第 8 章　安全管理——给用户授权

本章介绍 Oracle 9i 中安全性管理的内容。通过本章的学习，管理员可以全面掌握 Oracle 9i 数据库的安全性管理。

8.1　Oracle 数据库系统的安全性

8.1.1　Oracle 9i 的安全性体系

1. 物理层的安全性

数据库所在节点必须在物理上得到可靠的保护。

2. 用户层的安全性

哪些用户可以使用数据库，使用数据库的哪些数据对象，具有什么样的权限等。

3. 操作系统层的安全性

数据库所在的主机的操作系统的弱点将可能提供恶意攻击数据库的入口。

4. 网络层的安全性

Oracle 9i 数据库主要是面向网络提供服务，因此，网络软件的安全性和网络数据传输的安全性至关重要。

5. 数据库系统层的安全性

通过对用户授予特定的访问数据库对象的权利的办法来确保数据库系统层的安全。

8.1.2　Oracle 9i 的安全性机制

1. 系统安全性机制

系统安全性机制是指在整个的数据库系统级控制数据库的存取和使用的机制。

2. 数据安全性机制

数据安全性机制是指在对象级控制数据库的存取和使用的机制。

8.2　用户的管理

8.2.1　Oracle 9i 默认的用户

表 8.1　　Oracle 9i 默认的主要用户

用户名	口令	登录身份及说明
sys	change_on_install	SYSDBA 或 SYSOPER，但不能以 NORMAL 登录，可作为默认的系统管理员
system	Manager	SYSDBA 或 NORMAL，但不能以 SYSOPER 登录，可作为默认的系统管理员
scott	Tiger	NORMAL，普通用户
aqadm	aqadm	SYSDBA 或 NORMAL，高级队列管理员。
Dbsnmp	dbsnmp	SYSDBA 或 NORMAL，复制管理员。

