Bài thực hành số 1
QUẢN LÝ NGƯỜI DÙNG

❖ ***Tóm tắt nội dung:***

- Tablespace
- Schema
- User
- Resource (tài nguyên)
- Profile

I. Giới thiệu

A. Lý thuyết

1. Oracle Database Enterprise Edition

- Hãng Oracle cung cấp cho khách hàng các gói sản phẩm đa dạng với nhiều phiên bản khác nhau, thích hợp cho những những quy mô và mục đích khác nhau. Trong chương trình thực hành này, chúng ta sẽ sử dụng sản phẩm ***Oracle Database 10g Release 2 (10.2)*** hoặc ***Oracle Database 11g Release 2 (11.2)***, phiên bản ***Oracle Database Enterprise Edition***. Hai sản phẩm 10g và 11g có nhiều điểm khác nhau, tuy nhiên những điểm đó không ảnh hưởng đến chương trình thực hành này.
- Nhìn chung *Oracle Database* có tất cả 5 phiên bản:
  - ✓ Oracle Database Express Edition (Oracle Database XE)
  - ✓ Oracle Database Standard Edition One
  - ✓ Oracle Database Standard Edition
  - ✓ Oracle Database Personal Edition
  - ✓ Oracle Database Enterprise Edition
- Trong các phiên bản trên, *Express Edition* là phiên bản đơn giản nhất, download nhanh chóng, cài đặt và quản lý đơn giản, miễn phí cho lập trình, triển khai và mở rộng.

- Ngược lại với *Express Edition*, *Enterprise Edition* là phiên bản mạnh mẽ nhất, cung cấp nhiều tính năng bảo mật cao cấp, giúp cho các công ty quản lý, truy xuất các nguồn tài nguyên và dữ liệu hữu hiệu và tiện lợi hơn. Bên cạnh đó, *Personal Edition* là một sản phẩm đặc biệt, có chứa hầu hết các tính năng cao cấp của *Enterprise Edition*, phù hợp cho môi trường phát triển và triển khai 1 người dùng.
- Chương trình của chúng ta có các bài về *Virtual Private Database*, *Oracle Label Security* và *Fine-grained Auditing*. Đây là những công nghệ và tính năng chỉ có ở phiên bản *Enterprise Edition*.
- Phần mềm cài đặt có thể được tải về để sử dụng miễn phí cho mục đích học tập từ trang web chính thức của Oracle (SV cần đăng ký tài khoản miễn phí để có thể download được).

2. Phân biệt một số khái niệm

- **SQL**
  - ✓ Là một **ngôn ngữ khai báo** dùng để truy vấn, làm việc trên các cơ sở dữ liệu quan hệ. Ngôn ngữ này đã được chuẩn hóa để các cơ sở dữ liệu quan hệ của các hãng khác nhau có hỗ trợ SQL đều sẽ tuân thủ những quy định do chuẩn đưa ra.
  - ✓ SQL cũng được Oracle Database hỗ trợ. Một ví dụ về câu lệnh SQL:

```
SELECT COUNTRY_ID, COUNTRY_NAME FROM HR.COUNTRIES;
```

- **PL/SQL**
  - ✓ Là **ngôn ngữ thủ tục của Oracle**, dùng để viết các điều khiển của ứng dụng (application logic) và để thao tác dữ liệu bên ngoài CSDL.
  - ✓ Có thể bao gồm một tập con các lệnh SQL khi có yêu cầu truy xuất dữ liệu.
  - ✓ Có sẵn khi cài đặt Oracle Database.
- **SQL*Plus**
  - ✓ Là một **sản phẩm Oracle**, trong đó có thể dùng các ngôn ngữ SQL và PL/SQL. SQL*Plus có giao diện dạng màn hình lệnh (command line).
  - ✓ Ngoài ra còn có các ngôn ngữ lệnh riêng để điều khiển hành vi của sản phẩm và định dạng kết xuất từ các truy vấn SQL.
  - ✓ Tóm lại, SQL và PL/SQL là các ngôn ngữ dùng trong một số sản phẩm Oracle. SQL*Plus chỉ là một trong các sản phẩm có hỗ trợ chúng.

