# MySQL 创建三权分立账户指南

本文档详细介绍如何在 MySQL 数据库中创建符合等保三级要求的三权分立账户体系，确保数据库的安全管理。

## 目录

[MySQL 创建三权分立账户指南](#mysql-创建三权分立账户指南)

[目录](#目录)

[1. 三权分立概述](#X27fc2666ce3152ee5fc6cd2a9d8fa8f10e1cb23)

[2. 环境准备](#Xa796e158cafb48eb7c53cb2a79902e8bde6a912)

[3. 创建系统管理员账户](#X4875245d934d56ebbffad1065a4d3029827b0b1)

[4. 创建审计管理员账户](#X4c97fe955c55b445eef622f1bb4c75340687de0)

[5. 创建安全管理员账户](#X0a4eae61df9914cb863926ef16502746b7b27cd)

[6. 创建业务用户账户](#X35f8f5286ae87551f26e0427bf684002cb621f7)

[7. 权限验证与测试](#X2c99d53ca79a83fd4d1133c753976a784d5e404)

[8. 安全配置建议](#X027647f1da0eb374ec4b738ab8b7cdb9cf652b6)

[9. 常见问题与注意事项](#Xfff5e522748d88acc164d0ddd8fc7eebd189fbc)

## 1. 三权分立概述

根据等保三级要求，数据库管理需要实现三权分立，主要包括：

**系统管理员（System Administrator）**：负责数据库系统的安装、配置、维护和日常运维

**审计管理员（Audit Administrator）**：负责审计策略制定、审计日志管理和安全事件分析

**安全管理员（Security Administrator）**：负责用户权限管理、安全策略配置和访问控制

### 1.1 权限分离原则

每个管理员只拥有完成其职责所需的最小权限

关键操作需要多人协作完成

审计功能独立于其他管理功能

确保职责分离，避免权限过度集中

## 2. 环境准备

### 2.1 前提条件

MySQL 5.7 或更高版本

具有 root 权限的 MySQL 管理员账户

已启用 MySQL 审计插件（如 MySQL Enterprise Audit 或 MariaDB Audit Plugin）

### 2.2 连接数据库

# 使用root账户连接MySQL  
mysql -u root -p

### 2.3 检查当前用户和权限

-- 查看当前用户  
SELECT USER(), CURRENT\_USER();  
  
-- 查看所有用户  
SELECT user, host FROM mysql.user;  
  
-- 查看当前用户权限  
SHOW GRANTS;

## 3. 创建系统管理员账户

系统管理员主要负责数据库的系统级管理，包括安装、配置、备份恢复等。

### 3.1 创建系统管理员用户

-- 创建系统管理员账户  
CREATE USER 'sysadmin'@'localhost' IDENTIFIED BY 'SysAdmin@2024!';  
CREATE USER 'sysadmin'@'%' IDENTIFIED BY 'SysAdmin@2024!';  
  
-- 设置密码策略（可选）  
ALTER USER 'sysadmin'@'localhost' PASSWORD EXPIRE INTERVAL 90 DAY;  
ALTER USER 'sysadmin'@'%' PASSWORD EXPIRE INTERVAL 90 DAY;

### 3.2 分配系统管理权限

-- 授予系统管理相关权限  
GRANT SELECT, INSERT, UPDATE, DELETE ON \*.\* TO 'sysadmin'@'localhost';  
GRANT SELECT, INSERT, UPDATE, DELETE ON \*.\* TO 'sysadmin'@'%';  
  
-- 授予数据库管理权限  
GRANT CREATE, DROP, ALTER, INDEX ON \*.\* TO 'sysadmin'@'localhost';  
GRANT CREATE, DROP, ALTER, INDEX ON \*.\* TO 'sysadmin'@'%';  
  
-- 授予备份恢复权限  
GRANT LOCK TABLES, RELOAD, PROCESS ON \*.\* TO 'sysadmin'@'localhost';  
GRANT LOCK TABLES, RELOAD, PROCESS ON \*.\* TO 'sysadmin'@'%';  
  
