# Bài thực hành số 6

# ORACLE LABEL SECURITY (1)

## ❖ *Tóm tắt nội dung:*

- Mô hình DAC và MAC
- DAC và MAC trong Oracle
- Giới thiệu Oracle Label Security
- Hướng dẫn cài đặt Oracle Label Security
- Chính sách trong Oracle Label Security
- Các thành phần của nhãn trong Oracle Label Security
- Nhãn dữ liệu (data label)

## I. Giới thiệu

### A. Lý thuyết

#### 1. Mô hình DAC và MAC

- Có 2 mô hình tiêu biểu dùng để quản lý việc truy xuất dữ liệu một cách đúng đắn và bảo đảm an toàn cho dữ liệu là DAC (Discretionary Access Control) và MAC (Mandatory Access Control).
- DAC: quản lý việc truy xuất dữ liệu bằng cách quản lý việc cấp phát các quyền truy xuất cho những người dùng thích hợp tùy theo yêu cầu của các chính sách bảo mật.
- MAC: quản lý việc truy xuất dựa trên mức độ nhạy cảm của dữ liệu và mức độ tin cậy của người dùng truy xuất CSDL. Bằng cách phân lớp và gán nhãn cho dữ liệu và người dùng, đồng thời áp dụng quy tắc "*no read up - no write down*", mô hình MAC giúp ta tránh được việc rò rỉ dữ liệu có mức độ nhạy cảm cao ra cho những người dùng có độ tin cậy thấp.

#### 2. MAC và DAC trong Oracle

- DAC:

  Trong Oracle Database, các nhà quản trị có thể áp dụng mô hình DAC thông qua việc quản lý các truy xuất theo quyền đối tượng và quyền hệ thống (bài Lab 2 –

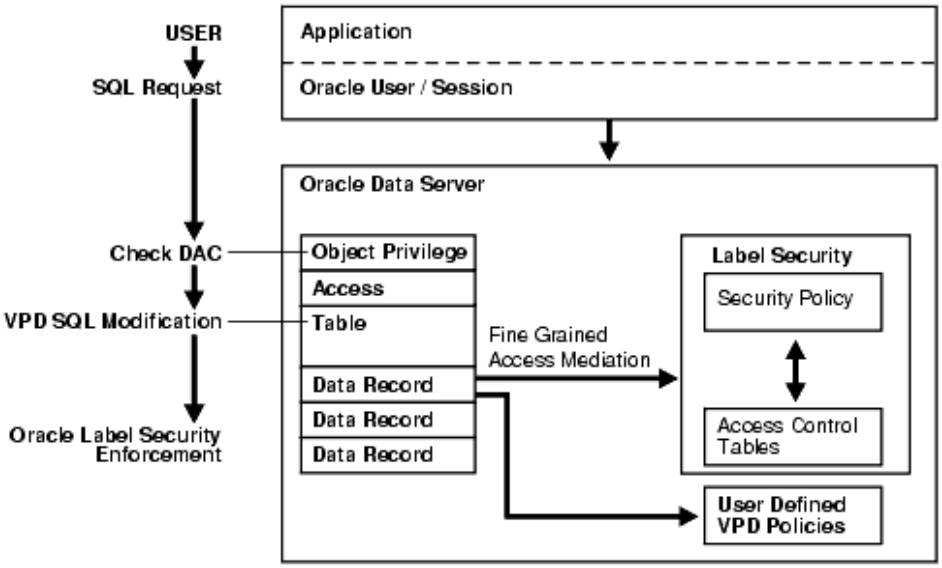
*Quyền và Role*).

- MAC:

  Oracle hiện thực mô hình MAC trên lý thuyết thành sản phẩm Oracle Label Security (OLS). Tuy nhiên, do mô hình MAC lý thuyết tuân theo nguyên tắc "*no read up - no write down*" nên chỉ bảo đảm tính bí mật mà không có tính toàn vẹn. Để cung cấp một mô hình bảo vệ tốt hơn cho CSDL của khách hàng, OLS của Oracle đã cải tiến mô hình MAC lý thuyết bằng cách thay đổi nguyên tắc trên thành "*no read up - no write up - limited write down*". Nhờ vậy, tính bảo mật và tính toàn vẹn của dữ liệu được bảo đảm. Mặt khác, khác với mô hình lý thuyết, OLS không bắt buộc áp dụng MAC cho toàn bộ CSDL. Người quản trị có thể chỉ định ra những table hoặc schema nào sẽ được áp dụng OLS.

