赛题 26

openGauss 数据库支持 Python 驱动

直播导师：田文罡

openGauss定位：一款高性能、高安全、高可靠的企业级开源关系型数据库。

关于openGauss

openGauss是一款开源关系型数据库管理系统，采用木兰宽松许可证v2发行。openGauss内核源自PostgreSQL，深度融合华为在数据库领域多年的经验，结合企业级场景需求，持续构建竞争力特性。同时openGauss也是一个开源的数据库平台，鼓励社区贡献、合作。

高性能

两路鲲鹏性能150万tpmC；面向多核架构的并发控制技术；NUMA-Aware存储引擎；SQL-Bypass智能选路执行技术；面向实时高性能场景的内存引擎。

高安全

业务无忧，故障切换时间RTO＜10s；精细安全管理：细粒度访问控制、多维度审计；全方位数据保护：存储&传输&导出加密。

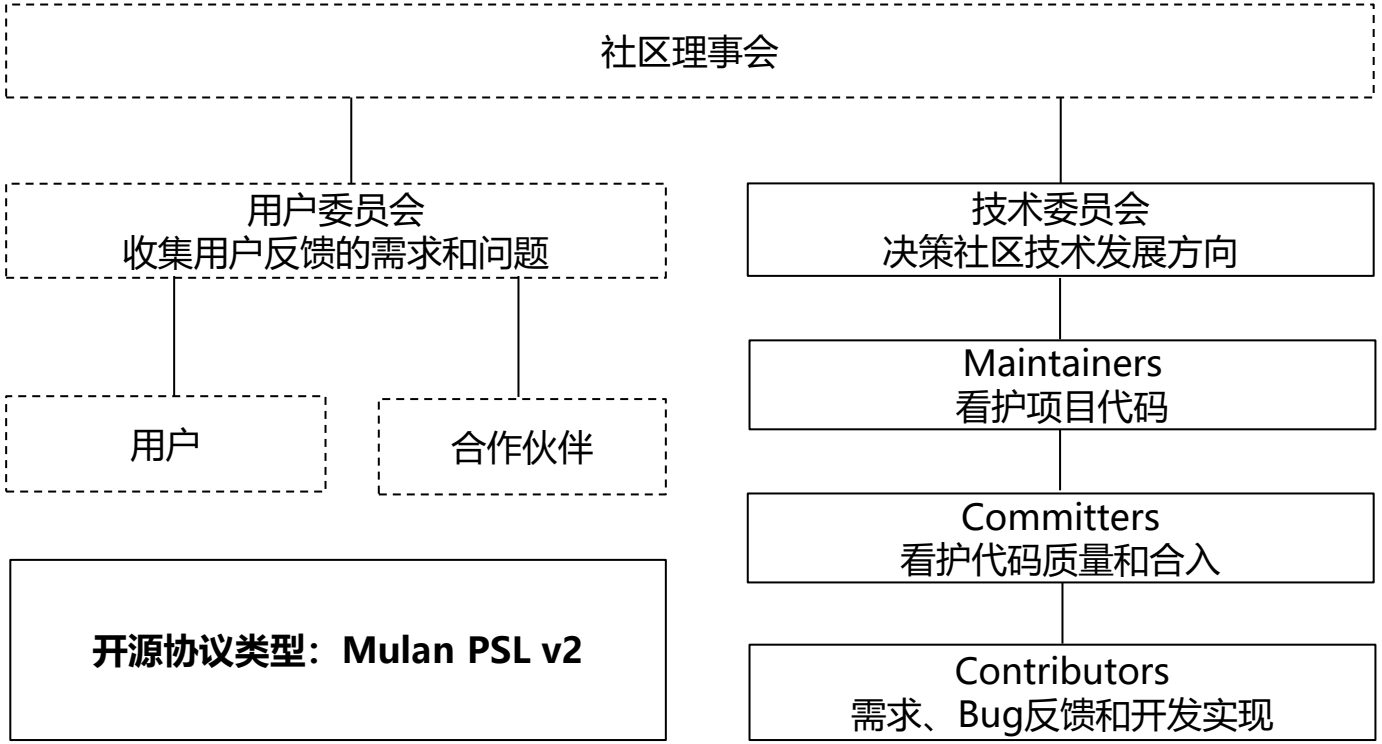
易运维

智能参数调优：结合深度强化学习和启发式算法，实现参数自动推荐；慢SQL诊断，多维性能自监控视图，实时掌控系统性能表现；提供在线自学习的SQL时间预测、快速定位、急速调优。

