解决方案实践

华为云数据要素流通解决方案实践

文档版本 1.0

发布日期 2024-10-23

华为技术有限公司

商标声明


和其他华为商标均为华为技术有限公司的商标。
本文档提及的其他所有商标或注册商标，由各自的所有人拥有。

注意

您购买的产品、服务或特性等应受华为公司商业合同和条款的约束，本文档中描述的全部或部分产品、服务或特性可能不在您的购买或使用范围之内。除非合同另有约定，华为公司对本文档内容不做任何明示或暗示的声明或保证。

由于产品版本升级或其他原因，本文档内容会不定期进行更新。除非另有约定，本文档仅作为使用指导，本文档中的所有陈述、信息和建议不构成任何明示或暗示的担保。

安全声明

漏洞处理流程

华为公司对产品漏洞管理的规定以“漏洞处理流程”为准，该流程的详细内容请参见如下网址：
https://www.huawei.com/cn/psirt/vul-response-process
如企业客户须获取漏洞信息，请参见如下网址：
https://securitybulletin.huawei.com/enterprise/cn/security-advisory

目 录

1 方案概述

项目背景

业务挑战

- 缺少互信环境和数据流通安全保障；
- 缺少数据全生命周期监控手段；
- 数据运营效率低：供需对接，业务审批等均线下操作；
- 数据治理和产品开发效率低：平台工具多厂商杂乱，标准规范、操作逻辑不统一。

解决方案场景

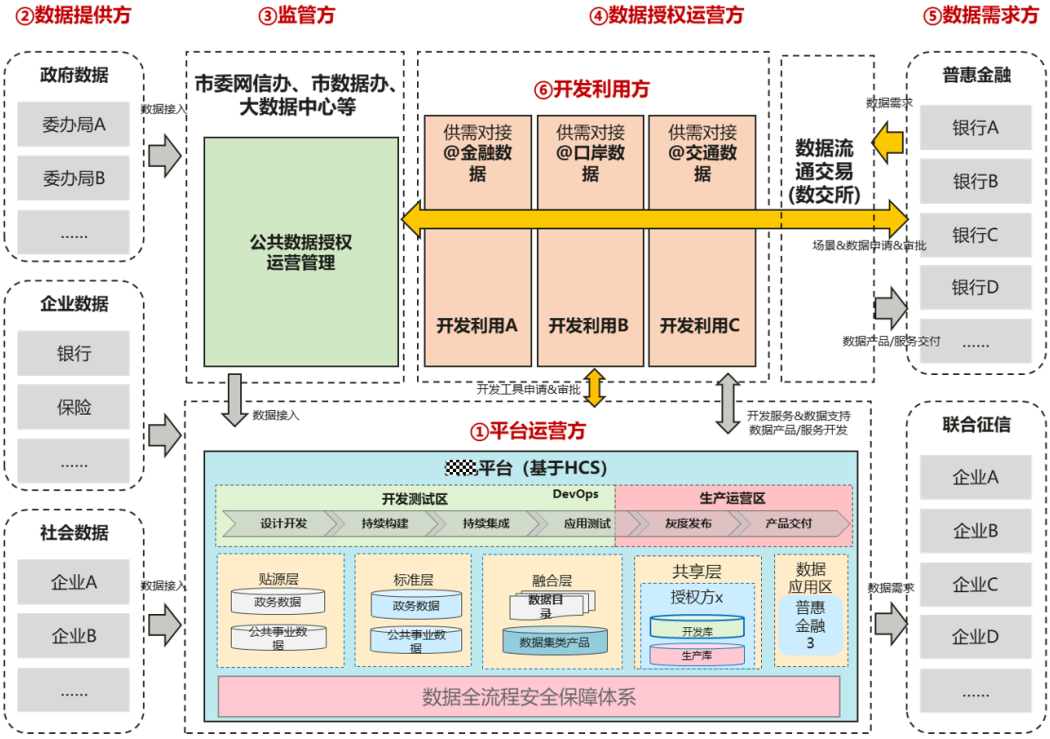
- 多场景可信数据流通：数据空间，隐私计算、区块链融合
- 数据全程合规：数据来源可确认、数据使用经授权、流通过程可追溯、 安全风险可防范
- 数据高效运营：实现授权、开发、运营、流通、监管等关键业务流程全线上化
- 凝聚生态，实现商业闭环：依托平台开展二次开发授权，凝聚开发者和供需生态，通过会员制+产品/服务订阅模式实现商业闭环

方案价值

- 一站式融合数据开发，数据高质量供给。
- 支撑多个参与全业务方线上化，合规高效运营。

整体方案设计

图 1-1 方案设计图

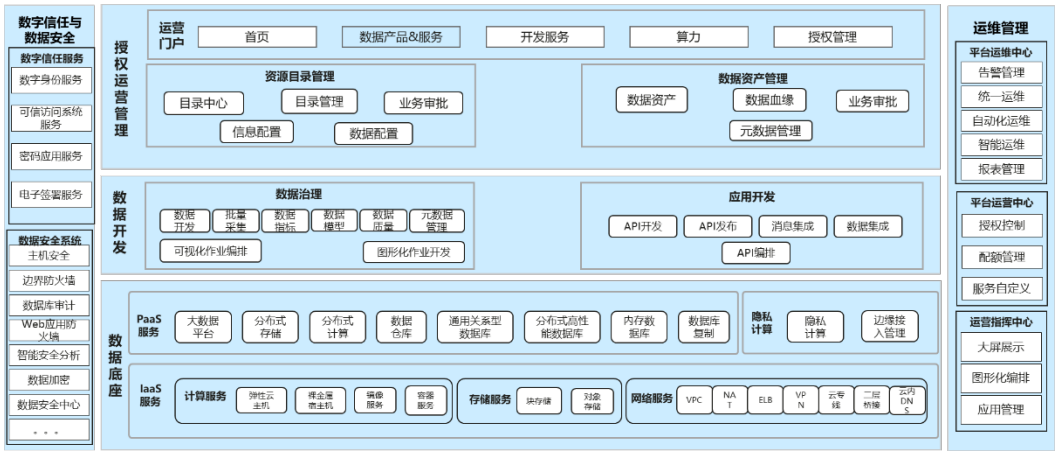


如上图所示，数据要素流通涉及六类参与方，包括平台运营方、数据提供方、监管方、数据授权运营方、数据需求方、开发利用方。其中平台运营方、授权运营方、开发利用方深度使用华为云Stack云平台和数据底座能力，包括云平台运营中心（智能云管理平台）、数据底座（MRS/DWS等）、数据治理工具（DataArts Studio/ROMA）等云服务和产品。

功能架构

运营平台整体功能设计如下，采用三横两纵架构，三横作为基础平台，主要包含数据底座、数据开发服务、数据授权运营管理三部分。两纵作为支撑部分，主要包含数字信任及数据安全、运维管理二部分。当期建设重点围绕公共数据资源承载，主要建设内容：

图 1-2 功能架构图



运营平台主要建设的功能模块如下：

- 数据底座：包含IaaS服务模块、PaaS服务模块、隐私计算模块。IaaS模块，提供计算服务、存储服务、网络服务等功能。PaaS服务模块，包提供大数据平台、数据仓库、通用关系型数据库、分布式高性能数据库、内存数据库、数据库复制等功能。隐私计算模块，提供全流程数据处理安全隐私保护能力，包含数据访问权限控制、数据使用审批、数据传输加密、数据密态计算、数据使用审计等功能。

  整体建设核心模块采用国产自主可控产品，实现可信安全、自主可控。提供大数据计算与分析相关技术组件（实时计算、资源调度、内存计算等）。打造湖仓一体、批流一体、存算分离的数据底座架构，实现对多种形态数据的汇聚、存储、计算能力。
- 数据开发服务：包含数据治理模块、应用开发模块。
- 授权运营管理：包含资源目录管理、数据资产管理模块。
- 数字信任与数据安全：包含数据安全系统、数字信任服务模块。
- 运维管理：包含平台运维中心、平台运营中心、运营指挥中心等模块。

集成架构

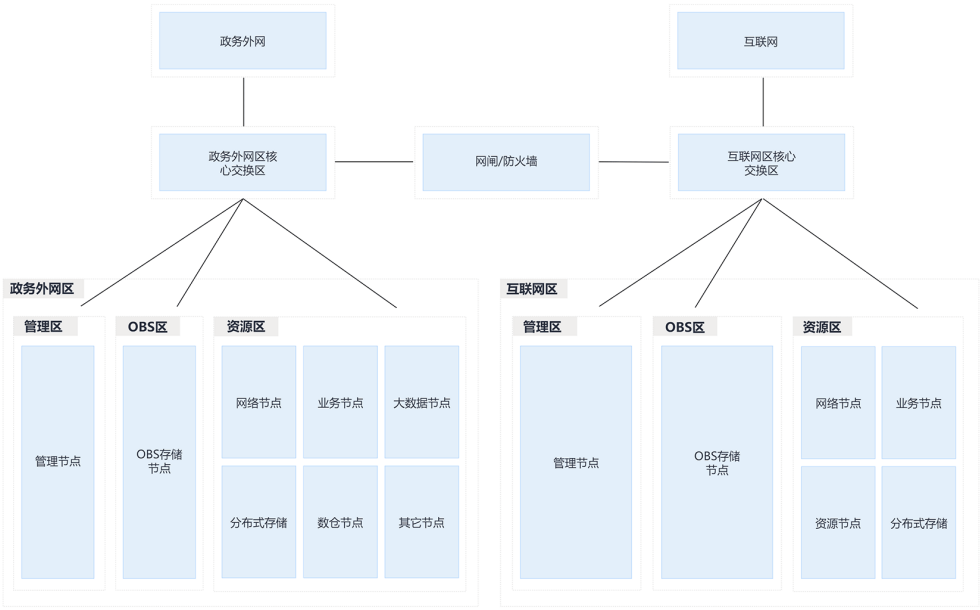
当期运营平台与周边平台、协作单位建设平台，进行系统集成对接，形成整体的公共数据开发与运营对外服务能力。

- 与监督管理方（市委网信办、数据办、大数据中心等）：作为数据授权管理方，进行公共数据授权运营管理的系统对接，通过数据场景化数据应用场景授权，进行上位管理。实现一场景、一授权，无场景不授权。
- 与数据提供方（大数据中心）：通过公共数据授权管理进行场景授权管理。授权后，数据通过多种数据汇聚采集方案，其中公共数据资源通过前置机方式，与大数据中心资源平台进行对接，采用批量或实时方式导入运营平台。
- 与开发利用方：授权主体开发利用，通过运营平台提供统一的数据开发服务工具能力，进行授权数据的加工、治理、服务、开发，实现公共数据、社会数据、行业数据等开发利用。
- 与数据需求方：数据使用方，如银行、医院、保险、社会用户等，通过授权运营管理平台，进行数据资产的开发使用或数据产品的申请使用，获取相关数据产品。

部署架构

- 本次运营平台建设主要接入公共数据资源，需依据市政务云管理办法要求建设，进行政务外网区和互联网区两个区域部署，整体方案建设满足三级等保要求。
- 针对政务外网区和互联网区，本项目规划两个region区域建设，通过政务外网区与大数据中心进行公共数据资源对接，通过互联网区域实现企业数据、部分行业数据的对接，整体符合政务云安全等级保护的要求。从当前实际业务看，本项目大部分数据来源于政务外网区，因此大数据、数仓、数据治理等数据类资源能力和相应数据安全能力主要部署在政务外网区。互联网区域提供来自互联网侧的数据需求方的数据安全访问能力。建设规模随后续企业类相关业务的增长需要再逐步扩容。

图 1-3 部署架构图



关键方案设计

【 平台资源与权限配置 】

- VDC整体规划方案

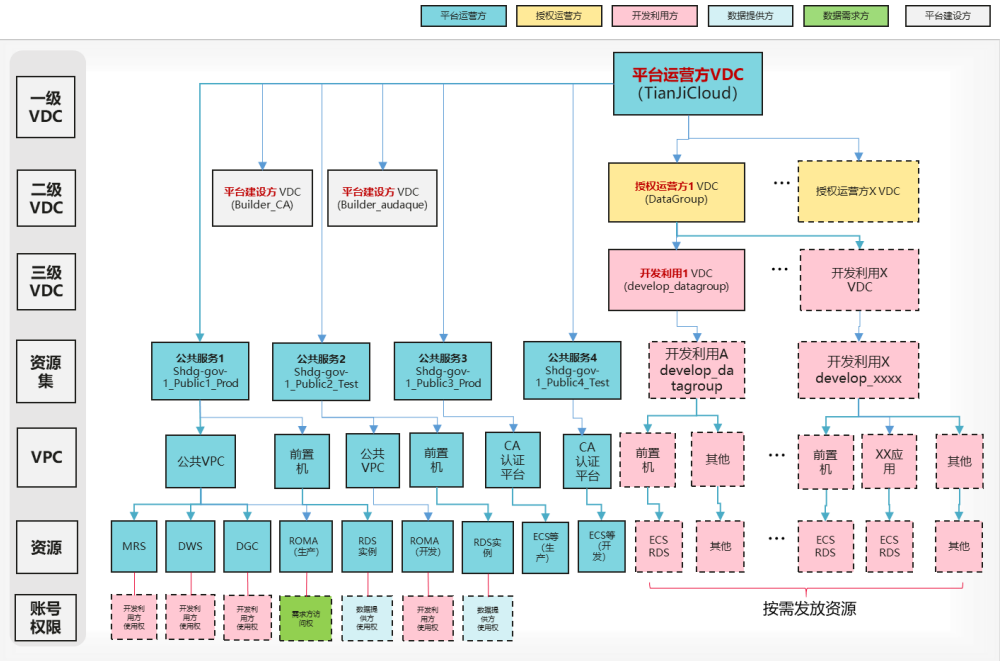
  相关概念：

  VDC是企业组织架构的逻辑映射，最多支持五层，VDC对应了企业的组织部门，VDC层级对应企业组织层级，VDC还提供了云资源配额控制、用户角色权限分配的作用。

  资源集是对云资源的分组，各个资源集之间资源相互隔离，一个VDC可以包含多个资源集，一个资源集只能属于一个VDC或企业项目。资源集可以授权给下级VDC下的用户组，只有授权了相应的资源集才能拥有相关资源权限。

  规划方案：

图 1-4 VDC 整体规划方案



如上图所示，根据资源划分的需求，将平台三类主要用户划分为三级VDC：

- 一级平台运营方VDC，作为全局唯一的一级VDC，负责统管全局公共资源，包括数据底座、数据开发工具、xx运营平台资源等；
- 二级授权运营方VDC，对应具备数据授权运营资质的企业，当前平台仅有一个二级授权运营方VDC，即数据集团；
- 二级平台建设方VDC，对应负责xx运营平台的建设的ISV，如华傲VDC、统一认证CA的VDC，在对应VDC下分配运维账号用于平台部署和维护；
- 三级开发利用方VDC，需要唯一归属指定的数据授权运营VDC，根据不同子公司或企业设置不同开发利用方VDC，将 用户添加至不同用户组，控制个人用户的访问权限；

资源集用于承载云平台的各类云服务资源，各类资源集具体划分如下：

- 公共服务1资源集，作为生产资源集，归属一级平台运营方VDC，负责承载MRS、DWS、DataArts Studio、ROMA Connect、TICS等生产实例和xx运营平台生产环境；
- 公共服务2资源集，作为开发测试资源集，归属一级平台运营方VDC，负责承载ROMA Connect开发实例、xx运营平台测试环境；
- 公共服务3资源集，作为CA认证平台生产资源集，归属一级平台运营方VDC，负责发放CA统一认证系统所需要的各类云主机、数据库、容器集群资源；
- 公共服务4资源集，作为CA认证平台开发测试资源集，归属一级平台运营方VDC，负责发放CA统一认证系统所需要的各类云主机、数据库、容器集群资源；
- 开发利用方资源集，按需为开发利用方创建资源集，用于开发利用方相关应用部署；

一级VDC下的公共资源集需要授权给二级、三级VDC下的用户组，以便各用户组具备公共资源使用权限，具体授权策略如下：

- 公共服务1、2资源集授权给二级授权运营方VDC，默认拥有全量资源权限；

- 公共服务1资源集授权给三级开发利用方VDC，默认分配DataArts Studio相关权限，以便进行数据治理开发工作；
- 公共服务2资源集授权给三级开发利用方VDC，默认分配ROMA Connect相关权限，以便进行数据服务API开发工作；
- 公共服务3、4资源集授权给二级平台建设方VDC（Builder_CA）,以便进行CA资源部署和运维工作；

- 参与方权限分配与隔离方案：华为云Stack提供三层权限管控体系满足不同租户和用户在平台的权限分配和隔离，如下图所示：

图 1-5 参与方权限分配和隔离方案图

- 第一层为组织人员管控，主要解决各方组织架构在华为云Stack的映射，并通过用户组和云服务角色权限实现各参与方用户在平台的权限管控
- 第二层为数据开发工具管控，主要解决开发利用方在DataArts Studio（简称DGC）和ROMA 工具上的权限管控，这部分主要依赖工具内部的角色权限管控能力
- 第三层为数据底座管控，主要解决各参与方在数据底座数据存储的权限管控，这部分主要通过对不同数据库账号设置不同的库操作权限实现，依赖MRS、DWS、RDS等数据库实例的权限管控体系

结合数据授权运营场景需求，各参与方在云平台的权限和隔离详细设计方案参考下表，后续实施指导中严格参考该表的权限和隔离方案进行：

表 1-1 运营平台各参与方权限分配和隔离方案

参与方	云平台	数据开发工具		数据底座（数据湖仓等）			
/	智能云管理平台	DataArts Studio	ROMA Connect	MRS	OBS	DWS	RDS

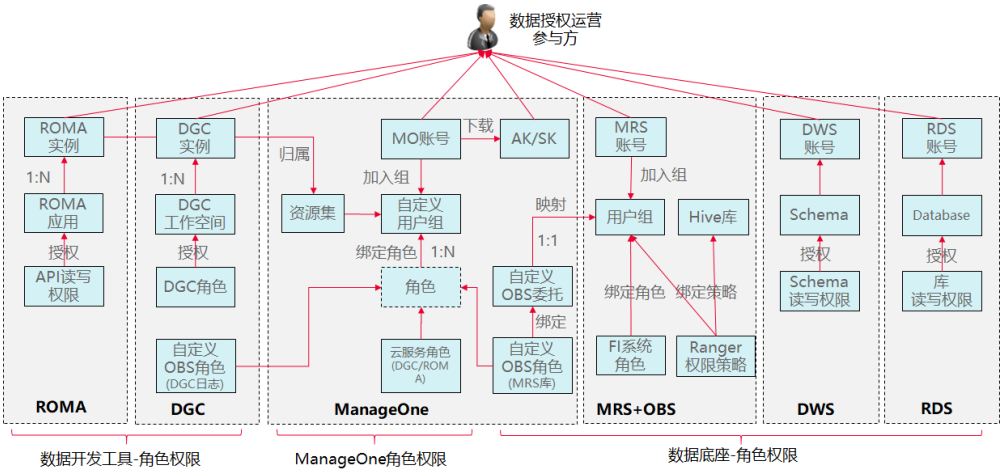
参与方	云平台	数据开发工具		数据底座（数据湖仓等）			
平台运营方	具备一级平台运营VDC管理员账号和权限 负责创建平台方的开发人员VDC账号 负责创建授权运营方VDC和相关人员账号 平台运营方全局唯一，无需隔离	具备全局实例管理员权限 负责为平台运营方创建生产和开发工作空间 负责将平台运营方开发等人员添加到工作空间	具备全局ROMA实例的管理员权限	具备MRS服务管理员权限 按需根据提供方创建对应贴源库和标准库，并作为库Owner 按需为开发利用方分配MRS库，并提供读写权限账号 按需为开发利用方授权平台运营方公共库只读权限	具备OBS服务的管理员权限 按需为平台运营方和开发利用方分配MRS数据库目录和自定义角色权限	具备DWS服务管理员权限 按需为平台运营方、开发利用方分配DWS库权限 按需为开发利用方分配DWS库权限	具备RDS服务管理员权限 负责为数据库提供方发放前置机RDS实例和账号

参与方	云平台	数据开发工具		数据底座（数据湖仓等）			
授权运营方	具备二级授权运营VDC管理员账号和权限 负责三级开发利用方VDC创建和对应开发、测试等人员账号创建 多个不同授权运营方通过不同二级VDC隔离	具备被授权实例管理员权限 负责为不同开发利用方创建生产和开发空间 负责并将开发利用方开发等人员添加到空间	具备被授权ROMA实例的管理员权限 按需为开发利用方和需求方创建ROMA应用	暂不分配账号	暂不分配权限	暂不分配账号	暂不分配账号
开发利用方	具备三级开发利用方VDC普通用户账号 不同开发利用方通过不同VDC进行隔离	具备开发利用方工作空间开发、运维、测试权限 不同开发利用方通过不同工作空间隔离	具备ROMA开发实例下指定应用的管理员权限 不同开发利用方通过不同ROMA应用隔离	具备分配给开发利用方对应MRS库读写权限 具备分配给开发利用方对应公共库的只读权限 不同开发利用方通过不同MRS账号隔离 不同开发利用方提交的任务通过不同的MRS租户隔离	具备OBS服务只读权限 具备开发利用对应MRS库所在OBS目录的读写权限	具备分配给开发利用方对应DWS库读写权限 不同开发利用方通过不同DWS账号隔离 不同开发利用方提交的后台作业通过不同队列隔离	按需分配RDS实例账号读写权限（暂无场景） 不同开发利用方通过不同RDS实例和账号隔离

参与方	云平台	数据开发工具		数据底座（数据湖仓等）			
数据提供方	无权限	无权限	无权限	无权限	无权限	无权限	按来源方分配RDS实例，并创建Database进行隔离 仅具备数据库地址和读写权限的账号给提供方
数据需求方	无权限	无权限	在ROMA生产实例分配客户端应用，并提供appkey、appsecret 不同数据需求方通过不同的客户端应用隔离	无权限	无权限	无权限	无权限
监督管理方	按需在平台运营方VDC分配只读权限账号	按需分配各工作空间访客权限	按需分配各ROMA应用只读权限	按需分配MRS只读账号权限	按需分配OBS只读账号权限	按需分配DWS只读账号权限	按需分配RDS只读账号权限

为实现上表中各参与方的权限分配和隔离，华为云Stack提供了完善的角色、权限、用户组等模型支撑用户的权限管理，具体逻辑关系模型参考下图：

图 1-6 逻辑关系模型图



华为云Stack的账号权限管理整体上总体上分成三部分，后续各场景下的角色授权操作将参考该逻辑模型图进行实施：

智能云管理平台角色权限

- 智能云管理平台提供华为云Stack账号的统一管理能力，为各个参与创建华为云Stack的登录账号并设置相关云服务的访问权限
- 智能云管理平台提供了VDC默认角色和各类云服务细粒度角色用于云服务权限管控。默认角色包括VDC管理员、VDC业务员、VDC只读用户，默认具备所有云服务的相关权限，比如VDC只读用户可以查看所有云服务但不能进行任何操作
- 针对需要限制账号的仅具备特定云服务权限的场景，智能云管理平台支持各云服务的细粒度权限创建自定义角色进行控制，比如DataArts Studio User角色，只能访问DataArts Studio服务，ROMA Administrator只能访问ROMA Connect服务
- 为方便角色统一授权，通常需要将用户账号添加到一个自定义用户组，通过给用户组授权相关角色实现对组内所有用户的授权
- 针对用户组角色的授权，需要在指定的资源集下进行，所有的角色权限都是需要关联到资源集
- 智能云管理平台账号能在个人中心下载AK/SK，用于相关云服务的访问，如OBS服务等

数据开发工具权限

- 数据工具主要包括DataArts Studio（简称DGC）和ROMA Connect两部分，各参与方可直接通过智能云管理平台账号登录华为云Stack进行数据工具服务的访问和操作
- DataArts Studio中提供了数据空间进行不同开发利用方的隔离，工作空间中提供了管理员、开发、运维、访客4类默认角色，支持自定义新角色，用于DataArts Studio中功能的细粒度控制
- ROMA Connect中提供了应用进行不同开发利用方的隔离，应用下提供了admin、modify、delete权限用于控制不同账号在应用下API操作权限

数据底座角色权限

- 数据底座目前主要包括MRS数据湖、DWS数据仓库、RDS关系型数据库三类
- 默认情况下开发利用方不分配MRS、DWS、RDS云服务的权限，只能通过由平台运营方管理员分配的数据底座相关账号进行数据访问

- 不同开发利用方通过不同的MRS账号进行隔离，需要在MRS集群的管理系统FusionInsight Manager（简称FI系统）上创建MRS账号。FusionInsight Manager上预置了各类角色进行账号权限的管控，确保相关账号仅具备授权组件的访问权限，比如限制只能访问Hive、Yarn或只能向某个MRS队列提交任务等
- MRS的账号目前主要用于Hive数据库权限的分配，这部分是通过FusionInsight Manager上提供的Ranger图形化管理界面实现的。Ranger支持通过自定义Policy策略为指定的FusionInsight Manger用户组设置指定数据库的细粒度读写权限，从而确保MRS的账号仅能基于指定的操作权限访问指定的Hive数据库
- 该项目中MRS数据湖采用存算分离架构，因此在分配MRS数据库账号的同时，需要对该账号对应的智能云管理平台账号进行OBS权限的管控，确保相应的智能云管理平台账号也只能在对应的OBS目录下进行数据的读写操作
- 通过智能云管理平台中自定义OBS角色授权给指定用户组来实现开发利用方OBS权限的管控，同时OBS角色需要通过自定义委托并映射到MRS用户组，实现MRS下对应用户组对OBS的细粒度权限管控
- DWS数据仓库中，不同开发利用方通过不同的Schema进行隔离，平台运营管理员通过命令行为开发利用方创建DWS数据仓库账号，并设置对应Schema的读写权限
- RDS关系型数据库中，不同开发利用方通过不同的RDS实例和Database进行隔离，平台运营管理员在指定的RDS实例创建Database和数据库账号，并将Database的读写权限授权给对应数据库账号

【数据授权运营平台集成】

授权运营平台包括门户、资源目录、业务中心、资产管理、统一用户体系、统一适配组件组成。

- 统一用户：数据底座与授权运营管理平台多套系统统一用户，实现业管用户、角色、权限一体化，多系统单点登录和权限控制。
- 统一目录：统一资产管理平台与数据底座多系统元数据集成对接，实现湖内、湖外统一数据目录、统一资产目录、数据血缘呈现与关系追踪。
- 统一授权：授权管理平台与数据底座集成对接，基于湖仓一体、存算分离架构，实现湖内、湖外用户场景与数据权限的统一下发。

图 1-7 周边系统集成关系（对接 MO）

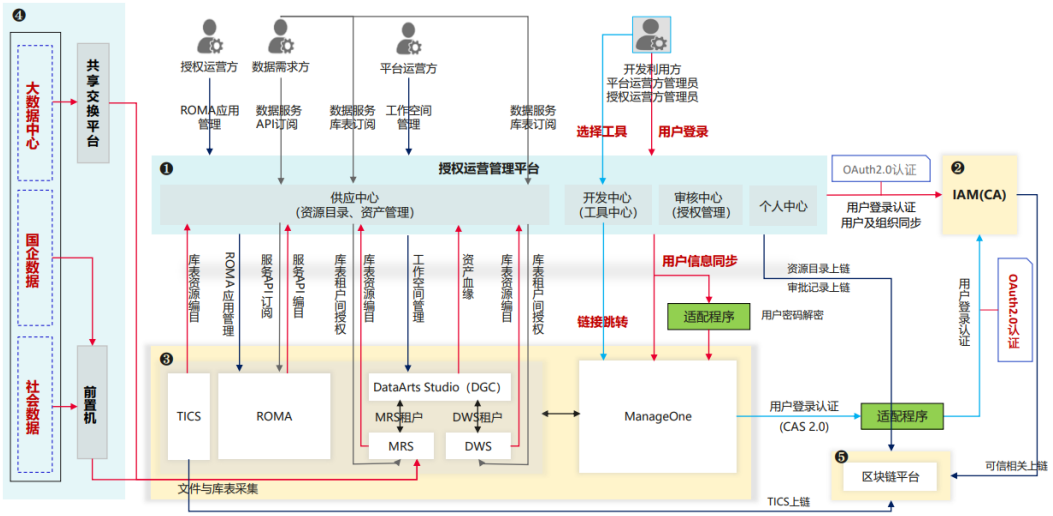


图 1-8 DGC/MRS/DWS 集成描述

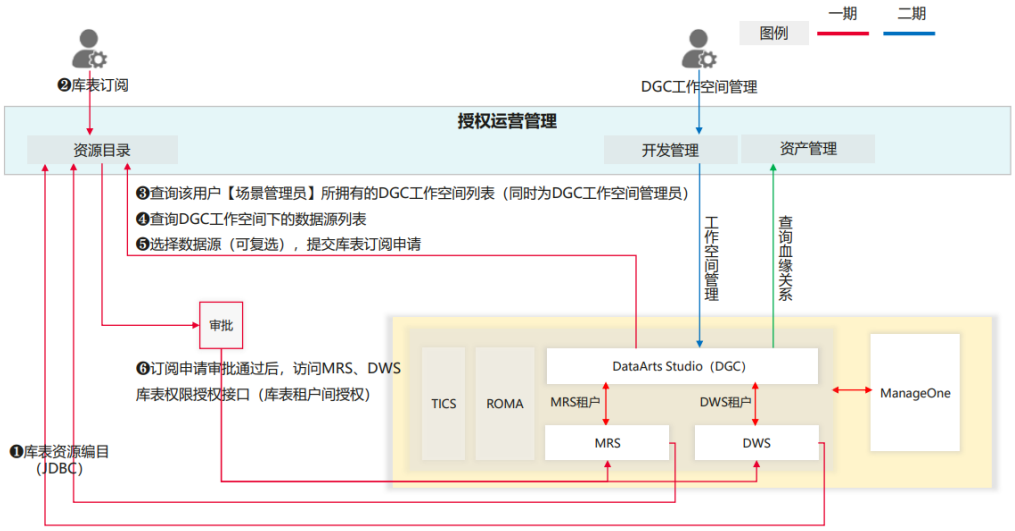
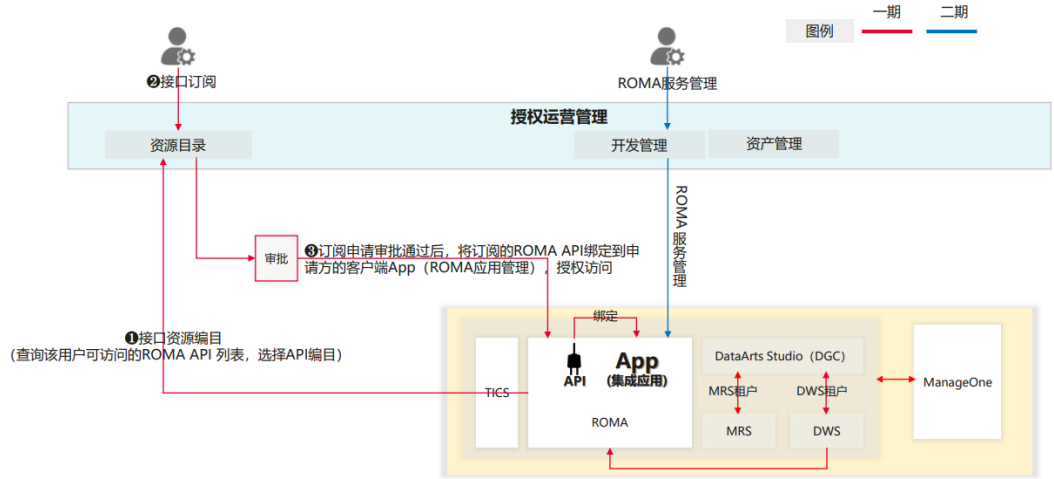


图 1-9 ROMA 集成描述

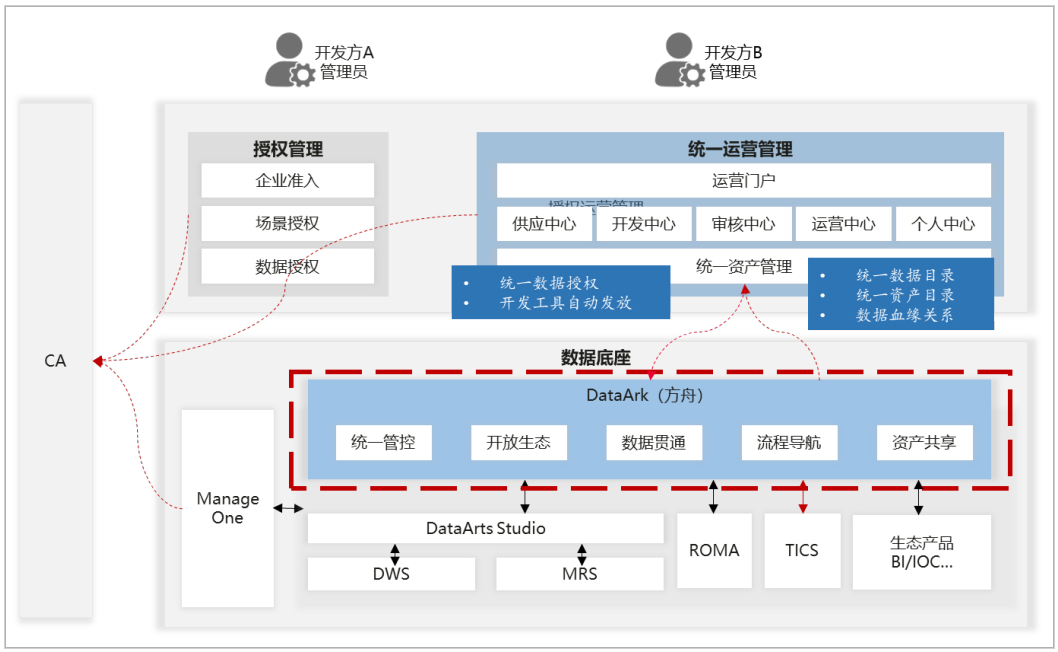


【 DataArk统一工作台 】

数智融合集成服务DataArk是融合华为DGC、ROMA等自有数据服务、集成生态伙伴治理能力、赋能行业场景经验的一站式数智融合集成使能平台。基于数据要素流通场景，DataArk实现：

- 开放框架，集成华为云Stack数据服务，提供统一API出口，简化运营平台对接。实现华为DGC、ROMA等自有云服务和集成生态伙伴的统一用户和统一角色权限管理，降低用户角色授权操作复杂度；
- 数据贯通，流程导航，提供资产共享与再部署能力，数据治理资产快速复用，提升开发利用方操作效率。

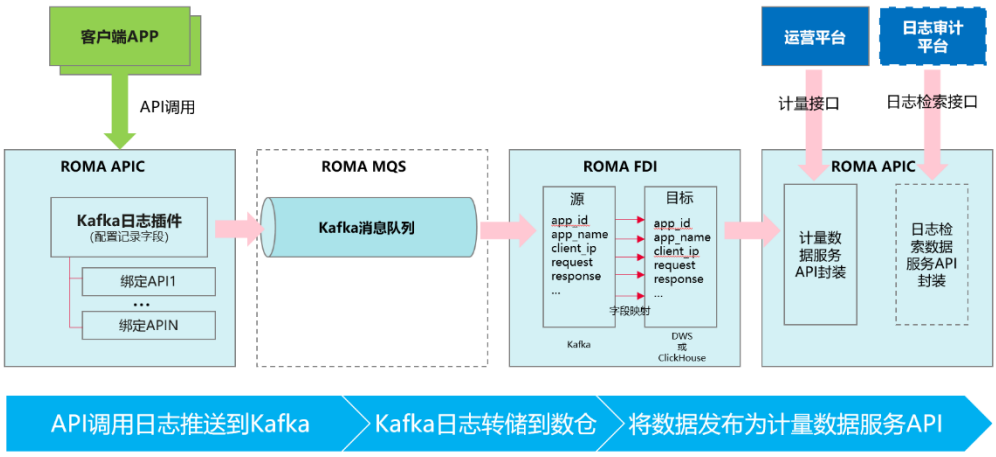
图 1-10 授权运营平台对接设计



【数据服务计量】

xx项目中，对于数据服务API的访问，需要进行计量和日志审计，要求能够记录访问请求的request header与request body等详细信息。ROMA自带的日志信息系统无法记录访问的详细信息，因此本文档给出了基于roma的kafka日志插件的一套方案。

图 1-11 数据服务计量



- 通过ROMA自身的插件功能，使用Kafka日志插件将API调用的日志详细信息（含response header和responsebody等信息）推送至ROMA的MQS中。
- 通过ROMA的FDI功能，将MQS中的日志信息实施的解析并导入至DWS的表格中。
- 通过将DWS的数据封装为API，提供计量数据和日志检索数据。

整体方案优势

- **湖仓一体存算分离：**核心平台采用业界当先的湖仓一体、存算分离架构，实现对海量的多类型数据资源进行7种汇聚方式，并实现数据分层计算存储，减少无效搬迁，一份入湖，多源使用。存算分离架构支撑未来PB级别、低成本存储计算扩容，支持与底层计算引擎融合的架构能力。
- **信创平台数据安全：**整体平台安全可信。其中核心数据存储、计算模块符合国家信创要求，周边平台模块全部采用国产化、依托于自主可控技术能力建设。

  全流程的数据安全能力。面向数据要素流通、数据资源要素化，提供身份管理、印章管理、签名验签、授权访问、权限控制等能力，并针对数据采集、传输、存储、加工、流通全流程提供数据分级分类、存储加密、数据脱敏、数据水印、授权访问等能力建设。
- **一站式便携使用：**便捷使用、全流程一站式的开发工具，面向开发按需使用。建设xx平台建设数据开发服务模块，包含数据治理服务、数据API服务、数据产品服务、应用开发服务等。面向数据运营商、企业、社会开发者提供丰富的数据开发服务，实现数据资源到数据资产、数据产品应用能力。
- **统一市场运营管控：**面向数据要素流通，进行统一产品上线流程，并全流程运营管理。建设授权管理系统模块，提供运营门户、运营管理系统，面向数据开发利用方、数据需求方等数据要素市场主体进行服务，实现用户注册、场景申请、数据商品市场、开发工具市场、算力市场、授权管理等服务能力。实现授权运营的全面流程管理、运营审核，助力数据产品、数据要素可信流通。

2 资源成本和规划

表 2-1 云平台资源清单

节点类型	节点名称	政务外网区	互联网区	规格
数据平台管理节点	管理节点1	2	2	CPU：2*64核 | 内存：16*32GB | 系统盘：2*480GB SSD
	管理节点2	12	5	CPU：2*64核 | 内存：24*32GB | 系统盘：2*960GB SSD | 数据盘：1*480GB SSD & 1*960GB SSD & 8*4TB SATA & 1*3.2T NVMe SSD
数据平台资源节点	业务节点	21	6	CPU：2*64核 | 内存：32*32GB | 系统盘：2*480GB SSD
	资源节点	13	8	CPU：2*64核 | 内存：32*32GB | 系统盘：2*480GB SSD
数据湖节点	大数据节点(类型1)	7	/	CPU：2*48核 | 内存：12*32GB | 系统盘：2*480GB SSD | 数据盘：4*960GB SSD
	大数据节点(类型2)	14	/	CPU：2*48核 | 内存：12*32GB | 系统盘：2*480GB SSD | 数据盘：4*960GB SSD
	大数据节点(类型3)	3	/	CPU：2*48核 | 内存：12*32GB | 系统盘：2*480GB SSD | 数据盘：24*1.8TB SAS
数仓节点	数仓节点	6	/	CPU：2*64/32核 | 内存：16*32GB | 系统盘：2*960GB SSD | 数据盘：12*3.84TB SSD
	数仓网关节点	2	/	CPU：2*48核 | 内存：6*32GB | 系统盘：2*480GB SSD

节点类型	节点名称	政务外网区	互联网区	规格
业务库节点	分布式数据库节点	6	/	CPU：2*64核 | 内存：32*32GB | 系统盘：2*480G SATA SSD/2*960G SATA SSD | 数据盘：12*3.84TB SSD
	分布式数据库网关	2	/	CPU：2*48核 | 内存：6*32GB | 系统盘：2*480GB SSD
对象存储节点类型1	对象存储节点1	/	2	CPU：2*32核 | 内存：12*16GB | 数据盘：2*480G SATA SSD & 1*960GB SATA SSD
	对象存储节点2	/	3	CPU：2*32核 | 内存：10*16GB | 数据盘：2*960GB SATA SSD & 4*3.2TB NVMe & 12*16TB SATA
对象存储节点类型2	对象存储节点3	2	/	CPU：2*32核 | 内存：12*16GB | 数据盘：2*480G SATA SSD & 1*960GB SATA SSD
	对象存储节点4	3	/	CPU：2*32核 | 内存：12*16GB | 数据盘：2*480G SATA SSD & 1*960GB SATA SSD
	对象存储节点5	3	/	CPU：2*32核 | 内存：12*16GB | 数据盘：2*480G SATA SSD & 1*960GB SATA SSD
	对象存储节点6	3	/	CPU：2*32核 | 内存：12*16GB | 数据盘：2*480G SATA SSD & 1*960GB SATA SSD
	对象存储节点7	3	/	CPU：2*32核 | 内存：8*16GB | 数据盘：2*480GB SATA SSD & 12*3.2TB NVMe
	对象存储节点8	4	/	CPU：2*32核 | 内存：8*32GB | 数据盘：2*960GB SATA SSD & 2*3.2TB NVMe & 36*16TB SATA
生产存储	块存储节点	4	3	CPU：2*48核 | 内存：24*16GB | 数据盘：2*480GB SSD & 12*7.68TB SSD

表 2-2 独立软件清单

软件系统	资源依赖	数量
授权运营管理系统	CentOS 7.6，MySQL（其他云服务参考云服务清单）	1

软件系统	资源依赖	数量
SSO adapter适配器	CentOS 7.6（其他云服务参考云服务清单）	1

3 实施步骤

3.1 场景一：数据授权运营场景资源&权限配置(MO 集成)

3.1.1 平台公共资源准备

3.1.1.1 场景说明

平台公共资源准备是平台使用的第一步，平台运营方管理员按照规划在云上完成平台的初始化工作，

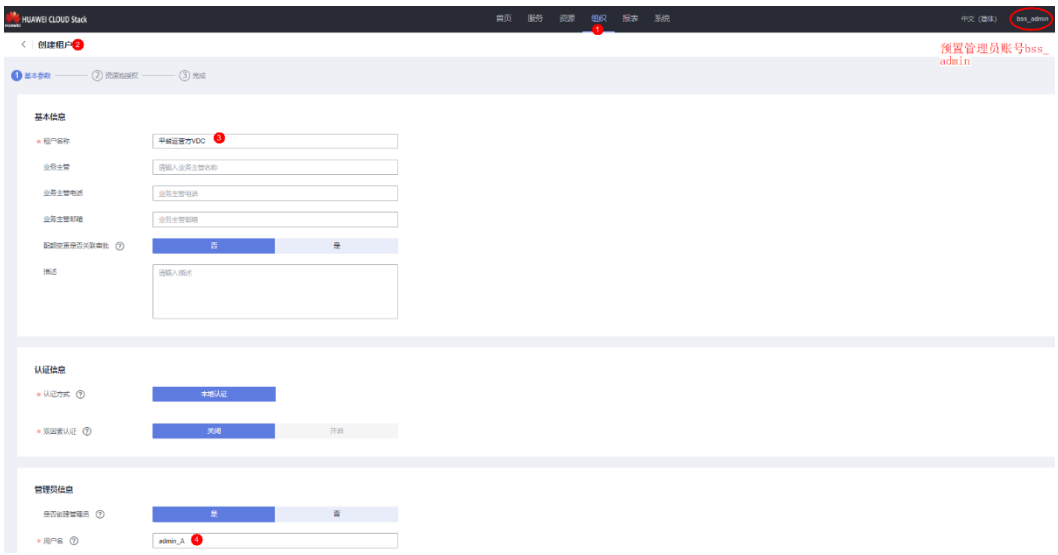
包括一二级VDC创建、公共资源集创建授权、公共云资源发放授权、数据底座初始化授权等。

此场景在平台初始搭建时完成一次即可。

3.1.1.2 一二级 VDC 发放

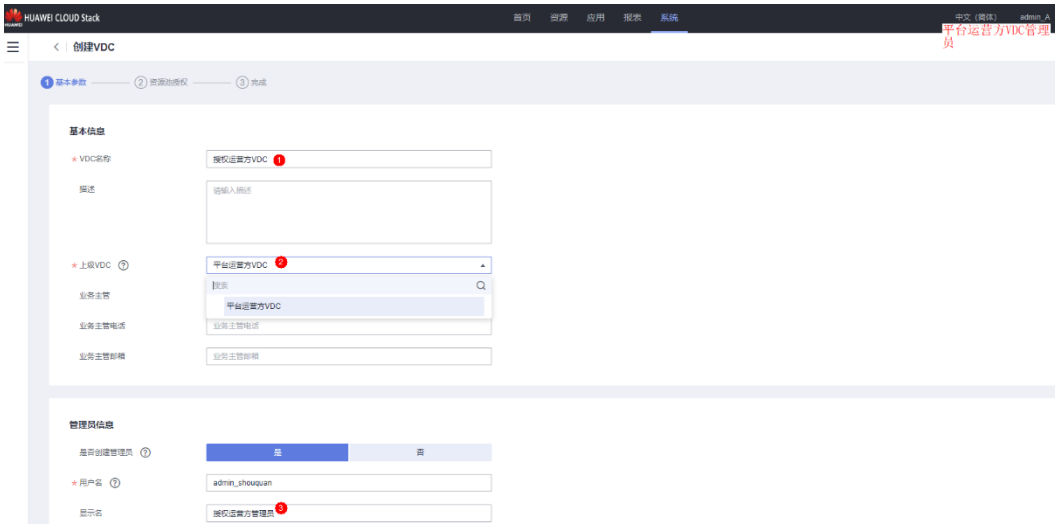
使用预置管理员账号bss_admin登录智能云管理平台平台，创建一级VDC"平台运营方VDC"，并设置VDC管理员（平台运营方-管理员）。

图 3-1 创建租户



使用上图创建的**平台运营方VDC-管理员**账号登录智能云管理平台平台，创建二级VDC"授权运营方VDC"，并设置VDC管理员（授权运营方-管理员）。

图 3-2 创建 VDC



3.1.1.3 公共资源集发放

公共服务资源集为公共数据接入和处理提供隔离，内包含必要云服务资源（DataArts Studio、MRS、DWS、ROMA Connect等）。

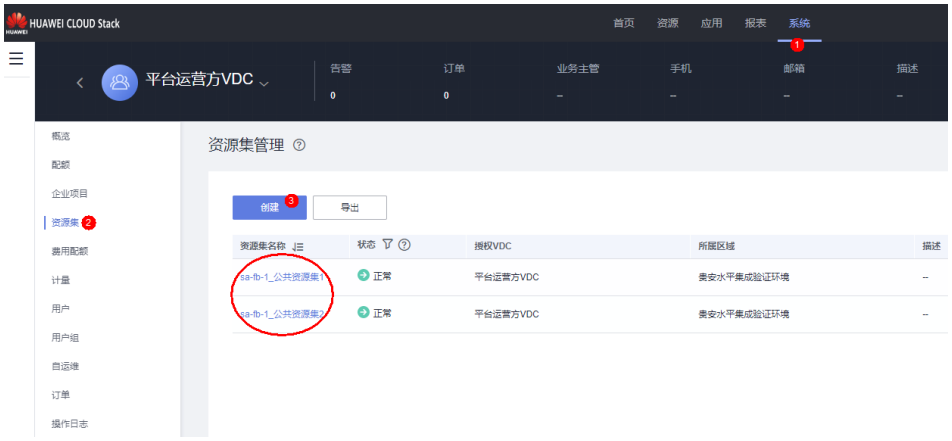
为保证云服务资源按照方案设计隔离，设置两个公共服务资源集。且不同公共资源集下的云服务实例使用VPC不相同，如实例需要通信场景，采用VPC-Peering打通，详见图1-4。