-- 授予复制相关权限（如果需要主从复制）  
GRANT REPLICATION SLAVE, REPLICATION CLIENT ON \*.\* TO 'sysadmin'@'localhost';  
GRANT REPLICATION SLAVE, REPLICATION CLIENT ON \*.\* TO 'sysadmin'@'%';  
  
-- 刷新权限  
FLUSH PRIVILEGES;

### 3.3 限制系统管理员权限

-- 系统管理员不应具有以下权限：  
-- 1. 用户管理权限（CREATE USER, DROP USER, GRANT OPTION）  
-- 2. 审计日志访问权限  
-- 3. 安全相关表的修改权限  
  
-- 验证权限分配  
SHOW GRANTS FOR 'sysadmin'@'localhost';

## 4. 创建审计管理员账户

审计管理员负责审计策略制定和审计日志管理。

### 4.1 创建审计管理员用户

-- 创建审计管理员账户  
CREATE USER 'auditadmin'@'localhost' IDENTIFIED BY 'AuditAdmin@2024!';  
CREATE USER 'auditadmin'@'%' IDENTIFIED BY 'AuditAdmin@2024!';  
  
-- 设置密码策略  
ALTER USER 'auditadmin'@'localhost' PASSWORD EXPIRE INTERVAL 90 DAY;  
ALTER USER 'auditadmin'@'%' PASSWORD EXPIRE INTERVAL 90 DAY;

### 4.2 分配审计管理权限

-- 授予审计日志查看权限  
GRANT SELECT ON mysql.general\_log TO 'auditadmin'@'localhost';  
GRANT SELECT ON mysql.general\_log TO 'auditadmin'@'%';  
  
GRANT SELECT ON mysql.slow\_log TO 'auditadmin'@'localhost';  
GRANT SELECT ON mysql.slow\_log TO 'auditadmin'@'%';  
  
-- 如果使用MySQL Enterprise Audit  
-- GRANT AUDIT\_ADMIN ON \*.\* TO 'auditadmin'@'localhost';  
-- GRANT AUDIT\_ADMIN ON \*.\* TO 'auditadmin'@'%';  
  
-- 授予性能监控权限  
GRANT SELECT ON performance\_schema.\* TO 'auditadmin'@'localhost';  
GRANT SELECT ON performance\_schema.\* TO 'auditadmin'@'%';  
  
-- 授予查看进程权限  
GRANT PROCESS ON \*.\* TO 'auditadmin'@'localhost';  
GRANT PROCESS ON \*.\* TO 'auditadmin'@'%';  
  
-- 刷新权限  
FLUSH PRIVILEGES;

### 4.3 配置审计日志

-- 启用审计日志（需要在my.cnf中配置）  
-- 在MySQL配置文件中添加：  
-- [mysqld]  
-- general\_log = ON  
-- general\_log\_file = /var/log/mysql/mysql.log  
-- slow\_query\_log = ON  
-- slow\_query\_log\_file = /var/log/mysql/mysql-slow.log  
-- long\_query\_time = 2  
  
-- 动态启用日志记录  
SET GLOBAL general\_log = 'ON';  
SET GLOBAL slow\_query\_log = 'ON';  
  
-- 查看审计配置  
SHOW VARIABLES LIKE '%log%';

## 5. 创建安全管理员账户

安全管理员负责用户权限管理和安全策略配置。

### 5.1 创建安全管理员用户

-- 创建安全管理员账户  
CREATE USER 'secadmin'@'localhost' IDENTIFIED BY 'SecAdmin@2024!';  
CREATE USER 'secadmin'@'%' IDENTIFIED BY 'SecAdmin@2024!';  
  
-- 设置密码策略  
ALTER USER 'secadmin'@'localhost' PASSWORD EXPIRE INTERVAL 90 DAY;  
ALTER USER 'secadmin'@'%' PASSWORD EXPIRE INTERVAL 90 DAY;