- Mối tương quan giữa DAC và MAC:

  Khi người dùng nhập vào 1 câu truy vấn SQL, đầu tiên Oracle sẽ kiểm tra DAC để bảo đảm rằng user đó có quyền truy vấn trên bảng được nhắc đến trong câu truy vấn. Kế tiếp Oracle sẽ kiểm tra xem có chính sách VPD (Virtual Private Database) nào được áp dụng cho bảng đó không. Nếu có, chuỗi điều kiện của chính sách VPD sẽ được nối thêm vào câu truy vấn gốc, giúp lọc ra được một tập các hàng dữ liệu thỏa điều kiện của VPD. Cuối cùng, Oracle sẽ kiểm tra các nhãn OLS trên mỗi hàng dữ liệu có trong tập trên để xác định những hàng nào mà người dùng có thể truy xuất (xem hình minh họa bên dưới).




***Kiến trúc của Oracle Label Security***

## 3. Giới thiệu Oracle Label Security

- Oracle Label Security (OLS) là một sản phẩm được hiện thực dựa trên nền tảng công nghệ Virtual Private Database (VPD), cho phép các nhà quản trị điều khiển truy xuất dữ liệu ở mức hàng (row-level) một cách tiện lợi và dễ dàng hơn. Nó điều khiển việc truy xuất nội dung của các dòng dữ liệu bằng cách so sánh nhãn của hàng dữ liệu với nhãn và quyền của user. Các nhà quản trị có thể dễ dàng tạo thêm các chính sách kiểm soát việc truy xuất các hàng dữ liệu cho các CSDL bằng giao diện đồ họa thân thiện người dùng có tên gọi là Oracle Policy Manager hoặc bằng các packages được xây dựng sẵn.
- Có 6 package được hiện thực sẵn cho OLS:
  - ✓ SA_SYSDBA: tạo, thay đổi, xóa các chính sách.
  - ✓ SA_COMPONENTS: định nghĩa và quản lý các thành phần của nhãn.
  - ✓ SA_LABEL_ADMIN: thực hiện các thao tác quản trị chính sách, nhãn.
  - ✓ SA_POLICY_ADMIN: áp dụng chính sách cho bảng và schema.
  - ✓ SA_USER_ADMIN: quản lý việc cấp phát quyền truy xuất và quy định mức độ tin cậy cho các user liên quan.
  - ✓ SA_AUDIT_ADMIN: thiết lập các tùy chọn cho các tác vụ quản trị việc audit.

  *(Trong chương trình này chúng ta chỉ tìm hiểu cách làm việc với OLS thông qua 5 package đầu trong 6 package liệt kê ở trên).*
- Trong OLS, ta dùng các chính sách (policy) để quản lý truy xuất. Đối với mỗi chính sách, ta cần định ra một tập nhãn để phân lớp dữ liệu từ cao xuống thấp dựa theo mức độ nhạy cảm của dữ liệu (ngoài ra các nhãn còn có những yếu tố khác mà ta sẽ bàn đến khi đi vào chi tiết). Các nhãn đó được gọi là các *nhãn dữ liệu* - "*data label*". Sau đó ta áp dụng các chính sách lên các bảng hoặc schema mà mình mong muốn bảo vệ. Mỗi khi một người dùng muốn truy xuất một hàng dữ liệu nào đó, hệ thống sẽ so sánh nhãn của người dùng (*user label*) tại thời điểm đó với nhãn dữ liệu để quyết định có cho phép việc truy xuất hay không.

## 4. Năm bước hiện thực OLS

- Quy trình cơ bản để hiện thực một chính sách OLS gồm 5 bước như sau:
  - ✓ B1: Tạo chính sách OLS.
  - ✓ B2: Định nghĩa các thành phần mà một nhãn thuộc chính sách trên có thể có.

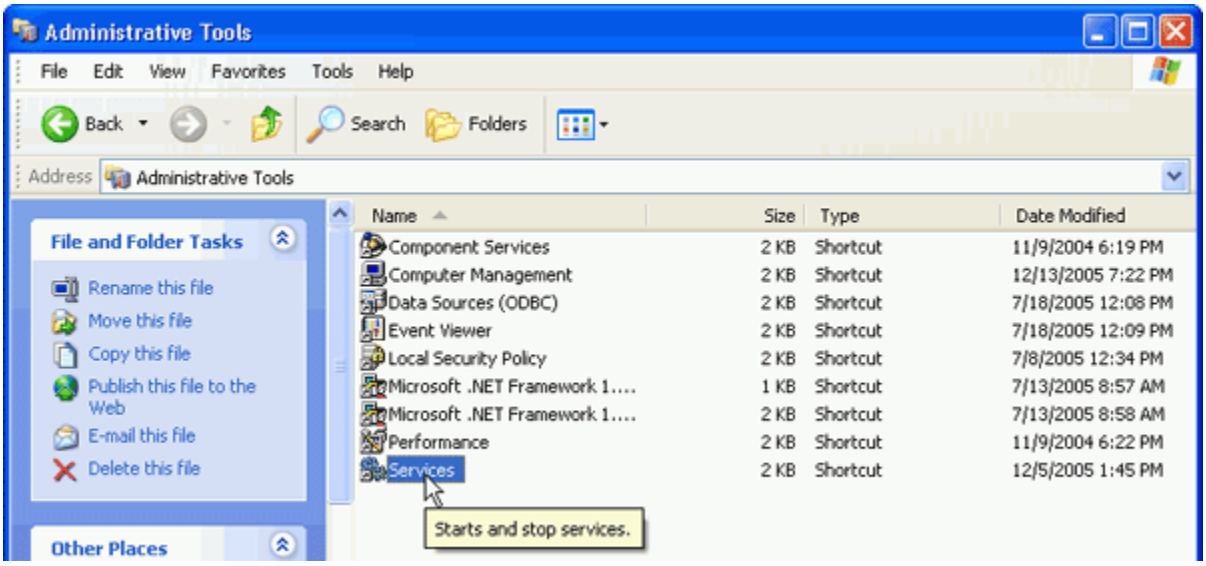
- ✓ B3: Tạo các nhãn dữ liệu thật sự mà bạn muốn dùng.
- ✓ B4: Gán chính sách trên cho các bảng hoặc schema mà bạn muốn bảo vệ.
- ✓ B5: Gán các giới hạn quyền, các nhãn người dùng hoặc các quyền truy xuất đặc biệt cho những người dùng liên quan.

