

19

管理用户

ORACLE®

Copyright © Oracle Corporation, 2001. All rights reserved.

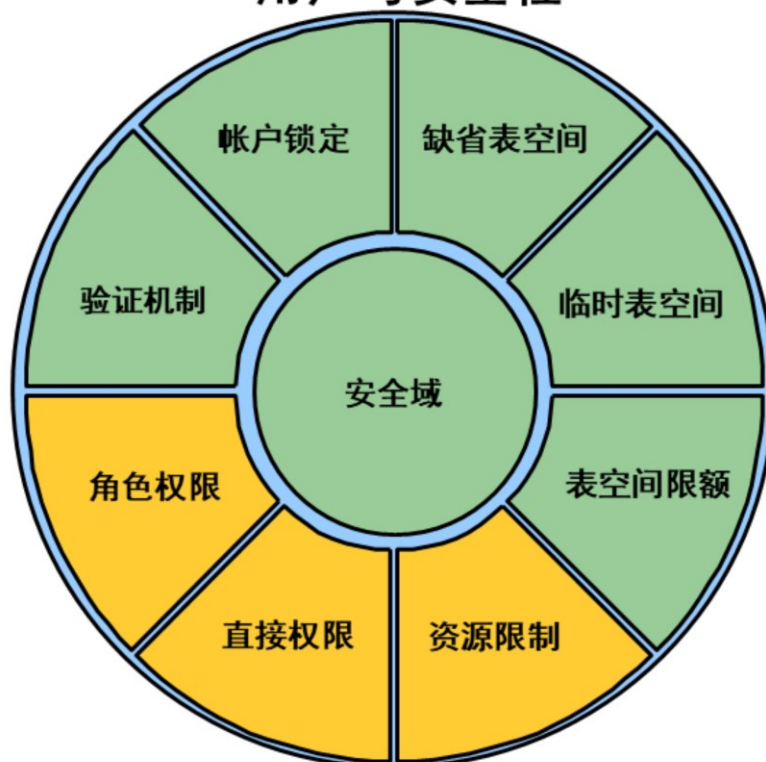
目标

完成这一课的学习后，您应该能达到下列目标：

- 创建新的数据库用户
- 改变和删除现有数据库用户
- 监视有关现有用户的信息

ORACLE

用户与安全性



ORACLE

15-3

Copyright © Oracle Corporation, 2001. All rights reserved.

用户与安全性

安全域：

数据库管理员负责定义可以访问数据库的用户名。安全域定义应用于用户的设置。

验证机制：

可通过以下方式之一对需要访问数据库的用户进行验证：

- 数据字典
- 操作系统
- 网络

验证方法是在数据库中定义用户时指定的，之后可随时改变。本课仅讨论通过数据库和操作系统进行验证的方式。

注：有关通过角色进行操作系统验证的详细信息，请参考“Oracle 服务器入门”一课。有关通过网络验证的方式，请参考 *Oracle 数据库管理基础 II* 这部分的课程。

用户与安全性（续）

表空间限额：

表空间限额控制分配给数据库中表空间用户的物理存储空间的大小。

缺省表空间：

如果用户在创建段时不明确指定表空间，那么缺省表空间会定义用户所创建段的存储位置。

临时表空间：

如果用户执行的操作要求将排序数据写入磁盘，那么临时表空间会定义 Oracle 服务器分配哪些区。

帐户锁定：

可锁定帐户以防止用户登录数据库。可以设置自动锁定，也可由数据库管理员手动锁定帐户或解除锁定。

资源限制：

可以对某些资源的使用加以限制，如：CPU 时间、逻辑输入/输出 (I/O) 以及用户打开的会话数目。

直接权限：

权限用于控制用户能在数据库中执行的操作。

角色权限：

可通过使用角色间接授予用户权限。

注：有关角色权限的信息，请参考“管理权限”与“管理角色”这两课。

本课讨论通过适当的验证机制定义用户、限制系统中用户对空间的使用和手动控制帐户锁定。

数据库方案

- 方案是一个特定的对象集合。
- 创建用户时，就会创建一个对应的方案。
- 一个用户只能与一个方案关联。
- 用户名和方案经常交换使用。

方案对象

表

触发器

约束

索引

视图

序列

存储程序单元

同义词

用户定义的数据类型

数据库链接

数据库方案

方案是与某个用户关联的表、视图、簇、过程和程序包等对象的特定集合。创建数据库用户时，就会相应地为该用户创建同名的方案。用户只能与同名的方案关联，因此用户名和方案经常互用。