- ✓ Để tham khảo các lệnh sử dụng trong SQL*Plus, ta tra cứu trong ebook *SQL*Plus User's Guide and Reference* nằm trong bộ thư viện *Documentation Library* (sẽ được giới thiệu ở phần 3).

- **iSQL*Plus**
  - ✓ Là phiên bản web của SQL*Plus với giao diện trực quan, thân thiện với người dùng hơn. Tuy nhiên có một số câu lệnh và chức năng có thể thực hiện trong SQL*Plus nhưng không thể thực hiện trong iSQL*Plus.
  - ✓ Vì một số vấn đề về bảo mật và tốn chi phí hỗ trợ nên Oracle đã ngưng cung cấp iSQL*Plus trong Oracle Database 11g. Người dùng có thể sử dụng Oracle SQL Developer để sử dụng các tính năng tương tự của iSQL*Plus.

3. Tài liệu tham khảo

- Bên cạnh nội dung các bài lab, trong quá trình thực hành SV cần phải thường xuyên tra cứu thêm một số tài liệu khác để có cái nhìn rõ ràng hơn về vấn đề đang học.
- Phần này đề nghị hai tài liệu cơ bản mà SV nên đọc kèm để phục vụ cho các bài lab:
  - ✓ D.C. Knox (2004). Effective Oracle Database 10g Security by Design, Oracle Press, ISBN 0-07-223130-0[1].
  - ✓ Oracle Database 10*g* Release 2 (10.2) Documentation Library.

    hoặc

    Oracle Database 11*g* Release 2 (11.2) Documentation Library.
- ***Oracle Database Documentation Library*** là bộ thư viện đầy đủ về toàn bộ phần mềm Oracle Database, được cung cấp bởi chính hãng Oracle. Bộ thư viện này bao gồm nhiều sách khác nhau, mô tả các chức năng từ cơ bản đến nâng cao và được trình bày theo cấu trúc rõ ràng, thuận tiện cho mục đích tham khảo.
- Đây là một số tựa sách (trong bộ thư viện trên) mà chúng ta sẽ tra cứu thường xuyên trong quá trình thực hành:
  - ✓ Concepts: cung cấp các khái niệm lý thuyết về toàn bộ cơ sở dữ liệu.
  - ✓ SQL Reference: dùng để tra cứu cú pháp và ý nghĩa của các câu lệnh SQL.
  - ✓ PL/SQL User's Guide and Reference: nội dung về ngôn ngữ PL/SQL.

[1] Ebook này dành cho Oracle Database 10g nhưng các kiến thức chính về các tính năng bảo mật của Oracle vẫn đúng cho Oracle Database 11g.

- ✓ PL/SQL Packages and Types Reference: dùng để tra cứu các packages xây dựng sẵn.

- Bộ thư viện trên có thể được xem online trên trang của Oracle hoặc download về để xem ở dạng PDF hoặc HTML.

B. Thực hành

1. Truy xuất Oracle

Ta có thể truy xuất, làm việc với Oracle Database theo 3 cách:

- Sử dụng **Oracle SQL*Plus**:
  - ✓ Start → All Programs → <Thư mục chương trình Oracle> → Application Development → SLQ Plus.
  - ✓ Cửa sổ chương trình Oracle SQL*Plus hiện ra. Nhập *username* và *password*. *Host string* có thể nhập hoặc không nhập. Khi có nhiều database, nhập vào *host string* tên của database mà mình muốn log in vào.
- Sử dụng **Command Prompt**:
  - ✓ Start → Run → gõ "cmd".
  - ✓ Cửa số Command Prompt xuất hiện. Gõ lệnh sau để đăng nhập CSDL:

    `sqlplus <username>/<password>`

    VD: `sqlplus system/p123`
  - ✓ Để đăng nhập bằng tài khoản SYS với quyền SYSDBA trong CMD, bạn cần dùng lệnh sau:

    `sqlplus SYS/<password> AS SYSDBA`
  - ✓ Nếu đang ở trong tài khoản có quyền **administration** của Windows, SV có thể log in vào tài khoản SYS bằng lệnh:

    `sqlplus / AS SYSDBA`
- Sử dụng **Oracle *i*SQL*Plus**:
  - ✓ Để sử dụng iSQL*Plus: vào một trình duyệt web, gõ địa chỉ URL sau:

    `http://<tên_máy_tính>:5560/isqlplus`

    hoặc `http://localhost:5560/isqlplus`
  - ✓ Nếu đang thực hành ở phòng lab, SV dùng đường link sau:

    `http://<địa_chỉ_server>:5560/isqlplus`

- ✓ Trang iSQL*Plus xuất hiện, nhập các thông số để log in. *Connect Identifier* có cùng ý nghĩa với *Host string* trong SQL*Plus.

- Sử dụng **Oracle SQL Developer** (SV tự tìm hiểu cách sử dụng)

Sau khi đã log in vào hệ thống, mỗi khi muốn log out/log in chuyển qua các tài khoản khác, ta dùng các lệnh sau:

- Log in vào 1 account:

  `CONNECT <username>/<password>`

  hoặc `CONNECT <username>`
- Log in vào tài khoản SYS:

  `CONNECT SYS/<password> AS SYSDBA`

  hoặc `CONNECT / AS SYSDBA` (dùng câu này với điều kiện đang ở trong tài khoản có quyền administration của Windows)
- Log out khỏi 1 account: `disconnect`

Lưu ý khi sử dụng các câu lệnh trên:

- Có thể thay `CONNECT` bằng `CONN`.
- Khi muốn đổi account, chỉ cần gõ lệnh log in vào account khác, không cần phải gõ lệnh log out.
- Trong iSQL*Plus, không thể log in vào tài khoản SYS.

2. Đăng nhập tại phòng lab

- Mỗi sinh viên sẽ được cấp 1 account với thông tin như sau:
  - ✓ Usename: `s<MSSV>`

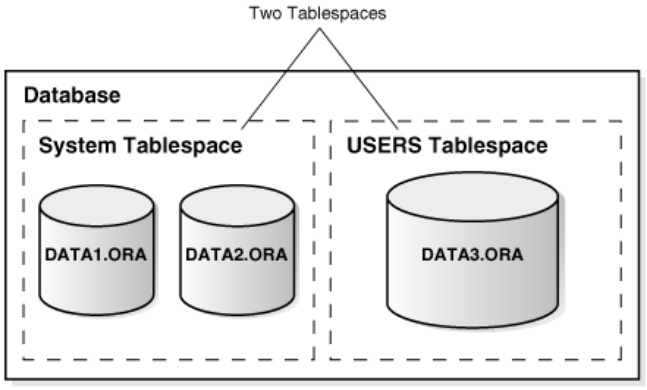
    VD: `s51001234`
  - ✓ Password: `p123`
- Đăng nhập:
  - ✓ Làm việc bằng giao diện isqlplus: http://172.28.14.19:5560/isqlplus
- Sau khi đăng nhập, sinh viên phải đổi password của mình bằng lệnh:

  `ALTER USER username IDENTIFIED BY new_password;`

II. Quản lý User

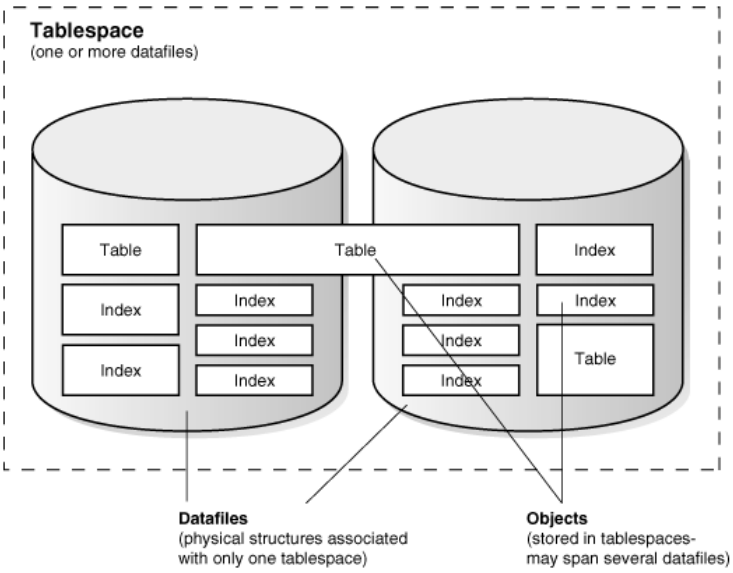
A. Lý thuyết

1. Tablespace



Một CSDL có 2 tablespace SYSTEM và USERS.

Tablespace SYSTEM chứa 2 datafile là DATA1.ORA và DATA2.ORA



Một tablespace chứa 2 datafile.

Bên trong các datafile là các đối tượng, như là table và index.

Các đối tượng trong tablespace có thể nằm trên vài datafile.

- Một CSDL Oracle được chia thành những đơn vị lưu trữ luận lý được gọi là các *tablespace*, nhằm mục đích gom nhóm các cấu trúc luận lý có liên quan với nhau.
- Mỗi CSDL có 1 hoặc nhiều các *tablespace*. Mỗi tablespace chứa 1 hoặc nhiều các

datafile. *Datafile* là các cấu trúc vật lý tương thích với hệ điều hành bên dưới, dùng để lưu trữ dữ liệu của các cấu trúc luận lý trong *tablespace* chứa nó. Kích thước tổng cộng của các *datafile* chính là dung tích lưu trữ tổng cộng của *tablespace* đó.

- Có 2 loại tablespace:
  - ✓ *System tablespace*:
    - Mọi CSDL Oracle đều có 2 *system tablespace* là SYSTEM và SYSAUX, được tạo ra một cách tự động.
    - Chứa thông tin về các *data dictionary views*, các định nghĩa của *stored procedures*, *packages*, và các *database triggers* dưới dạng PL/SQL *program units*, SYSTEM *rollback segment*,…
    - Không nên chứa dữ liệu người dùng trong loại *tablespace* này mặc dù có thể.
  - ✓ *Non-system tablespace*:
    - Dùng để chứa các loại dữ liệu còn lại, đặc biệt là các dữ liệu của người dùng.
- Một cách phân loại khác của tablespace:
  - ✓ *Temporary tablespace*: được sử dụng để dành riêng cho các thao tác sắp xếp dữ liệu.
  - ✓ *Permanent tablespace*: Các *tablespaces* không phải là *temporary tablespaces* được gọi là các *permanent tablespaces*. Các *permanent tablespace* được sử dụng để lưu trữ dữ liệu trong database.

2. Schema

- *Schema* là một tập hợp các đối tượng cơ sở dữ liệu (vd: table, view, index,…).
- Mỗi *schema* được sở hữu bởi một user và có cùng tên với user.
- Không có mối quan hệ nào giữa *schema* và *tablespace*. Các đối tượng thuộc 1 *schema* có thể nằm trên các *tablespace* khác nhau và 1 *tablespace* có thể chứa các đối tượng thuộc nhiều *schema* khác nhau.

