

云数据库 GaussDB

最佳实践

文档版本 01
发布日期 2024-03-21



版权所有 © 华为云计算技术有限公司 2024。保留一切权利。

非经本公司书面许可，任何单位和个人不得擅自摘抄、复制本文档内容的部分或全部，并不得以任何形式传播。

商标声明



HUAWEI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云计算技术有限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，华为云计算技术有限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。

华为云计算技术有限公司

地址：贵州省贵安新区黔中大道交兴功路华为云数据中心 邮编：550029

网址：<https://www.huaweicloud.com/>

目录

1 概览	1
2 Oracle 迁移至 GaussDB 最佳实践	2
2.1 概述.....	2
2.2 资源规划.....	4
2.3 操作流程.....	6
2.4 创建 VPC 和安全组.....	6
2.5 创建 GaussDB 实例.....	9
2.6 迁移前构造数据.....	11
2.7 迁移数据库.....	17
2.8 迁移后进行数据校验.....	25
3 GaussDB 安全最佳实践	29
3.1 概要.....	29
3.2 安全介绍.....	29
3.2.1 相关最大连接数配置.....	29
3.2.2 安全认证配置.....	29
3.2.3 用户密码的安全策略.....	30
3.2.4 权限管理.....	30
3.2.5 数据库审计.....	31
3.2.6 WAL 归档配置.....	31
3.2.7 备份管理.....	31

1 概览

本手册基于GaussDB数据库实践所编写，用于指导您完成相关设置，购买更符合业务的数据库实例。

章节名称	简介
Oracle迁移至GaussDB最佳实践	介绍通过DRS的实时同步功能将本地Oracle数据库实时迁移至华为云GaussDB。
GaussDB安全最佳实践	介绍GaussDB提供的多种安全能力，提高对GaussDB资源的整体安全防御能力，保护存储的数据不泄露、不被篡改，以及数据传输过程中不泄露、不被篡改。

2 Oracle 迁移至 GaussDB 最佳实践

2.1 概述

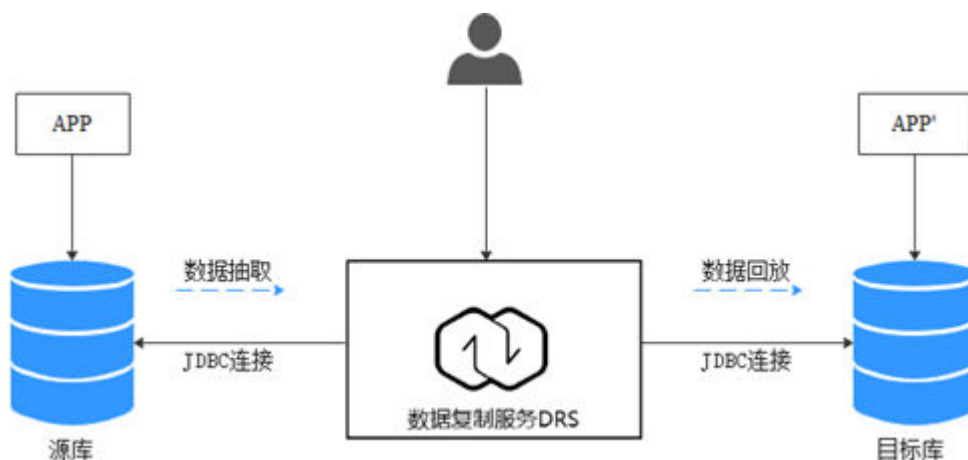
场景描述

本实践使用DRS的实时同步功能将本地Oracle数据库实时迁移至华为云GaussDB。通过全量+增量同步，实现源数据库Oracle和目标数据库GaussDB的数据长期同步。

解决问题

- 企业业务高速发展，传统数据库扩容性差，迫切需要分布式化改造。
- 传统数据库需要自购并安装服务器、系统、数据库等软件，运维成本高、难度大。
- 传统数据库性能瓶颈问题，复杂查询性能较差。
- 如何不中断业务并且平滑的实现数据迁移。

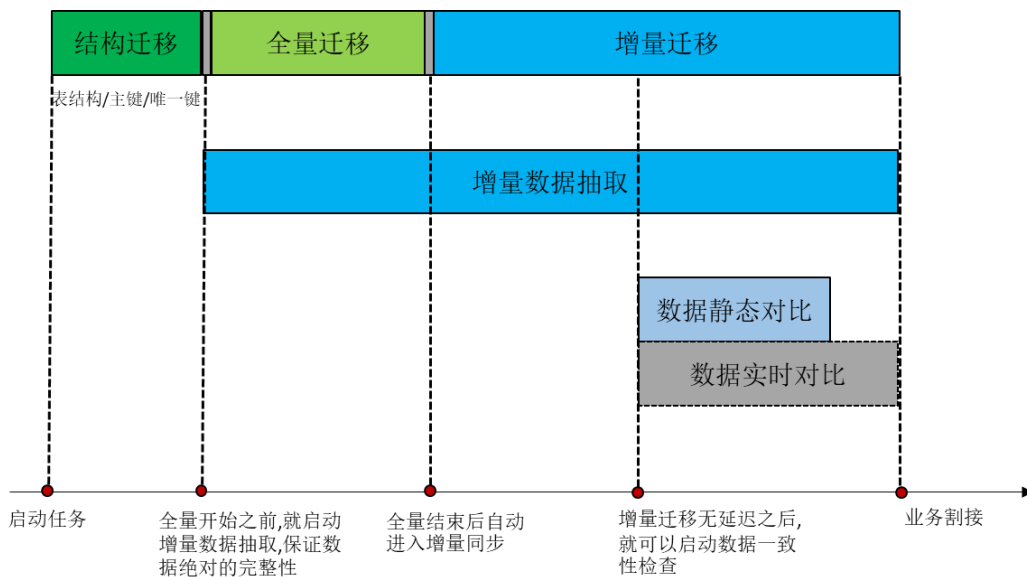
业务架构图



迁移原理

本次实践使用全量+增量同步功能，原理如下：

1. 全量同步阶段，先进行结构迁移，例如表、主键、唯一键的迁移。
2. 结构迁移完成后，启动增量数据抽取，以确保全量数据同步期间的增量数据完整的抽取到DRS实例。
3. 启动全量迁移任务。
4. 全量迁移完成后自动进入增量同步，从全量迁移开始抽取的位点开始回放。
5. 当增量回放全部完成后，启动比对任务进行一致性检查，支持实时比对。
6. 实时比对数据一致时，可以启动业务割接。



服务列表

- 虚拟私有云 VPC
- 云数据库 GaussDB
- 数据复制服务 DRS
- 数据管理服务 DAS

使用说明

- 本实践的资源规划仅作为演示，实际业务场景资源以用户实际需求为准。
- 本实践端到端的数据为测试数据，仅供参考。
- 全量同步可以实现数据迁移；增量同步可以实现实时同步源端和目标端两个库之间的数据。