该幻灯片显示用户能在 Oracle 数据库中拥有的某些对象。

创建对象

类别	语句
序列	Create sequence xxx start with xxx increment by xxx minvalue nocache
同义词	Create synonym xxx for xxx
数据库链接	Create database link xxx connect to xxx identified by xxx using 'xxx'

ORACLE

创建用户操作的核对清单

- 确定用户需要在其中存储对象的表空间。
- 确定每个表空间的限额。
- 指定一个缺省表空间与临时表空间。
- 创建用户。
- 向用户授予权限与角色。

ORACLE®

创建新用户： 数据库验证

设置初始口令：

```
CREATE USER aaron  
IDENTIFIED BY soccer  
DEFAULT TABLESPACE data  
TEMPORARY TABLESPACE temp  
QUOTA 15M ON data  
QUOTA 10M ON users  
PASSWORD EXPIRE;
```

ORACLE

15-8

Copyright © Oracle Corporation, 2001. All rights reserved.

创建新用户：数据库验证

语法：

使用以下命令创建新用户：

```
CREATE USER user  
IDENTIFIED {BY password | EXTERNALLY}  
[ DEFAULT TABLESPACE tablespace ]  
[ TEMPORARY TABLESPACE tablespace ]  
[ QUOTA {integer [K | M] | UNLIMITED } ON tablespace  
[ QUOTA {integer [K | M] | UNLIMITED } ON tablespace  
...] ]  
[ PASSWORD EXPIRE ]  
[ ACCOUNT { LOCK | UNLOCK } ]  
[ PROFILE { profile | DEFAULT } ]
```


创建新用户：数据库验证（续）

语法（续）：

其中：

User：是用户名

BY password：指定用户在登录时需通过数据库验证，还必须提供口令

EXTERNALLY：指定用户需通过操作系统验证

GLOBALLY AS：指定对用户进行全局验证

DEFAULT 或 TEMPORARY TABLESPACE：为用户标识缺省或临时表空间

QUOTA：定义表空间中允许用户拥有对象所具有的最大空间（可将限额定义为整数字节或千字节/兆字节。关键字 UNLIMITED 用于指定用户拥有的对象可使用表空间内的全部可用空间。缺省情况下，用户在任何表空间上都没有限额。）

PASSWORD EXPIRE：强制用户在使用 SQL*Plus 登录到数据库时重置口令（该选项仅在用户通过数据库进行验证时有效）。

ACCOUNT LOCK/UNLOCK：可用于显式锁定或解除锁定用户帐户（UNLOCK 为缺省设置）

PROFILE：用于控制资源使用和指定用户的口令控制机制。

注：有关创建配置文件的信息，请参考“管理配置文件”一课。

口令验证方法是必需的。如果指定了口令，则 Oracle 服务器将在数据字典中对其进行维护。用户通过服务器进行验证时，可使用 Oracle 服务器提供的口令控制机制。

设置了口令之后，当用户使用 SQL*Plus 登录时将接收到下列登录消息，同时系统提示用户输入新口令：

ERROR:

ORA-28001: 该帐户已过期

更改 PETER 的口令

旧口令:

新口令:

重新键入新口令:

口令已更改

创建新用户：操作系统验证

OS_AUTHENT_PREFIX 初始化参数用于指定用户名的格式。

缺省为 OPS\$。

Windows平台，若不在域内需设置注册表中

HKEY_LOCAL_MACHINE\SOFTWARE\ORACLE\KEY_OraDb19g_home1下建立串**OSAUTH_PREFIX_DOMAIN**为**false**

```
CREATE USER ops$administrator
IDENTIFIED EXTERNALLY
DEFAULT TABLESPACE USERS
TEMPORARY TABLESPACE temp
QUOTA 15m ON data
PASSWORD EXPIRE;
```

ORACLE

15-10

Copyright © Oracle Corporation, 2001. All rights reserved.

