**《数据库安全基线标准》附件三：**

|  |
| --- |
| **中国投资有限责任公司**  **MYSQL数据库**  **安全基线及配置、检查手册**  **（试行版）** |

中国投资有限责任公司

信息技术部

二零一三年一月

|  |
| --- |
| 目录 |
| [一. 概述 1](#_Toc345593479)  [1.1 版本号 1](#_Toc345593480)  [1.2 适用范围 1](#_Toc345593481)  [1.3 解释权 1](#_Toc345593482)  [1.4 基线及配置、检查依据 1](#_Toc345593483)  [二. 数据库安全目标和总体安全要求 2](#_Toc345593484)  [三. 生产及测试环境安全基线及配置、检查 3](#_Toc345593485)  [3.1 身份鉴别 3](#_Toc345593486)  [3.1.1 多余账户锁定策略 3](#_Toc345593487)  [3.1.2 口令策略设定 4](#_Toc345593488)  [3.2 访问控制 4](#_Toc345593489)  [3.2.1 基本访问控制 4](#_Toc345593490)  [3.2.2 共享账号检查 5](#_Toc345593491)  [3.2.3 用户权限控制 6](#_Toc345593492)  [3.2.4 运行账号安全 7](#_Toc345593493)  [3.3 安全审计 7](#_Toc345593494)  [3.3.1 安全日志完备性要求 7](#_Toc345593495)  [3.4 资源控制 8](#_Toc345593496)  [3.4.1 连接数设置 8](#_Toc345593497)  [3.5 备份和恢复 9](#_Toc345593498)  [3.5.1 数据库备份和恢复 9](#_Toc345593499) |

1. 概述

本文档是中国投资有限责任公司系统内使用MySQL数据库应当遵循的安全性配置标准，主要适用于MySQL安全基线及配置、检查方面的基本要求，用于指导安全例行工作、新系统入网安全检查等场合。

* 1. 版本号

V0.5

* 1. 适用范围

中国投资有限责任公司

* 1. 解释权

中国投资有限责任公司信息技术部

* 1. 基线及配置、检查依据

本文档参考国家等级保护规范和中投技术管理办法，制定此标准依据如下：

* 《商业银行信息科技风险管理指引》（银监发[2009]19号）
* 《信息安全等级保护管理办法》（公通字[2007]43号）
* 《关于开展全国重要信息系统安全等级保护定级工作的通知》（公信安[2007]861）
* 《信息系统等级保护安全设计技术要求》（GB/T 24856—2009）
* 《信息系统安全等级保护基本要求》（ GB/T 22239-2008 ）
* 《中国投资有限责任公司信息技术管理办法》（CIC-IT-MPP-001）

1. 数据库安全目标和总体安全要求

数据库安全是整个安全链条上的一个重要环节，如果数据库安全中的任何环节出现问题都可能会损害整个链的牢固性，给我们整个系统的安全带来严重的损失。数据库中存放的数据（包括业务数据）是企业信息资产的核心，如果数据被破坏/ 篡改或非授权获取将给企业带来严重的损失，甚至会给国家安全带来威胁。

制定数据库安全基线是为了提升数据库在安装、管理、运维、审计过程中的配置安全性，保障各业务系统顺畅、稳定、安全运行。其总体安全要求包括以下6个方面：

* 身份鉴别
* 访问控制
* 安全审计
* 入侵防范
* 资源控制
* 备份和恢复

1. 生产及测试环境安全基线及配置、检查

该部分主要依据“等级保护三级”要求，适用于安全级别要求较高的业务系统。其中定义数据库安全配置的基本要求，在MySQL数据库中，对应配置项分为身份鉴别、访问控制、安全审计、资源控制、备份和恢复这5个方面，建议在进行安全配置前，系统管理员和数据库管理员进行提前测试或做好备份措施。