前提条件

- 拥有华为云实名认证账号。
- 账户余额大于等于0元。
- 如果测试使用，需要自行在本地搭建Oracle数据库。

- 已知待迁移Oracle数据库的IP地址，端口，账户和密码。

2.2 资源规划

表 2-1 资源规划

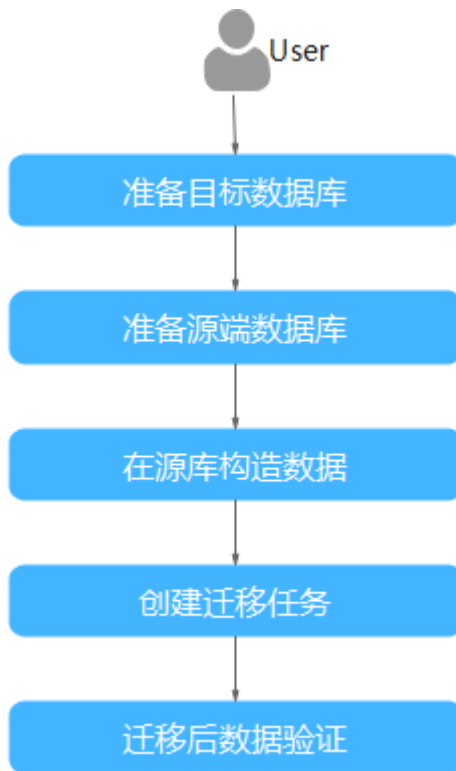
类别	子类	规划	备注
VPC	VPC名称	vpc-src-172	自定义，易理解可识别。
	所属Region	测试Region	现网实际选择时建议选择和自己业务区最近的Region，减少网络时延。
	可用区	可用区3	-
	子网网段	172.16.0.0/16	子网选择时建议预留足够的网络资源。
	子网名称	subnet-src-172	自定义，易理解可识别。
本地Oracle数据库	名称	orcl	自定义，易理解可识别。
	规格	16vCPUs 32GB	-
	数据库版本	11.2.0.1	-
	数据库用户	test_info	可以自定义用户，但是迁移时最小权限为：CREATE SESSION,SELECT ANY TRANSACTION, SELECT ANY TABLE, SELECT ANY DICTIONARY, EXECUTE_CATALOG_ROLE
GaussDB	实例名	Auto-drs-gaussdbv5-tar-1	自定义，易理解可识别。
	数据库版本	GaussDB 3.226企业版	-
	实例类型	分布式版，3CN，3DN，3副本	本示例中为分布式实例。
	部署形态	独立部署	-
	事务一致性	强一致性	-
	分片数量	3	-

类别	子类	规划	备注
	协调节点数量	3	-
	存储类型	超高IO	-
	可用区	可用区2	本示例中选择了单可用区，实际建议选择多可用区，以提高实例的高可用性。
	性能规格	独享型（1:8）8 vCPUs 64GB	本示例中为测试实例，选择较小的测试规格，实际选择规格以业务诉求为准。
	存储空间	480G	本示例中为测试实例，选择较小的存储空间，实际选择存储空间大小以业务诉求为准。
	加密磁盘	不加密	本示例中选择磁盘不加密，选择加密后会提高数据安全性，但对数据库读写性能有少量影响，实际请按照业务使用策略进行选择。
DAS登录数据库	数据库引擎	GaussDB	-
	数据库来源	GaussDB	勾选本示例中创建的GaussDB实例
	数据库名称	postgres	-
	登录用户名	root	-
	密码	-	本示例中创建的GaussDB实例root用户密码
DRS迁移任务	迁移任务名	DRS-test-info	自定义。
	目标库名称	test_database_info	自定义，易理解可识别，但是需要确保兼容模式为Oracle模式。
	源数据库引擎	Oracle	-
	目标数据库引擎	GaussDB	-
	网络类型	公网网络	本示例中采用公网网络。

2.3 操作流程

本实践的主要任务流如图2-1所示：


图 2-1 操作流程



2.4 创建 VPC 和安全组

创建VPC和安全组，为创建GaussDB实例准备网络资源和安全组。

创建 VPC

- 步骤1** 登录[华为云控制台](#)。
- 步骤2** 单击管理控制台左上角的 ，选择区域。
- 步骤3** 单击左侧的服务列表图标，选择“网络 > 虚拟私有云 VPC”。
进入虚拟私有云信息页面。
- 步骤4** 单击“创建虚拟私有云”购买VPC。

基本信息

区域
不同区域的资源之间内网不互通。请选择靠近您客户的区域，可以降低网络时延、提高访问速度。

名称

IPv4网段 · · · /
建议使用网段: 10.0.0.0/8-24 (选择) 172.16.0.0/12-24 (选择) 192.168.0.0/16-24 (选择)

高级配置 ▾ 标签 | 描述

默认子网

可用区 ⓘ

名称

子网IPv4网段 · · · / ⓘ 可用IP数: 251
子网创建完成后，子网网段无法修改

子网IPv6网段 开启IPv6 ⓘ

关联路由表 默认 ⓘ

高级配置 ▾ 网关 | DNS服务器地址 | DHCP租约时间 | 标签 | 描述

步骤5 单击“立即创建”。


步骤6 返回VPC列表，查看创建VPC是否创建完成。

当VPC列表的VPC状态为“可用”时，表示VPC创建完成。

----结束

创建安全组

步骤1 登录[华为云控制台](#)。

步骤2 单击管理控制台左上角的 ，选择区域。

步骤3 单击左侧的服务列表图标，选择“网络 > 虚拟私有云”。

进入虚拟私有云信息页面。

步骤4 选择“访问控制 > 安全组”。

步骤5 单击“创建安全组”。

步骤6 填写安全组名称等信息。

创建安全组

* 名称

* 企业项目 [新建企业项目](#) ?

* 模板

描述

通用Web服务器，默认放通22、3389、80、443端口和ICMP协议。适用于需要远程登录、公网ping及用于网站服务的云服务器场景。

 0/255

[查看模板规则](#) ▼

步骤7 单击“确定”。

步骤8 返回安全组列表，单击安全组名称“sg-01”。

步骤9 选择“入方向规则”，单击“添加规则”。

基本信息 | **入方向规则** | 出方向规则 | 关联实例

步骤10 配置入方向规则，添加源库的IP地址。

添加加入方向规则 教我设置 ×

1 安全组规则对不同规格的云服务器生效情况不同，为了避免您的安全组规则不生效，请查看安全组规则限制。

安全组 default

如您要添加多条规则，建议单击 [导入规则](#) 以进行批量导入。

优先级	策略	协议端口	类型	源地址	描述	操作
1-100	允许	基本协议/自定义TCP 例如：22或22,24或22-30	IPv4	IP地址 0.0.0.0/0		复制 删除

+ 增加1条规则


确定 取消

----结束

2.5 创建 GaussDB 实例

本章节介绍创建GaussDB实例，作为迁移任务目标库。

步骤1 登录[华为云控制台](#)。

步骤2 单击管理控制台左上角的 ，选择区域。

步骤3 单击左侧的服务列表图标，选择“数据库 > 云数据库 GaussDB”。

步骤4 在左侧导航栏选择GaussDB > 实例管理。

步骤5 单击“购买数据库实例”。

步骤6 参考[图1](#)，配置实例名称，选择计费模式、产品类型、数据库引擎版本、实例类型、事务一致性、分片数量、协调节点数量和可用区。

图 2-2 基本信息

计费模式 包年/包月 按需计费 ?

区域 ?
不同区域的资源之间内网不互通。请选择靠近您客户的区域，可以降低网络时延、提高访问速度。

实例名称 ?

产品类型 企业版 基础版

数据库引擎版本 8.102 3.226

实例类型 分布式版 主备版 ?

部署形态 独立部署 ?

是否支持日志节点 是

事务一致性 强一致性 最终一致性 ?

副本集数量 ?

分片数量 ?

协调整节点数量 ?
协调整节点数量设为1时，只能用于测试，不能用于生产环境。

可用区 可用区一 可用区二 可用区三 可用区七 ?
只支持选择一个或者三个不同的可用区。

时区 ?

步骤7 选择实例规格。

性能规格 独享型 (1.8) 鲲鹏独享型 (1.8) ?

规格名称

- 8 vCPUs | 64 GB
- 16 vCPUs | 128 GB
- 32 vCPUs | 256 GB
- 64 vCPUs | 512 GB

当前选择实例 独享型 (1.8) | 8 vCPUs | 64 GB

存储类型 超高性能 您可以点此了解，存储类型详情

存储空间 (GB) ?
120 14,450 28,800 43,150 72,000
GaussDB给您提供相同大小的备份存储空间，超出部分将按照GaussDB的备份空间计费信息收取费用。

赠送备份空间 480 GB
免费赠送存储空间等量的备份空间，超出免费备份空间部分采用按需计费方式。
实例创建默认自动备份，数据保留7天，您可修改保留时长。

磁盘加密 不加密 加密 ?