- Trong chương trình của chúng ta, các khái niệm và đối tượng OLS sẽ lần lượt được giới thiệu theo thứ tự của các bước trong quy trình hiện thực cơ bản một chính sách OLS để giúp các bạn dễ theo dõi và thực hành.

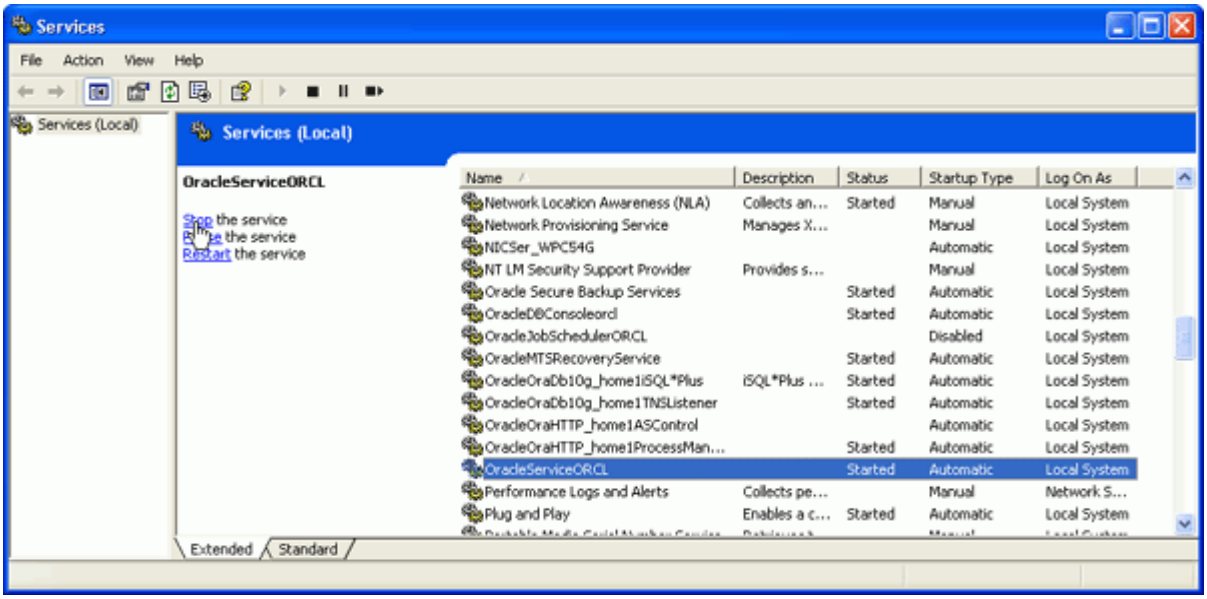
## B. Thực hành

### 1. Cài đặt OLS

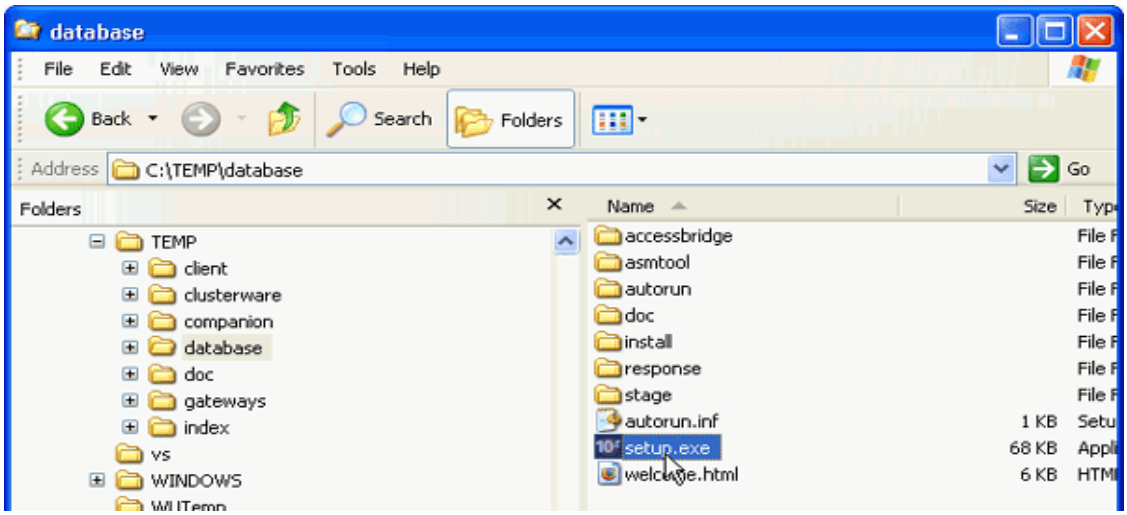
- Cài đặt mặc định của Oracle không bao gồm tính năng OLS. Do vậy phần này sẽ hướng dẫn các bạn cài đặt thêm tính năng OLS cho một cơ sở dữ liệu có sẵn. Bạn phải có quyền admin để có thể thực hiện việc cài đặt này.
- Trong ví dụ minh họa bên dưới, tên (*System Identifier Database - SID*) của cơ sở dữ liệu đang tồn tại có tên là **ORCL**.
