oracle 安全加固

1.删除或锁定账号

alter user username lock;

drop user username cascade;

2.更改密码

alter user username identified by "password"

3.限制数据库超级管理员远程登录

3.1.在 spfile 中设置

REMOTE_LOGIN_PASSWORDFILE=NONE

3.2.在 sqlnet.ora 中设置

SQLNET.AUTHENTICATION_SERVICES=NONE 禁用 SYSDBA 角色的自动登录

4.启用审计日志

1. 通过设置参数 audit_trail = db 或 os 来打开数据库审计。
2. 然后可使用 Audit 命令对相应的对象进行审计设置

5.设置只有信任的 IP 地址才能通过监听器访问数据库：

在服务器上的文件$ORACLE_HOME/network/admin/sqlnet.ora 中设置以下行：

tcp.validnode_checking = yes

tcp.invited_nodes = (ip1,ip2…)

6.设置数据库连接超时 （10 分钟）

在 sqlnet.ora 中设置下面参数：

SQLNET.EXPIRE_TIME=10

7.Oracle 数据库可通过设置 listener.ora 文件限制客户端 IP 地址对数据库的访问，具体操作包括以下步骤：

tcp.validnode_checking = YES

tcp.excluded_nodes = (list of IP addresses)

tcp.invited_nodes = (list of IP addresses)

重启 listener

8.失败的登录尝试

检查失败的登录尝试

SQL> select * from dba_profiles where RESOURCE_NAME = 'FAILED_LOGIN_ATTEMPTS';

如果 LIMIT 为 NULL，建议修改失败的登录尝试

ALTER PROFILE "DEFAULT" LIMIT FAILED_LOGIN_ATTEMPTS 3;

9.默认情况下，口令明文传输

通过配置在网络上通过 DES 加密传输

在 Client 上将 ORA_ENCRYPT_LOGIN 变量设置成 TURE

在 Server 上将 DBLINK_ENCRYPT_LOGIN 参数设置成 TURE

10.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

通过/etc/passwd 文件来检查是否有其它用户在 DBA 组中。

11、为数据库监听器（LISTENER）的关闭和启动设置密码

通过下面命令设置密码：

$ lsnrctl

LSNRCTL> change_password

Old password: <OldPassword> Not displayed

New password: <NewPassword> Not displayed

Reenter new password: <NewPassword> Not displayed

Connecting to (DESCRIPTION=(ADDRESS=(PROTOCOL=TCP)(HOST=prolin1)(PORT=1521)(IP=FIRST)))

Password changed for LISTENER

The command completed successfully

LSNRCTL> save_config

12、设置只有信任的 IP 地址才能通过监听器访问数据库

只需在服务器上的文件$ORACLE_HOME/network/admin/sqlnet.ora 中设置以下行：

tcp.validnode_checking = yes

tcp.invited_nodes = (ip1,ip2...)

13、根据业务要求制定数据库审计策略

1. 通过设置参数 audit_trail = db 或 os 来打开数据库审计。
2. 然后可使用 Audit 命令对相应的对象进行审计设置。