步骤1 在一级VDC下创建两个资源集：公共资源集1，公共资源集2。

- 使用一级VDC的**平台运营方-管理员账号**登录智能云管理平台页面首页，单击上方导航栏中“系统”。

- 单击“一级VDC”名称，在一级VDC下选择左侧导航栏中“资源集”，创建资源集：公共资源集1，公共资源集2。

图 3-3 创建资源集



步骤2 使用一级VDC的**平台运营方-管理员账号**为公共资源集1发放VPC1，以及VPC1下的MRS、DWS、DataArts Studio和ROMA Connect(生产)实例。

图 3-4 生产实例

步骤3 使用一级VDC的**平台运营方-管理员账号**为公共资源集2发放VPC2，以及VPC2下的ROMA Connect(开发)实例。

图 3-5 开发实例

----结束

3.1.1.4 公共资源集授权

一级VDC"平台运营方VDC"下2个公共资源集需要被正确授权给下级VDC用户，资源集下的资源才能被访问与使用。

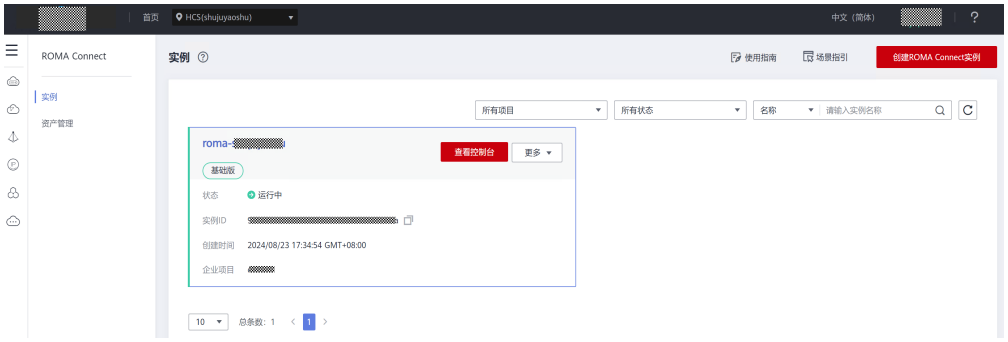
步骤1 使用一级VDC的**平台运营方-管理员**账号登录智能云管理平台平台，在“系统>资源集”列表中，单击选择“公共资源集1”；

步骤2 单击“已授权用户组”，选择“添加用户组”。在该资源集下添加用户组，选择“**授权运营方-VDC管理员**”用户组；

图 3-6 添加用户组

步骤3 使用二级VDC的**授权运营方-管理员账号**登录智能云管理平台平台，管理员账号可以访问公共服务资源集1中的所有云服务，且授权运营方-VDC管理员用户组下用户均可以访问公共服务资源集1中的所有云服务。

图 3-7 实例



----结束

3.1.1.5 用户组创建及授权

平台公共资源准备时，需对本级VDC（平台运营方VDC）和下级VDC（授权运营方VDC）的用户分别进行创建、管理及授权操作。

每个平台（即每级VDC）的不同用户组分别授予不同的云服务权限。通过对用户组粒度进行授权，实现不同用户组中的用户对云服务访问控制。

平台运营方 VDC 管理

- **创建平台运营方用户组**
  a. 平台运营方-管理员登录智能云管理平台平台，单击“一级VDC”名称，进入该VDC操作页面。
  b. 单击“用户组>创建“，创建自定义用户组；
  平台运营方（一级VDC）下自定义用户组包括：平台运营方-云服务开发、平台运营方-云服务测试。

  图 3-8 创建自定义用户组

- **授权用户组**

  用户组创建完成后，根据不同用户组职责需要，授予其对应的云服务访问权限。自定义用户组职责及权限分配详见下图**表1 平台运营方用户组职责及授权角色**

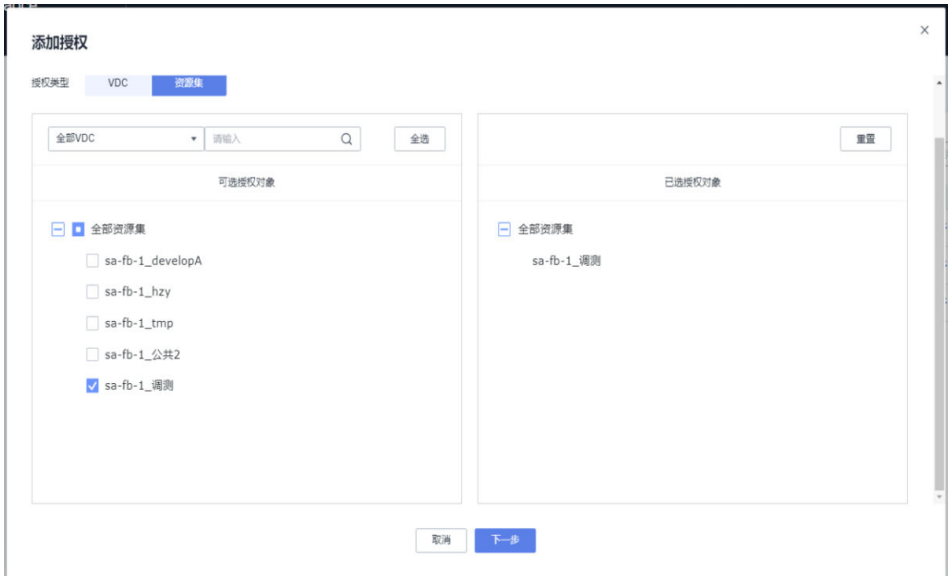
  a. 在对应用户组后，选择“用户组>添加授权”；

  图 3-9 添加授权

  b. 授权类型选择“资源集”，勾选要授权的资源集名称，单击“下一步”；

  图 3-10 资源集

  c. 在权限列表中勾选该用户组需要使用的系统角色。角色以服务为粒度，控制云服务访问权限。

  图 3-11 添加授权

表 3-1 平台运营方用户组职责及授权角色

用户组	职责	授权角色
平台运营方-开发人员	在平台运营方DataArts Studio开发空间进行开发工作	DataArts Studio User; ROMA Administrator; MRS ReadOnlyAccess; DWS ReadOnlyAccess; VPC Administrator； Server Administrator；
平台运营方-测试人员	在平台运营方DataArts Studio开发空间进行测试工作	DataArts Studio User; ROMA Administrator; MRS ReadOnlyAccess; DWS ReadOnlyAccess; VPC Administrator； Server Administrator；
平台运营方-运维人员	在平台运营方VDC进行运维工作，具体如下： 1. 将DataArts Studio开发空间的资产导入到生产空间发布； 2. 负责MRS/DWS数据库、账号的管理； 3. 根据订阅申请授权公共数据的只读权限给开发利用方；	一级VDC业务员（创建用户组>系统预置）

说明

授权角色以云服务为粒度，由于多数高阶云服务都依赖计算、存储、网络基础云服务，使用时需要同时授予**VPC Administrator**、**Server Administrator**的权限。

授权运营方 VDC 管理

- **创建授权运营方用户组。**
  a. 授权运营方管理员登录智能云管理平台平台，单击“授权运营方VDC”名称，进入该VDC管理页面。
  b. 单击“用户组>创建“，创建自定义用户组；创建授权运营方-运维人员用户组。
- **授权运营方-运维用户组角色授权。**
  a. 平台运营方-管理员登录智能云管理平台，在运维人员用户组后，选择“用户组>添加授权”；
  b. 授权类型选择“资源集”，勾选要授权的资源集名称，单击“下一步”；

图 3-12 添加授权

c. 在权限列表中勾选该用户组需要使用的系统角色。角色以服务为粒度，控制云服务访问权限。用户组职责及权限分配详见表2。

表 3-2 授权运营方-运维人员职责及授权角色

用户组	职责	授权角色
授权运营方-运维人员	将ROMA Connect开发实例的应用包导入生产实例API并发布；	ROMA Administrator; MRS ReadOnlyAccess; DWS ReadOnlyAccess; VPC Administrator; Server Administrator

说明

授权角色以云服务为粒度，由于多数高阶云服务都依赖计算、存储、网络基础云服务，使用云服务时需要授予其**VPC Administrator**、**Server Administrator**的权限。

3.1.1.6 搭建公共工作空间

创建DataArts Studio公共工作空间，用于公共接入数据的处理。并授权给平台运营方开发、测试和运维人员用户组。

- **创建公共工作空间**

  平台运营方-管理员登录DataArts Studio云服务控制台，在实例中创建“平台运营方-生产”和“平台运营方-开发”工作空间。

- **创建工作空间自定义角色**

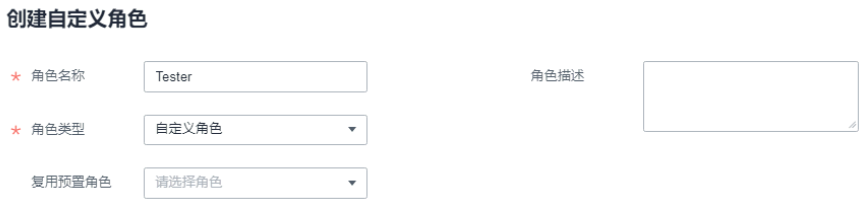
  DataArts Studio工作空间预置有管理员、开发者、运维者和访客四种角色，也可以根据对DataArts Studio不同功能的访问需要进行细粒度功能授权，自定义工作空间角色。

  a. 使用**平台运营方-管理员**账号登录DataArts Studio控制台，选择实例，单击“进入控制台”，选择“角色管理>新建"。

图 3-13 角色管理

b. 创建自定义角色“Tester”。

图 3-14 创建自定义角色



c. 根据角色职责，勾选不同功能对应操作权限。测试用户只拥有作业的查看&运行权限，勾选”云数据迁移”的”查询”权限和”数据开发”的”操作”、”查询”权限。

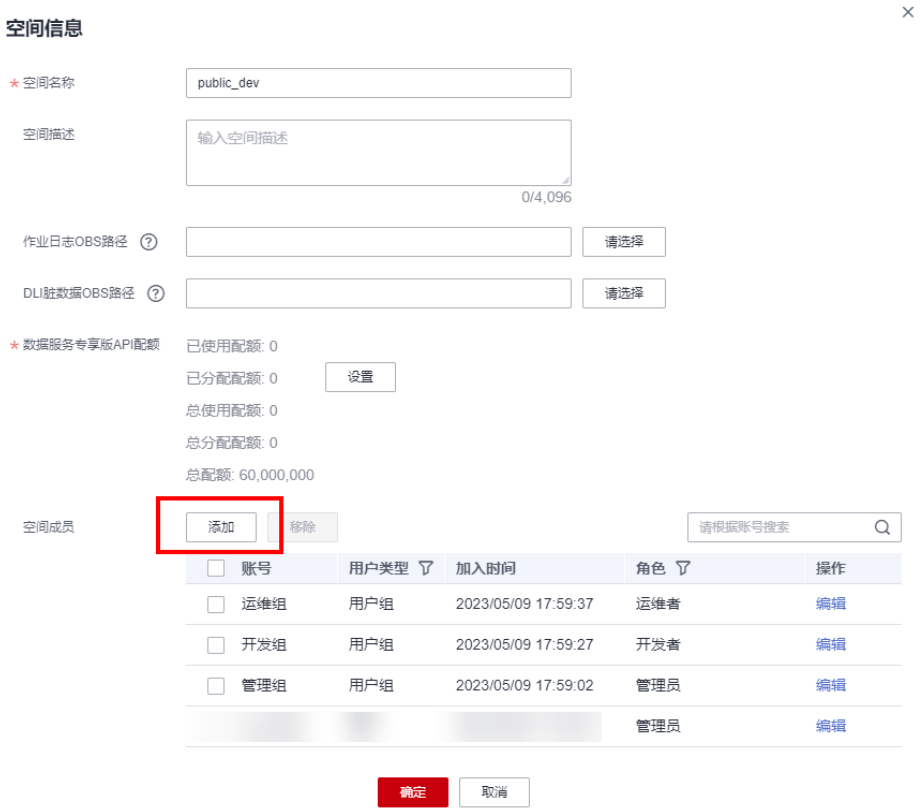
图 3-15 查看&运行权限

- **公共工作空间授权**

  平台运营方-管理员登录DataArts Studio实例，依据DataArts Studio空间角色，授予权限给对应用户组。

a. 登录DataArts Studio 控制台。选择"空间管理"，单击工作空间后对应"编辑"按钮，选择"空间成员>添加成员"。

图 3-16 空间管理



b. 选择"按用户组添加"，选择对应角色，单击“确定”。工作空间角色授权详见**表3-3**。

图 3-17 添加成员

表 3-3 工作空间角色授权

用户组	DataArts Studio 工作空间角色
平台运营方-管理员	开发/生产空间-管理员
平台运营方-开发用户组	开发空间-开发者
平台运营方-测试用户组	开发空间-Tester（自定义角色）
平台运营方-运维用户组(即平台预置VDC业务员用户组)	生产空间-运维者

- **DLF日志路径配置**

  为所有用到DataArts Studio云服务的用户组，创建日志桶存储角色，并绑定至用户组。

  a. 使用**平台运营方VDC管理员账号**账号登录智能云管理平台，选择“存储 > 对象存储服务 3.0”，进入对象存储服务界面。

  选择左侧导航栏的“并行文件系统”，进入并行文件系统控制台。

  b. 单击界面右上角的“创建并行文件系统”，进入创建页面，创建桶“mrs-obs”。

  c. 使用**平台运营方VDC管理员账号**登录智能云管理平台运营面，单击主菜单的“系统”。

  d. 选择“安全管理 > 角色管理”，创建角色。参考**表3-4**填写参数。

表 3-4 DataArts Studio 日志桶存储角色

参数类别	参数名称	说明
基本信息	名称	角色名称，如policy-dlf_log_obs_role
	作用范围	全局服务
	描述	为所有用到DataArts Studio云服务的用户组，创建日志桶存储角色
授权配置方	JSON视图	JSON视图形式展开

参数类别	参数名称	说明

JSON视图	JSON视图	JSON样例如下，在“Resource”配置中手动指定特定资源。
		● Effect（作用）
		● Action（授权项）
		● Resource（资源）
		策略示例：
		GetObject：获取对象内容、获取对象元数据
		ListMultipartUploadParts：列举已上传的段
		ListBucket：列举桶内对象
		PutObject：PUT上传、POST上传、复制对象、追加写对象、初始化上传段任务、上传段、合并段
		DeleteObject：删除对象、批量删除对象
		{
		"Version": "1.1",
		"Statement": [
		{
		"Effect": "Allow",
		"Action": [
		"obs:object:PutObject",
		"obs:object:DeleteObject",
		"obs:object:GetObject",
		"obs:object:ListMultipartUploadParts",
		"obs:bucket:ListBucket"
		],
		"Resource": [
		"obs:*:*:object:mrs-obs/dlf-log-9b5bfc8e6650450d829b3ab2d01f9462",
		"obs:*:*:object:mrs-obs/dlf-log-9b5bfc8e6650450d829b3ab2d01f9462/*",
		"obs:*:*:bucket:mrs-obs"
		]
		}
		]
		}

e. 单击“确认”，完成角色创建。

f. 将该角色绑定至所有使用DataArts Studio 云服务的用户组。

说明

OBS桶路径mrs-obs/dlf-log-9b5bfc8e6650450d829b3ab2d01f9462，其中9b5bfc8e6650450d829b3ab2d01f9462为DataArts Studio实例所在projectid，DataArts Studio的实例ID可以从DataArts Studio控制台的URI链接中获取。如图所示，DataArts Studio实例id为instanceId后数字。

图 3-18 DataArts Studio 实例 id 为 instanceId 后数字

3.1.1.7 数据底座初始化授权

MRS ECS/BMS集群支持将业务数据存储在OBS 3.0服务的并行文件系统中，使用MRS集群计算资源进行数据处理的存算分离模式，从而提供按需灵活扩展、低成本的海量数据分析方案。

在初始化数据底座资源配置时，完成创建OBS全局委托并绑定至MRS集群、修改Ranger默认权限的一次性动作。

创建 OBS 委托并绑定 MRS 集群

- 创建OBS全局委托。

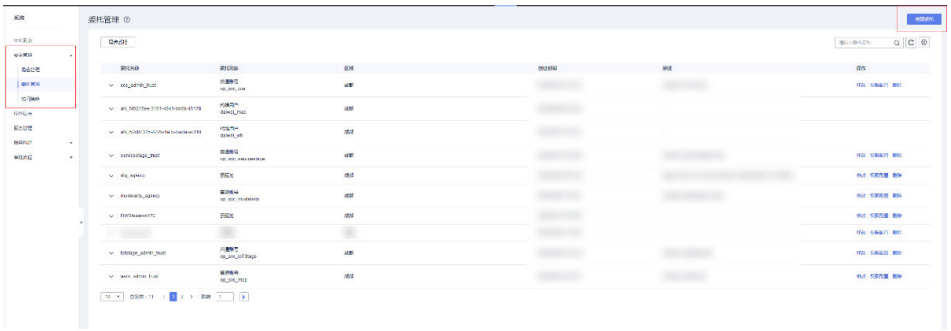
  创建OBS委托，并绑定至MRS集群，使集群内用户具备对OBS的访问权限。为MRS集群绑定一个OBS权限委托策略，以允许集群内的服务访问OBS文件系统。委托默认将对该MRS集群上所有的用户（包括内置用户）及用户组生效，一个MRS集群只可以绑定一个全局委托。

  a. 以**平台运营方VDC管理员账号**登录智能云管理平台运营面，单击主菜单的“系统”。

  b. 选择“权限管理 > 角色管理”，搜索并查看当前的OBS权限策略。

  c. 选择“权限管理 > 委托管理”，在“委托管理”界面单击“创建委托”。

  图 3-19 创建委托

  d. 在“创建委托”页面，设置“委托名称”。

  委托类型”选择“云服务”，在“云服务”中选择“弹性云服务器ECS 裸金属服务器BMS”，授权ECS或BMS调用OBS服务。

图 3-20 委托类型

e. 在“基于区域授权”区域中，单击“全局服务”，然后搜索并勾选系统预置的OBS Buckets Viewer权限。

图 3-21 基于区域授权

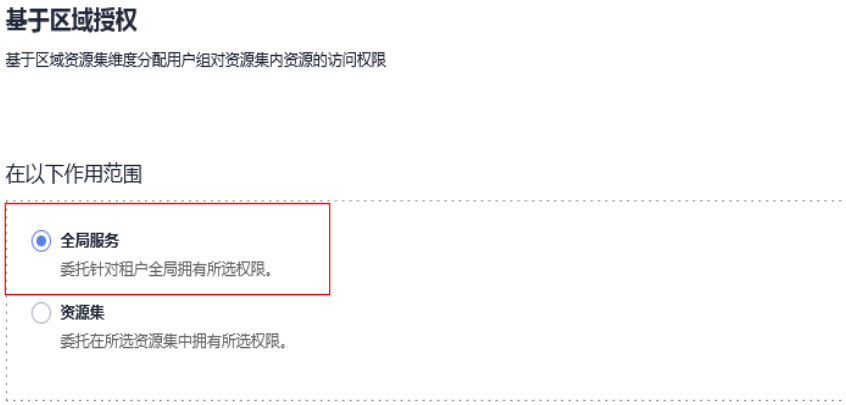


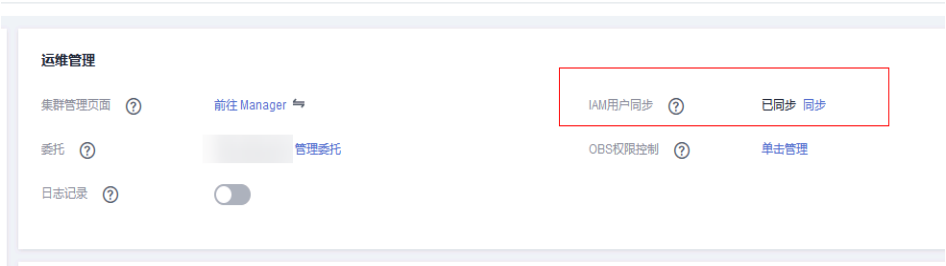
图 3-22 拥有权限

- 为MRS集群绑定全局委托。
  a. 使用**平台运营方运维人员账号**登录智能云管理平台运营面，在页面左上角服务列表中选择“EI 企业智能 > MapReduce 服务”。

b. 在导航栏选择“集群列表 > 现有集群”。单击集群名称，进入集群详情页面。

c. 在集群详情页的“概览”页签，单击“IAM用户同步”右侧的“同步”进行IAM用户同步。

图 3-23 IAM 用户同步



d. 用户同步完成后，在“概览”页签单击“管理委托”。在委托列表中选择需要绑定至当前集群的委托，然后单击“确定”。

图 3-24 管理委托

说明

- 委托变更后不能立即生效，生效时长15分钟左右。
- 变更MRS集群的委托权限时，建议通过新建权限策略和委托，再修改集群对应委托的方式来实现；直接修改旧的权限策略和委托可能会影响其他用户的正常权限控制。

配置 OBS 组件回收清理策略

组件用户删除的文件数据并不会直接被删除，而是会保存到OBS文件系统内的用户回收站目录中，本章节用于指导用户设置OBS文件系统内回收站目录的生命周期策略，以定时自动清理相关数据。

注意

- 配置集群使用存算分离方案后，必须参考本章节内容配置相关目录的生命周期策略，否则会有存储空间被占满的风险。
- 由于回收站目录是以用户维度进行创建，当MRS集群内新创建了用户且该用户具备组件数据的删除权限时，也需要参考本章节配置新用户的回收站目录清理策略。

MRS集群内各组件默认需至少配置的回收站目录如表4-5所示。

例如集群新增的用户具有以下权限时，也需在并行文件系统中创建**对应用户**回收站目录清理策略。

- 具有HDFS文件删除权限的用户。
- 具有Hive表DROP、INSERT OVERWRITE、TRUNCATE操作的用户。
- 具有HetuEngine DROP、TRUNCATE、DELETE、INSERT OVERWRITE、LOADOVERWRITE操作权限的用户。

表 3-5 存算分离场景组件默认回收站目录

组件	回收站目录
Hive	● user/omm/.Trash ● user/hive/.Trash
Spark2x	● user/omm/.Trash ● user/root/.Trash ● user/spark2x/.Trash
HetuEngine	● user/omm/.Trash ● user/hetuserver/.Trash

- 配置用户回收站目录

  除了MRS集群预置用户所涉及的回收站目录外（例如“user/omm/.Trash”），对于其他新增的有防误删需求的用户，同样需要为其配置回收站目录：user/<用户名>/.Trash。

  a. 配置当前用户所对应的OBS委托策略，至少包含了以下目录的操作权限，若未配置可参考#ZH-CN_TOPIC_0000001705437473/section165618252032创建OBS委托并绑定至MRS集群进行操作。

     – user/omm/.Trash

     – user/hive/.Trash

     – user/<新增的业务用户>/.Trash

  b. 以VDC管理员或VDC业务员账号登录智能云管理平台运营面-服务列表-存储-对象存储服务 3.0，选择“并行文件系统>文件系统名称>user”。

  c. 对应的“.Trash”文件夹若不存在需使用omm用户通过集群客户端手动创建。

     例如执行以下命令：hdfs dfs -mkdir obs://OBS并行文件系统名称/文件夹路径

- 配置 OBS 目录生命周期规则

  a. 手动创建MRS集群预置用户所涉及的回收站目录（如“user/omm/.Trash”，具体操作参考配置用户回收站目录中步骤），以及新增有防误删需求的用户回收站目录“user/<用户名>/.Trash”。

  b. 单击当前MRS集群使用的文件系统名称-生命周期规则-创建-填写参数-确定：

     表 3-6 生命周期规则创建填写参数

参数名称	描述	示例
状态	是否启用本条生命周期规则。	启用

参数名称	描述	示例
规则名称	规则名称，可自定义，用于识别不同的生命周期配置。	rule-mrs-trash
策略	策略配置范围。 ● 按前缀配置：满足指定前缀的对象将受生命周期规则管理，输入的对象前缀不能包括\:*?"<>|特殊字符，不能以/开头，不能两个/相邻。 ● 配置到整个文件系统：文件系统内所有对象都将受生命周期规则管理。 说明：为防止其他业务数据被误删除，不建议使用配置到整个文件系统或者层级较高的目录的生命周期规则。	按前缀配置
前缀	生命周期规则适用的对象前缀，MRS集群组件数据回收站目录通常为如下路径，该文件夹若不存在，需提前手动创建： user/<用户名>/.Trash	user/omm/.Trash
过期删除/天数	策略配置范围内的对象最后一次更新后时间达到指定的天数后，对象将过期并自动被OBS删除。	30天

Ranger 权限配置

- 修改ranger默认权限：任何用户均可创建库到HDFS

  ranger默认策略中，所有用户均可以在HDFS创建默认库。修改该默认权限。

  a. **平台运维方-运维人员**获取具有MRS admin权限的安全认证账号（非初始admin账号），详见4.1.2.3.1 准备工作；

  b. 进入MRS集群实例页面，单击”前往Manager”，使用步骤1获取的账号登录MRS FI页面；

图 3-25 前往 Manager

c. 在主页中选择ranger集群，或单击"集群>ranger"，进入ranger集群详情页。

图 3-26 集群>ranger

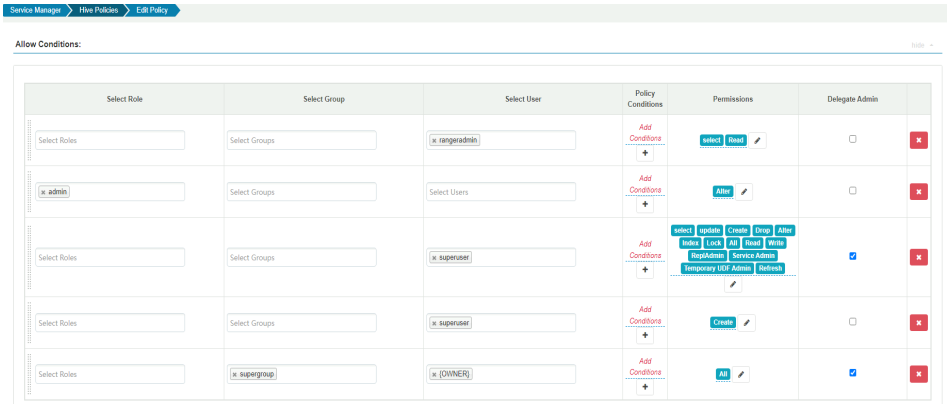
d. 单击进入Ranger WebUI“RangerAdmin”页面。

图 3-27 RangerAdmin

e. 单击hive模块，修改hive默认策略。

f. 单击权限策略中"all database"的默认权限，去掉"public"用户组的"create"权限。修改后权限配置可参考下图。

图 3-28 修改后权限配置



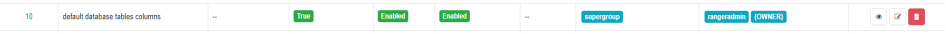
- 修改ranger默认default库建表权限

  ranger默认策略中，所有用户均可以在default库中创建数据表，修改该默认权限。

  a. 在ranger中，单击hive模块，修改hive默认策略。

  b. 单击名称为：default database tables columns后的修改按钮，修改hive默认default库的权限策略。

  图 3-29 修改 hive 默认 default 库的权限策略

  c. 在Allow Conditions允许条件中，删除public用户组create建库权限；删除superuser用户组下hive user ALL权限。

图 3-30 删除 superuser 用户组下 hive user ALL 权限

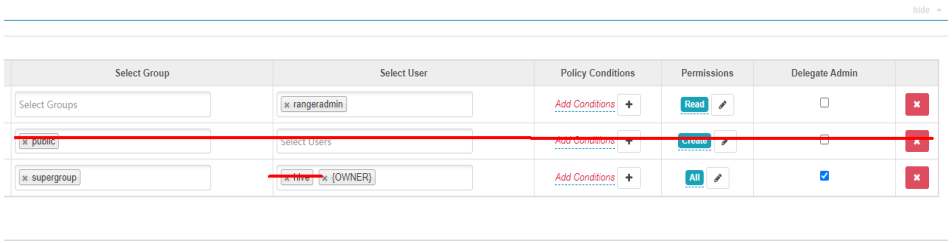
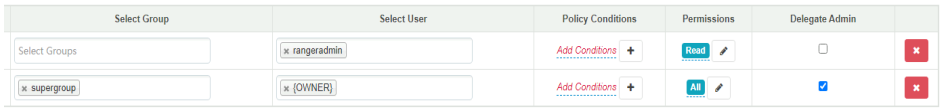


图 3-31 修改后的策略如图



配置完成后，仅supergroup下{OWNER}用户具有在default库建表权限。

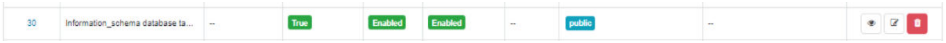
- （可选）修改可见表信息权限

  ranger默认hive策略中，库表信息对所有用户可见，修改该默认权限。

  a. 在ranger中，单击hive模块，修改hive默认策略。

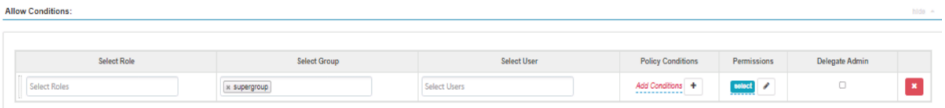
  b. 单击名称为：Information_schema database tables columns后的修改按钮，修改hive默认库表信息的权限策略。

  图 3-32 修改 hive 默认库表信息的权限策略

  c. 在Allow Conditions允许条件中，将public用户组改为supergroup。

  图 3-33 修改后的策略如图

3.1.2 数据提供方资源分配

3.1.2.1 场景说明

当全新的数据提供方接入时，由平台运营方为数据提供方提供前置机和数据库，用于数据提供方同步数据到前置机；

并为数据提供方分配独立的MRS开发/生产库用于数据集成的相关操作。

每新增一个数据提供方，进行一次该章节操作。

3.1.2.2 RDS 前置机发放

平台运营方-管理员在公共服务资源集1和公共服务资源集2下，为新接入的数据提供方发放RDS服务。

步骤1 平台运营方管理员登录智能云管理平台平台，选择公共服务资源集1。

图 3-34 选择公共服务资源集 1

步骤2 选择云数据库RDS，单击“创建数据库实例”，申请云数据库RDS服务。

图 3-35 选择服务

步骤3 选择数据库规格，并设置数据库用户名和密码。将数据库地址、用户名和密码等信息发给数据提供方。

----结束

3.1.2.3 MRS 分配和授权

完成数据底座初始化授权工作（详见**3.1.1.7 数据底座初始化授权**章节），即MRS集群已具有OBS访问权限后，为数据提供方创建指定OBS路径的MRS数据库。

准备工作

平台运营方-运维人员使用预置FusionInsight管理员（初始admin账号）创建安全认证管理员账号，并通过委托配置，分配给该账号OBS管理员权限。

步骤1 进入MRS集群实例页面，单击”前往Manager”；

步骤2 使用管理员账号（初始admin账号）登录FI页面，选择导航栏中“系统”；

步骤3 在左侧导航栏中选择“用户”一栏，单击“添加用户”，创建tianji_admin用户；

步骤4 为该账号分配用户组“supergroup”以及MRS FusionInsight管理员权限，配置详见下图。

图 3-36 配置

----结束

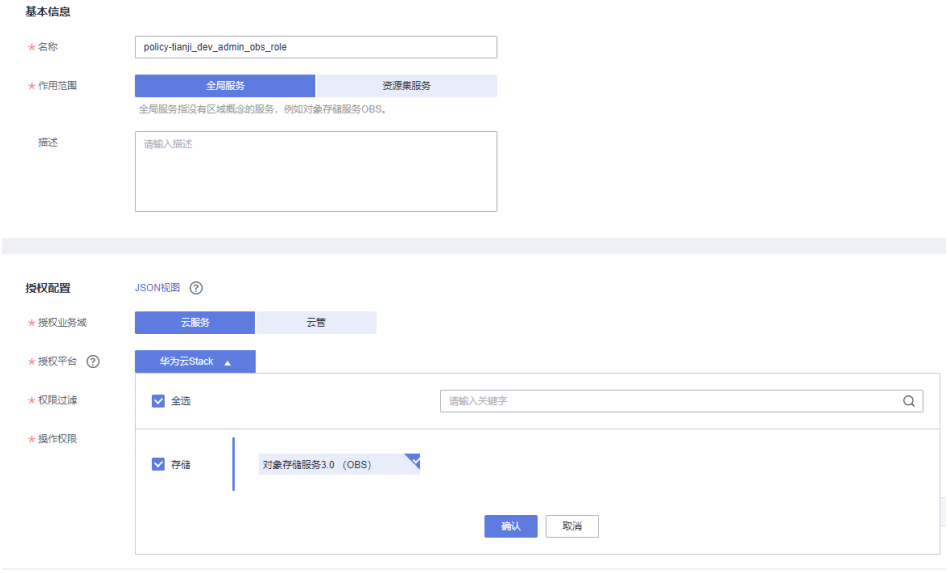
OBS 权限策略及委托配置

存算分离场景中，MRS用户建库、表在OBS指定路径时，需要有OBS对应目录权限。

为MRS管理员账号配置OBS管理员权限策略，并且绑定委托映射至管理员账号，使MRS管理员账号拥有为每个接入的开发利用方在指定OBS目录建库的权限。

- 创建具有OBS管理员权限的IAM策略。
  a. 使用浏览器，以VDC管理员账号登录智能云管理平台。
  b. 单击主菜单的“系统”。单击“安全管理 > 角色管理 > 创建角色”。
  c. 创建OBS管理员角色。作用范围选择“全局服务”，授权平台选择“对象存储服务OBS3.0”，操作权限全选。

图 3-37 创建 OBS 管理员角色



d. 单击“确认”保存策略。

- 将角色绑定至委托。

a. 创建委托，委托类型选择"普通账号"，输入被委托方租户名称。（被委托方租户名称为智能云管理平台的资源租户名称，租户名称查看参见说明）。

图 3-38 创建委托

说明

VDC管理员登录智能云管理平台，单击右上角登录用户名>个人设置，查看所属租户名称。

b. 拥有权限选择"自定义角色"，勾选创建的"自定义角色"。

图 3-39 自定义角色"

- 将OBS管理员权限的委托，映射至准备工作中创建的MRS "tianji_admin”用户。
  a. 单击现有集群下MRS集群名称 > 概览 >运维管理 >OBS权限控制 > 单击管理。

图 3-40 概览

  b. 单击“添加映射”，配置IAM委托和用户组直接映射关系。类型选择“User”，MRS用户（组）选择准备工作中创建的MRS用户账号tianji_admin。

图 3-41 添加映射

创建 OBS 桶目录

平台运营方-运维人员创建平台运营方OBS目录，负责管理和隔离各数据提供方（各委办局）数据接入库。

在OBS并行文件系统，创建OBS桶目录。

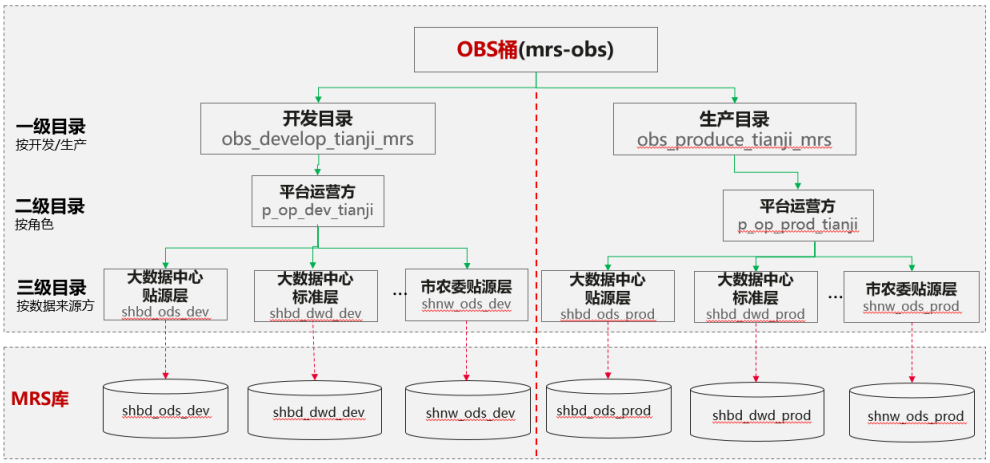
步骤1 使用账号登录智能云管理平台，选择“存储 > 对象存储服务 3.0”，进入对象存储服务界面。

步骤2 选择左侧导航栏的“并行文件系统”，进入并行文件系统控制台。

步骤3 单击界面右上角的“创建并行文件系统”，进入创建页面。

步骤4 根据平台运营方OBS目录架构（如下图所示），设置并行文件系统的区域和名称，配置策略为“私有”。

图 3-42 平台运营方 OBS 目录架构



步骤5 单击“新建文件夹”，为新增数据提供方，创建三级目录。

图 3-43 新建文件夹

说明

- 并行文件系统创建成功后，不能修改名称，请提前规划合适的名称。
- 由于通过URL访问并行文件系统时，名称会作为URL的一部分，根据DNS标准，URL不支持大写字母，无法区分带大写字母的并行文件系统。因此，名称仅支持小写字母、数字、“-”、“.”。例如：若想通过URL访问名为“MyFileSystem”的文件系统，该URL将解析成名为“myfilesystem”的文件系统，导致访问出错。

----结束

创建 Hive 数据库

平台运营方-运维人员使用Hive 组件对接 OBS 文件系统，并建库、建表时指定 Location 为 OBS 路径。

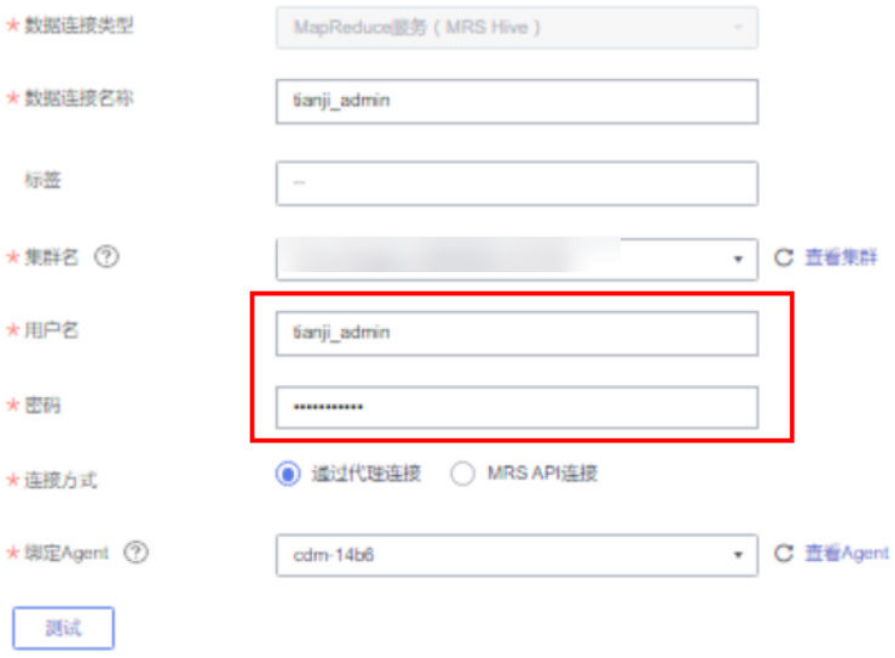
用户可在DataArts Studio-数据开发功能模块，进行建库，建表操作；也可通过Hive客户端进行建库、建表操作。

- 使用DataArts Srudio创建数据库

  通过DataArts Studio-数据开发模块，为数据提供方创建Hive数据库。

  a. **平台运营方-运维人员**进入DataArts Studio-公共工作空间，单击“管理中心>创建数据连接”，使用tianji_admin用户名和密码创建数据连接。

  图 3-44 创建 Hive 数据库 1

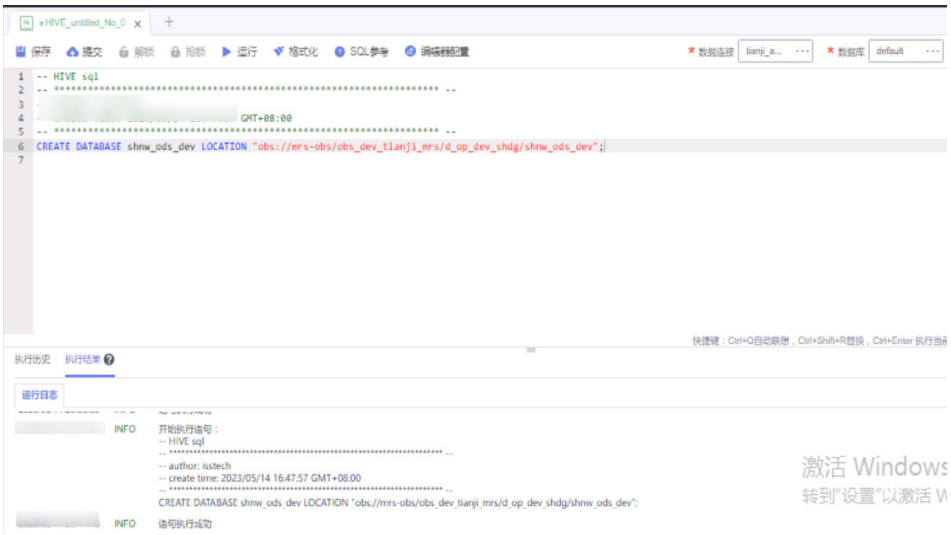
  b. 进入“数据开发”功能模块，单击”新建脚本>新建HiveSQL脚本”。

  在OBS并行文件系统：“OBS桶/运营平台开发/平台运营方/大数据中心贴源层“目录下，创建开发贴源库，用于数据提供方A数据接入。

  建库语句示例：

  ```
  CREATE DATABASE dev_shnw_dwd LOCATION "obs://mrs-obs/obs_dev_tianji_mrs/
  p_op_dev_shdg/shnw_ods_dev"
  ```

图 3-45 创建 Hive 数据库 2



重复步骤2中建库语句的执行，为数据提供方A创建生产贴源库。

- （可选）使用MRS-Hive客户端创建数据库

  a. 使用安装客户端用户登录客户端安装节点，客户端下载和安装指导请参考 **https://support.huaweicloud.com/usermanual-mrs/mrs_01_0089.html**

  b. 执行如下命令初始化环境变量。source /客户端安装目录/bigdata_env

  c. 安全集群，执行以下命令进行用户认证（该用户需要具有Hive操作的权限）kinit Hive组件操作用户。

  如kinit tianji_admin，输入安全账户用户密码。

  d. beeline进入hive客户端，进行建库、建表操作。

  在OBS并行文件系统：“OBS桶/运营平台开发/平台运营方/大数据中心贴源层“目录下，创建开发贴源库，用于数据提供方A数据接入。

  建库语句示例：

  ```
  create  database dev_shnw_dwd LOCATION "obs://mrs-obs/obs_dev_tianji_mrs/
  p_op_dev_shdg/shnw_ods_dev"
  ```

  重复步骤4中建库语句的执行，为数据提供方A创建生产贴源库。

3.1.3 开发利用方资源分配

场景说明

针对新增开发利用方场景，需要为其创建新的三级VDC，并完成云服务授权、数据底座授权操作。此场景在每次新增开发利用方时需要完成一次，操作主体为**平台运营方-管理员**和**授权运营方-管理员**。

三级 VDC 发放

授权运营方-管理员登录智能云管理平台平台，创建三级VDC-开发利用方，并设置VDC管理员。

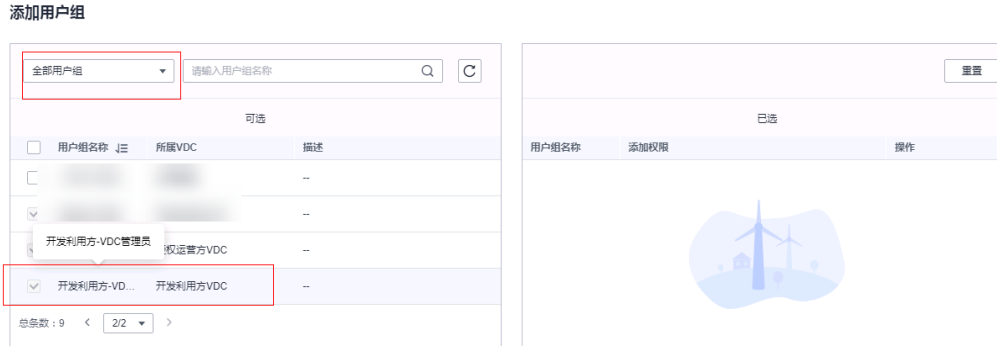
公共资源集授权

公共服务资源集属于平台运营方（一级VDC）下资源，因此公共资源集授权动作只能由一级VDC管理员完成。

步骤1 **平台运营方-管理员**登录智能云管理平台平台，在“系统-资源集”列表中，单击选择“公共服务资源集1”；

步骤2 单击“已授权用户组”，选择“添加用户组”。下拉框选择”全部用户组”，在该资源集下选择“开发利用方-VDC管理员”用户组；

图 3-46 添加用户组



步骤3 **平台运营方-管理员**登录智能云管理平台平台，在“系统-资源集”列表中，单击选择“公共服务资源集2”；

步骤4 单击“已授权用户组”，选择“添加用户组”。下拉框选择”全部用户组”，在该资源集下选择“开发利用方-VDC管理员”用户组；

步骤5 使用三级VDC开发利用方-管理员账号登录智能云管理平台平台，该用户组下用户可以访问公共服务资源集1、公共服务资源集2中的所有云服务。

----结束

用户组创建及授权

三级VDC用户组的创建和授权由**授权运营方-管理员**统一管控。

步骤1 **授权运营方-管理员**登录智能云管理平台平台，在“系统>VDC列表”中单击对应“三级VDC”名称，进入该VDC管理页面；

步骤2 单击“用户组-创建“，创建自定义用户组：开发利用方-云服务开发、开发利用方-云服务测试、开发利用方-云服务运维；

图 3-47 创建用户组

步骤3 **平台运营方-管理员**登录智能云管理平台平台，在“系统>VDC列表”中单击对应“三级VDC”名称，进入该VDC管理页面；

步骤4 单击列表“用户组”，在对应用户组后，单击“添加授权”（以云服务开发用户组为例）；

图 3-48 用户组

步骤5 授权类型选择“资源集”，勾选“公共服务资源集1”，单击“下一步”；

图 3-49 添加授权

步骤6 在权限列表中勾选公共服务资源集1中，云服务开发用户组需要使用的系统角色；

图 3-50 选择授权角色

步骤7 如步骤4-6，添加“公共服务资源集2”中，云服务开发用户组需要使用的系统角色。

图 3-51 系统角色

角色以服务为粒度，控制云服务访问权限。开发利用方VDC下用户组系统权限配置详见**表1 开发利用方VDC用户组角色**

表 3-7 开发利用方 VDC 用户组角色

用户组	VDC角色
开发利用方-管理员	三级VDC管理员
开发利用方-开发人员	公共服务资源集1： DataArts Studio User； MRS ReadOnlyAccess； DWS ReadOnlyAccess； 公共服务资源集2： ROMA Administrator； VPC Administrator； Server Administrator；