- Các bước cài đặt OLS:
  a. Trước khi cài đặt, cần đảm bảo là dịch vụ **OracleService<SID>** đã được tắt. Trong ví dụ minh họa ở đây, dịch vụ có tên là *OracleServiceORCL*. Để tắt dịch vụ này, chọn **Start → Settings → Control Panel → Administrative Tools → Services.**



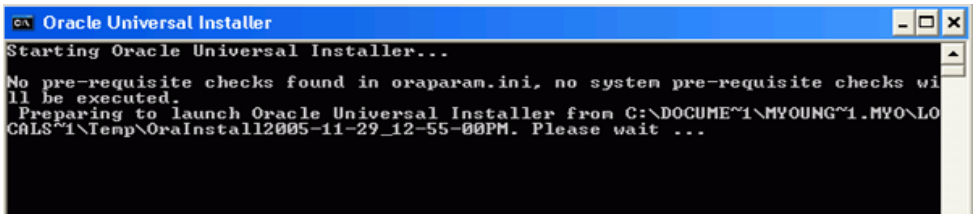
b. Chọn dịch vụ *OracleServiceORCL* và nhấn chuột phải, chọn **Stop** để tắt dịch vụ này.



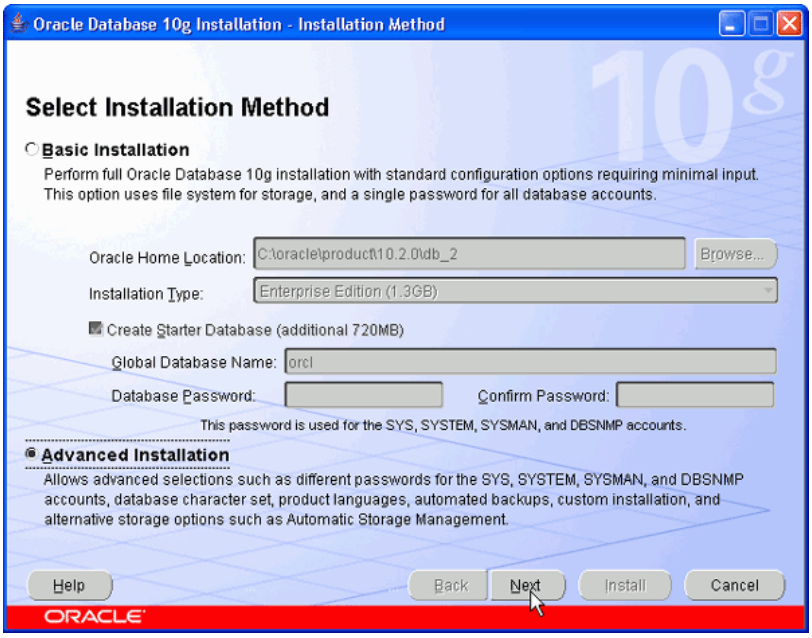

c. Sau khi đã tắt dịch vụ *OracleServiceORCL*, mở thư mục chứa chương trình cài đặt *Oracle Database Enterprise Edition*, nhấp đôi lên file **setup.exe**.



