数据资产	已发布资产	在发布新的数据资产（即可供订阅）时生成事件	事件
数据资产	资产架构已更改	自上次摄取任务以来，当资产架构发生变化时会生成事件	事件

事件类别	事件名称	事件描述	事件类型
订阅	订阅已创建	当有人请求订阅数据资产时会生成事件	任务
订阅	订阅已批准	当发布的项目所有者或贡献者批准订阅时，就会生成事件	事件
订阅	订阅被拒绝	当发布的项目所有者或贡献者拒绝订阅时，就会生成事件	事件
订阅	订阅已删除	订阅者取消订阅时生成事件	事件
订阅	已申请订阅资助	当有人请求访问资产时会生成事件	事件
订阅	订阅授权已完成	当发布的项目所有者或贡献者向订阅授予对资源的访问权限时，就会生成事件	事件
订阅	订阅授权失败	订阅授权失败时生成事件	事件
订阅	已申请撤销订阅授权	当发布的项目所有者或贡献者启动已撤销的订阅授权时，就会生成事件	事件
订阅	订阅授权撤销已完成	在订阅授权撤销完成时生成事件	事件
订阅	撤销订阅授权失败	撤销订阅授权失败时生成事件	事件

事件类别	事件名称	事件描述	事件类型
自动生成企业名称	公司名称已成功生成	自动生成公司名称的任务成功完成时生成事件	事件
自动生成企业名称	公司名称生成失败	自动生成的公司名称任务失败时生成事件	事件
数据源运行	数据源已创建	创建新数据源时会生成事件	事件
数据源运行	数据源已更新	更新现有数据源时会生成事件	事件
数据源运行	数据源运行已触发	事件是在数据源运行启动时生成的	事件
数据源运行	数据源运行成功	当数据源成功运行时生成事件	事件
数据源运行	数据源运行失败	数据源运行失败时生成事件	事件

要查看数据门户收件箱中的任务，请完成以下步骤：

1. 使用 DataZone 数据门户 URL 导航至 Amazon 数据门户，然后使用您的 SSO 或 AWS 凭证登录。如果您是亚马逊 DataZone 管理员，则可以通过使用创建亚马逊 DataZone 域名的 AWS 账户访问亚马逊 DataZone 控制台 https://console.aws.amazon.com/datazone 来获取数据门户网址。
2. 在数据门户中，要查看包含最近一组任务的弹出窗口，请选择搜索栏旁边的钟形图标。
3. 选择 “查看全部” 以查看所有任务。您可以通过选择 “事件” 选项卡来更改视图并查看所有事件。
4. 您可以按事件主题、活动或非活动状态或日期范围筛选搜索。
5. 选择任何单个任务以导航到您可以响应该任务的位置。

要查看数据门户收件箱中的事件，请完成以下步骤：

1. 使用 DataZone 数据门户 URL 导航至 Amazon 数据门户，然后使用您的 SSO 或 AWS 凭证登录。如果您是亚马逊 DataZone 管理员，则可以在创建亚马逊 DataZone 根域名的 AWS 账户中访问亚马逊 DataZone 控制台 https://console.aws.amazon.com/datazone，获取数据门户网址。
2. 在数据门户中，要查看最近一组事件的弹出窗口，请选择搜索栏旁边的钟形图标。
3. 选择 “查看全部” 以查看所有事件。您可以通过选择 “任务” 选项卡来更改视图并查看所有任务。
4. 按事件主题或日期范围筛选搜索。
5. 选择任何单个事件以导航到可以查看该事件详细信息的位置。

通过 Amazon EventBridge 默认总线处理事件

除了将消息发送到数据门户中的专用收件箱外， DataZone 还可以使用托管亚马逊 DataZone 根域名的同一 AWS 账户将这些消息发送到您的亚马逊 EventBridge 默认事件总线。这可以实现事件驱动的自动化，例如订阅履行或与其他工具的自定义集成。您可以创建与传入的亚马逊 EventBridge 事件相匹配的规则，并将它们发送到亚马逊 EventBridge 目标进行处理。一条规则可以将一个事件发送到多个目标，然后这些目标将可并行运行。

以下是一个示例事件：

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

Ama DataZone zon 支持的详情类型的完整列表包括：

- 订阅请求已创建
- 订阅请求已接受
- 订阅请求被拒绝
- 订阅请求已删除
- 已申请订阅资助
- 订阅拨款已完成
- 订阅授权失败
- 已申请撤销订阅授权
- 订阅授权撤销已完成
- 订阅授权撤销失败
- 资产已添加到库存
- 资产已添加到目录
- 资产架构已更改

- 数据源状态更改
- 数据源已创建
- 数据源已更新
- 数据源运行已触发
- 数据源运行成功
- 数据源运行失败
- 域创建成功
- 域创建失败
- 域删除成功
- 域名删除失败
- 环境部署已启动
- 环境部署已完成
- 环境部署失败
- 环境删除已开始
- 环境删除已完成
- 环境删除失败
- 项目创建成功
- 成功添加项目成员
- 已成功移除项目成员
- 项目成员角色更改成功
- 环境部署客户工作流程已启动
- 成功生成企业名称
- 公司名称生成失败

有关更多信息，请参阅 Amazon EventBridge。

Amazon 的安全 DataZone

云安全 AWS 是重中之重。作为 AWS 客户，您可以受益于专为满足大多数安全敏感型组织的要求而构建的数据中心和网络架构。

安全是双方共同承担 AWS 的责任。责任共担模式将其描述为云的安全性和云中的安全性：

- 云安全 — AWS 负责保护在云中运行 AWS 服务的基础架构 AWS Cloud。 AWS 还为您提供可以安全使用的服务。作为AWS 合规计划合规计划合规计划合的一部分，第三方审计师定期测试和验证我们安全的有效性。要了解适用于亚马逊的合规计划 DataZone，请参阅按合规计划提供的范围内的 AWS 服务按合规计划。
- 云端安全-您的责任由您使用的 AWS 服务决定。您还需要对其他因素负责，包括您的数据的敏感性、您公司的要求以及适用的法律法规。

本文档可帮助您了解在使用 Amazon 时如何应用分担责任模型 DataZone。以下主题向您展示如何配置 Amazon DataZone 以满足您的安全与合规目标。您还将学习如何使用其他 AWS 服务来帮助您监控和保护您的 Amazon DataZone 资源。

主题

- 亚马逊的数据保护 DataZone
- 在 Amazon 中授权 DataZone
- 使用 IAM 控制对亚马逊 DataZone 资源的访问
- Amazon 合规性验证 DataZone
- Amazon 安全最佳实践 DataZone
- Amazon 的弹性 DataZone
- Amazon 的基础设施安全 DataZone
- 亚马逊的跨服务混淆了副手预防 DataZone
- Amazon 的配置和漏洞分析 DataZone

亚马逊的数据保护 DataZone

分 AWS 担责任模式适用于亚马逊的数据保护 DataZone。如本模型所述 AWS ，负责保护运行所有内容的全球基础架构 AWS Cloud。您负责维护对托管在此基础架构上的内容的控制。您还负责您所使用

的 AWS 服务 的安全配置和管理任务。有关数据隐私的更多信息，请参阅数据隐私常见问题。有关欧洲数据保护的信息，请参阅 AWS Security Blog 上的 AWS Shared Responsibility Model and GDPR 博客文章。

出于数据保护目的，我们建议您保护 AWS 账户 凭证并使用 AWS IAM Identity Center 或 AWS Identity and Access Management (IAM) 设置个人用户。这样，每个用户只获得履行其工作职责所需的权限。我们还建议您通过以下方式保护数据：

- 对每个账户使用多重身份验证（MFA）。
- 使用 SSL/TLS 与资源通信。 AWS 我们要求使用 TLS 1.2，建议使用 TLS 1.3。
- 使用设置 API 和用户活动日志 AWS CloudTrail。
- 使用 AWS 加密解决方案以及其中的所有默认安全控件 AWS 服务。
- 使用高级托管安全服务（例如 Amazon Macie），它有助于发现和保护存储在 Amazon S3 中的敏感数据。
- 如果您在 AWS 通过命令行界面或 API 进行访问时需要经过 FIPS 140-2 验证的加密模块，请使用 FIPS 端点。有关可用的 FIPS 端点的更多信息，请参阅《美国联邦信息处理标准 (FIPS) 第 140-2 版》。

我们强烈建议您切勿将机密信息或敏感信息（如您客户的电子邮件地址）放入标签或自由格式文本字段（如名称字段）。这包括您 AWS 服务 使用控制台、API DataZone 或 AWS SDK 与 Amazon 或其他机构合作的情况。 AWS CLI在用于名称的标签或自由格式文本字段中输入的任何数据都可能会用于计费或诊断日志。如果您向外部服务器提供网址，强烈建议您不要在网址中包含凭证信息来验证对该服务器的请求。

数据加密

在授予权限时，由您决定谁将获得对哪些 Amazon DataZone 资源的权限。您可以对这些资源启用希望允许的特定操作。因此，您应仅授予执行任务所需的权限。实施最低权限访问对于减小安全风险以及可能由错误或恶意意图造成的影响至关重要。

静态加密

默认情况下，Amazon 使用为您 AWS 拥有和管理的AWS 密钥管理服务 (AWS KMS) 密钥 DataZone 加密您的所有数据。您还可以使用您通过 AWS KMS 管理的密钥对存储在 Amazon DataZone 目录中的数据进行加密。

在 Amazon 中创建域时 DataZone，您可以通过选中 “数据加密” 下的 “自定义加密设置（高级）” 旁边的复选框并提供 KMS 密钥来提供加密设置。

传输中加密

Amazon DataZone 使用传输层安全 (TLS) 和客户端加密对传输过程进行加密。与 Amazon DataZone 的通信始终通过 HTTPS 进行，因此您的数据在传输过程中始终处于加密状态。

互联网络流量隐私

为了保护账户之间的连接，Amazon DataZone 使用服务角色和 IAM 角色来安全地连接到客户账户并代表客户执行操作。

主题

- Amazon 的静态数据加密 DataZone
- 使用适用于亚马逊的接口 VPC 终端节点 DataZone

Amazon 的静态数据加密 DataZone

默认情况下，静态数据加密有助于降低保护敏感数据的操作开销和复杂性。同时，它还支持构建符合严格加密合规性和监管要求的安全应用程序。

Amazon DataZone 使用默认 AWS拥有的密钥自动加密您的静态数据。您无法查看、管理或审核 AWS 自有密钥的使用情况。有关更多信息，请参阅AWS 自有密钥。

虽然您无法禁用此加密层或选择其他加密类型，但您可以在创建 Amazon DataZone 域名时选择客户管理的密钥，从而在现有 AWS 拥有的加密密钥上添加第二层加密。Amazon DataZone 支持使用对称的客户托管密钥，您可以创建、拥有和管理这些密钥，在现有 AWS 自有加密的基础上添加第二层加密。由于您可以完全控制此加密层，因此可以在其中执行以下任务：

- 制定和维护关键政策
- 制定和维护 IAM 策略和授权
- 启用和禁用密钥策略
- 轮换密钥加密材料
- 添加标签
- 创建密钥别名

- 计划要删除的密钥

有关更多信息，请参阅客户管理的密钥。

> **Note**
>
> Amazon 使用 AWS 自有密钥 DataZone 自动启用静态加密，从而免费保护客户数据。AWS 使用客户托管密钥需支付 KMS 费用。有关定价的更多信息，请参阅AWS 密钥管理服务定价。

Amazon 如何在 AWS KMS 中 DataZone 使用补助金

Amazon DataZone 需要三项授权才能使用您的客户托管密钥。当您创建使用客户托管密钥加密的 Amazon DataZone 域名时，亚马逊 DataZone 会通过向 AWS KMS 发送CreateGrant请求来代表您创建补助金和子授权。 AWS KMS 中的赠款用于授予亚马逊 DataZone 访问您账户中的 KMS 密钥的权限。Amazon DataZone 创建以下授权，以使用您的客户托管密钥进行以下内部操作：

