

# 项目申请书

项目名称: openGauss权限扫描

项目主导师: 崔永泉 [yqcui1977@hust.edu.cn](mailto:yqcui1977@hust.edu.cn)

申请人: 陈贤文

日期: 2023年5月9日

邮箱: [mcxw@hust.edu.cn](mailto:mcxw@hust.edu.cn)

## 项目申请书

### 1.项目背景

### 2.技术方法及可行性

### 3.项目实施细节梳理

#### 3.1 探索openGauss中的访问控制模型

认证

授权

审计

#### 3.2 用户权限检查

设计用户权限检查项

开发扫描程序

实现openGauss数据库权限扫描功能

设计文档

### 4.规划

#### 1.项目研发第一阶段

#### 2.项目研发第二阶段

#### 3.项目测试和部署

## 1.项目背景

openGauss是一种高性能、高可靠、高安全性的开源数据库系统，由华为公司发起和维护。在实际应用中，由于复杂的配置和管理需求，openGauss数据库可能存在各种违规操作和安全隐患。因此，需要根据openGauss的数据库配置和用户权限，检查数据库中是否存在违规操作的可能和安全隐患。

技术要求：

- 了解openGauss的基础功能
- 了解访问控制

项目产出：

- 探索openGauss中的访问控制模型，完成技术洞察博客一篇。

2. 设计用户权限检查项，开发扫描程序，实现数据库权限扫描功能，扫描数据库中是否有违规操作的可能和安全隐患，完成设计文档。

## 2.技术方法及可行性

---

该扫描程序将基于Java语言和openGauss JDBC驱动程序实现，使用Spring Boot框架构建。

- Java语言和JDBC API：用于与openGauss数据库交互。
- Spring Boot框架：用于构建和管理Web应用程序。

对JDBC开发有项目经历，曾基于Spring Boot框架，Mybatis和Spring JDBC开发小程序，用Thymeleaf模板引擎，设计web应用。

## 3.项目实施细节梳理

---

### 3.1 探索openGauss中的访问控制模型

openGauss是一种开源的、关系型数据库管理系统，它提供了多种安全机制来控制用户对数据库资源的访问。在openGauss中，访问控制模型包括认证、授权和审计等功能。本文将探索openGauss中的访问控制模型，并编写实现细节。

#### 认证

如果主机需要远程连接数据库，必须在数据库系统的配置文件中增加此主机的信息，并且进行客户端接入认证。配置文件（默认名称为pg\_hba.conf）存放在数据库的数据目录里。hba（host-based authentication）表示是基于主机的认证。

- 本产品支持如下三种认证方式，这三种方式都需要配置“pg\_hba.conf”文件。
  - 基于主机的认证：服务器端根据客户端的IP地址、用户名及要访问的数据库来查看配置文件从而判断用户是否通过认证。
  - 口令认证：包括远程连接的加密口令认证和本地连接的非加密口令认证。
  - SSL加密：使用OpenSSL（开源安全通信库）提供服务器端和客户端安全连接的环境。
- “pg\_hba.conf”文件的格式是一行写一条信息，表示一个认证规则，空白和注释（以#开头）被忽略。
- 每个认证规则是由若干空格和/，空格和制表符分隔的字段组成。如果字段用引号包围，则它可以包含空白。一条记录不能跨行存在。

#### 授权

数据库对象创建后，进行对象创建的用户就是该对象的所有者。openGauss安装后的默认情况下，未开启 **三权分立**，数据库系统管理员具有与对象所有者相同的权限。也就是说对象创建后，默认只有对象所有者或者系统管理员可以查询、修改和销毁对象，以及通过 **GRANT** 将对象的权限授予其他用户。

为使其他用户能够使用对象，必须向用户或包含该用户的角色授予必要的权限。

openGauss支持以下的权限：SELECT、INSERT、UPDATE、DELETE、TRUNCATE、REFERENCES、CREATE、CONNECT、EXECUTE、ALTER、DROP、COMMENT、INDEX、VACUUM和USAGE。不同的权限与不同的对象类型关联。有关各权限的详细信息，请参见 [GRANT](#)。

要撤销已经授予的权限，可以使用 [REVOKE](#)。对象所有者的权限（例如ALTER、DROP、COMMENT、INDEX、VACUUM、GRANT和REVOKE）是隐式的，无法授予或撤销。即只要拥有对象就可以执行对象所有者的这些隐式权限。对象所有者可以撤销自己的普通权限，例如，使表对自己以及其他人只读，系统管理员用户除外。