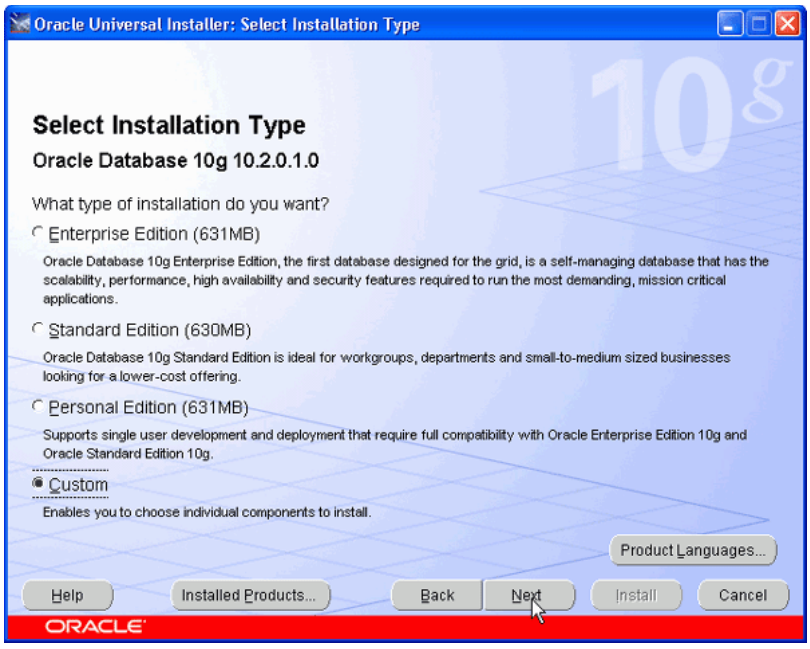

d. *Oracle Universal Installer* được khởi động:



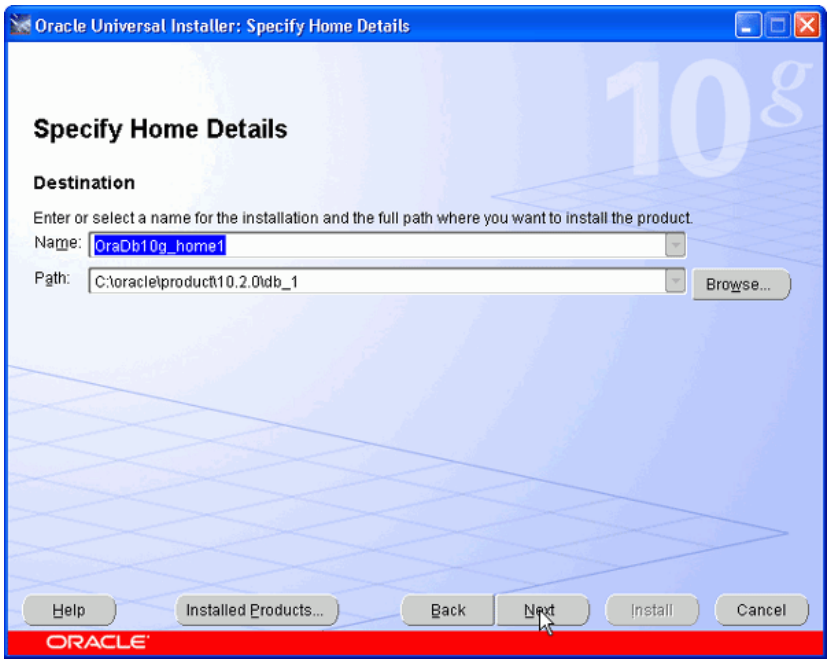
e. Click chọn **Advanced Installation** trong cửa sổ **Installation Method** rồi nhấn **Next**.



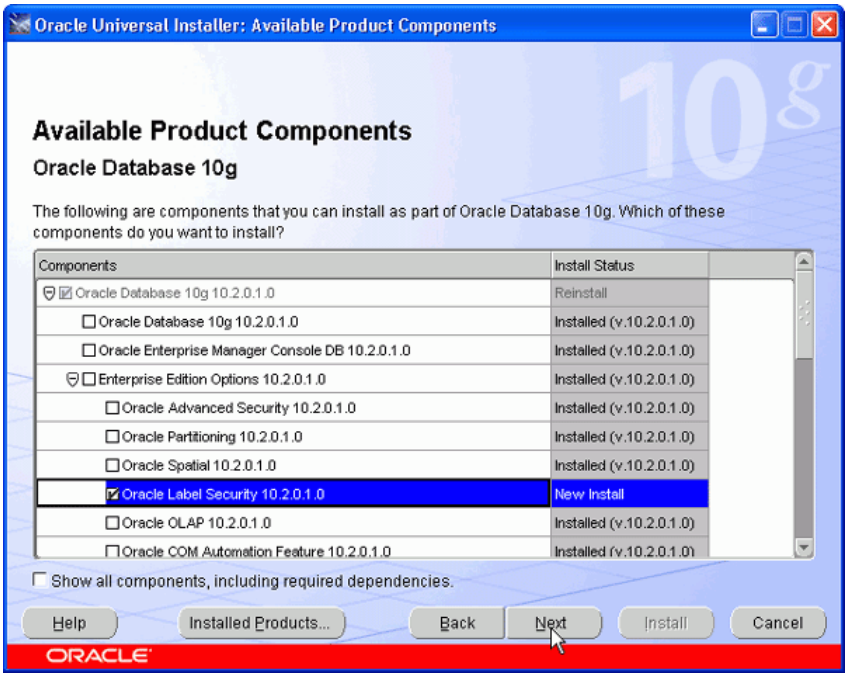

f. Chọn **Custom** trong cửa sổ **Select Installation Type** và nhấn **Next**.