一项授权，用于加密您的静态数据，用于以下操作：

- 向 AWS KMS 发送DescribeKey请求，以验证在创建 Amazon DataZone 域集合时输入的对称客户托管 KMS 密钥 ID 是否有效。
- 发送GenerateDataKeyrequests到 AWS KMS 以生成由您的客户托管密钥加密的数据密钥。
- 向 AWS KMS 发送解密请求以解密加密的数据密钥，以便它们可用于加密您的数据。
- RetireGrant在删除域名时取消授权。

两项用于搜索和发现您的数据的资助：

- 补助金 2：
  - DescribeKey
  - GenerateDataKey
  - 加密、解密、ReEncrypt
  - CreateGrant为内部使用的 AWS 服务设立儿童补助金 DataZone。
  - RetireGrant
- 补助金 3：
  - GenerateDataKey

- Decrypt
- RetireGrant

您可以随时撤销授予访问权限，或删除服务对客户托管密钥的访问权限。如果您这样做，Amazon 将 DataZone 无法访问由客户托管密钥加密的任何数据，这会影响依赖该数据的操作。例如，如果您尝试获取 Amazon DataZone 无法访问的数据资产详情，则该操作将返回`AccessDeniedException`错误。

创建客户托管密钥

您可以使用 AWS 管理控制台或 AWS KMS API 创建对称客户托管密钥。

要创建对称客户托管密钥，请按照《密钥管理服务开发人员指南》中创建对称客户托管 AWS 密钥的步骤进行操作。

密钥策略-密钥策略控制对客户托管密钥的访问权限。每个客户托管式密钥必须只有一个密钥政策，其中包含确定谁可以使用密钥以及如何使用密钥的声明。创建客户托管式密钥时，可以指定密钥政策。有关更多信息，请参阅《密钥管理服务开发人员指南》中的管理客户托管密 AWS 钥的访问权限。

要将您的客户托管密钥与您的 Amazon DataZone 资源一起使用，密钥政策中必须允许以下 API 操作：

- kms: CreateGrant — 向客户托管密钥添加授权。授予对指定 KMS 密钥的控制访问权限，从而允许访问授予 Amazon DataZone 要求的操作。有关使用授权的更多信息，请参阅 AWS 密钥管理服务开发人员指南。
- kms: DescribeKey — 提供客户托管密钥的详细信息以允许 Amazon DataZone 验证密钥。
- kms: GenerateDataKey — 返回一个唯一的对称数据密钥以供在 AWS KMS 之外使用。
- kms: decrypt — 解密由 KMS 密钥加密的密文。

以下是您可以为 Amazon 添加的政策声明示例 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**
>
> 拒绝 KMS 策略不适用于通过 Amazon DataZone 数据门户访问的资源。

有关在策略中指定权限的更多信息，请参阅《 AWS 密钥管理服务开发人员指南》。

有关密钥访问疑难解答的更多信息，请参阅 AWS 密钥管理服务开发人员指南。

为 Amazon 指定客户托管密钥 DataZone

Amazon DataZone 加密环境

加密上下文是一组可选的键值对，包含有关数据的其他上下文信息。

AWS KMS 使用加密上下文作为额外的经过身份验证的数据来支持经过身份验证的加密。当您在加密数据的请求中包含加密上下文时， AWS KMS 会将加密上下文绑定到加密数据。要解密数据，您必须在请求中包含相同的加密上下文。

Amazon DataZone 使用以下加密环境：

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

使用加密环境进行监控-当您使用对称客户托管密钥加密 Amazon 时 DataZone，您还可以在审计记录和日志中使用加密上下文来识别客户托管密钥的使用情况。加密上下文还会显示在 AWS CloudTrail 或 Amazon Logs 生成的 CloudWatch 日志中。

使用加密上下文来控制对客户托管密钥的访问权限-您可以使用密钥策略和 IAM 策略中的加密上下文作为控制对称客户托管密钥访问权限的条件。您也可以在授予中使用加密上下文约束。

Amazon 在授权中 DataZone 使用加密上下文限制来控制对您账户或地区中客户托管密钥的访问权限。授权约束要求授权允许的操作使用指定的加密上下文。

以下是密钥策略声明示例，用于授予对特定加密上下文的客户托管密钥的访问权限。此策略语句中的条件要求授权具有指定加密上下文的加密上下文约束。

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

监控您的 Amazon 加密密钥 DataZone

当您在亚马逊 DataZone 资源中使用 AWS KMS 客户托管密钥时，您可以使用AWS CloudTrail来跟踪亚马逊 DataZone 向 AWS KMS 发送的请求。以下示例是`CreateGrant`、`GenerateDataKeyDecrypt`、和`DescribeKey`监控 Amazon DataZone 为访问

由您的客户托管密钥加密的数据而调用的 KMS 操作 AWS CloudTrail 的事件。当您使用 AWS KMS 客户托管密钥加密您的亚马逊 DataZone域名时，亚马逊 DataZone 会代表您发送访问您 AWS 账户中的 KMS 密钥的CreateGrant请求。Amazon DataZone 创建的授权特定于与 AWS KMS 客户托管密钥关联的资源。此外，当您删除域名时，Amazon 会 DataZone 使用该RetireGrant操作来删除授权。以下示例事件记录了 CreateGrant 操作：


```
{
    "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"
}
```

创建涉及加密 AWS Glue 目录的数据湖环境

在高级用例中，当您使用加密的 AWS Glue 目录时，必须授予对 Amazon DataZone 服务的访问权限才能使用您的客户管理的 KMS 密钥。为此，您可以更新自定义 KMS 策略并在密钥中添加标签。要授予访问亚马逊 DataZone 服务的权限以处理加密 AWS Glue 目录中的数据，请完成以下操作：

- 将以下策略添加到您的自定义 KMS 密钥。有关更多信息，请参阅更改密钥政策。

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

- 将以下标签添加到您的自定义 KMS 密钥。有关更多信息，请参阅使用标签控制 KMS 密钥的访问权限。

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

使用适用于亚马逊的接口 VPC 终端节点 DataZone

如果您使用亚马逊虚拟私有云（亚马逊 VPC）托管 AWS 资源，则可以在您的亚马逊 VPC 和亚马逊之间建立连接 DataZone。您 DataZone 无需通过公共互联网即可与 Amazon 使用此连接。

Amazon VPC 允许您在自定义虚拟网络中启动 AWS 资源。可以使用 VPC 控制您的网络设置，例如 IP 地址范围、子网、路由表和网络网关。有关 VPC 的更多信息，请参阅《Amazon VPC 用户指南》。

要将您的 Amazon VPC 连接到亚马逊 DataZone，您必须首先定义一个接口 VPC 终端节点，这样您就可以将 VPC 与其他 AWS 服务连接起来。该端点提供了可靠且可扩展的连接，无需互联网网关、网络地址转换 (NAT) 实例或 VPN 连接。有关如何创建 VPC 终端节点的更多信息和详细步骤，请参阅 Amazon VPC 用户指南中的接口 VPC 终端节点 (AWS PrivateLink)。

> **Important**
>
> 在 VPC 中，终端节点策略是一种基于资源的策略，您可以将其附加到 VPC 终端节点，以控制哪些 AWS 委托人可以使用该终端节点访问服务。 AWS
> 在当前版本的 Amazon 中 DataZone，不支持使用终端节点策略来建立和使用您的 Amazon VPC 和亚马逊之间的连接 DataZone。Amazon DataZone 访问管理依赖于在服务级别定义的 RAM 配置和 IAM 主体策略。

在 Amazon 中授权 DataZone

Amazon DataZone 的界面由内部的管理控制台 AWS 和非控制台的 Web 应用程序（数据门户）组成。

AWS 管理员可以使用 Amazon DataZone 管理控制台进行 top-level-resource API，包括创建和管理域、这些域的 AWS 账户关联以及您要将访问管理委托给亚马逊的数据源 DataZone。您可以使用 Amazon DataZone 管理控制台管理为其明确配置的 AWS 账户向 Amazon DataZone 服务委派访问管理控制所需的所有 IAM 角色和配置。Amazon DataZone 数据门户是面向 SSO 用户的第一方 AWS 身份中心应用程序。如果启用，则获得授权的 IAM 委托人也可以使用控制台来联合数据门户，而不是使用 SSO 身份。

Amaz DataZone on 的数据门户主要供经 AWS IAM Identity Center 认证的用户使用，以管理对数据的访问以及执行数据发布、发现、订阅和分析任务。

在 Amazon DataZone 控制台中进行授权

Amazon DataZone 控制台授权模型使用 IAM 授权。管理员主要使用控制台进行设置。Amazon DataZone 使用域管理员 AWS 账户和成员 AWS 账户的概念，所有这些账户都使用控制台来建立信任关系，同时尊重 AWS 组织界限。

Amazon DataZone 门户网站中的授权

Amazon DataZone 数据门户授权模型是一种分层 ACL，具有包括管理员和查看者在内的静态角色原型（配置文件）。例如，用户可以拥有管理员或用户的个人资料。在域级别，他们可能将域用户指定为数据所有者。在项目层面，用户可以是所有者或贡献者。这些配置文件可以配置为两种类型之一：用户和群组。然后，这些配置文件将与域和项目关联，这些权限的状态存储在关联表中。

在这种授权模式中，Amazon DataZone 允许用户管理用户和群组权限。用户管理项目成员资格、申请项目成员资格和批准成员资格。用户发布数据、定义数据订阅批准者、订阅数据和批准订阅。

当用户的数据门户客户端请求 Amazon 根据用户在特定项目环境中的有效个人资料 DataZone 生成的 IAM 会话证书时，用户会在特定项目中执行数据分析。此会话的范围既限于用户的权限，也包括特定项目的资源。然后，用户进入 Athena 或 Redshift 来查询相关数据，所有底层 IAM 工作都被完全抽象出来。

Amazon DataZone 个人资料和角色

用户通过身份验证后，经过身份验证的上下文将映射到用户配置文件 ID。此用户配置文件可以有多个不同的关联（项目所有者、域管理员等），用于对用户进行授权。每个协会（例如，项目所有者、域管理员等）都具有基于上下文的某些活动的权限。例如，具有域管理员关联的用户可以创建其他域，可以为该域分配其他域管理员，还可以在其域中创建项目模板。项目所有者可以为其项目添加或移除项目成员，他们可以与域创建发布协议，并将资源发布到域中。

使用 IAM 控制对亚马逊 DataZone 资源的访问

你需要 AWS Identity and Access Management (IAM) 来完成以下与安全相关的任务：

- 在您的下创建用户和群组 AWS 账户。
- 为你旗下的每个用户分配唯一的安全证书 AWS 账户。
- 控制每个用户使用 AWS 资源执行任务的权限。
- 允许其他用户共享 AWS 账户 您的 AWS 资源。
- 为您创建角色 AWS 账户 并定义可以担任这些角色的用户或服务。
- 使用企业的现有身份授予使用 AWS 资源执行任务的权限

有关 IAM 的更多信息，请参阅以下文档：

- AWS Identity and Access Management (IAM)
- 入门
- IAM 用户指南

以下各节描述了设置 Amazon 及其组件所需的策略 DataZone 和权限，例如域（包括域）、关联账户、项目和数据源。有关更多信息，请参阅 Amazon DataZone 术语和概念。

内容

- AWS Amazon 的托管政策 DataZone
- Amazon 的 IAM 角色 DataZone

- 临时证书
- 主体权限

AWS Amazon 的托管政策 DataZone

AWS 托管策略是由创建和管理的独立策略 AWS。 AWS 托管策略旨在为许多常见用例提供权限，以便您可以开始为用户、组和角色分配权限。

请记住， AWS 托管策略可能不会为您的特定用例授予最低权限权限，因为它们可供所有 AWS 客户使用。我们建议通过定义特定于您的使用场景的客户管理型策略来进一步减少权限。

您无法更改 AWS 托管策略中定义的权限。如果 AWS 更新 AWS 托管策略中定义的权限，则更新会影响该策略所关联的所有委托人身份（用户、组和角色）。 AWS 最有可能在启动新的 API 或现有服务可以使用新 AWS 服务 的 API 操作时更新 AWS 托管策略。