系统表和系统视图要么只对系统管理员可见，要么对所有用户可见。标识了需要系统管理员权限的系统表和视图只有系统管理员可以查询。有关信息，请参考 [系统表和系统视图](#)。

数据库提供对象隔离的特性，对象隔离特性开启时，用户只能查看有权限访问的对象（表、视图、字段、函数），系统管理员不受影响。有关信息，请参考 [ALTER DATABASE](#)。

## 审计

数据库安全对数据库系统来说至关重要。openGauss将用户对数据库的所有操作写入审计日志。数据库安全管理员可以利用这些日志信息，重现导致数据库现状的一系列事件，找出非法操作的用户、时间和内容等。

关于审计功能，用户需要了解以下几点内容：

- 审计总开关 [audit\\_enabled](#) 支持动态加载。在数据库运行期间修改该配置项的值会立即生效，无需重启数据库。默认值为on，表示开启审计功能。
- 除了审计总开关，各个审计项也有对应的开关。只有开关开启，对应的审计功能才能生效。
- 各审计项的开关支持动态加载。在数据库运行期间修改审计开关的值，不需要重启数据库便可生效。

目前，openGauss支持以下审计项如 [表1](#) 所示。

**表 1** 配置审计项

配置项	描述
用户登录、注销审计	参数： <code>audit_login_logout</code> 默认值为7，表示开启用户登录、退出的审计功能。设置为0表示关闭用户登录、退出的审计功能。不推荐设置除0和7之外的值。
数据库启动、停止、恢复和切换审计	参数： <code>audit_database_process</code> 默认值为1，表示开启数据库启动、停止、恢复和切换的审计功能。
用户锁定和解锁审计	参数： <code>audit_user_locked</code> 默认值为1，表示开启审计用户锁定和解锁功能。
用户访问越权审计	参数： <code>audit_user_violation</code> 默认值为0，表示关闭用户越权操作审计功能。
授权和回收权限审计	参数： <code>audit_grant_revoke</code> 默认值为1，表示开启审计用户权限授予和回收功能。
数据库对象的CREATE，ALTER，DROP操作审计	参数： <code>audit_system_object</code> 默认值为12295，表示只对DATABASE、SCHEMA、USER、DATA SOURCE这四类数据库对象的CREATE、ALTER、DROP操作进行审计。
具体表的INSERT、UPDATE和DELETE操作审计	参数： <code>audit_dml_state</code> 默认值为0，表示关闭具体表的DML操作（SELECT除外）审计功能。
SELECT操作审计	参数： <code>audit_dml_state_select</code> 默认值为0，表示关闭SELECT操作审计功能。
COPY审计	参数： <code>audit_copy_exec</code> 默认值为1，表示开启copy操作审计功能。
存储过程和自定义函数的执行审计	参数： <code>audit_function_exec</code> 默认值为0，表示不记录存储过程和自定义函数的执行审计日志。
SET审计	参数： <code>audit_set_parameter</code> 默认值为1，表示记录set操作审计日志。

安全相关参数及默认值请参见 [表2](#)。

表 2 安全相关参数及默认值

参数名	默认值	说明
<code>ssl</code>	on	指定是否启用SSL连接。
<code>require_ssl</code>	off	指定服务器端是否强制要求SSL连接。
<code>ssl_ciphers</code>	ALL	指定SSL支持的加密算法列表。
<code>ssl_cert_file</code>	server.crt	指定包含SSL服务器证书的文件的名称。
<code>ssl_key_file</code>	server.key	指定包含SSL私钥的文件名称。
<code>ssl_ca_file</code>	cacert.pem	指定包含CA信息的文件的名称。
<code>ssl_crl_file</code>	NULL	指定包含CRL信息的文件的名称。
<code>password_policy</code>	1	指定是否进行密码复杂度检查。