用户组	VDC角色
开发利用方-测试人员	公共服务资源集1： DataArts Studio User； MRS ReadOnlyAccess; DWS ReadOnlyAccess; 公共服务资源集2： ROMA Administrator; VPC Administrator; Server Administrator;
开发利用方-运维人员	公共服务资源集1： DataArts Studio User； MRS ReadOnlyAccess; DWS ReadOnlyAccess;

说明

授权角色以云服务为粒度，由于多数高阶云服务都依赖计算、存储、网络基础云服务，使用云服务时需要授予其**VPC Administrator**、**Server Administrator**的权限。

----结束

ak/sk策略配置：为所有开发利用方自定义用户组绑定ak/sk获取访问密钥权限。

步骤1 **授权运营方-管理员**登录智能云管理平台平台，单击主菜单的“系统”。单击“权限管理 > 角色管理 > 创建角色”。

步骤2 创建策略policy_download_aksk，授权类别选择“云管”，授权对象选择“个人中心”，权限过滤选择“查看个人信息”、“修改个人信息”。

图 3-52 创建策略

步骤3 绑定该角色至开发利用方自定义用户组。单击列表“用户组”，在对应用户组后，单击“添加授权”，授权类型选择“VDC”。

搜索并选择步骤2中创建的自定义角色。

图 3-53 自定义角色

步骤4 开发利用方用户即可在“智能云管理平台账户-个人设置-管理访问密钥”中单击“新增访问密钥”下载ak/sk文件。

图 3-54 新增访问密钥

----结束

3.1.3.1 数据工具授权

DataArts Studio 工具授权

被赋予DataArts Studio User策略的用户仅具有访问DataArts Studio云服务的权限，在使用该服务时具有什么权限，依赖于该用户在工作空间中被赋予的角色。

- 创建工作空间

  授权运营方-管理员登录DataArts Studio云服务控制台，在实例中创建“开发利用方-生产”和“开发利用方-开发”工作空间，用于开发利用方进行场景化开发和生产工作。

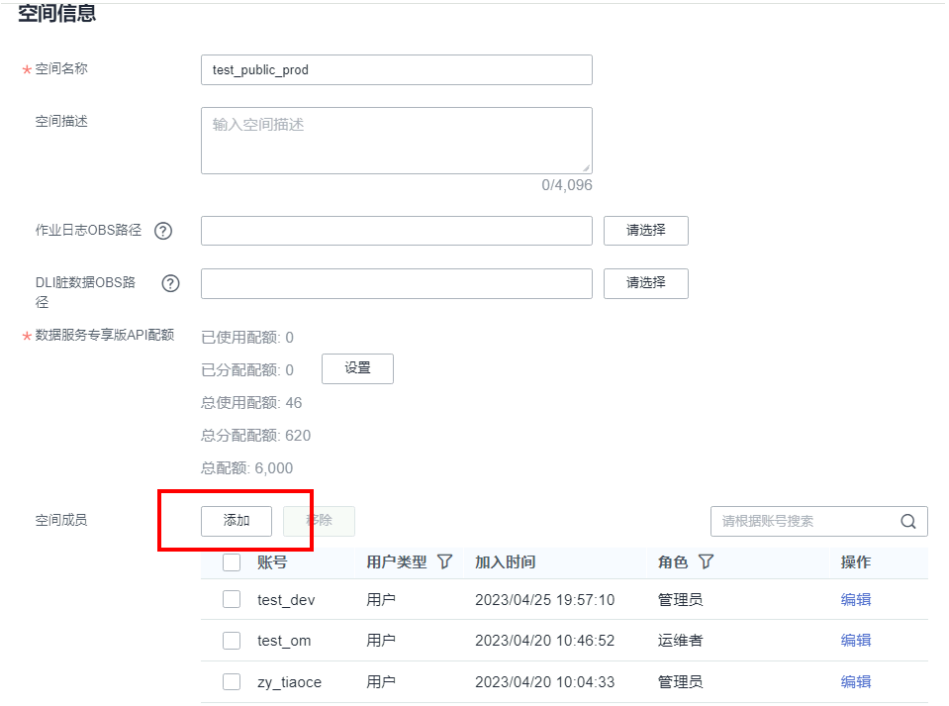
- 工作空间授权

  通过用户组对DataArts Studio工作空间进行授权。只有被添加到该工作空间的用户组下用户，可以看到该工作空间。

  授权运营方-管理员登录DataArts Studio实例，依据DataArts Studio空间角色，授予权限给对应用户组。

  a. 登录DataArts Studio 控制台。选择"空间管理"，单击工作空间后对应"编辑"按钮，选择"空间成员>添加成员"。

图 3-55 空间信息



b. 选择"按用户组添加"，选择对应角色。工作空间角色授权详见表3-8。

图 3-56 添加成员

表 3-8 工作空间角色授权

用户组	DataArts Studio 工作空间角色
开发利用方-管理员	开发/生产空间-管理员
开发利用方-开发用户组	开发空间-开发者

用户组	DataArts Studio 工作空间角色
开发利用方-测试用户组	开发空间-Tester（自定义角色）
开发利用方-运维用户组	生产空间-运维者

ROMA Connect 开发工具授权

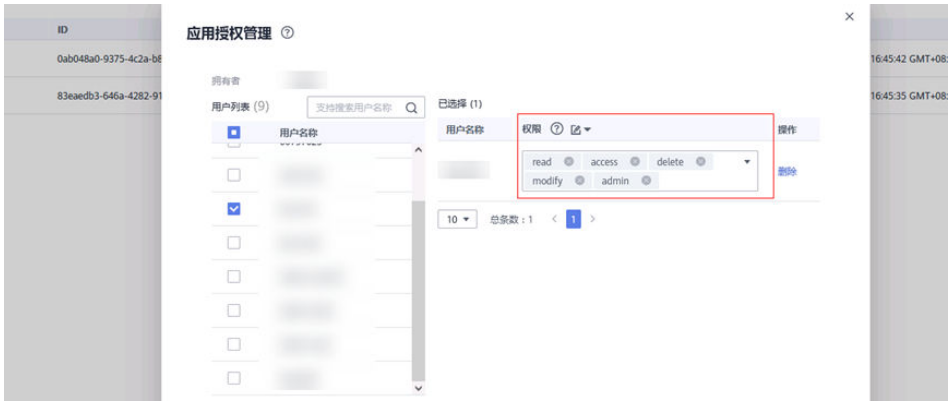
- ROMA Connect集成应用创建

  使用**授权运营方-管理员**账号登录智能云管理平台平台，在ROMA Connect开发实例中创建集成应用a,在ROMA Connect生产实例中创建集成应用a1。

- ROMA Connect集成应用授权

  a. 使用授权运营方-管理员账号登录智能云管理平台平台。在ROMA Connect开发实例中，单击“集成应用a>应用授权管理”，授予开发利用方-管理员admin权限（勾选admin默认添加全部权限）；

  图 3-57 应用授权管理

  b. 在ROMA Connect生产实例中，单击“集成应用a1>应用授权管理”，授予授权运营方-运维人员admin权限（勾选admin默认添加全部权限）；

  c. 使用开发利用方-管理员账号登录智能云管理平台平台。在ROMA Connect开发实例中，单击“集成应用a>应用授权管理”，授予开发利用方-开发人员modify/delete权限；测试人员modify权限。

  表 3-9 ROMA Connect 集成应用授权

/	操作者	工作职责	ROMA Connect角色
ROMA Connect开发实例	开发利用方-管理员	在ROMA Connect云服务界面，将开发/测试用户添加到所属开发ROMA Connect实例应用中；	开发实例应用管理员（admin）
	开发利用方-开发人员	导出ROMA Connect开发实例中待上线应用为本地文件，发给授权运营方-运维人员；	开发实例应用-开发人员（modify/delete)

/	操作者	工作职责	ROMA Connect角色
	开发利用方-测试人员	负责基于开发人员发布的作业、模型、API等，进行测试验证；	开发实例应用-测试人员（modify）
ROMA Connect生产实例	授权运营方-运维人员	将ROMA Connect开发实例的应用包导入API并发布	生产实例应用管理员(admin)

3.1.3.2 数据底座授权

数据底座授权分为OBS授权、MRS授权和DWS授权三部分。

- MRS采用存算分离设计方案，在对MRS进行授权之前，还需对OBS 面向对象存储服务进行目录划分和授权操作。
- 对于MRS组件用户的授权，通过创建MRS用户及用户组以及ranger策略实现权限划分。并且通过对MRS用户组的权限配置，使得属于该用户组的用户，对非自己创建的数据库有操作/只读权限。
- 对于DWS的授权，通过对schema授权的SQL语句，实现不同开发利用方DWS用户对公共数据的访问。

3.1.3.2.1 OBS 分配和授权

创建 OBS 桶目录

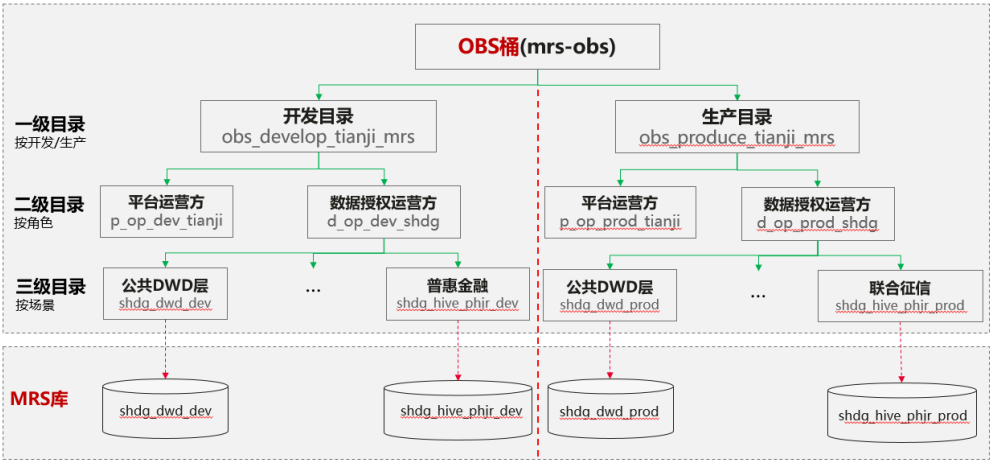
步骤1 使用账号登录智能云管理平台，选择“存储 > 对象存储服务 3.0”，进入对象存储服务界面。

步骤2 选择左侧导航栏的“并行文件系统”，进入并行文件系统控制台。

步骤3 单击界面右上角的“创建并行文件系统”，进入创建页面。

步骤4 根据OBS目录架构（如下图所示），设置并行文件系统的区域和名称，配置策略为“私有”。

图 3-58 OBS 目录架构



说明

- 并行文件系统创建成功后，不能修改名称，请提前规划合适的名称。
- 由于通过URL访问并行文件系统时，名称会作为URL的一部分，根据DNS标准，URL不支持大写字母，无法区分带大写字母的并行文件系统。因此，名称仅支持小写字母、数字、“-”、“.”。例如：若想通过URL访问名为“MyFileSystem”的文件系统，该URL将解析成名为“myfilesystem”的文件系统，导致访问出错。

----结束

创建 OBS 细粒度权限角色和委托

在为集群配置全局委托后可继续配置单独的OBS权限映射关系，对个别用户或用户组配置细粒度的OBS访问权限策略。

- 配置IAM权限策略

  通过配置IAM POLICY，可以更细粒度的控制用户对不同OBS桶目录的访问权限。

  a. 创建IAM策略。使用浏览器，以VDC管理员账号登录智能云管理平台。

  b. 单击主菜单的“系统”。单击“权限管理 > 角色管理 > 创建角色”。

  c. 参考表3-10填写参数。

表 3-10 OBS IAM 权限策略参数

参数类别	参数名称	说明
基本信息	名称	角色名称，如dev_shdg_phjr_obs_role(开发利用方A接入）
	作用范围	全局服务
	描述	对于所创建角色的描述。
授权配置方	JSON视图	以JSON形式展开

参数类别	参数名称	说明
JSON视图	JSON视图	如需添加针对特定资源的细粒度权限（例如指定的OBS目录），需使用JSON视图进行配置。 JSON样例如下，在“Resource”配置中手动指定特定资源。 ● Effect（作用） ● Action（授权项） ● Resource（资源） OBS只有两种资源类型：bucket和object，设置特定目录资源时，“object”需同时配置当前目录以及通配符。 例如设置“/tmp”目录的权限，需要同时配置“obs_bucket_name/tmp/”、“obs_bucket_name/tmp/*”的权限。其他目录权限请参考以下样例进行配置，对应目录及该目录下所有对象的资源路径。 **指定目录所有策略示例：** *GetObject：获取对象内容、获取对象元数据* *ListMultipartUploadParts：列举已上传的段* *ListBucket：列举桶内对象* *PutObject：PUT上传、POST上传、复制对象、追加写对象、初始化上传段任务、上传段、合并段* *DeleteObject：删除对象、批量删除对象* { "Version": "1.1", "Statement": [{ "Effect": "Allow", "Action": ["obs:object:PutObject", "obs:object:DeleteObject", "obs:object:GetObject", "obs:object:ListMultipartUploadParts", "obs:bucket:ListBucket"], "Resource": ["obs:*:*:object:mrs-obs/obs_dev_tianji_mrs/d_op_dev_shdg/shdg_phjr_hive_dev", "obs:*:*:object:mrs-obs/obs_dev_tianji_mrs/d_op_dev_shdg/shdg_phjr_hive_dev/*", "obs:*:*:object:mrs-obs/user/omm/.Trash",

参数类别	参数名称	说明

		"obs:*:*:object:mrs-obs/user/omm/.Trash/*",
		"obs:*:*:object:mrs-obs/user/hive/.Trash",
		"obs:*:*:object:mrs-obs/user/hive/.Trash/*",
		"obs:*:*:object:mrs-obs/user/datagroup_dev_admin/.Trash",
		"obs:*:*:object:mrs-obs/user/datagroup_dev_admin/.Trash/*",
		"obs:*:*:bucket:mrs-obs"
		]
		}
		]
		}
		指定目录只读策略示例：
		{
		"Version": "1.1",
		"Statement": [
		{
		"Effect": "Allow",
		"Action": [
		"obs:object:GetObject",
		"obs:bucket:ListBucket"
		],
		"Resource": [
		"obs:*:*:object:mrs-obs/obs_dev_tianji_mrs/d_op_dev_shdg/shdg_dwd_dev",
		"obs:*:*:object:mrs-obs/obs_dev_tianji_mrs/d_op_dev_shdg/shdg_dwd_dev/*",
		"obs:*:*:object:mrs-obs/user/omm/.Trash",
		"obs:*:*:object:mrs-obs/user/omm/.Trash/*",
		"obs:*:*:object:mrs-obs/user/hive/.Trash",
		"obs:*:*:object:mrs-obs/user/hive/.Trash/*",
		"obs:*:*:object:mrs-obs/user/datagroup_dev_admin/.Trash",
		"obs:*:*:object:mrs-obs/user/datagroup_dev_admin/.Trash/*",
		"obs:*:*:bucket:mrs-obs"
		]
		}
		]

参数类别	参数名称	说明
		}

说明

Hive用户在配置OBS委托策略时，不仅需要配置对应OBS目录的访问权限，还需要配置用户回收站目录的操作权限。详见配置组件回收清理策略章节。

用户回收站目录：

"obs:*:*:object:mrstest/user/omm/.Trash",

"obs:*:*:object:mrstest/user/omm/.Trash/*",

"obs:*:*:object:mrstest/user/hive/.Trash",

"obs:*:*:object:mrstest/user/hive/.Trash/*",

"obs:*:*:object:mrstest/user/<新增的业务用户>/.Trash",

"obs:*:*:object:mrstest/user/<新增的业务用户>/.Trash/*"

d. 单击“确认”保存策略。

- 将角色绑定至IAM委托。

a. 创建委托，委托类型选择"普通账号"，输入被委托方租户名称；

图 3-59 创建委托

b. 拥有权限选择"自定义角色"，勾选创建的"自定义角色"。委托与角色映射关系详见表3-11。

图 3-60 自定义角色

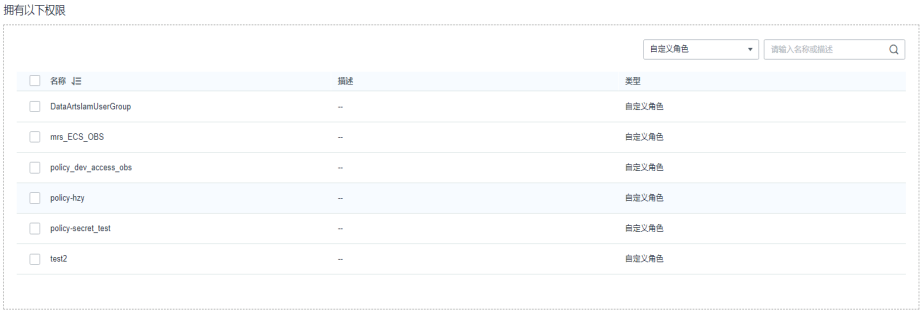


表 3-11 IAM POLICY 和委托映射关系

场景	IAM自定义角色	自定义角色用途	绑定委托	映射用户组
运营平台运营方-开发测试组	develop_access_obs_role	运营平台开发接入库-所有	develop_access_obs_agency	dev_access_group
	produce_access_obs_role	运营平台生产接入库-所有	produce_access_obs_agency	prod_access_group
普惠金融场景-开发测试组（举例）	develop_datagroup_obs_role	普惠金融开发融合库-所有	develop_datagroup_obs_agency	datagroup_dev_group
	tianji_access_dev_readonly	运营平台开发接入库-只读		
	produce_datagroup_obs_role	普惠金融生产融合库-所有	produce_access_obs_agency	datagroup_prod_group
	tianji_access_prod_readonly	运营平台生产接入库-只读		

配置组件回收清理策略

⚠ 注意

由于OBS回收站目录是以用户维度进行创建，当MRS集群内新创建了用户且该用户具备组件数据的删除权限时，也需要参考本章节配置新用户的回收站目录清理策略。

- 配置用户回收站目录

  除了MRS集群预置用户所涉及的回收站目录外（例如“user/omm/.Trash”，参考表3-12），对于其他新增的有防误删需求的用户，同样需要为其配置回收站目录：user/<用户名>/.Trash。

a. 配置当前用户所对应的OBS委托策略，至少包含了以下目录的操作权限，若未配置可参考**创建OBS细粒度权限角色和委托**进行操作；

   – user/omm/.Trash

   – user/hive/.Trash

   – user/<新增的业务用户>/.Trash

b. 以VDC管理员或VDC业务员账号登录智能云管理平台运营面-服务列表-存储-对象存储服务 3.0，选择“并行文件系统>文件系统>user”；

c. 对应的“.Trash”文件夹若不存在需使用omm用户通过集群客户端手动创建。

   例如执行以下命令：hdfs dfs -mkdir obs://OBS并行文件系统名称/文件夹路径

- 配置 OBS 目录生命周期规则

a. 手动创建MRS集群新增用户所涉及的回收站目录（如“user/datagroup_dev_admin/.Trash”，具体操作参考配置用户回收站目录中步骤）；

b. 单击当前MRS集群使用的文件系统名称-生命周期规则-创建-填写参数-确定：

表 3-12 配置用户回收站目录

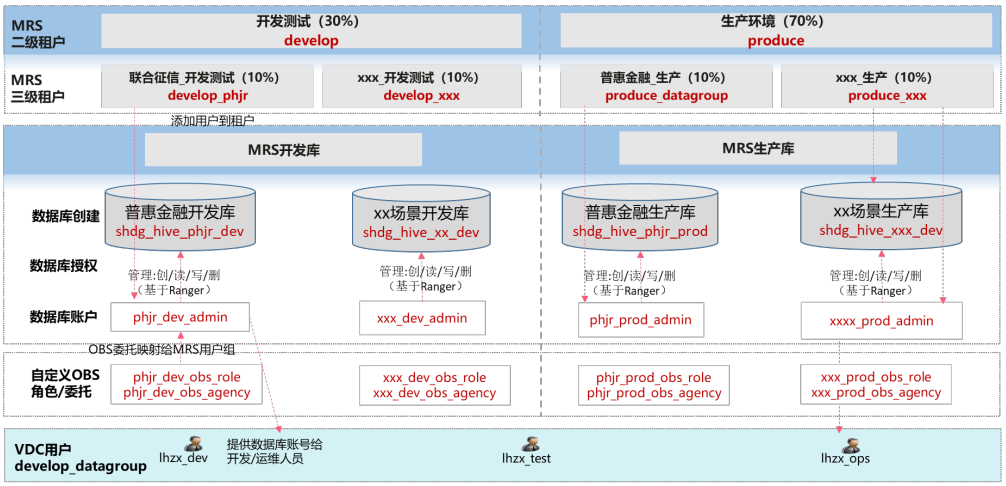
参数名称	描述	示例
状态	是否启用本条生命周期规则。	启用
规则名称	规则名称，可自定义，用于识别不同的生命周期配置。	rule-mrs-trash
策略	策略配置范围。 • 按前缀配置：满足指定前缀的对象将受生命周期规则管理，输入的对象前缀不能包括\:*?"<>|特殊字符，不能以/开头，不能两个/相邻。 • 配置到整个文件系统：文件系统内所有对象都将受生命周期规则管理。 说明 为防止其他业务数据被误删除，不建议使用配置到整个文件系统或者层级较高的目录的生命周期规则。	按前缀配置
前缀	生命周期规则适用的对象前缀，MRS集群组件数据回收站目录通常为如下路径，该文件夹若不存在，需提前手动创建。 user/<用户名>/.Trash	user/omm/.Trash

参数名称	描述	示例
过期删除/天数	策略配置范围内的对象最后一次更新后时间达到指定的天数后，对象将过期并自动被OBS删除。	30天

3.1.3.2.2 MRS 分配和授权

本章节指导平台运营方-运维人员为对应开发利用方创建指定目录下的Hive生产融合数据库，并且在MRS ranger中为其配置指定生产融合库以及公共接入数据库的访问策略。

图 3-61 MRS 分配和授权



以上图为例，开发利用方的MRS分配和授权比较复杂，涉及MRS租户创建、MRS用户和用户组创建、Hive数据库创建、Ranger授权、OBS委托映射等步骤。

创建 MRS 租户

使用MRS管理员账号（默认admin账号）登录MRS FusionInsight页面。

步骤1 添加租户，创建两个二级租户：develop和produce，租户类型选择“非叶子租户”。

图 3-62 创建 MRS 租户

说明

如果已经创建produce和develop二级租户，则跳过该步骤。

步骤2 在已创建的二级租户下，选择添加子租户，创建三级租户。如devlop_phjr，租户类型选择“叶子租户”，注意父租户需要区分开发和生产二级租户。

图 3-63 添加子租户

说明

在添加一个租户时，指定租户是否是一个叶子租户：

- 非叶子租户：支持子租户的创建。
- 叶子租户：最后一级租户，不能进行子租户的创建。叶子租户可与服务相关联。

----结束

创建 MRS 用户/用户组

MRS的用户体系不同于智能云管理平台 IAM用户体系，因此在进行数据底座授权时，需要登录MRS FusionInsight创建MRS账号，提供给对应开发利用方。

步骤1 **平台运营方-运维人员**使用MRS FI安全认证管理员账号（已在**准备工作**中创建）登录FI页面，选择导航栏中“系统”。

步骤2 在左侧导航栏中选择“用户”一栏，单击“添加用户”。

步骤3 在左侧导航栏中选择“用户组”一栏，单击“添加用户组”。

步骤4 创建MRS用户，选择并加入对应用户组。依照下表1与表2完成用户和用户组创建。

说明

hive用户组为普通用户组。Hive用户必须属于该用户组。

图 3-64 选择并加入对应用户组

步骤5 将用户添加到对应租户下。在“角色”中，添加对应租户角色。

如将datagroup_dev_admin用户，添加至“develop_phjr”租户资源下：

图 3-65 选择并绑定角色

表 3-13 MRS 用户组设置

MRS用户	职责	MRS DATABASE	所属租户
datagroup_dev_access	负责运营平台(公共数据接入)开发，创建对应数据库	shdg_ods_dev shdg_dwd_dev	develop_datagroup
datagroup_prod_access	负责运营平台(公共数据接入)生产，创建对应数据库	shdg_ods_prod shdg_dwd_prod	produce_datagroup
datagroup_dev_admin	负责phjr场景开发，创建开发环境对应数据库	shdg_hive_phjr_dev	develop_phjr
datagroup_prod_admin	负责phjr场景开发，创建生产环境对应数据库	shdg_hive_phjr_prod	produce_phjr

表 3-14 MRS 用户创建

MRS用户	MRS用户组	权限
datagroup_dev_access	dev_access_group	运营平台开发接入库-操作权限
datagroup_prod_access	access_prod_group	运营平台生产接入库-操作权限
datagroup_dev_admin	datagroup_dev_group	phjr开发融合库-操作权限
	tianji_access_dev_readonly	运营平台开发接入库-只读权限
datagroup_prod_admin	datagroup_prod_group	phjr生产融合库-操作权限
	tianji_access_prod_readonly	运营平台生产接入库-只读权限

----结束

创建 Hive 数据库

平台运营方-运维人员为开发利用方分配MRS-Hive库，并在建库时指定 Location 为OBS对应目录路径。

- 使用DataArts Srudio创建数据库

  通过DataArts Studio-数据开发功能，为开发利用方创建数据库。

  a. 进入“DataArts Studio”，单击“管理中心”，创建数据连接。用户名和密码填写tianji_admin账号（MRS FI安全认证管理员账号）和对应密码。

  b. 进入“数据开发”页面，单击新建脚本“新建HiveSQL脚本”。

在OBS并行文件系统：“OBS桶/运营平台开发/数据授权运营方/普惠金融”目录下，创建开发贴源库，用于开发利用方数据开发工作。

建库语句示例：

```
CREATE DATABASE shdg_phjr_hive_dev LOCATION "obs://mrs-obs/obs_dev_tj_mrs/
d_op_dev_shdg/dev_shdg_phjr_hive";
```

图 3-66 新建 HiveSQL 脚本

重复步骤2语句执行，为开发利用方A创建生产库。

- 可选使用MRS-Hive客户端创建数据库

  通过MRS-Hive客户端，为开发利用方创建数据库。

  a. 使用安装客户端用户登录客户端安装节点，客户端下载和安装指导请参考 **https://support.huaweicloud.com/usermanual-mrs/mrs_01_0089.html**

  b. 执行如下命令初始化环境变量，source 客户端安装目录/bigdata_env。

  c. 安全集群，执行以下命令进行用户认证（该用户需要具有Hive操作的权限）kinit Hive组件操作用户。

  如kinit tianji_admin，输入安全账户用户密码。

  d. beeline进入hive客户端，进行建库、建表操作。

  在OBS并行文件系统：“OBS桶/运营平台开发/数据授权运营方/普惠金融”目录下，创建开发贴源库，用于开发利用方数据开发工作。

  建库语句示例：

  ```
  CREATE DATABASE shdg_phjr_hive_dev LOCATION "obs://mrs-obs/obs_dev_tj_mrs/
  d_op_dev_shdg/dev_shdg_phjr_hive";
  ```

创建 Ranger 授权策略

本章节介绍平台运营管理员为MRS用户（组）创建hive ranger策略，ranger策略通过对Hive数据库、表添加针对不同MRS用户（组）对应权限，实现数据库权限访问控制。

Hive数据库权限划分详见**表3-15**。

【示例】分配给开发利用方的MRS账号(datagroup_dev_admin)拥有对应生产融合库的所有权以及对公共数据库的只读权限。

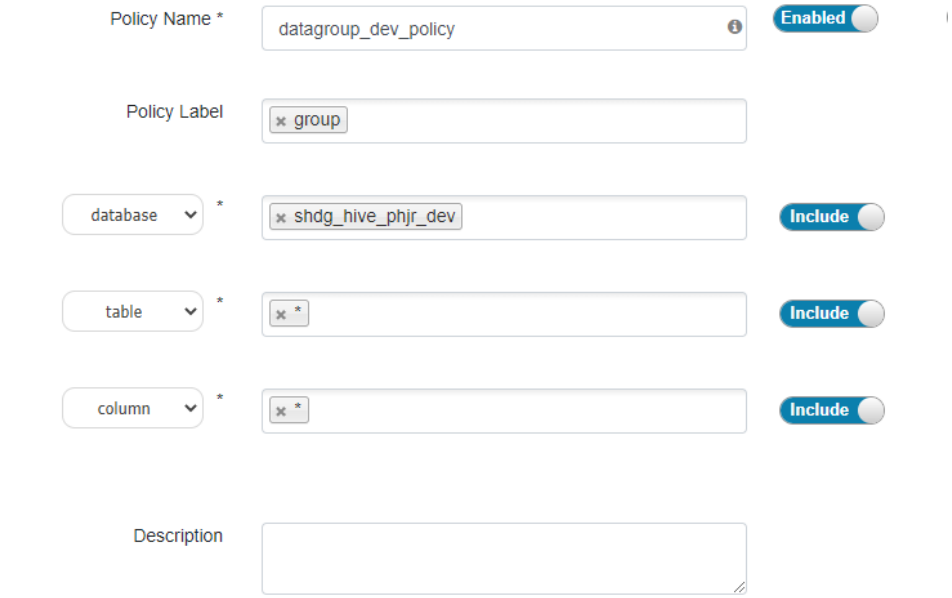
步骤1 以平台运营管理员角色登录智能云管理平台运营平台，跳转到MRS云服务界面，单击MRS集群名称进入概览页，单击集群管理。

步骤2 以管理员账号登录FusionInsight Manager，进入到ranger admin页面，单击右上角"add new policy"新建ranger访问策略。

步骤3 策略对象选择“database”，根据用户组职责需要，选择对应数据库、数据表；

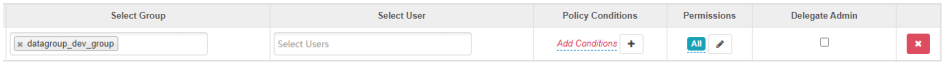
- 配置phjr场景开发融合库策略dev_datagroup_policy：

图 3-67 创建 Ranger 授权策略 1



授予datagroup_dev_group用户组shdg_phjr_hive_dev库*表*列的所有权：ALL

图 3-68 创建 Ranger 授权策略 2

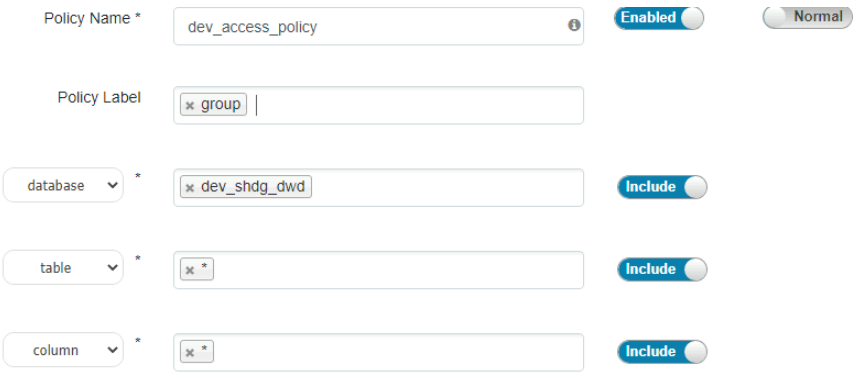


- 配置公共数据开发接入库策略dev_access_policy：

  授予access_dev_group用户组shdg_ods_dev、shdg_dwd_dev库*表*列的所有权，

  授予tianji_access_dev_readonly用户组shbd_ods_dev、shbd_dwd_dev库*表*列的select/read权限。

图 3-69 配置公共数据开发接入库策略



设置用户组对应权限，如ALL/READ/SELECT。

图 3-70 Ranger 权限策略说明

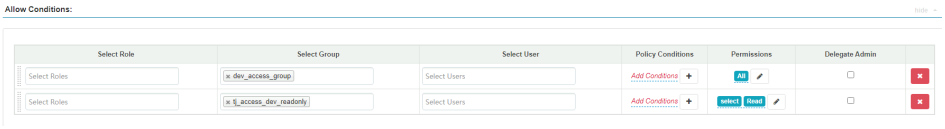


表 3-15 Ranger 权限策略说明

POLICY名称	用户组	Hive库	权限
dev_datagroup_policy	datagroup_dev_group用户组	shdg_hive_phjr_dev库 *表*列	所有权
prod_datagroup_policy	datagroup_prod_group	shdg_hive_phjr_pro库 *表*列	所有权
dev_access_policy	access_dev_group用户组	shbd_ods_dev、shbd_dwd_dev库 *表*列	所有权
	tj_access_dev_readonly用户组	shbd_ods_dev、shbd_dwd_dev库 *表*列	select/read权限
prod_access_policy	access_prod_group用户组	shbd_ods_prod、shbd_dwd_prod库 *表*列	所有权
	tj_access_prod_readonly用户组	shbd_ods_prod、shbd_dwd_prod库 *表*列	select/read权限

----结束

MRS 用户组映射 OBS 委托

将不同权限的委托，映射至MRS用户组。

步骤1 登录智能云管理平台运营平台，跳转到MRS云服务界面，单击MRS集群名称进入概览页，单击“OBS权限控制”右侧的“单击管理”。

步骤2 单击“添加映射”，参考表3-16配置IAM委托和用户组直接映射关系。类型选择“Group”。

图 3-71 OBS 权限控制

表 3-16 IAM 委托和用户组映射关系

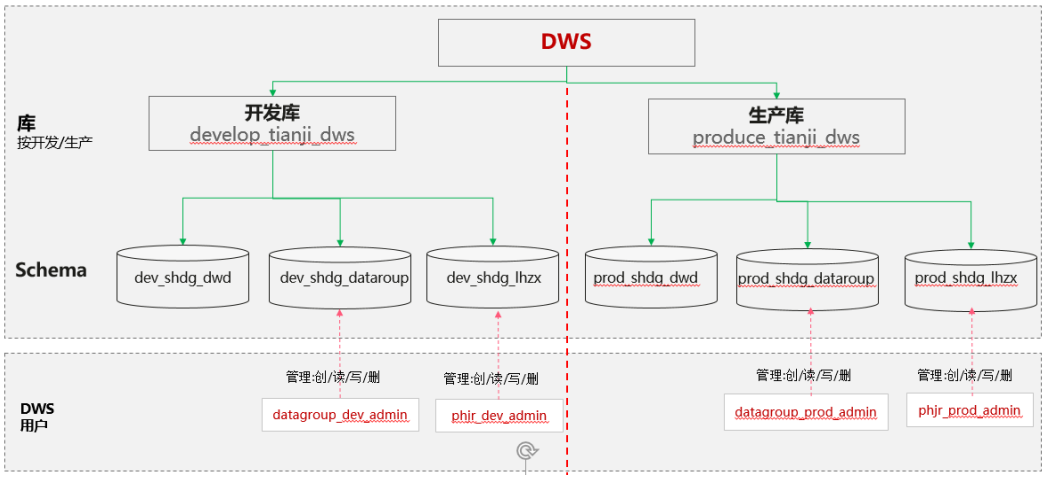
名称	绑定委托	映射用户组
运营平台	develop_access_obs_agency	dev_access_group
	produce_access_obs_agency	prod_access_group
phjr场景	develop_datagroup_obs_agency	datagroup_dev_group
	produce_access_obs_agency	datagroup_prod_group

步骤3 单击勾选“我同意授权MRS用户（组）与IAM委托之间的信任关系”，更新映射表，完成MRS用户（组）细粒度权限控制。

----结束

3.1.3.2.3 DWS 分配和授权

图 3-72 DWS 分配和授权



DWS库分为开发库和生产库，由数据库管理员统一创建；不同开发利用方通过schema进行隔离，每个开发利用方分配一个生产和一个开发schema。

创建 DWS 用户

平台运营方-运维人员使用SQL客户端工具或者JDBC等第三方驱动程序连接集群，访问集群中的数据库。

以使用DataStudio客户端工具连接DWS集群为例。

步骤1 使用SQL客户端工具DataStudio连接集群。客户端下载和安装指导请参考**https://support.huaweicloud.com/tg-dws/DWS_DS_006.html**

步骤2 使用DWS集群默认管理员账号dbadmin和密码，连接默认数据库gaussdb；

步骤3 创建DWS用户：

```
CREATE USER phjr_dev_admin PASSWORD 'password';
CREATE USER phjr_prod_admin PASSWORD 'password';
```

通过CREATE USER创建的用户，默认具有LOGIN权限；通过CREATE USER创建用户的同时系统会在执行该命令的数据库中，默认为该用户创建一个同名的schema，需要执行以下命令行收回该用户在同名schema的权限：

```
REVOKE ALL ON ALL TABLES IN SCHEMA phjr_dev_admin FROM phjr_dev_admin;
REVOKE ALL ON ALL TABLES IN SCHEMA phjr_prod_admin FROM phjr_prod_admin;
```

说明

phjr为普惠金融开发利用方缩写示例，其他开发利用方请注意替换成其他名字。

----结束

创建数据库和 Schema

步骤1 **平台运营方-运维人员**使用管理员账号dbadmin连接默认数据库gaussdb；

步骤2 创建运营平台开发和生产数据库dev_tianji_dws和prod_tianji_dws；

```
CREATE DATABASE dev_tianji_dws;
CREATE DATABASE prod_tianji_dws;
```

说明

该步骤为一次性操作，如果已经创建则跳过即可。

步骤3 创建schema。schema又称作模式，通过schema，允许多个用户使用同一数据库而不相互干扰。在dev_tianji_dws库下，执行如下命令来创建schema，并将权限授权给不同DWS用户；

```
CREATE SCHEMA dev_tianji_dws.dev_shdg_phjr AUTHORIZATION phjr_dev_admin;
CREATE SCHEMA prod_tianji_dws.prod_shdg_phjr AUTHORIZATION phjr_prod_admin;
```

步骤4 修改用户的默认查询路径，使用户登录到数据库时查找的默认schema为步骤3中创建的对应schema。

```
ALTER USER phjr_dev_admin SET SEARCH_PATH to dev_shdg_phjr;
ALTER USER phjr_prod_admin SET SEARCH_PATH to prod_shdg_phjr;
```

说明

phjr为普惠金融开发利用方缩写示例，其他开发利用方场景请注意替换成其他名字。

----结束

（可选）Schema 授权

【示例】以phjr场景下，开发人员账号访问公共数据schema为例。

步骤1 使用dbadmin账号连接dev_tianji_dws数据库；

步骤2 将Schema dev_shdg_dwd的权限赋给用户后，将公共数据Schema下，表public的select权限赋给phjr场景下的开发用户，DWS用户授权具体参照表3-17；

```
GRANT USAGE ON SCHEMA dev_shdg_dwd TO phjr_dev_admin;
GRANT SELECT ON TABLE dev_shdg_dwd.public TO phjr_dev_admin;
```

步骤3 使用phjr_dev_admin账号连接dev_tianji_dws数据库，可对公共数据Schema进行SELECT相关操作。

表 3-17 DWS 用户授权

场景	DWS用户	Database	Schema
数据库管理员	dbadmin	dev_tianji_dws（创建者） prod_tianji_dws（创建者）	dev_shdg_ods（创建者） dev_shdg_dwd（创建者）
开发	datagroup_dev_admin	dev_tianji_dws	dev_shdg_dataroup（ALL） dev_shdg_dwd（SELECT）
	phjr_dev_admin	dev_tianji_dws	dev_shdg_phjr（ALL） dev_shdg_dwd（SELECT）
生产	datagroup_prod_admin	prod_tianji_dws	prod_shdg_dataroup（ALL） prod_shdg_dwd（SELECT）
	phjr_prod_admin	prod_tianji_dws	prod_shdg_phjr（ALL） prod_shdg_dwd（SELECT）

说明

将Schema中的表或者视图对象授权给其他用户或角色时，需要将表或视图所属Schema的USAGE权限同时授予该用户或角色。否则用户或角色将只能看到这些对象的名字，并不能实际进行对象访问.

----结束

3.1.4 开发利用方数据开发

场景说明

该场景主要描述了开发利用方各类角色基于DataArtsStudio工具展开数据治理的关键操作，开发利用方按需日常操作。

说明

这里仅举例了部分数据工具的操作作为参考，其他详细的操作可以参考相关工具的用户指南材料。

授权运营方管理员-DataArts Studio 工具准备

DataArts Studio实例中默认不包含数据集成的CDM集群，如需使用数据集成功能，需要**授权运营方-管理员**根据业务场景，为开发利用方工作空间发放CDM增量包。

步骤1 **授权运营方-管理员**登录智能云管理平台平台，单击DataArts Studio云服务，单击已开通实例卡片上的“创建增量包”；

步骤2 进入创建DataArts Studio增量包页面，参照**表3-18**进行配置。为保证网络互通，虚拟私有云，子网，安全组需与MRS、DWS集群一致；

图 3-73 配置数据集成的增量包参数

表 3-18 配置数据集成的增量包参数

参数	说明
增量包类型	选择“批量数据迁移增量包”。
工作空间	选择需要使用数据集成增量包的工作空间。例如在DataArtsStudio实例test的A工作空间中创建数据集成的增量包，这里工作空间选择A。创建成功后，即可通过A工作空间查看到已经创建的数据集成集群。
集群名称	自定义数据集成集群名称。
实例类型	选择数据集成集群实例规格。

参数	说明
虚拟私有云	DataArts Studio实例中的数据集成CDM集群所属的VPC。VPC即虚拟私有云，是通过逻辑方式进行网络隔离，提供安全、隔离的网络环境。如果DataArts Studio实例或CDM集群需连接云上服务（如DWS、MRS、RDS等），则您需要确保CDM集群与该云服务网络互通。同区域情况下，同虚拟私有云、同子网、同安全组的不同实例默认网络互通，如果同虚拟私有云而子网或安全组不同，还需配置路由规则及安全组规则。VPC、子网、安全组的详细操作，请参见《虚拟私有云用户指南》。 **说明** 目前CDM实例创建完成后不支持切换虚拟私有云，请谨慎选择所属虚拟私有云
子网	DataArts Studio实例中的数据迁移CDM集群所属的子网。通过子网提供与其他网络隔离的、可以独享的网络资源，以提高网络安全。如果DataArts Studio实例或CDM集群需连接云上服务（如DWS、MRS、RDS等），则您需要确保CDM集群与该云服务网络互通。同区域情况下，同虚拟私有云、同子网、同安全组的不同实例默认网络互通，如果同虚拟私有云而子网或安全组不同，还需配置路由规则及安全组规则。VPC、子网、安全组的详细操作，请参见《虚拟私有云用户指南》。 **说明** 目前CDM实例创建完成后不支持切换子网，请谨慎选择所属子网。

参数	说明
安全组	DataArts Studio实例中的数据集成CDM集群所属的安全组。安全组是一组对弹性云服务器的访问规则的集合，为同一个VPC内具有相同安全保护需求并相互信任的弹性云服务器提供访问策略。如果DataArts Studio实例或CDM集群需连接云上服务（如DWS、MRS、RDS等），则您需要确保CDM集群与该云服务网络互通。同区域情况下，同虚拟私有云、同子网、同安全组的不同实例默认网络互通，如果同虚拟私有云而子网或安全组不同，还需配置路由规则及安全组规则。VPC、子网、安全组的详细操作，请参见《虚拟私有云用户指南》。 **说明** 目前CDM实例创建完成后不支持切换安全组，请谨慎选择所属安全组。

步骤3 单击“立即创建”，确认规格后单击“创建”；

步骤4 创建成功后，即可返回对应的工作空间查看已创建的数据集成集群。

----结束

测试人员-数据清理转换作业调试

开发利用方-测试人员负责对开发空间的ETL作业等进行测试验证，测试验证通过后将作业导出至DataArts Studio生产空间进行上线发布。

1. 选择"数据开发>作业"，单击"执行调度"，对数据治理作业进行测试；
2. 在"作业监控"页面，查看作业运行情况。

图 3-74 作业监控

运维人员-跨工作空间作业导出

开发利用方-运维人员将开发利用方DataArts Studio开发空间的各委办局开发接入库的数据清理转换作业等导出包导入到DataArts Studio生产空间上线发布；将数据开发作业导出有两种操作方式：

方式一：单个作业导出

方式二：批量作业导出

- 方式一：在作业开发页面导出某一个作业

  双击作业名称，进入某一作业的开发页面，单击画布上方的导出按钮，选择导出作业的类型。

  - 只导出作业：导出作业中节点的连接关系，以及各节点的属性配置到本地，不包含密码等敏感信息。导出后，通过浏览器下载内容获取到zip格式的压缩包文件。
  - 导出作业及其依赖脚本：导出作业中节点的连接关系、各节点的属性配置以及作业的调度配置、参数配置、依赖的脚本、资源定义到本地，不包含密码等敏感信息。导出后，通过浏览器下载内容获取到zip格式的压缩包文件。

  图 3-75 导出作业

- 方式二：在作业目录中导出一个或多个作业

  a. 单击作业目录右侧按钮，选择“显示复选框”。

图 3-76 显示复选框

b. 勾选需要导出的作业，单击 > 导出作业，可选择“只导出作业”或“导出作业及其依赖脚本和资源定义”。导出完成后，即可通过浏览器下载地址，获取到导出的zip文件。

c. 作业中使用集群等不存在时，选择本工作空间下已创建的CDM集群。

图 3-77 导入作业

说明

CDM节点等依赖其他作业的节点， 需要将对应CDM作业，需要在"数据集成-作业管理"中，将原空间中作业导入新的工作空间。

3.1.5 开发利用方新增账号

场景说明

该场景主要描述开发利用方已经完成初次资源分配后新增人员入场的场景，由授权运营方管理员为新入场人员新建三级VDC账号并分配数据开发工具权限的操作。此场景在开发利用方每增加一个账号时配置一次。

创建 VDC 账号

授权运营方-管理员为三级VDC新增人员创建用户账号，并且将用户添加到对应用户组。

步骤1 **授权运营方-管理员**登录智能云管理平台页面，单击“开发利用方VDC”。

步骤2 在左侧导航栏单击“用户-创建”，新建该VDC下的账号。

步骤3 在左侧导航栏单击“用户组”，在对应用户组的操作列选择“添加用户”，将新增用户加入对应用户组。

如：新增账号为开发人员，将其加入"开发利用方VDC-云服务开发人员用户组"。

图 3-78 创建 VDC 账号

----结束

DataArts Studio 工具授权

DataArts Studio在开发利用方资源分配时，根据用户组进行授权（具体操作请见工作空间授权）。因此已经加入对应用户组的开发、测试、运维人员不需要再进行授权操作，可直接访问对应DataArts Studio工作空间，并进行相关开发、测试等操作。

ROMA Connect 工具授权

开发利用方-管理员登录智能云管理平台平台，进入ROMA Connect开发实例，给开发人员、测试人员用户组授权。

步骤1 在ROMA Connect开发实例中，单击集成应用的“应用授权管理”，授予新增开发人员modify+delete权限（默认添加read权限）；

步骤2 单击集成应用操作列的“应用授权管理”，授予新增测试人员modify权限（默认添加read权限）；

图 3-79 应用授权管理

----结束

3.1.6 开发利用方申请平台公共数据权限

场景说明

开发利用方为开展场景化的数据融合汇聚工作，向平台运营方申请平台公共数据只读权限，由平台运营方为其分配MRS开发/生产库的只读权限，或DWS相关Schema只读权限的相关操作。

开发利用方申请公共数据权限

开发利用方根据需要，通过线下提交申请方式向平台运营方申请公共数据只读权限。

需反馈信息如表-申请公共数据信息反馈表。

表 3-19 申请公共数据信息反馈表（MRS 库）-示例

申请账号	公共数据库类型	公共数据库名称	公共数据表名称
datagroup_dev_admin	MRS-HIVE库	dev_shdg_dwd	test_public1

表 3-20 申请公共数据信息反馈表（DWS 库）-示例

申请账号	公共数据库类型	公共数据库名称	公共数据schema及表名称
datagroup_dev_admin	DWS库	dev_tianji_dws	dev_shdg_dwd.test_public1

平台运营方公共数据库授权

- MRS-HIVE库

  【示例】以开发利用方访问公共数据库shbd_dwd_dwv库为例。

  为开发利用方的MRS用户（组）创建公共数据库只读权限的hive ranger策略。

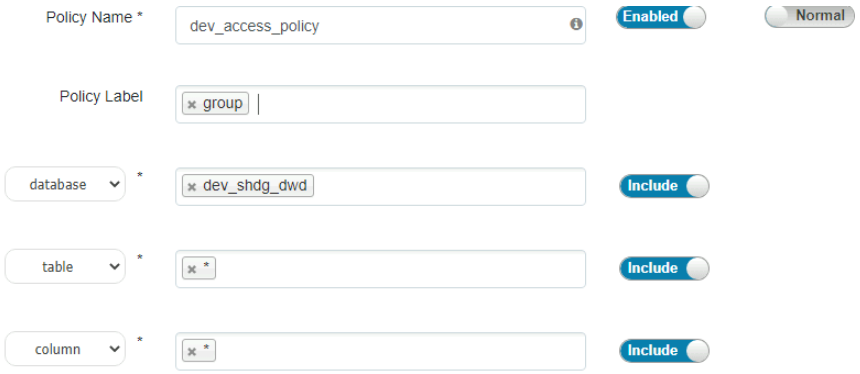
a. 登录ranger admin页面，单击右上角"add new policy"新建ranger访问策略。

b. 策略对象选择“database”，根据开发利用方反馈所需公共数据的需求，选择对应数据库、数据表；

选择对应数据库所在策略dev_access_policy；如访问单表需新建策略。

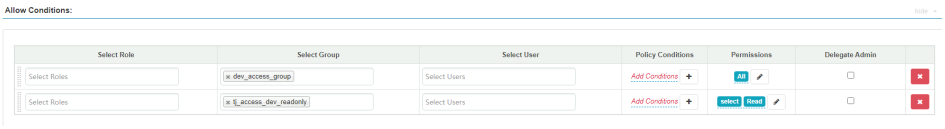
授予tianji_access_dev_readonly用户组shbd_dwd_dev库*表*列的select/read权限。

图 3-80 MRS-HIVE 库



c. 添加用户组对应权限，READ/SELECT。

图 3-81 添加用户组对应权限



- DWS库

默认情况下，用户只能访问属于自己的schema中的数据库对象。如果需要访问其他schema的对象，则该schema的所有者应该赋予他对该schema的usage权限。

【示例】以phjr场景下，开发人员账号访问公共数据schema为例。

a. 使用dbadmin账号连接dev_tianji_dws数据库；

b. 将Schema dev_shdg_dwd的权限赋给用户后，将公共数据Schema下，表public的select权限赋给phjr场景下的开发用户。

```
GRANT USAGE ON SCHEMA dev_shdg_dwd TO phjr_dev_admin;
GRANT SELECT ON TABLE dev_shdg_dwd.public to phjr_dev_admin;
```

说明

将Schema中的表或者视图对象授权给其他用户或角色时，需要将表或视图所属Schema的USAGE权限同时授予该用户或角色。否则用户或角色将只能看到这些对象的名字，并不能实际进行对象访问.