有关更多信息，请参阅《IAM 用户指南》中的 AWS 托管式策略。

内容

- AWS 托管策略：AmazonDataZoneFullAccess
- AWS 托管策略： AmazonDataZoneFullUserAccess
- AWS 托管策略： AmazonDataZoneCustomEnvironmentDeploymentPolicy
- AWS 托管策略：AmazonDataZoneEnvironmentRolePermissionsBoundary
- AWS 托管策略：AmazonDataZoneRedshiftGlueProvisioningPolicy
- AWS 托管策略：AmazonDataZoneGlueManageAccessRolePolicy
- AWS 托管策略：AmazonDataZoneRedshiftManageAccessRolePolicy
- AWS 托管式策略：AmazonDataZoneCrossAccountAdmin
- AWS 托管策略：AmazonDataZoneDomainExecutionRolePolicy
- AWS 托管策略：AmazonDataZoneSageMakerProvisioning
- AWS 托管策略：AmazonDataZoneSageMakerAccess
- AWS 托管策略：AmazonDataZoneSageMakerEnvironmentRolePermissionsBoundary
- 亚马逊 DataZone 更新了托 AWS 管政策

AWS 托管策略：AmazonDataZoneFullAccess

您可以将 `AmazonDataZoneFullAccess` 策略附加到 IAM 身份。

本政策允许 DataZone 通过以下方式访问亚马逊 AWS Management Console。

权限详细信息

该策略包含以下权限：

- datazone— 授予委托人 DataZone通过 Amazon 的完全访问权限。 AWS Management Console
- kms— 允许委托人列出别名和描述密钥。
- s3— 允许委托人选择现有或创建新的 S3 存储桶来存储 Ama DataZone zon 数据。
- ram— 允许委托人跨 DataZone 域共享 Amazon 域名。 AWS 账户
- iam— 允许委托人列出和传递角色并获取策略。
- sso— 允许委托人获取已启 AWS IAM Identity Center 用的区域。
- secretsmanager— 允许委托人创建、标记和列出带有特定前缀的密钥。

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Sid": "AmazonDataZoneStatement",
            "Effect": "Allow",
            "Action": [
                "datazone:*"
            ],
            "Resource": [
                "*"
            ]
        },
        {
            "Sid": "ReadOnlyStatement",
            "Effect": "Allow",
            "Action": [
                "kms:DescribeKey",
                "kms:ListAliases",
                "iam:ListRoles",
                "sso:DescribeRegisteredRegions",
                "s3:ListAllMyBuckets",
                "redshift:DescribeClusters",
                "redshift-serverless:ListWorkgroups",
                "ec2:DescribeSecurityGroups",
```

```
                "ec2:DescribeSubnets",
                "ec2:DescribeVpcs",
                "secretsmanager:ListSecrets"
            ],
            "Resource": [
                "*"
            ]
        },
        {
            "Sid": "BucketReadOnlyStatement",
            "Effect": "Allow",
            "Action": [
                "s3:ListBucket",
                "s3:GetBucketLocation"
            ],
            "Resource": "arn:aws:s3:::*"
        },
        {
            "Sid": "CreateBucketStatement",
            "Effect": "Allow",
            "Action": "s3:CreateBucket",
            "Resource": "arn:aws:s3:::amazon-datazone*"
        },
        {
            "Sid": "RamCreateResourceStatement",
            "Effect": "Allow",
            "Action": [
                "ram:CreateResourceShare"
            ],
            "Resource": "*",
            "Condition": {
                "StringEqualsIfExists": {
                    "ram:RequestedResourceType": "datazone:Domain"
                }
            }
        },
        {
            "Sid": "RamResourceStatement",
            "Effect": "Allow",
            "Action": [
                "ram:DeleteResourceShare",
                "ram:AssociateResourceShare",
                "ram:DisassociateResourceShare",
                "ram:RejectResourceShareInvitation"
```

```
            ],
            "Resource": "*",
            "Condition": {
                "StringLike": {
                    "ram:ResourceShareName": [
                        "DataZone*"
                    ]
                }
            }
        },
        {
            "Sid": "RamResourceReadOnlyStatement",
            "Effect": "Allow",
            "Action": [
                "ram:GetResourceShares",
                "ram:GetResourceShareInvitations",
                "ram:GetResourceShareAssociations",
                "ram:ListResourceSharePermissions"
            ],
            "Resource": "*"
        },
        {
            "Sid": "IAMPassRoleStatement",
            "Effect": "Allow",
            "Action": "iam:PassRole",
            "Resource": [
                "arn:aws:iam::*:role/AmazonDataZone*",
                "arn:aws:iam::*:role/service-role/AmazonDataZone*"
            ],
            "Condition": {
                "StringEquals": {
                    "iam:passedToService": "datazone.amazonaws.com"
                }
            }
        },
        {
            "Sid": "IAMGetPolicyStatement",
            "Effect": "Allow",
            "Action": "iam:GetPolicy",
            "Resource": [
                "arn:aws:iam::*:policy/service-role/
AmazonDataZoneRedshiftAccessPolicy*"
            ]
        },
```

```
        {
            "Sid": "DataZoneTagOnCreateDomainProjectTags",
            "Effect": "Allow",
            "Action": [
                "secretsmanager:TagResource"
            ],
            "Resource": "arn:aws:secretsmanager:*:*:secret:AmazonDataZone-*",
            "Condition": {
                "ForAllValues:StringEquals": {
                    "aws:TagKeys": [
                        "AmazonDataZoneDomain",
                        "AmazonDataZoneProject"
                    ]
                },
                "StringLike": {
                    "aws:RequestTag/AmazonDataZoneDomain": "dzd_*",
                    "aws:ResourceTag/AmazonDataZoneDomain": "dzd_*"
                }
            }
        },
        {
            "Sid": "DataZoneTagOnCreate",
            "Effect": "Allow",
            "Action": [
                "secretsmanager:TagResource"
            ],
            "Resource": "arn:aws:secretsmanager:*:*:secret:AmazonDataZone-*",
            "Condition": {
                "ForAllValues:StringEquals": {
                    "aws:TagKeys": [
                        "AmazonDataZoneDomain"
                    ]
                },
                "StringLike": {
                    "aws:RequestTag/AmazonDataZoneDomain": "dzd_*",
                    "aws:ResourceTag/AmazonDataZoneDomain": "dzd_*"
                }
            }
        },
        {
            "Sid": "CreateSecretStatement",
            "Effect": "Allow",
            "Action": [
                "secretsmanager:CreateSecret"
```

```
            ],
            "Resource": "arn:aws:secretsmanager:*:*:secret:AmazonDataZone-*",
            "Condition": {
                "StringLike": {
                    "aws:RequestTag/AmazonDataZoneDomain": "dzd_*"
                }
            }
        }
    ]
}
```

政策注意事项和限制

该AmazonDataZoneFullAccess政策未涵盖某些功能。

- 如果您使用自己的 AWS KMS 密钥创建亚马逊 DataZone 域名，则必须拥有成功创建域名的权限，并拥有该密钥才能调用其他 Amazon DataZone API（例如listDataSources和）的权限createDataSource。kms:CreateGrant kms:GenerateDataKey kms:Decrypt而且您还必须在该密钥的资源策略kms:DescribeKey中拥有kms:CreateGrantkms:Decryptkms:GenerateDataKey、、和权限。

  如果您使用默认的服务拥有的 KMS 密钥，则不需要这样做。

  有关更多信息，请参阅 AWS Key Management Service。
- 如果您想在 Amazon DataZone 控制台中使用创建和更新角色功能，则必须具有管理员权限或具有创建 IAM 角色和创建/更新策略所需的 IAM 权限。所需的权限包括iam:CreateRole、iam:CreatePolicy、iam:CreatePolicyVersioniam:DeletePolicyVersi和iam:AttachRolePolicy权限。
- 如果您在激活 AWS IAM Identity Center 用户登录的情况下在亚马逊 DataZone 创建新域名，或者如果您为亚马逊中的现有域名激活该域名 DataZone，则必须拥有以下权限：sso:CreateManagedApplicationInstancesso:DeleteManagedApplicationInstance、和sso:PutApplicationAssignmentConfiguration。
- 要在 Amazon 上接受 AWS 账户关联请求 DataZone，您必须ram:AcceptResourceShareInvitation获得许可。

AWS 托管策略： AmazonDataZoneFullUserAccess

此政策授予对 Amazon 的完全访问权限 DataZone，但不允许管理域名、用户或关联账户。

权限详细信息

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Sid": "AmazonDataZoneUserOperations",
            "Effect": "Allow",
            "Action": [
                "datazone:PostTimeSeriesDataPoints",
                "datazone:ListTimeSeriesDataPoints",
                "datazone:GetTimeSeriesDataPoint",
                "datazone:DeleteTimeSeriesDataPoints",
                "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",
                "datazone:ListLineageNodeHistory",
                "datazone:GetLineageNode",
                "datazone:CreateAssetFilter",
                "datazone:DeleteAssetFilter",
                "datazone:GetAssetFilter",
                "datazone:ListAssetFilters",
                "datazone:UpdateAssetFilter"
            ],
            "Resource": "*"
        },
        {
            "Sid": "RAMResourceShareOperations",
            "Effect": "Allow",
            "Action": "ram:GetResourceShareAssociations",
            "Resource": "*"
        }
    ]
}
```

AWS 托管策略： AmazonDataZoneCustomEnvironmentDeploymentPolicy

您可以使用此策略来更新使用自定义蓝图创建的环境的配置。此政策还可用于创建 Amazon DataZone 订阅目标和数据源。

权限详细信息

```
{
 "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 托管策略：AmazonDataZoneEnvironmentRolePermissionsBoundary

> **Note**
>
> 此策略是权限边界。权限边界设置基于身份的策略可以向 IAM 实体授予的最大权限。您不应自行使用和附加 Amazon DataZone 权限边界策略。亚马逊 DataZone 权限边界策略应仅附加到亚马逊 DataZone 托管角色。有关权限边界的更多信息，请参阅 IAM 用户指南中的 IAM 实体的权限边界。

当您通过 Amazon DataZone 数据门户创建环境时，Amazon 会将此权限边界 DataZone 应用于在创建环境期间生成的 IAM 角色。权限边界限制了 Amazon DataZone 创建的角色和您添加的任何角色的范围。

Amazon DataZone 使用AmazonDataZoneEnvironmentRolePermissionsBoundary托管策略来限制其所关联的预配置 IAM 委托人。委托人可以采用亚马逊 DataZone 可以代表交互式企业用户或分析服务（例如）担任的用户角色的形式AWS Glue，然后执行操作来处理数据，例如从 Amazon S3 读取和写入数据或运行。 AWS Glue 爬网程序

该AmazonDataZoneEnvironmentRolePermissionsBoundary政策授予亚马逊对诸如亚马逊 DataZone S3 AWS Glue、、Amazon Redshift 和亚马逊 Athena 等服务的读写权限。 AWS Lake Formation该策略还向使用这些服务所需的某些基础设施资源（例如网络接口和 AWS KMS 密钥）授予读写权限。

亚马逊 DataZone 将AmazonDataZoneEnvironmentRolePermissionsBoundary AWS 托管策略应用为所有亚马逊 DataZone 环境角色（所有者和贡献者）的权限边界。此权限边界将这些角色限制为仅允许访问环境所需的资源和必要的操作。

边界包括以下 JSON 语句：

```
{
  "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 托管策略：AmazonDataZoneRedshiftGlueProvisioningPolicy

该AmazonDataZoneRedshiftGlueProvisioningPolicy政策授予亚马逊 DataZone 与 AWS Glue 和 Amazon Redshift 互操作所需的权限。

```
{
 "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 托管策略：AmazonDataZoneGlueManageAccessRolePolicy

该政策授予亚马逊向目录发布 AWS Glue 数据的 DataZone 权限。它还授予亚马逊授予访问 DataZone 权限或撤销对目录中已发布的 AWS Glue 资产的访问权限的权限。