【参见光盘文件】：第 8 章\selectdbausers.sql 和 selectuserusers.sql。

8.2.2　在【企业管理器】中如何创建用户

（1）如图 8.1 所示。

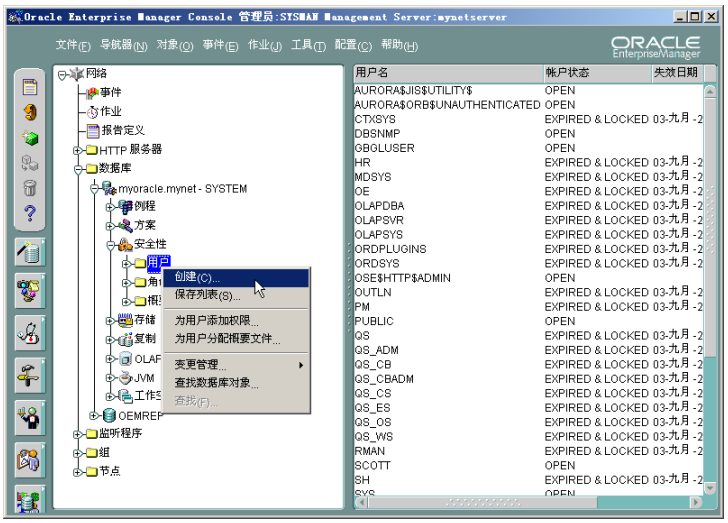


图 8.1　选择创建用户

（2）出现如图 8.2 所示的创建用户的【一般信息】选项卡。

（3）图 8.3 所示为创建用户的【角色】选项卡。

图 8.2　创建用户的【一般信息】选项卡

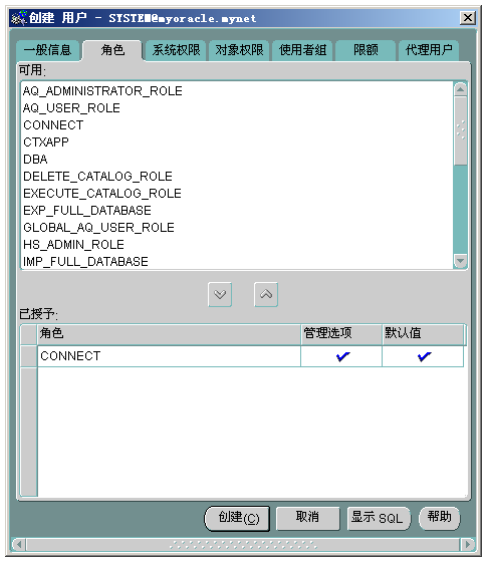


图 8.3　创建用户的【角色】选项卡

（4）图 8.4 所示为创建用户的【系统权限】选项卡。

（5）如图 8.5 所示为创建用户的【对象权限】选项卡。

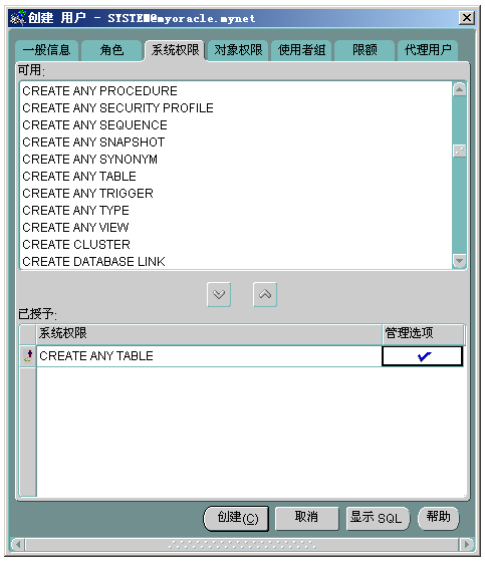


图 8.4　创建用户的【系统权限】选项卡

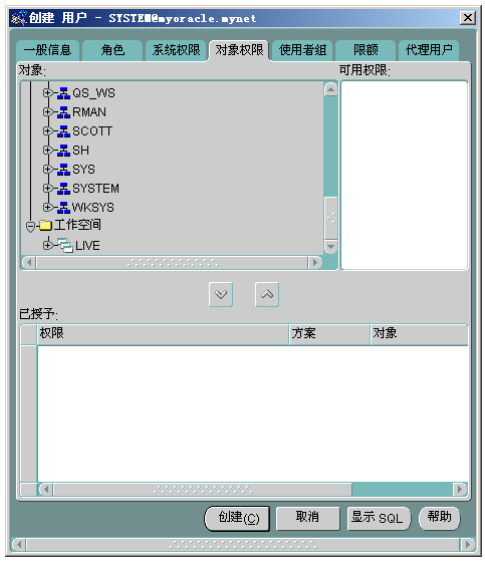


图 8.5　创建用户的【对象权限】选项卡

（6）图 8.6 所示为创建用户的【使用者组】选项卡。

（7）图 8.7 所示为创建用户的【限额】选项卡。

图 8.6　创建用户的【使用者组】选项卡

图 8.7　创建用户的【限额】选项卡

（8）如图 8.8 所示为创建用户的【代理用户】选项卡。

（9）成功创建用户后出现如图 8.9 所示界面。

图 8.8　创建用户的【代理用户】选项卡

图 8.9　【成功创建用户】界面

（10）上述过程对应的 SQL 代码如下。

```
CREATE USER "TEMPUSER"  PROFILE "DEFAULT"
    IDENTIFIED BY "tempuser" DEFAULT TABLESPACE "USERS"
    ACCOUNT UNLOCK;
GRANT CREATE ANY TABLE TO "TEMPUSER" WITH ADMIN OPTION;
GRANT "CONNECT" TO "TEMPUSER" WITH ADMIN OPTION;
```

```
BEGIN
    dbms_resource_manager_privs.grant_switch_consumer_group(
        grantee_name => 'TEMPUSER',
        consumer_group => 'DEFAULT_CONSUMER_GROUP',
        grant_option => TRUE
    );
END;
BEGIN
    dbms_resource_manager.set_initial_consumer_group(
        user => 'TEMPUSER',
        consumer_group => 'DEFAULT_CONSUMER_GROUP'
    );
END;
```