3.1.7 数据需求方资源分配

场景说明

该场景主要描述为保障数据需求方正常调用ROMA Connect数据服务API，由平台运营管理员在ROMA Connect中为其分配客户端App等相关操作。该场景下，为每一个数据

需求方单独创建一个客户端（即一个空的集成应用），将数据需求方需要访问的API授权给该客户端。然后给需求企业提供该客户端的key和secret，供访问使用。

ROMA 客户端 APP 发放

平台运营方-管理员为数据需求方在ROMA生产实例创建客户端应用。

客户端定义了一个API调用者的身份。可以将一个API授权给多个客户端，也可以将多个API授权给同一个客户端。 可以通过新建应用来添加客户端配置。

步骤1 平台运营方-管理员登录智能云管理平台，选择公共服务资源集1（ROMA生产实例所在资源集）。

步骤2 在导航栏选择ROMA Connect服务，进入控制台，在“实例”页面单击实例上的“查看控制台”，进入实例控制台。

步骤3 在左侧的导航栏选择“集成应用”，单击页面右上角的“创建集成应用”。

图 3-82 创建集成应用

步骤4 在创建集成应用弹窗中填写集成应用的“名称”，设置key和secret，然后单击“确认”。

----结束

绑定数据服务 API 到指定需求方客户端 APP

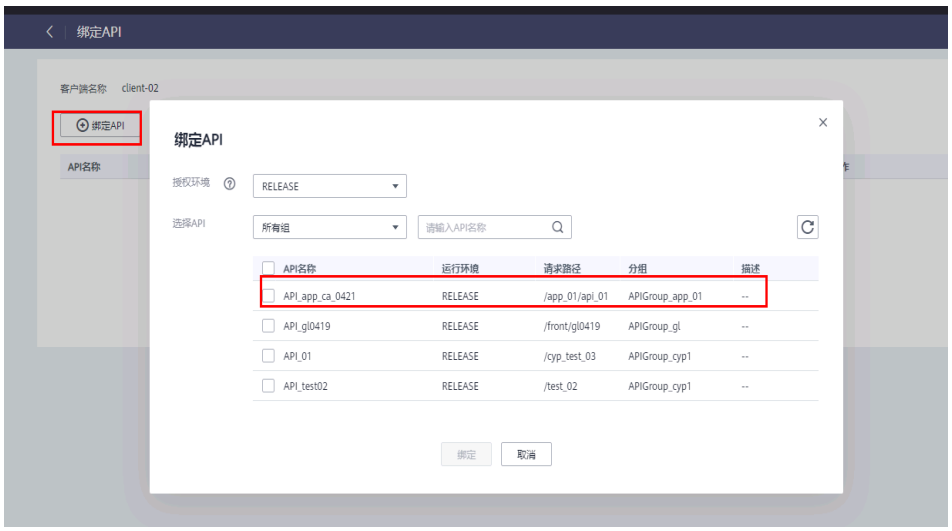
将数据服务API绑定至指定需求方客户端有两种操作方式：

- 通过客户端绑定；
- 在API授权信息标签页，将该API授权给指定客户端。

  a. 方式一：通过将客户端绑定API

图 3-83 客户端绑定 API

图 3-84 绑定 API



b. 方式二：或单击API，选择授权信息标签页，添加授权，将API授权给对应的客户端。

图 3-85 添加授权

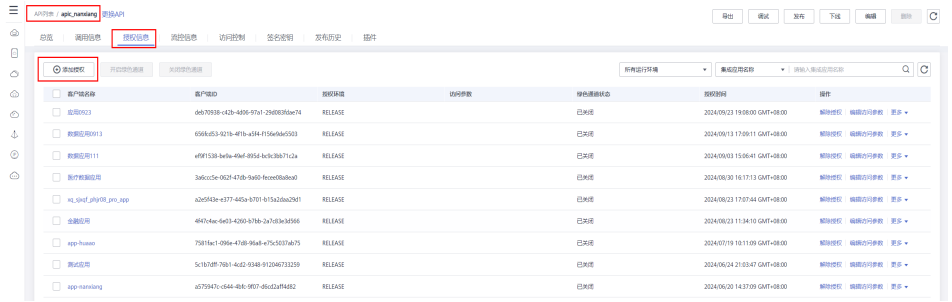
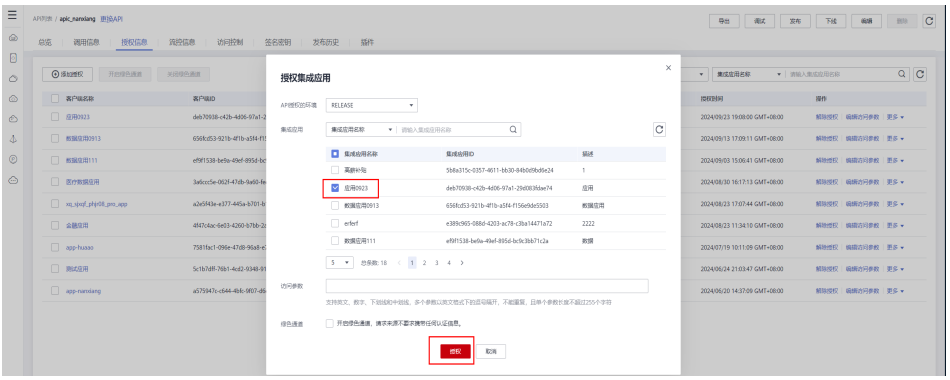


图 3-86 授权集成应用



数据需求方调用数据服务 API

数据需求方调用API过程请参考**3.4 场景四：数据需求方数据服务可信访问**。

3.2 场景二：运营平台授权运营管理

3.2.1 用户注册

授权运营平台用户分为企业角色和个人角色，企业角色为数据需求方、开发利用方、授权运营方等六类平台角色，个人角色为管理、开发、测试、运维等个人用户角色。各类平台角色的用户注册流程类似，本章节以数据需求方企业角色和个人角色注册为例。

企业角色注册

使用UK登录，进入授权运营平台后，单击“注册平台角色“进入平台角色注册页面；

图 3-87 注册平台角色

单击企业角色下拉框，选择“数据需求方“，企业名称输入框和企业统一信用代码框默认置灰，自动检索 USBKEY 的内置信息并展示。填写法人名称和企业联系人手机，单击“提交“按钮，将填好的企业角色注册信息提交给权限管理员审批。

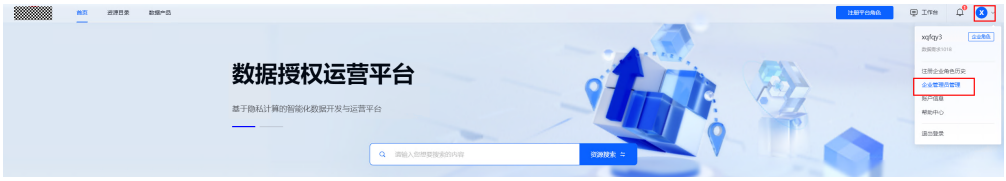
个人角色注册

企业角色注册好后，需先为企业注册管理员，由管理员注册企业的个人角色用户。

- 管理员注册

使用企业角色登录平台，先将光标移动至头像处，单击“创建管理员“；

图 3-88 创建管理员



在创建管理员页面，填写管理员账号、姓名、证件号等信息，单击“确认“按钮提交信息。

图 3-89 确认

- 运维人员注册

  各个人角色注册流程类似，此处以运维人员注册为例。

  使用**管理员注册**创建的企业管理员账号登录平台，先将光标移动至头像处，单击“创建企业员工“-“创建企业个人用户“；

图 3-90 创建企业员工

图 3-91 创建企业个人用户

选择“个人角色“为“运维人员“，填写个人账号、姓名、证件等信息，单击“确认“提交信息。

3.2.2 数据提供方企业资源编目

企业目录正编目

- 库表正编目

a. 使用**数据提供方-业务管理员**账号登录平台，单击“工作台“，选择“资源目录系统“；

图 3-92 资源目录系统

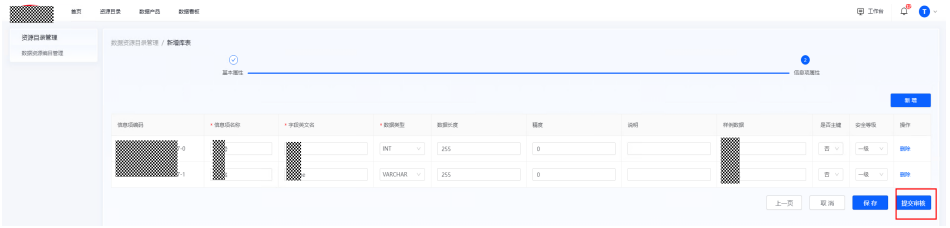
b. 单击“数据资源编目管理“ ，进入数据资源目录编目页面；

图 3-93 数据资源目录编目

c. 单击“库表目录“，在弹出页面对应的输入框中输入基本信息，单击“下一步“按钮；

d. 单击新增按钮，在输入框中输入对应的信息。输入完毕后单击输入框最右侧的保存按钮保存信息；

图 3-94 新增



e. 单击提交审核，将填写好的信息发送到审核方进行审核。

- API正编目

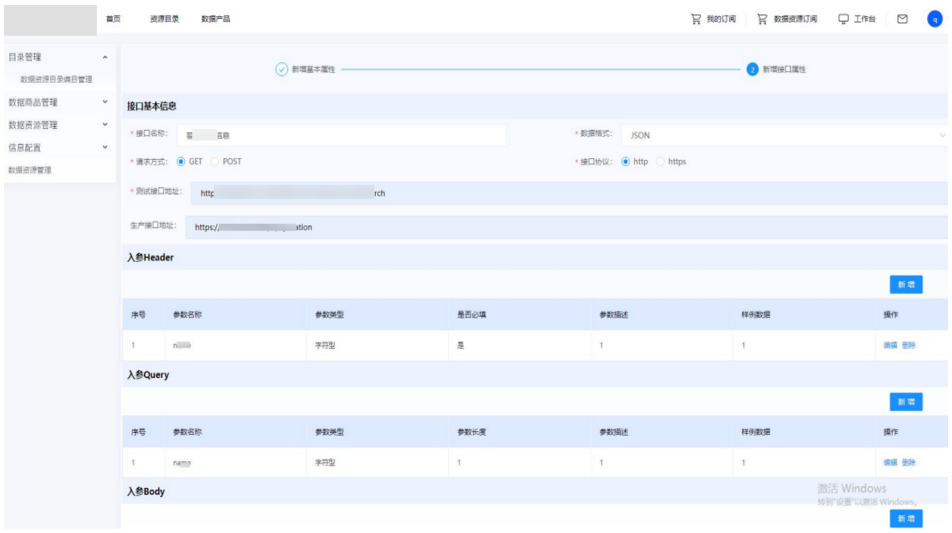
a. 使用**数据提供方-业务管理员**账号登录平台，单击“工作台“，选择“资源目录系统“；

b. 单击“目录管理>资源目录系统编目管理“ ，进入数据资源目录编目页面；

c. 单击“新增API目录“，在弹出页面对应的输入框中输入基本信息，单击“下一步“按钮；

d. 填入对应的 api 接口信息和接口参数 ；

图 3-95 填入对应信息和参数



e. 单击提交审核，将填写好的信息发送到审核方进行审核。

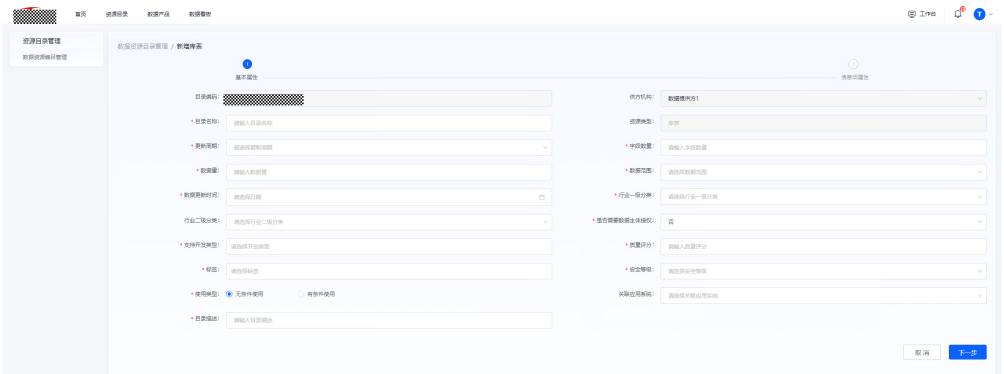
测试资源反编目

步骤1 使用**数据提供方-业务管理员**账号登录平台，在数据资源目录编目页面，选择“待编目“，查看待编目资源列表；

图 3-96 待编目

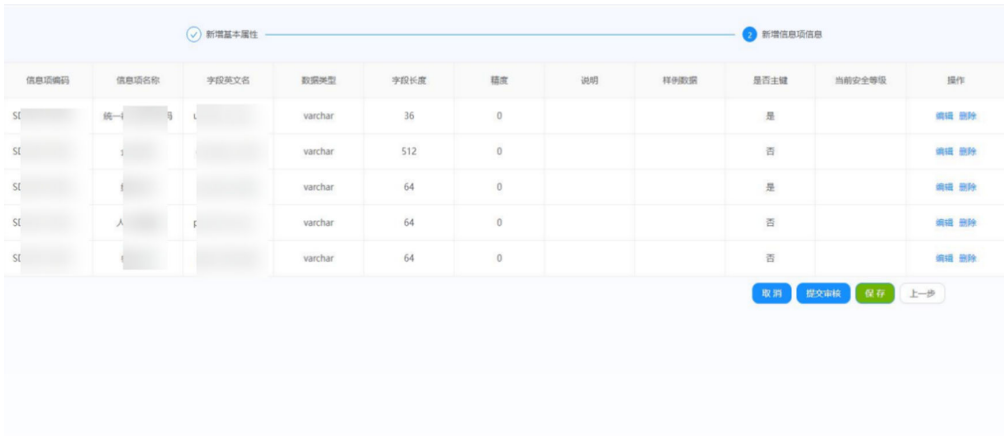
步骤2 单击对应测试资源后的“编目“按钮，在弹出页面填写测试资源基本属性；

图 3-97 编目



步骤3 单击“下一步“，在新增信息项信息页面核对测试资源的字段信息，确认无误后单击“提交审核“，发送到审核方进行审核。

图 3-98 提交审核



----结束

3.2.3 授权运营方授权运营目录编目

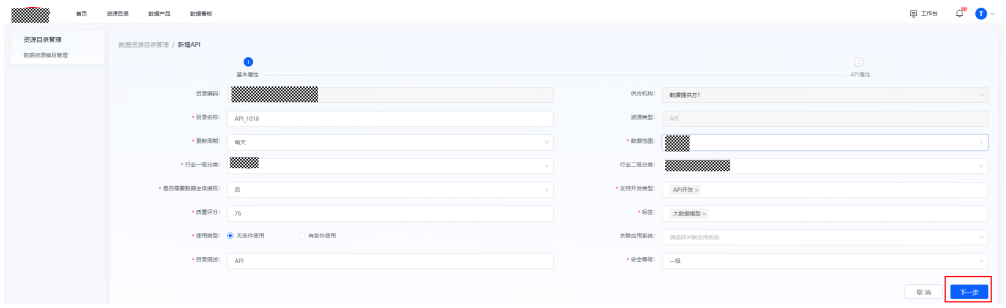
API 正编目

步骤1 使用**授权运营方-数据资源管理员**账号登录平台，选择“资源目录管理“；

步骤2 单击“数据资源编目管理“；

步骤3 单击“数据资源目录编目”，进而单击“新增API”创建一个新的 api目录；

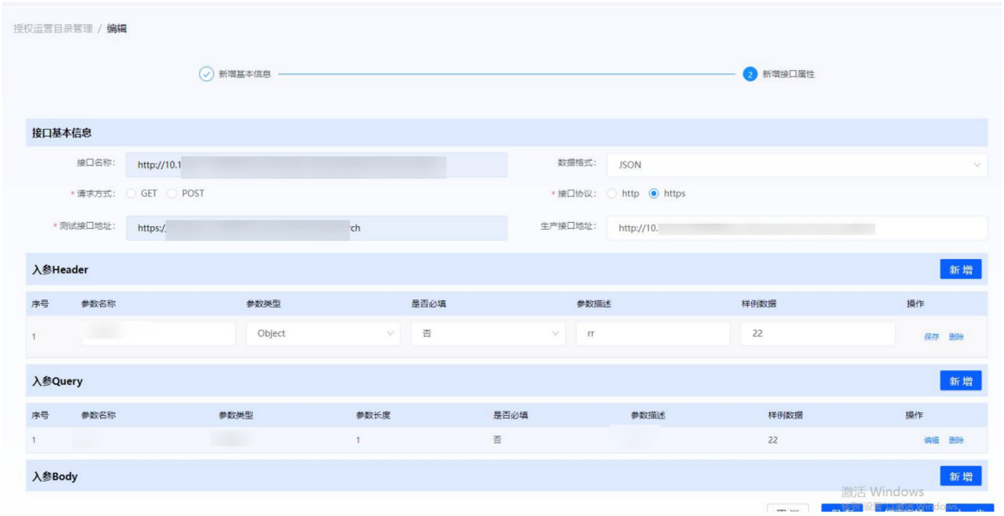
图 3-99 数据资源目录编目



步骤4 在弹出页面对应的输入框填入接口基本信息；

步骤5 单击“下一步“，在接口属性页面填写api接口信息和接口参数；

图 3-100 填写 api 接口信息和接口参数



步骤6 单击提交审核按钮，把填写好的目录发送到审核方审核。

----结束

库表反编目

步骤1 使用**授权运营方-数据资源管理员**账号登录平台，单击“工作台“，选择“资源目录系统“；

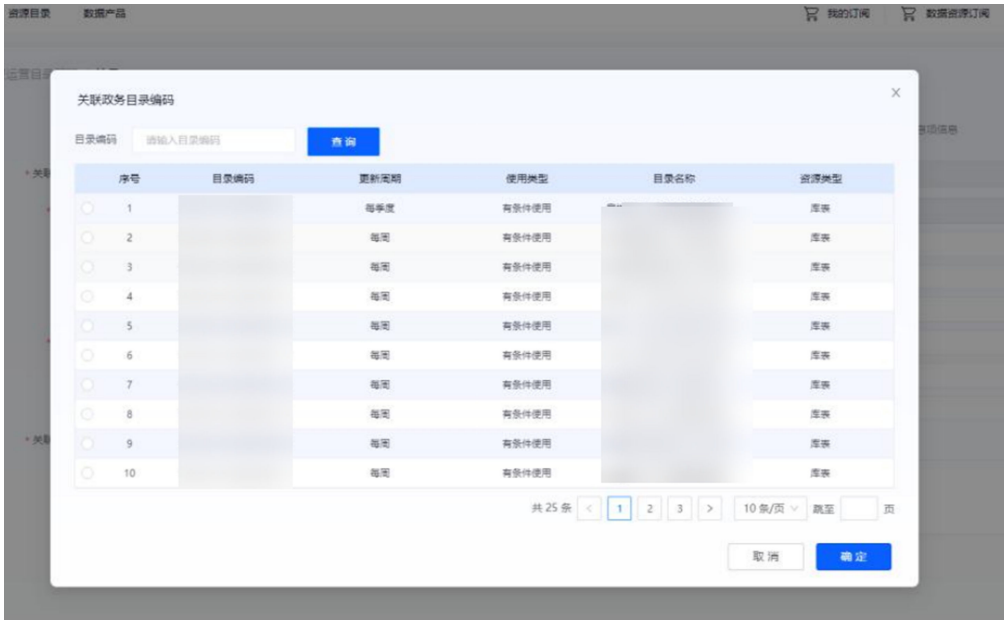
步骤2 单击“数据资源管理>授权运营目录管理>反编目“；

步骤3 选择待编目资源列表后的“编目“按钮，进行库表反编目；

图 3-101 编目

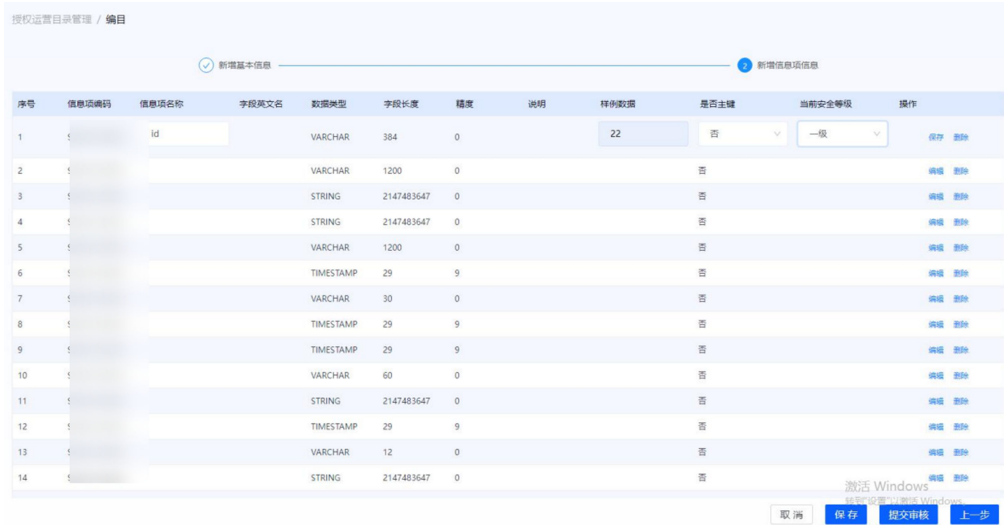
步骤4 在编目页面，单击“选择政务目录“，将对应资源关联到政务目录编码，勾选后单击“确定“；

图 3-102 关联到政务目录编码



步骤5 在输入框填写完成基本信息后，单击“下一步“，在信息项信息页面检查、编辑信息项；

图 3-103 检查、编辑信息



步骤6 单击“提交审核“将对应目录提交到审核方审批。

----结束

3.2.4 数据需求方需求申请

企业访问应用注册

数据需求方获取数据商品前，需要先完成企业访问应用的注册，获取访问密钥。

步骤1 使用**数据需求方-业务管理员**账号登录平台，将光标移动到头像处，单击“我的办理“；

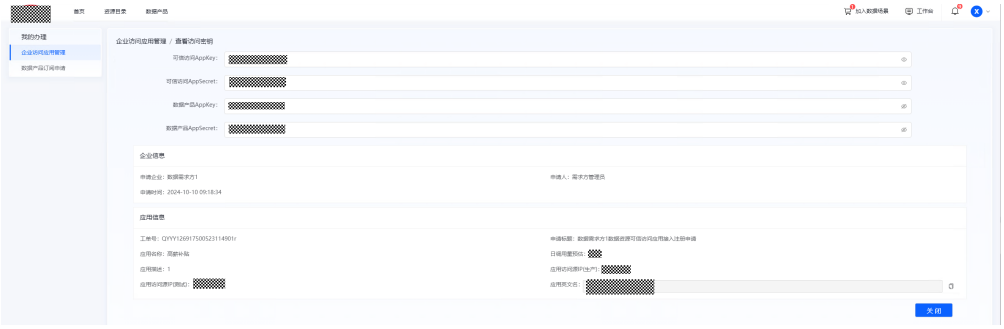
步骤2 单击左侧“我的发起>企业访问应用注册“，在弹出页面填写注册信息；

图 3-104 企业访问应用注册

步骤3 确认信息无误后，单击“提交“将注册信息提交审核；

步骤4 审核通过后，在企业访问应用注册页面，单击“查看申请访问密钥“，可查看到访问应用的密钥信息和企业信息。

图 3-105 企业访问应用注册页面

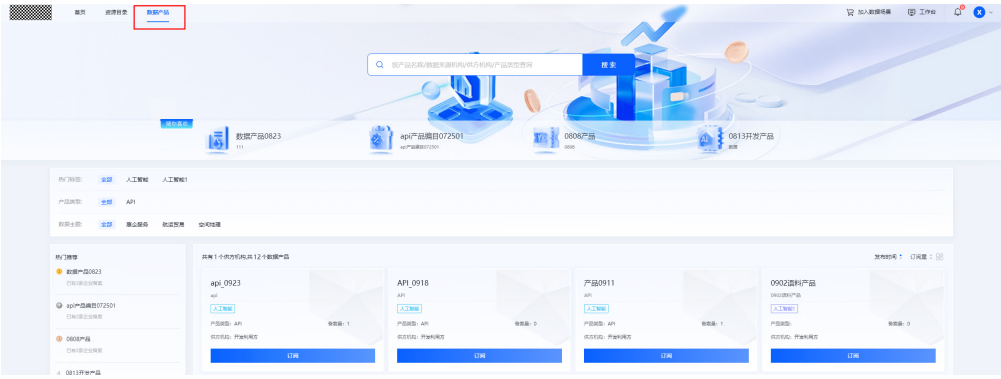


----结束

数据产品订阅

步骤1 使用**数据需求方-业务管理员**账号登录平台，在平台首页单击“数据产品“；

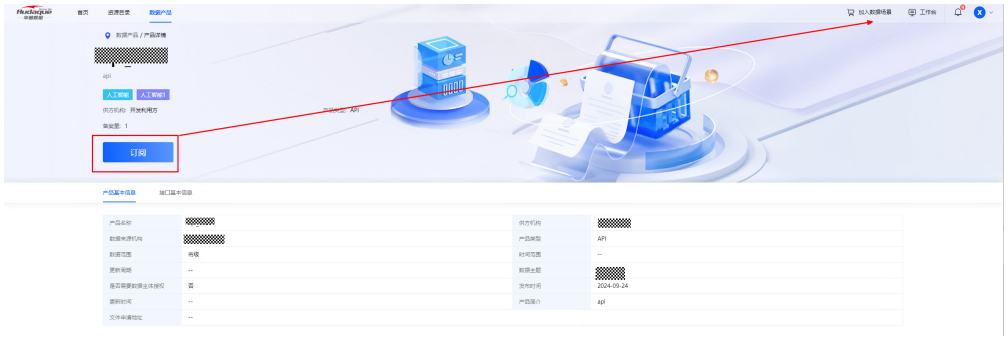
图 3-106 数据产品



步骤2 选择一个数据商品，单击进入详情页；

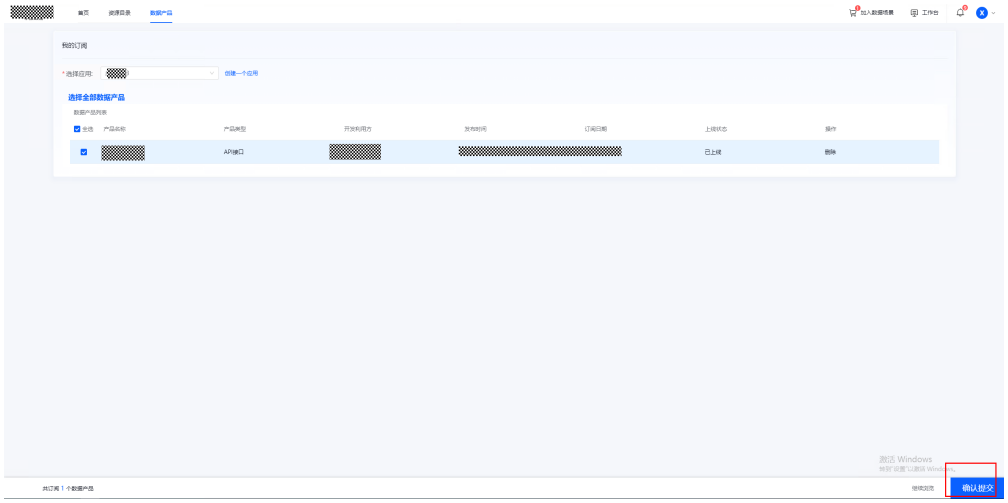
步骤3 单击“订阅“按钮，订阅成功后单击“我的订阅“；

图 3-107 我的订阅



步骤4 选择一个应用并且勾选选择的产品，单击提交订单，完成数据产品的订阅。

图 3-108 提交订单



----结束

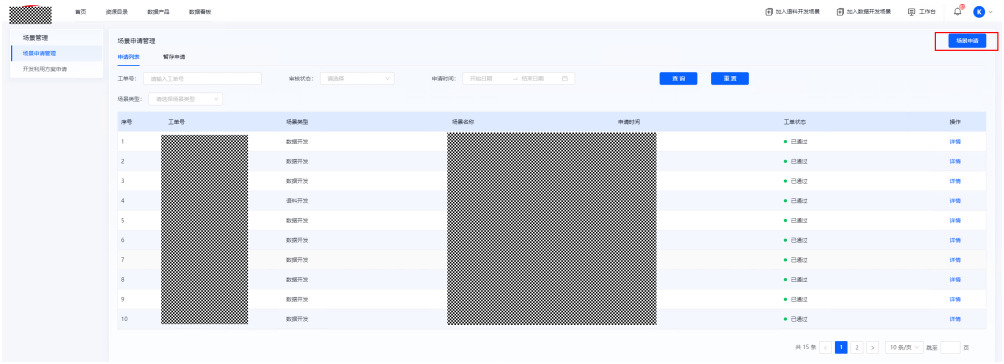
3.2.5 开发利用方场景开发及工具使用

场景申请

步骤1 使用**开发利用方-产品经理**账号登录平台，光标移动至头像处，单击“我的办理“；

步骤2 在“我的办理“页面，单击导航栏“我的发起>场景申请管理“，单击“场景申请“；

图 3-109 场景申请



步骤3 在弹出页面中填写场景申请对应的信息，并上传附件，单击“确认“提交申请；

图 3-110 确认

----结束

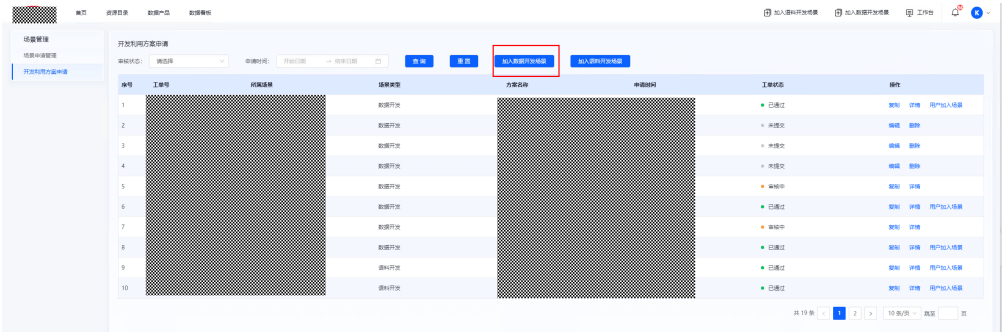
开发方案申请

完成**场景申请**及审核通过后，进行开发方案（子场景）的申请。

步骤1 使用**开发利用方-产品经理**账号登录平台，光标移动至头像处，单击“我的办理“；

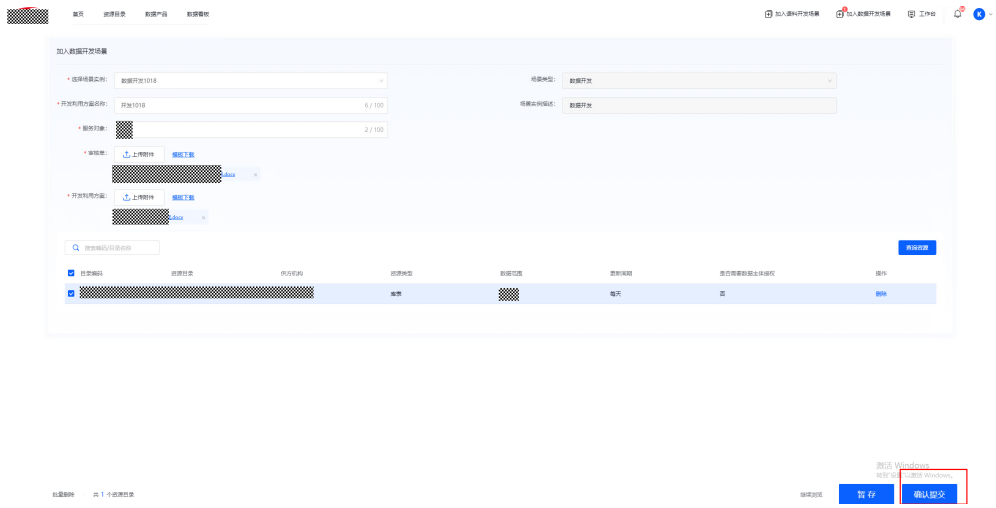
步骤2 在“我的办理“页面，单击导航栏“我的发起>数据资源加入场景（子场景）“，在页面中单击“开发利用方案申请“；

图 3-111 开发利用方案申请



步骤3 在弹出页面填写方案申请对应的信息，并上传附件，勾选数据资源，单击“确认“提交申请。

图 3-112 确认



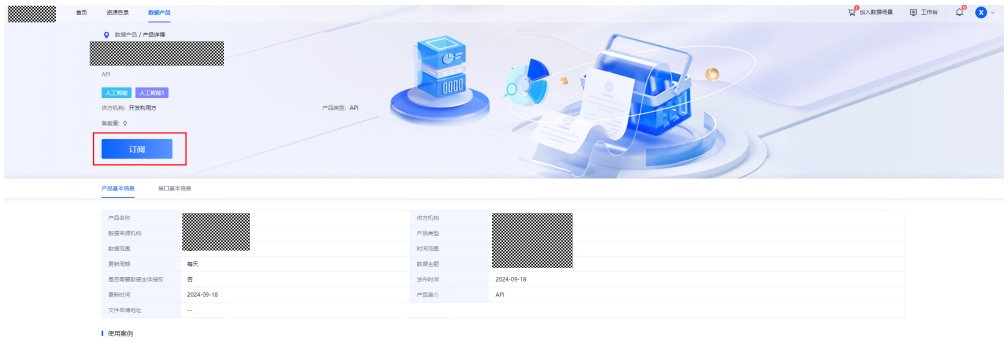
----结束

测试资源订阅

步骤1 使用**开发利用方-产品经理**账号登录平台，在首页单击“资源目录“；

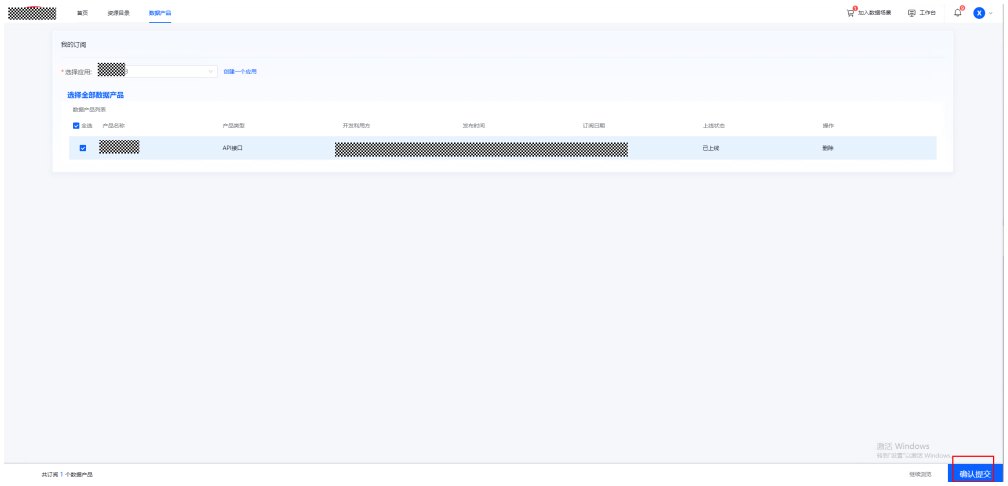
步骤2 选择需要的测试资源，单击进入详情页，在详情页中单击“订阅“完成订阅；

图 3-113 订阅



步骤3 在提示弹窗中单击“进入我的订阅“，在数据商品列表中勾选需要的数据资源，单击“提交订阅“提交审核。

图 3-114 提交订阅



----结束

生产数据申请

生产数据申请流程同**测试资源订阅**。

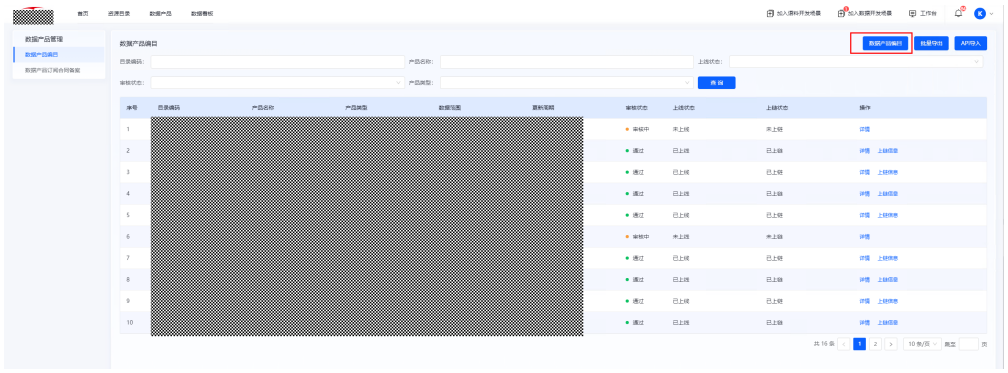
产品编目与发布

在完成数据治理后，开发利用方可将封装好的API资产上架到平台作为数据商品进行编目和发布。

步骤1 使用**开发利用方-数据商品管理员**账号登录平台，光标移动至头像处，单击“个人中心“；

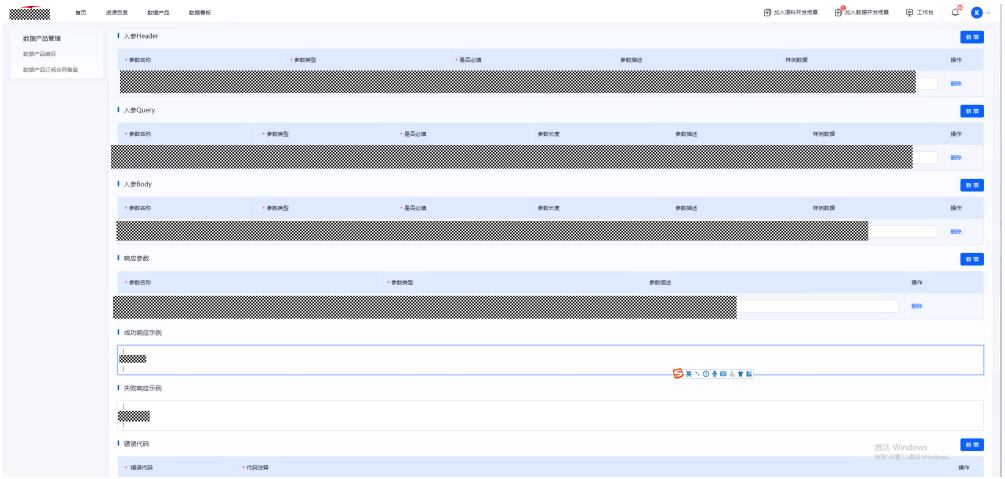
步骤2 在左侧导航栏选择“数据商品管理>数据商品编目管理“，单击“数据商品编目“；

图 3-115 数据商品编目



步骤3 在弹出页面填写数据商品基本属性信息和接口属性，单击“提交审核“将数据商品提交审核。

图 3-116 提交审核



----结束

3.3 场景三：一站式工作台授权（DataArk)

3.3.1 开发工具集成与授权

DataArk定位为融合华为DataArts Studio、ROMA Connect、TICS和生态伙伴能力的一站式数智融合集成使能平台，在一个界面集成各云服务，同时统一用户和统一角色权限管理，降低用户角色授权操作复杂度。在公共数据授权运营场景下，提升开发利用方操作效率。

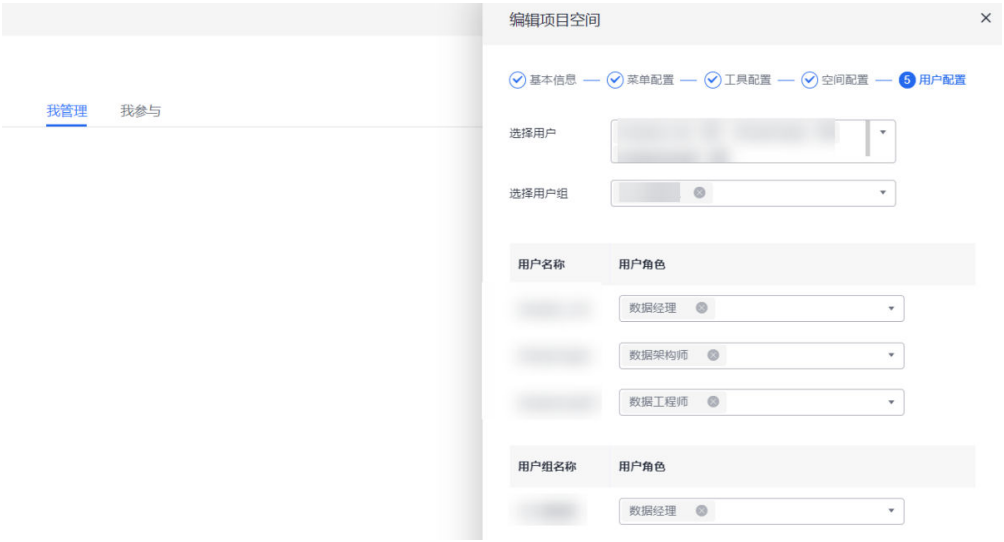
DataArts Studio 集成与授权

步骤1 使用**平台运营方-管理员**账号登录平台，进入DataArk控制台，在左侧导航栏单击”运营管理>工作空间管理>添加工作空间”，为开发利用方新建工作空间；

步骤2 在”空间配置” 页面，关联DataArts Studio工作空间选择”创建全新的DataArts Studio工作空间”，在”用户配置”页面，添加开发利用方管理员为空间”数据经理”角色，单击”确定”创建；

步骤3 使用**开发利用方-管理员**账号登录平台，进入DataArk控制台，在左侧导航栏单击”运营管理>工作空间管理”，编辑步骤2创建的工作空间，在”用户配置”页面添加开发利用方各用户并赋予对应权限。