password_reuse_time	60	指定是否对新密码进行可重用天数检查。
password_reuse_max	0	指定是否对新密码进行可重用次数检查。
password_lock_time	1	指定帐户被锁定后自动解锁的时间。
failed_login_attempts	10	如果输入密码错误的次数达到此参数值时，当前帐户被锁定。
password_encryption_type	2	指定采用何种加密方式对用户密码进行加密存储。
password_min_uppercase	0	密码中至少需要包含大写字母的个数。
password_min_lowercase	0	密码中至少需要包含小写字母的个数。
password_min_digital	0	密码中至少需要包含数字的个数。
password_min_special	0	密码中至少需要包含特殊字符的个数。
password_min_length	8	密码的最小长度。说明：在设置此参数时，请将其设置成不大于password_max_length，否则进行涉及密码的操作会一直出现密码长度错误的提示。
password_max_length	32	密码的最大长度。说明：在设置此参数时，请将其设置成不小于password_min_length，否则进行涉及密码的操作会一直出现密码长度错误的提示。
password_effect_time	90	密码的有效期限。
password_notify_time	7	密码到期提醒的天数。
audit_enabled	on	控制审计进程的开启和关闭。
audit_directory	pg_audit	审计文件的存储目录。
audit_data_format	binary	审计日志文件的格式，当前仅支持二进制格式（binary）。
audit_rotation_interval	1d	指定创建一个新审计日志文件的时间间隔。当现在的时间减去上次创建一个审计日志的时间超过了此参数值时，服务器将生成一个新的审计日志文件。
audit_rotation_size	10MB	指定审计日志文件的最大容量。当审计日志消息的总量超过此参数值时，服务器将生成一个新的审计日志文件。
audit_resource_policy	on	控制审计日志的保存策略，以空间还是时间限制为优先策略，on表示以空间为优先策略。
audit_file_remain_time	90	表示需记录审计日志的最短时间要求，该参数在 <a href="#">audit_resource_policy</a> 为off时生效。
audit_space_limit	1GB	审计文件占用磁盘空间的最大值。
audit_file_remain_threshold	1048576	审计目录下审计文件的最大数量。
audit_login_logout	7	指定是否审计数据库用户的登录（包括登录成功和登录失败）、注销。
audit_database_process	1	指定是否审计数据库启动、停止、切换和恢复的操作。
audit_user_locked	1	指定是否审计数据库用户的锁定和解锁。
audit_user_violation	0	指定是否审计数据库用户的越权访问操作。
audit_grant_revoke	1	指定是否审计数据库用户权限授予和回收的操作。
audit_system_object	12295	指定是否审计数据库对象的CREATE、DROP、ALTER操作。

audit_dml_state	0	指定是否审计具体表的INSERT、UPDATE、DELETE操作。
audit_dml_state_select	0	指定是否审计SELECT操作。
audit_copy_exec	0	指定是否审计COPY操作。
audit_function_exec	0	指定在执行存储过程、匿名块或自定义函数（不包括系统自带函数）时是否记录审计信息。
audit_set_parameter	1	指定是否审计SET操作。
enableSeparationOfDuty	off	指定是否开启三权分立。
session_timeout	10min	建立连接会话后，如果超过此参数的设置时间，则会自动断开连接。
auth_iteration_count	10000	认证加密信息生成过程中使用的迭代次数。

审计操作步骤

- 1. 以操作系统用户omm登录数据库主节点。
- 2. 使用如下命令连接数据库。

```
""gsql -d postgres -p 8000
```

postgres为需要连接的数据库名称，8000为数据库主节点的端口号。

连接成功后，系统显示类似如下信息：

```
""gsql ((openGauss 1.0 build 290d125f) compiled at 2020-05-08 02:59:43 commit 2143 last mr
131
Non-SSL connection (SSL connection is recommended when requiring high-security)
Type "help" for help.

openGauss=#
```

- 3. 检查审计总开关状态。
  - a. 用show命令显示审计总开关audit\_enabled的值。


```
""SHOW audit_enabled;
```

如果显示为off，执行“\q”命令退出数据库。

- b. 执行如下命令开启审计功能，参数设置立即生效。

```
""gs_guc set -N all -I all -c "audit_enabled=on"
```

- 4. 配置具体的审计项。

 说明：

- 只有开启审计功能，用户的操作才会被记录到审计文件中。
- 各审计项的默认参数都符合安全标准，用户可以根据需要开启其他审计功能，但会对性能有一定影响。

以开启对数据库所有对象的增删改操作的审计开关为例，其他配置项的修改方法与此相同，修改配置项的方法如下所示：

```
"gs_guc reload -N all -I all -c "audit_system_object=12295"
```