```
{
 "Version": "2012-10-17",
 "Statement": [
  {
   "Sid": "GlueTagDatabasePermissions",
   "Effect": "Allow",
   "Action": [
    "glue:TagResource",
    "glue:UntagResource",
    "glue:GetTags"
   ],
   "Resource": "*",
   "Condition": {
    "StringEquals": {
     "aws:ResourceAccount": "${aws:PrincipalAccount}"
    },
    "ForAnyValue:StringLikeIfExists": {
     "aws:TagKeys": "DataZoneDiscoverable_*"
    }
   }
  },
  {
   "Sid": "GlueDataQualityPermissions",
   "Effect": "Allow",
   "Action": [
    "glue:ListDataQualityResults",
    "glue:GetDataQualityResult"
   ],
   "Resource": "arn:aws:glue:*:*:dataQualityRuleset/*",
   "Condition": {
    "StringEquals": {
     "aws:ResourceAccount": "${aws:PrincipalAccount}"
    }
   }
```

```
  },
  {
   "Sid": "GlueTableDatabasePermissions",
   "Effect": "Allow",
   "Action": [
    "glue:CreateTable",
    "glue:DeleteTable",
    "glue:GetDatabases",
    "glue:GetTables"
   ],
   "Resource": [
    "arn:aws:glue:*:*:catalog",
    "arn:aws:glue:*:*:database/*",
    "arn:aws:glue:*:*:table/*"
   ],
   "Condition": {
    "StringEquals": {
     "aws:ResourceAccount": "${aws:PrincipalAccount}"
    }
   }
  },
  {
   "Sid": "LakeformationResourceSharingPermissions",
   "Effect": "Allow",
   "Action": [
    "lakeformation:BatchGrantPermissions",
    "lakeformation:BatchRevokePermissions",
    "lakeformation: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 托管策略：AmazonDataZoneRedshiftManageAccessRolePolicy

该政策允许亚马逊将亚马 DataZone 逊 Redshift 数据发布到目录中。它还允许亚马逊授予访问 DataZone 权限或撤销对目录中已发布的亚马逊 Redshift 或 Amazon Redshift Serverless 资源的访问权限或撤消访问权限。

```
{
 "Version": "2012-10-17",
 "Statement": [
  {
   "Sid": "redshiftDataScopeDownPermissions",
   "Effect": "Allow",
   "Action": [
    "redshift-data:BatchExecuteStatement",
    "redshift-data:DescribeTable",
    "redshift-data:ExecuteStatement",
    "redshift-data:ListTables",
    "redshift-data:ListSchemas",
    "redshift-data:ListDatabases"
   ],
   "Resource": [
    "arn:aws:redshift-serverless:*:*:workgroup/*",
    "arn:aws:redshift:*:*:cluster:*"
   ],
   "Condition": {
    "StringEquals": {
     "aws:ResourceAccount": "${aws:PrincipalAccount}"
    }
   }
  },
  {
   "Sid": "listSecretsPermission",
   "Effect": "Allow",
   "Action": "secretsmanager:ListSecrets",
   "Resource": "*"
  },
  {
   "Sid": "getWorkgroupPermission",
```

```
    "Effect": "Allow",
    "Action": "redshift-serverless:GetWorkgroup",
    "Resource": [
     "arn:aws:redshift-serverless:*:*:workgroup/*"
    ],
    "Condition": {
     "StringEquals": {
      "aws:ResourceAccount": "${aws:PrincipalAccount}"
     }
    }
   },
   {
    "Sid": "getNamespacePermission",
    "Effect": "Allow",
    "Action": "redshift-serverless:GetNamespace",
    "Resource": [
     "arn:aws:redshift-serverless:*:*:namespace/*"
    ],
    "Condition": {
     "StringEquals": {
      "aws:ResourceAccount": "${aws:PrincipalAccount}"
     }
    }
   },
   {
    "Sid": "redshiftDataPermissions",
    "Effect": "Allow",
    "Action": [
     "redshift-data:DescribeStatement",
     "redshift-data:GetStatementResult",
     "redshift:DescribeClusters"
    ],
    "Resource": "*"
   },
   {
    "Sid": "dataSharesPermissions",
    "Effect": "Allow",
    "Action": [
     "redshift:AuthorizeDataShare",
     "redshift:DescribeDataShares"
    ],
    "Resource": [
     "arn:aws:redshift:*:*:datashare:*/datazone*"
    ],
```

```
   "Condition": {
    "StringEquals": {
     "aws:ResourceAccount": "${aws:PrincipalAccount}"
    }
   }
  },
  {
   "Sid": "associateDataShareConsumerPermission",
   "Effect": "Allow",
   "Action": "redshift:AssociateDataShareConsumer",
   "Resource": "arn:aws:redshift:*:*:datashare:*/datazone*"
  }
 ]
}
```

AWS 托管式策略：AmazonDataZoneCrossAccountAdmin

您可以将该 AmazonDataZoneCrossAccountAdmin 策略附加到您的 IAM 身份。

该政策允许用户使用Amazon DataZone 关联账户。

```
{
    "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 托管策略：AmazonDataZoneDomainExecutionRolePolicy

这是 Amazon DataZone `DomainExecutionRole` 服务角色的默认策略。亚马逊使用此角色 DataZone 对亚马逊 DataZone 域中的数据进行分类、发现、管理、共享和分析。该角色提供对使用数据门户所需的所有 Amazon DataZone API 的访问权限，以及支持在亚马逊 DataZone 域中使用关联账户的 RAM 权限。

您可以将该 AmazonDataZoneDomainExecutionRolePolicy 政策附加到您的`AmazonDataZoneDomainExecutionRole`。

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Sid": "DomainExecutionRoleStatement",
            "Effect": "Allow",
            "Action": [
                "datazone:ListTimeSeriesDataPoints",
```

```
                "datazone:GetTimeSeriesDataPoint",
                "datazone:DeleteTimeSeriesDataPoints",
                "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",
                "datazone:GetEnvironmentAction",
                "datazone:ListEnvironmentActions",
                "datazone:ListLineageNodeHistory",
                "datazone:GetLineageNode",
                "datazone:CreateAssetFilter",
                "datazone:DeleteAssetFilter",
                "datazone:GetAssetFilter",
                "datazone:ListAssetFilters",
                "datazone:UpdateAssetFilter"
            ],
            "Resource": "*"
        },
        {
            "Sid": "RAMResourceShareStatement",
            "Effect": "Allow",
            "Action": "ram:GetResourceShareAssociations",
            "Resource": "*"
        }
    ]
}
```

AWS 托管策略：AmazonDataZoneSageMakerProvisioning

该 AmazonDataZoneSageMakerProvisioning 政策授予亚马逊 DataZone 与亚马逊 SageMaker互操作所需的权限。

```
{
 "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 托管策略：AmazonDataZoneSageMakerAccess

该政策授予亚马逊将亚马逊 SageMaker 资产发布到目录的 DataZone 权限。它还授予亚马逊授予访问 DataZone 权限或撤销对亚马逊在目录中 SageMaker 发布的资产的访问权限的权限。

此策略包括以下权限：

- cloudtrail — 检索有关 CloudTrail 跟踪的信息。
- cloudwatch — 检索当前 CloudWatch 警报。
- 日志-检索 CloudWatch 日志的指标筛选器。
- sns — 检索 SNS 主题的订阅列表。
- config-检索有关配置记录器、资源和 AWS Config 规则的信息。还允许服务相关角色创建和删除 AWS Config 规则，以及根据规则运行评估。
- iam — 获取并生成账户的凭证报告。
- 组织-检索组织的帐户和组织单位 (OU) 信息。
- securityhub — 检索有关如何配置 Security Hub 服务、标准和控件的信息。
- tag — 检索有关资源标签的信息。

```
{
 "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 托管策略：AmazonDataZoneSageMakerEnvironmentRolePermissionsBoundary

> **Note**
>
> 此策略是权限边界。权限边界设置基于身份的策略可以向 IAM 实体授予的最大权限。您不应自行使用和附加 Amazon DataZone 权限边界策略。亚马逊 DataZone 权限边界策略应仅附加到亚马逊 DataZone 托管角色。有关权限边界的更多信息，请参阅 IAM 用户指南中的 IAM 实体的权限边界。

当您通过亚马逊 DataZone 数据门户创建亚马逊 SageMaker环境时，亚马逊会 DataZone 将此权限边界应用于在创建环境期间生成的 IAM 角色。权限边界限制了 Amazon DataZone 创建的角色和您添加的任何角色的范围。

Amazon DataZone 使用AmazonDataZoneSageMakerEnvironmentRolePermissionsBoundary托管策略来限制其所关联的预配置 IAM 委托人。委托人可以采取亚马逊 DataZone 可以代表交互式企业用户或分析服务

（例如）担任的用户角色的形式，然后执行操作来处理数据AWS SageMaker，例如从Amazon S3或Amazon Redshift读取和写入数据，或者运行 AWS Glue爬虫。

该AmazonDataZoneSageMakerEnvironmentRolePermissionsBoundary政策授予亚马逊对亚马逊 SageMaker、 AWS Glue、Amazon DataZone S3、La AWS ke Formation、Amazon Redshift和Amazon Athena等服务的读写权限。该策略还向使用这些服务所需的某些基础设施资源授予读写权限，例如网络接口、Amazon ECR 存储库和 AWS KMS 密钥。它还允许访问亚马逊 SageMaker应用程序，例如Amazon SageMaker Canvas。

亚马逊 DataZone 将AmazonDataZoneSageMakerEnvironmentRolePermissionsBoundary托管策略应用为所有亚马逊 DataZone 环境角色（所有者和贡献者）的权限边界。此权限边界将这些角色限制为仅允许访问环境所需的资源和必要的操作。

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

亚马逊 DataZone 更新了托 AWS 管政策

查看 DataZone 自该服务开始跟踪这些变更以来亚马逊 AWS 托管政策更新的详细信息。要获取有关此页面变更的自动提醒，请订阅 Amazon DataZone 文档历史记录页面上的 RSS feed。

更改	描述	日期
AmazonDataZoneExecutionRolePolicy 以及 AmazonDataZoneFullUserAccess -政策更新	对AmazonDataZoneExecutionRolePolicy 和的策略进行了更新 AmazonDataZoneFullUserAccess，以启用对数据沿袭和细粒度访问控制 API 的支持。	2024年6月27日
AmazonDataZoneGlueManageAccessRolePolicy -政策更新	的AmazonDataZoneGlueManageAccessRolePolicy政策更新增加了亚马逊自助订阅功能所需的 IAM 权限，DataZone 以缩小湖形成时授予的权限范围。使用自助订阅功	2024年6月14日

更改	描述	日期
	能，只能向带标签的资源授予湖泊形成权限。	
AmazonDataZoneDomainExecutionRolePolicy -政策更新	的政策更新为AmazonDataZoneDomainExecutionRolePolicy亚马逊添加了新的 API DataZone ，使用户能够为其亚马逊 DataZone 环境配置操作。	2024年6月14日
AmazonDataZoneFullAccess -政策更新	的政策更新AmazonDataZoneFullAccess使得 Amazon DataZone 管理控制台能够代表用户使用域和项目标签创建密钥。还包括允许域名所有者账户的管理员查看关联账户的账户关联状态的`ram:ListResourceSharePermissions` 操作。	2024年6月14日
AmazonDataZoneSageMakerEnvironmentRolePermissionsBoundary -新的权限边界	新的权限边界已调用AmazonDataZoneSageMakerEnvironmentRolePermissionsBoundary。当您通过亚马逊 DataZone 数据门户创建亚马逊 SageMaker 环境时，亚马逊会 DataZone 将此权限边界应用于在创建环境期间生成的 IAM 角色。权限边界限制了 Amazon DataZone 创建的角色和您添加的任何角色的范围。	2024年4月30日

更改	描述	日期
AmazonDataZoneSageMakerAccess -新政策	名AmazonDataZoneSageMakerAccess为的新政策授予亚马逊向目录发布亚马逊 SageMaker 资产的 DataZone 权限。它还授予亚马逊授予访问 DataZone权限或撤销对亚马逊在目录中 SageMaker 发布的资产的访问权限的权限。	2024年4月30日
AmazonDataZoneFullAccess -政策更新	对AmazonDataZoneFullAccess策略的更新，增加了 `DescribeSecurityGroups` 操作访问权限，以提高账户管理员的可用性，在控制台中配置蓝图和`GetPolicy` 操作以帮助检索有关指定托管策略的信息。	2024年4月30日
AmazonDataZoneSageMakerProvisioning -新政策	名为的新政策AmazonDataZoneSageMakerProvisioning授 DataZone 予亚马逊与亚马逊 SageMaker互操作所需的权限。	2024年4月30日
AmazonDataZoneS3Manage-<region>-<domainId>-新角色	名为 AmazonDataZoneS3Manage 的新角色—— <region><domainId>亚马逊致 DataZone 电 L AWS ake Formation 注册亚马逊简单存储服务 (Amazon S3) 位置时使用该角色。 AWS Lake Formation 在访问该位置的数据时扮演这个角色。	2024年4月1日