g. Ở cửa sổ **Specify File Locations**, nhập **Global Database Name** vào **Home**và đường dẫn của **Oracle Home** vào **Path** rồi nhấn **Next**. Thông thường, nếu khi cài đặt Oracle, bạn không thay đổi giá trị mặc định của vị trí cài đặt thì giá trị của đường dẫn là **C:\oracle\product\10.2.0\db_1.**



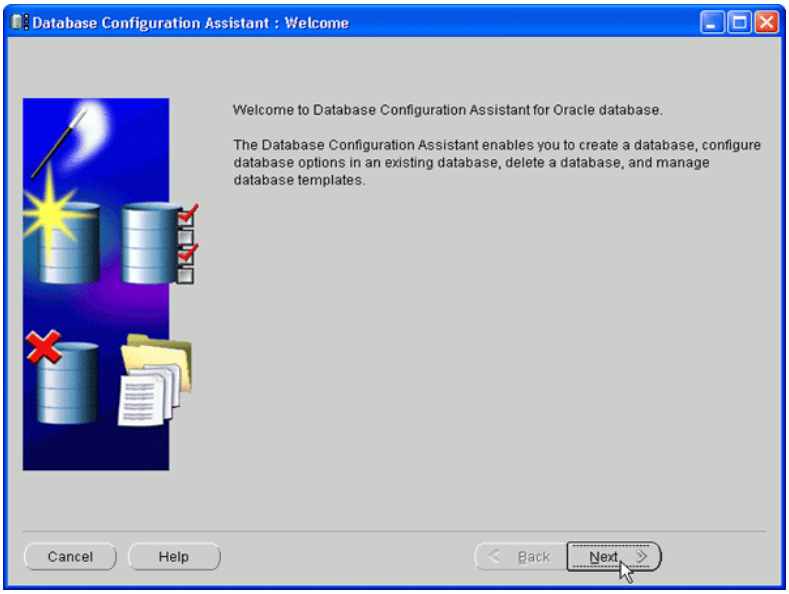

h. Trong cửa sổ **Available Product Components**đánh dấu vào ô **Oracle Label Security.**



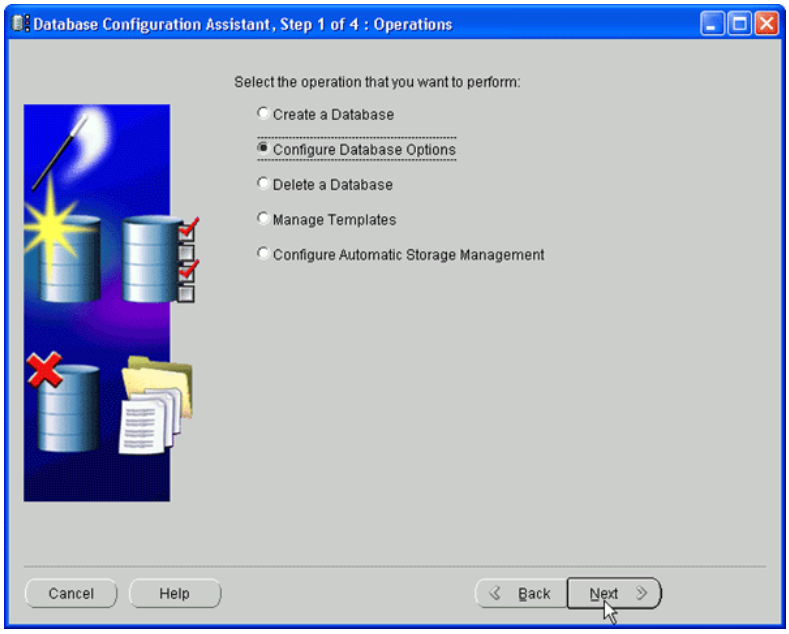

i. Các bước kế tiếp làm theo hướng dẫn trong cửa sổ hiển thị (cách làm giống như quá trình cài đặt Oracle Database).