图 3-117 编辑项目空间



----结束

ROMA Connect 集成与授权

基于ROMA Connect集成应用隔离开发利用方，需要先参照章节**ROMA Connect开发工具授权**完成集成应用用户权限分配。

步骤1 使用**平台运营方-管理员**账号创建空间时，在”菜单配置”页面，单击”数据服务>数据服务API”，子系统选择”ROMA”；

图 3-118 菜单配置

步骤2 单击”下一步”，在空间配置页面，关联ROMA工作空间选择对应的ROMA实例。

----结束

TICS 工具集成

使用**平台运营方-管理员**账号创建空间时，在”菜单配置”页面，单击”数据安全>可信计算”，“是否启用“选择“启用“，子系统选择”TICS”。

3.3.2 数据底座自动授权

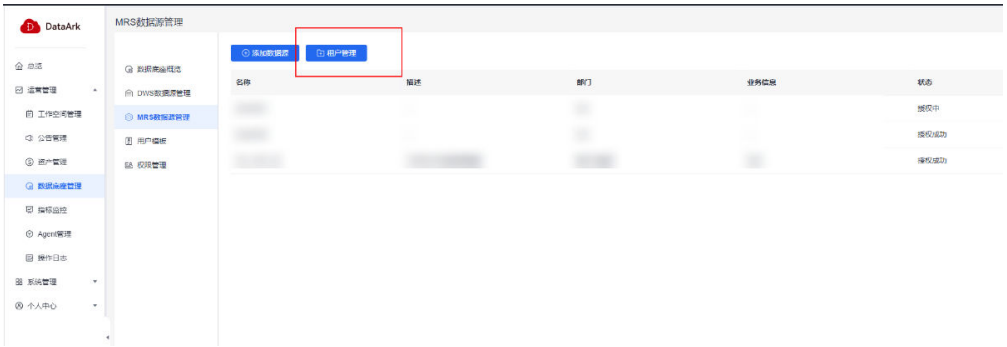
手工完成数据底座授权操作界面多、步骤长，且需要通过JSON和SQL语句繁琐配置。本章节旨在指导通过DataArk统一平台完成数据底座自动授权，具体授权用户和授权策略请参考3.1.3.2 数据底座授权。

MRS 自动授权

创建MRS租户

步骤1 使用**开发利用方-管理员**账号登录智能云管理平台，进入DataArk控制台，在左侧导航栏选择“运营管理>数据底座管理>MRS数据源管理“；

图 3-119 租户管理



步骤2 单击“租户管理“，跳转至MRS租户管理页面；

步骤3 添加租户，创建两个二级租户：develop和produce，租户类型选择“非叶子租户”；

图 3-120 添加租户

步骤4 在已创建的二级租户下，选择添加子租户，创建三级租户。如devlop_phjr，租户类型选择“叶子租户”，注意父租户需要区分开发和生产二级租户。

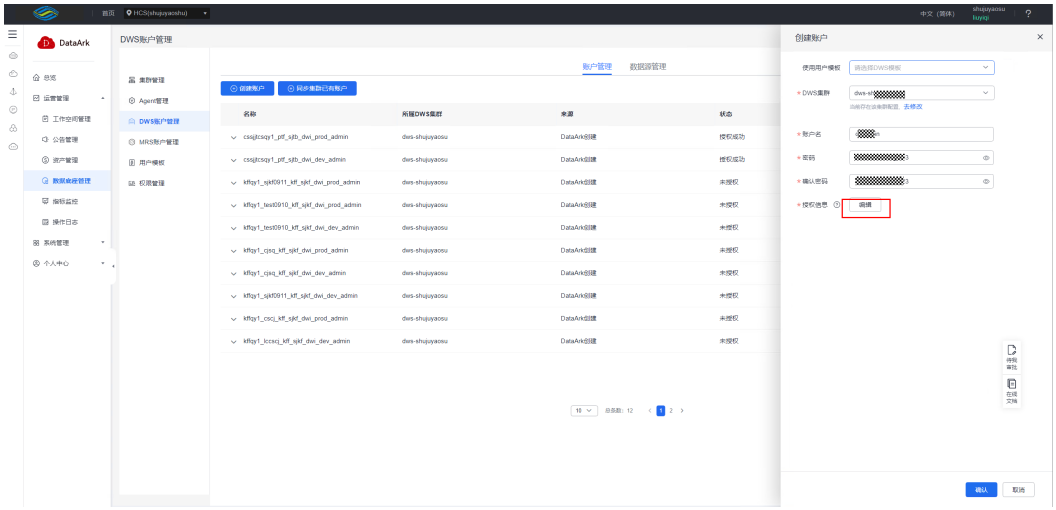
----结束

DWS 自动授权

步骤1 使用**开发利用方-管理员**账号登录智能云管理平台，进入DataArk控制台，在左侧导航栏选择“运营管理>数据底座管理>DWS数据源管理“；

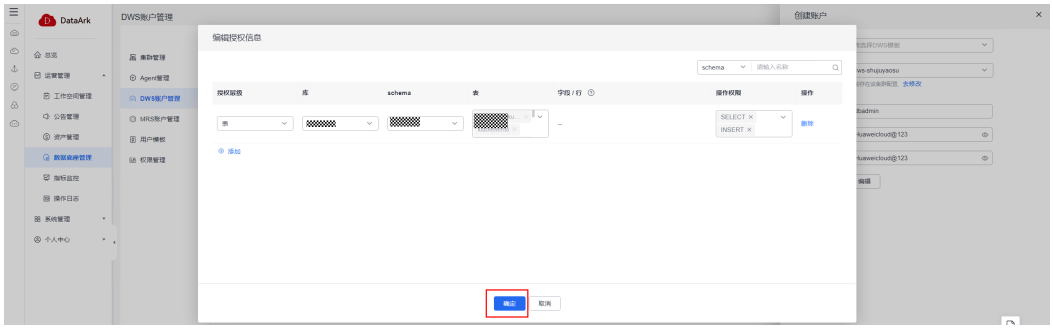
步骤2 单击“创建账户“，在弹出界面选择DWS实例，输入用户名、密码；

图 3-121 添加数据源



步骤3 单击“编辑“授权信息，在弹出页面添加授权信息；

图 3-122 编辑授权信息



步骤4 单击“确认“后添加数据源成功，用户和对应权限创建、授予成功。

----结束

3.3.3 资产跨空间/实例高效共享

开发工具DataArts Studio、ROMA Connect开发测试空间/实例和生产空间/实例相互隔离，生产环境上线操作依托于人工导出、导入，操作复杂，效率低下。DataArk可实现跨工作空间/实例的资产高效共享，数据治理资产一键归档、部署。

数据治理资产高效共享

DataArk可实现数据治理资产，如调研模板、流程设计、主题设计、数据码表、数据标准、关系模型、维度模型等资产全量和增量细粒度高效共享。

须知

部分数据治理资产类型的部署存在约束条件：

- 开发资源：目录无jarPackage文件夹；
- 质量规则：目标空间已有同步数据源；
- 原子指标/衍生指标/复合指标/时间限定：部署用户为目标空间审批人，且前置的维度与事实表已发布；
- 开发作业：目标空间已有可用cdm集群。

- 全量数据治理资产共享

  a. 使用**开发利用方-管理员**账号登录智能云管理平台，进入DataArk控制台，在左侧导航栏选择“运营管理>资产管理>归档资产“；

  b. 单击“归档“，在弹出界面选择归档来源工作空间，资产类型选择“全选“，资产范围选择“全部资产“；

  图 3-123 归档 1

  c. 全量资产归档成功后，单击“分享“，选择目标工作空间；

  d. 单击“公共资产“，在界面中找到步骤3分享的全量资产，单击“部署“，将资产部署到目标工作空间。

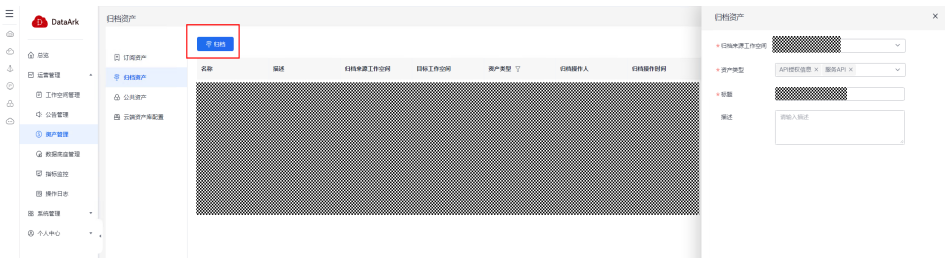
- 数据服务API高效共享

  公共数据授权运营场景下，集成应用对应数据开发利用方，客户端对应数据需求方，为每一个企业单独创建一个客户端（即一个空的集成应用），将需求企业需要访问的API授权给该客户端。因此，数据服务API从开发实例迁移至生产实例需要同时迁移服务API和授权信息。

  a. 使用**开发利用方-管理员**账号登录智能云管理平台，进入DataArk控制台，在左侧导航栏选择“运营管理>资产管理>归档资产“；

  b. 单击“归档“，在弹出界面选择归档来源工作空间，资产类型选择“服务API“和“API授权信息“，资产范围选择“全部资产“；

  图 3-124 归档 2

c. 归档成功后，单击“分享“，选择目标工作空间；
d. 单击“公共资产“，在步骤3分享的资产后单击“部署“，选择目标工作空间，先完成“服务API“部署；
e. 进入ROMA Connect生产实例，在API列表中将步骤4部署的API全部上线；
f. 再在“公共资产页面“，完成“API授权信息“的部署。

3.4 场景四：数据需求方数据服务可信访问

3.4.1 数据运营方准备环境

环境准备

概述：ROMA Connect实例发放后，配置参数提供了实例内组件的公共参数配置，通过修改配置参数，可以调整组件的相关功能配置。该章节根据运营平台的可信访问的需求，对ROMA Connect的实例进行参数配置，以满足APP验证、公网访问等功能的使用要求。

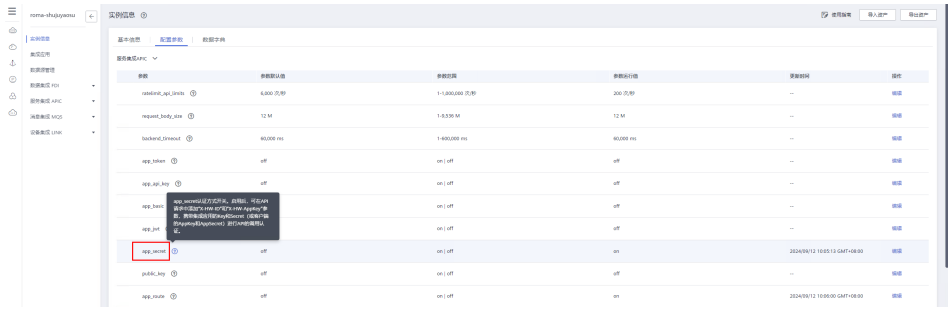
前提条件：已创建ROMA Connect实例。修改实例配置参数会引起APIC业务中断，建议在无业务运行或业务低峰时修改配置参数。

操作步骤

1. ROMA Connect的API验证分为如下四类：
   - APP认证：表示由ROMA Connect对API请求进行安全认证。用户调用API时，使用授权集成应用的Key和Secret进行API请求的安全认证。使用该方式的API适合所有用户调用。
   - 华为IAM认证：表示由IAM对API请求进行安全认证。用户调用API时，使用Token或AK/SK进行API请求的安全认证。使用该方式的API仅适合同一云服务平台的用户调用。
   - 自定义认证：表示使用自定义的函数API对API请求进行安全认证。使用该方式的API适合所有用户调用。
   - 无认证：表示API请求不需要认证。使用该方式的API适合所有用户调用。

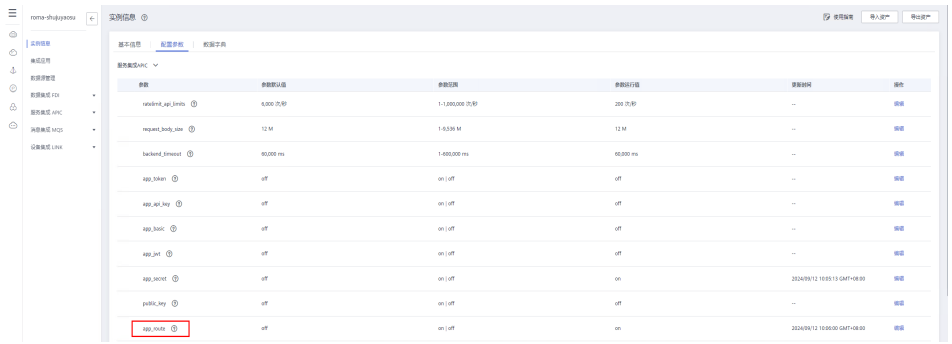
   本方案中需要使用**APP认证**，因此数据运营方需要在ROMA Connect的实例的配置参数设置中打开"app_secret"，从而开启APP认证功能。（单击“编辑”，可修改“参数运行值”）。

   图 3-125 环境准备 1



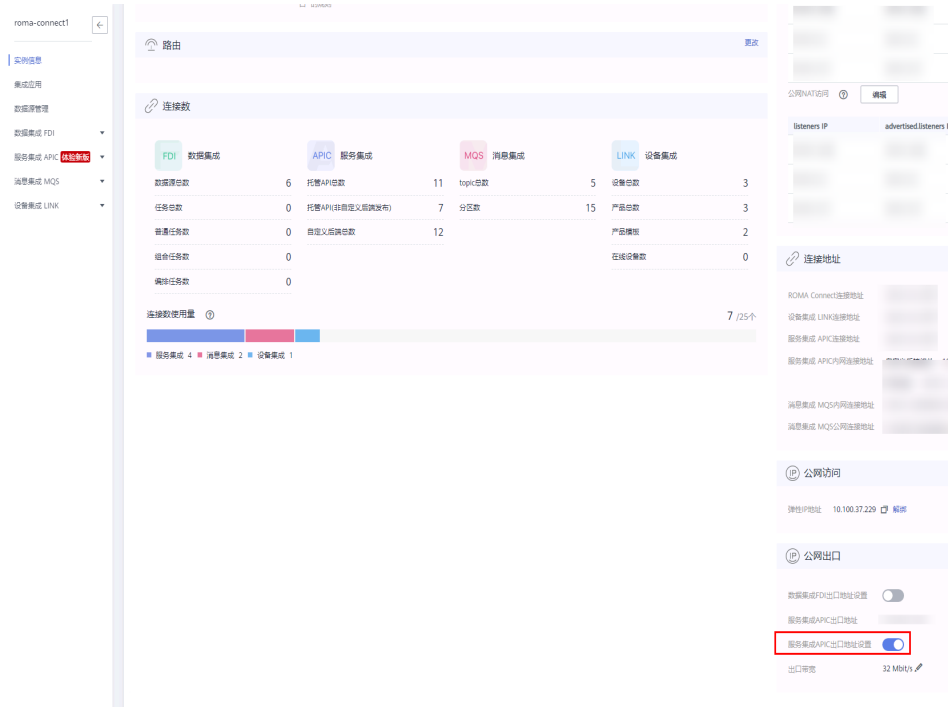
2. 由于开发过程中需要使用**ip访问**API，需要在ROMA实例的配置参数设置中打开"app_route"。

图 3-126 环境准备 2



3. 在可信访问过程中，验证token时需要调用位于公网的CA的接口，因此需要放开APIC的**出口地址设置**开关，并在防火墙中放开该EIP。

图 3-127 环境准备 3



4. 若ROMA Connect实例与后端服务在同一区域的不同VPC内时，可通过**创建VPC对等连接**，将两个VPC的网络打通，实现同一区域跨VPC访问后端服务。
5. 若ROMA Connect实例与后端服务在不同区域的不同VPC内时，可通过**创建云连接实例**并加载需要互通的VPC，将两个VPC的网络打通，实现跨区域跨VPC访问后端服务。

应用和客户端的准备

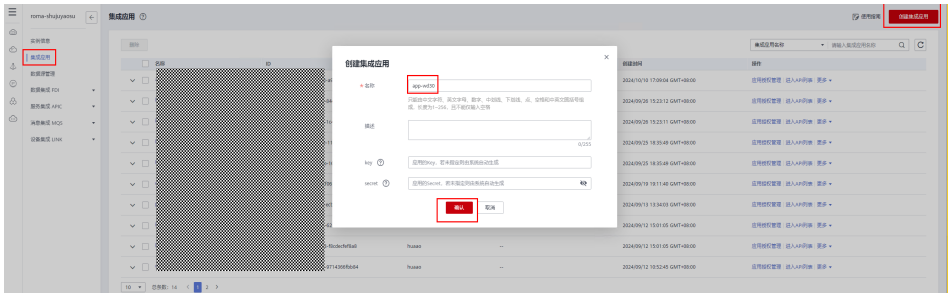
概述：ROMA Connect通过**集成应用**来实现同一实例内不同用户间的资源隔离。用户在ROMA Connect实例中创建的资源（如数据源、API、Topic、产品等）都要有归属的集成应用，非管理员权限的用户默认只能查看和管理自己创建的集成应用和资源，无法查看其他用户创建的集成应用和资源，管理员权限的用户可查看和管理其下所有用户所创建的资源。

前提条件：运营管理员已获取需要创建的集成应用的清单，集成应用对应数据开发利用方，客户端对应数据需求方。其中客户端为空白集成应用，命名建议使用前缀区分。

操作步骤

1. ROMA Connect实例中的资源都要归属到某个集成应用下，在创建其他资源前，您需要确保有一个集成应用。若已有可用的集成应用，可跳过此步骤。
   - 登录ROMA Connect控制台，在“实例”页面单击实例上的“查看控制台”，进入实例控制台。
   - 在左侧的导航栏选择“集成应用”，单击页面右上角的“创建集成应用”。
   - 在创建集成应用弹窗中填写集成应用的“名称”，然后单击“确认”。

   图 3-128 创建集成应用

2. 客户端定义了一个API调用者的身份。可以将一个API授权给多个客户端，也可以将多个API授权给同一个客户端。 可以通过新建应用来添加客户端配置。

   对应数据需求企业，为每一个企业单独创建一个客户端（即一个空的集成应用），将需求企业需要访问的API授权给该客户端。然后给需求企业提供该客户端的key和secret，供访问使用。
   - 方法一：通过将客户端绑定API

   图 3-129 通过将客户端绑定 API

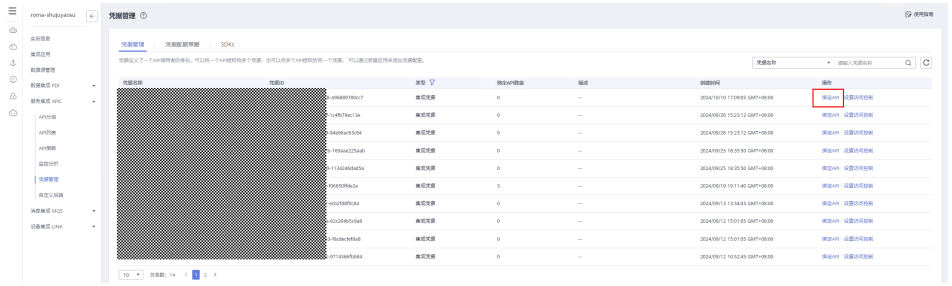
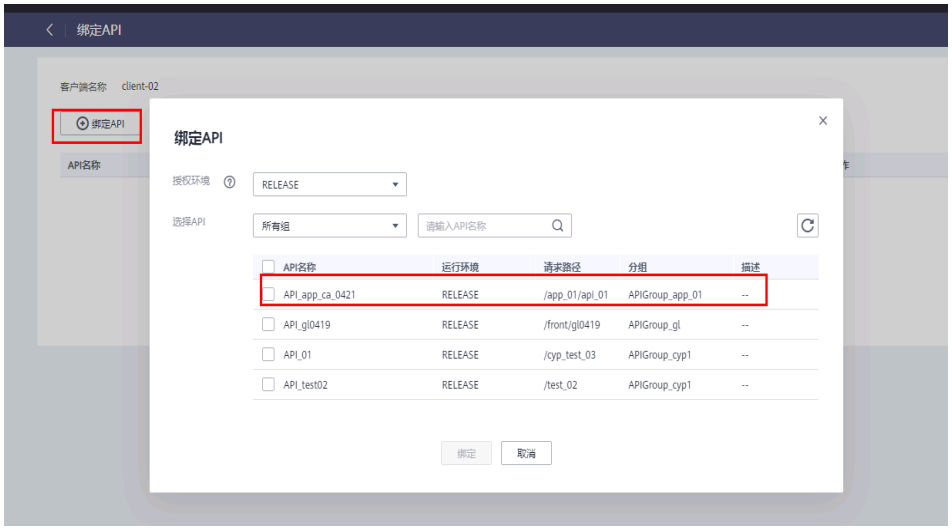
   

图 3-130 绑定 API



- 方法二：单击API，选择授权信息标签页，添加授权，将API授权给对应的客户端。

图 3-131 添加授权 1

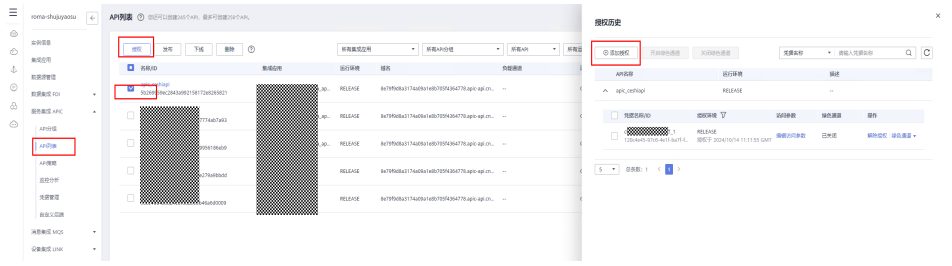
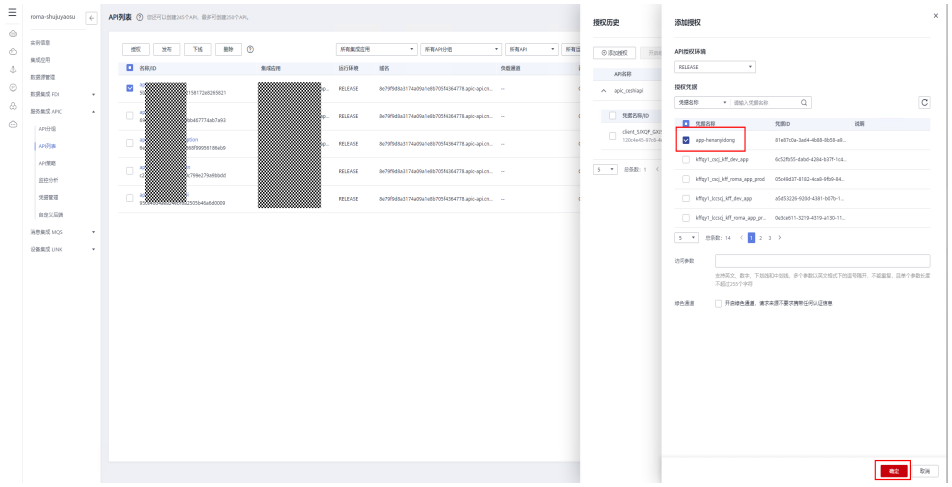


图 3-132 添加授权 2



3.4.2 开发利用方开发 API

3.4.2.1 创建 API 分组

概述

API分组是同一类业务API的集合，API开发者以API分组为单位，管理分组内的所有API。每个API都要归属到某个API分组下，在创建API前应提前创建API分组。

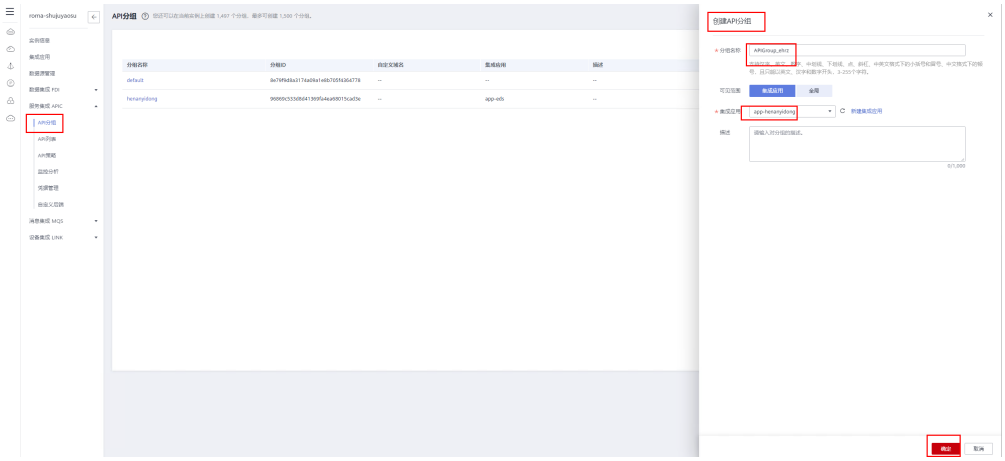
前提条件

每个API分组都要归属到某个集成应用下，在创建API分组前您需要有可用的集成应用，数据开发利用方需要由运营方管理员分配应用权限。

操作步骤

1. 登录ROMA Connect控制台，在“实例”页面单击实例上的“查看控制台”，进入实例控制台。
2. 在左侧的导航栏选择“服务集成 APIC > API管理”，在“API分组”页签中单击“创建分组”。
3. 在创建分组弹窗中配置API分组相关信息，然后单击“确定”，创建API分组。

图 3-133 创建 API 分组



3.4.2.2 配置数据源

概述

在创建数据API之前，您需要先接入数据源，确保可以正常从数据源读取数据。根据数据源类型的不同，数据源的接入配置有所差异。

具体数据源参数配置请参考《**应用与数据集成平台(ROMA Connect) 1.10.0 使用指南 (for 华为云Stack 8.2.1) 02**》中的"5.数据源管理"。

前提条件

1. 在接入数据源前，请确保ROMA Connect实例与您的数据源所在网络互通。
   - 若ROMA Connect实例与数据源在相同VPC内时，可直接访问数据源。
   - 若ROMA Connect实例与数据源在同一区域的不同VPC内时，可通过**创建VPC对等连接**，将两个VPC的网络打通，实现同一区域跨VPC访问数据源。

- 若ROMA Connect实例与数据源在不同区域的不同VPC内时，可通过**创建云连接实例**并加载需要互通的VPC，将两个VPC的网络打通，实现跨区域跨VPC访问数据源。
- 若ROMA Connect实例与数据源通过公网互通，请确保ROMA Connect实例已绑定弹性IP，且弹性IP与公网互通。

2. 若ROMA Connect实例跨VPC内网访问数据源时，需要完成实例到数据源所在子网的路由配置。
3. 如果需要使用公网地址访问数据源，请提前开启数据集成FDI公网出口。
4. 数据源连接信息，请联系数据运营方获取。

操作步骤

说明

本章节示例所使用的为模拟数据源（RDS）和模拟数据，因此操作包含数据源的申请创建和数据的写入。实际操作中，如若已经有数据源和数据表格，请直接跳转至**步骤3**。

如果需要使用公网地址访问数据源，请提前开启”实例信息”页面-->”公网出口”-->”数据集成FDI出口地址设置”。

步骤1 这里数据后端以RDS for MySQL为例，创建RDS实例后，单击实例管理页面登录，输入数据库账号密码登录。

图 3-134 登录

图 3-135 实例管理页面登录

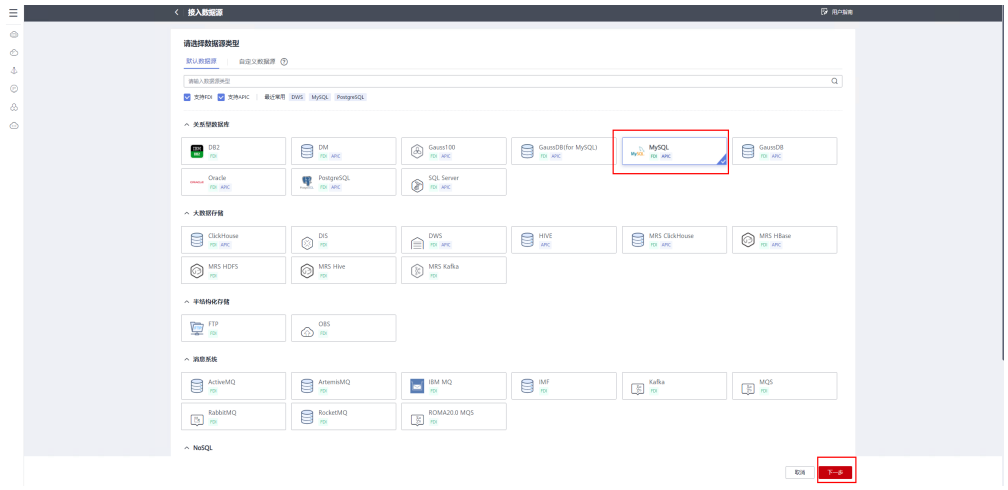
步骤2 单击打开对应数据库，打开SQL窗口，输入所需要的DDL语句，完成数据源和表格的创建。

图 3-136 SQL 查询

步骤3 单击进入ROMA Connect的应用，如下图，单击添加输入源，选择”Mysql”类型数据源，然后单击”下一步”。

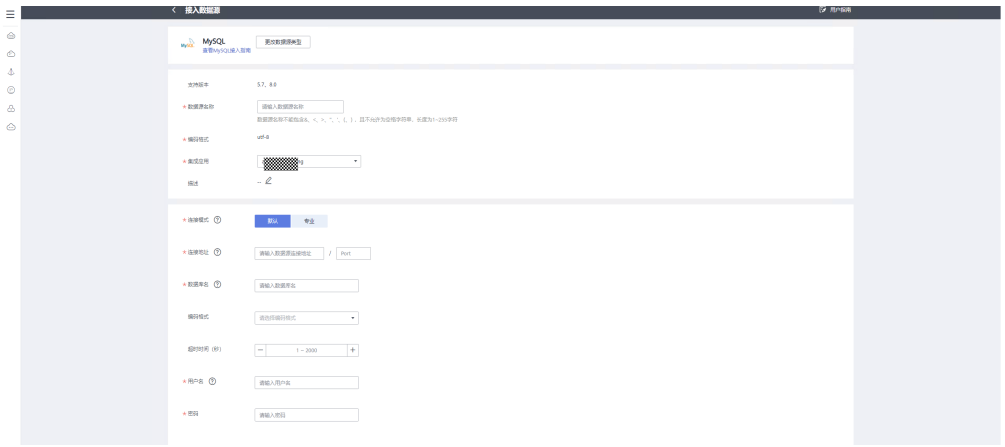
图 3-137 数据源

图 3-138 建入数据源



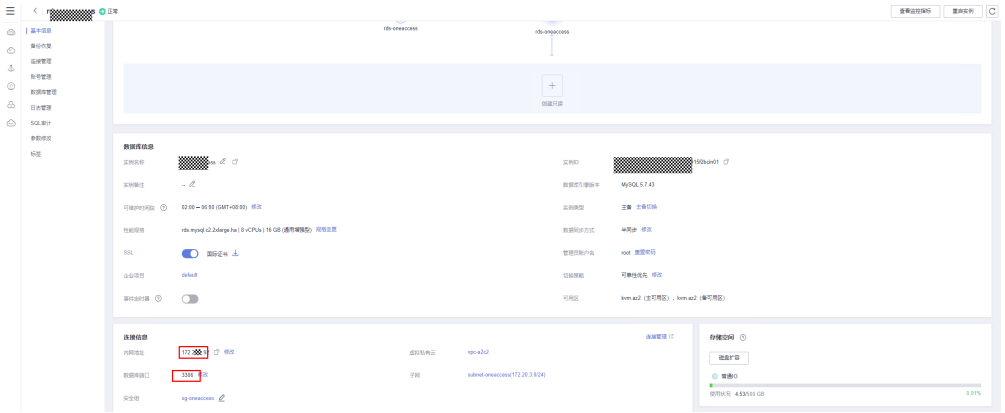
选择应用，为该应用创建数据连接。根据数据库实例中的连接地址和接口完成接入数据源接入信息，单击测试连接。验证通过后单击保存即可完成数据连接创建。

图 3-139 建数据连接



步骤4 从RDS实例页面获取接入地址和端口，并输入账号密码

图 3-140 输入账号密码



----结束

3.4.2.3 创建数据后端

概述

ROMA Connect支持把数据源定义为后端服务，可以通过SQL的形式查询数据库中的数据，实现从数据源中读写数据，并以API的形式对外开放。

前提条件

数据源已创建，数据源存储的单行数据大小建议不超过2KB，若超过该限制会导致自定义后端响应异常。

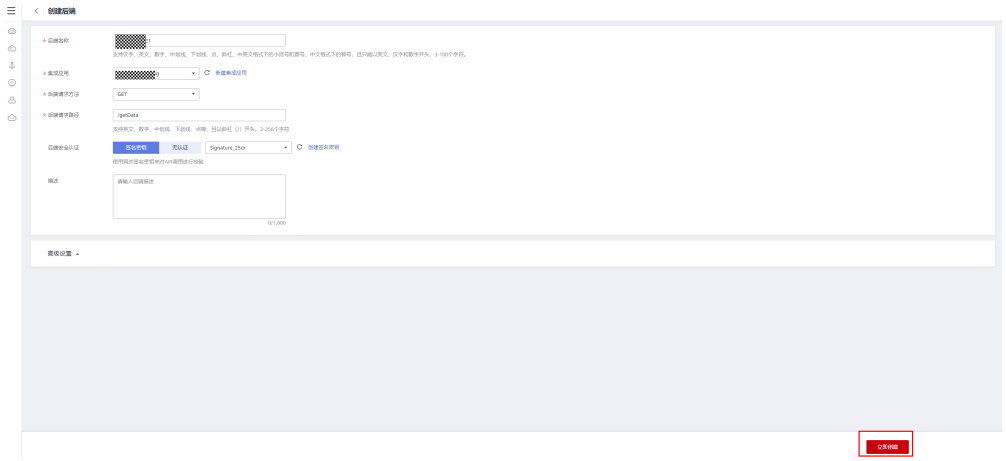
操作步骤

步骤1 登录ROMA Connect控制台，在“实例”页面单击实例上的“查看控制台”，进入实例控制台。

步骤2 在左侧的导航栏选择“服务集成 APIC > 自定义后端”，在“后端列表”页签中单击“创建后端”。

步骤3 在创建后端页面配置后端信息，完成后单击“立即创建”。后端创建完成后，页面自动跳转到该后端的编辑器页面，后端类型默认为数据后端。

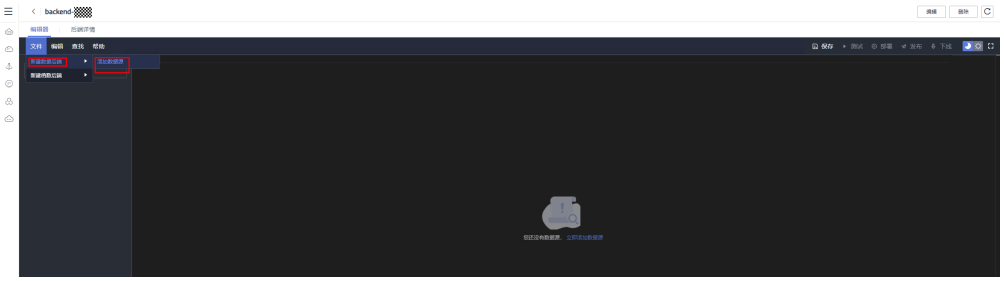
图 3-141 后端创建



步骤4 配置数据后端。

1. 在编辑器页面左侧单击“添加数据源”。

图 3-142 添加数据源



2. 在添加数据源弹窗中配置数据源信息，完成后单击“立即添加”，详细配置请参考**表3-21**。

图 3-143 添加数据源

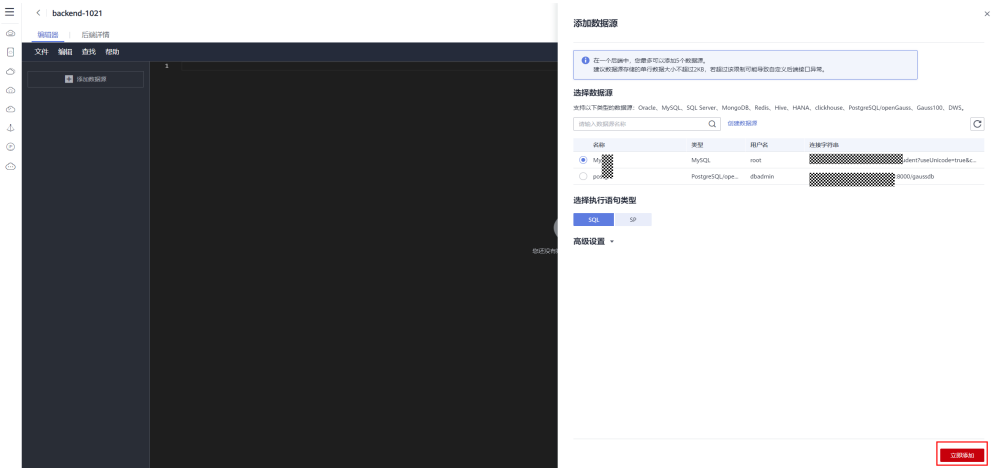
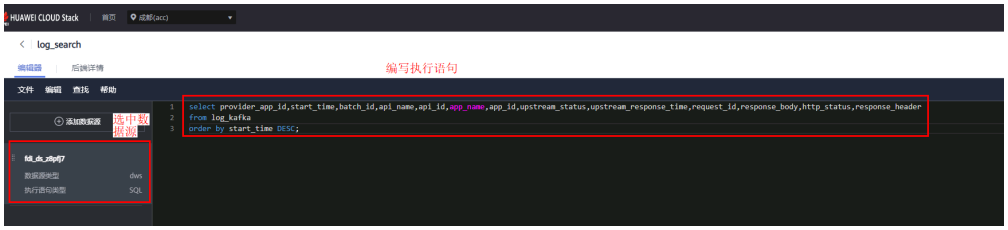


表 3-21 数据源配置

参数	配置说明
选择数据源	选择3.4.2.2 配置数据源中已配置的数据源
选择执行语句类型	选择执行语句的类型，可选择“SQL”和“SP”（Stored Procedure）。如果是Redis或MongoDB数据源，选择“SQL”，实际执行语句为NoSQL。
高级设置	
返回对象	填写返回对象的名称，执行语句的执行结果将封装在该对象中返回。
结果分页选项	执行语句的执行结果是否支持分页返回。若同一个数据后端添加多个数据源时，不支持配置“结果分页选项”。 若开启结果分页选项，可在后端请求中添加查询参数pageNum和pageSize，对查询结果进行分页，并指定返回第几页的数据。 – pageNum：分页时指定要返回第几页的数据，从1开始。 – pageSize：分页时每页包含的数据条数。开启和关闭结果分页选项时，响应结果的结构会有所不同，具体请参见《应用与数据集成平台(ROMA Connect) 1.10.0 使用指南(for 华为云Stack 8.2.1) 02》中结果分页示例说明。 **说明** 结果分页当前仅支持2000条以内数据的分页，若超过2000条数据，建议在执行语句中携带offset和limit参数进行分页。未开启“预编译”时，使用示例如下：select * from table01 limit ${limit} offset${offset}其中offset和limit参数key在后端服务请求的Headers、Parameters或Body中传递。若数据源开启了“预编译”，则还需要调用相应的函数对offset和limit参数进行数据类型转换，具体请参见《应用与数据集成平台(ROMA Connect) 1.10.0 开发指南(for 华为云Stack8.2.1)》的“服务集成开发指导 > 自定义后端开发（数据后端）”章节。
预编译	是否对执行语句进行预编译，可以防止SQL注入风险。

步骤5 添加数据源后，在编辑器左侧选择数据源，然后可以在右侧的语句编辑框中编写执行语句。

图 3-144 选择数据源

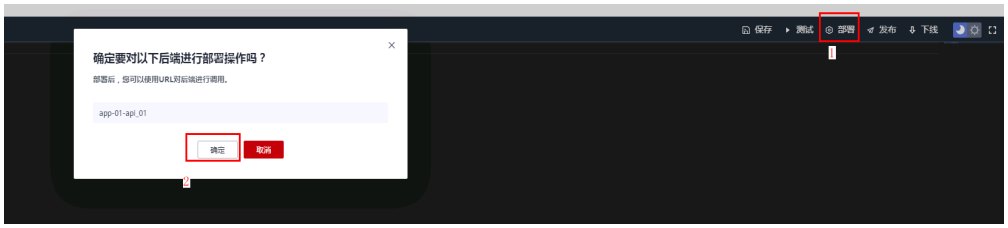


步骤6 测试后端功能。在页面右上角单击“测试”，在下方的“测试参数”处，根据后端的定义添加请求参数，然后单击“立即测试”，发送请求。

- 在“执行结果”处，可查看后端的响应结果。
- 在“执行历史”处，可查看后端的历史测试记录。单击测试记录，可以将历史测试参数导入到左侧测试参数中，并再次测试。

步骤7 后端测试完成后，在页面右上角单击“部署”，在确认弹窗中单击“确定”，部署后端服务。

图 3-145 部署后端



----结束

3.4.2.4 创建函数后端

概述

ROMA Connect支持把自定义函数定义为后端服务，把函数的能力以API的形式对外开放。

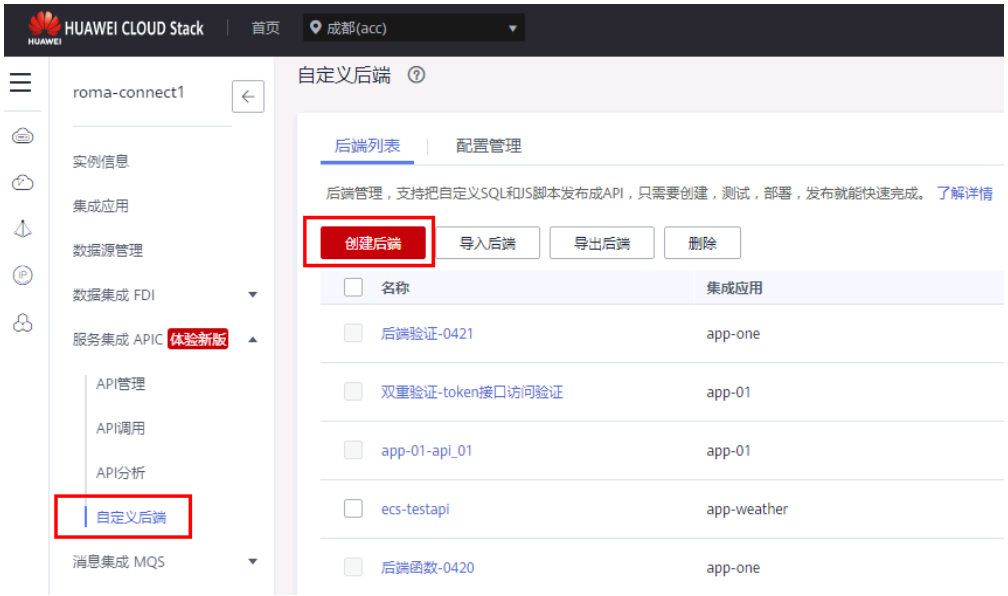
前提条件

如果后端服务需要使用签名密钥请求发送方进行认证，请提前创建签名密钥。

操作步骤

步骤1 ROMA Connect支持把自定义函数定义为后端服务，把函数的能力以**API的形式对外开放**，或使用函数的能力进行**自定义认证**。创建函数后端方式如下图

图 3-146 创建函数后端



步骤2 如果函数作为自定义认证的后端函数，请求方法则必须为post。因为认证的请求会将原访问的headers和parameter等全部放在body内。

图 3-147 编辑后端

参数说明见表3-22

表 3-22 后端配置

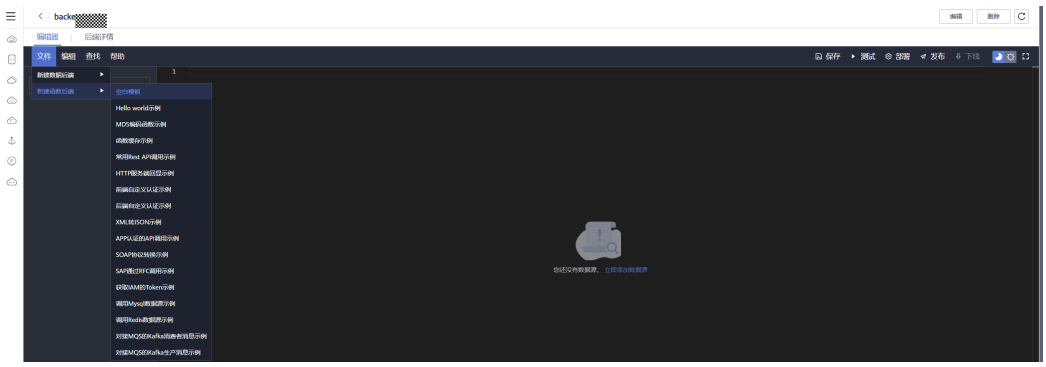
参数	说明
后端名称	填写后端的名称，根据规划自定义。建议您按照一定的命名规则填写后端名称，方便您快速识别和查找。
集成应用	选择后端所属的集成应用。若没有可用的集成应用，可单击右侧的“新建集成应用”，创建一个集成应用。
后端请求方法	选择后端的请求方法，可选择“GET”、“POST”、“PUT”和“DELETE”。
后端请求路径	填写后端的请求路径，格式如：/getUserInfo/userId。 请求路径中的内容区分大小写。若函数后端需要作为API的后端接入，则该路径需要和API路径一致。
后端安全认证	选择后端的安全认证方式。 签名密钥：使用签名密钥对后端请求进行认证。若使用签名密钥进行认证，该后端服务对应的前端API也需要绑定相同的签名密钥。 无认证：不对调用请求进行认证。
描述	填写后端的描述信息。

说明

如果开启了后端安全认证的签名密钥，则访问该后端的API需要绑定对应的签名密钥

步骤3 完成上述参数配置后单击完成，进图函数后端页面，ROMA提供了一些常见的函数后端的模板，可以通过模板快速构建自己需要的函数后端：

图 3-148 构建自己需要的函数后端



步骤4 测试后端功能。在页面右上角单击“测试”，在下方的“测试参数”处，根据后端的定义添加请求参数，然后单击“立即测试”，发送请求。

- 在“执行结果”处，可查看后端的响应结果。
- 在“执行历史”处，可查看后端的历史测试记录。单击测试记录，可以将历史测试参数导入到左侧测试参数中，并再次测试。

步骤5 这里以常见restAPI访问的代码为例，编辑完成单击保存，然后**部署**。只有处于部署状态的后端函数才能被前端API调用，如果需要直接将后端发布为API，可以单击**发布**进行快速自动构建。如果需要手动配置前后端的请参考**操作步骤**。

----结束

3.4.2.5 自定义认证

概述

通过自定义认证，将客户的CA用于API调用的第二重认证。

自定义认证包括前端和后端两种类型：

- 前端自定义认证：指ROMA Connect使用自定义的认证函数，对收到的API请求进行安全认证。
- 后端自定义认证：指API的后端服务使用自定义的认证函数，对来自ROMA Connect转发的后端服务请求进行安全认证。

