Mysql服务安全加固

1.帐号安全

禁止Mysql以管理员帐号权限运行

以普通帐户安全运行mysqld，禁止mysql以管理员帐号权限运行；

下可以通过在/etc/my.cnf中设置：

[mysql.server]

user=mysql

避免不同用户间共享帐号

//创建用户

mysql> mysql> insert into

mysql.user(Host,User,Password,ssl\_cipher,x509\_issuer,x509\_sub

ject) values("localhost","pppadmin",password("passwd"),'','','');

这样就创建了一个名为：phplamp 密码为：1234 的用户。

然后登录一下。

mysql>exit;

@>mysql -u phplamp -p

@>输入密码

mysql>登录成功

删除无关帐号

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帐户权限记录。

2.口令

检查帐户默认密码和弱密码, 口令长度至少8位，并包括数字、小写字母、大写字母和特殊符号四类中至少两类。且5次以内不得设置相同的口令。密码应至少每90天进行更换。

修改帐户弱密码

如要修改密码，执行如下命令：

mysql> update user set password=password('test!p3') where user='root';

mysql> flush privileges;

3.授权

在数据库权限配置能力内，根据用户的业务需要，配置其所需的最小权限。

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;

回收不必要的或危险的授权，可以执行revoke命令：

mysql> help revoke

Name: 'REVOKE'

Description:

Syntax:

REVOKE

priv\_type [(column\_list)]

[, priv\_type [(column\_list)]] ...

ON [object\_type]

{

\*

| \*.\*

| db\_name.\*

| db\_name.tbl\_name

| tbl\_name

| db\_name.routine\_name

}

FROM user [, user] ...

4.开启日志审计功能

数据库应配置日志功能，便于记录运行状况和操作行为。

mysql有以下几种日志：

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

在mysql的安装目录下，打开my.ini,在后面加上上面的参数，保存后重启mysql服务就行了。

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

1、 补充操作说明

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

5.安装最新补丁

系统安装了最新的安全补丁 （注：在保证业务及网络安全的前提下，经过兼容性测试后）

6.如果不需要，应禁止远程访问

禁止网络连接，防止猜解密码攻击，溢出攻击和嗅探攻击。（仅限于应用和数据库在同一台主机的情况）。

如果数据库不需远程访问，可以禁止远程tcp/ip连接, 通过在mysqld服务器中参数中添加 —skip-networking 启动参数来使mysql不监听任何TCP/IP连接，增加安全性。

您可以使用阿里云安全组进行内外网访问控制，建议不要将数据库高危服务开放到互联网上。

7.设置可信IP地址访问控制

通过数据库所在操作系统或防火墙限制，只有信任的IP地址才能通过监听器访问数据库。

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

8.连接数设置

根据机器性能和业务需求，设制最大最小连接数。

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。