其中audit\_system\_object代表审计项开关，12295为该审计开关的值。

## 3.2 用户权限检查

设计用户权限检查项，开发扫描程序，实现数据库权限扫描功能，扫描数据库中是否有违规操作的可能和安全隐患，完成设计文档。

在openGauss数据库中，存在各种类型的用户和角色，并且每个用户/角色都有不同的权限和访问级别。为了确保数据库安全性，我们需要开发一个程序来检查数据库中的违规操作和安全隐患。以下是我们将采取的实现细节：

### 设计用户权限检查项

为了检查数据库中是否存在违规操作和安全隐患，我们需要设计一系列用户权限检查项。以下是一些示例检查项：

- 是否存在default账户？
- 是否存在弱口令？
- 是否存在超级用户？
- 是否允许远程连接？
- 是否启用密码策略？
- 是否设置了正确的SSL证书？
- 是否过期的账号和密码？
- 是否关闭了未使用的服务？
- 是否启用了审计功能？

### 开发扫描程序

为了实现openGauss数据库权限扫描功能，我们将使用Java编写扫描程序。以下是主要步骤：

1. 读取配置文件：从配置文件中读取数据库连接信息和需要扫描的检查项。
2. 连接到数据库：使用JDBC连接到openGauss数据库。
3. 执行查询语句：执行相应的SQL查询或命令，如SELECT、CREATE等。
4. 解析结果：解析查询结果，并确定数据库是否存在违规行为。
5. 输出结果：将扫描结果输出到日志文件或控制台。

### 实现openGauss数据库权限扫描功能

为了实现openGauss数据库权限扫描功能，我们将采用以下技术：

- JDBC API：用于与数据库交互。
- Spring Boot框架：用于构建和管理Web应用程序。
- Thymeleaf模板引擎：用于生成报告和分析。
- Bootstrap框架：用于设计和排版Web界面。

以下是大致步骤：

1. 用户在Web界面上选择需要扫描的检查项。

2. 程序读取配置文件中的数据库连接信息，并使用JDBC连接到openGauss数据库。
3. 程序根据用户选择的检查项执行相应的查询语句，如SELECT、CREATE等。
4. 程序解析查询结果，并确定数据库是否存在违规行为。
5. 程序将扫描结果输出到Web界面上，并提供详细的报告和分析。

## 设计文档

为了记录openGauss数据库权限扫描功能的设计和实现细节，我们需要编写设计文档。该文档应包括以下内容：

- 项目背景和目标；
- 技术架构和实现细节；
- 用户权限检查项和扫描程序设计；
- 数据库权限扫描功能实现方法；
- 代码示例和测试结果；
- 总结和未来工作。

通过编写设计文档，我们可以更好地管理和维护openGauss数据库权限扫描功能，并为后续的开发工作提供参考。

## 4.规划

---

### 1.项目研发第一阶段

(07 月 01 日 - 08 月01 日)：

在这个阶段，需要探索openGauss中的访问控制模型，并撰写技术洞察博客。以下是实现细节：

- 阅读openGauss官方文档，了解openGauss的基本架构和特性。
- 探索openGauss中的访问控制模型，包括用户、角色和权限等组件。
- 实践openGauss，在虚拟机或云环境中安装并配置openGauss。
- 撰写技术洞察博客，介绍openGauss的访问控制模型和基本使用方法。

### 2.项目研发第二阶段

(08 月 02日 - 08 月 30 日)：

在这个阶段，将设计和开发openGauss数据库权限扫描程序，以便检查数据库中的违规操作和安全隐患。以下是实现细节：

- 设计用户权限检查项，确定需要检查的数据库资源和操作。
- 使用Java编写扫描程序，连接到openGauss数据库并执行相应的查询语句。
- 解析查询结果，确定是否存在违规行为和安全隐患。
- 输出扫描结果到日志文件或Web界面。
- 编写设计文档，记录openGauss数据库权限扫描功能的实现细节和测试结果。



### 3.项目测试和部署

(08 月 30日 - 09 月 30 日)：

在这个阶段，将对openGauss数据库权限扫描功能进行测试，并部署到生产环境中。以下是实现细节：

- 编写单元测试，确保程序能够正确执行和输出必要的结果。
- 进行系统测试，检查是否存在任何问题和异常情况。
- 部署程序到生产环境，确保其可以在实际运行中正常工作。
- 提供用户培训和支持，以便他们能够使用和理解开发的程序。
- 编写用户文档，介绍openGauss数据库权限扫描功能的基本用法和注意事项。