* 1. 身份鉴别
     1. 多余账户锁定策略

|  |  |
| --- | --- |
| **安全配置编号** | **数据库—MYSQL—配置—1** |
| **配置项** | 删除或锁定与数据库运行、维护等工作无关的账号，工作无关的账号会成为安全风险，如若被不适当授权，安全风险加大。 |
| **配置值** | 结合实际业务情况，删除无关账户和匿名账户。 |
| **配置操作指南** | （1）删除无关账户  DROP USER语句用于删除一个或多个MySQL账户。要使用DROP USER，必须拥有MySQL数据库的全局CREATE USER权限或DELETE权限。账户名称的用户和主机部分与用户表记录的User和Host列值相对应。  使用DROP USER，您可以取消一个账户和其权限，操作如下：  DROP USER user;  该语句可以删除来自所有授权表的账户权限记录。  要点：  DROP USER不能自动关闭任何打开的用户对话。而且，如果用户有打开的对话，此时取消用户，则命令不会生效，直到用户对话被关闭后才生效。一旦对话被关闭，用户也被取消，此用户再次试图登录时将会失败。  （2）删除匿名账户  mysql> delete from user where user='';  mysql> flush privileges; |
| **检查操作指南** | MySQL 查看所有用户的语句：  mysql> select user,password from mysql.user;  依次检查所列出的账户是否为必要账户，删除无关账户和匿名账户。  注：匿名账户为user和password字段均为空的行。 |
| **备注** | 需人工判断，根据实际情况判断账户是否为无关账户，可能误删除有用账户，请谨慎操作。 |

* + 1. 口令策略设定

|  |  |
| --- | --- |
| **安全配置编号** | **数据库—MYSQL—配置—2** |
| **配置项** | 配置密码策略，避免使用空、弱口令或默认口令，降低密码被暴力破解的可能性。 |
| **配置值** | 数据库的账户口令策略应符合相关管理规定，建议：   1. 口令应符合以下条件：数字、大写字母、小写字母、特殊符号4类中至少3类，并且混排无规律的方式； 2. 口令的长度至少为8位； 3. 口令至少90天更换1次，更新的口令至少3次内不能重复。   如果数据库口令长度不支持要求的位数或其他复杂度要求，口令应使用所支持的最长长度并适当缩小更换周期；也可以使用动态密码卡等一次性口令认证方式。 |
| **配置操作指南** | mysql> update user set password=password('password') where user='root';  mysql> flush privileges; |
| **检查操作指南** | 检查本地密码：(注意，管理账号root默认是空密码)  mysql> use mysql;  mysql> select Host,User,Password,Select\_priv,Grant\_priv from user; |
| **备注** | 可以在管理制度上进行要求，结合登陆尝试判断密码是否符合要求。 |

* 1. 访问控制
     1. 基本访问控制

|  |  |
| --- | --- |
| **安全配置编号** | **数据库—MYSQL—配置—3** |
| **配置项** | 应限制访问数据库的源IP地址，防止非授权访问。 |
| **配置值** | 通过数据库所在操作系统或防火墙限制，只有信任的IP地址才能访问数据库。 |
| **配置操作指南** | （1）在防火墙上配置允许或阻断策略。  （2）数据库访问控制  执行命令：mysql> GRANT ALL PRIVILEGES ON db.\*  ·-> -> TO 用户名@'IP子网/掩码';  只有通过指定IP地址段的用户才可以登录。 |
| **检查操作指南** | （1）检查防火墙是否有针对数据库的访问控制措施；  （2）在非信任的客户端以数据库账户登陆被提示拒绝。 |
| **备注** | 可能影响应用 |

* + 1. 共享账号检查

|  |  |
| --- | --- |
| **安全配置编号** | **数据库—MYSQL—配置—4** |
| **配置项** | 数据库应按照用户分配账号，避免不同用户间共享账号。共享账号带来管理和操作记录无法对应到各个用户使用者，以造成审计和记录不便，存在安全风险。 |
| **配置值** | 需要根据数据库运行、维护实际情况，为不同用户分配不同的账号。 |
| **配置操作指南** | 创建用户：  mysql> insert into mysql.user(Host,User,Password,ssl\_cipher,x509\_issuer,x509\_sub  ject) values("localhost"," phplamp",password("passwd"),'','','');  这样就创建了一个名为：phplamp 密码为：passwd的用户。  然后登录一下。  mysql>exit;  @>mysql -u phplamp -p  @>输入密码  mysql>登录成功 |
| **检查操作指南** | MySQL 查看所有用户的语句：  输入指令select user();  依次检查所列出的账户是否存在共享账户。 |
| **备注** |  |

* + 1. 用户权限控制

|  |  |
| --- | --- |
| **安全配置编号** | **数据库—MYSQL—配置—5** |
| **配置项** | 应根据实际业务需要，配置用户的最小权限。 |
| **配置值** | 根据业务需要修改数据库授权情况和用户权限为满足需要的最小权限。 |
| **配置操作指南** | 一般应用用户建议授予最小权限，例如：  grant select,insert,delete on db.table to test@localhost;  回收不必要的或危险的授权，可以执行revoke命令。 |
| **检查操作指南** | 查看数据库授权情况：  mysql> use mysql;  mysql> select \* from user;  mysql>select \* from db;  mysql>select \* from host;  mysql>select \* from tables\_priv;  mysql>select \* from columns\_priv;  查看用户权限： |
| **备注** |  |