步骤8 选择实例所属的VPC（创建VPC）和安全组（创建安全组），配置数据库端口。



步骤9 配置实例密码等信息。



步骤10 单击“立即购买”，确认信息并提交。

步骤11 返回实例列表。

当实例运行状态为“正常”时，表示实例创建完成。

----结束

2.6 迁移前构造数据

迁移前需要在源库构造一些数据类型，供迁移完成后验证数据。

DRS支持的数据类型如下所示：

表 2-2 数据类型映射关系

源库数据类型	目标库数据类型	源库数据类型做主键，同步能力	源库数据类型做非主键，同步能力	源库数据类型做主键，对比能力	源库数据类型做非主键，对比能力	备注
CHAR	character	支持	支持	支持，忽略字符前后的空格	支持，忽略字符前后的空格	-
VARCHAR	character varying	支持	支持	支持	支持	源目标库数据表示范围不同，存在精度损失。

源库数据类型	目标库数据类型	源库数据类型做主键，同步能力	源库数据类型做非主键，同步能力	源库数据类型做主键，对比能力	源库数据类型做非主键，对比能力	备注
VARCHAR2	character varying	支持	支持	支持	支持	-
NCHAR	character	支持	支持	支持，忽略字符前后的空格	支持，忽略字符前后的空格	-
NVARCHAR2	nvarchar2	支持	支持	支持	支持	-
NUMBER	numeric	支持	支持	支持	支持	-
NUMBER (6,3)	numeric(6,3)	支持	支持	支持	支持	-
NUMBER (6,0)	Integer	支持	支持	支持	支持	-
NUMBER (3)	smallint	支持	支持	支持	支持	-
NUMBER (6,-2)	integer	支持	支持	支持	支持	-
BINARY_FLOAT	real	不支持（目标库不支持做主键建表）	支持	不支持	支持	源目标库数据表示范围不同，存在精度损失。
BINARY_DOUBLE	double precision	不支持（目标库不支持做主键建表）	支持	不支持	支持	-
FLOAT	real	不支持（目标库不支持做主键建表）	支持	不支持	支持	源目标库数据表示范围不同，存在精度损失。
INT	numeric	支持	支持	支持	支持	-
INTEGER	numeric	支持	支持	支持	支持	-

源库数据类型	目标库数据类型	源库数据类型做主键，同步能力	源库数据类型做非主键，同步能力	源库数据类型做主键，对比能力	源库数据类型做非主键，对比能力	备注
DATE	date	支持	支持	不支持	支持	DRS在目标库建表时类型为date，此时源目标库数据表示范围不同，存在精度损失，不支持对比。
TIMESTAMP	timestamp(6) without time zone	支持	支持	不支持	校验到小数点后6位	源库使用限制：支持的最大精度是6。
TIMESTAMP_TZ	timestamp(6) with time zone	不支持 (源库不支持做主键建表)	支持	不支持	过滤该列	-
TIMESTAMP_LTZ	timestamp(6) with time zone	不支持 (目标库不支持做主键建表)	支持	不支持	过滤该列	-
INTERVAL_YM	interval year to month	支持	支持	不支持	不支持	增量同步不支持该类型。
INTERVAL_DS	interval day to second	支持	支持	不支持	不支持	增量同步不支持该类型。源库使用限制：支持的最大精度是6。
BLOB	bytea	不支持 (源库不支持做主键建表)	支持	不支持	过滤该列	-

源库数据类型	目标库数据类型	源库数据类型做主键，同步能力	源库数据类型做非主键，同步能力	源库数据类型做主键，对比能力	源库数据类型做非主键，对比能力	备注
CLOB	text	不支持 (源库不支持做主键建表)	支持	不支持	过滤该列	-
NCLOB	text	不支持 (源库不支持做主键建表)	支持	不支持	过滤该列	-
LONG	text	不支持 (源库不支持做主键建表)	支持	不支持	过滤该列	-
LONG_RAW	bytea	不支持 (源库不支持做主键建表)	支持	不支持	过滤该列	-
RAW	bytea	不支持 (目标库不支持做主键建表)	支持	不支持	支持	-
RowID	character varying(18)	支持	支持	支持	支持	-
BFILE	-	不支持	不支持	不支持	不支持	源库使用限制：不支持 bfile 类型。
XMLTYPE	-	不支持	不支持	不支持	不支持	源库使用限制：不支持 xmltype 类型。
UROWID	-	不支持	不支持	不支持	不支持	全量增量都不支持同步。

源库数据类型	目标库数据类型	源库数据类型做主键，同步能力	源库数据类型做非主键，同步能力	源库数据类型做主键，对比能力	源库数据类型做非主键，对比能力	备注
sdo_geometry	-	不支持	不支持	不支持	不支持	源库使用限制：不支持 sdo_geometry 类型。
NUMBER(*, 0)	numeric	支持	支持	支持	支持	-

执行如下步骤在源库构造数据：

步骤1 根据本地的Oracle数据库的IP地址，通过数据库连接工具连接数据库。

步骤2 根据DRS支持的数据类型，在源库执行语句构造数据。

1. 创建一个测试用的用户。

```
create user test_info identified by xxx;
```

test_info为本次实践创建的用户，xxx为用户的密码，请根据实际情况替换。

2. 给用户赋权。

```
grant dba to test_info;
```

3. 在当前用户下创建一个数据表。

```
CREATE TABLE test_info.DATATYPELIST(
  ID INT,
  COL_01_CHAR_____E CHAR(100),
  COL_02_NCHAR____E NCHAR(100),
  COL_03_VARCHAR___E VARCHAR(1000),
  COL_04_VARCHAR2__E VARCHAR2(1000),
  COL_05_NVARCHAR2_E NVARCHAR2(1000),
  COL_06_NUMBER____E NUMBER(38,0),
  COL_07_FLOAT_____E FLOAT(126),
  COL_08_BFLOAT____E BINARY_FLOAT,
  COL_09_BDOUBLE___E BINARY_DOUBLE,
  COL_10_DATE_____E DATE DEFAULT SYSTIMESTAMP,
  COL_11_TS_____E TIMESTAMP(6),
  COL_12_TSTZ_____E TIMESTAMP(6) WITH TIME ZONE,
  COL_13_TSLTZ____E TIMESTAMP(6) WITH LOCAL TIME ZONE,
  COL_14_CLOB_____E CLOB DEFAULT EMPTY_CLOB(),
  COL_15_BLOB_____E BLOB DEFAULT EMPTY_BLOB(),
  COL_16_NCLOB_____E NCLOB DEFAULT EMPTY_CLOB(),
  COL_17_RAW_____E RAW(1000),
```

```
COL_19_LONGRAW___E LONG RAW,  
COL_24_ROWID_____E ROWID,  
PRIMARY KEY(ID)  
);
```

4. 插入两行数据。


```
insert into test_info.DATATYPELIST  
values(4,'huawei','xian','shanxi','zhongguo','shijie',  
666,12.321,1.123,2.123,sysdate,sysdate,sysdate,sysdate,'hw','cb','df','FF','FF',  
'AAAYEVAAJAAAACrAAA');
```

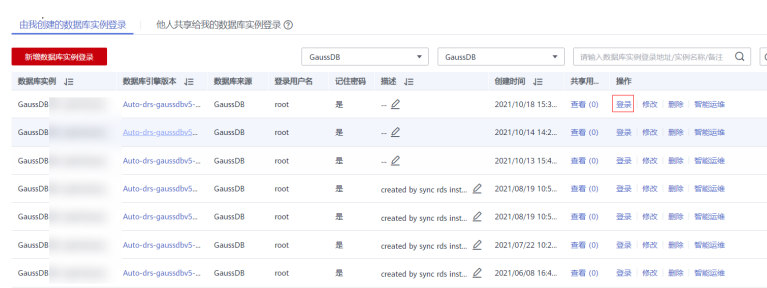
```
insert into test_info.DATATYPELIST values(2,'Migrate-  
test','test1','test2','test3','test4',  
666,12.321,1.123,2.123,sysdate,sysdate,sysdate,sysdate,'hw','cb','df','FF','FF',  
'AAAYEVAAJAAAACrAAA');
```