更改	描述	日期
AmazonDataZoneGlue ManageAccessRolePolicy -政策更新	更新了AmazonDataZoneGlue ManageAccessRolePolicy以启用对允许 Amazon DataZone 启用发布和数据访问权限的权限的支持。	2024年4月1日
AmazonDataZoneDomainExecutionRolePolicy 以及 AmazonDataZoneFullUserAccess -政策更新	更新了AmazonDataZoneDomainExecutionRolePolicy和AmazonDataZoneFullUserAccess以启用对 `CancelMetadataGenerationRun` API 的支持。	2024 年 3 月 29 日
AmazonDataZoneFullAccess -政策更新	更新了，使用户`AmazonDataZoneFullAccess` 能够在 Amazon DataZone 管理控制台中选择自己的密钥、集群、vpc 和子网，而不必在文本框中键入它们。	2024 年 3 月 13 日
AmazonDataZoneDomainExecutionRolePolicy -政策更新	通过确定哪些蓝图在哪个账户和区域启用，更新了以启用对创建环境配置文件所需的 `ListEnvironmentBlueprintConfigurationSummaries` API 的支持。AmazonDataZoneDomainExecutionRolePolicy	2024年2月1日
AmazonDataZoneGlue ManageAccessRolePolicy -政策更新	更新了AmazonDataZoneGlue ManageAccessRolePolicy以启用对 AWS Lake Formation 混合模式的支持。	2023 年 12 月 14 日

更改	描述	日期
AmazonDataZoneFull UserAccess 以及 AmazonDataZoneDomainExecutionRolePolicy -政策更新	更新了AmazonDataZoneFull UserAccess和AmazonDataZoneDomainExecutionRolePolicy政策，以支持 Amazon DataZone 中由人工智能驱动的生成式数据描述功能。	2023 年 11 月 28 日
AmazonDataZoneEnvironmentRolePermissionsBoundary -政策更新	Amazon 对AmazonDataZoneEnvironmentRolePermissionsBoundary托管策略 DataZone 进行了更新，其中包括根据ResourceTag 条件限定的额外athena:GetQueryResultsStream 权限。	2023 年 11 月 17 日
AmazonDataZoneRedshiftManageAccessRolePolicy -政策更新	Amazon AmazonDataZoneRedshiftManageAccessRolePolicy通过取消对组织编号的检查来 DataZone 更新该redshift:AssociateDataShareConsumer 操作。这使您能够在 AWS 组织之间共享资源。	2023 年 11 月 16 日
AmazonDataZoneFull UserAccess -政策更新	亚马逊 DataZone 更新了授予亚马逊完全访问权限的AmazonDataZoneFull UserAccess政策 DataZone，但不允许管理域名、用户或关联账户。	2023年10月2日

更改	描述	日期
AmazonDataZonePortalFullAccessPolicy -政策已弃用	亚马逊 DataZone 弃用了。AmazonDataZonePortalFullAccessPolicy	2023 年 9 月 29 日
AmazonDataZonePreviewConsoleFullAccess -政策已弃用	亚马逊 DataZone 弃用了。AmazonDataZonePreviewConsoleFullAccess	2023 年 9 月 29 日
AmazonDataZoneDomainExecutionRolePolicy -新政策	亚马逊 DataZone 添加了一项名为 “” 的新政策AmazonDataZoneDomainExecutionRolePolicy。 这是 Amazon DataZone `AmazonDataZoneDomainExecutionRole` 服务角色的默认策略。亚马逊使用此角色 DataZone 对亚马逊 DataZone 域中的数据进行分类、发现、管理、共享和分析。 您可以将该`AmazonDataZoneDomainExecutionRolePolicy` 政策附加到您的`AmazonDataZoneDomainExecutionRole` 。	2023 年 9 月 25 日
AmazonDataZoneCrossAccountAdmin -新政策	亚马逊 DataZone 添加了一项名为的新政策 AmazonDataZoneCrossAccountAdmin，允许用户使用亚马逊 DataZone 及其关联账户。	2023 年 9 月 19 日

更改	描述	日期
AmazonDataZoneFull UserAccess -新政策	亚马逊 DataZone 添加了一项名为的新政策 AmazonDataZoneFullUserAccess，该政策授予对亚马逊的完全访问权限 DataZone，但它不允许管理域名、用户或关联账户。	2023 年 9 月 12 日
AmazonDataZoneRedshiftManageAccessRolePolicy -新政策	亚马逊 DataZone 添加了一项名为的新政策 AmazonDataZoneRedshiftManageAccessRolePolicy，该政策授予 DataZone 允许亚马逊启用数据发布和访问权限的权限。	2023 年 9 月 12 日
AmazonDataZoneGlueManageAccessRolePolicy -新政策	亚马逊 DataZone 添加了一项名为的新政策 AmazonDataZoneGlueManageAccessRolePolicy，该政策授予亚马逊向目录发布 AWS Glue数据的 DataZone 权限。它还授予亚马逊授予访问 DataZone 权限或撤销对目录中已发布的 AWS Glue 资产的访问权限的权限。	2023 年 9 月 12 日
AmazonDataZoneRedshiftGlueProvisioningPolicy -新政策	亚马逊 DataZone 添加了一项名为的新政策 AmazonDataZoneRedshiftGlueProvisioningPolicy，该政策向亚马逊 DataZone 授予与支持的数据源进行互操作所需的权限。	2023 年 9 月 12 日

更改	描述	日期
AmazonDataZoneEnvironmentRolePermissionsBoundary -新政策	Amazon DataZone 添加了一项名为的新政策 AmazonDataZoneEnvironmentRolePermissionsBoundary，该政策限制了其所关联的预配置 IAM 委托人。	2023 年 9 月 12 日
AmazonDataZoneFullAccess -新政策	亚马逊 DataZone 添加了一项名为的新政策 AmazonDataZoneFullAccess， DataZone 通过 AWS 管理控制台提供对亚马逊的完全访问权限。	2023 年 9 月 12 日
托管式策略更新	包含额外`iam:GetPolicy` 权限的AmazonDataZonePreviewConsoleFullAccess托管策略的更新。	2023 年 6 月 13 日
亚马逊 DataZone 开始追踪变更	亚马逊 DataZone 开始跟踪其 AWS 托管政策的变更。	2023 年 3 月 20 日

Amazon 的 IAM 角色 DataZone

主题

- AmazonDataZoneProvisioningRole-<domainAccountId>
- AmazonDataZoneDomainExecutionRole
- AmazonDataZoneGlueAccess-<region>-<domainId>
- AmazonDataZoneRedshiftAccess-<region>-<domainId>
- AmazonDataZone<region>S3Manage--<domainId>
- AmazonDataZoneSageMakerManageAccessRole-<region>-<domainId>
- AmazonDataZoneSageMakerProvisioningRole-<domainAccountId>

AmazonDataZoneProvisioningRole-<domainAccountId>

AmazonDataZoneRedshiftGlueProvisioningPolicy附上AmazonDataZoneProvisioningRole-<domainAccountId>了。此角色向亚马逊 DataZone 授予与 AWS Glue 和 Amazon Redshift 互操作所需的权限。

默认情况下附加AmazonDataZoneProvisioningRole-<domainAccountId>了以下信任策略：

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

AmazonDataZoneDomainExecutionRole

AmazonDataZoneDomainExecutionRole已AmazonDataZoneDomainExecutionRolePolicy附加 AWS 托管策略。Amazon 代表您 DataZone 创建此角色。对于数据门户中的某些操作，Amazon DataZone 将在创建该角色的账户中担任此角色，并检查该角色是否有权执行该操作。

托管您的 Amazon DataZone 域名的AmazonDataZoneDomainExecutionRole角色是必需的。 AWS 账户 此角色是在您创建 Amazon DataZone 域名时自动为您创建的。

默认AmazonDataZoneDomainExecutionRole角色具有以下信任策略。

```
{
```

```
    "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>

该AmazonDataZoneGlueAccess-<region>-<domainId>角色AmazonDataZoneGlueManageAccessRolePolicy附带了。此角色授予亚马逊向目录发布 AWS Glue 数据的 DataZone 权限。它还授予亚马逊授予访问 DataZone 权限或撤销对目录中已发布的 AWS Glue 资产的访问权限的权限。

默认AmazonDataZoneGlueAccess-<region>-<domainId>角色附加了以下信任策略：

```
{
  "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>

该AmazonDataZoneRedshiftAccess-<region>-<domainId>角色AmazonDataZoneRedshiftManageAccessRolePolicy附带了。此角色授予亚马逊向 DataZone 目录发布亚马逊 Redshift 数据的权限。它还允许亚马逊授予访问 DataZone 权限或撤销对目录中已发布的亚马逊 Redshift 或 Amazon Redshift Serverless 资源的访问权限或撤消访问权限。

默认AmazonDataZoneRedshiftAccess-<region>-<domainId>角色附加了以下内联权限策略：

```
{
   "Version":"2012-10-17",
   "Statement":[
      {
         "Sid": "RedshiftSecretStatement",
         "Effect":"Allow",
         "Action":"secretsmanager:GetSecretValue",
         "Resource":"*",
         "Condition":{
            "StringEquals":{
               "secretsmanager:ResourceTag/AmazonDataZoneDomain":"{{domainId}}"
            }
         }
      }
   ]
}
```

默认情况下附加AmazonDataZoneRedshiftManageAccessRole<timestamp>了以下信任策略：

```
{
  "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>S3Manage--<domainId>

当亚马逊致<region><domainId> DataZone电 La AWS ke Formation 注册亚马逊简单存储服务 (Amazon AmazonDataZone S3) 分店时，会使用 S3Manage- AWS Lake Formation 在访问该位置的数据时扮演这个角色。有关更多信息，请参阅用于注册营业地点的角色要求。

此角色附加了以下内联权限策略。

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Sid": "LakeFormationDataAccessPermissionsForS3",
            "Effect": "Allow",
```

```
            "Action": [
                "s3:PutObject",
                "s3:GetObject",
                "s3:DeleteObject"
            ],
            "Resource": "*",
            "Condition": {
                "StringEquals": {
                    "aws:ResourceAccount": "{{accountId}}"
                }
            }
        },
        {
            "Sid": "LakeFormationDataAccessPermissionsForS3ListBucket",
            "Effect": "Allow",
            "Action": [
                "s3:ListBucket"
            ],
            "Resource": "*",
            "Condition": {
                "StringEquals": {
                    "aws:ResourceAccount": "{{accountId}}"
                }
            }
        },
        {
            "Sid": "LakeFormationDataAccessPermissionsForS3ListAllMyBuckets",
            "Effect": "Allow",
            "Action": [
                "s3:ListAllMyBuckets"
            ],
            "Resource": "arn:aws:s3:::*",
            "Condition": {
                "StringEquals": {
                    "aws:ResourceAccount": "{{accountId}}"
                }
            }
        },
        {
            "Sid": "LakeFormationExplicitDenyPermissionsForS3",
            "Effect": "Deny",
            "Action": [
                "s3:PutObject",
                "s3:GetObject",
```

```
                "s3:DeleteObject"
            ],
            "Resource": [
                "arn:aws:s3:::[[BucketNames]]/*"
            ],
            "Condition": {
                "StringEquals": {
                    "aws:ResourceAccount": "{{accountId}}"
                }
            }
        },
        {
            "Sid": "LakeFormationExplicitDenyPermissionsForS3ListBucket",
            "Effect": "Deny",
            "Action": [
                "s3:ListBucket"
            ],
            "Resource": [
                "arn:aws:s3:::[[BucketNames]]"
            ],
            "Condition": {
                "StringEquals": {
                    "aws:ResourceAccount": "{{accountId}}"
                }
            }
        }
    ]
}
```