## 2. Cấu hình để sử dụng OLS

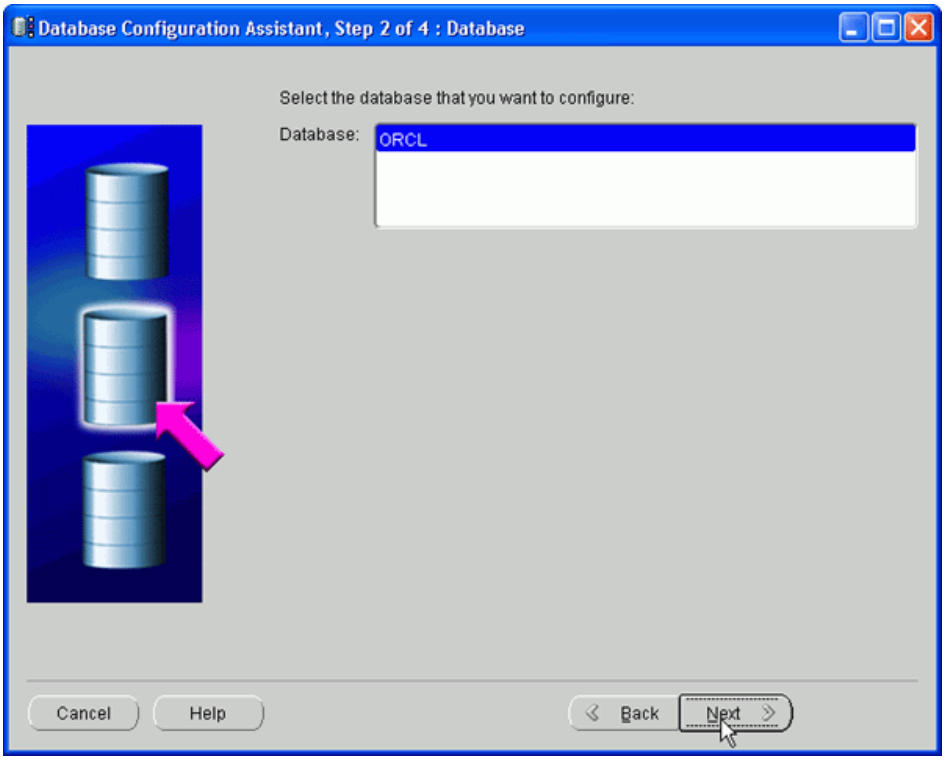
a. Chọn Start → **Programs** → **Oracle-OraDb10g_home1** → **Configuration and Migration Tools** → **Database Configuration Assistant**. Cửa sổ chương trình sẽ hiện ra như hình bên dưới. Click **Next** để tiếp tục.



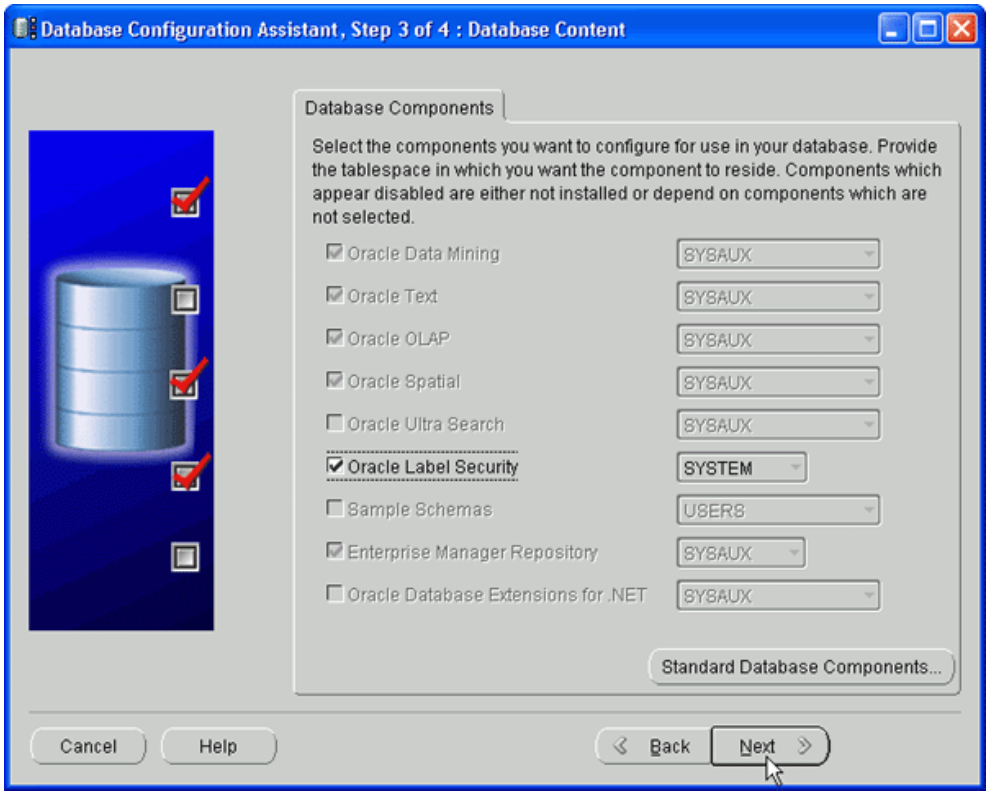

b. Trong cửa sổ **Step 1**, chọn **Configure Database Options** và click **Next**.