5. 使语句生效。

```
commit;
```

步骤3 在目标端创建库。

1. 登录[华为云控制台](#)。
2. 单击管理控制台左上角的 ，选择区域。
3. 单击左侧的服务列表图标，选择“数据库 > 数据管理服务 DAS”。
4. 在数据管理服务DAS左侧导航栏，单击“开发工具”，进入开发工具数据库登录列表页面。
5. 单击“新增数据库实例登录”，打开新增数据库实例登录窗口。
6. 选择“数据库引擎”、“数据库来源”、目标实例，填写登录用户名、密码以及描述（非必填项）信息，开启定时采集、SQL执行记录功能。
如开启“定时采集”，需勾选“记住密码”。
7. 单击“测试连接”测试连接是否成功。
如测试连接成功，将提示“连接成功”，您可继续新增操作。如测试连接失败，将提示连接失败原因，您需根据提示信息进行修改，以便新增数据库登录成功。
8. 设置完登录信息，单击“立即新增”。
9. 新增完成后，单击新增登录的“登录”，登录当前数据库。



数据库实例	引擎	数据库引擎版本	数据库来源	登录用户名	记住密码	描述	创建时间	共享组	操作
GaussDB	Auto-drs-gaussdbv5...	GaussDB	root	是	--		2021/10/18 15:3...	查看 (0)	登录 修改 删除 暂停连接
GaussDB	Auto-drs-gaussdbv5...	GaussDB	root	是	--		2021/10/14 14:2...	查看 (0)	登录 修改 删除 暂停连接
GaussDB	Auto-drs-gaussdbv5...	GaussDB	root	是	--		2021/10/13 15:4...	查看 (0)	登录 修改 删除 暂停连接
GaussDB	Auto-drs-gaussdbv5...	GaussDB	root	是		created by sync rds inst...	2021/08/19 10:5...	查看 (0)	登录 修改 删除 暂停连接
GaussDB	Auto-drs-gaussdbv5...	GaussDB	root	是		created by sync rds inst...	2021/08/19 10:5...	查看 (0)	登录 修改 删除 暂停连接
GaussDB	Auto-drs-gaussdbv5...	GaussDB	root	是		created by sync rds inst...	2021/07/22 10:2...	查看 (0)	登录 修改 删除 暂停连接
GaussDB	Auto-drs-gaussdbv5...	GaussDB	root	是		created by sync rds inst...	2021/06/08 16:4...	查看 (0)	登录 修改 删除 暂停连接

10. 选择“SQL操作” > “SQL查询”进入SQL查询页面。



11. 执行如下语句创建兼容Oracle的数据库。

此例中为：test_database_info，请根据实际情况选择。

```
CREATE DATABASE test_database_info DBCOMPATIBILITY 'ORA';
```

----结束

2.7 迁移数据库

本章节介绍创建DRS实例，将本地Oracle上的test_info数据库迁移到GaussDB实例中test_database_info数据库中。

迁移前检查

在创建任务前，需要针对迁移条件进行手工自检，以确保您的迁移任务更加顺畅。

在迁移前，您需要参考[入云使用须知](#)获取迁移相关说明。

创建迁移任务

步骤1 登录[华为云控制台](#)。

步骤2 单击管理控制台左上角的📍，选择区域。

选择目标实例所在的区域。

步骤3 单击左侧的服务列表图标，选择“数据库 > 数据复制服务 DRS”。

步骤4 左侧导航栏选择“实时同步管理”，单击“创建同步任务”。

步骤5 配置同步实例信息。

1. 选择区域，计费模式，项目，填写任务名称。

The screenshot shows the configuration form for creating a DRS task. It includes the following fields:

- 计费模式** (Billing Mode): Radio buttons for '包年/包月' (Pay-as-you-go) and '按需计费' (Pay-as-you-go), with '按需计费' selected.
- 区域** (Region): A dropdown menu with a location pin icon and a help icon. Below it is a note: '不同区域的资源之间内网不互通。请选择靠近您业务的区域，可以降低网络时延、提高访问速度。' (Resources in different regions are not connected via the intranet. Please select a region close to your business to reduce network latency and improve access speed.)
- 项目** (Project): A dropdown menu.
- * 任务名称** (Task Name): A text input field containing 'DRS-7176' and a help icon.
- 描述** (Description): A text area with a help icon and a character count '0/256' at the bottom right.

- 配置同步实例信息，选择“数据流动方向”、“源数据库引擎”、“目标数据库引擎”、“网络类型”、“DRS任务类型”、“目标数据库实例”、“同步实例所在子网”、“同步模式”、“指定公网IP”（网络类型选择公网网络时需要配置该参数）、“规格类型”、“可用区”和“企业项目”，选填“标签”。

同步实例信息 ^①

以下信息确认后不可修改，请谨慎填写，以免因为配置项错误，需要重新创建任务。

* 数据流动方向 入云 出云 自建-自建 ^①

DRS要求源数据库和目标数据库中至少有一方为本云数据库实例。入云指目标数据库为本云数据库实例之间的同步，请选择入云。

* 源数据库引擎 MySQL Oracle DB2 for LUW DDM MariaDB MongoDB PostgreSQL Microsoft SQL Server GaussDB(for MySQL) TiDB

* 目标数据库引擎 MySQL DDM GaussDB(DWS) GaussDB 分布式版 GaussDB 主备版 PostgreSQL GaussDB(for MySQL)

* 网络类型 ^①

DRS将会自动为DRS实例指定弹性公网IP。该任务结束后将自动删除弹性公网IP。指定公网IP时，具体数据同步费用请参考弹性公网IP服务的计价标准。

* DRS任务类型 单AZ 双AZ

采用单个节点部署架构，与多AZ部署方式相比，每个任务只创建一个节点，但具有高性价比。适用于业务数据量较小、短期同步，并对中断时间无严格要求的场景。

* 目标数据库实例

* 同步实例所在子网 ^①

* 同步模式 全量-增量 全量 增量 ^①

该模式为数据增量实时同步，通过全量过程完成目标数据库的初始化后，增量同步阶段通过解析日志等技术，将源库和目标数据库保持数据持续一致。

* 指定公网IP

* 规格类型 极小 小 中 大 超大

极小规格最高同步性能可达300行/秒，小规格最高同步性能可达3000行/秒，中规格最高同步性能可达7500行/秒，大规格最高同步性能可达10000行/秒，超大规格最高同步性能可达20000行/秒。

* 可用区 可用区1 可用区2 可用区3 可用区7

DRS实例将创建在此可用区，选择源或目标库所在的可用区性能更优。

* 企业项目 ^①

标签 ^① ^②

如果您需要使用同一标签标识多种云资源，即所有服务均可在标签输入框下拉选择同一标签，建议在TMS中创建预定义标签。 ^① ^②

在下方键值输入框输入内容后单击添加，即可将标签加入此处。

您还可以添加20个标签。

- 单击“开始创建”。

步骤6 配置源库及目标库信息。

- 选择“是否配置自建DNS服务”、填写源库的IP、端口、用户、密码等信息。填写完成后，需要单击“测试连接”，测试连接信息是否正确。

自建DNS服务配置 ?

是否配置自建DNS服务

源库信息

选择连接信息 查看不可选连接信息

不支持数据库参数和系统数据库迁移，源数据库参数设置和用户、作业将不会迁移至目标数据库中，请在目标数据库中使用参数组修改参数，手工导出导入用户和作业。

IP地址或域名
对于RAC集群，建议使用SCANIP+SERVICE_NAME方式创建任务，提高访问性能。 ?

端口

数据库服务名 Service Name ?

PDB名称 ?