【参见光盘文件】: 第 8 章\createtempuser.sql。

8.2.3 在【SQLPlus Worksheet】中如何创建用户

（1）在【SQLPlus Worksheet】中不能直接执行 createtempuser.sql 文件完成用户的创建，否则将出现错误。

（2）将 createtempuser.sql 文件的执行分成 3 个步骤。

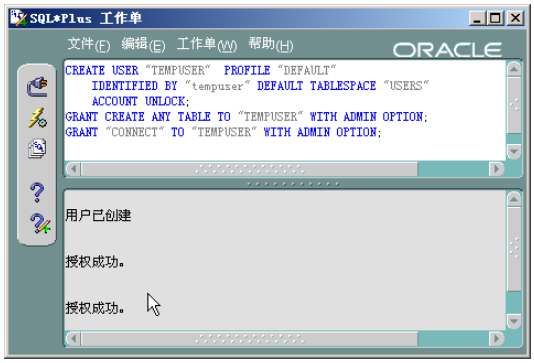
（3）首先执行以下代码，执行结果如图 8.10 所示。

```
/*【一般信息】选项卡的配置*/
CREATE USER "TEMPUSER"  PROFILE "DEFAULT"
    IDENTIFIED BY "tempuser" DEFAULT TABLESPACE "USERS"
    ACCOUNT UNLOCK;
/*【系统权限】选项卡的配置*/
GRANT CREATE ANY TABLE TO "TEMPUSER" WITH ADMIN OPTION;
/*【对象权限】选项卡的配置*/
GRANT "CONNECT" TO "TEMPUSER" WITH ADMIN OPTION;
```

【参见光盘文件】: 第 8 章\createtempuser-1.sql。

（4）然后在【SQLPlus Worksheet】中执行下列代码，执行结果如图 8.11 所示。

```
/*【使用者组】选项卡的配置，授予切换资源使用者组的权限*/
BEGIN
    dbms_resource_manager_privs.grant_switch_consumer_group(
        grantee_name => 'TEMPUSER',
        consumer_group => 'DEFAULT_CONSUMER_GROUP',
        grant_option => TRUE
    );
END;
```



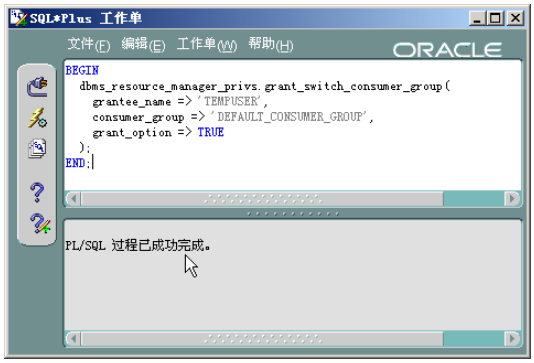


图 8.10　在【SQLPlus Worksheet】中创建用户第 1 步图 8.11　在【SQLPlus Worksheet】中创建用户第 2 步

（5）最后在【SQLPlus Worksheet】中执行下列代码，执行结果如图 8.12 所示。

```
/*【使用者组】选项卡的配置，设置初始化资源使用者组*/
BEGIN
    dbms_resource_manager.set_initial_consumer_group(
        user => 'TEMPUSER',
        consumer_group => 'DEFAULT_CONSUMER_GROUP'
    );
END;
```

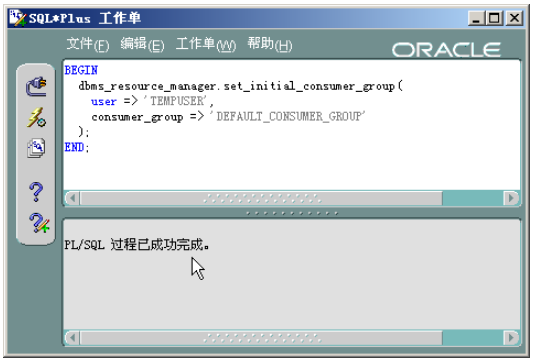


图 8.12　在【SQLPlus Worksheet】中创建用户第 3 步

8.2.4　创建用户中常见问题及解决方法

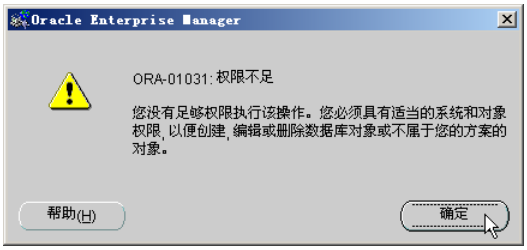


图 8.13　创建用户中权限不足的提示信息

8.2.5　用户的修改

（1）如图 8.14 所示。

（2）在出现的各选项卡中可以修改用户的各种配置参数。对应用户的修改的 SQL 语句为“ALTER USER”。

实例 1：将用户账号的状态设置为“锁定”的 SQL 代码如下。

```
ALTER  USER "TEMPUSER"  ACCOUNT  LOCK
```

【参见光盘文件】：第 8 章\locktempuser.sql。

实例 2：修改用户的验证口令为“TEMP”的 SQL 代码如下。

```
ALTER USER "TEMPUSER" IDENTIFIED BY "temp"
```