B. Thực hành

1. Tạo mới User

a. Tạo 1 user mới với câu lệnh sau:

```
CREATE USER salapati IDENTIFIED BY sammyy1;
User created.
```

Khi tạo mới 1 user, ta có thể quy định về default tablespace, temporary tablespace, quota trên các tablespace, thời hạn hiệu lực của password,… ngay trong câu lệnh tạo user hoặc sẽ chỉ định cụ thể sau này.

b. Hiển thị tablespace của user vừa mới tạo:

```
SELECT default_tablespace, temporary_tablespace
FROM dba_users
WHERE username='SALAPATI';

DEFAULT_TABLESPACE  TEMPORARY_TABLESPACE
------------------- -------------------------
USERS               TEMP
```

Tuy trong câu lệnh tạo user ở trên ta không chỉ định default tablespace và temporary tablespace, Oracle đã tự gán các giá trị mặc định cho user này. Các giá trị này được thiết lập theo tham số của hệ thống. Ta có thể xem các tham số này bằng câu lệnh sau:

```
SELECT * FROM database_properties
WHERE    property_name LIKE '%TABLESPACE';
```

Sử dụng ALTER DATABASE để gán lại các giá trị default tablespace và default temporary tablespace của database (*SV tự tìm hiểu và thực hành ở nhà, không được phép thực hành lệnh này tại lớp*).

c. Log out khỏi user hiện tại và log in bằng user vừa mới tạo, sẽ nhận được thông báo:

```
ERROR:
```

```
Ora-01045: user SALAPATI lacks CREATE SESSION privilege;
logon denied
```

Lý do: user vừa mới tạo chưa được cấp quyền cho phép kết nối đến database. Để user vừa mới tạo có thể login được, ta phải cấp quyền **CREATE SESSION.**

Đăng nhập lại user ban đầu và cấp quyền cho user salapati như sau:

```
GRANT CREATE SESSION TO salapati;
Grant succeeded.
```

d. Khi user mới được tạo ra, nếu ta không cấp các quyền tạo các loại object (table, index,…) thì user đó không thể tạo được các object. Tùy thuộc vào nhu cầu của từng user, ta chỉ nên cấp những quyền cần thiết chứ không nên cấp dư.

Một điều kiện bắt buộc khác để user có thể tạo được các object là ta phải cấp quota cho user trên các tablespace tương ứng. Một user có thể được cấp quota sử dụng trên 1 hoặc nhiều tablespace. Quota có thể limited hoặc unlimited.

Ví dụ sau cho thấy khi user salapati tạo mới 1 bảng sẽ hiển thị thông báo lỗi:

```
GRANT CREATE TABLE TO salapati;
Grant succeeded.
CONNECT salapati/sammyy1
Connected.
CREATE TABLE xyz (name VARCHAR2(30));
create table xyz (name varchar2(30))
*
ERROR at line 1:
ORA-01950: no privileges on tablespace 'USERS'[1]
```

[1] Đối với Oracle 11g Release 2, tính năng mới Deferred Segment Creation được thiết lập mặc định là TRUE sẽ khiến cho các user có quyền CREATE TABLE đều có thể tạo bảng trên bất kỳ tablespace nào bất kể có được cấp quota hay không. Thông báo lỗi ORA-01950 sẽ chỉ xuất hiện khi insert dữ liệu lần đầu tiên vào bảng. Để thực hiện được phần thực hành trên, SV dùng câu lệnh sau để thiết lập lại tham số môi trường cho hệ thống: ALTER SYSTEM SET deferred_segment_creation = FALSE. Để hiểu thêm về vấn đề này, SV có thể tham khảo tại đây:
http://www.dba-oracle.com/t_oracle_deferred_segment_creation.htm
http://docs.oracle.com/cd/E14072_01/server.112/e10595/tables002.htm#CHDGJAGB

Để khắc phục lỗi trên, log in lại vào user sinh viên của mình và thực hiện các câu lệnh sau:

```
ALTER USER salapati
QUOTA 100M ON users;
User altered.
```

