云数据库 RDS for PostgreSQL

故障排除

文档版本 01

发布日期 2025-04-09

华为云计算技术有限公司

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。

目 录

1 RDS for PostgreSQL 有大量 owner 是 rdsadmin 的 schema 怎么删除

场景描述

RDS for PostgreSQL有大量owner是rdsadmin的schema，怎么删除这些schema。

原因分析

RDS for PostgreSQL中的临时表分为会话级临时表和事务级临时表。

- 在会话级临时表中，数据可以存在于整个会话的生命周期中。默认创建的是会话级别的临时表。
- 在事务级临时表中，数据只能存在于事务的生命周期中。

PostgreSQL临时表是schema下所生成的一个特殊的表，这个schema的名称为“pg_temp_n”，其中n代表数字，不同的session数字不同。

用户业务使用了大量临时表，此类临时表不能删除，删除后，也会很快被重新创建。

2 RDS for PostgreSQL 数据库创建索引时索引名可以包含 schema 名

场景描述

PostgreSQL官方标准语法里面创建索引时索引名不能包含schema名，例如“CREATE UNIQUE INDEX fee_code_desc_uni_idx”是正确的，如果增加了schema名，例如“CREATE UNIQUE INDEX "isp-1".fee_code_desc_uni_idx”就会报语法解析错误。

但是在华为云RDS for PostgreSQL 11创建索引时索引名可以包含schema名，华为云RDS for PostgreSQL 12创建索引时索引名不支持包含schema名。

原因分析

华为云RDS for PostgreSQL 11修改了create index的语法解析，增加了对index名schema的解析，所以可以包含schema名。

华为云RDS for PostgreSQL 12未做修改。

3 RDS for PostgreSQL 通过应用程序访问数据库时提示不支持身份验证

场景一

- 场景描述

  当通过PostgreSQL的任何应用程序连接到RDS for PostgreSQL数据库时，如果客户端不支持scram-sha-256身份验证方法，会出现报错：

  ```
  Authentication method not supported (Received: 10)
  ```

- 原因分析

  出现此问题的原因是使用的客户端版本较低，与数据库使用的加密算法不兼容导致的。

- 解决方案

  a. 检查客户端或客户端驱动程序（如JDBC驱动程序），确保将其更新到最新版本，以确保支持最新的身份验证方法。

  如果仍然不支持最新的身份验证，执行下一步。

  b. 在实例的参数配置中，修改“password_encryption”参数值为“md5”。

  须知

  “password_encryption”参数修改后，需要重置密码才能生效。

  c. 如果以上方式都不生效，可以**修改pg_hba**，查看是否有配置认证方式为“scram-sha-256”，如果有则修改为“md5”，保存后重试连接。

场景二

- 场景描述

  当数据库从低版本迁移到高版本后，业务无法连接数据库，报错如下：

  ```
  unsupported authentication method requested by the server: 10
  ```

- 原因分析

  低版本实例的“password_encryption”参数值为“md5”，迁移到高版本后，高版本实例的“password_encryption”参数默认值为“scram-sha-256”，重新修改参数值为“md5”，由于未重置密码，导致密码认证方式失败，业务无法连接。

- 解决方案
  “password_encryption”参数修改后，重置密码使之生效。

场景三

- 场景描述
  使用JDBC应用程序连接到RDS for PostgreSQL数据库时，由于JDBC版本过低不支持scram-sha-256身份验证，在console错误日志中出现如下报错信息：
  ```
  unsupported frontend protocol 1234.5680: server supports 2.0 to 3.0
  ```
- 原因分析
  使用JDBC连接数据库，由于JDBC版本过低，导致无法连接。
- 解决方案
  下载并使用最新版本的JDBC。

4 RDS for PostgreSQL 数据库已有连接执行业务时报错

故障描述

客户端通过已有连接执行业务时，返回如下报错信息：

- 故障一
  ```
  org.postgresql.util.PSQLException: An I/O error occurred while sending to the backend.
  ```
- 故障二
  ```
  org.postgresql.util.PSQLException: The connection attempt failed
  ...
  Caused by: java.net.SocketException: Connection reset
  ```