【参见光盘文件】：第 8 章\passwordtempuser.sql。

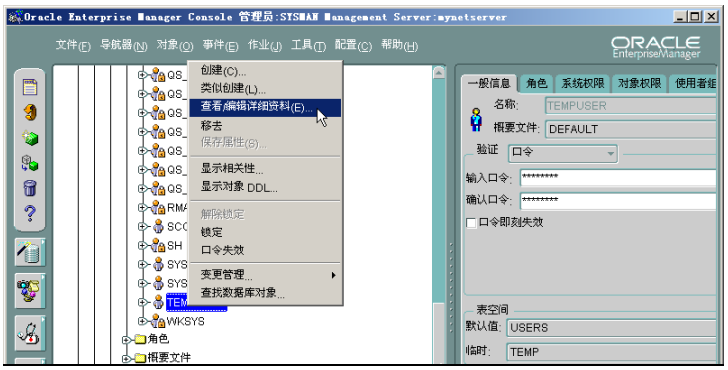


图 8.14　选择修改用户

8.2.6　用户的删除

（1）如图 8.15 所示的【用户删除确认】界面。

图 8.15　【用户删除确认】界面

（2）上述过程对应的 SQL 代码如下。

```
 DROP  USER  TEMPUSER CASCADE
```

【参见光盘文件】：第 8 章\droptempuser.sql。

8.3　角色的管理

8.3.1　Oracle 9i 预定义的角色

表 8.2　　Oracle 9i 预定义的角色

角色名称	说明
CONNECT	数据库连接角色，用于连接数据库，具有创建簇、数据库链接、序列、同义词、表和视图，以及修改会话的权利
DBA	数据库管理员角色，具有所有使用 ADMIN 选项创建的系统权限，可以将系统权限授予其他用户或角色
DELETE_CATALOG_ROLE	删除目录角色，可以删除或重建数据字典
EXECUTE_CATALOG_ROLE	执行目录角色，能够执行所有系统包
EXP_FULL_DATABASE	能够使用导出程序执行数据库的完全和增量导出
IMP_FULL_DATABASE	能够使用导入程序执行数据库的完全导入
RESOURCE	可以创建簇、表、序列以及 PL/SQL 编程用方案对象，包括过程、程序包、触发器等
SELECT_CATALOG_ROLE	查询数据字典表或视图