AmazonDataZoneS3Manage-<region>-<domainId>附带了以下信任政策：

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Sid": "TrustLakeFormationForDataLocationRegistration",
            "Effect": "Allow",
            "Principal": {
                "Service": "lakeformation.amazonaws.com"
            },
            "Action": "sts:AssumeRole",
```

```
            "Condition": {
                "StringEquals": {
                    "aws:SourceAccount": "{{source_account_id}}"
                }
            }
        }
    ]
}
```

AmazonDataZoneSageMakerManageAccessRole-<region>-<domainId>

AmazonDataZoneSageMakerManageAccessRole角色AmazonDataZoneGlueManageAccessRolePolicy附AmazonDataZoneSageMakerAccess有Amazon和。此角色授予亚马逊发布和管理数据湖、数据仓库和 Amazon Sagemaker 资产订阅的 DataZone 权限。

该AmazonDataZoneSageMakerManageAccessRole角色附加了以下内联策略：

```
{
   "Version":"2012-10-17",
   "Statement":[
      {
         "Sid": "RedshiftSecretStatement",
         "Effect":"Allow",
         "Action":"secretsmanager:GetSecretValue",
         "Resource":"*",
         "Condition":{
            "StringEquals":{
               "secretsmanager:ResourceTag/AmazonDataZoneDomain":"{{domainId}}"
            }
         }
      }
   ]
}
```

该AmazonDataZoneSageMakerManageAccessRole角色附加了以下信任策略：

```
{
```

```
  "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>

该AmazonDataZoneSageMakerProvisioningRole角色AmazonDataZoneRedshiftGlueProvisioningPolicy附带AmazonDataZoneSageMakerProvisioning和。该角色向亚马逊授予与 AWS Glue、Amazon Redshift 和 Amazon Sagemaker 互操作所需的 DataZone 权限。

该AmazonDataZoneSageMakerProvisioningRole角色附加了以下内联策略：

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Sid": "SageMakerStudioTagOnCreate",
            "Effect": "Allow",
            "Action": [
                "sagemaker:AddTags"
            ],
```

```
            "Resource": "arn:aws:sagemaker:*:{{AccountId}}:*/*",
            "Condition": {
                "Null": {
                    "sagemaker:TaggingAction": "false"
                }
            }
        }
    ]
}
```

该AmazonDataZoneSageMakerProvisioningRole角色附加了以下信任策略：

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Sid": "DataZoneTrustPolicyStatement",
      "Effect": "Allow",
      "Principal": {
        "Service": "datazone.amazonaws.com"
      },
      "Action": "sts:AssumeRole",
      "Condition": {
        "StringEquals": {
            "aws:SourceAccount": "{{domain_account}}"
        }
      }
    }
  ]
}
```

临时证书

当您使用临时证书登录时，某些 AWS 服务不起作用。有关更多信息，包括哪些 AWS 服务可使用临时证书，请参阅 IAM 用户指南中的与 IAM 配合使用的AWS 服务。

如果您使用除用户名和密码之外的任何方法登录，则 AWS Management Console 使用的是临时证书。例如，当您 AWS 使用公司的单点登录 (SSO) 链接进行访问时，该过程会自动创建临时证书。当您以

用户身份登录控制台，然后切换角色时，您还会自动创建临时凭证。有关切换角色的更多信息，请参阅《IAM 用户指南》中的 切换到角色（控制台）。

您可以使用 AWS CLI 或 AWS API 手动创建临时证书。然后，您可以使用这些临时证书进行访问 AWS。 AWS 建议您动态生成临时证书，而不是使用长期访问密钥。有关更多信息，请参阅 IAM 中的临时安全凭证。

主体权限

当您使用 IAM 用户或角色在中执行操作时 AWS，您被视为委托人。策略向主体授予权限。使用某些服务时，您可能会执行一个操作，此操作然后在不同服务中触发另一个操作。在这种情况下，您必须具有执行这两个操作的权限。要查看某项操作是否需要策略中的其他相关操作，请参阅《服务授权参考》中的 “AWS 文档要点的操作、资源和条件密钥”。

Amazon 合规性验证 DataZone

要了解是否属于特定合规计划的范围，请参阅AWS 服务 “按合规计划划分的范围” ”，然后选择您感兴趣的合规计划。 AWS 服务 有关一般信息，请参阅AWS 合规计划AWS。

您可以使用下载第三方审计报告 AWS Artifact。有关更多信息，请参阅中的 “下载报告” 中的 “ AWS Artifact。

您在使用 AWS 服务 时的合规责任取决于您的数据的敏感性、贵公司的合规目标以及适用的法律和法规。 AWS 提供了以下资源来帮助实现合规性：

- 安全与合规性快速入门指南 — 这些部署指南讨论了架构注意事项，并提供了在这些基础上 AWS 部署以安全性和合规性为重点的基准环境的步骤。
- 在 A@@ mazon Web Services 上构建 HIPAA 安全与合规性 — 本白皮书描述了各公司如何使用 AWS 来创建符合 HIPAA 资格的应用程序。

> **Note**
>
> 并非所有 AWS 服务 人都符合 HIPAA 资格。有关更多信息，请参阅符合 HIPAA 要求的服务参考。

- AWS 合规资源AWS — 此工作簿和指南集可能适用于您所在的行业和所在地区。
- AWS 客户合规指南 — 从合规角度了解责任共担模式。这些指南总结了保护的最佳实践， AWS 服务 并将指南映射到跨多个框架（包括美国国家标准与技术研究院 (NIST)、支付卡行业安全标准委员会 (PCI) 和国际标准化组织 (ISO)）的安全控制。

- 使用AWS Config 开发人员指南中的规则评估资源 — 该 AWS Config 服务评估您的资源配置在多大程度上符合内部实践、行业准则和法规。
- AWS Security Hub— 这 AWS 服务 可以全面了解您的安全状态 AWS。Security Hub 通过安全控件评估您的 AWS 资源并检查其是否符合安全行业标准和最佳实践。有关受支持服务及控件的列表，请参阅 Security Hub 控件参考。
- Amazon GuardDuty — 它通过监控您的 AWS 账户环境中是否存在可疑和恶意活动，来 AWS 服务检测您的工作负载、容器和数据面临的潜在威胁。 GuardDuty 通过满足某些合规性框架规定的入侵检测要求，可以帮助您满足各种合规性要求，例如 PCI DSS。
- AWS Audit Manager— 这 AWS 服务 可以帮助您持续审计 AWS 使用情况，从而简化风险管理以及对法规和行业标准的合规性。

Amazon 安全最佳实践 DataZone

Amazon DataZone 提供了许多安全功能，供您在制定和实施自己的安全策略时考虑。以下最佳实践是一般指导原则，并不代表完整安全解决方案。由于这些最佳实践可能不适合您的环境或不满足您的环境要求，因此将其视为有用的考虑因素而不是惯例。

实施最低权限访问

在授予权限时，由您决定谁将获得对哪些 Amazon DataZone 资源的权限。您可以对这些资源启用希望允许的特定操作。因此，您应仅授予执行任务所需的权限。实施最低权限访问对于减小安全风险以及可能由错误或恶意意图造成的影响至关重要。

使用 IAM 角色

创建器和客户端应用程序必须具有有效凭证才能访问 Amazon DataZone 资源。您不应将 AWS 证书直接存储在客户端应用程序或 Amazon S3 存储桶中。这些是不会自动轮换的长期凭证，如果它们受到损害，可能会对业务产生重大影响。

相反，您应该使用 IAM 角色来管理您的创建器和客户端应用程序访问亚马逊 DataZone资源的临时证书。在使用角色时，您不必使用长期凭证（如用户名和密码或访问密钥）来访问其他资源。

有关更多信息，请参阅 IAM 用户指南中的以下主题：

- IAM 角色
- 针对角色的常见情形：用户、应用程序和服务

实施从属资源中的服务器端加密

静态数据和传输中的数据可以在 Amazon 中进行加密 DataZone。

CloudTrail 用于监控 API 调用

DataZone Amazon 与 AWS CloudTrail一项服务集成，该服务可记录用户、角色或 AWS 服务在亚马逊中执行的操作 DataZone。

通过收集的信息 CloudTrail，您可以确定向亚马逊发出的请求 DataZone、发出请求的 IP 地址、谁提出请求、何时提出请求以及其他详细信息。

Amazon 的弹性 DataZone

AWS 全球基础设施是围绕 AWS 区域 可用区构建的。 AWS 区域 提供多个物理隔离和隔离的可用区，这些可用区通过低延迟、高吞吐量和高度冗余的网络连接。利用可用区，您可以设计和操作在可用区之间无中断地自动实现失效转移的应用程序和数据库。与传统的单个或多个数据中心基础设施相比，可用区具有更高的可用性、容错性和可扩展性。

有关 AWS 区域 和可用区的更多信息，请参阅AWS 全球基础设施。

除了 AWS 全球基础设施外，Amazon 还 DataZone 提供多项功能来帮助支持您的数据弹性和备份需求。

主题

- 数据源弹性
- 资产弹性
- 资产类型和元数据形成弹性
- 词汇表弹性
- 全球搜索弹性
- 订阅弹性
- 环境弹性
- 环境蓝图弹性
- 项目弹性
- RAM 弹性
- 用户配置文件管理弹性

- 域弹性

数据源弹性

在 Amazon DataZone 可用性事件期间，DataSource任务将定期重试，最长 24 小时。如果任务由于配置错误而失败，则会发出一个DataSourceRunFailed事件。如果 Amazon DataZone 域配置 AmazonDataZoneDomainExecutionRole 了 KMS 密钥，并且在任务运行期间无法访问该密钥，则运行将以该INACCESSIBLE状态结束。恢复 KMS 访问权限后，应手动更新任务以触发向可用状态的过渡。

资产弹性

在 Amazon 中 DataZone，资产是版本控制的。如果资产的某个版本需要回滚，则可以使用上一个稳定版本的内容创建新版本。可以发布资源版本。除非发布新版本，否则无法编辑资源的已发布版本。可以订阅已发布的资产（又名上市）。为了防止对某项资源进行新订阅，可以取消发布该资产。取消发布资源不会对现有订阅产生影响。删除资源将删除该资源的所有未发布版本。资源的已发布版本必须单独删除。只有在没有订阅的情况下才能删除资源的已发布版本。

资产类型和元数据形成弹性

在 Amazon 中 DataZone，资产类型和元数据表单类型是版本控制的。如果资源正在使用某一资产类型，则无法将其删除。如果资产类型或资产正在使用元数据表单类型，则无法将其删除。如果你不 metadata-form-type 想将特定内容用于策展，你可以禁用它们，这不会影响它已经附加到的内容。

词汇表弹性

在 Amazon 中 DataZone，如果术语表和词汇表术语正在使用中，则无法将其删除。如果你不想使用特定的词汇表或术语表术语进行整理，你可以将其禁用，这不会影响已经附加到的词汇表或词汇表。

全球搜索弹性

在 Amazon 中 DataZone，可以通过全球搜索发现已发布的资产（又名清单）。可以通过取消发布资源来回滚该资源的发布。取消发布资源不会影响现有订阅。通过重新发布已发布的资源，可以将该资源回滚到该资源的特定版本。这不会影响现有订阅。

订阅弹性

在亚马逊 DataZone，SubscriptionGrant 配送将在失败之前尝试两次退役。如果失败，则必须手动将其删除才能重试。如果 Amazon DataZone 无法撤销订阅权限，则删除订阅可能会失败。应该解决潜在的

错误，或者可以在 DeleteSubscriptionGrant API操作中使用该retainPermissions标志来强制从Amazon删除授权， DataZone 而无需撤销权限。

如果 Amazon DataZone 域配置了 KMS 密钥，并且在SubscriptionGrant工作流程中无法访问该密钥，则AmazonDataZoneDomainExecutionRole会标记授权INACCESSIBLE。恢复 KMS 访问权限后，必须删除并重新创建INACCESSIBLE授权。

环境弹性

如果 Amazon DataZone 域配置AmazonDataZoneDomainExecutionRole了 KMS 密钥，并且在环境工作流程中无法访问该密钥，则环境将被标记INACCESSIBLE。恢复 KMS 访问权限后，必须删除并重新创建INACCESSIBLE环境。环境创建将在失败之前尝试两次退役。如果失败，则必须手动将其删除才能重试。如果环境工作流程失败，环境将进入失败状态。此时，只能将其删除并重新创建。

