实用数据库11

2018年4月3日 8:41

Oracle 安全

3A

1. 验证
2. 授权
3. 审核

sys

1. 操作系统验证（优先）
   禁用操作系统验证：**SQLNET.AUTHENTICATION_SERVICES= (NONE)**
2. 口令文件验证 -- remote_login_passwordfile
   orapwd file=C:\Oracle\product\11.2.0\dbhome_1\database\PWDsales.ora password=admin force=y entries=1
   a. NONE
   b. EXCLUSIVE (单例程，多用户)
   c. SHARED (多例程，单用户)

```
SQL> show parameter remote

NAME                                 TYPE                 VALUE
------------------------------------ -------------------- ------------------------------
remote_dependencies_mode             string               TIMESTAMP
remote_listener                      string
remote_login_passwordfile            string               EXCLUSIVE
remote_os_authent                    boolean              FALSE
remote_os_roles                      boolean              FALSE
result_cache_remote_expiration       integer              0
SQL> show parameter remote_login_passwordfile

NAME                                 TYPE                 VALUE
------------------------------------ -------------------- ------------------------------
remote_login_passwordfile            string               EXCLUSIVE
```

Entries=0~4: 除了sys用户之外，最多还允许4个用户登录，5~8，最多8个，以此类推。

默认情况下只有sys用户可以as sysdba来连接

```
NAME                                 TYPE                 VALUE
------------------------------------ -------------------- ---------------
remote_login_passwordfile            string               EXCLUSIVE
SQL>
SQL> select USERNAME, SYSDBA from v$pwfile_users;

USERNAME                                                      SYSDBA
------------------------------------------------------------ ----------
SYS                                                           TRUE
```

授予用户sysdba权限：

```
SQL> grant sysdba to scott;

授权成功。

SQL> select USERNAME, SYSDBA from v$pwfile_users;

USERNAME                                                         SYSDBA
---------------------------------------------------------------- ----------
SYS                                                              TRUE
SCOTT                                                            TRUE
```

撤销sysdba权限：

```
SQL> revoke sysdba from scott;

撤销成功。
```

non-sys

1. 数据库验证

```
SQL> create user u1 identified by u1;

用户已创建。

SQL> grant create session to u1;

授权成功。
```

2. 操作系统验证

网络

1. 资源共享
2. 集中管理
3. 安全

Runas user:sucker cmd

系统权限（create table）
对象权限
权限的传递原则

1. 系统权限不连带 sys -> a, a -> b, revoke from a， b 还是有权限
2. 对象权限是连带 …（上述对象权限传递），b 没有权限

Grant create table to a with admin option
Revoke create table from a
传递系统权限：Grant select on scott.emp to a
传递对象权限：grant 。。。 To a with grant option

角色

1. 用户自定义角色
2. 预定义角色
3. 应用程序角色

默认角色靠登录激活

```
Create role app_r1 identified using scott.p11;
Grant select on scott.emp to app_r1;
Create or replace procedure scott.p11
Authid current_user
As
    Begin
        Dbms_session.set_role('APP_R1');
    End;
/

Grant execute on scott.p11 to a, b;
```

审核

1. 强制审核（默认审核）-- 警告日志文件
2. 标准数据库审核
   a. 启用审核 -- 修改初始化参数

      Alter system set audit_trail= scope=spfile;

```
SQL> show parameter audit_trail

NAME                                 TYPE                 VALUE
------------------------------------ -------------------- ------------------------------
audit_trail                          string               DB
SQL> show parameter audit_file_dest

NAME                                 TYPE                 VALUE
------------------------------------ -------------------- ------------------------------
audit_file_dest                      string               C:\ORACLE\ADMIN\SALES\ADUMP
```

      Select count(*) from aud$;

      Trancate table aud$;

      desc dba_audit_trail

   b. 指定审核选项
      i. 用户审核（权限审核）

         Audit select any table by scott;

      ii. 对象审核

         Audit delete on scott.emp;

      iii. 语句审核 -- 与用户和对象无关

         Audit create trigger

      Noaudit delete on scott.emp;

      Audit delete on scott.emp whenever successful; -- 删除成功就记录

      Audit session whenever not successful; -- 记录登录失败

Audit update on scott.emp by session;
Audit update on scott.emp by access;

Audit 步骤:

```
SQL> desc dba_audit_trail
SQL> show parameter audit

NAME                                 TYPE                 VALUE
------------------------------------ -------------------- ------------------------------
audit_file_dest                       string               C:\ORACLE\ADMIN\SALES\ADUMP
audit_sys_operations                  boolean              FALSE
audit_trail                           string               DB

SQL> grant select, insert, update, delete on SCOTT.emp to a;
SQL> select USERNAME, TIMESTAMP, ACTION_NAME from dba_audit_trail order by TIMESTAMP;

USERNAME       TIMESTAMP       ACTION_NAME
-------------- -------------- ----------------------------------
SCOTT          24-3?  -18      LOGON
SCOTT          24-3?  -18      LOGOFF
SYSTEM         24-3?  -18      LOGON
SYSTEM         24-3?  -18      DROP PUBLIC SYNONYM
SYSTEM         24-3?  -18      DROP PUBLIC SYNONYM
SYSTEM         24-3?  -18      CREATE PUBLIC SYNONYM
SYSTEM         24-3?  -18      CREATE PUBLIC SYNONYM
SYSTEM         24-3?  -18      LOGOFF
SCOTT          24-3?  -18      LOGON
SCOTT          24-3?  -18      LOGOFF
SCOTT          24-3?  -18      LOGOFF

USERNAME       TIMESTAMP       ACTION_NAME
-------------- -------------- ----------------------------------
SCOTT          24-3?  -18      LOGON
SYSMAN         24-3?  -18      LOGON
SYSMAN         24-3?  -18      LOGON
SYSMAN         24-3?  -18      LOGON
SYSMAN         24-3?  -18      LOGON
SYSMAN         24-3?  -18      LOGOFF
U1             03-4?  -18      LOGON
OPS$JOHNSON-XPS 03-4?  -18      LOGON
```

\SUCKER

SYS 03-4? -18 LOGON

USERNAME TIMESTAMP ACTION_NAME
---------- ---------- ----------
OPS$JOHNSON-XPS 03-4? -18 LOGON
\SUCKER

OPS$JOHNSON-XPS 03-4? -18 LOGON
\SUCKER

OPS$JOHNSON-XPS 03-4? -18 LOGON
\JOHNSON CHEN

SUCKER 03-4? -18 LOGON
OPS$JOHNSON-XPS 03-4? -18 LOGON

USERNAME TIMESTAMP ACTION_NAME
---------- ---------- ----------
\SUCKER

A 03-4? -18 LOGON
A 03-4? -18 LOGON
A 03-4? -18 LOGOFF
A 03-4? -18 LOGON
A 03-4? -18 SELECT

已选择30行。