8.3.2　在【企业管理器】中创建角色

（1）如图 8.16 所示。

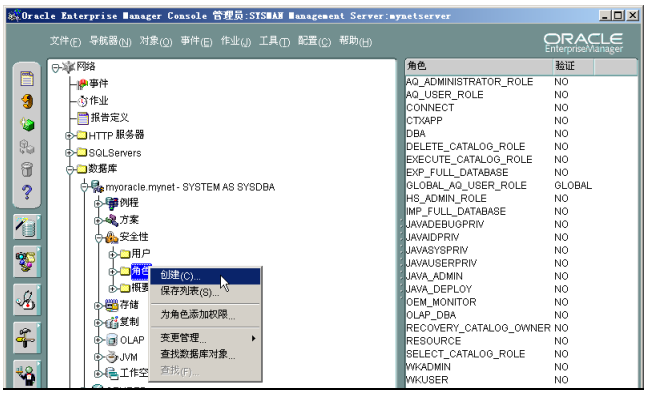


图 8.16　选择创建角色

（2）出现如图 8.17 所示的创建角色的【一般信息】选项卡。

（3）图 8.18 所示为创建角色的【角色】选项卡。用于为多个角色分配子角色。

图 8.17　创建角色的【一般信息】选项卡

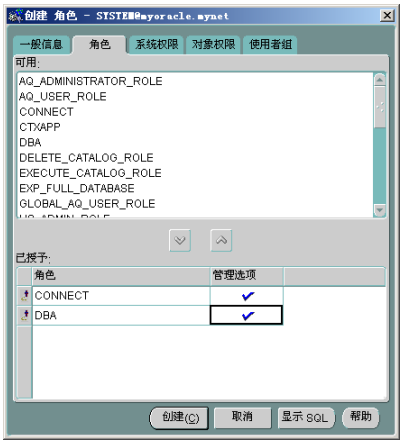


图 8.18　创建角色的【角色】选项卡

（4）图 8.19 所示为创建角色的【系统权限】选项卡。

（5）如图 8.20 所示为创建角色的【对象权限】选项卡。

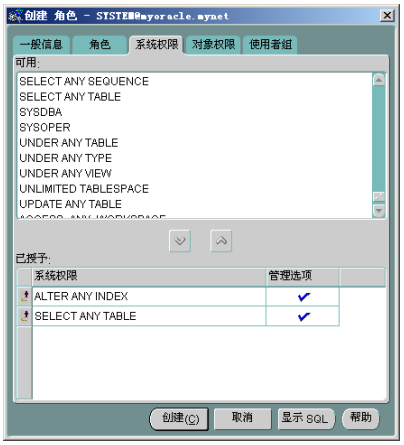


图 8.19　创建角色的【系统权限】选项卡

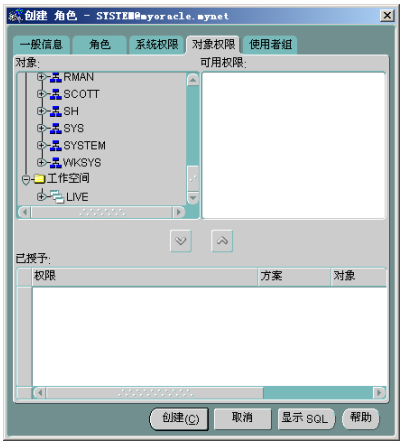


图 8.20　创建角色的【对象权限】选项卡

（6）图 8.21 所示为创建角色的【使用者组】选项卡。

（7）成功创建角色后出现如图 8.22 所示界面。

图 8.21　创建角色的【使用者组】选项卡

图 8.22　【成功创建角色】界面

（8）上述过程创建角色的 SQL 代码如下。

```
CREATE ROLE "TEMPROLE"
    IDENTIFIED BY "temprole";
GRANT ALTER ANY INDEX TO "TEMPROLE" WITH ADMIN OPTION;
GRANT SELECT ANY TABLE TO "TEMPROLE" WITH ADMIN OPTION;
GRANT "CONNECT" TO "TEMPROLE" WITH ADMIN OPTION;
GRANT "DBA" TO "TEMPROLE" WITH ADMIN OPTION;
BEGIN
    dbms_resource_manager_privs.grant_switch_consumer_group(
        grantee_name => 'TEMPROLE',
        consumer_group => 'DEFAULT_CONSUMER_GROUP',
        grant_option => FALSE
    );
END;
```

【参见光盘文件】：第 8 章\createrole.sql。

8.3.3　在【SQLPlus Worksheet】中创建角色

（1）在【SQLPlus Worksheet】中直接执行 createrole.sql 文件将完成角色的创建，执行结果如图 8.23 所示。

（2）表明已经成功创建角色 TEMPROLE。

图 8.23　在【SQLPlus Worksheet】中创建角色

8.3.4　角色的修改

（1）如图 8.24 所示。

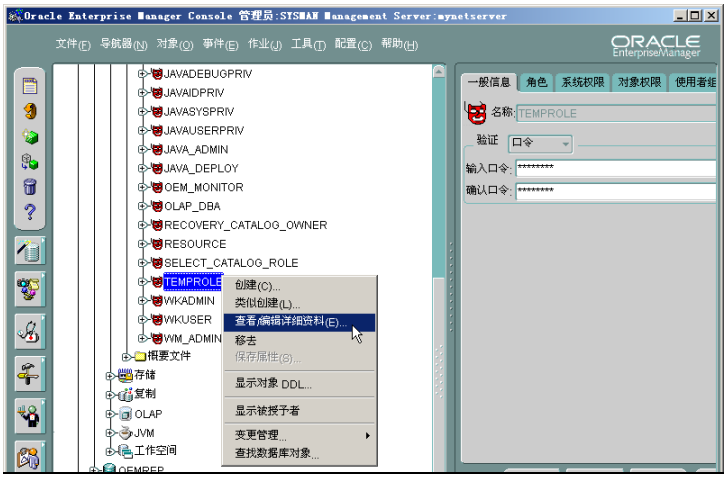


图 8.24　选择修改角色

（2）在出现的各选项卡中可以修改角色的各种配置参数，对应角色的修改的 SQL 语句为“ALTER ROLE”或者“REVOKE”。

实例 1：将角色的验证方式更改为“外部”的 SQL 代码如下。

```
ALTER ROLE "TEMPROLE"  IDENTIFIED EXTERNALLY;
```

```
--------------------------------------------------------------------------------
```