本章节主要介绍如何创建一个**前端自定义认证**。您需要先创建一个函数后端作为认证函数，并在自定义认证中使用该函数后端作为认证后端。

前提条件

已获取CA认证鉴权接口地址，且打开“实例信息“-->“公网出口“-->“服务集成APIC出口地址“开关。并在防火墙中放开APIC出口地址。

操作步骤

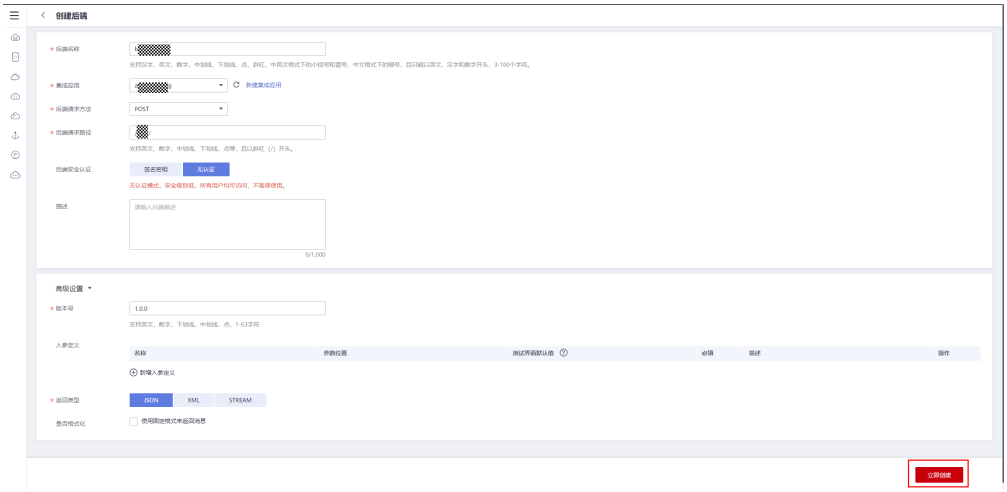
步骤1 登录ROMA Connect控制台，在“实例”页面单击实例上的“查看控制台”，进入实例控制台。

步骤2 在左侧的导航栏选择“服务集成 APIC > 自定义后端”，在“后端列表”页签中单击“创建后端”。

步骤3 在创建后端页面配置后端信息，完成后单击“立即创建”。

- “后端请求方法”必须为“POST”。
- 入参无需设置，用于自定义认证的函数后端会获取API请求中的Header和Query参数。
- 其他参数请参考创建函数后端进行设置。后端创建完成后，页面自动跳转到后端列表页面。

图 3-149 创建后端



步骤4 在后端列表中单击自定义后端的名称，进入后端编辑器页面。

步骤5 在编辑器的左上角单击“文件 > 新建函数后端 > 空白模板”，在弹窗中单击“确定”，然后编写用于安全认证的函数脚本，完成后单击“保存”。

函数后端调用CA接口进行token验证的js脚本示例如下：

```
importClass(com.roma.apic.livedata.client.v1.HttpClient);
importClass(com.roma.apic.livedata.config.v1.HttpConfig);

//CA的token验证接口，入参需要idAccessToken
var address = "http://120.46.162.201:60991/trust-access/id/corporate"
function execute(data) {
 data = JSON.parse(data)
 //自定义验证的函数后端会将请求的headers中的所有参数放在body中，具体路径为data.body.headers[]
 var token = data.body.headers["idaccesstoken"]
 var result = {
    "status": "deny"
 }
 var requestConfig = new HttpConfig();
 requestConfig.setMethod('GET');
 requestConfig.setUrl(address);
 requestConfig.setContent("body");
 requestConfig.setParameter("idaccesstoken",token); //js不区分大小写，请使用全部小写的参数名
 requestConfig.setContentType('application/json');

 var httpClient = new HttpClient();
```

```
 var resp = httpClient.request(requestConfig)

 if (JSON.parse(resp.body().string())["result"]){
     result = {
         "status": "allow",
         "context": {
             "token": token,
          }
      }
   }
   return result
}
```

从data中获取访问令牌后，将访问令牌放在请求头headers中的idAccessToken中，对CA的token验证接口进行访问。

```
当id_access_token值校验通过后会返回：
{
"msg": "成功",
"result": True,
"code": 0
}
当id_access_token为其他值时就会返回：
{
"msg": "失败",
"result": False,
"code": 1
}
```

说明

注意原请求的headers和param都被ROMA放在了函数后端的body中，token的取出方式请参考上述代码中的路径。

函数脚本定义的响应消息：

响应消息体不能大于1M，响应内容必须满足如下格式：

```
{
 "status": "allow/deny",
 "context": {
 "user": "abc"
 }
}
```

- status：必选字段，用于标识认证结果。只支持“allow”或“deny”，“allow”表示认证成功，“deny”表示认证失败。
- context：必选字段，为认证的响应结果。只支持字符串类型键值对，键值不支持JSON对象或数组。

context中的数据为您自定义的字段，认证通过后可作为系统参数（前端认证参数）映射到API的后端服务请求参数中。其中API后端服务中填写的“系统参数名称”与context中的参数名称必须完全一致，且区分大小写。context中的参数名称必须以英文字母开头，支持英文大小写字母、数字、下划线和中划线，且长度为1-32个字符。

步骤6 测试函数后端的功能。

在页面右上角单击“测试”，在下方的“测试参数”处，根据函数后端中的脚本定义，增加认证所需的请求参数，然后单击“立即测试”，发送请求。当测试结果返回的status值为“allow”时，表示测试成功。“测试参数”处填写的是后端请求参数，Header、Query和Body认证参数均需要填写在后端请求的Body参数中，以步骤**步骤5**的脚本示例为例，各认证参数的填写示例如下：

```
{
   "headers":
```

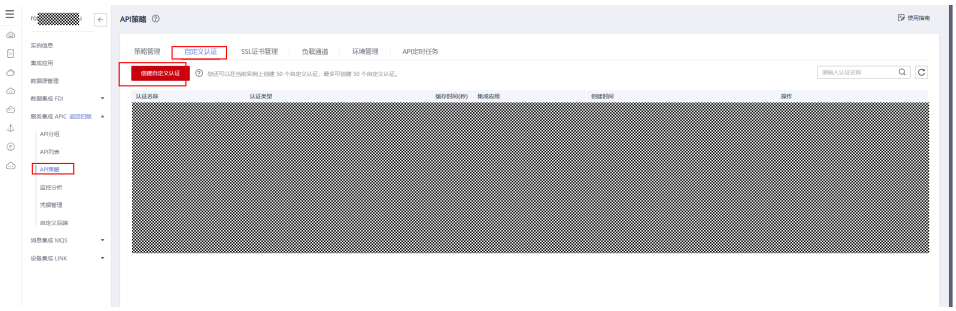
```
  {
    "idaccesstoken":"huawei@123"
  }
}
```

步骤7 部署函数后端：后端测试完成后，在页面右上角单击“部署”，在确认弹窗中单击“确定”，部署函数后端。

步骤8 创建自定义认证：

- 在实例控制台左侧的导航栏选择“服务集成 APIC > API策略”，在“自定义认证”页签下单击“创建自定义认证”。

图 3-150 创建自定义认证

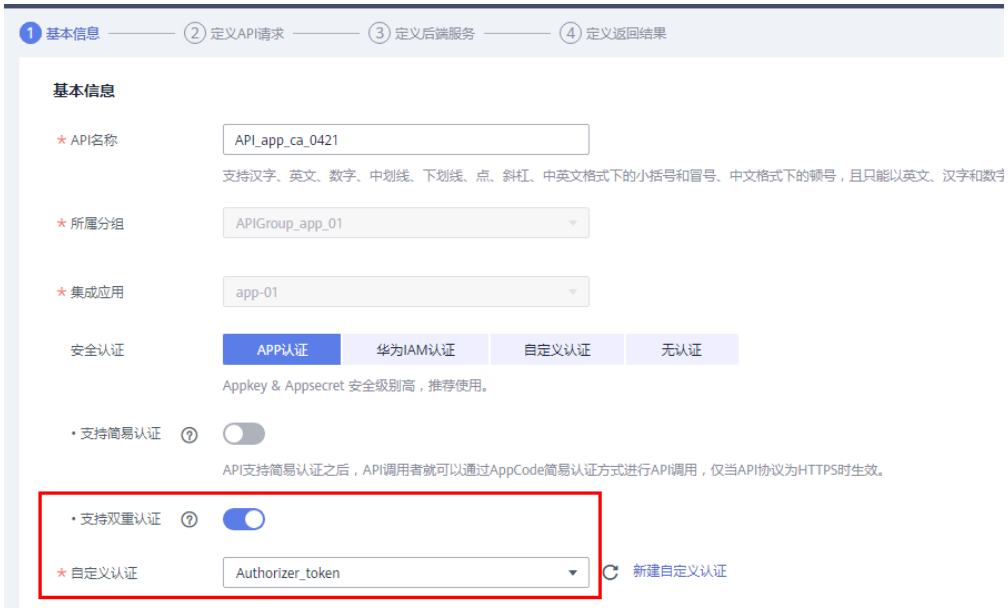


- 在创建自定义认证弹窗中配置后端自定义认证信息，完成后单击“确定”。

图 3-151 确定

步骤9 为API绑定自定义认证：启用第三方CA的验证需要在创建API时开启双重认证，或编辑API开启支持双重认证。选择以上步骤创建的自定义认证。

图 3-152 API 绑定自定义认证



----结束

3.4.2.6 创建 API

概述

通过创建API，把已有后端服务封装成标准的RESTful API，并开放给数据需求方使用。

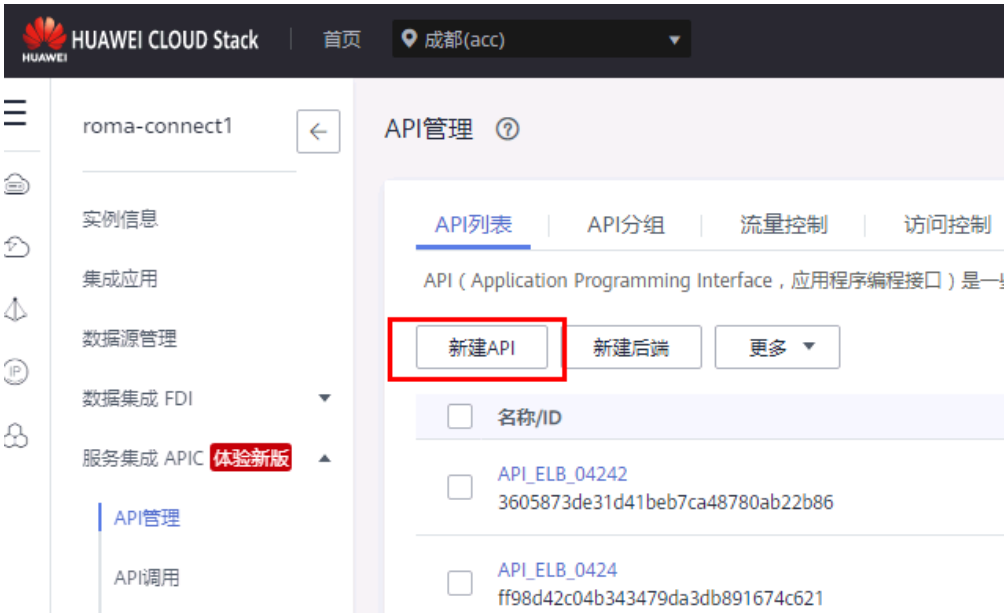
前提条件

1. 每个API都要归属到某个集成应用下，在创建API前您需要**有可用的集成应用**，否则请提前创建集成应用。
2. 每个API都要归属到某个API分组下，在创建API前您需要**有可用的API分组**，否则请提前创建API分组。
3. 如果需要使用负载通道访问后端服务所在的服务器，请提前创建负载通道。
4. 在创建API前，请确保ROMA Connect实例与您的后端服务所在网络互通。请参考**环境准备**中的配置。

操作步骤

步骤1 完成后端和自定义认证的创建后，需要新建API并将API绑定对应的后端和自定义认证，单击服务集成API-->API管理-->新建API。

图 3-153 新建 API



步骤2 进入创建API界面，分为如下四步。

图 3-154 创建 API 界面

步骤3 基本信息，选择认证方式为APP认证，将**表3-23**中创建的自定义认证选中，单击下一步。

图 3-155 基本信息配置

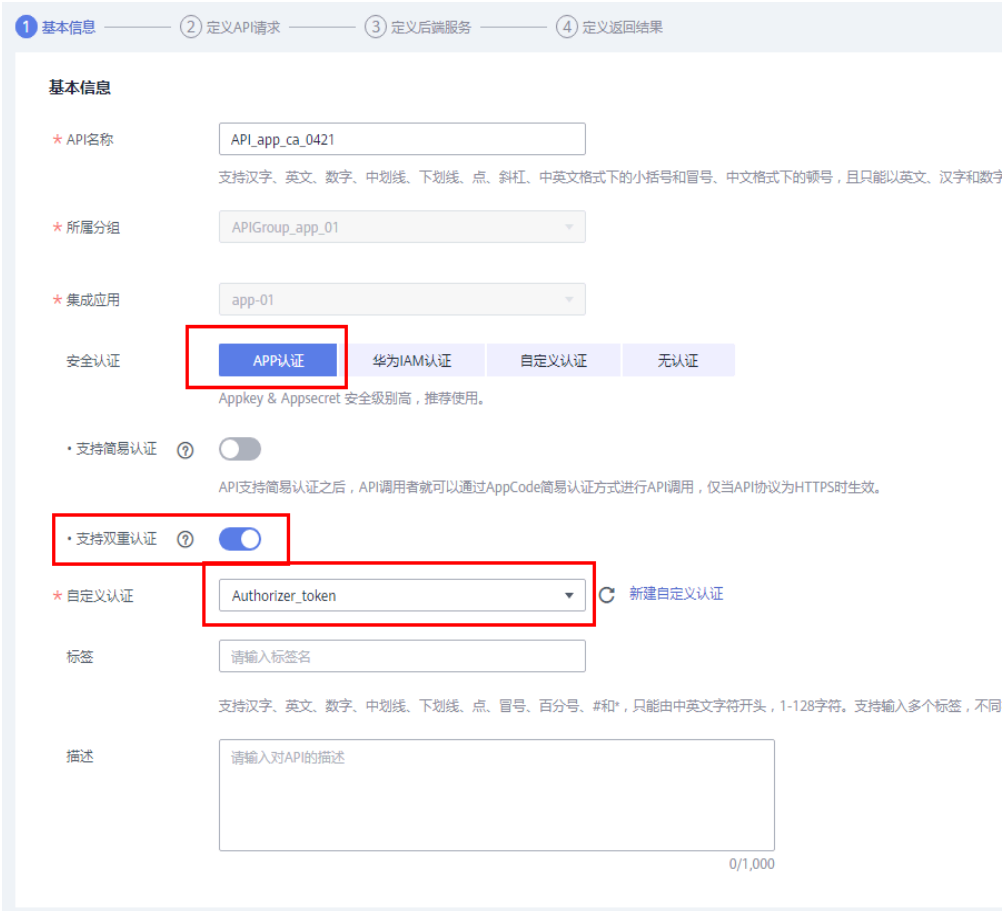


表 3-23 基本信息配置

参数	说明
API名称	填写API的名称，根据规划自定义。建议您按照一定的命名规则填写API名称，方便您快速识别和查找。
所属分组	选择API所属的API分组。若没有可用的API分组，可单击右侧的“新建分组”，创建一个API分组。
集成应用	**仅当“所属分组”选择全局类型分组时可配置。** 选择API所属的集成应用。若没有可用的集成应用，可单击右侧的“新建集成应用”，创建一个集成应用。

参数	说明
安全认证	选择API的安全认证方式，推荐使用APP认证方式。 • APP认证：表示由ROMA Connect对API请求进行安全认证。用户调用API时，使用授权集成应用的Key和Secret进行API请求的安全认证。使用该方式的API适合所有用户调用。 • 华为IAM认证：表示由IAM对API请求进行安全认证。用户调用API时，使用Token或AK/SK进行API请求的安全认证。使用该方式的API仅适合同一云服务平台的用户调用。 • 自定义认证：表示使用自定义的函数API对API请求进行安全认证。使用该方式的API适合所有用户调用。 • 无认证：表示API请求不需要认证。使用该方式的API适合所有用户调用。
支持简易认证	**仅当“安全认证”选择“APP认证”时可配置。** 是否对API的调用使用简易安全认证，仅当API请求协议为HTTPS时生效。若选择启用，则用户调用API时携带AppCode进行安全认证，无需对API请求进行签名校验。
支持双重认证	**仅当“安全认证”选择“APP认证”或“华为IAM认证”时可配置。** 是否对API的调用进行双重安全认证。若选择启用，则在使用APP认证或IAM认证对API请求进行安全认证时，同时使用自定义的函数API对API请求进行安全认证。
自定义认证	**仅当“安全认证”选择“APP认证”或“华为IAM认证”且“支持双重认证”开启时，或者“安全认证”选择“自定义认证”时需要配置。** 选择已创建的前端类型自定义认证。若没有可用的自定义认证，可单击右侧的“新建自定义认证”，创建一个前端类型的自定义认证。
标签	添加API的标签信息，用于快速过滤和查找API。
描述	填写API的描述信息。
请求体内容描述	**仅当“Method”选择“POST”、“PUT”、“PATCH”或“ANY”时可配置。** 填写API请求中请求体的描述信息，用于帮助API调用者理解如何正确封装API请求。

步骤4 定义API请求路径，并建议选择HTTPS，并设定API的请求方式GET、POST、PUT等。详细信息见**表3-24**

图 3-156 定义 API 请求路径

表 3-24 API 请求配置

参数	配置说明
请求协议	选择API使用的请求协议，可选择“HTTP”、“HTTPS”和“HTTP&HTTPS”，传输重要或敏感数据时推荐使用HTTPS。
请求Path	填写API的请求路径，格式如：/getUserInfo/{userId}。请求路径中可包含Path参数，以{参数名}形式表示。 • Path参数应匹配"/"之间的一整段，不支持匹配"/"之间的一部分，例如不支持/abc{userId}。若匹配模式为准确匹配，则尾部的Path参数可以添加+号，例如/users/{p+}，其中变量p匹配一或多段"/"之间的部分。 • 请求路径中包含Path参数时，必须配置对应的入参定义。 • 请求路径中的内容区分大小写。

参数	配置说明
匹配模式	选择API请求路径的匹配模式。 ● 准确匹配：API请求中的请求路径要与“请求Path”的配置一致。 ● 前缀匹配：API请求中的请求路径要以“请求Path”的配置为前缀。例如，“请求Path”为“/test/AA”，使用前缀匹配时，通过/test/AA/BB和/test/AA/CC都可以访问API，但是通过/test/AACC无法访问。 **说明** 使用前缀匹配时，匹配剩余的请求路径将透传到后端服务。例如，“请求Path”为“/test”，“后端请求Path”为“/test2”，使用前缀匹配时，通过/test/AA/CC访问API，后端服务收到的请求路径为/test2/AA/CC。
Method	选择API的请求方法。“ANY”表示该API支持任意请求方法。
支持CORS	是否支持跨域访问API。 浏览器出于安全性考虑，限制从页面脚本内发起的跨域请求，此时页面只能访问同源的资源。而CORS允许浏览器向跨域服务器发送XMLHttpRequest请求，从而实现跨域访问。跨域访问API请参见配置跨域访问API。

参数	配置说明
入参定义（可选）	根据实际需要定义API的请求参数。请求路径中包含请求参数时，必须配置对应的入参定义。 在“入参定义”下单击“添加入参定义”，添加API的请求参数。 ● 参数名：请求参数的名称。参数位置为“PATH”时，参数名需要与“请求Path”中的参数名称一致。 ● 参数位置：请求参数在API请求中的位置，可选择“PATH”、“HEADER”和“QUERY”。 ● 类型：选择请求参数的数据类型，可选择“STRING”和“NUMBER”。 ● 必填：在API请求中，请求参数是否必填。 ● 透传：请求参数是否透传到后端服务。 ● 默认值：仅当“必填”为“否”时可配置请求参数的默认值。 ● 枚举：请求参数的枚举值，请求参数的值只能从枚举值中选择，多个枚举值间用英文逗号隔开。 ● 最大长度/最大值：“类型”为“STRING”时，设置参数值的最大字符串长度，“类型”为“NUMBER”时，设置参数值的最大值。 ● 最小长度/最小值：“类型”为“STRING”时，设置参数值的最小字符串长度，“类型”为“NUMBER”时，设置参数值的最小值。 最小长度/最小值和最大长度/最大值同时设置成0时，表示不做限制。 ● 示例：请求参数值的填写示例。 ● 描述：请求参数的描述信息。 ● 参数名不能以x-apig- 、x-sdk-开头，不能是x-stage，不区分大小写。 ● 参数位置为HEADER时，参数名不能是Authorization和X-Auth-Token，不区分大小写。
请求体内容描述	**仅当“Method”选择“POST”、“PUT”、“PATCH”或“ANY”时可配置。** 填写API请求中请求体的描述信息，用于帮助API调用者理解如何正确封装API请求。

步骤5 定义后端服务，后端服务地址和后端请求Path路径可在对应函数后端的请求地址中获取。

图 3-157 定义后端服务

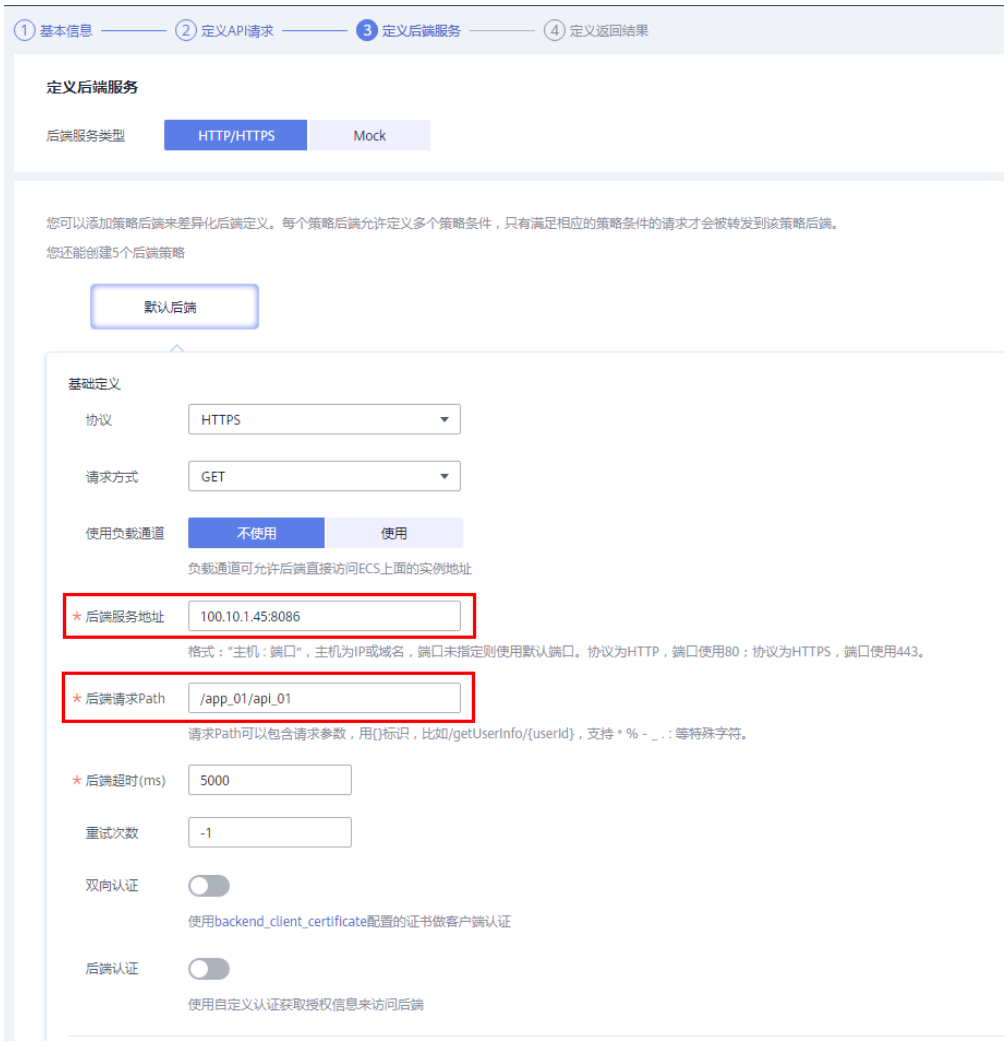
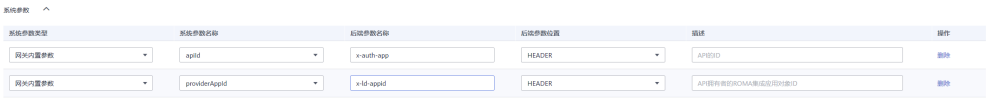


图 3-158 创建后端

另需要添加两个系统参数到后端参数中，x-auth-app和x-ld-appid，如下图：

图 3-159 添加两个系统参数



步骤6 返回结果基础定义，完成API创建，单击发布API，选择发布环境。

图 3-160 返回结果基础定义

图 3-161 单击发布 API

步骤7 如果后端函数开启了签名认证，则API还需要绑定对应的签名证书。每个API只能绑定一个签名密钥。绑定方法如下图：

图 3-162 API 管理

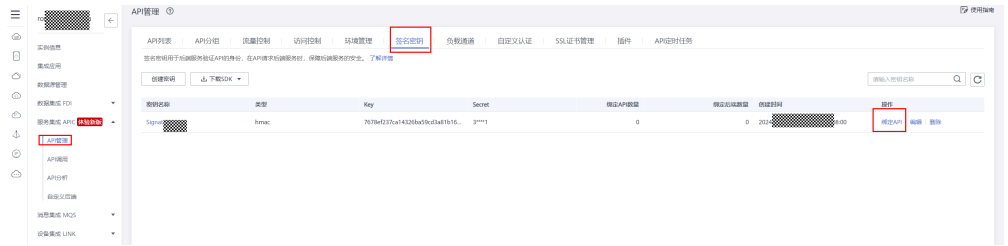


图 3-163 绑定 API

步骤8 若需要为特定客户端提供API访问权限，请参考**应用和客户端的准备**对客户端进行授权。

----结束

3.4.2.7 API 调试

概述

在API创建后，您可以使用ROMA Connect提供的调试功能对API进行调试，确保API的功能正常。

前提条件

1. 后端服务请求路径中含有环境变量的API不支持调试。
2. 在调试API时，API绑定流控策略无效。
3. 若定义API后端服务时配置的“后端超时(ms)”与“重试次数”相乘的值大于30秒，则调试API会超时。

操作步骤

步骤1 登录ROMA Connect控制台，在“实例”页面单击实例上的“查看控制台”，进入实例控制台。

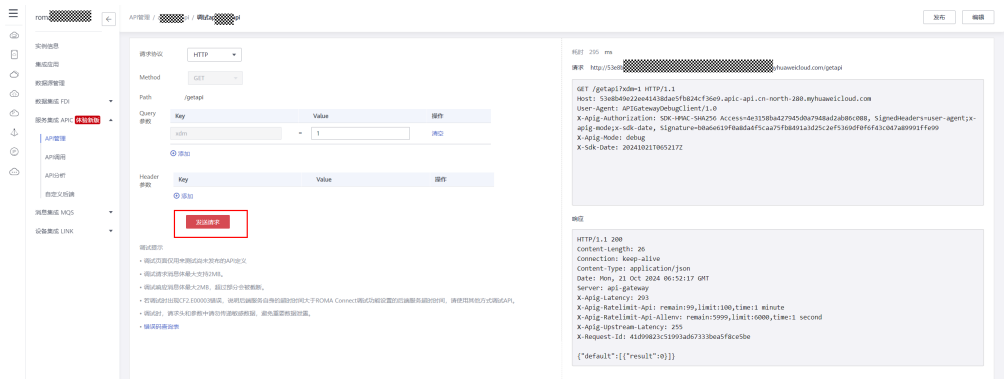
步骤2 在左侧的导航栏选择“服务集成 APIC > API管理”，在“API列表”页签中单击API右侧的“更多 > 调试”。

步骤3 在调试页面中，左侧为API请求参数配置区域，根据API的定义配置API的请求信息。

图 3-164 定义配置 API

如下图，根据接口的要求，填写请求的参数和请求头。其中请求头不需要携带key/secret，如果采用postman等第三方调试工具，则请求头还需要加入应用的key和secret。详细请参考**访问客户端**。

图 3-165 填写请求的参数和请求头



----结束

3.4.2.8 发布 API

概述

在API创建后，您需要把API发布到环境，API只有在发布到环境后，才支持被其他用户调用。

前提条件

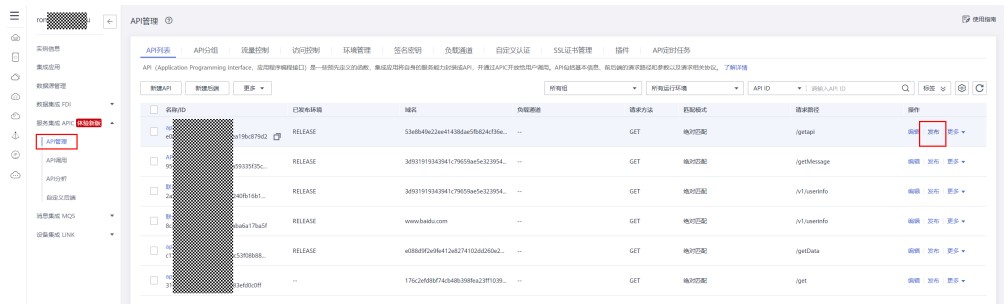
系统已提供了默认发布环境RELESE，如果您需要把API发布到其他环境，请提前创建发布环境。

操作步骤

步骤1 登录ROMA Connect控制台，在“实例”页面单击实例上的“查看控制台”，进入实例控制台。

步骤2 在左侧的导航栏选择“服务集成 APIC > API列表”，在页面中单击API右侧的“发布”。

图 3-166 发布



步骤3 在发布API页面中配置发布信息，完成后单击“发布”。

----结束

3.4.3 数据需求方可信访问验证

概述：数据开发利用方将API在发布到环境后，支持被授予权限的数据需求方用户调用。调用过程请参考可信接入流程。

前提：在调用API前，确保数据需求方所在网络与API的访问域名或地址互通。

- 若数据需求方与ROMA Connect实例在相同VPC内时，可直接访问API。
- 若数据需求方与ROMA Connect实例在同一区域的不同VPC内时，可通过**创建VPC对等连接**，将两个VPC的网络打通，实现同一区域跨VPC访问API。
- 若数据需求方与ROMA Connect实例在不同区域的不同VPC内时，可通过**创建云连接实例**并加载需要互通的VPC，将两个VPC的网络打通，实现跨区域跨VPC访问API。
- 若数据需求方与ROMA Connect实例通过公网互通，请确保ROMA Connect实例已绑定弹性IP，且弹性IP与公网互通。

对于API的高并发业务场景，建议使用“铂金版X8-服务集成”规格的实例，并为APIC开启外置ELB。

可信应用注册

- 概述：数据需求方需要通过可信访问代理（SDK）的【可信应用注册】接口，向可信访问平台进行应用注册，成为可信应用。
- 前提条件：数据需求方首先需要根据应用开发语言类型，向CA线下提交可信应用接入申请表，申请通过后CA向应用方返回appID、appSecret、SDK软件包。本操作文档不包该流程，请联系相关人员进行申请。
- 接口规范

  接口描述：数据需求方通过SDK对应用进行可信注册，接口调用成功后会在本地生成应用签名证书。签名证书会在后续CA接口调用中用于请求签名。

表 3-25 请求参数

参数名称	类型	必选	参数说明
appID	string	是	应用id，由可信访问平台分配
appSecret	string	是	应用密钥，由可信访问平台分配
corpName	string	是	单位名称
corpCode	string	是	统一社会信用代码

表 3-26 响应参数

参数名称	类型	必选	参数说明
code	int	是	返回码，0表示成功
msg	string	是	返回消息，多用于描述失败时的错误信息

从 CA 申领可信访问令牌

- 概述：数据需求方需要调用可信访问代理（SDK）的【申领法人可信访问令牌】接口，向可信访问平台申领可信访问令牌。
- 前提条件：完成可信应用注册。
- 接口规范：法人用户进行身份认证后，数据需求方调用该SDK接口申领可信访问令牌。可信访问令牌默认有效期为5分钟，数据需求方需要在失效后重新申请新的可信访问令牌。

表 3-27 请求参数

参数名称	类型	必选	参数说明
transactionId	string	是	业务流水号
authType	string	是	认证方式，取值范围为{1：法人四要素；2：对公打款；3：数字证书；4：电子营业执照；5：二维码}
corpName	string	是	单位名称，认证方式为1-4时该项必填
corpCode	string	是	统一社会信用代码，认证方式为1-4时该项必填
qrCode	string	否	二维码码值，认证方式为5时该项必填
location	string	否	设备地理位置
permission	string	否	访问授权凭证，格式为{授权方:授权码} 调用第三方授权服务获取授权码，授权方为TP。

表 3-28 响应参数

参数名称	类型	必选	参数说明
code	int	是	返回码，0表示成功
msg	string	是	返回消息，多用于描述失败时的错误信息
data	string	是	可信访问令牌

数据服务公共认证部分

概述：参考可信接入流程中的数据服务访问流程，数据需求方调用运营平台已申请订阅的数据服务接口，按照本章节要求，在请求头部携带由可信访问平台分配的可信访

问令牌和从数据集团获取的X-HW-ID/X-HW-AppKey，进行数据需求方身份和访问权限的校验。

前提条件

- 数据开发方已完成服务API的开发，并开放API。
- 数据需求方已完成可信注册并获取访问令牌。

认证规范

- 接口路径示例：https://ROMA Connect地址或域名:端口 /数据服务URL路径
- 调用方法：GET、POST
- 接口协议：接口统一采用Restful协议，请求和响应体采用标准JSON结构
- 接口描述：数据需求方调用数据服务API所需要的公共认证参数和认证失败的响应。
- 请求头部公共参数

表 3-29 请求头部公共参数

参数名称	类型	必选	参数说明
X-HW-ID	string	是	从数据集团获取的X-HW-ID
X-HW-AppKey	string	是	从数据集团获取的X-HW-AppKey
idAccessToken	string	是	可信访问平台分配的法人可信访问令牌

表 3-30 认证失败响应参数

参数名称	类型	必选	参数说明
error_code	string	是	返回码，用于表示错误类型
error_msg	string	是	返回消息，多用于描述失败时的错误信息
request_id	string	是	此次请求的ID，用于问题定位

调用示例

GET: https://ROMA Connect地址或域名:端口/xxxx?id=xxxx HTTP/1.1

消息头：

```
Content-Type: application/json;charset=UTF8
Accept: application/json
X-HW-ID: xxxx
X-HW-AppKey: xxxx
idAccessToken: xxxx
```

认证失败响应示例：

```
{
"error_code" : "APIC.0303",
"error_msg" : "Incorrect app authentication information:xxx",
" request_id" : "c77f5e81d9cb4424bf704ef2b0ac7601",
}
```

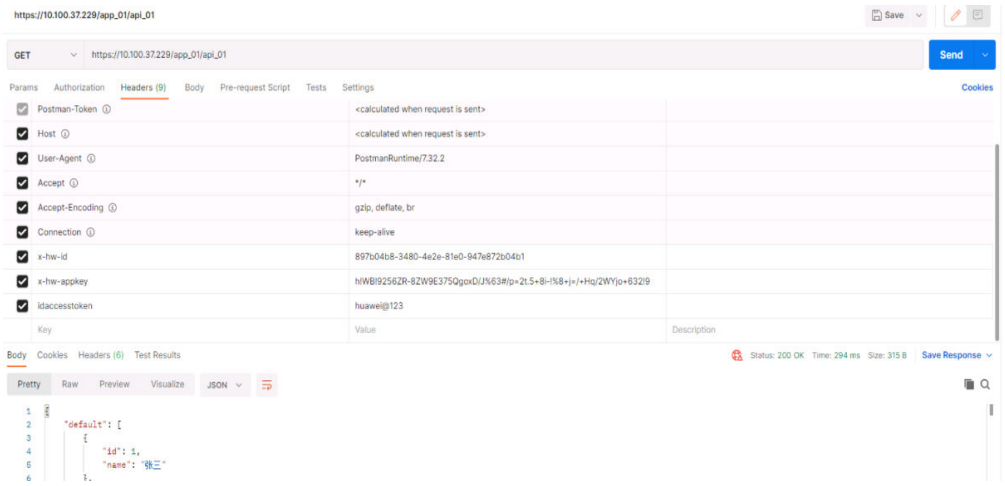
认证成功时响应实际数据结果，以各个数据服务接口响应内容为准。

访问客户端

1. 通过在内网使用ip访问api

   【示例】通过postman调用接口，接口uri：https://10.100.37.229/app_01/api_01

   图 3-167 内网使用 ip 访问 api

   - x-hw-id：被授权的集成应用的key
   - x-hw-appkey：被授权的集成应用的secret，与x-hw-id完成ROMA的app认证
   - idaccesstoken：模拟自定义认证过程中接口请求携带的CA下发的token，用于请求在通过app认证后，将该值传递至前端认证中的后端函数中，通过接口请求的方式向公网搭建的CA认证本次请求是否可信

   说明

   访问https的接口需要将postman的设置中的SSL certificate verification关闭!

   图 3-168 设置

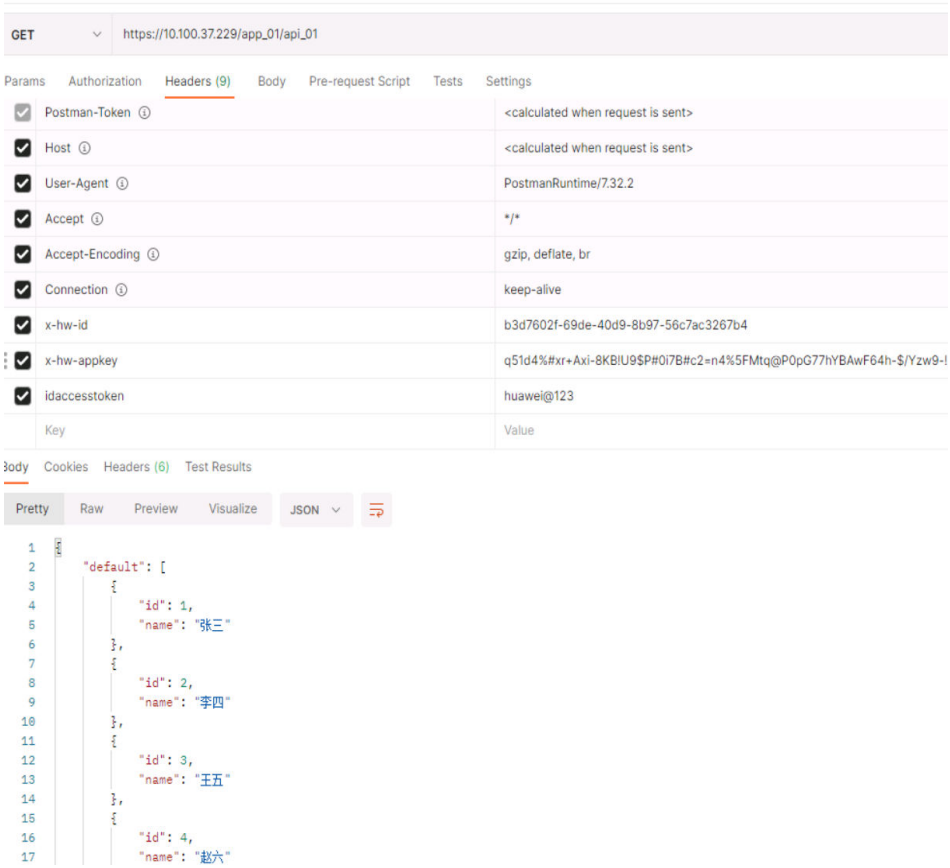
2. 前端认证中的后端函数中访问的CA，为搭建在云服务器上的模拟CA工作的web服务，该服务主要实现为：当请求模拟CA的idaccesstoken为huawei@123时，模拟CA返回true，当idaccesstoken为其他值时，返回false，从而实现模拟认证通过和失败。

图 3-169 访问客户端

```
@app.route('/trust-access/id/corporate', method='GET')
def post_handler():
    data = request.query.idaccesstoken
    logging.error(data)
    response.status = 200
    tmp = "huawei@123"
    reTrue = {
        "msg": "成功",
        "result": True,
        "code": 0
    }
    reFalse = {
        "msg": "失败",
        "result": False,
        "code": 1
    }
    if data == tmp:
        return reTrue
    else:
        return reFalse
```

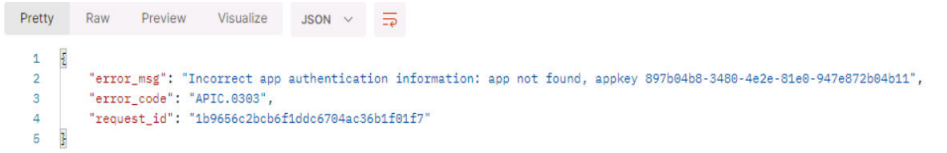
– x-hw-id、x-hw-appkey、idaccesstoken均符合要求，访问结果如下：

图 3-170 访问结果 1



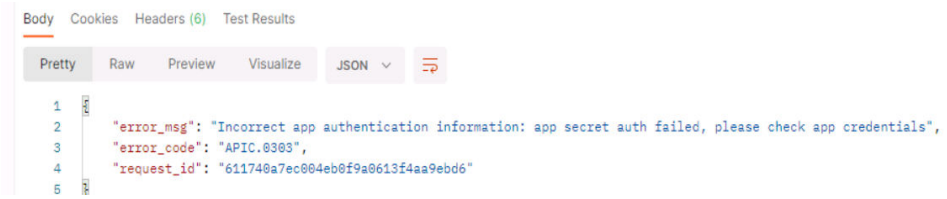
- x-hw-id不符合要求时，访问结果如下：

图 3-171 访问结果 2



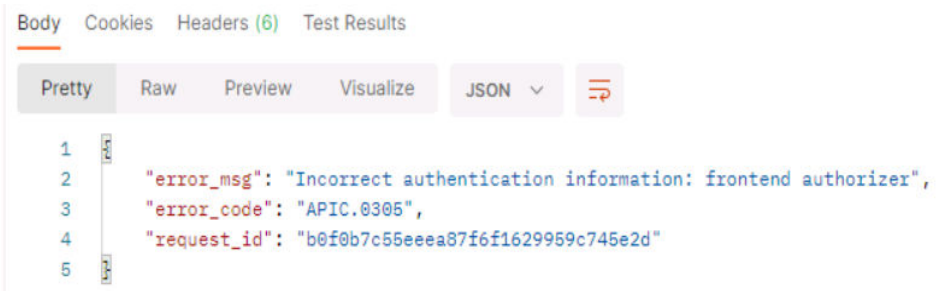
- x-hw-appkey不符合要求时，访问结果如下：

图 3-172 访问结果 3



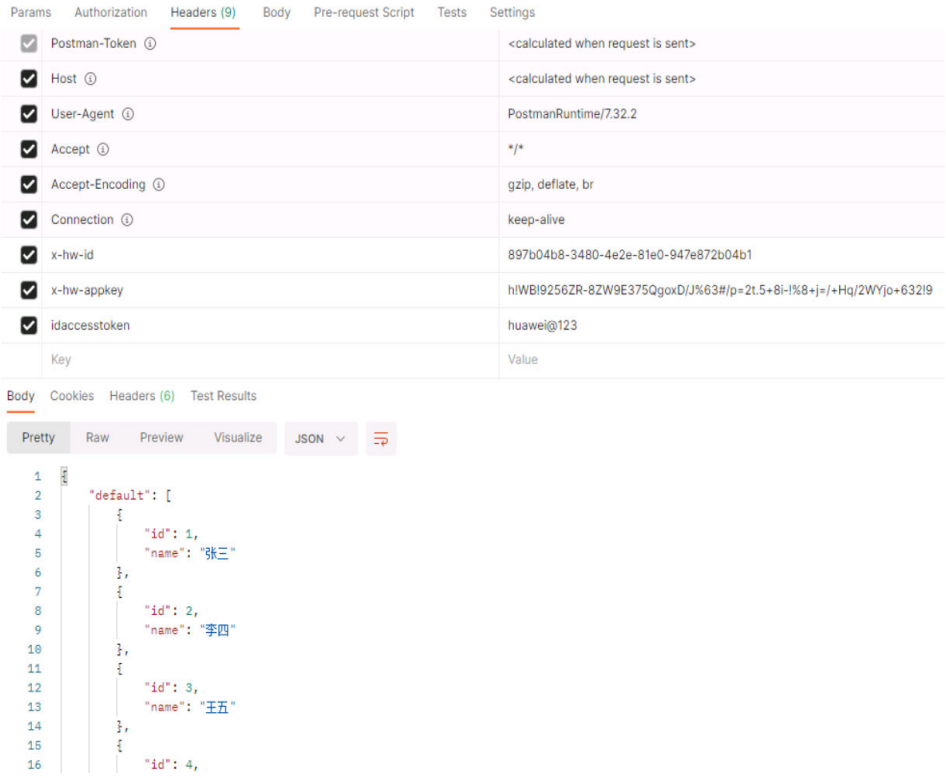
- idaccesstoken不符合要求时，访问结果如下：

图 3-173 访问结果 4



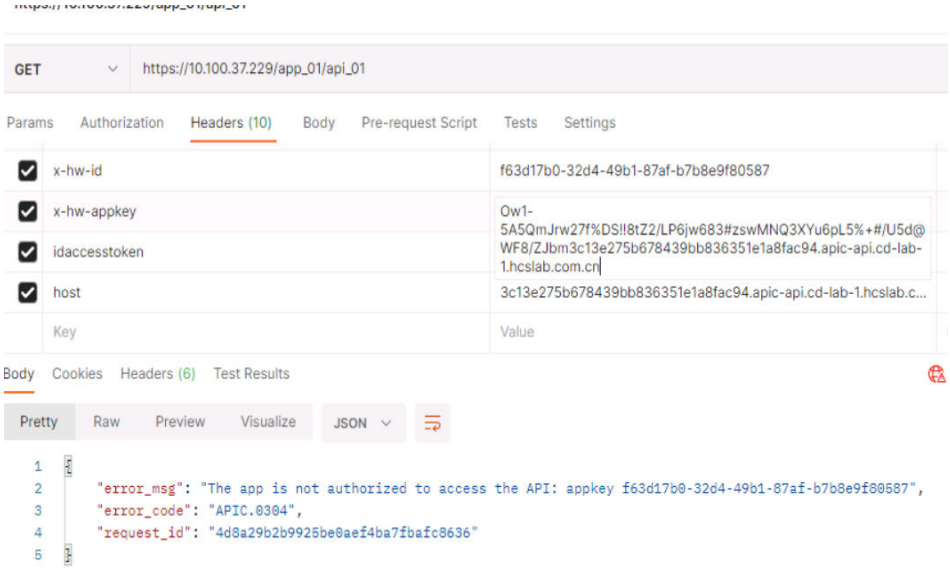
- 当使用的x-hw-id、x-hw-appkey为api授权的其它集成应用的key和secret时，访问结果如下：

图 3-174 访问结果 5



- 当使用的x-hw-id、x-hw-appkey为api未授权的其它集成应用或客户端的key和secret时，访问结果如下：

图 3-175 访问结果 6



3.5 场景五：数据需求方数据服务计量

3.5.1 将 API 计量信息推送至 MQS

3.5.1.1 创建日志消息队列所属的集成应用

概述

ROMA Connect通过**集成应用**来实现同一实例内不同用户间的资源隔离。用户在ROMA Connect实例中创建的资源（如数据源、API、Topic、产品等）都要有归属的集成应用，非管理员权限的用户默认只能查看和管理自己创建的集成应用和资源，无法查看其他用户创建的集成应用和资源，管理员权限的用户可查看和管理其下所有用户所创建的资源。