数据库用户名

数据库密码

SSL安全连接

如启用SSL安全连接，请在源库开启SSL，并确保相关配置正确，并上传SSL证书

加密证书 选择文件

测试连接 待实例创建成功后再进行测试连接

2. 填写目标库的账户和密码。
填写完成后，需要单击“测试连接”，测试连接信息是否正确。

目标库信息

数据库实例名称

数据库用户名

数据库密码

测试连接 待实例创建成功后再进行测试连接

3. 单击“下一步”，仔细阅读提示内容后，单击“同意，并继续”。

提示 ×

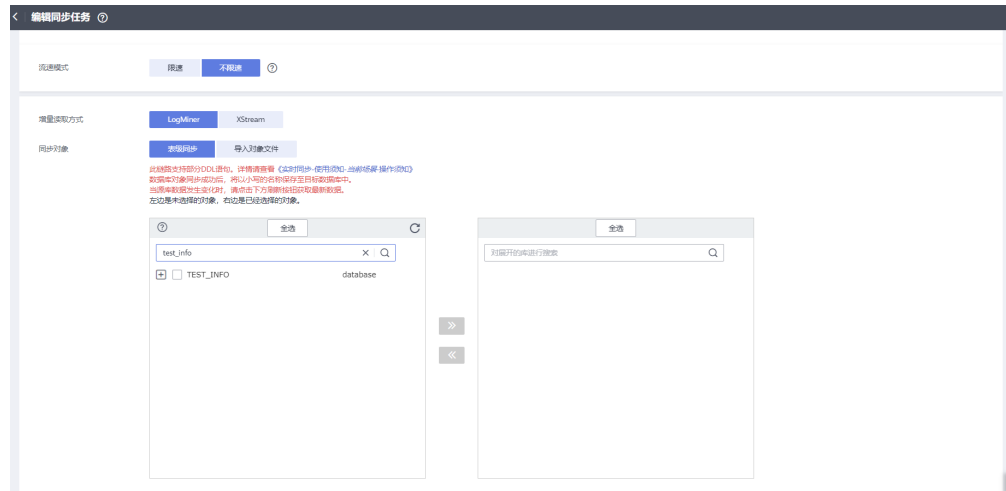
我同意本次任务临时收集和使用涉及的数据库的IP地址或域名、端口、用户名和密码。上述信息将被暂存，直至该任务删除后清除。