环境蓝图弹性

在 Amazon 中 DataZone，如果存在任何底层环境配置文件，则无法删除环境蓝图。

项目弹性

在 Amazon 中 DataZone，如果项目包含任何环境，则无法删除。

RAM 弹性

有关 RAM 弹性信息，请参阅 https://docs.aws.amazon.com/ram/latest/userguide/ security-disaster-recovery-resiliency .html。

用户配置文件管理弹性

有关用户配置文件弹性的信息，请参阅AWS 身份中心。

域弹性

在 Amazon 中 DataZone，如果域名包含项目或数据源，则无法将其删除。

Amazon 的基础设施安全 DataZone

作为一项托管服务，Amazon DataZone 受到 AWS 全球网络安全的保护。有关 AWS 安全服务以及如何 AWS 保护基础设施的信息，请参阅AWS 云安全。要使用基础设施安全的最佳实践来设计您的 AWS 环境，请参阅 S AWS ecurity Pillar Well-Architected Fram ework 中的基础设施保护。

您可以使用 AWS 已发布的 API 调用 DataZone 通过网络访问亚马逊。客户端必须支持以下内容：

- 传输层安全性协议 (TLS) 我们要求使用 TLS 1.2，建议使用 TLS 1.3。
- 具有完全向前保密 (PFS) 的密码套件，例如 DHE（临时 Diffie-Hellman）或 ECDHE（临时椭圆曲线 Diffie-Hellman）。大多数现代系统（如 Java 7 及更高版本）都支持这些模式。

此外，必须使用访问密钥 ID 和与 IAM 主体关联的秘密访问密钥来对请求进行签名。或者，您可以使用 AWS Security Token Service（AWS STS）生成临时安全凭证来对请求进行签名。

亚马逊的跨服务混淆了副手预防 DataZone

混淆代理问题是一个安全性问题，即不具有操作执行权限的实体可能会迫使具有更高权限的实体执行该操作。在中 AWS，跨服务模仿可能会导致混乱的副手问题。一个服务（呼叫服务）调用另一项服务（所谓的服务）时，可能会发生跨服务模拟。可以操纵调用服务以使用其权限对另一个客户的资源进行操作，否则该服务不应有访问权限。为了防止这种情况，我们 AWS 提供了一些工具，帮助您保护所有服务的数据，这些服务委托人已被授予访问您账户中资源的权限。

我们建议在资源策略中使用 aws: SourceAccount 全局条件上下文密钥来限制 Amazon DataZone 向该资源提供的其他服务的权限。SourceAccount 如果您想允许该账户中的任何资源与跨服务使用相关联，请使用 aws:。

Amazon 的配置和漏洞分析 DataZone

AWS 处理基本的安全任务，例如客户机操作系统 (OS) 和数据库修补、防火墙配置和灾难恢复。这些流程已通过相应第三方审核和认证。有关更多信息，请参阅责任 AWS 共担模型。

要添加到允许列表的域名

要使亚马逊 DataZone 数据门户能够访问亚马逊 DataZone 服务，您必须将以下域添加到数据门户尝试访问该服务的网络上的允许列表中。

- `*.api.aws`
- `*.on.aws`

监控亚马逊 DataZone

监控是维护 Amazon DataZone 和您的其他 AWS 解决方案的可靠性、可用性和性能的重要组成部分。AWS 提供以下监控工具，用于监视 Amazon DataZone，在出现问题时进行报告，并在适当时自动采取措施：

- Amazon 会实时 CloudWatch监控您的 AWS 资源和您运行 AWS 的应用程序。您可以收集和跟踪指标，创建自定义的控制平面，以及 设置警报以在指定的指标达到您指定的阈值时通知您或采取措施。例如，您可以 CloudWatch 跟踪您的 Amazon EC2 实例的 CPU 使用率或其他指标，并在需要时自动启动新实例。有关更多信息，请参阅 Amazon CloudWatch 用户指南。
- Amazon CloudWatch Logs 允许您监控、存储和访问来自 Amazon EC2 实例和其他来源的日志文件。 CloudTrail CloudWatch 日志可以监视日志文件中的信息，并在达到特定阈值时通知您。您还可以在高持久性存储中检索您的日志数据。有关更多信息，请参阅 Amazon CloudWatch 日志用户指南。
- Amazon EventBridge 可用于实现 AWS 服务自动化，并自动响应系统事件，例如应用程序可用性问题或资源更改。来自 AWS 服务的事件几乎实时 EventBridge 地传送到。您可以编写简单的规则来指示您关注的事件，并指示要在事件匹配规则时执行的自动化操作。有关更多信息，请参阅 Amazon EventBridge 用户指南。
- AWS CloudTrail捕获由您的账户或代表您的 AWS 账户进行的 API 调用和相关事件，并将日志文件传输到您指定的 Amazon S3 存储桶。您可以识别哪些用户和帐户拨打了电话 AWS、发出呼叫的源 IP 地址以及呼叫发生的时间。有关更多信息，请参阅 AWS CloudTrail 《用户指南》。

监控亚马逊中的亚马逊 DataZone 事件 EventBridge

您可以在中监控 Amazon DataZone 事件 EventBridge，它会提供来自您自己的应用程序、 software-as-a-service (SaaS) 应用程序和 AWS 服务的实时数据流。 EventBridge将该数据路由到目标，例如 AWS Lambda 和 Amazon 简单通知服务。这些事件与 Amazon Events 中显示 CloudWatch 的事件相同，Amazon Events 提供描述 AWS 资源变化的近乎实时的系统事件流。

有关更多信息，请参阅 通过 Amazon EventBridge 默认总线处理事件。

使用记录亚马逊 DataZone API 调用 AWS CloudTrail

DataZone Amazon 与 AWS CloudTrail一项服务集成，该服务可记录用户、角色或 AWS 服务在亚马逊中执行的操作 DataZone。 CloudTrail 将亚马逊的所有 API 调用捕获 DataZone 为事件。捕获

的调用包括来自亚马逊 DataZone 控制台的调用和对亚马逊 DataZone API 操作的代码调用。如果您创建了跟踪，则可以允许将 CloudTrail事件持续传输到 Amazon S3 存储桶，包括针对亚马逊的事件 DataZone。如果您未配置跟踪，您仍然可以在 CloudTrail 控制台的 “事件历史记录” 中查看最新的事件。通过收集的信息 CloudTrail，您可以确定向亚马逊发出的请求 DataZone、发出请求的 IP 地址、谁提出请求、何时提出请求以及其他详细信息。

要了解更多信息 CloudTrail，请参阅《AWS CloudTrail 用户指南》。

亚马逊 DataZone 信息位于 CloudTrail

CloudTrail 在您创建账户 AWS 账户 时已在您的账户上启用。当 Amazon DataZone 管理控制台中发生活动时，该活动会与其他 AWS 服务 CloudTrail 事件一起记录在事件历史记录中。您可以在中查看、搜索和下载最近发生的事件 AWS 账户。有关更多信息，请参阅使用事件历史记录查看 CloudTrail 事件。

要持续记录您的 AWS 账户事件（包括 Amazon 的事件） DataZone，请创建跟踪。跟踪允许 CloudTrail 将日志文件传输到 Amazon S3 存储桶。预设情况下，在控制台中创建跟踪记录时，此跟踪记录应用于所有 AWS 区域。跟踪记录 AWS 分区中所有区域的事件，并将日志文件传送到您指定的 Amazon S3 存储桶。此外，您可以配置其他 AWS 服务，以进一步分析和处理 CloudTrail 日志中收集的事件数据。有关更多信息，请参阅下列内容：

- 创建跟踪记录概述
- CloudTrail 支持的服务和集成
- 配置 Amazon SNS 通知 CloudTrail
- 接收来自多个区域的 CloudTrail 日志文件和接收来自多个账户的 CloudTrail 日志文件

Amazon 的所有 DataZone 操作都由记录 CloudTrail。

对亚马逊进行故障排除 DataZone

如果您在与 Amazon 合作时遇到访问被拒绝问题或类似困难， DataZone请参阅本节的主题。

对亚马逊 AWS Lake Formation 权限进行故障排除 DataZone

本节包含您在遇到时可能遇到的问题的疑难解答说明为亚马逊配置 Lake Formation 权限 DataZone。

数据门户中的错误消息	解决方案
无法担任数据访问角色。	当 Amazon DataZone 无法假设您在账户DefaultDataLakeBlueprint中启用时使用的AmazonDataZoneGlueDataAccessRole，则会显示此错误。要解决此问题，请访问您的数据资产所在账户中的 AWS IAM 控制台，并确保与 Amazon DataZone 服务委托人AmazonDataZoneGlueDataAccessRole有正确的信任关系。有关更多信息，请参阅 AmazonDataZoneGlueAccess-<region>-<domainId>。
数据访问角色没有必要的权限来读取您尝试订阅的资产的元数据。	当 Amazon DataZone 成功担任该AmazonDataZoneGlueDataAccessRole角色但该角色没有必要的权限时，就会显示此错误。要修复此问题，请转到您的数据资产所在账户中的 AWS IAM 控制台，并确保该角色已AmazonDataZoneGlueManageAccessRolePolicy附加该数据。有关更多信息，请参阅 AmazonDataZoneGlueAccess-<region>-<domainId>。
资产是一种资源链接。Amazon DataZone 不支持订阅资源链接。	当您尝试发布到亚马逊的资产是指向 AWS GI DataZone ue 表的资源链接时，就会显示此错误。
资产不由 La AWS ke Formation 管理。	此错误表示未对您要发布的资产强制执行 AWS Lake Formation 权限。在以下情况下可能会发生这种情况。

数据门户中的错误消息	解决方案
	• 该资产的亚马逊 S3 位置未在 La AWS ke Formation 中注册。要解决此问题，请使用表格所在的账户登录您的 L AWS ake Formation 控制台，然后在 L AWS ake Formation 模式或混合模式下注册 Amazon S3 位置。有关更多信息，请参阅 Registering an Amazon S3 location（注册 Amazon S3 位置）。有几种情况需要进一步修改。其中包括加密的 AmazonS3 存储桶或跨账户 S3 存储桶和 Glue 目录设置 AWS 。在这种情况下，可能需要修改 KMS 和/或 S3 设置。有关更多信息，请参阅 Registering an encrypted Amazon S3 location。 • Amazon S3 位置已在 AWS Lake Format AllowedPrincipal ion 模式下注册，但是 IAM 已添加到表的权限中。要解决此问题，您可以 AllowedPrincipal从表的权限中移除 IAM，也可以在混合模式下注册 S3 位置。有关更多信息，请参阅关于升级到 Lake Formation 权限模型。如果您的 S3 位置已加密，或者 S3 位置与您的 AWS Glue 表位于不同的账户中，请按照注册加密的 Amazon S3 营业地点中的说明进行操作。

数据门户中的错误消息	解决方案
数据访问角色没有必要的 Lake Formation 权限来授予对该资产的访问权限。	此错误AmazonDataZoneGlueDataAccessRole表明，您用于在账户DefaultDataLakeBlueprint中启用的，不具备亚马逊 DataZone 管理已发布资产权限的必要权限。您可以通过添加AmazonDataZoneGlueDataAccessRole作为 AWS Lake Formati AmazonDataZoneGlueDataAccessRoleon 管理员或向要发布的资产授予以下权限来解决问题。 • 描述和描述对资产所在数据库的可授予权限 • 描述、选择、描述可授予权限、选择对数据库中所有资产的可授予权限，这些资产是您希望 Ama DataZone zon 代表您管理的访问权限。

亚马逊配额 DataZone

您的 AWS 账户对每项 AWS 服务都有默认配额，以前称为限制。除非另有说明，否则，每个配额是区域特定的。

Amazon DataZone 有以下配额和限制。

资源	描述	值
数据资产类型	在一个 DataZone 域中可以创建的最大数据资产类型数量	1000
数据资产	可以在一个 Amazon DataZone 域中创建的最大数据资产数量	100 万
词汇表	你可以在一个域中创建的最大商业词汇表数量	1000
商业词汇表术语	您可以在一个域中创建的最大业务词汇表术语总数	10000
域中的环境	一个 Amazon DataZone 域中的最大环境数量	500