前提条件

运营管理员已获取需要创建的集成应用的清单，集成应用对应数据开发利用方，客户端对应数据需求方。其中客户端为空白集成应用，命名建议使用前缀区分。

操作步骤

ROMA Connect实例中的资源都要归属到某个集成应用下，在创建其他资源前，您需要确保有一个集成应用。若已有可用的集成应用，可跳过此步骤。

- 登录ROMA Connect控制台，在“实例”页面单击实例上的“查看控制台”，进入实例控制台。
- 在左侧的导航栏选择“集成应用”，单击页面右上角的“创建集成应用”。
- 在创建集成应用弹窗中填写集成应用的“名称”，然后单击“确认”。这里以“app-API_log”为应用名称。

图 3-176 创建集成应用

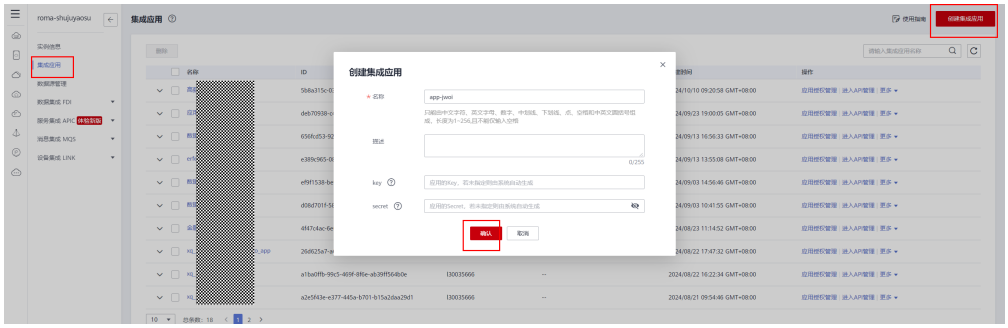


表 3-31 创建应用

参数	配置说明
名称	自定义应用名称。 这里以“app-API_log”为应用名称。
描述	填写对该应用的描述内容，选填项。
Key	集成应用的Key，若未指定则由系统自动生成。
Secret	集成应用的Secret，若未指定则由系统自动生成。

3.5.1.2 创建 MQS Topic

概述

创建用于存储消息的Topic，供消息生产方发布消息和供消息消费方订阅消息。

前提条件

每个Topic都要归属到某个集成应用下，在创建Topic前您需要有可用的集成应用，否则请提前创建集成应用。

操作步骤

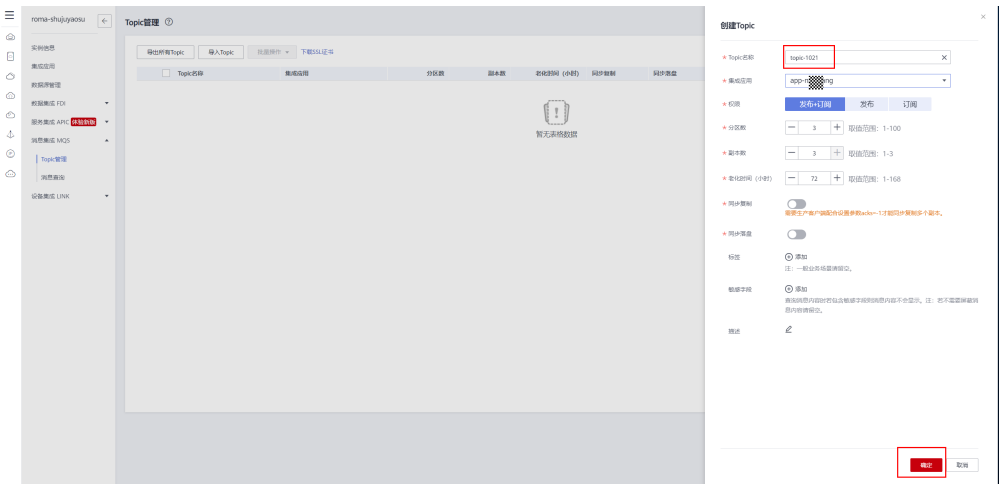
步骤1 登录ROMA Connect控制台，在“实例”页面单击实例上的“查看控制台”，进入实例控制台。

步骤2 在左侧的导航栏选择“消息集成 MQS > Topic管理”，单击页面右上角的“创建Topic”。

图 3-177 创建 Topic

步骤3 在创建Topic弹窗中配置Topic相关信息，完成后单击“确定”。

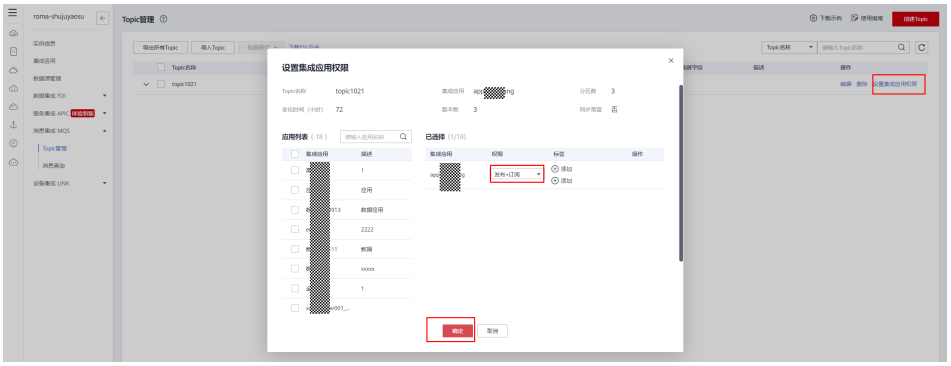
图 3-178 确定



步骤4 为集成应用设置权限：

1. 需要推送API日志的集成应用和MQS所属集成应用，为其添加发布权限。
2. 需要订阅MQS的数据连接的集成应用，为期添加订阅权限。

图 3-179 集成应用设置权限



3. 本示例中“app-api_log”既是MQS所属应用也是DWS连接所属应用，因此需要为期添加发布+订阅权限

说明

若无发布权限则无法发布消息到MQS，若无订阅权限，FDI任务将会提示目标端异常。

----结束

3.5.1.3 创建 Kafka 日志推送插件

概述

ROMA Connect支持收集服务集成下已开放API的调用日志信息。Kafka日志推送插件提供了把API的详细调用日志推送到Kafka的能力，方便用户获取API的调用日志信息。

使用限制

- 同一个ROMA Connect实例内最多可创建5个Kafka日志推送插件，推荐使用全局可见的kafka推送日志，一个日志插件推送所有的API调用日志信息，配置方式见**3.5.1.3.1 创建插件**。
- 推送的日志信息中，响应数据暂不支持Transfer Encoding响应头参数。
- Kafka日志插件默认的响应体和请求体的大小为1000B，该数值最大支持4K，修改该参数请参考**3.5.1.3.5 修改请求体和响应体默认大小**。

说明

Transfer-Encoding 响应头用于告诉客户端服务器发送内容的编码格式，**建议开发规范中禁止使用该参数。**

其可选值有：

- chunked：数据分块发送。此时应缺省 Content-Length 响应头。
- compress：使用 **Lempel-Ziv-Welch** 算法进行传输的格式，目前没有浏览器在支持。
- deflate：使用 **deflate** 压缩算法 **zlib** 结构。
- gzip：使用 **Lempel-Ziv coding** 编码的压缩格式。
- identity：标识身份函数（e.g. no compression, nor modification）。

也可以同时指定多个值，用逗号分隔，像这样：Transfer-Encoding: gzip, chunked。

3.5.1.3.1 创建插件

步骤1 登录ROMA Connect控制台，在“实例”页面单击实例上的“查看控制台”，进入实例控制台。

步骤2 在左侧的导航栏选择“服务集成APIC > API管理 > 插件”，单击页面左侧的“创建插件”。

图 3-180 创建插件

步骤3 在创建插件页面填写相关参数：

- 插件名称以“Plugin_API_log”为示例，插件类型选择“Kafka日志推送”。
- 可见范围推荐使用“全局”，因此该插件可用于所有集成应用下的API。
- 插件内容选择“表单配置”

图 3-181 表单配置

----结束

3.5.1.3.2 策略基本信息

配置说明请参考**表3-32**。

表 3-32 策略基本信息

参数	配置说明
策略基本信息	
Broker地址	日志要推送的目标Kafka连接地址列表，多个地址间以英文逗号（,）隔开。
Topic主题	日志要推送的目标Kafka Topic名称。
Key	填写消息的Key值，表示消息存储在Kafka的指定分区，可以当成有序消息队列使用。如果Key为空，则消息分布式存储在不同的消息分区。
失败重试配置	日志推送到Kafka失败后的重试配置。 ● 重试次数：失败后的重试次数，范围为0-5次。 ● 重试间隔：失败后的重试时间间隔，范围为1-10秒。

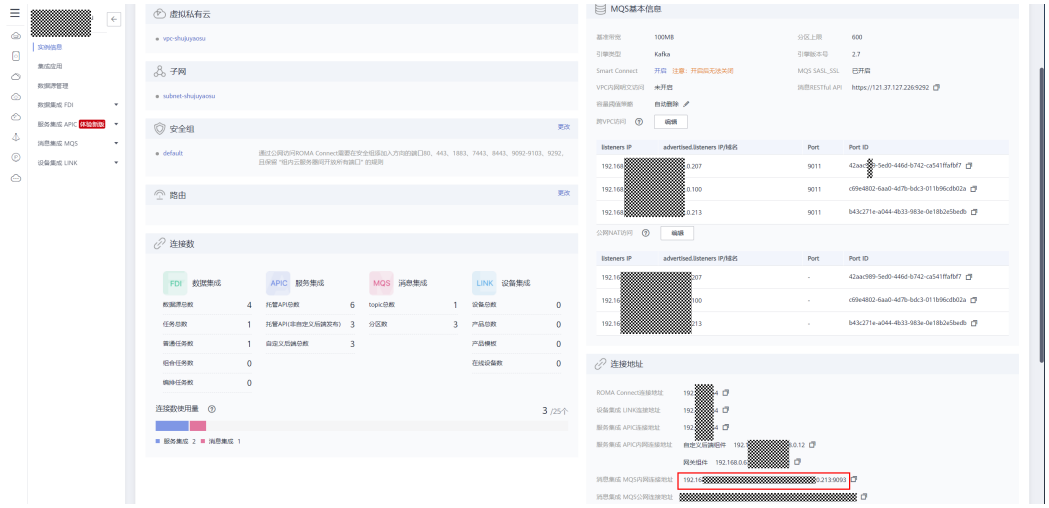
示例

配置填写详细说明：

图 3-182 填写详细说明

Broker地址：进入实例控制台，单击“实例信息”，复制“连接地址”中的“消息集成MQS内网连接地址”。

图 3-183 Broker 地址



Topic主题：**3.5.1.2 创建MQS Topic**中所创建的Topic名称。

3.5.1.3.3 SASL 配置信息

配置说明请参考**表3-33**。

说明

若MQS开启了SASL_SSL则安全协议必须选择SASL_SSL方式，查看MQS是否开启SASL_SSL请参考图1

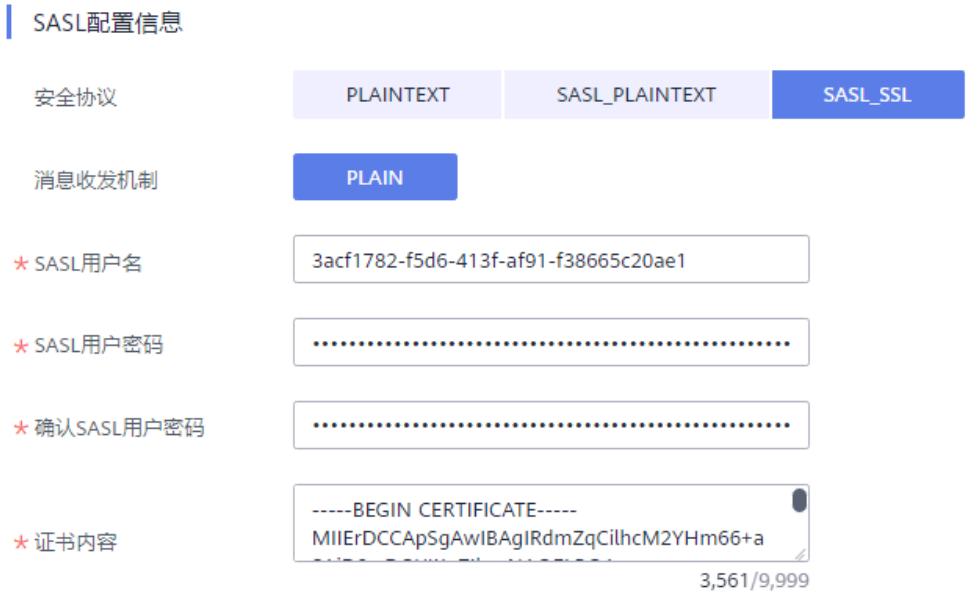
图 3-184 MQS 是否开启 SASL_SSL

表 3-33 SASL 配置信息

参数	配置说明
SASL配置信息	
安全协议	连接目标Kafka所使用的安全协议。 ● PLAINTEXT：默认接入点的用户认证协议。 ● SASL_PLAINTEXT：SASL用户认证协议。 ● SASL_SSL：SSL用户认证协议。
消息收发机制	目标Kafka的消息收发的机制，默认为PLAIN，但是当MQS开启了SASL_SSL时，需要选择SASL_SSL。
SASL用户名	**仅当“安全协议”选择“SASL_PLAINTEXT”或“SASL_SSL”时需配置。** SASL或SSL认证所使用的用户名。
SASL用户密码	**仅当“安全协议”选择“SASL_PLAINTEXT”或“SASL_SSL”时需配置。** SASL或SSL认证所使用的用户密码。
证书内容	**仅当“安全协议”选择“SASL_SSL”时需配置。** SSL认证所使用的CA证书内容。

示例

图 3-185 配置填写详细说明



1. SASL用户名：topic所在集成应用的key
   SASL用户密码：topic所在集成应用的secret
   获取方式如下：
   - 登录ROMA Connect控制台，在“实例”页面单击实例上的“查看控制台”，进入实例控制台。
   - 在左侧的导航栏选择“集成应用”，单击MQS所属应用的名称仅需应用管理界面。

图 3-186 集成应用

- 复制粘贴应用的key和secret：

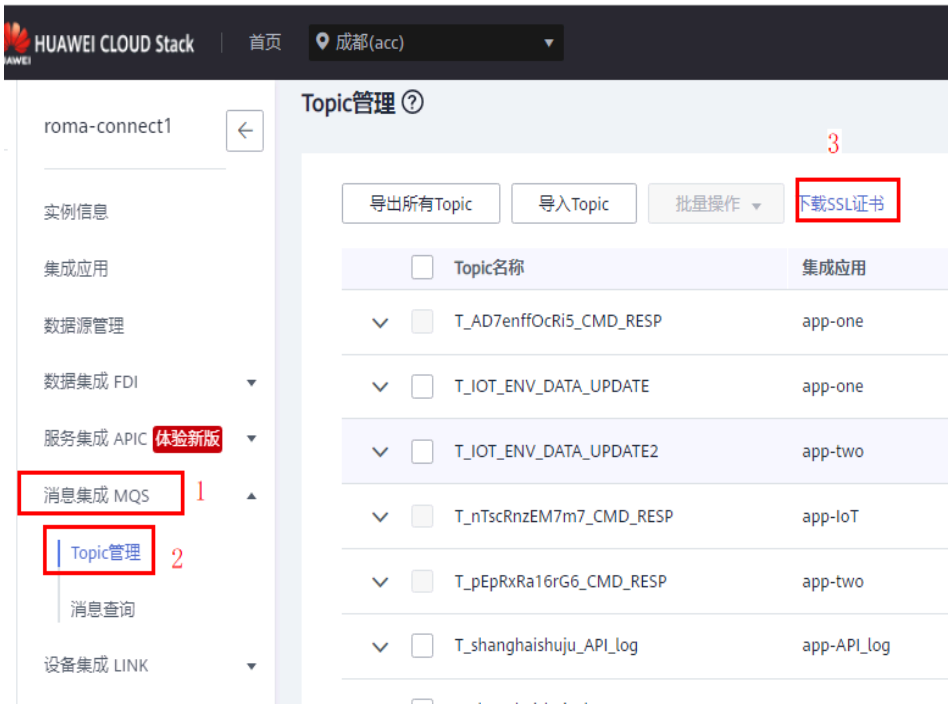
图 3-187 复制粘贴应用

2. 证书内容：ROMA Connect MQS的SSL证书

   获取方法如下：

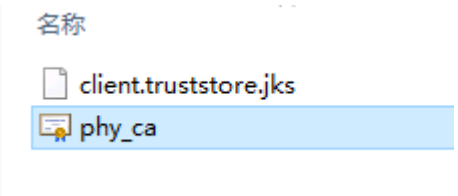
   - 登录ROMA Connect控制台，在“实例”页面单击实例上的“查看控制台”，进入实例控制台。
   - 在左侧的导航栏选择“消息集成MQS > Topic管理”，单击页面的“下载SSL证书”。

图 3-188 下载 SSL 证书



- 解压后，使用notepad++或其他文本编辑工具打开phy_ca的证书文件。

图 3-189 编辑工具打开 phy_ca



- 复制文件内容，文件内容格式如下，将其填入证书内容。

```
-----BEGIN CERTIFICATE-----
****略****
-----END CERTIFICATE-----
-----BEGIN CERTIFICATE-----
****略****
-----END CERTIFICATE-----
```

3.5.1.3.4 元数据配置信息

配置信息请参考**表3-34**

表 3-34 元数据配置信息

参数	配置说明
元数据配置信息	

参数	配置说明
系统元数据	推送的日志中，需要携带的系统字段信息。 其中，start_time、request_id、client_ip、request_time、http_status、scheme、request_method、host、uri、upstream_addr、upstream_status、upstream_response_time、http_x_forwarded_for、http_user_agent和error_type字段信息默认在日志中携带，其他系统字段需勾选后才携带。
请求数据	推送的日志中，需要携带的API请求信息。 • 日志包含请求头域信息：勾选后，需填写日志中要携带的请求Header参数。多个字段间使用英文逗号（,）分隔，支持使用*进行通配设置。 • 日志包含请求QueryString信息：勾选后，需填写日志中要携带的请求Query参数信息。多个字段间使用英文逗号（,）分隔，支持使用*进行通配设置。 • 日志包含请求Body体信息：勾选后，日志中会携带API请求的Body体信息。
响应数据	推送的日志中，需要携带的API响应信息。 • 日志包含响应头域信息：勾选后，需填写日志中要携带的响应Header参数。多个字段间使用英文逗号（,）分隔，支持使用*进行通配设置。 • 日志包含响应Body体信息：勾选后，日志中会携带响应Body体信息。
自定义认证配置	推送的日志中，需要携带的自定义认证信息。 • 前端：填写日志中要携带的前端自定义认证的响应字段信息，多个字段间使用英文逗号（,）分隔。 • 后端：填写日志中要携带的后端自定义认证的响应字段信息，多个字段间使用英文逗号（,）分隔。

示例

根据需要选择日志中所携带的系统元数据，推荐元数据参数类别见**表3-35**。

图 3-190 日志系统元数据列表

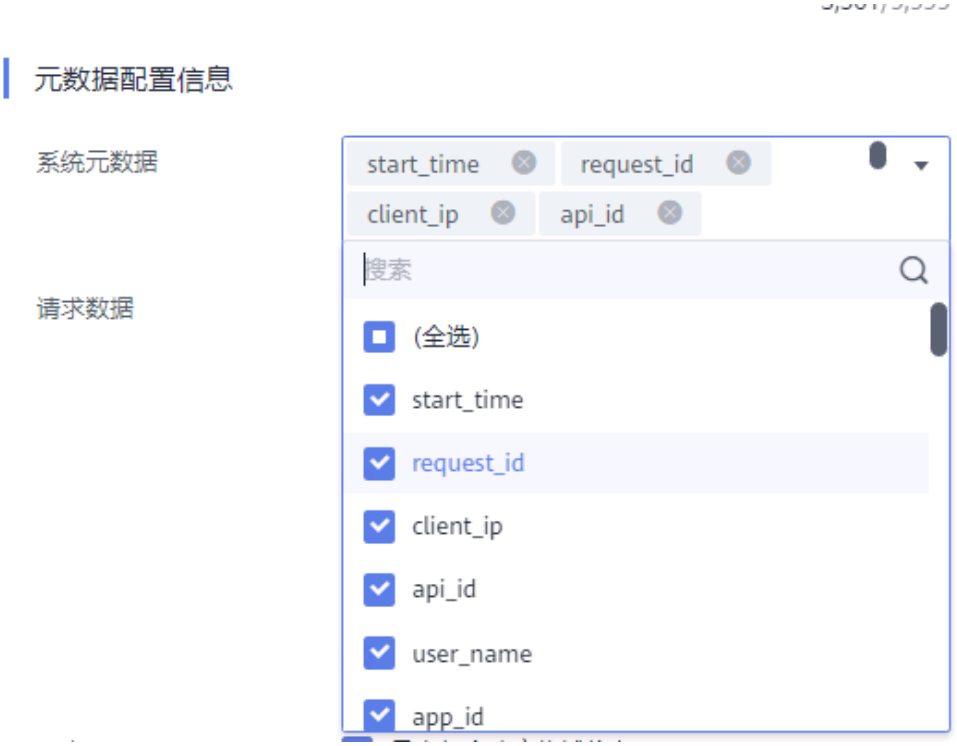


表 3-35 日志系统元数据列表

/	参数名称	参数说明	解析路径
基础信息	uri	请求URI	system.uri
	start_time	请求开始时间，使用unix时间戳，保留小数点后三位，精确至毫秒	system.start_time
	client_ip	客户端请求IP	system.client_ip
	user_name	用户ID	system.user_name
	http_status	响应状态码	system.http_status
	api_id	API ID	system.api_id
	api_name	API名称	system.api_name
	api_uri_mode	API请求模式，前缀匹配SWA或准确匹配NORMAL	system.api_uri_mode
	app_id	客户端的APP ID	system.app_id
	app_name	客户端的APP name	system.app_name
	provider_app_id	API所属的应用的id	system.provider_app_id

/	参数名称	参数说明	解析路径
	provider_app_name	API所属的应用的名称	system.provider_app_name
	request_id	请求ID	system.request_id
	access_model1	认证模式1，若开启APP认证，则为APP_SECRET	system.access_model1
	access_model2	认证模式2，开启双重认证，为自定义认证的id	system.access_model2
	error_type	API请求的错误类型。0：非流控错误。1：流控错误。	system.error_type
后端信息	upstream_uri	后端请求uri	system.upstream_uri
	upstream_addr	后端请求地址	system.upstream_addr
	upstream_header_time	从开始与后端建立连接到从后端获取到首字节所用时间，单位秒。	system.upstream_header_time
	upstream_response_time	从开始与后端建立连接到从后端获取到最后一个字节所用时间，单位秒。	system.upstream_response_time
	upstream_status	后端响应状态码。	system.upstream_status
响应信息	response_size	响应体大小	system.response_size
	response_body	响应体内容	call_data.response_body
	response_header	响应头内容	call_data.response_header
请求信息	body_bytes_sent	API请求的Body体大小，单位字节。	system.body_bytes_sent
	request_size	请求大小	system.request_size
	request_body	请求体	call_data.request_body
	request_query_string	请求参数	call_data.request_query_string
	request_header	请求头	call_data.request_header
	request_time	请求时延（单位：s）	system.request_time

勾选下图中的：“日志包含请求头域信息”、“日志包含请求QueryString信息”、“日志包含请求Body体信息”、“日志包含响应头信息”、“日志包含响应Body体信息”。所携带的参数可使用“*”来进行全选。

图 3-191 云数据配置信息

3.5.1.3.5 修改请求体和响应体默认大小

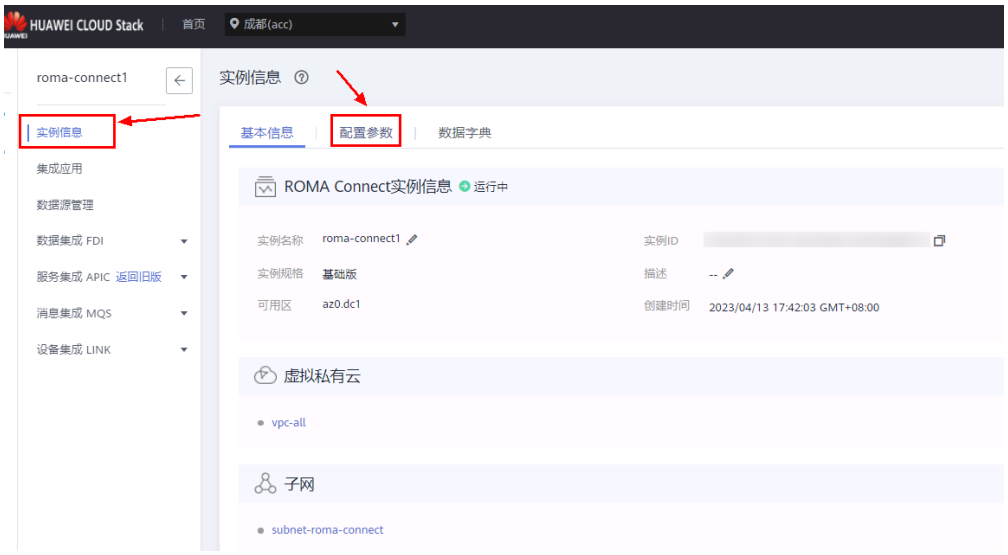
概述

配置参数提供了实例内组件的公共参数配置，通过修改配置参数，可以调整组件的相关功能配置，将kafka日志推送插件的请求体和响应体大小修改为最大4K。

操作步骤：

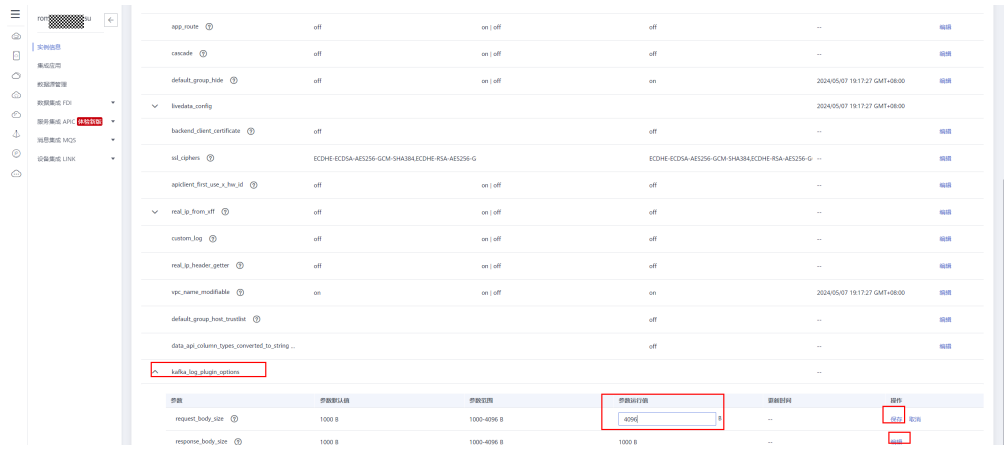
步骤1 在实例控制台的“实例信息”页面选择“配置参数”页签，可查看实例的配置参数，也可修改“参数运行值”。

图 3-192 配置参数



步骤2 配置参数下拉至最后，修改参数kafka_log_plugin_options，将参数改为4096B（请根据项目实际需求修改）。

图 3-193 编辑



----结束

3.5.1.4 插件绑定 API

概述

插件和API本身相互独立，只有为API绑定插件后，插件才对API生效。为API绑定插件时需指定发布环境，插件只对指定环境上的API生效。

前提条件

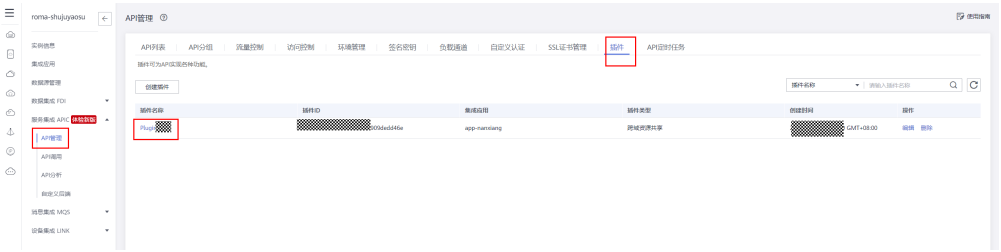
已创建插件，并且插件对API可见。因此创建插件时建议使用全局可见。

操作步骤

步骤1 登录ROMA Connect控制台，在“实例”页面单击实例上的“查看控制台”，进入实例控制台。

步骤2 在左侧的导航栏选择“服务集成 APIC > API管理”，在“插件”页签下单击需要绑定API的插件名称。

图 3-194 插件

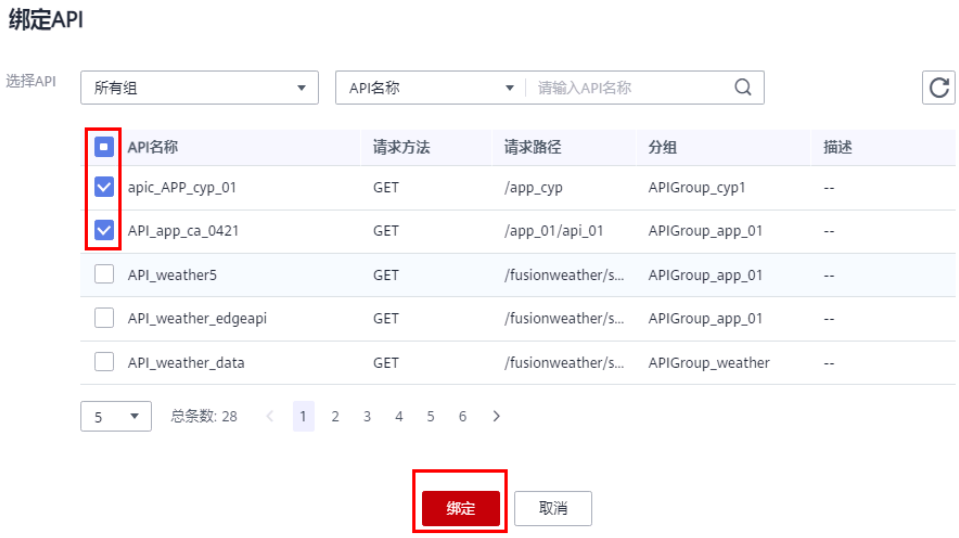


步骤3 进入插件页面，单击需要绑定的API的“环境”，然后单击“绑定API”。

图 3-195 绑定 API

步骤4 选择要推送日志的API（全选），单击“绑定”。

图 3-196 绑定



----结束

3.5.2 将 MQS 中日志导入 DWS

3.5.2.1 配置数据源

添加 MQS 数据源

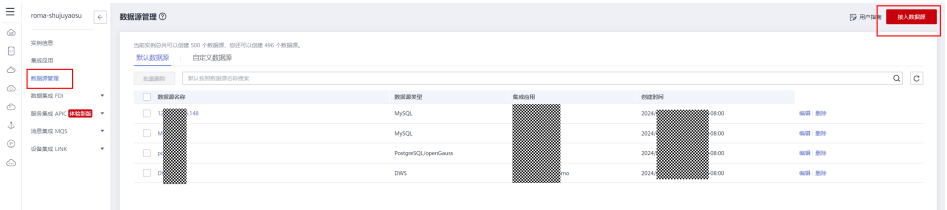
概述：ROMA Connect支持把MQS数据库作为一个数据源。在使用MQS数据源前，您需要先接入数据源。

前提条件：每个接入的数据源都要归属到某个集成应用下，在接入数据源前您需要有可用的集成应用，否则请提前创建集成应用。

操作步骤

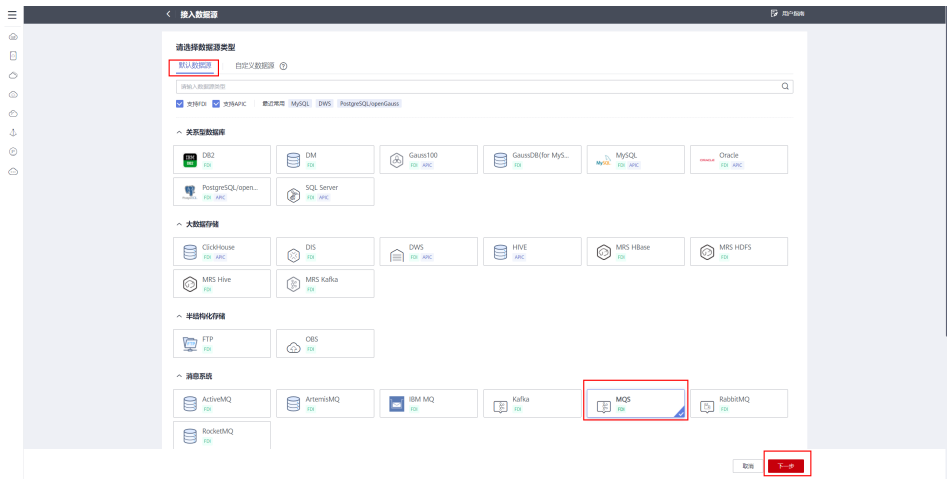
1. 登录ROMA Connect控制台，在“实例”页面单击实例上的“查看控制台”，进入实例控制台。
2. 在左侧的导航栏选择“数据源管理”，单击页面右上角的“接入数据源”。

图 3-197 接入数据源



3. 在接入数据源页面的“默认数据源”页签下，选择“MQS”类型的数据源，然后单击“下一步”。

图 3-198 默认数据源



4. 在页面中配置数据源的连接信息。集成应用请选择**3.5.1.1 创建日志消息队列所属的集成应用**中所创建的集成应用。下图为启用SSL的情况下的参数截图，参数获取可参考**3.5.1.3 创建Kafka日志推送插件**。

图 3-199 数据源连接信息

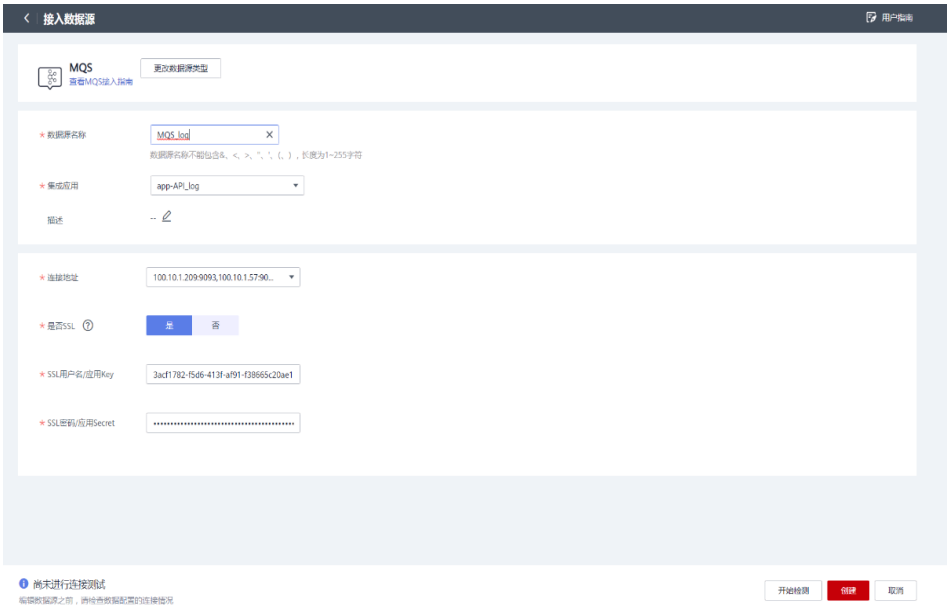


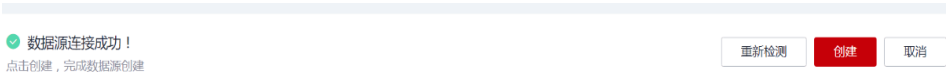
表 3-36 数据源连接信息

参数	配置说明
数据源名称	填写数据源的名称，根据规划自定义。建议您按照一定的命名规则填写数据源名称，方便您快速识别和查找。
集成应用	选择数据源所归属的集成应用。
描述	填写数据源的描述信息。
连接地址	选择当前实例下MQS的内网链接地址，IPv6实例支持选择IPv6内网链接地址。

参数	配置说明
是否SSL	ROMA Connect与MQS的连接是否使用SSL认证加密。 若MQS同时开启了SSL与VPC内网明文访问，请选择“否”。
SSL用户名/应用Key	**仅当“是否SSL”选择“是”时需要配置。** SSL认证所使用的用户名，如果使用ROMA Connect的消息集成作为MQS数据源，则用户名为集成应用的Key。
SSL密码/应用Secret	**仅当“是否SSL”选择“是”时需要配置。** SSL认证所使用的用户密码，如果使用ROMA Connect的消息集成作为MQS数据源，则密码为集成应用的Secret。

5. 完成数据源接入配置后，单击“开始检测”，检测ROMA Connect与数据源之间是否能够连通。。
   - 若测试结果为“数据源连接成功！”，则继续下一步。
   - 若测试结果为“数据源连接失败！”，则检查数据源状态和数据源连接参数配置，然后单击“重新检测”，直到连接成功为止。

   图 3-200 数据源连接成功

6. 单击“创建”，完成数据源的接入。

添加 DWS 数据源

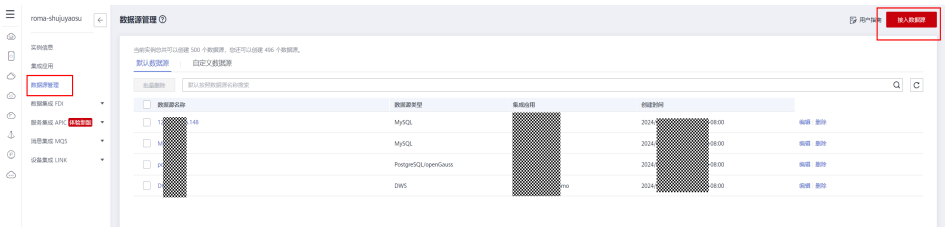
概述：ROMA Connect支持把DWS（数据仓库服务）作为一个数据源，并用于数据集成任务或用于创建数据API。在使用DWS数据源前，您需要先接入数据源。

前提条件：每个接入的数据源都要归属到某个集成应用下，在接入数据源前您需要有可用的集成应用，否则请提前**3.5.1.1 创建日志消息队列所属的集成应用**。

操作步骤：

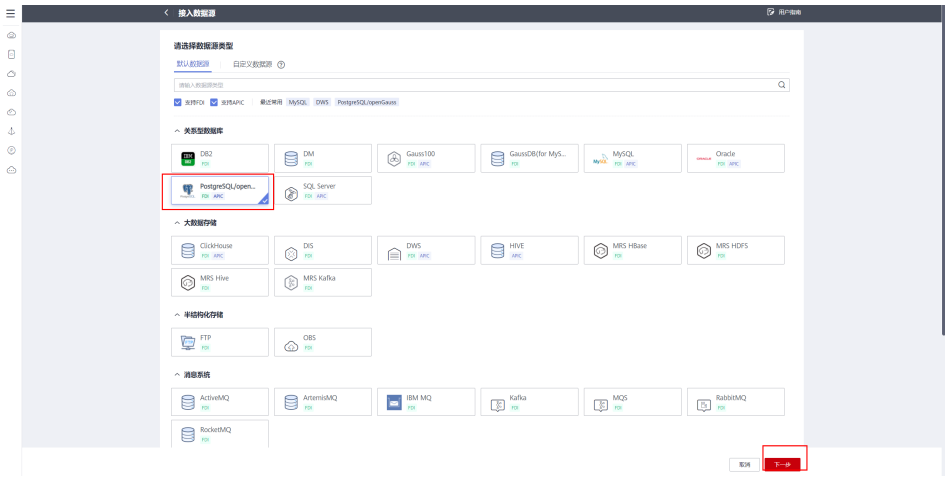
1. 登录ROMA Connect控制台，在“实例”页面单击实例上的“查看控制台”，进入实例控制台。
2. 在左侧的导航栏选择“数据源管理”，单击页面右上角的“接入数据源”。

   图 3-201 接入数据源

3. 在接入数据源页面的“默认数据源”页签下，选择“DWS”类型的数据源，然后单击“下一步”。

图 3-202 默认数据源

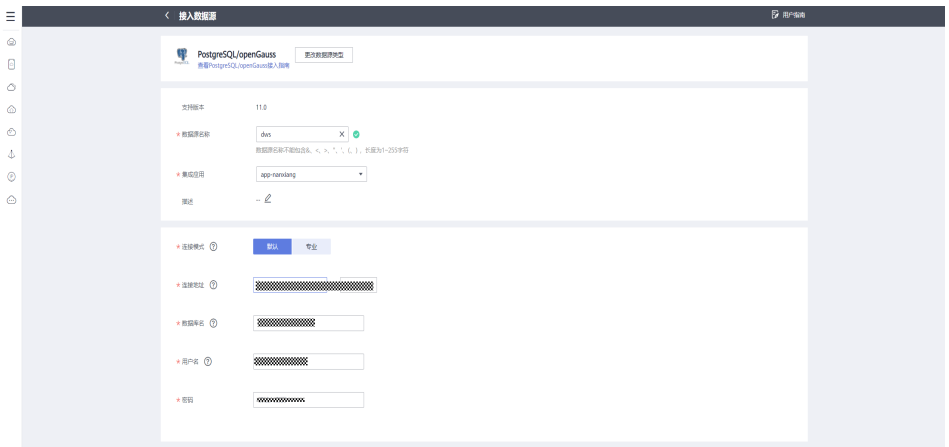


4. 在页面中配置数据源的连接信息。数据可的链接信息可在云服务页面查看。

图 3-203 查看

图 3-204 连接信息

图 3-205 创建



说明

DWS数据源建议使用内网地址，若使用EIP请放开防火墙。

表 3-37 数据连接信息

参数	配置说明
数据源名称	填写数据源的名称，根据规划自定义。建议您按照一定的命名规则填写数据源名称，方便您快速识别和查找。
集成应用	选择数据源所归属的集成应用。
描述	填写数据源的描述信息。
连接地址	填写DWS集群中数据库的连接IP地址和端口号。
数据库名	填写DWS集群中要接入的数据库名。
用户名	填写连接数据库的用户名。
密码	填写连接数据库的用户密码。

5. 完成数据源接入配置后，单击“开始检测”，检测ROMA Connect与数据源之间是否能够连通。
   - 若测试结果为“数据源连接成功！”，则继续下一步。
   - 若测试结果为“数据源连接失败！”，则检查数据源状态和数据源连接参数配置，然后单击“重新检测”，直到连接成功为止。
6. 单击“创建”，完成数据源的接入。

3.5.2.2 准备 DWS 表

使用 Data Studio 连接 DWS

- Data Studio概述

  Data Studio通过提供图形化界面来展示数据库的主要功能，简化了数据库开发和应用构建任务。

  数据库开发人员可以使用Data Studio所提供的特性，创建和管理数据库对象（数据库对象包含数据库、模式、函数、存储过程、表、序列、列、索引、约束条件、视图等），执行SQL语句/SQL脚本，编辑和执行PL/SQL语句，以及导入和导出表数据。

  数据库开发人员可在Data Studio中通过单步进入、单步退出、单步跳过、继续、终止调试等操作调试并修复PL/SQL代码中的缺陷。

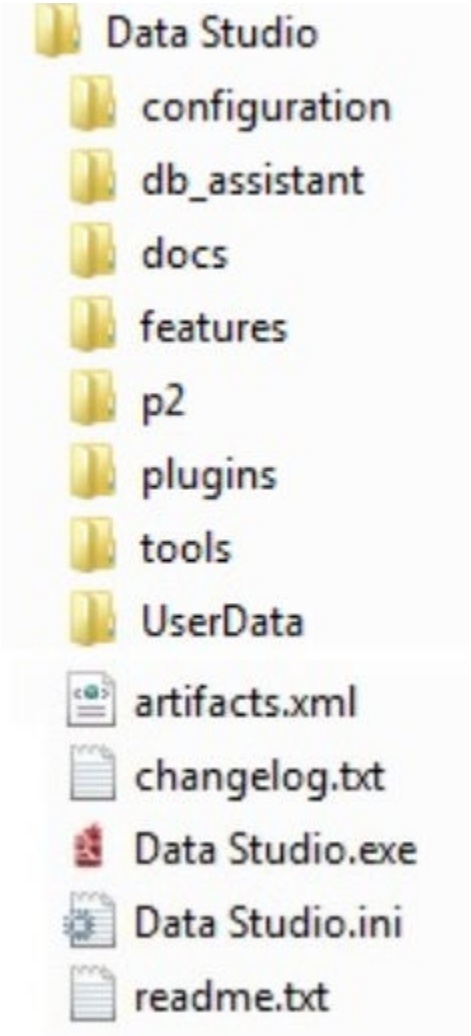
- Data Studio安装配置

  a. 登录数据仓库服务界面，打开“连接管理”，单击Data Studio图形界面客户端“下载”按钮。

图 3-206 下载

b. 解压安装包后即可运行Data Studio。解压后可以获取如下文件和文件夹：

图 3-207 解压安装包



c. 定位并双击Data Studio.exe，启动Data Studio客户端。

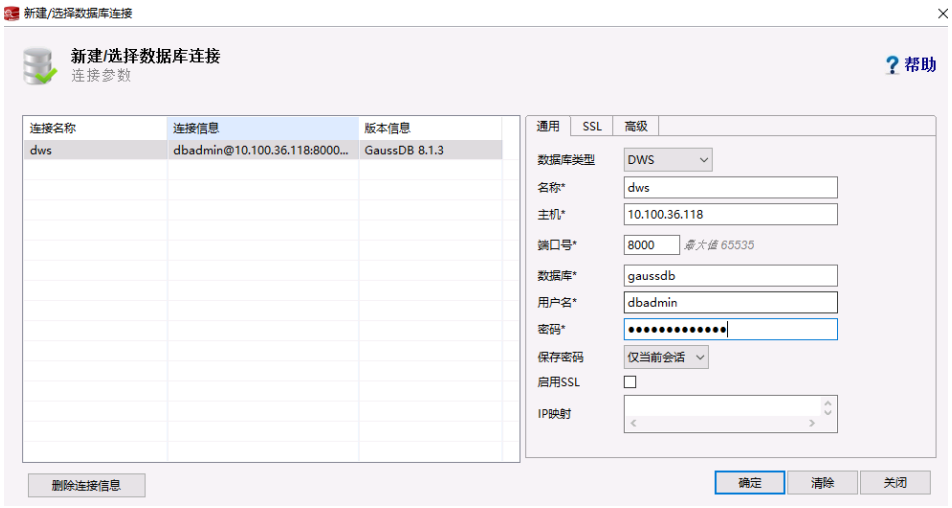
d. 如果安装出现错误，请参考**工具说明**。

- Data Studio连接配置

  a. 在主菜单中选择“**文件** > **新建连接**”，或单击工具栏上左上角的“新建连接”或按“Ctrl+N”连接到数据库服务器，弹出“**新建/选择数据库连接**”对话框。

  b. 设置如下参数，创建数据库连接：

图 3-208 设置参数

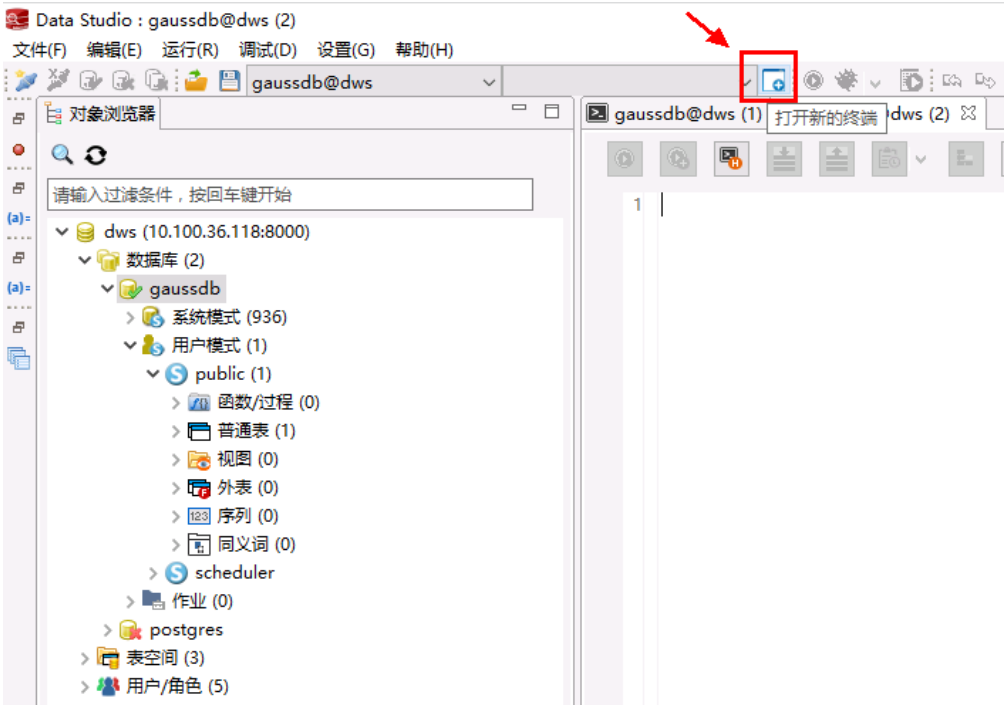


c. 单击“**确定**”建立连接。

创建表

1. 在“**对象浏览器**”窗格中，右键单击所需数据库，选择“**打开新的终端**”，或在工具栏中单击，或使用快捷键“Ctrl+T”打开新的SQL终端。

图 3-209 打开新的终端



显示“SQL终端”页签。

2. 使用SQL语句创建需要DWS表格，语法请参考**DWS文档**。
3. 【示例】SQL，选取**图3-190**中参数作为列参。使用如下语句编译执行。

```
create schema apilog;
create table apilog.log_kafka(
```

```
batchid VARCHAR,
uri VARCHAR,
start_time NUMBER,
client_ip VARCHAR,
user_name VARCHAR,
http_status  INTEGER,
api_id VARCHAR,
api_name VARCHAR,
api_uri_mode VARCHAR,
app_id VARCHAR,
app_name VARCHAR,
provider_app_id VARCHAR,
provider_app_name VARCHAR,
request_id VARCHAR,
access_model1 VARCHAR,
access_model2 VARCHAR,
error_type INTEGER,
upstream_uri VARCHAR,
upstream_addr VARCHAR,
upstream_header_time NUMBER,
upstream_response_time NUMBER,
upstream_status INTEGER,
response_size INTEGER,
response_body VARCHAR,
response_header VARCHAR,
body_bytes_sent INTEGER,
request_size INTEGER,
request_body VARCHAR,
request_query_string VARCHAR,
request_header VARCHAR,
request_time NUMBER
);
```