同意，并继续

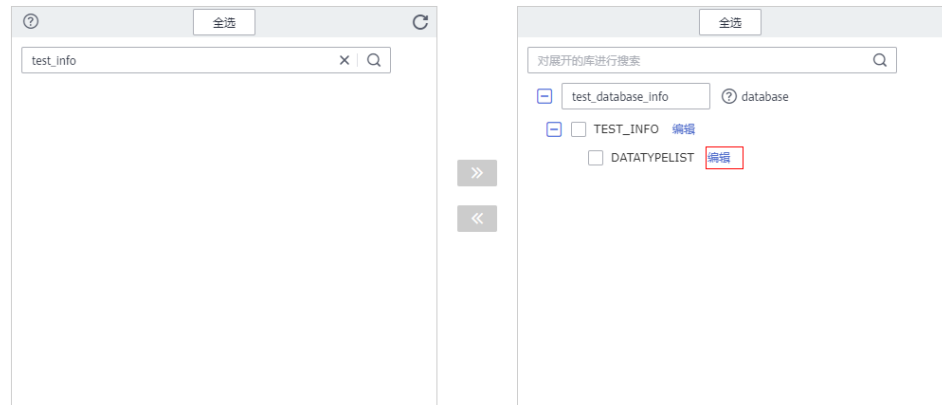
不同意

步骤7 设置同步。

1. 在源库选择需要迁移的数据库和表。本次实践中选择“test_info”中的“DATATYPELIST”表。



2. 选择完成后，可以设置迁移后是否重新命名库名和表名。



3. 本次实践将表名重新命名为“DATATYPELIST_After”。
注意重新命名时不要使用特殊符号，否则会导致迁移后执行SQL语句报错。

新表名

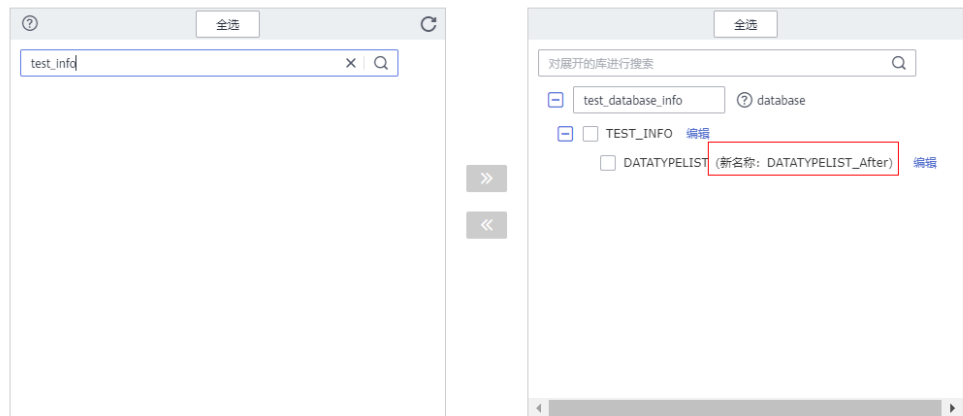
编辑表名后，目标数据库的表名为修改后的名称。

编辑表名

是

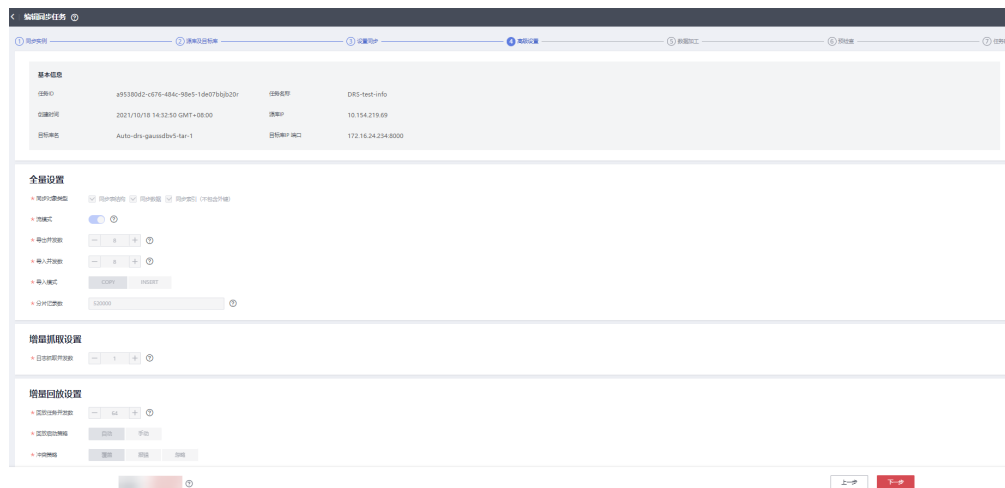
否

4. 确认重命名设置内容，单击“下一步”。



步骤8 高级设置。

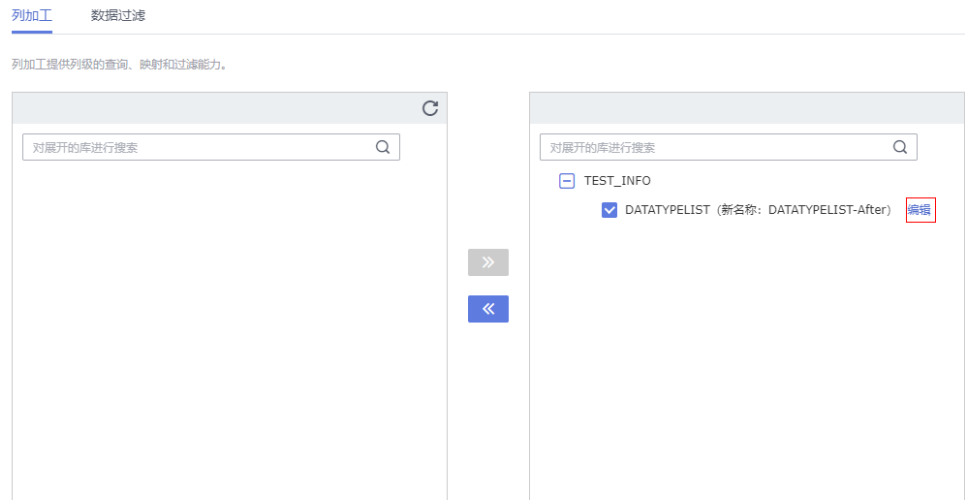
本页面内容仅做确认，无法修改，确认完成后单击“下一步”。



步骤9 数据加工。

在该页面可以对迁移的表进行加工。包括选择迁移的列，重新命名迁移后的列名，本次实践将“COL_01_CHAR_____E”重新命名为“new-line”。

1. 选择需要加工的表。



2. 编辑“COL_01_CHAR____E”列。

编辑列

i 编辑列名后，目标数据库的列名为修改后的名称。
注意：只有勾选的列才会被同步。

库名: TEST_INFO 表名: DATATYPELIST

<input checked="" type="checkbox"/> 列名	新列名	类型	约束类型
<input type="checkbox"/> ID		NUMBER	主键
<input checked="" type="checkbox"/> COL_01_CHAR____E		CHAR	
<input checked="" type="checkbox"/> COL_02_NCHAR____E			
<input checked="" type="checkbox"/> COL_03_VARCHAR____E			
<input checked="" type="checkbox"/> COL_04_VARCHAR2____E		VARCHAR2	
<input checked="" type="checkbox"/> COL_05_NVARCHAR2____E		NVARCHAR2	
<input checked="" type="checkbox"/> COL_06_NUMBER____E		NUMBER	
<input checked="" type="checkbox"/> COL_07_FLOAT____E		FLOAT	

编辑列名

3. 将“COL_01_CHAR____E”重新命名为“new-line”，单击“确定”。

编辑列

i 编辑列名后，目标数据库的列名为修改后的名称。
注意：只有勾选的列才会被同步。

库名: TEST_INFO 表名: DATATYPELIST

<input checked="" type="checkbox"/> 列名	新列名	类型	约束类型
<input type="checkbox"/> ID		NUMBER	主键
<input checked="" type="checkbox"/> COL_01_CHAR____E	new-line	CHAR	
<input checked="" type="checkbox"/> COL_02_NCHAR____E		NCHAR	
<input checked="" type="checkbox"/> COL_03_VARCHAR__E		VARCHAR2	
<input checked="" type="checkbox"/> COL_04_VARCHAR2__E		VARCHAR2	
<input checked="" type="checkbox"/> COL_05_NVARCHAR2_E		NVARCHAR2	
<input checked="" type="checkbox"/> COL_06_NUMBER____E		NUMBER	
<input checked="" type="checkbox"/> COL_07_FLOAT____E		FLOAT	

4. 单击“下一步”。

步骤10 预检查。

1. 所有配置完成后，进行预检查，确保迁移成功。

编辑迁移任务

① 逐步实例 ② 源实例目标库 ③ 配置映射 ④ 数据设置 ⑤ 数据加工 ⑥ 预检查

基本信息

任务ID	a95380d2-c676-484c-98e5-1de07bbjb20r	任务名称	DRS-test-info
创建时间	2021/10/18 14:32:50 GMT+08:00	源库IP	10.154.219.69
目标库名	Auto-drs-gaussdbv5-tar-1	目标库IP 端口	172.16.242.34:8000

预检查

预检查通过率 0% 提示：所有检查项的通过率均为“通过”，默存在“错误”时，需要查看任务日志才可进行详细操作。

检查项	检查结果
数据性参数检查	
源库表字段数据类型	正在检查
目标库表字段数据类型匹配度	正在检查
源库表字段数据类型匹配度	正在检查
目标库可用连接数是否充足	正在检查
目标库对象一致性检查	正在检查
目标库是否支持分区表的副本	正在检查
源库外键检查	正在检查
源库无主键表检查	正在检查
源库表字段数据类型支持	正在检查
源库可用连接数是否充足	正在检查
源库数据类型检查	正在检查

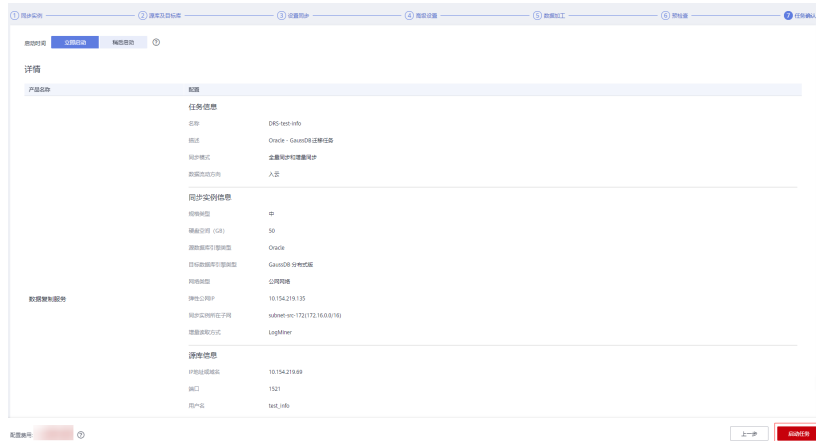
2. 对于未通过的项目，根据检查结果中的提示信息修复，修复完成后，单击“重新校验”，直到预检查通过率为100%。



3. 预检查全部通过后，单击“下一步”。

步骤11 任务确定。


1. 检查所有配置项是否正确。




2. 单击“启动任务”，仔细阅读提示后，勾选“我已阅读启动前须知”。

3. 单击“启动任务”，完成任务创建。

启动前须知

 1、同步过程中，请不要通过控制台对目标实例进行其它操作，例如重启、修改参数组等，否则会影响同步任务。启动任务前，请仔细阅读[同步前须知](#)，遵循该指引可以有效确保同步的稳定性。

 异常状态超过14天，通常任务已无法续传，任务将会自动结束，请密切关注监控告警，并及时处理和修复任务，避免长时间异常后无法断点续传和恢复。

我已阅读启动前须知

启动任务

步骤12 任务创建成功。

任务创建成功后，返回任务列表查看创建的任务状态。



名称/ID	注	状态	进度	是否计费中	数据流动方向	数据传输引擎	注	同步模式	创建时间	网络类型	描述	操作
DRS-test-info		启动中	--	否	入云	Oracle-GaussDB...		全量 + 增量	2021/10/18 14:32:50 GM...	公网网络	Oracle - GaussDB...	续传
1894595-4124-4386-9880-41...		已完成	--	否	入云	Oracle-GaussDB...		全量 + 增量	2021/10/13 22:45:01 GM...	VPN 专...	Auto-RACLEDOPE...	删除

----结束

2.8 迁移后进行数据校验

当任务状态变为“增量同步”，说明全量同步已经完成，全量同步完成后，登录 GaussDB 查看数据迁移结果。

步骤1 等待迁移任务状态变为“增量同步”。

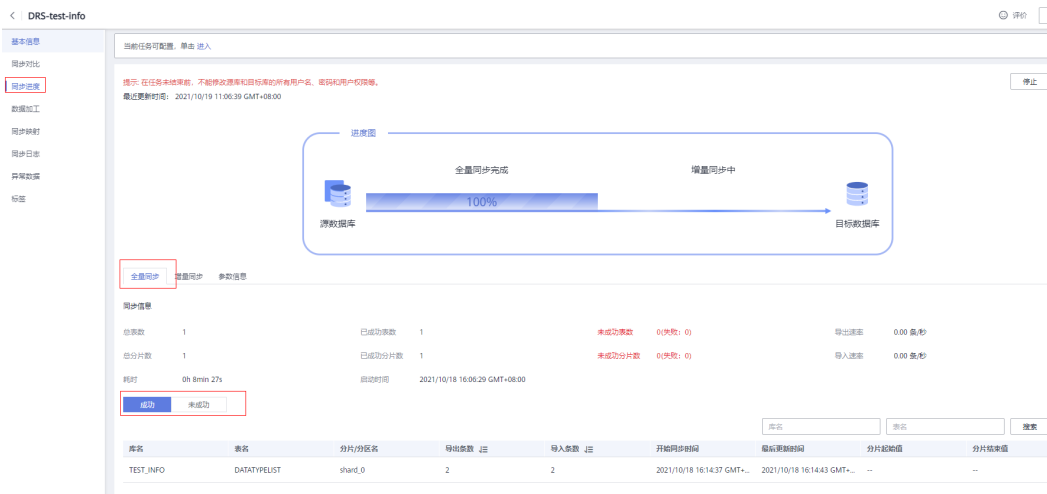


<input type="checkbox"/>	DRS-test-info	69c6b78d-f3fd-4348-8010-2ea...	增量同步	11.51s	否	入云	Or
--------------------------	---------------	--------------------------------	------	--------	---	----	----