Nếu muốn user có thể sử dụng tối đa 1 tablespace nào đó thì dùng cú pháp sau:

```
ALTER USER salapati
QUOTA UNLIMITED ON users;
```

e. Vì một user có thể được cấp quota trên nhiều tablespace khác nhau, nên khi tạo các đối tượng, user có thể chỉ định cụ thể tablespace mà mình muốn tạo đối tượng trên đó. Nếu không chỉ định, hệ thống sẽ tự động tạo trên default tablespace của user đó.

```
CREATE TABLE abc (name varchar2(30)) TABLESPACE users;
```

f. Nếu muốn user có thể tạo object trên bất kỳ tablespace nào thì cấp quyền sau:

```
GRANT UNLIMITED TABLESPACE TO salapati;
Grant succeeded.
```

g. Có thể xem thông tin về quota được cấp cho các user thông qua view **DBA_TS_QUOTAS**

```
SELECT      tablespace_name, username, bytes
FROM        DBA_TS_QUOTAS;
```

h. Có thể gán tablespace lúc tạo mới user như sau:

```
CREATE USER salapati_new IDENTIFIED BY sammyy1
TEMPORARY TABLESPACE TEMPTBS01
DEFAULT TABLESPACE USERS
QUOTA 500M ON USERS;
User created.
```

2. Thay đổi các đặc tính của user

a. Thay đổi password:

```
ALTER USER salapati IDENTIFIED BY susana;
```

Hoặc:

```
ALTER USER salapati IDENTIFIED BY susana REPLACE sammyy1;
```

b. Password expiration:

Ta có thể làm cho 1 password hết hạn bằng 2 cách:

```
ALTER USER salapati IDENTIFIED BY susana PASSWORD EXPIRE;
```

Hoặc

```
ALTER USER salapati PASSWORD EXPIRE;
User altered.
```

Ta cũng có thể bắt buộc password expire ngay khi tạo mới một user:

```
CREATE USER paris IDENTIFIED BY p124 PASSWORD EXPIRE;
```

Sau khi làm expire password các user trên, hãy log in vào các user đó (salapati, paris) và tự rút ra nhận xét.

c. Trạng thái account:

Ta có thể thay đổi trạng thái tài khoản (lock/unlock) của một user để cho phép/không cho phép user đó truy xuất vào CSDL.

```
ALTER USER salapati ACCOUNT LOCK;
ALTER USER paris ACCOUNT UNLOCK;
```

Xem trạng thái tài khoản (Account Status) của tất cả các user:

```
SELECT username, account_status
FROM dba_users;
```

3. Xóa User

```
DROP USER salapati;
User Dropped.
```

Lưu ý: lệnh DROP USER không chỉ xóa user mà còn xóa tất cả object thuộc về user đó. Khi user đã có object thì phải dùng thêm tùy chọn CASCADE:

```
DROP USER salapati CASCADE;
User Dropped.
```

III. User Profile

A. Lý thuyết

1. Profile

- Một profile là một tập hợp có tên của các giới hạn tài nguyên, được gán cho một hay nhiều user trong CSDL Oracle.
- Profile cung cấp một cách quản lý dễ dàng việc giới hạn tài nguyên. Nó giúp giới hạn việc sử dụng quá mức các tài nguyên của toàn hệ thống. Profile cũng là cách để quản lý các chính sách về password.
- Trong một CSDL có thể tạo nhiều profile. Một profile mặc định (tên là DEFAULT) sẽ được dùng để gán cho những user không được gán profile một cách tường minh.
- Lưu ý rằng các giá trị mặc định đều được thiết lập là "unlimited".