* + 1. 运行账号安全

|  |  |
| --- | --- |
| **安全配置编号** | **数据库—MYSQL—配置—6** |
| **配置项** | 以普通账户安全运行mysqld，禁止MySQL以管理员账号权限运行，Unix下禁止以root账号运行mysqld。 |
| **配置值** | 以普通账户运行mysqld。 |
| **配置操作指南** | Unix下可以通过在/etc/my.cnf中设置：  [mysql.server]  user=mysql |
| **检查操作指南** | 检查进程属主和运行参数是否包含--user=mysql类似语句：  # ps –ef | grep mysqld  #grep -i user /etc/my.cnf |
| **备注** |  |

* 1. 安全审计
     1. 安全日志完备性要求

|  |  |
| --- | --- |
| **安全配置编号** | **数据库—MYSQL—配置—7** |
| **配置项** | 数据库应配置日志功能 |
| **配置值** | 在my.ini配置文件中配置日志记录使用的文件。 |
| **配置操作指南** | 在mysql的安装目录下，打开my.ini，配置日志记录文件，保存后重启mysql服务。  例如：  #Enter a name for the binary log. Otherwise a default name will be used.  #log-bin=  #Enter a name for the query log file. Otherwise a default name will be used.  #log=  #Enter a name for the error log file. Otherwise a default name will be used.  log-error=  #Enter a name for the update log file. Otherwise a default name will be used.  #log-update=  上面只开启了错误日志，要开其他的日志就把前面的“#”去掉。 |
| **检查操作指南** | 在mysql的安装目录下，打开my.ini，查看以下日志记录是否开启：  错误日志： -log-err  查询日志： -log （可选）  慢查询日志: -log-slow-queries （可选）  更新日志: -log-update  二进制日志： -log-bin  例如：  [mysqld]  log = filename  show variables like 'log\_%';查看所有的log命令；  show variables like 'log\_bin';查看具体的log命令。 |
| **备注** | 启用审核对系统性能略有影响。 |

* 1. 资源控制
     1. 连接数设置

|  |  |
| --- | --- |
| **安全配置编号** | **数据库—MYSQL—配置—8** |
| **配置项** | 连接数设置 |
| **配置值** | 根据机器性能和业务需求，设置最大连接数 |
| **配置操作指南** | 编辑MySQL配置文件：my.cnf 或者是 my.ini  在[mysqld]配置段添加：  max\_connections = 1000  保存，重启MySQL服务。 |
| **检查操作指南** | 用命令：SHOW [FULL] PROCESSLIST显示哪些线程正在运行  mysql admin -uroot -p variables  输入root数据库账号的密码后可看到  | max\_connections | 1000 | |
| **备注** | 可选 |

* 1. 备份和恢复
     1. 数据库备份和恢复

|  |  |
| --- | --- |
| **安全配置编号** | **数据库—MYSQL—配置—9** |
| **配置项** | 根据实际业务情况，配置数据库备份和恢复策略。 |
| **配置值** | 按照《中国投资有限责任公司信息技术管理办法》（CIC-IT-MPP-001）  第三十三条 备份与恢复相关要求执行。 |
| **配置操作指南** |  |
| **检查操作指南** |  |
| **备注** | **第三十三条 备份与恢复：**  系统上线前应根据系统的重要程度制定相应的系统数据的备份和恢复策略，并填写《备份作业说明书》；  备份策略应主要包括备份数据内容、备份方式、备份频率、操作方法、备份及恢复操作步骤、备份介质存放地点等内容；  如果备份策略不能满足业务需求，应由系统负责人组织进行及时更新；  备份操作人员负责执行备份操作，检查备份结果，定期打印备份日志并签字确认。离线备份的存储介质应进行适当的安全保护；  员工或第三方人员在接触备份介质前应首先经过信息技术部主管领导的审批确认。申请审批过程应记录在《备份介质访问申请表》中；  系统备份介质需定期（每年）进行恢复测试，以保证数据能够准确及完整的恢复。测试人员应将测试过程记录及结果记录在《备份恢复测试记录表》中，签字确认并负责归档；  当业务需要或系统故障等情况需要进行备份恢复时，申请人应在《备份恢复管理表》中说明备份恢复原因，提交申请人主管领导和备份主管领导审批；审批通过后执行备份恢复；申请人应检查备份恢复结果，确认签字并负责归档。 |