步骤2 单击任务名称，进入任务详情页。

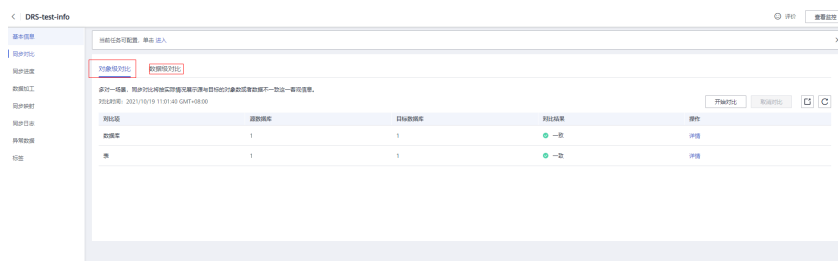
步骤3 在“同步进度”页签查看全量同步结果。

如图所示，本次实践将 TEST_INFO 库中 DATATYPELIST 表迁移至 shard_0，共迁移了两条数据。

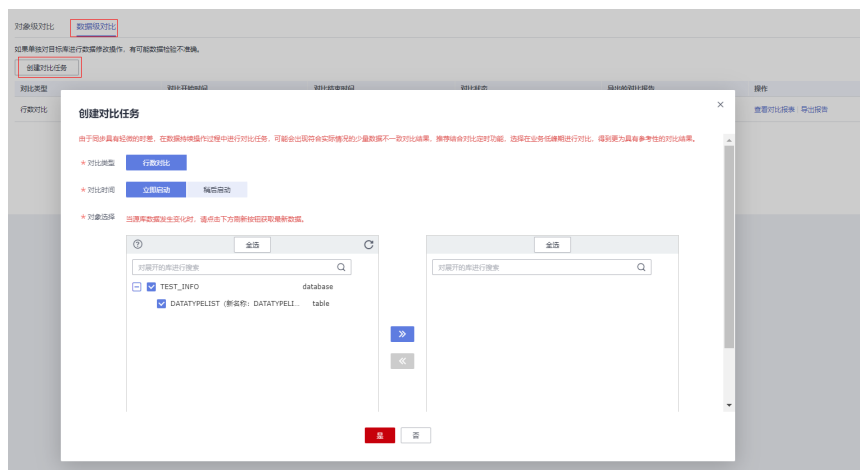


步骤4 验证数据一致性。

1. 在“同步对比 > 对象级对比”页面，查看库和表的迁移结果。



2. 在“同步对比 > 数据级对比”页面，创建对比任务，查看表中行的迁移结果。



步骤5 通过DAS连接GaussDB的目标库“test_database_info”。

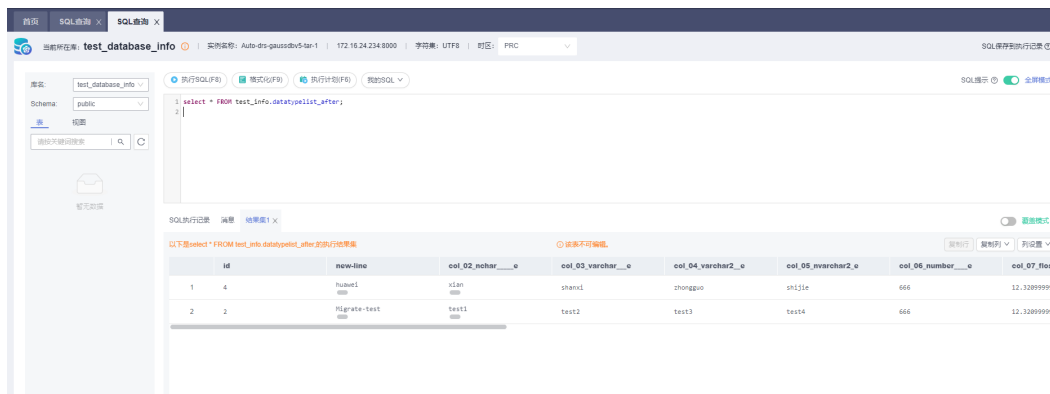
DAS连接实例的方法请参考[新增数据库登录](#)。

步骤6 执行如下语句，查询全量同步结果。

```
SELECT * FROM test_info.datatypeplist_after;
```

Oracle数据库中的模式迁移完成后，会在GaussDB库中作为Schema，所以查询语句中添加Schema精确查询。

如图所示，查询表中的各个数据类型都迁移成功，并且数据正确无误。



步骤7 验证增量同步。

由于本次实践为“全量+增量”同步模式，全量同步完成后，如果在创建任务后有数据写入，这些写入的数据会一直同步至目标库中，直到任务结束。下面我们模拟写入另外的数据。

1. 根据本地的Oracle数据库的IP和地址，通过数据库连接工具连接数据库。
2. 执行如下语句，在源库插入一条数据。

我们插入一条“id”为1的数据。

```
insert into test_info.DATATYPELIST values(1,'Migrate-test','test1','test2','test3','test4',666,12.321,1.123,2.123,sysdate,sysdate,sysdate,sysdate,'hw','cb','df','FF','FF','AAAYEVAJAAACrAAA');
commit;
```

3. 在目标库执行如下语句查询结果。
SELECT * FROM test_info.datatypeplist_after;

如图所示，在源库新增的数据，可以实时同步至目标库。

步骤8 结束迁移任务。

根据业务情况，待业务完全迁移至目标库，可以结束当前任务。

1. 单击“操作”列的“结束”。

名称ID	状态	编辑	显示计算中	数据库活动方向	数据库引擎	同步模式	创建时间	网络类型	描述	操作
DRS-test-info 09020760-4248-4248-8070-2aa...	C 迁移同步	4.6s	否	入云	Oracle-GaussDB...	全量+增量	2021/10/18 15:47:59 GMT...	公网网络	源库中地址或域名...	编辑 结束

2. 仔细阅读提示后，单击“是”，结束任务。

结束任务



确定结束以下任务吗？

名称	状态
DRS-test-info	增量同步



强制结束会优先终止迁移任务。



因xstream任务在源库打开了一个xstream outbound，任务释放时请在源库执行“BEGIN DBMS_XSTREAM_ADM.DROP_OUTBOUND(server_name => '<server_name>');END;”以释放该xstream outbound，[参考链接](#)

强制结束任务

结束任务说明：

· 该任务结束后将无法恢复。

是

否

步骤9 迁移完成后，进行性能测试。

测试云数据库GaussDB性能的方法请参见[性能白皮书](#)。

----结束

3 GaussDB 安全最佳实践

3.1 概要

安全性是华为云与您的共同责任。华为云负责云服务自身的安全，提供安全的云；作为租户，您需要合理使用云服务提供的安全能力对数据进行保护，安全地使用云。详情请参见[责任共担](#)。

本文提供了GaussDB使用过程中的安全最佳实践，旨在为提高整体安全能力提供可操作的规范性指导。根据该指导文档您可以持续评估GaussDB的安全状态，更好的组合使用GaussDB提供的多种安全能力，提高对GaussDB的整体安全防御能力，保护存储在GaussDB的数据不泄露、不被篡改，以及数据传输过程中不泄露、不被篡改。