【参见光盘文件】：第 8 章\alterrole.sql。

实例 2：将角色的系统权限“DBA”删除的 SQL 代码如下。

```
--------------------------------------------------------------------------------
REVOKE "DBA"  FROM "TEMPROLE";
--------------------------------------------------------------------------------
```

【参见光盘文件】：第 8 章\revokerole.sql。

8.3.5　角色的删除

（1）如图 8.25 所示【角色删除确认】界面。

图 8.25　【角色删除确认】界面

（2）上述过程对应的 SQL 代码如下。

```
--------------------------------------------------------------------------------
  DROP  ROLE  TEMPROLE;
--------------------------------------------------------------------------------
```

【参见光盘文件】：第 8 章\droprole.sql。

8.4　概要文件的管理

8.4.1　在【企业管理器】中创建概要文件

（1）如图 8.26 所示。

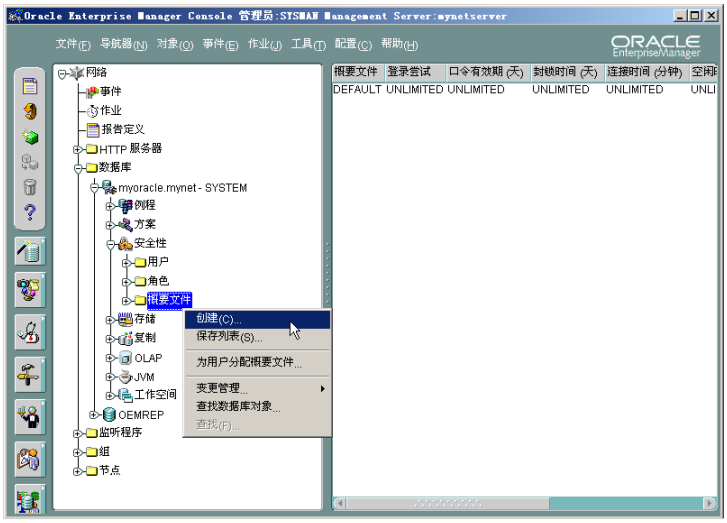


图 8.26　选择创建概要文件

（2）出现如图 8.27 所示的创建概要文件的【一般信息】选项卡。

图 8.27　创建概要文件的【一般信息】选项卡

（3）图 8.28 所示为创建概要文件的【口令】选项卡。

图 8.28　创建概要文件的【口令】选项卡

（4）出现如图 8.29 所示界面。

图 8.29　【成功创建概要文件】界面

（5）按照上述配置创建概要文件的 SQL 代码如下。

```
CREATE PROFILE "TEMPPROFILE"
     /*【一般信息】选项卡对应的配置参数*/
    LIMIT CPU_PER_SESSION 1000
    CPU_PER_CALL 1000
    CONNECT_TIME 30
    IDLE_TIME DEFAULT
    SESSIONS_PER_USER 10
    LOGICAL_READS_PER_SESSION 1000
    LOGICAL_READS_PER_CALL 1000
    PRIVATE_SGA 16K
    COMPOSITE_LIMIT 1000000
    /*【口令】选项卡对应的配置参数*/
    FAILED_LOGIN_ATTEMPTS 3
    PASSWORD_LOCK_TIME 5
    PASSWORD_GRACE_TIME 60
    PASSWORD_LIFE_TIME 30
    PASSWORD_REUSE_MAX DEFAULT
    PASSWORD_REUSE_TIME 30
    PASSWORD_VERIFY_FUNCTION DEFAULT
```