创建新用户：操作系统验证

操作系统验证：

用 CREATE USER 命令的 IDENTIFIED EXTERNALLY 子句指定用户必须通过操作系统进行验证。当用户直接登录到运行 Oracle 服务器的计算机上时，该选项通常很有用。

操作系统验证的用户名：

OS_AUTHENT_PREFIX 初始化参数用来指定操作系统验证的用户名的格式。该参数的缺省值为 OPS\$，以便与 Oracle 服务器的早期版本向后兼容。要将前缀设置为 NULL 值，请将该初始化参数指定为：

```
OS_AUTHENT_PREFIX = ''
```

幻灯片中的示例显示如何在数据库内定义用户 aaron。此处指定允许操作系统用户 administrator 无需经过 Oracle 服务器验证即可访问数据库。因此，若要使用 SQL*Plus 登录到系统，则用户 administrator 必须从该操作系统输入下列命令：

```
d:\> sqlplus /
```

创建新用户：操作系统验证（续）

操作系统验证的用户名：

注：

- 使用 OS_AUTHENT_PREFIX=OPS\$ 时：提供了灵活的用户验证方式，既可通过操作系统进行验证，也可通过 Oracle 服务器进行验证。在这种情况下，DBA 可通过输入下列格式的命令创建用户：

```
CREATE USER ops$user  
IDENTIFIED BY password ...
```

- 登录到运行 Oracle 服务器的计算机上的用户无需提供口令。如果用户从远程客户机连接，则可提供口令以实现连接。
- 设置另一个初始化参数 REMOTE_OS_AUTHENT=TRUE，指定用户可通过远程操作系统进行验证。缺省值 FALSE 表示用户只能通过运行 Oracle 服务器的计算机进行验证。应小心使用该参数，因为可能存在安全隐患。
- 如果数据库中的某些用户通过操作系统进行验证，则更改 OS_AUTHENT_PREFIX 可防止这些用户登录到数据库。

更改用户的表空间限额

- 在下列情况下需要修改用户的表空间限额：
 - 当用户所拥有表的增长速度异常快时。
 - 当应用程序得到增强而要求额外的表或索引时。
 - 当重新安排对象并将其置入不同的表空间时。
- 修改用户的表空间限额：

```
ALTER USER aaron  
QUOTA 0 ON USERS;
```

ORACLE

15-12

Copyright © Oracle Corporation, 2001. All rights reserved.

更改用户的表空间限额

使用下列命令修改表空间限额或重新分配表空间：

```
ALTER USER user  
[ DEFAULT TABLESPACE tablespace]  
[ TEMPORARY TABLESPACE tablespace]  
[ QUOTA {integer [K | M] | UNLIMITED } ON tablespace  
[ QUOTA {integer [K | M] | UNLIMITED } ON tablespace ]  
...]
```

如果分配的限额为 0，用户拥有的对象仍保留在撤消的表空间内，但不能给它们分配新的空间。例如，如果表空间 USERS 内有一个 10 MB 的表，若将该表空间的限额改为 0，则不能再为该表分配新区。

任何未更改的选项保持不变。

注：对于 UNLIMITED TABLESPACE 权限应格外注意，因为它优先于限额设置。

删除用户

- 如果方案中含有对象，请使用 **CASCADE** 子句删除该方案中的所有对象。

```
DROP USER aaron;
```

- 不能删除当前与 **Oracle** 服务器连接的用户。

```
DROP USER aaron CASCADE;
```

ORACLE

15-13

Copyright © Oracle Corporation, 2001. All rights reserved.

删除用户

```
DROP USER user [CASCADE]
```

原则：

- 在删除用户前，**CASCADE** 选项将删除方案中的所有对象。如果方案中包含任何对象，则必须指定该选项。
- 不能删除当前与 **Oracle** 服务器连接的用户。

获取用户信息

可以通过查询以下视图来获取有关用户的信息：

- **DBA_USERS**
- **DBA_TS_QUOTAS**

ORACLE

15-14

Copyright © Oracle Corporation, 2001. All rights reserved.

获取用户信息

使用以下查询查找用于所有用户的 default_tablespace。

```
SQL> SELECT username, default_tablespace
2    FROM dba_users;
```

USERNAME	DEFAULT_TABLESPACE
-----	-----
SYS	SYSTEM
SYSTEM	SYSTEM
OUTLN	SYSTEM
DBSNMP	SYSTEM
HR	SAMPLE
OE	SAMPLE

小结

在这一课中，您应该能够掌握：

- 通过指定适当的口令机制来创建用户
- 控制用户对空间的使用

ORACLE®