全开放

采用木兰宽松许可证协议，允许对代码自由修改、使用、引用；完全开放数据库内核能力，联合开发者和伙伴共同打造工具等数据库周边能力；开放伙伴认证、培训体系及高校课程。

openGauss社区组织架构



openGauss社区角色

- **TC**：Technical Committee。openGauss社区技术管理机构，提供技术决策、指导和监督。
- **SIG**：专项兴趣小组（Special Interest Groups）。包括SQLEngine、StorageEngine、Connectors、Tools、Docs、Security、Infra等。
- **Maintainer**：负责看护SIG项目架构设计、保证SIG项目代码质量，拥有SIG项目代码检视和合入代码权限；定期召集、组织社区SIG项目例会，代表SIG参加技术委员会组织的活动和特定会议。
- **Committer**：负责SIG日常运作，拥有其所属SIG项目的代码检视和合入权限。负责SIG日常运作，拥有其所属SIG项目的代码检视和合入权限，可参加Maintainer组织的SIG项目例会，并代表SIG与TC、其他SIG及用户进行交流协同。
- **Contributor**：需签署社区贡献者协议（CLA），并在openGauss社区有一个或以上被合入的Pull Request。

题目：openGauss 数据库支持 Python 驱动

1、Python是目前最为流行的全场景编程语言之一，在Web、大数据、人工智能和嵌入式开发等领域均有广泛的使用。

2、 openGauss 数据库支持 Python 驱动，使得Python语言开发应用可以使用openGauss数据库。

1、现在主流编程语言主要是C/C++，JAVA和Python。openGauss已经支持C/C++和JAVA语言驱动。支持 Python 驱动，使得openGauss数据库的开发生态更为完善。

2、题目就是为openGauss增加Python语言访问数据库的能力。

1、主要的知识点为数据库客户端和服务器通信认证的流程，SHA256算法，SSL协议认证流程，不涉及权限管理。

2、实现思路：在开源psycopg基础上进行定制开发。

3、openGauss主要对内核修改了很大改动，客户端和服务端的驱动协议修改比较少，主要是支持了SHA256等新的密码存储鉴权方式。建议以psycopg2驱动为基础进行修改，参照如下过程。

1、参照PostgreSQL 中文链接 http://www.postgres.cn/docs/10/protocol-message-types.html 看一下 前后端的通信鉴权格式。
2、配置 hab.conf 为trust，跳过认证。
3、配置hab.conf为 MD5方式，修改postgresq.conf配置文件中的 GUC参数 password_encryption_type 为 0，表示MD5密码存储方式。在这种方式下，与原来PG基本是一样，方便调通流程。可以看一下MD5认证的基本流程。
3、配置hab.conf为 sha256方式，修改postgresq.conf配置文件中的 GUC参数 password_encryption_type 为 2 表示SHA256 密码存储方式。这是openGauss新的鉴权方式。调整SHA256认证方式。
4、看看pytyon是否支持SSL认证，调试一下SSL的认证方式。
5、cert和gss不要求。
authmehod-options支持以下选项：

- trust：不验密，禁止远程主机使用trust方式访问集群
- reject：拒绝访问
- md5：md5认证，默认不支持
- sha256：sha256认证（推荐使用）
- cert：客户端证书认证
- gss：kerberos认证

password_encryption_type
参数说明：该字段决定采用何种加密方式对用户密码进行加密存储。修改此参数的配置不会自动触发已有用户密码加密方式的修改，只会影响新创建用户或修改用户密码操作。
该参数属于SIGHUP类型参数，请参考表4-134中对应设置方法进行设置。
取值范围：0、1、2

- 0表示采用md5方式对密码加密。
- 1表示采用sha256和md5两种方式分别对密码加密。
- 2表示采用sha256方式对密码加密。

1、交付件：psycopg2驱动。

2、功能就是能够支持SHA256鉴权方式，以及通过psycopg2 能够执行操作数据库的各SQL语句，并且功能正常。