【参见光盘文件】：第 8 章\createprofile.sql。

8.4.2　在【SQLPlus Worksheet】中创建概要文件

在【SQLPlus Worksheet】中直接执行 createprofile.sql 文件将完成概要文件的创建，执行结果如图 8.30 所示。表明已经成功创建概要文件 TEMPPROFILE。

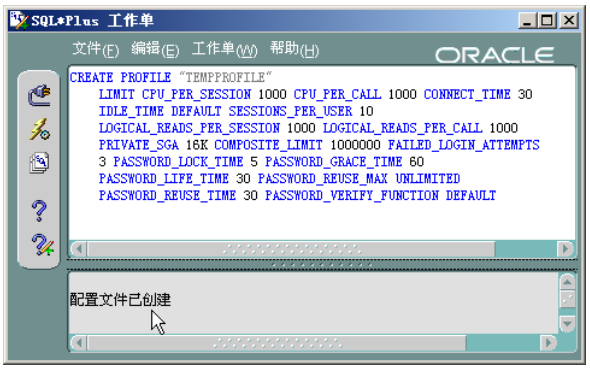


图 8.30　在【SQLPlus Worksheet】中创建概要文件

8.4.3　概要文件的修改

（1）如图 8.31 所示。

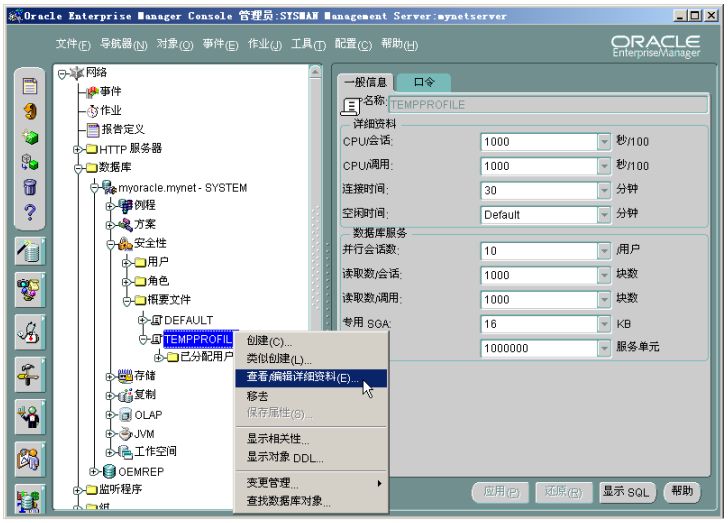


图 8.31　选择修改概要文件

（2）在出现的编辑概要文件的【一般信息】和【口令】选项卡中可以修改概要文件的配置参数，对应修改概要文件的 SQL 语句为“ALTER PROFILE”。

实例：将 CPU/会话参数设置为 6000 的 SQL 代码如下。

```
ALTER PROFILE "TEMPPROFILE"  LIMIT CPU_PER_SESSION 6000
```