故障一的解决方案

原因分析：

- SQL语句参数过多
- 连接被释放

解决方案：

- 对于SQL语句参数过多的情况，需要自行排查业务，对包含较多参数SQL进行适当拆分。
- 对于连接被释放导致报错的情况，排查客户端连接相关参数，如连接超时时间。业务上建议增加自动重试机制。

故障二的解决方案

这类问题是由于已有连接被释放掉，使用已经释放的连接会出现这个报错。可能原因主要有以下几种：

- 网络链路问题
- 数据库重启或后端进程crash
- 空闲连接超时释放

解决方案：

1. 首先排查网络连通性，判断是否有网络链路因素（丢包率、重传比例高）导致连接断开。
2. 如果没有网络层面的问题，需要排查业务是否有其他报错导致连接断开。
3. 如果业务上也没有其他报错，则尝试排查连接超时参数（如jdbc连接池参数sockettimeout和connecttimeout），如果设置值较小，会导致连接被主动释放。

5 RDS for PostgreSQL 实例 inodes 过多导致数据库重启缓慢

实例inodes指标值过大，常见的原因是临时文件堆积、表对象过多。这两种情况下发生异常重启时，均会拖慢启动进程。

场景一

- 场景描述

  使用RDS for PostgreSQL数据库时，业务执行大量复杂SQL，造成临时文件堆积，内存耗尽发生OOM，数据库重启过程非常缓慢，导致业务较长时间不可用。

- 原因分析

  由于业务执行复杂SQL，如果SQL中涉及排序、Hash join、聚合等操作，超过配置work_mem参数大小时，会生成临时文件。大量执行这样的SQL，在发生OOM时，数据库进程被OS杀掉，此时内核不会对临时文件进行清理，从而导致临时文件的堆积。过多的临时文件会拖慢数据库启动，这是因为在PostgreSQL数据库进程启动时，需要删除所有之前产生的所有临时文件，如果存在大量临时文件堆积，将导致数据库启动缓慢。

- 解决方案

  建议业务侧优化SQL，或适当调大work_mem参数值（会增加内存占用），减少临时文件生成。

场景二

- 场景描述

  使用RDS for PostgreSQL数据库时，业务创建了大量的表。某一时间连接数与业务量激增，数据库进程内存耗尽发生OOM，从而导致数据库重启，但重启过程非常缓慢，导致业务较长时间不可用。

- 原因分析

  由于数据库发生了OOM进而导致进程重启，在启动时会进入故障恢复模式，这时内核进程会遍历所有表并做fsync（将os缓存内容刷新至磁盘），如果业务创建的表对象过多，在启动时便会消耗大量时间进行遍历，从而导致数据库启动缓慢，影响业务可用性。

- 解决方案
  - 建议业务侧限制创建表的数量，单实例表数量最好不超过2万，单库表数量最好不超过4千，详见**实例使用规范**。

- 建议业务侧配置内存监控，必要时扩充内存规格，尽量避免OOM发生。同时关注inode数监控指标，控制创建的对象数量。

6 RDS for PostgreSQL 创建数据库用户报错：password is easily cracked

场景描述

RDS for PostgreSQL执行创建数据库用户时报错：password is easily cracked

图 6-1 报错信息

原因分析

这是因为使用了弱密码被拦截导致的。在RDS for PostgreSQL 11.22、12.22、13.18、14.15、15.10、16.6及以上的版本中，默认开启弱密码检测。使用弱密码创建用户时，就会发生如上报错。

解决方案

- 建议使用更复杂的密码进行设置，防止密码被暴力破解。
- 如果需要关闭弱密码拦截，可以将参数“passwordcheck.rds_enable_cracklib”的值设置为“off”，从而屏蔽弱密码校验，只做最基本的规则检测。具体操作，请参见**修改RDS for PostgreSQL实例参数**。

  基本规则检测：

- 密码长度必须大于等于8
- 必须包含字母和非字母
- 密码不能包含用户名