2. Các loại tài nguyên

- Một profile có thể mô tả các loại giới hạn tài nguyên sau:
  - ✓ Số lượng các session đồng thời mà user có thể thực hiện.
  - ✓ Thời gian xử lý CPU cho một session của user đó hoặc cho một cuộc gọi (call) tới Oracle bởi 1 câu lệnh SQL.
  - ✓ Số lần đọc luận lý I/O cho một session của user đó hoặc cho một cuộc gọi (call) tới Oracle bởi 1 câu lệnh SQL.
  - ✓ Lượng thời gian nhàn rỗi cho session của user.
  - ✓ Lượng thời gian connect cho một session.
  - ✓ Các quy định về password (số lần cố gắng login thất bại, thời gian hiệu lực của 1 password,…)

B. Thực hành

1. Tạo mới Profile

a. Trước hết, để hệ thống có thể thi hành việc ràng buộc các giới hạn tài nguyên, ta cần enable tham số hệ thống RESOURCE_LIMIT bằng câu lệnh sau:

```
ALTER SYSTEM SET RESOURCE_LIMIT = TRUE;
```

Tham số RESOURCE_LIMIT có giá trị mặc định ban đầu là FALSE.

b. Tạo mới 1 profile bằng câu lệnh sau:

```
CREATE PROFILE app_user LIMIT
   FAILED_LOGIN_ATTEMPTS          3
   SESSIONS_PER_USER              UNLIMITED
   CPU_PER_SESSION                UNLIMITED
   CPU_PER_CALL                   3000
   CONNECT_TIME                   45
   IDLE_TIME                      60
   LOGICAL_READS_PER_SESSION      DEFAULT
   LOGICAL_READS_PER_CALL         1000;
```

Lưu ý, để tạo PROFILE, cần có quyền CREATE PROFILE.

2. Gán profile

a. Có thể gán profile khi vừa tạo user:

```
CREATE USER salapati IDENTIFIED BY sammyy1
TEMPORARY TABLESPACE TEMPTBS01
DEFAULT TABLESPACE USERS
QUOTA 500M ON USERS
PROFILE app_user;
User created.
```

b. Khi tạo mới user, nếu không gán tường minh thì user sẽ được gán profile mặc định:

```
CREATE USER venice IDENTIFIED BY sammyy1;
User created.
SELECT profile FROM dba_users
WHERE username = 'VENICE';
PROFILE
-----------
DEFAULT
```

Để xem thông tin về profile mặc định:

```
SELECT DISTINCT resource_name, limit
FROM dba_profiles
WHERE profile='DEFAULT';
```

c. Gán profile cho 1 user:

```
ALTER USER venice
PROFILE app_user;
```

3. Thay đổi profile

```
ALTER PROFILE app_user LIMIT
SESSIONS_PER_USER 4
FAILED_LOGIN_ATTEMPTS 4;
```

4. Xóa profile

```
DROP PROFILE test CASCADE;
```

IV. Bài Tập

1. Tìm hiểu sự khác biệt của tài khoản SYS và SYSTEM.
2. Tạo một profile "MyPassword" thỏa mãn:
   a) Thời hạn sử dụng là 60 ngày.
   b) Gia hạn 10 ngày.
   c) Số ngày mà sau đó password mới được sử dụng lại là 1 ngày.
   d) Số lần thay đổi password trước khi được sử lại password cũ là 5 lần.
   e) Số lần nhập sai password là 3.
3. Kiểm tra profile vừa tạo:
   a) Tạo mới user John với password p123.
   b) Gán profile "MyPassword" vừa tạo cho user này.
   c) Thực hiện những câu lệnh cần thiết để kiểm tra tác dụng của câu **1d**. Cho biết kết quả.
   d) Hiện tượng gì xảy ra khi nhập password sai 4 lần? Làm sao để khắc phục hậu quả vừa xảy ra?
4. Cho câu lệnh sau:

```
CREATE USER mybear IDENTIFIED BY pretty
DEFAULT TABLESPACE USERS
QUOTA 500M ON SYSTEM;
```

Theo bạn câu lệnh trên có vấn đề gì cần lưu ý, có thể gây bất cập gì cho việc sử dụng CSDL của user mybear về sau?