【参见光盘文件】：第 8 章\alterprofile.sql。

8.4.4　将概要文件分配给用户

（1）如图 8.32 的【分配概要文件】界面。

图 8.32　【分配概要文件】界面

（2）上述过程对应的 SQL 代码如下。

```
ALTER  USER  TEMPUSER  PROFILE  TEMPPROFILE;
```

【参见光盘文件】：第 8 章\alteruserprofile.sql。

8.4.5　概要文件的删除

（1）如图 8.33 所示的【概要文件删除确认】界面。

（2）删除概要文件的 SQL 代码如下。

```
DROP  PROFILE  TEMPPROFILE
```

【参见光盘文件】：第 8 章\dropprofile.sql。

图 8.33　【删除概要文件确认】界面

8.5 审计

8.5.1 审计的作用

1. 审查可疑的活动
2. 监视和收集关于指定数据库活动的数据

8.5.2 审计的类型

1. 语句审计（STATEMENT AUDITING）
2. 权限审计（PRIVILEGE AUDITING）
3. 对象审计（OBJECT AUDITING）

8.5.3 审计的信息

AUD$表记录的审计信息包括。

- SESSIONID：会话的数字 ID。
- ENTRYID：审计信息项的 ID。
- STATEMENT：每个执行的命令的数字 ID。
- TIMESTAP#：设计信息生成的日期和时间。
- USERID：被审计的用户使用的 Oracle 用户 ID。
- USERHOST：被审计的用户使用的数据库例程的数字 ID。
- TERMINAL：被审计的用户的操作系统终端描述字。
- ACTION#：被审计的操作的标识。
- RETURNCODE：每个被审计的命令执行后的返回代码，若为 0，表明操作成功。
- OBJ$CREATOR：被一个操作影响到的对象的创建者（对操作审计）。
- OBJ$NAME：被一个操作影响到的对象的名称（对操作审计）。
- AUTH$PRIVILEGES：使用的系统权限。
- AUTH$GRANTEE：使用的对象权限。
- NEW$OWNER：在列 NEW_NAME 中命名的对象的所有者。
- NEW$NAME：在列 NEW_NAME 中命名的对象的名称。
- SES$ACTIONS：会话小结的字符串，记录了不同操作的成功和失败的信息。
- SES$TID：会话的事务 ID。
- LOGOFF$LREAD：在会话中执行的逻辑读个数。
- LOGOFF$PREAD：在会话中执行的物理读个数。
- LOGOFF$LWRITE：在会话中执行的逻辑写个数。
- LOGOFF$DEAD：在会话中检测到的死锁个数。
- LOGOFF$TIME：用户退出系统的日期和时间。
- COMMENT$TEXT：对设计信息项的文本注释。
- CLIENTID：客户机 ID。
- SPARE1：备用。

- SPARE2：备用。
- OBJ$LABEL：与对象关联的标签。
- SES$LABEL：与会话关联的标签。
- PRIV$USED：执行操作的系统权限。
- SESSIONCPU：会话占用的 CPU 时间。

8.5.4　审计的启动

如图 8.34 所示的编辑数据库配置的【所有参数】选项卡。

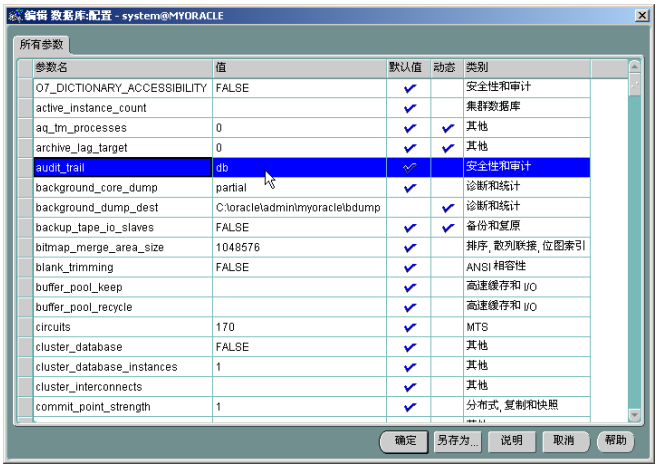


图 8.34　编辑数据库配置的【所有参数】选项卡

8.5.5　审计的实例

（1）以 SYSTEM 用户登录【SQLPlus Worksheet】，执行如下 SQL 代码，执行结果如图 8.35 所示。

```
AUDIT SESSION;
```

【参见光盘文件】：第 8 章\auditsession.sql。

图 8.35　审计数据库的断开及连接操作

（2）以 SCOTT 用户登录另外一个【SQLPlus Worksheet】。

（3）查询 AUD$表的内容，主要的审计信息如下。

```
SESSIONID：518
ENTRI\YID：1
STATEMENT：1
TIMESTAMP#：13-二月 -2003 11:28:24 AM
USERID：SCOTT
TERMINAL：MYNETSERVER
ACTION#：100
RETURNCODE：0
COMMENT$TEXT：Authenticated by: DATABASE; Client address:
              ADDRESS=(PROTOCOL=tcp)(HOST=128.0.0.1)(PORT=1088))
SPARE1：MYNETSERVER\Administrator
PRIV$USED：5
```

8.6　习题

（1）Oracle 9i 的安全性体系包含哪些内容？

（2）什么是 Oracle 9i 的系统安全性机制和数据安全性机制？

（3）Oracle 9i 默认的用户及口令是什么？各有什么身份？

（4）试通过实验熟悉创建用户、删除和修改用户的方法。

（5）角色有什么作用？

（6）试通过实验熟悉创建角色、删除和修改角色的方法。

（7）概要文件有什么作用？

（8）试通过实验熟悉创建概要文件、删除和修改概要文件的方法。

（9）审计有什么作用？

（10）试通过实验熟悉审计的使用。