# MySQL 数据库安全配置方案

### 一、数据库安全配置归类

数据库安全配置，主要涉及账户、口令、权限、访问控制、日志等方面；

为了更好地进行分类编制，按安全配置项类型进行归类编排，方便加固实施操作

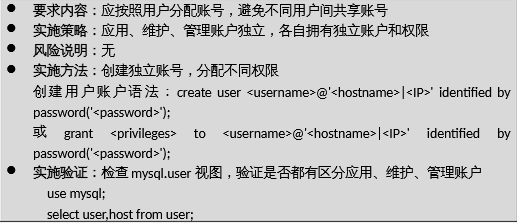


### 二、数据库安全配置策略

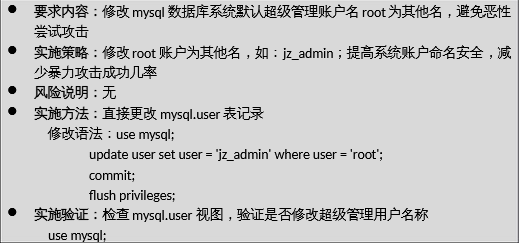
为了统一实施，方便管理识别，按类进行分类实施

#### 2.1 账户

##### 2.1.1 按用户分片数据库账号



##### 2.1.2 更改默认mysql管理员账号

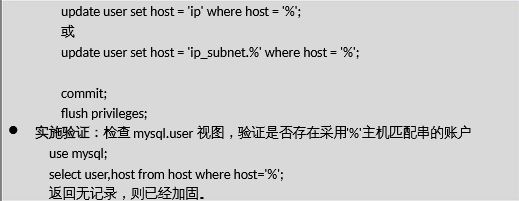
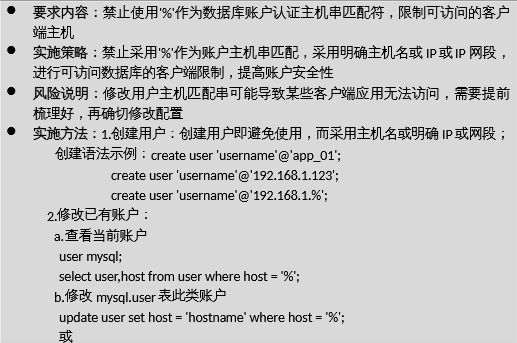




##### 2.1.3 删除匿名账户



##### 2.1.4 禁止实用'%'作为用户认证主机匹配符

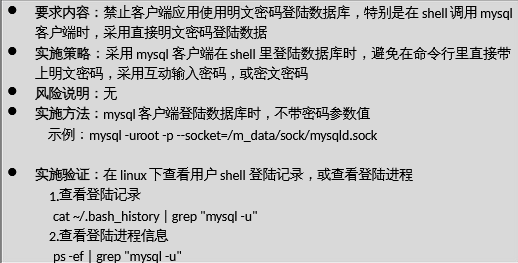


#### 2.2 口令

##### 2.2.1 禁止使用空密码

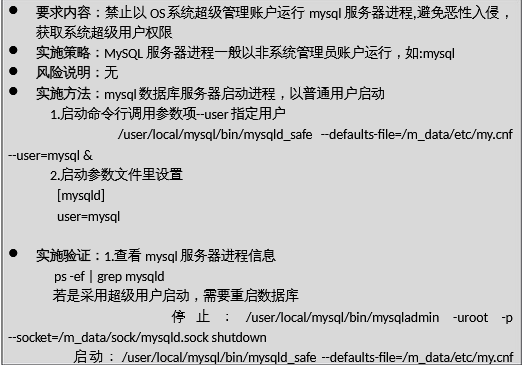


##### 2.2.2 禁止在mysql登陆使用明文密码

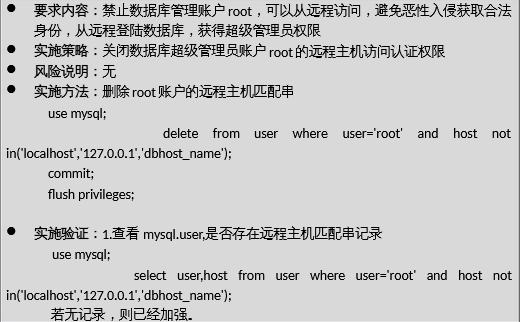


#### 2.3 权限

##### 2.3.1 禁止mysql以管理员账号权限运行

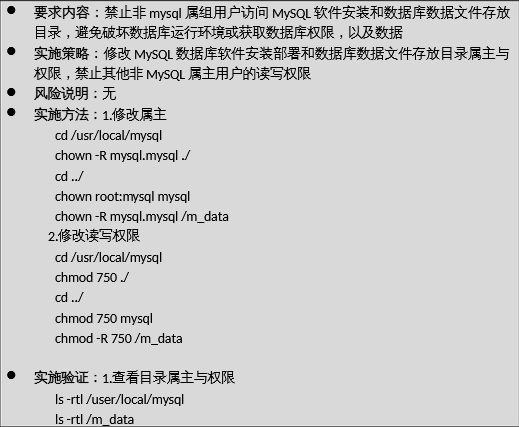


##### 2.3.2 禁止root超级管理账户远程登陆



##### 2.3.3 禁止mysql对本地文件存取

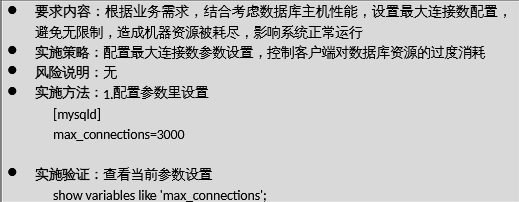
##### 2.3.4 禁止其他用户访问mysql安装目录和数据目录



##### 2.3.5 禁止其他用户访问mysql home目录下的.bash\_history和.mysql\_history

#### 2.4 配置

##### 2.4.1 根据机器性能和业务需求，设置最大连接数



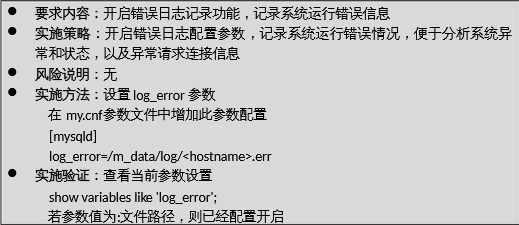
##### 2.4.2 删除测试安装的test库

#### 2.5 日志

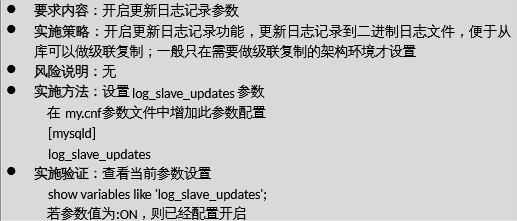
##### 2.5.1 开启查询日志

##### 2.5.2 开启慢查询日志

##### 2.5.3 开启错误日志



##### 2.5.4 开启更新日志



##### 2.5.5 开启二进制日志

### 三 参考文档

[MySQL数据库安全配置方案](https://www.modb.pro/doc/2264?aq)