Amazon DataZone 用户指南的文档历史记录

下表描述了 Amazon 发布的文档 DataZone。

变更	说明	日期
AmazonDataZoneExecutionRolePolicy 以及 AmazonDataZoneFullUserAccess -政策更新	对AmazonDataZoneExecutionRolePolicy和的策略进行了更新 AmazonDataZoneFullUserAccess，以启用对数据沿袭和细粒度访问控制 API 的支持。有关更多信息，请参阅 Amazon 对 AWS 托管策略的 DataZone 更新。	2024 年 6 月 27 日
AmazonDataZoneGlueManageAccessRolePolicy -政策更新	的AmazonDataZoneGlueManageAccessRolePolicy 政策更新增加了亚马逊自助订阅功能所需的 IAM 权限，DataZone 以缩小湖形成时授予的权限范围。使用自助订阅功能，只能向带标签的资源授予湖泊形成权限。有关更多信息，请参阅 Amazon 对 AWS 托管策略的 DataZone 更新。	2024年6月14日
AmazonDataZoneFullAccess -政策更新	的政策更新AmazonDataZoneFullAccess 使得 Amazon DataZone 管理控制台能够代表用户使用域和项目标签创建密钥。还包括允许域名所有者账户的管理员查看关联账户的账户关联状态的`ram:ListResourceSharePermissions` 操作。有关更多信息，请参阅 Amazon	2024年6月14日

	对 AWS 托管策略的 DataZone 更新。	
AmazonDataZoneDomainExecutionRolePolicy -政策更新	的政策更新为AmazonDataZoneDomainExecutionRolePolicy 亚马逊添加了新的 API DataZone ，使用户能够为其亚马逊 DataZone 环境配置操作。有关更多信息，请参阅 Amazon 对 AWS 托管策略的 DataZone 更新。	2024年6月14日
AmazonDataZoneSageMakerProvisioning -新政策	名为的新政策AmazonDataZoneSageMakerProvisioning授 DataZone 予亚马逊与亚马逊 SageMaker互操作所需的权限。有关更多信息，请参阅 Amazon 对 AWS 托管策略的 DataZone 更新。	2024 年 4 月 30 日
AmazonDataZoneSageMakerEnvironmentRolePermissionsBoundary -新的权限边界	新的权限边界已调用 AmazonDataZoneSageMakerEnvironmentRolePermissionsBoundary。当您通过亚马逊 DataZone 数据门户创建亚马逊 SageMaker 环境时，亚马逊会 DataZone 将此权限边界应用于在创建环境期间生成的 IAM 角色。权限边界限制了 Amazon DataZone 创建的角色和您添加的任何角色的范围。有关更多信息，请参阅 Amazon 对 AWS 托管策略的 DataZone 更新。	2024 年 4 月 30 日

AmazonDataZoneSageMakerAccess -新政策	名为的新政策AmazonDataZoneSageMakerAccess授DataZone 予亚马逊授予用户访问亚马逊 SageMaker环境中各种资源所需的权限。有关更多信息，请参阅 Amazon 对 AWS 托管策略的 DataZone 更新。	2024 年 4 月 30 日
AmazonDataZoneFullAccess -政策更新	对AmazonDataZoneFullAccess策略的更新，增加了 `DescribeSecurityGroups` 操作访问权限，以提高账户管理员的可用性，在控制台中配置蓝图和`GetPolicy` 操作以帮助检索有关指定托管策略的信息。有关更多信息，请参阅 Amazon 对 AWS 托管策略的 DataZone 更新。	2024 年 4 月 30 日
AmazonDataZoneS3Manage---新角色 <region><domainId>	名为 AmazonDataZoneS3Manage- <region>的新角色<domainId>用于亚马逊致 DataZone 电 AWS Lake Formation 注册亚马逊简单存储服务 (Amazon S3) 地点。AWS Lake Formation 在访问该位置的数据时扮演这个角色。有关更多信息，请参阅 Amazon 对 AWS 托管策略的 DataZone 更新。	2024 年 4 月 1 日

AmazonDataZoneGlueManageAccessRolePolicy -政策更新	更新了AmazonDataZoneGlueManageAccessRolePolicy以启用对允许 Amazon DataZone 启用发布和数据访问权限的权限的支持。有关更多信息，请参阅 Amazon 对 AWS 托管策略的 DataZone 更新。	2024 年 4 月 1 日
AmazonDataZoneDomainExecutionRolePolicy 以及 AmazonDataZoneFullUserAccess -政策更新	更新了AmazonDataZoneDomainExecutionRolePolicy和AmazonDataZoneFullUserAccess以启用对 `CancelMetadataGenerationRun` API 的支持。有关更多信息，请参阅 Amazon 对 AWS 托管策略的 DataZone 更新。	2024 年 3 月 29 日
AmazonDataZoneFullAccess -政策更新	更新了，使用户`AmazonDataZoneFullAccess` 能够在 Amazon DataZone 管理控制台中选择自己的密钥、集群、vpc和子网，而不必在文本框中键入它们。有关更多信息，请参阅 Amazon 对 AWS 托管策略的 DataZone 更新。	2024 年 3 月 13 日
AmazonDataZoneDomainExecutionRolePolicy -政策更新	通过确定哪些蓝图在哪个账户和区域启用，更新了以启用对创建环境配置文件所需的ListEnvironmentBlueprintConfigurationSummaries API 的支持。AmazonDataZoneDomainExecutionRolePolicy有关更多信息，请参阅 Amazon 对 AWS 托管策略的 DataZone 更新。	2024年2月1日

AmazonDataZoneGlueManageAccessRolePolicy -政策更新	更新了AmazonDataZoneGlueManageAccessRolePolicy以启用对 AWS Lake Formation 混合模式的支持。有关更多信息，请参阅 Amazon 对 AWS 托管策略的 DataZone 更新。	2023 年 12 月 14 日
AmazonDataZoneFullUserAccess 以及 AmazonDataZoneDomainExecutionRolePolicy -政策更新	亚马逊 DataZone 更新了AmazonDataZoneFullUserAccess和AmazonDataZoneDomainExecutionRolePolicy政策，以支持亚马逊 DataZone中由人工智能驱动的生成式数据描述功能。有关更多信息，请参阅 Amazon 对 AWS 托管策略的 DataZone 更新。	2023 年 11 月 28 日
AmazonDataZoneEnvironmentRolePermissionsBoundary -政策更新	Amazon 对AmazonDataZoneEnvironmentRolePermissionsBoundary托管策略 DataZone 进行了更新，其中包括根据ResourceTag 条件限定的额外athena:GetQueryResultsStream 权限。有关更多信息，请参阅 Amazon 对 AWS 托管策略的 DataZone 更新。	2023 年 11 月 17 日

AmazonDataZoneRedshiftManageAccessRolePolicy -政策更新	亚马逊 DataZone 更新了AmazonDataZoneRedshiftManageAccessRolePolicy政策，取消了对该`redshift:AssociateDataShareConsumer` 操作的组织编号的检查。这使您能够在 AWS 组织之间共享资源。有关更多信息，请参阅Amazon 对 AWS 托管策略的 DataZone 更新。	2023 年 11 月 16 日
AmazonDataZoneFullUserAccess -政策更新	亚马逊 DataZone 更新了授予亚马逊完全访问权限的AmazonDataZoneFullUserAccess政策 DataZone，但不允许管理域名、用户或关联账户。有关更多信息，请参阅亚马逊对 AWS 托管政策的 DataZone 更新。	2023 年 10 月 2 日
AmazonDataZonePreviewConsoleFullAccess -政策已弃用	亚马逊 DataZone 已弃用AmazonDataZonePreviewConsoleFullAccess。有关更多信息，请参阅亚马逊对 AWS 托管 DataZone 策略的更新。	2023 年 9 月 29 日
AmazonDataZonePortalFullAccessPolicy -政策已弃用	亚马逊 DataZone 已弃用AmazonDataZonePortalFullAccessPolicy。有关更多信息，请参阅亚马逊对 AWS 托管 DataZone 策略的更新。	2023 年 9 月 29 日

AmazonDataZoneDomainExecutionRolePolicy -新政策	亚马逊 DataZone 添加了一项名为 “” 的新政策AmazonDataZoneDomainExecutionRolePolicy。这是 Amazon DataZone `AmazonDataZoneDomainExecutionRole` 服务角色的默认策略。亚马逊使用此角色 DataZone 对亚马逊 DataZone 域中的数据进行分类、发现、管理、共享和分析。您可以将该`AmazonDataZoneDomainExecutionRolePolicy` 政策附加到您的`AmazonDataZoneDomainExecutionRole` 。有关更多信息，请参阅 Amazon 对 AWS 托管策略的 DataZone 更新。	2023 年 9 月 25 日
AmazonDataZoneCrossAccountAdmin -新政策	亚马逊 DataZone 添加了一项名为的新政策 AmazonDataZoneCrossAccountAdmin，允许用户使用亚马逊 DataZone 及其关联账户。有关更多信息，请参阅 Amazon 对 AWS 托管策略的 DataZone 更新。	2023 年 9 月 19 日

AmazonDataZoneRedshiftManageAccessRolePolicy - 新政策	亚马逊 DataZone 添加了一项名为的新政策 AmazonDataZoneRedshiftManageAccessRolePolicy，该政策授予 DataZone 允许亚马逊启用数据发布和访问权限的权限。有关更多信息，请参阅 Amazon 对 AWS 托管策略的 DataZone 更新。	2023 年 9 月 12 日
AmazonDataZoneRedshiftGlueProvisioningPolicy -新政策	亚马逊 DataZone 添加了一项名为的新政策 AmazonDataZoneRedshiftGlueProvisioningPolicy，该政策向亚马逊 DataZone授予与支持的数据源进行互操作所需的权限。有关更多信息，请参阅 Amazon 对 AWS 托管策略的 DataZone 更新。	2023 年 9 月 12 日
AmazonDataZoneGlueManageAccessRolePolicy -新政策	亚马逊 DataZone 添加了一项名为 “AmazonDataZoneGlueManageAccessRolePolicy授予亚马逊向目录发布 AWS Glue 数据的 DataZone权限” 的新政策。它还授予亚马逊授予访问DataZone权限或撤销对目录中已发布的 AWS Glue 资产的访问权限的权限。有关更多信息，请参阅 Amazon 对 AWS 托管策略的 DataZone 更新。	2023 年 9 月 12 日

AmazonDataZoneFullUserAccess -新政策	亚马逊 DataZone 添加了一项名为的新政策 AmazonDataZoneFullUserAccess，该政策允许 DataZone 通过数据门户网站访问亚马逊。有关更多信息，请参阅 Amazon 对 AWS 托管策略的 DataZone 更新。	2023 年 9 月 12 日
AmazonDataZoneFullAccess -新政策	亚马逊 DataZone 添加了一项名为的新政策 AmazonDataZoneFullAccess， DataZone 通过 AWS 管理控制台提供对亚马逊的完全访问权限。有关更多信息，请参阅 Amazon 对 AWS 托管策略的 DataZone 更新。	2023 年 9 月 12 日
AmazonDataZoneEnvironmentRolePermissionsBoundary -新政策	Amazon DataZone 添加了一项名为的新政策 AmazonDataZoneEnvironmentRolePermissionsBoundary，该政策限制了其所关联的预配置 IAM 委托人。有关更多信息，请参阅 Amazon 对 AWS 托管策略的 DataZone 更新。	2023 年 9 月 12 日
托管政策更新	对 AmazonDataZonePreviewConsoleFullAccess 托管策略的更新。有关更多信息，请参阅 Amazon 对 AWS 托管策略的 DataZone 更新。	2023 年 6 月 13 日

托管政策更新	对 AmazonDataZoneProjectDeploymentPermissionsBoundary 托管策略的更新。有关更多信息，请参阅 Amazon 对 AWS 托管策略的 DataZone 更新。	2023 年 4 月 3 日
???	亚马逊 DataZone （预览版）用户指南的初始版本。	2023 年 3 月 29 日

本文属于机器翻译版本。若本译文内容与英语原文存在差异，则一律以英文原文为准。