说明

示例未指定分布列和主键等参数，根据实际项目中的查询需求，请自行添加，参考**SQL语法说明**。

3.5.2.3 配置 FDI 任务

概述

通过在ROMA Connect中创建数据集成任务，您可以实现不同数据源之间的数据集成转换。本节主要提供数据集成任务（MQS->DWS）基本信息和任务计划的配置说明。

前提条件

- ROMA Connect已接入源端和目标端数据源，具体请参考**接入数据源**。
- ROMA Connect具备向目标端数据源写入数据的权限。
- 若需要配置同步异常的数据存储，需要完成OBS数据源的接入配置，具体请参见**接入OBS数据源**。

配置基本信息

- 登录ROMA Connect控制台，在“实例”页面单击实例上的“查看控制台”，进入实例控制台。
- 在左侧的导航栏选择“数据集成 FDI > 任务管理”，单击页面的“创建普通任务”。

图 3-210 创建普通任务

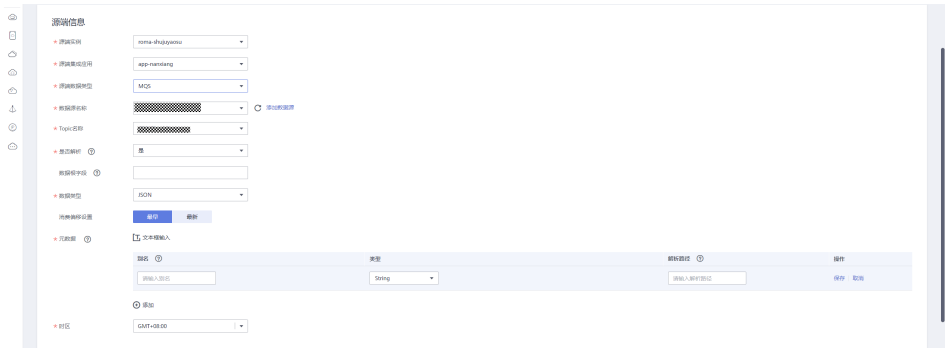
- 在创建任务页面中配置任务基本信息。

  a. 集成模式选择实时。

  图 3-211 创建任务

  b. 源端信息请选择MQS，指定为**添加MQS数据源**所创建的MQS。Topic使用**3.5.1.2 创建MQS Topic**所创topic。具体配置如下，解析路径参考**图3-190**

  图 3-212 源端信息



  示例中DWS中的数据格式和Json解析的类型对应使用如下，但也可以全部使用String，经测试FDI能够自动转换数据结构：

表 3-38 数据类型对应

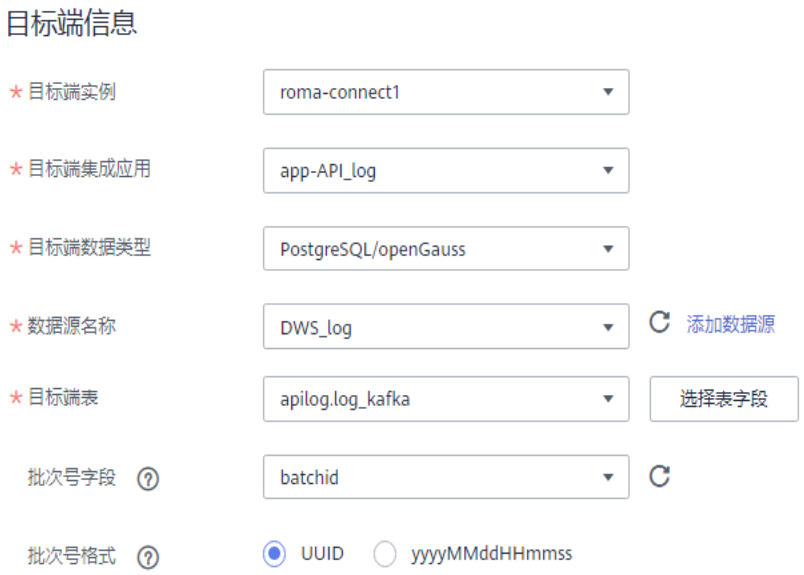
Json解析类型	DWS字段类型
String	VARCHAR
Integer	INTEGER
Double	NUMBER

说明

消息偏移设置若选择最早，则FDI会将所有MQS中的数据同步到DWS。
消息偏移设置若选择最新，则FDI知会将启动任务后MQS中新添加的数据同步到DWS。

c. 目的端信息请选择DWS，指定为**添加DWS数据源**所创建的DWS数据源。

图 3-213 目的端信息



d. Mapping信息：可使用自动Mapping，同名字段会自动映射。

图 3-214 Mapping 信息

e. 单击保存，显示任务提交成功。

图 3-215 保存

f. 返回任务列表，单击“启动”。

图 3-216 启动

3.5.3 日志查询

MQS 中查看

- 概述：ROMA Connect提供了可视化的消息查询功能，可在控制台界面查看Topic中存储的消息数据，可以更直观方便的查看消息正文。

  同一时间只能查询一个Topic的消息。若需要更强大的查询，请参考**DWS中查看**。

- 操作步骤

  a. 登录ROMA Connect控制台，在“实例”页面单击实例上的“查看控制台”，进入实例控制台。

  b. 在左侧的导航栏选择“消息集成 MQS > 消息查询”，进入消息查询页面。

  c. 在页面右上角选择要查询消息的Topic，界面自动展示该Topic中存储的消息记录。

图 3-217 查询消息

默认按消息生产时间查询最近 10 分钟内生产的消息。若要查询更大时间范围内的消息或按其它方式查询请使用高级搜索功能。若查询超时，请在高级搜索中适当调小查询时间范围。

图 3-218 高级搜索

另外高级搜索也支持按偏移量查询。

图 3-219 按偏移量查询

表 3-39 消息内容说明

参数	说明
Topic名称	消息所在的Topic名称。
消息ID	每条消息的标识，用户通过生产消息的消息头中message_id的值确定。
应用Key	每条消息的应用Key，用户通过生产消息的消息头中TAGS的值确定。
分区	消息所在的分区，编号从0开始。查询方式为“按偏移量查询”时必填。
偏移量	消息在分区中的偏移量。
业务Key	消息中携带的业务Key，用于标识消息发送所属的业务。
标签	客户端向Topic生产消息时所携带的标签，一般业务场景下不使用标签。
消息大小(B)	消息的大小。
生产时间	消息生产的时间。

d. 单击消息记录上的“消息内容”，在消息详情弹窗中可查看消息的具体内容。

图 3-220 消息详情

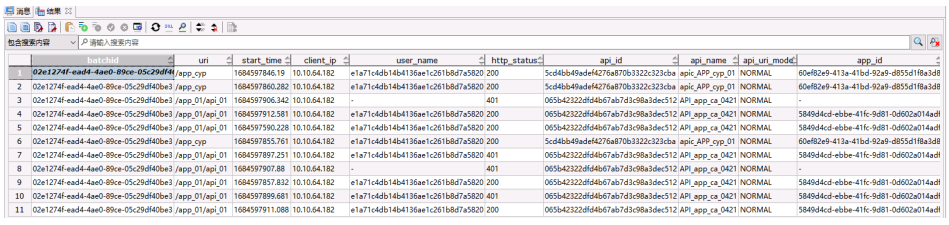
DWS 中查看

- 概述：使用Data Studio或者DGC中的作业开发均可查询DWS中的表格数据，本章节主要介绍如何使用SQL查询DWS中的日志信息。
- 操作步骤
  a. 参考**使用Data Studio连接DWS**链接DWS。
  b. 在SQL终端中使用SQL查询日志信息。

【示例】全表查询

```
select
 *
from
 apilog.log_kafka;
```

图 3-221 全表查询



batchid	uri	start_time	client_ip	user_name	http_status	api_id	api_name	api_uri_mode	app_id
1	02e1274f-ead4-4ae0-89ce-05c29df4	/app_cyp	1684597846.19	10.10.64.182	e1a71c4db14b4136ae1c261b8d7a5820	200	5cd4bb49adef4276a870b3322c323cba	apic_APP_cyp_01	NORMAL	60ef82e9-413a-41bd-92a9-d855d1f8a3d8
2	02e1274f-ead4-4ae0-89ce-05c29df40be3	/app_cyp	1684597860.282	10.10.64.182	e1a71c4db14b4136ae1c261b8d7a5820	200	5cd4bb49adef4276a870b3322c323cba	apic_APP_cyp_01	NORMAL	60ef82e9-413a-41bd-92a9-d855d1f8a3d8
3	02e1274f-ead4-4ae0-89ce-05c29df40be3	/app_01/api_01	1684597906.342	10.10.64.182	-	401	065b42322dfd4b67ab7d3c98a3dec512	API_app_ca_0421	NORMAL	-
4	02e1274f-ead4-4ae0-89ce-05c29df40be3	/app_01/api_01	1684597912.581	10.10.64.182	e1a71c4db14b4136ae1c261b8d7a5820	200	065b42322dfd4b67ab7d3c98a3dec512	API_app_ca_0421	NORMAL	5849d4cd-ebbe-41fc-9d81-0d602a014adf
5	02e1274f-ead4-4ae0-89ce-05c29df40be3	/app_01/api_01	1684597590.228	10.10.64.182	e1a71c4db14b4136ae1c261b8d7a5820	200	065b42322dfd4b67ab7d3c98a3dec512	API_app_ca_0421	NORMAL	5849d4cd-ebbe-41fc-9d81-0d602a014adf
6	02e1274f-ead4-4ae0-89ce-05c29df40be3	/app_cyp	1684597855.761	10.10.64.182	e1a71c4db14b4136ae1c261b8d7a5820	200	5cd4bb49adef4276a870b3322c323cba	apic_APP_cyp_01	NORMAL	60ef82e9-413a-41bd-92a9-d855d1f8a3d8
7	02e1274f-ead4-4ae0-89ce-05c29df40be3	/app_01/api_01	1684597897.251	10.10.64.182	e1a71c4db14b4136ae1c261b8d7a5820	401	065b42322dfd4b67ab7d3c98a3dec512	API_app_ca_0421	NORMAL	5849d4cd-ebbe-41fc-9d81-0d602a014adf
8	02e1274f-ead4-4ae0-89ce-05c29df40be3	/app_01/api_01	1684597907.88	10.10.64.182	-	401	065b42322dfd4b67ab7d3c98a3dec512	API_app_ca_0421	NORMAL	-
9	02e1274f-ead4-4ae0-89ce-05c29df40be3	/app_01/api_01	1684597857.832	10.10.64.182	e1a71c4db14b4136ae1c261b8d7a5820	200	065b42322dfd4b67ab7d3c98a3dec512	API_app_ca_0421	NORMAL	5849d4cd-ebbe-41fc-9d81-0d602a014adf
10	02e1274f-ead4-4ae0-89ce-05c29df40be3	/app_01/api_01	1684597899.681	10.10.64.182	e1a71c4db14b4136ae1c261b8d7a5820	401	065b42322dfd4b67ab7d3c98a3dec512	API_app_ca_0421	NORMAL	5849d4cd-ebbe-41fc-9d81-0d602a014adf
11	02e1274f-ead4-4ae0-89ce-05c29df40be3	/app_01/api_01	1684597911.088	10.10.64.182	e1a71c4db14b4136ae1c261b8d7a5820	200	065b42322dfd4b67ab7d3c98a3dec512	API_app_ca_0421	NORMAL	5849d4cd-ebbe-41fc-9d81-0d602a014adf

查询指定参数并按照访问的start_time排序

```
select

start_time,batch_id,api_id,app_id,upstream_status,upstream_response_time,request_id,response_b
ody,response_header
from
 apilog.log_kafka
order by
 start_time
DESC;
```

查询指定集成应用的总访问量

```
select
count(*)
from
 apilog.log_kafka
where
 provider_app_id=
'fcec3c73-cfe0-418c-b775-42d084199510'
;
```

说明

请根据实际需求使用SQL语法

3.5.4 将计量数据发布为 API

概述

通过将DWS中日志表的数据发开为API，可以将日志的计量数据发布，供BI或其他第三方调用展示或监控。

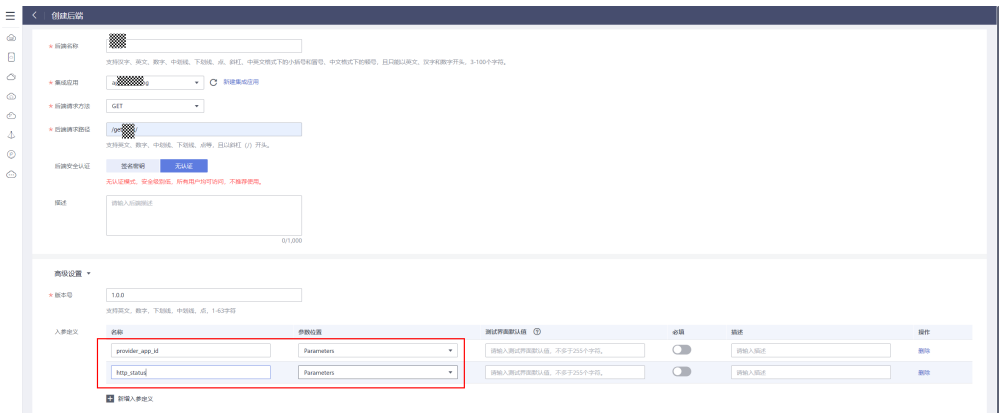
操作步骤

主要步骤请参考《xx服务可信访问操作指导》，本章节主要介绍使用参数传递方式动态的查询计量数据。

步骤1 创建后端，进入高级设置，添加入参定义。

步骤2 根据想要查询的计量逻辑，添加入参。示例添加两个参数“provider_app_id”和“http_status”，选择参数位置为“Parameters”，单击“创建”。

图 3-222 创建

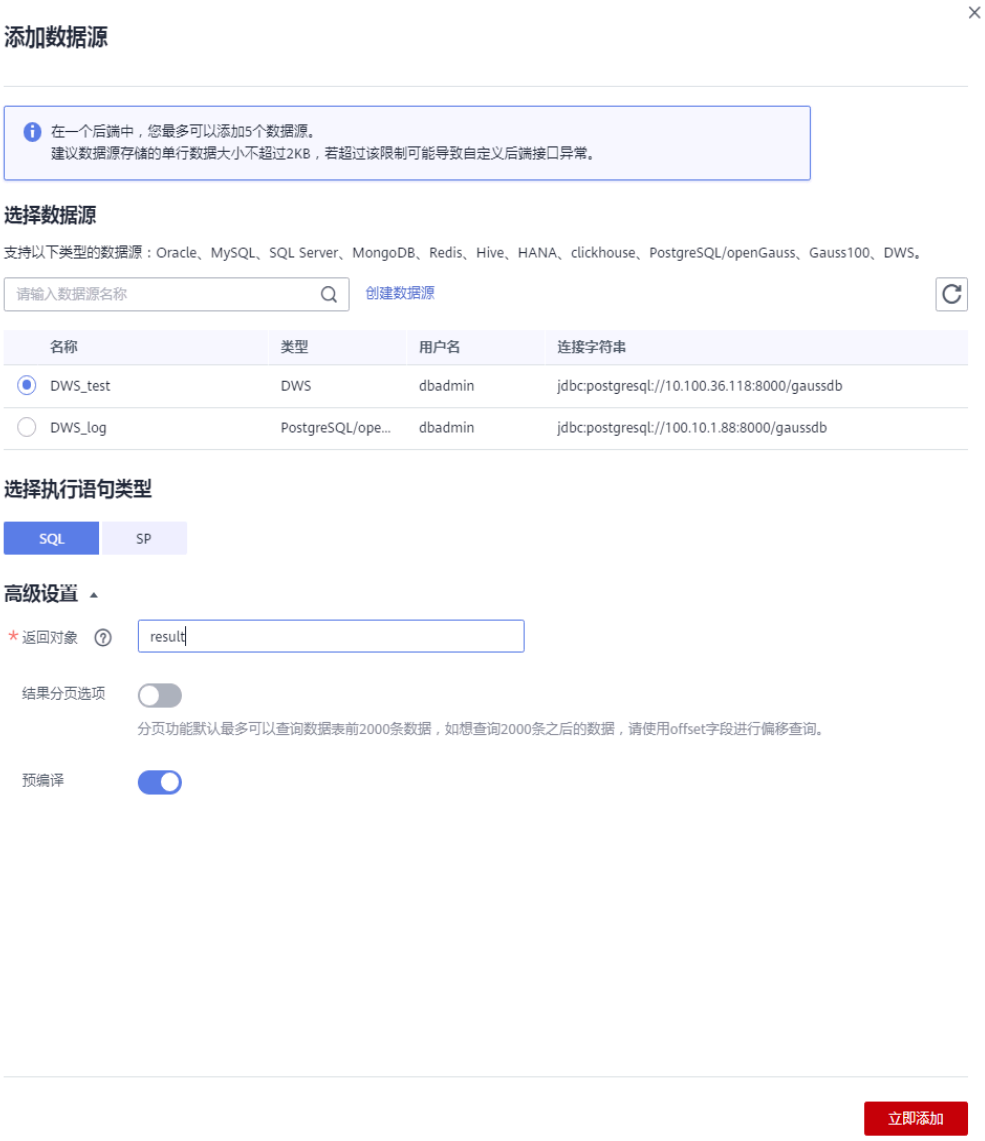


步骤3 【示例】进入后端页面，选择“文件”->“新建数据后端”->“添加数据源”，

图 3-223 添加数据源 1

选择对应的DWS数据源，和SQL执行语句。

图 3-224 添加数据源 2

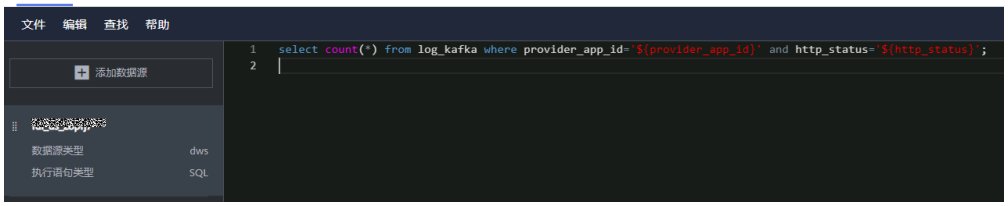


使用SQL查询指定的集成应用中成功返回的请求数量。

入参可以使用'${参数名称}'的方式进行注入

```
select count(*) from log_kafka where provider_app_id='${provider_app_id}' and http_status='${http_status}';
```

图 3-225 SQL 查询



步骤4 单击保存，然后进行测试，填写入参后测试结果如下。

表名该集成应用的成功访问次数

说明

除了使用SQL，存储过程或函数后端的方式都可以开放数据API。请根据实际情况使用

步骤5 单击部署和发布即可。

图 3-226 部署和发布

----结束

4 验证指导

4.1 DataArts Studio 工具权限验证

只有被授予了某工作空间角色的用户，才能访问（可见）该工作空间。通过对工作空间以用户组为粒度进行授权，实现了不同开发场景下生产空间和开发工作空间的隔离。

按照**DataArts Studio工具授权**操作后，可按照本章节步骤对DataArts Studio权限分配进行验证。

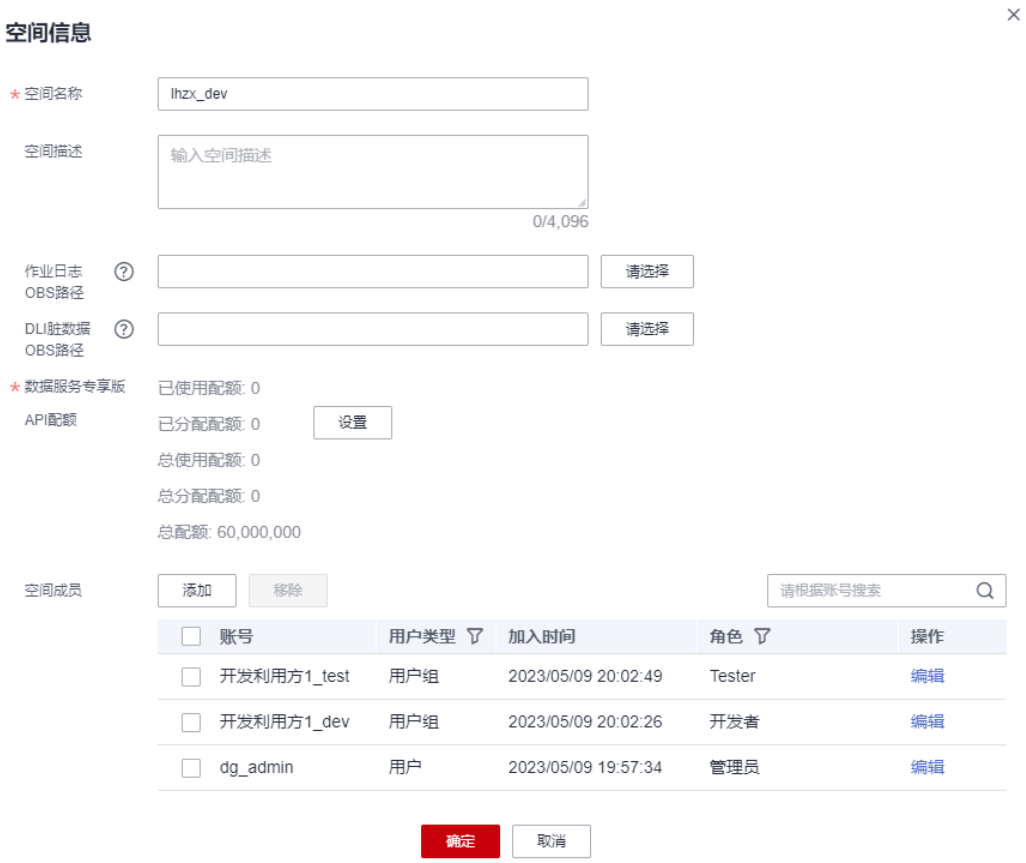
DataArts Studio 工作空间隔离验证

前提条件：授权运营方-管理员为不同开发利用方创建对应生产和开发空间。

操作步骤：

步骤1 将开发利用方-开发人员用户组“开发利用方1_dev”，授权给lhzx_dev开发空间。

图 4-1 空间信息 1



步骤2 将开发利用方-运维人员用户组“开发利用方1_om”，授权给lhzx_prod开发空间。

图 4-2 空间信息 2

步骤3 使用开发利用方1_dev用户组下用户“dev1”登录DataArt Studio实例，无法访问（不可见）工作空间phjr_prod。实现了生产空间和开发空间隔离。

图 4-3 工作空间

----结束

4.2 ROMA Connect 工具权限验证

按照**ROMA Connect集成与授权**完成ROMA Connect开发工具授权操作后，可按照本章节步骤对ROMA Connect权限分配进行验证。

ROMA Connect 实例隔离验证

开发利用方-开发人员、测试人员仅有ROMA Connect开发实例所在的资源集权限，无法在智能云管理平台平台上看到生产实例。授权运营方-运维人员仅有ROMA Connect生产实例所在资源集权限，无法在智能云管理平台平台上看到开发实例。

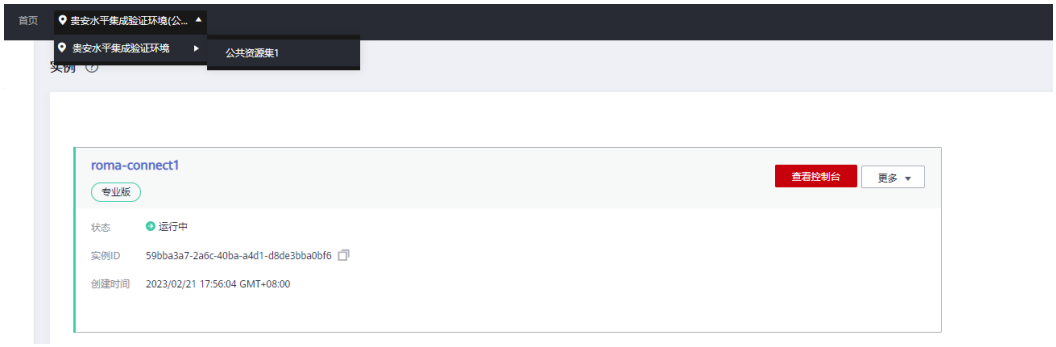
步骤1 使用开发利用方-开放人员账号登录智能云管理平台平台，进入公共服务资源集2可以正常访问开发实例，进入公共服务资源集1则弹出访问权限报错，无法看到生产实例；

图 4-4 生产实例

步骤2 使用开发利用方-测试人员账号登录智能云管理平台平台，进入公共服务资源集2可以正常访问开发实例，进入公共服务资源集1则弹出访问权限报错，无法看到生产实例；

步骤3 使用授权运营方-运维人员账号登录智能云管理平台平台，进入公共服务资源集1可以正常访问生产实例，无法进入公共服务资源集2访问开发实例。

图 4-5 开发实例



----结束

ROMA Connect 应用隔离验证

完成ROMA Connect集成应用授权后，对应账号才能访问该实例中集成应用。以如下场景为例：开发利用方-开发人员已有集成应用a相应权限，在开发实例中再创建集成应用b、c。

步骤1 使用授权运营方管理员账号登录智能云管理平台平台，在ROMA Connect开发实例中创建集成应用b、集成应用c；

图 4-6 创建集成应用

步骤2 使用开发利用方-开发人员登录智能云管理平台平台，进入ROMA Connect开发实例，仅能访问已授权的集成应用a。

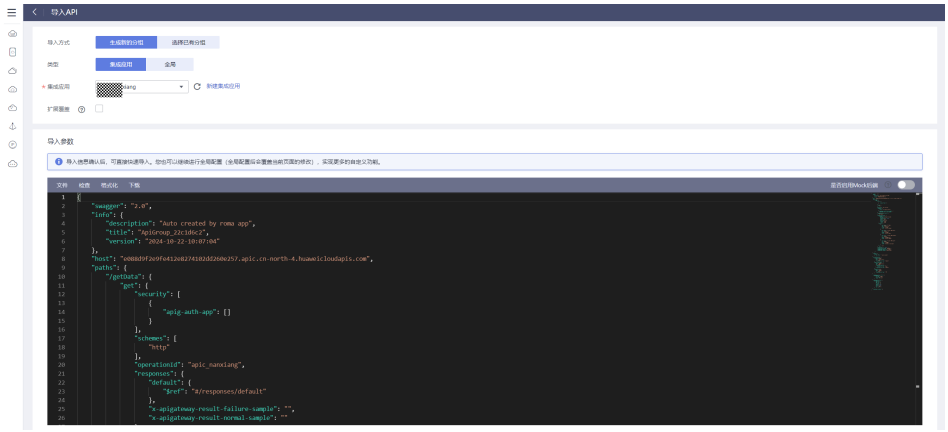
图 4-7 开发实例

----结束

ROMA Connect 运维操作验证

- 导出ROMA Connect开发实例中集成应用a的API
  a. 使用开发利用方-开发人员账号登录智能云管理平台平台，进入ROMA Connect开发实例，单击集成应用a后的“进入API管理”，进入集成应用a的API管理页面，全选后单击“更多”—“导出API”；
  b. 导出api的json文件保存至本地，然后发送给授权运营方-运维人员。
- 在ROMA Connect生产实例中导入步骤1导出的API
  a. 使用授权运营方运维人员账号登录智能云管理平台平台，进入ROMA Connect生产实例，单击集成应用a1后的“进入API管理”，进入集成应用a1的API管理页面，单击“更多”—“导入API”；
  b. 导入API界面中，单击“文件”，上传步骤1保存至本地的json文件，确认信息无误后单击“快速导入”完成API的导入。

图 4-8 快速导入



4.3 MRS 权限验证

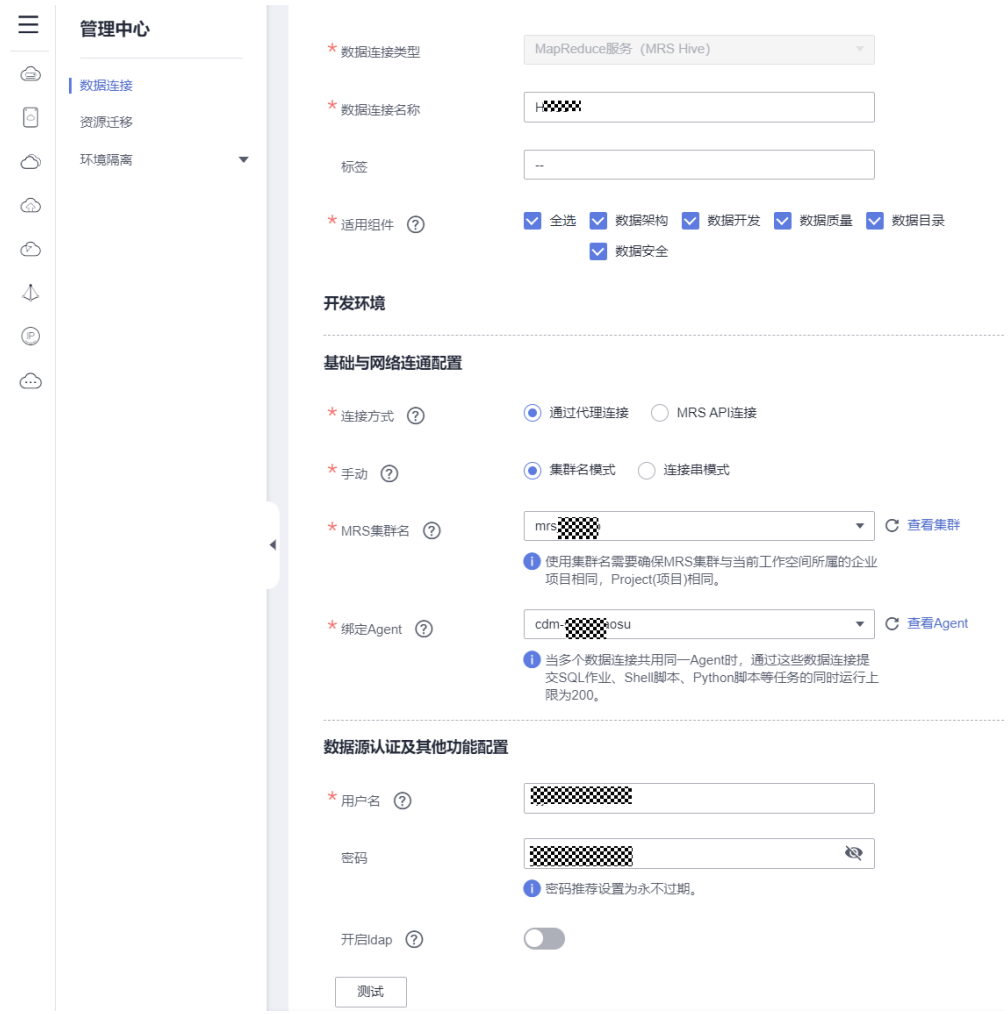
按照**3.1.3.2.1 OBS分配和授权**、**3.1.3.2.2 MRS分配和授权**完成MRS数据底座授权操作后，可按照本章节步骤对MRS库权限分配进行验证。

平台运营方权限隔离验证

平台运营方-运维人员的MRS FI安全认证管理员账号映射了OBS管理员权限，可以基于数据提供方接入数据创建开发、生产接入数据库。

步骤1 **平台运营方-运维人员**使用安全认证管理员账号在DataArts Studio对应开发工作空间创建数据链接tianji_admin；

图 4-9 平台运营方



步骤2 新增数据提供方。平台运营方-开发人员登录DataArts Studio服务，进入“数据开发”功能模块，单击“新建Hive SQL脚本”。

在右上角配置相关数据链接和数据库信息。配置数据链接为步骤一中创建的tianji_admin；配置数据库为default。

创库语句示例：

```
CREATE DATABASE shnw_ods_dev LOCATION "obs://mrs-obs/obs_dev_tianji_mrs/p_op_dev_tianji/shnw_ods_dev";
```

图 4-10 新增数据提供方

步骤3 新增开发利用方。平台运营方-开发人员登录DataArts Studio服务，进入“数据开发”功能模块，单击“新建Hive SQL脚本”。

在右上角配置相关数据链接和数据库信息。配置数据链接为步骤一中创建的tianji_admin；配置数据库为default。

创库语句示例：

```
CREATE DATABASE shdg_phjr_hive_dev LOCATION "obs://mrs-obs/obs_dev_tianji_mrs/d_op_dev_tianji/shdg_phjr_hive_dev";
```

图 4-11 新增开发利用方

----结束

开发利用方权限隔离验证

步骤1 开发利用方（MRS账号：datagroup_dev_admin）在DataArts Studio对应开发工作空间创建数据链接datagroup_phjr_hive_link。

步骤2 使用开发利用方-开发人员账号登录DataArts Studio服务，进入“数据开发”功能模块，单击“新建Hive SQL脚本”。

步骤3 验证开发利用方人员在本场景下对生产融合库的所有权。

在右上角配置相关数据链接和数据库信息。配置数据链接为步骤一中创建的datagroup_phjr_hive_link；配置数据库为shdg_phjr_hive_dev。

验证结果

开发利用方人员可以在已被授予所有权的数据库中进行建表/读写等操作。

图 4-12 具有 CREATE 权限

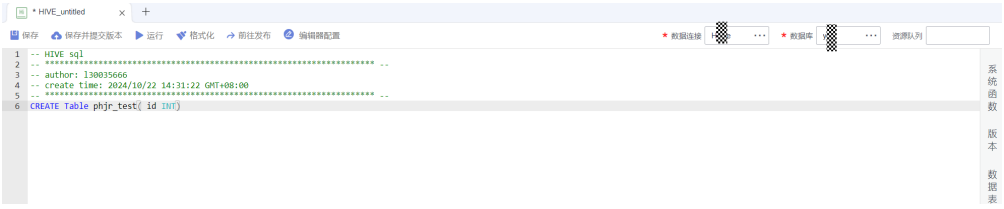
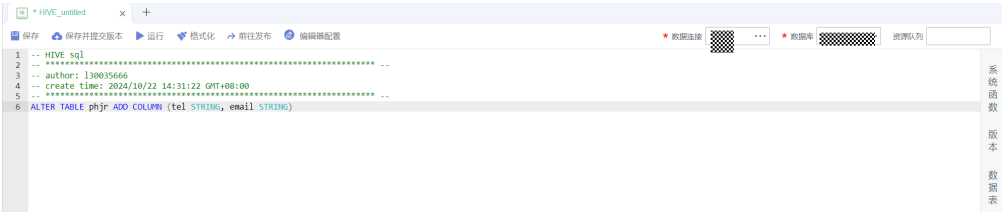


图 4-13 具有 ALTER 权限



步骤4 验证开发利用方人员拥有公共接入库的只读权限。

在右上角配置相关数据链接和数据库信息。配置数据链接为步骤一中创建的datagroup_phjr_hive_link；配置数据库为shdg_dwd_dev。

验证结果

开发利用方人员具备已经分配给该开发利用方公共库的只读权限，可以进行读操作，不可进行写、删除等操作；

图 4-14 具有 SELECT 权限

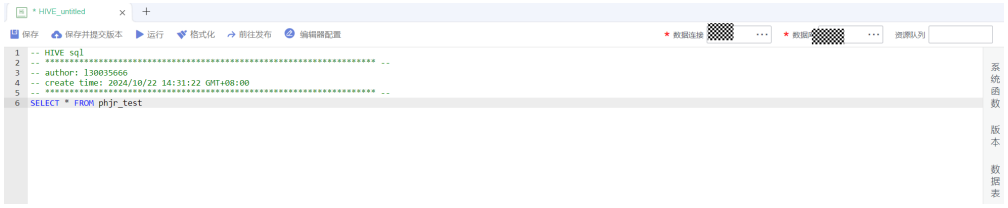


图 4-15 不具有 ALTER 权限

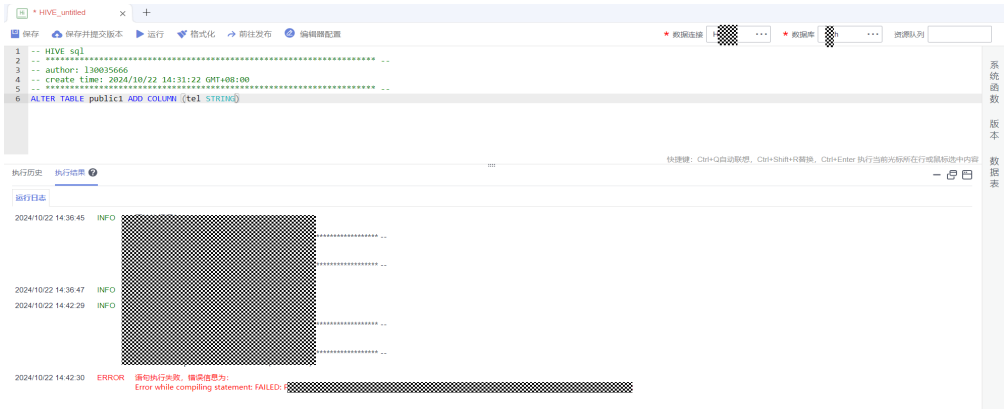
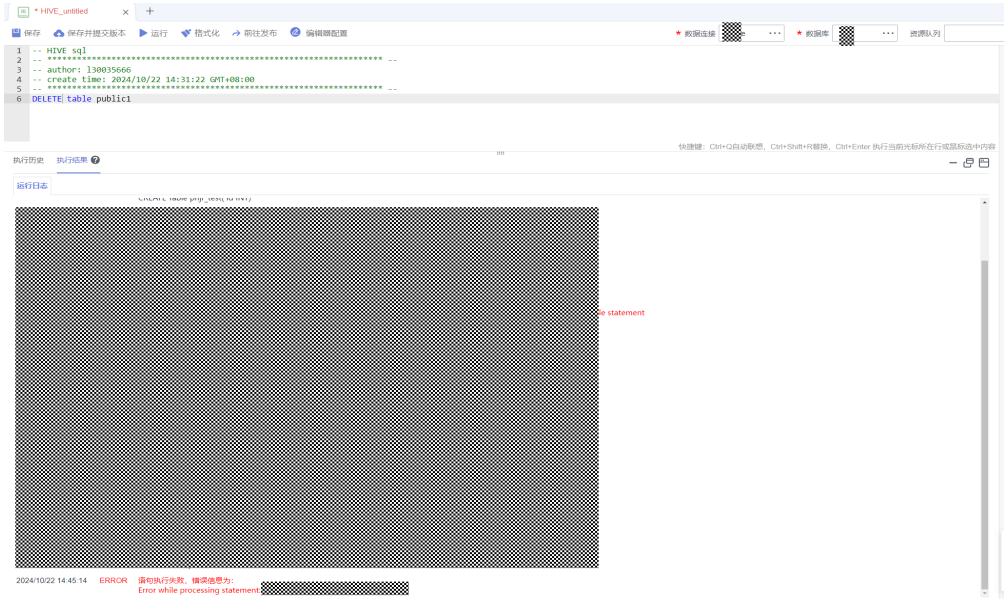


图 4-16 不具有 DELETE 权限



步骤5 验证开发利用方人员对其他未被授权的MRS库不可访问。

在右上角配置相关数据链接和数据库信息。配置数据链接为步骤一中创建的datagroup_phjr_hive_link；配置数据库为shnw_test_b。

报错信息：user [datagroup_dev_admin] does not have [USE] privilege on [shnw_test_b/test]

图 4-17 报错信息

----结束

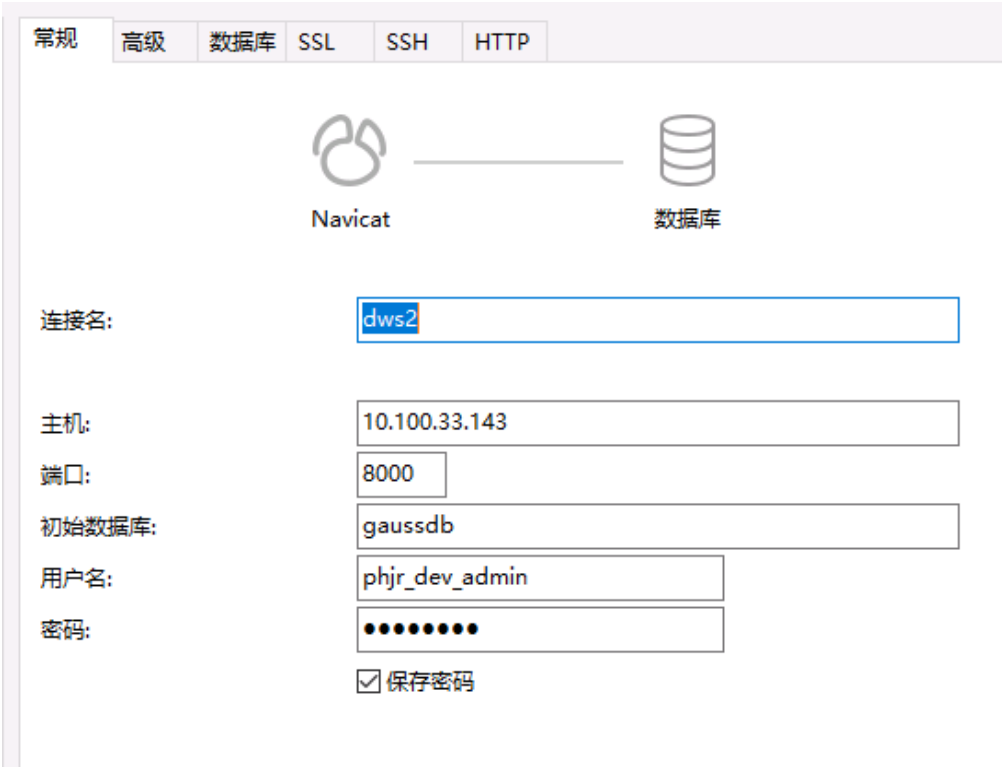
4.4 DWS 权限验证

按照**3.1.3.2.3 DWS分配和授权**完成授权操作后，可按照本章节步骤对DWS库表权限分配进行验证。

步骤1 验证开发利用方人员拥有公共接入库的只读权限。

使用DWS账号phjr_dev_admin连接数据库。

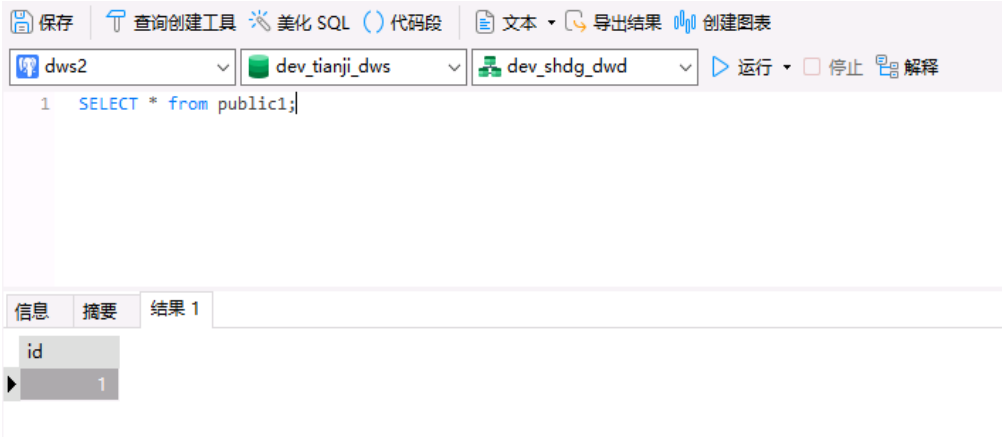
图 4-18 连接数据库



步骤2 配置相关数据库和schema信息。选择数据库：dev_tianji_dws；公共schema：dev_shdg_dwd。

验证结果：开发利用方人员拥有公共接入schema下表的SELECT权限。

图 4-19 配置相关数据库和 schema 信息



验证结果：开发利用方人员不具有公共接入schema下表的INSERT权限。

图 4-20 验证结果

----结束

5 修订记录

表 5-1 修订记录

发布日期	修订记录
2024-10-23	第一次正式发布。