云数据库 GaussDB

最佳实践

文档版本 01

发布日期 2025-01-22

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。

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 GaussDB 安全配置建议

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使用过程中的安全配置建议，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。

本文从以下几个维度给出建议，您可以评估GaussDB的使用情况，并根据业务需要在本指导的基础上进行安全配置。

- **最大连接数配置**
- **安全认证配置**
- **用户密码的安全策略**
- **权限管理**
- **数据库审计**
- **WAL 归档配置**
- **备份管理**

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，可以修改max_connections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。

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
```

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，如果需要修改密码有效期，可以通过修改**password_effect_time**来更改。

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TRUE，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所有的角色信息。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pubilc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。

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**。

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。

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**。