### 5.2 分配安全管理权限

-- 授予用户管理权限  
GRANT CREATE USER ON \*.\* TO 'secadmin'@'localhost' WITH GRANT OPTION;  
GRANT CREATE USER ON \*.\* TO 'secadmin'@'%' WITH GRANT OPTION;  
  
-- 授予权限管理相关权限  
GRANT SELECT, INSERT, UPDATE, DELETE ON mysql.user TO 'secadmin'@'localhost';  
GRANT SELECT, INSERT, UPDATE, DELETE ON mysql.user TO 'secadmin'@'%';  
  
GRANT SELECT, INSERT, UPDATE, DELETE ON mysql.db TO 'secadmin'@'localhost';  
GRANT SELECT, INSERT, UPDATE, DELETE ON mysql.db TO 'secadmin'@'%';  
  
GRANT SELECT, INSERT, UPDATE, DELETE ON mysql.tables\_priv TO 'secadmin'@'localhost';  
GRANT SELECT, INSERT, UPDATE, DELETE ON mysql.tables\_priv TO 'secadmin'@'%';  
  
-- 授予角色管理权限（MySQL 8.0+）  
-- GRANT ROLE\_ADMIN ON \*.\* TO 'secadmin'@'localhost';  
-- GRANT ROLE\_ADMIN ON \*.\* TO 'secadmin'@'%';  
  
-- 刷新权限  
FLUSH PRIVILEGES;

### 5.3 限制安全管理员权限

-- 安全管理员不应具有以下权限：  
-- 1. 直接的数据操作权限（除权限管理相关表外）  
-- 2. 系统管理权限（如RELOAD, SHUTDOWN等）  
-- 3. 审计日志的修改权限  
  
-- 验证权限分配  
SHOW GRANTS FOR 'secadmin'@'localhost';

## 6. 创建业务用户账户

为不同的业务应用创建专门的数据库用户。

### 6.1 创建业务用户

-- 创建业务应用用户  
CREATE USER 'app\_user'@'localhost' IDENTIFIED BY 'AppUser@2024!';  
CREATE USER 'app\_user'@'192.168.1.%' IDENTIFIED BY 'AppUser@2024!';  
  
-- 创建只读用户  
CREATE USER 'readonly\_user'@'localhost' IDENTIFIED BY 'ReadOnly@2024!';  
CREATE USER 'readonly\_user'@'192.168.1.%' IDENTIFIED BY 'ReadOnly@2024!';

### 6.2 分配业务权限

-- 为业务用户分配特定数据库权限  
GRANT SELECT, INSERT, UPDATE, DELETE ON business\_db.\* TO 'app\_user'@'localhost';  
GRANT SELECT, INSERT, UPDATE, DELETE ON business\_db.\* TO 'app\_user'@'192.168.1.%';  
  
-- 为只读用户分配查询权限  
GRANT SELECT ON business\_db.\* TO 'readonly\_user'@'localhost';  
GRANT SELECT ON business\_db.\* TO 'readonly\_user'@'192.168.1.%';  
  
-- 刷新权限  
FLUSH PRIVILEGES;

## 7. 权限验证与测试

### 7.1 测试系统管理员权限

# 使用系统管理员账户登录  
mysql -u sysadmin -p

-- 测试数据库操作权限  
CREATE DATABASE test\_sysadmin;  
USE test\_sysadmin;  
CREATE TABLE test\_table (id INT PRIMARY KEY, name VARCHAR(50));  
INSERT INTO test\_table VALUES (1, 'test');  
SELECT \* FROM test\_table;  
DROP DATABASE test\_sysadmin;  
  
-- 尝试用户管理操作（应该失败）  
-- CREATE USER 'test\_user'@'localhost' IDENTIFIED BY 'password'; -- 应该报错