3.2 安全介绍

3.2.1 相关最大连接数配置

如果GaussDB连接数过高，会消耗服务器大量资源，导致操作响应变慢，参考以下几个参数进行优化，具体内容请参见[连接设置](#)：

- `max_connections`：允许和数据库连接的最大并发连接数，此参数会影响集群的并发能力。
- `max_inner_tool_connections`：允许和数据库连接的工具有的最大并发连接数，此参数会影响GaussDB的工具连接并发能力。
- `sysadmin_reserved_connections`：为管理员用户预留的最少连接数，不建议设置过大。该参数和`max_connections`参数配合使用，管理员用户的最大连接数等于`max_connections + sysadmin_reserved_connections`。

该参数属于POSTMASTER类型参数，具体内容请参见[设置参数](#)中对应设置方法进行设置。

3.2.2 安全认证配置

为了保证用户体验，同时为了防止账户被人通过暴力破解，GaussDB设置了账户登录重试次数及失败后自动解锁时间的保护措施，GaussDB针对账户提供了以下能力：

- failed_login_attempts: 允许用户设置最大登录失败次数。
- password_lock_time: 此参数允许用户修改账户被锁定后自动解锁时间, 单位为天。

若管理员发现某账户被盗、非法访问等异常情况, 可手动锁定该账户。当管理员认为账户恢复正常后, 可手动解锁该账户。

以手动锁定和解锁用户joe为例, 命令格式如下:

- 手动锁定

```
gaussdb=# ALTER USER joe ACCOUNT LOCK;  
ALTER ROLE
```
- 手动解锁

```
gaussdb=# ALTER USER joe ACCOUNT UNLOCK;  
ALTER ROLE
```

3.2.3 用户密码的安全策略

GaussDB为了客户账号的安全, GaussDB对用户密码进行了以下设置:

- 用户密码存储在系统表pg_authid中, 为防止用户密码泄露, GaussDB对用户密码进行加密存储, 所采用的加密算法由配置参数password_encryption_type决定。
- GaussDB数据库用户的密码都有密码有效期, 可以通过参数password_notify_time提醒客户修改密码, 如果需要修改密码有效期, 可以通过修改password_effect_time来更改。

3.2.4 权限管理

- 虚拟私有云可以为GaussDB实例构建隔离的、用户自主配置和管理的虚拟网络环境。子网提供与其他网络隔离的、可以独享的网络资源, 以提高网络安全性, 可以使用IAM为企业中的员工设置不同的访问权限, 以达到不同员工之间的权限隔离, 通过IAM进行精细的权限管理。具体内容请参见[权限管理](#)。
- 保障数据库的安全性和稳定性在使用数据库实例之前务必先设置安全组, 具体内容请参见[设置安全组规则](#)。
- 为防止PUBLIC拥有CREATE权限, 导致数据库任何账户都可以在PUBLIC模式下创建表或者其他数据库对象, 其他用户也可以修改这些数据, 可以如下SQL语句来查询:

```
SELECT CAST(has_schema_privilege('public','public','CREATE') AS TEXT);
```

- 如果返回为TURE, 执行如下SQL语句进行修复:

```
REVOKE CREATE ON SCHEMA public FROM PUBLIC;
```

- PUBLIC角色属于任何用户, 如果将对象的所有权限授予PUBLIC角色, 则任意用户都会继承此对象的所有权限, 违背权限最小化原则, 为了保障数据库数据的安全, 此角色应该拥有尽可能少的权限。通过执行如下SQL语句来确定所有权限是否授权PUBLIC角色:

```
SELECT relname,relacl FROM pg_class WHERE (CAST(relacl AS TEXT) LIKE '%,=arwdDxt/%}' OR CAST(relacl AS TEXT) LIKE '{=arwdDxt/%}') AND (CAST(relacl AS TEXT) LIKE '%,=APmiv/%}' OR CAST(relacl AS TEXT) LIKE '{=APmiv/%}');
```

- 为空则说明已授权, 如果已授权, 可通过执行如下SQL语句来修复:

```
REVOKE ALL ON <OBJECT_NAME> FROM PUBLIC;
```

- pg_catalog模式下的pg_authid系统表中包含了数据库中的所有角色信息。由于所有用户会继承PUBLIC角色的权限, 为了防止敏感信息泄露或被更改, PUBLIC角色

不允许拥有pg_authid系统表的任何权限，执行如下SQL语句，如果查询结果显示不为空，则已经被授权：

```
SELECT relname,relacl FROM pg_class WHERE relname = 'pg_authid' AND  
CAST(relacl AS TEXT) LIKE '%,=%}';
```

- 如果已授权，通过执行如下SQL语句进行修复：

```
REVOKE ALL ON pg_authid FROM PUBLIC;
```

- 普通用户指用于执行普通业务操作的非管理员用户。作为普通用户，不应该拥有超出其正常权限范围的管理权限，例如创建角色权限，创建数据库权限，审计权限，监控权限，运维权限，安全策略权限等，在满足正常业务需求的前提下，为了确保普通用户权限最小化，应撤销普通用户非必须的管理权限。
- 在创建函数时声明SECURITY DEFINER表示函数以创建它的用户权限执行，如果使用不当会导致函数执行者借助创建者的权限执行越权操作，所以一定确保这样的函数不被滥用。为了安全考虑，禁止PUBLIC角色执行SECURITY DEFINER类型的函数，执行如下SQL语句查询public角色是否有SECURITY DEFINER类型的函数：

```
SELECT a.proname, b.nspname FROM pg_proc a, pg_namespace b where  
a.pronamespace=b.oid and b.nspname <> 'pg_catalog' and a.prosecdef='t';
```

- 如果返回非空，执行如下SQL语句检查是否有执行权限：

```
SELECT CAST(has_function_privilege('public',  
'function_name([arg_type][, ...])', 'EXECUTE') AS TEXT);
```

- 返回TRUE，则代表拥有，执行下面的SQL语句进行修复：

```
REVOKE EXECUTE ON FUNCTION function_name([arg_type][, ...])  
FROM PUBLIC;
```

- SECURITY INVOKER函数是以调用它的用户的权限来执行，使用不当会导致函数创建者借助执行者的权限执行越权操作，所以在调用非自身创建的这类函数时，一定要先检查函数执行内容，避免造成函数创建者借助执行者的权限执行了越权的操作。

3.2.5 数据库审计

- GaussDB可以记录实例相关的操作，但是仅针对支持的审计操作，请在操作前查询操作列表，具体内容请参见[支持审计的关键操作列表](#)。
- 确保配置开启数据库对象的添加、删除、修改审计，具体内容请参见[数据库审计](#)。
- 支持审计日志可视化查看，可开启LTS的能力，具体内容可参见[LTS日志](#)。

3.2.6 WAL 归档配置

WAL(Write Ahead Log)即预写式日志，也称为Xlog。wal_level决定了写入WAL的信息量。为了在备机上开启只读查询，wal_level需要在主机上设置成hot_standby，并且备机设置hot_standby参数为on。对于分布式环境，不支持设置hot_standby为off，因此wal_level不可设置为archive或minimal，否则数据库将无法启动。建议设置wal_level参数为默认值hot_standby。

3.2.7 备份管理

GaussDB支持数据库实例的备份和恢复，以保证数据可靠性。备份目前将以未加密的方式存储，防止客户误操作或者服务异常的情况下，因没有开启备份而造成数据丢失的情况，GaussDB针对备份提供了以下能力：

- 提供了自动和手动的备份功能，具体内容请参见[备份概述](#)，在创建GaussDB实例时，系统默认开启实例级自动备份策略。实例创建成功后，您可根据业务需要修改实例级自动备份策略。
- 提供了自动备份策略，定时定期对数据库进行备份。具体内容请参见[设置自动备份策略](#)。
- 提供了导出备份文件的能力，具体内容请参见[导出备份信息](#)。