【应用安全】浅谈 LINUX 系统 MYSQL 安全配置

文/EmmaDai

0x00 MySQL 应用介绍

MySQL 是一个关系型数据库管理系统，由瑞典 MySQLAB 公司开发，目前属于 Oracle 旗下产品。MySQL 最流行的关系型数据库管理系统，在 WEB 应用方面 MySQL 是最好的 RDBMS(Relational Database Management System，关系数据库管理系统)应用软件之一。

0x01 为什么要做安全配置

MySQL 数据库安全不仅仅是及时安装补丁进行升级就能保证数据库的安全。如果一个最新版本的 MySQL 存在空密码或匿名账号，无需密码就能够登录，会更加容易被攻击。因此做好 MySQL 的安全配置同样十分的重要。

0x02 如何进行安全配置

1. 禁止 mysql 以管理员账号权限运行

MySQL 应该使用非管理员账号运行，以普通帐户安全运行 mysqld

加固方法：
在 MySQL my.cnf 配置文件中应配置 user=mysql

2. 配置日志功能

MySQL 应该配置日志功能，其中包含错误日志、二进制日志、置慢查询日志、通用查询日志、更新日志。

加固方法：
编辑 my.cnf 文件，设置 log_error=/home/mysql.err、log_bin =mysql-bin、slow_query_log=1、general_log =1、log_slave_updates=1

3. 不存在匿名账户

数据库用户应不存在匿名账户，匿名帐户是具有空用户名的用户。 匿名帐户没有密码，所以任何人都可以使用它们连接到 MySQL 服务器。

加固方法：
使用查询语句，查找数据库中的匿名用户，为每个匿名用户分配一个名字，或删除此用户。

```
SELECT user,host FROM mysql.user WHERE user = '';
```

4. 不存在空密码

数据库中所有用户应都配置密码，空密码允许用户在不使用密码的情况下登录。

加固方法：
使用以下语句为用户设置一个密码（示例）：

```
SET PASSWORD FOR <user>@'<host>' =PASSWORD('<clear password>')
```

5. 配置合适的密码复杂度

数据库用户密码复杂性包括密码特征，如长度，大小写，长度和字符集。

加固方法：
添加以下配置到全局配置
plugin-load=validate_password.so
validate-password=FORCE_PLUS_PERMANENT
validate_password_length=14
validate_password_mixed_case_count=1
validate_password_number_count=1
validate_password_special_char_count=1
validate_password_policy=MEDIUM
并更改密码与用户名相同的用户密码

6. 删除测试安装的 test 库

默认的 MySQL 安装包含一个名为 test 的未使用数据库。建议删除 test 数据库。

加固方法：
执行以下 SQL 语句删除 test 数据库：

```
DROP DATABASE "test";
```

7. 禁止 MySQL 对本地文件存取

应禁止 MySQL 对本地文件存取，local_infile 参数决定 MySQL 客户端计算机上的文件是否可以通过 LOAD DATA INFILE 或 SELECT 加载或查询。

加固方法：
在数据库 my.cnf 文件中应配置 local-infile=0

8. MySQL 用户禁用交互式登录

创建时，MySQL 用户可以交互访问操作系统，这意味着 MySQL 用户可以像任何其他用户那样登录主机。应禁用 MySQL 用户交互式登录

加固方法：
执行以下命令：

```
usermod-s /bin/false
usermod -s /sbin/nologin
```

9. 安装最新的安全补丁

MySQL 应安装最新补丁进行升级，以防止漏洞被攻击者利用。

加固方法：
升级 MySQL 到最新版

10. 'mysqld'启动没有配置'--skip-grant-tables'

MySQL 配置文件中 skip-grant-tables 选项会导致 MySQL 在不使用权限系统的情况下启动。

加固方法：
MySQL 配置文件中 skip-grant-tables 应设置为：FALSE，并且启动参数不包含--skip-grant-tables

11. 用户密码过期时间小于等于 90 天

数据库提供了配置配置数据库密码的过期时间，用户密码过期时间应设置小于等于 90 天。

加固方法：
配置 MySQL RDBMS：
全局策略：SET GLOBAL default_password_lifetime=90
并配置：default_password_lifetime=90

12. 数据库位于非系统分区

通常情况下，主机操作系统应该包含不同的文件系统分区以用于不同的目的。一组文件系统通常称为"系统分区"，通常用于主机系统/应用程序操作。另一组文件系统被称为"非系统分区"，一般用于存储数据。MySQL 数据库的 datadir 挂载点应不为：root('/')，"/var" 和 "/usr"。

加固方法：
1） 为 MySQL 数据选择一个非系统分区的新位置
2） 执行如下命令停止 mysqld：servicemysql stop
3） 执行如下命令复制数据：cp-rp <datadir> <新位置>
在 MySQL 配置文件中将 datadir 设置为新位置
执行如下命令启动 mysqld：servicemysql start

13. 只有管理用户具有完整的数据库访问权限

MySQL 数据库中 mysql.user 和 mysql.db 表列出了可以授予（或拒绝）给 MySQL 用户的各种权限。一些关注的特权包括：Select_priv，Insert_priv，Update_priv，Delete_priv，Drop_priv 等等。通常，这些特权不应该对每个 MySQL 用户都可用，而且通常只保留给管理员使用。

加固方法：
列举审计程序结果统计的非管理员用户，对于每个非管理用户，使用 REVOKE 语句来适当删除权限。

14. 禁用 MySQL 命令历史记录

在 Linux/UNIX 系统中，MySQL 客户端将交互式执行的语句记录到历史文件中。默认情况下，该文件在用户的主目录中被命名为.mysql_history。在 MySQL 客户端应用程序中运行的大多数交互式命令都被保存到历史文件中。应该禁用 MySQL 命令历史记录。

加固方法：
1） 删除.mysql_history（如果存在）。
2） 使用方法防止再次创建：
将 MYSQL_HISTFILE 环境变量设置为/dev/null。需要放在 shell 启动脚本中。
创建软链接。> ln -s /dev/null $HOME/.mysql_history

15. 所有远程用户的'ssl_type'应设置为 'ANY', 'X509', 'SPECIFIED'

所有网络流量在不受信任的网络上传输时必须使用 SSL/TLS。对于通过网络进入系统的用户，每个必须强制使用 SSL/TLS。

加固方法：
使用 GRANT 语句配置使用 SSL：

```
GRANT USAGE ON *.* TO 'my_user'@'app1.example.com' REQUIRESSL;
```

0x03 总结

对 MySQL 进行安全配置可以有效的防范一些常见安全问题，按照基线标准做好安全配置能够减少安全事件的发生。国内常见的基线标准有中国信息安全等级保护、工信部基线配置要求，美国 CIS 基线也有详细的 MySQL 基线标准，不同的企业也可以根据自身企业业务制定符合自己企业的安全基线标准。

0x04 参考链接

- 国家信息安全等级保护制
- CIS_Oracle_MySQL_Community_Server_5.7_Benchmark_v1.0.0
- YDT 2700-2014 电信网和互联网安全防护基线配置要求及检测要求 数据库