### 7.2 测试审计管理员权限

# 使用审计管理员账户登录  
mysql -u auditadmin -p

-- 测试审计日志查看权限  
SELECT \* FROM mysql.general\_log LIMIT 10;  
SELECT \* FROM mysql.slow\_log LIMIT 10;  
  
-- 查看当前连接  
SHOW PROCESSLIST;  
  
-- 尝试数据操作（应该失败）  
-- CREATE DATABASE test\_audit; -- 应该报错

### 7.3 测试安全管理员权限

# 使用安全管理员账户登录  
mysql -u secadmin -p

-- 测试用户管理权限  
CREATE USER 'test\_user'@'localhost' IDENTIFIED BY 'TestUser@2024!';  
GRANT SELECT ON mysql.user TO 'test\_user'@'localhost';  
SHOW GRANTS FOR 'test\_user'@'localhost';  
DROP USER 'test\_user'@'localhost';  
  
-- 查看用户权限信息  
SELECT user, host, authentication\_string FROM mysql.user;  
  
-- 尝试数据库操作（应该失败）  
-- CREATE DATABASE test\_security; -- 应该报错

## 8. 安全配置建议

### 8.1 密码策略配置

-- 配置密码验证插件（MySQL 5.7+）  
INSTALL PLUGIN validate\_password SONAME 'validate\_password.so';  
  
-- 设置密码策略  
SET GLOBAL validate\_password\_policy = 'STRONG';  
SET GLOBAL validate\_password\_length = 12;  
SET GLOBAL validate\_password\_number\_count = 2;  
SET GLOBAL validate\_password\_special\_char\_count = 2;  
  
-- 查看密码策略设置  
SHOW VARIABLES LIKE 'validate\_password%';

### 8.2 连接安全配置

-- 限制连接数  
SET GLOBAL max\_connections = 200;  
SET GLOBAL max\_user\_connections = 50;  
  
-- 配置连接超时  
SET GLOBAL wait\_timeout = 3600;  
SET GLOBAL interactive\_timeout = 3600;  
  
-- 查看连接配置  
SHOW VARIABLES LIKE '%timeout%';  
SHOW VARIABLES LIKE '%connection%';

### 8.3 审计配置优化

-- 配置详细的审计日志  
SET GLOBAL general\_log\_file = '/var/log/mysql/general.log';  
SET GLOBAL slow\_query\_log\_file = '/var/log/mysql/slow.log';  
SET GLOBAL log\_output = 'FILE';  
  
-- 启用二进制日志（用于恢复和复制）  
-- 在my.cnf中配置：  
-- log-bin = /var/log/mysql/mysql-bin.log  
-- binlog\_format = ROW  
-- expire\_logs\_days = 7

## 9. 常见问题与注意事项

### 9.1 权限最小化原则

每个账户只分配完成其职责所需的最小权限

定期审查和清理不必要的权限

避免使用通配符权限（如 \*.\*），尽可能精确到具体数据库和表

### 9.2 账户安全管理

定期更换密码

启用账户锁定策略

监控异常登录行为

及时删除不再使用的账户

### 9.3 审计日志管理

确保审计日志的完整性和不可篡改性

定期备份审计日志

设置日志轮转策略，避免日志文件过大

建立日志分析和告警机制

### 9.4 备份与恢复

# 定期备份用户权限信息  
mysqldump -u root -p --single-transaction --routines --triggers mysql > mysql\_grants\_backup.sql  
  
# 备份业务数据库  
mysqldump -u sysadmin -p --single-transaction --routines --triggers business\_db > business\_db\_backup.sql

### 9.5 监控和告警

监控登录失败次数

监控权限变更操作

监控异常的SQL执行

设置关键操作的告警机制

**注意事项：**

本指南中的密码仅为示例，实际使用时请设置复杂且唯一的密码

根据实际网络环境调整主机地址限制

定期审查和更新权限配置

确保遵循组织的安全策略和合规要求

在生产环境中实施前，请在测试环境中充分验证所有配置