【应用安全】浅谈 LINUX 系统 ORACLE 安全配置

文/小白

0x00 Oracle 应用介绍

Oracle Database，又名 Oracle RDBMS，或简称 Oracle。是甲骨文公司的一款关系数据库管理系统。Oracle 数据库系统可移植性好、使用方便、功能强，适用于各类大、中、小、微机环境。它是一种高效率、可靠性好的 适应高吞吐量的数据库解决方案。

0x01 为什么要做安全配置

数据库 Oracle 存在安全配置不恰当导致的安全问题。因此，安全配置 Oracle 数据库能有效的减少安全威胁，下面将对 Oracle 安全配置进行讨论。加固方法以 Oracle 11g 为例。

0x02 如何进行安全配置

1. 数据字典保护

启用数据字典保护，只有 SYSDBA 用户才能访问数据字典基础表。

加固方法：
设置初始化参数 O7_DICTIONARY_ACCESSIBILITY = FALSE。

2. 限制 DBA 组中的用户数量

限制在 DBA 组中的操作系统用户数量，通常 DBA 组中只有 Oracle 安装用户。

加固方法：
使用 userdel 命令删除多余的 DBA 组中的操作系统用户，DBA 组中只留一个 Oracle 安装用户。

3. 设置数据库口令复杂度

对采用静态口令进行认证的数据库，设置所有开启用户的口令长度至少 6 位，并包括数字、小写字母、大写字母和特殊符号 4 类中至少 2 类

加固方法：
修改相关 profile，设置 PASSWORD_VERIFY_FUNCTION，指定密码复杂度。

4. 数据库用户口令生存周期

对于采用静态口令认证技术的数据库，设置账户口令的生存期不长于 90 天。

加固方法：
修改相关 profile，将 PASSWORD_LIFE_TIME 设置为小于等于 90。

5. 限制具有数据库超级管理员(SYSDBA)权限的用户远程登录

禁止具有数据库超级管理员(SYSDBA)权限的用户从远程登陆。

加固方法：
修改 spfile，将 REMOTE_LOGIN_PASSWORDFILE 设置为 NONE。

6. 开启数据库审计

开启数据库审计功能，根据业务要求制定数据库审计策略。

加固方法：
登录数据库，执行以下命令打开数据库审计，并重启数据库。

```
SQL> alter system set audit_trail='DB or OS' scope=spfile;
```

7. 设置数据库监听器密码

为数据库监听器（LISTENER）的关闭和启动设置密码。

加固方法：

```
$ lsnrctl
LSNRCTL> set current_listener LISTENER
Current Listener is LISTENER
LSNRCTL> change_password
Old password:
New password:
Reenter new password:
Connecting to (DESCRIPTION=(ADDRESS=(PROTOCOL=TCP)(HOST=hostname)(PORT=1521)))
Password changed for LISTENER
The command completed successfully
LSNRCTL> save_config
```

8. 配置可信 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。

加固方法：
编辑 $ORACLE_HOME/network/admin/sqlnet.ora 文件，添加或修改如下配置，重启数据库。

```
tcp.validnode_checking = yes
tcp.invited_nodes = (ip1,ip2…)
```

9. 数据库连接超时

在某些应用环境下可设置数据库连接超时，比如数据库将自动断开超过 15 分钟的空闲远程连接。

加固方法：
编辑 $ORACLE_HOME/network/admin/sqlnet.ora 文件，设置 SQLNET.EXPIRE_TIME 参数。

10. 网络传输数据加密

使用 Oracle 提供的高级安全选件来加密客户端与数据库之间或中间件与数据库之间的网络传输数据。

加固方法：
编辑 $ORACLE_HOME/network/admin/sqlnet.ora 文件，设置 sqlnet.encryption 参数。

11. 设置连接数

根据机器性能和业务需求，设置最大连接数。。

加固方法：
以管理员权限登录数据库，执行下列命令修改连接数，如 200，重启数据库。

```
SQL> alter system set processes=200 scope=spfile;
```

0x03 总结

对 Oracle 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、电信网和互联网安全防护基线配置要求及检测要求 ,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度要求

电信网和互联网安全防护基线配置要求及检测要求