华为技术有限公司

**EMUI产品部函件**

EMUI产品部函件(2014)XXX号 签发人：

**MySQL数据库安全配置规范**

# 目的

为规范生产环境中MySQL数据库的使用，降低数据库的安全风险，确保数据库安全可靠的运行，特制定此安全配置规范。

# 范围

本规范适用于MySQL 5.6,用于生产环境部署MySQL数据库。

# 内容

1. **身份管理**

**帐号管理(must)**

为防止数据库账号被非法获取、非法使用，以及盗用数据库安装后的默认账号，从而导致数据库数据泄露，需要严格控制数据库账号：

1. 所有数据库帐号安装后必须立即需改口令，所有MySQL数据库中帐号都必须依据账号管理的相关策略和规定要求登记相关责任人。
2. 数据库管理员账号由数据库运维统一管理，仅限数据库运维组内部使用，不扩散使用范围。
3. 检查MySQL库下user表，帐号密码不能为空，系统默认帐号中只保留一个root帐号,限本地登录，其他默认帐号都需要删除。
4. 数据库管理账号dba\_man，只限于数据库跳板机访问，用于管理数据库账号、数据库变更操作，仅限于数据库运维使用，不扩散使用范围。
5. **认证**

**密码规则(Must)**

按照终端云密码管理策略，统一制定账户密码。提高密码复杂度，防止恶意用户“猜出”密码。

1. **授权**

**业务使用须知(must)**

授权原则：MySQL数据库业务账号按需申请，控制业务账号的使用范围，降低业务服务器被攻破后，对数据库造成的威胁。

**用户资源**

严格控制账号权限，屏蔽不必要的权限，特别是高风险权限，要评估必要性和风险，并备案。比如：file权限就有可能带来脚本攻击，导致数据库数据丢失、篡改、泄露，甚至数据库瘫痪。

1. 禁止设置MySQL软件Owner帐号为root组成员。(must)
2. 非特殊申请禁止将all或者super权限授权给普通用户。(must)
3. MySQL运维管理需要如下专用帐号与及相应权限：

|  |  |  |  |
| --- | --- | --- | --- |
| **帐号名** | **用途** | **权限** | **指定访问源** |
| replica | 主从复制专用帐号 | Replication slave | 备机 |
| dbbackup | 数据备份帐号 | SELECT,  RELOAD,  LOCK TABLES, REPLICATION CLIENT, SHOW VIEW,  event | Localhost |
| dba\_man | 运维普通帐号 | select,  insert,  update,  delete,  drop,  alter,  create,  execute,  grant option | 数据库windows跳板机 |

1. **信息保护与保密**

**数据库主机保护**

数据库服务器(包括数据库备份服务器)只保留运维管理账号，由数据库运维管理、使用。不允许其他人员访问数据库主机。

数据库服务器开放端口：数据库服务器只开放ssh、mysql服务端口，其他服务端口均关闭。

**数据库台账管理**

数据库台账包含数据库主机列表、密码、账号分配。其中涉及密码和账号的文档需要设置文档密码，防止账号密码泄露。

1. **安全性保障**

**限制OS设置(must)**

安装MySQL数据库的OS操作系统，应按照运维部主机安全配置规范要求进行配置，数据库的主机安全统一由主机组保证。

**数据库文件权限(must)**

为防止root和mysql之外的用户获取数据库相关文件，MySQL数据库内文件必须按照以下要求进行设置：

|  |  |  |
| --- | --- | --- |
| **文件** | **属性** | **属主** |
| my.cnf文件 | 600 | mysql |
| 数据文件 | 600 | mysql |
| 联机日志 | 660 | mysql |
| err日志 | 644 | mysql |

**应用IP访问限制**

为限制数据库的访问源，防止非法用户使用已泄漏的合法账号和密码，可以采取以下两种方案：

1、通过iptable设定，限制只有特定网段的IP可以访问MySQL服务器端口。

2、对于只有一个访问网段的情况，使用MySQL自身ip限制技术。

1. **安全日志管理**

**数据库日志保存要求(must)**

数据库系统err日志(/opt/huawei/db/data/`hostname`.err)必须至少保留3个月。在数据库发现异常的情况下，可以从err日志中查找原因。

EMUI产品部

二〇一四年五月一十四日

报送：无

主送：

抄送：

华为技术有限公司EMUI产品部 二〇一四年五月一十四日（印发1份）