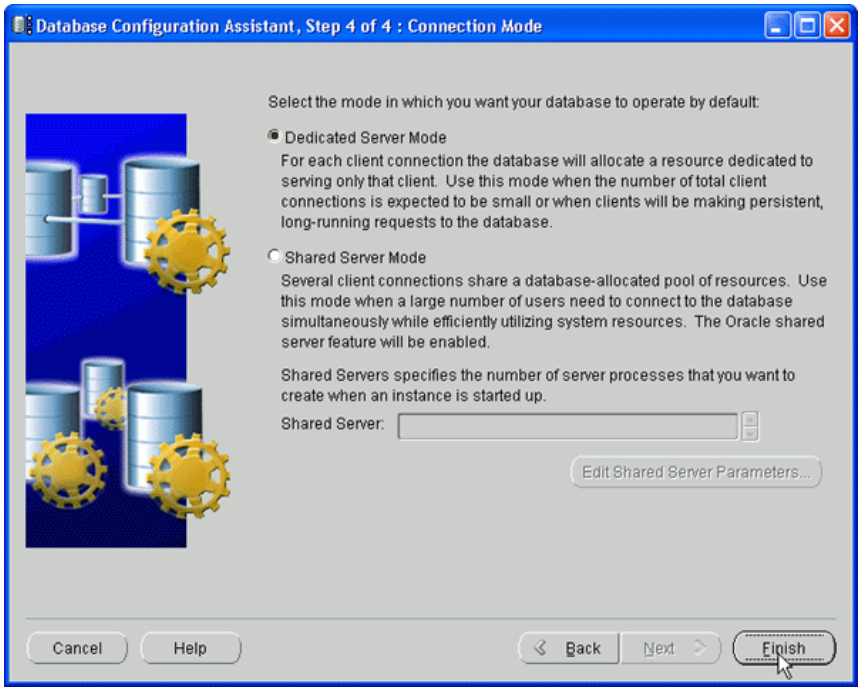
c. Trong **Step 2**, chọn cơ sở dữ liệu mà bạn muốn cài đặt thêm OLS và click **Next**.




d. Trong **Step 3**, chọn **Oracle Label Security** và click **Next**.

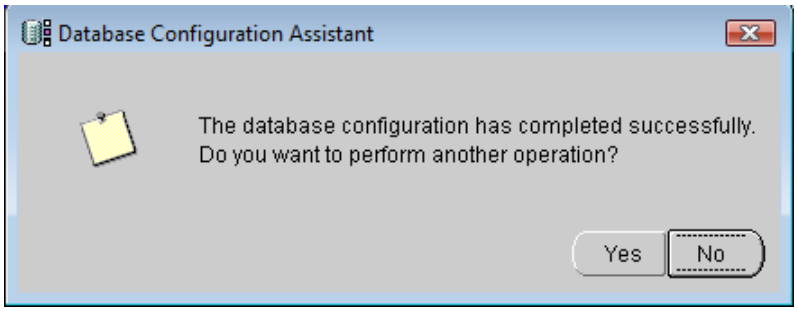


e. Trong **Step 4**, để mặc định và chọn **Finish**.




f. Lần lượt 2 ô cửa sổ **Restart Database** và **Confirmation** xuất hiện, nhấn **OK** trong mỗi cửa sổ đó.

g. Sau khi chương trình cài đặt thành công, click **No** trong cửa sổ **Do you want to perform another operation?** để thoát ra khỏi chương trình.




### 3. Kích hoạt tài khoản LBACSYS

Để sử dụng OLS bảo vệ cho cơ sở dữ liệu, ta cần tạo ra các chính sách (policy) quy định các mức độ nhạy cảm của dữ liệu và mức độ tin cậy của những người dùng liên quan. Muốn tạo ra các chính sách, ta phải đăng nhập bằng tài khoản **LBACSYS**. Tuy nhiên, mặc định tài khoản này bị khóa. Dùng lệnh sau để kích hoạt tài khoản này.

```
ALTER USER lbacsys IDENTIFIED BY lbacsys ACCOUNT UNLOCK[1];
```

[1]Sinh viên log on vào tài khoản có đầy đủ các quyền, ví dụ sMSSV.

## 4. Chuẩn bị dữ liệu

- Để minh họa cho phần thực hành của các bài lab về OLS, chúng ta cần tạo trước một số tài khoản và role.
- Thông thường, ngữ cảnh mà trong đó dữ liệu cần được bảo vệ sẽ gồm các thành phần:
  - ✓ Dữ liệu cần được bảo vệ.
  - ✓ Chủ sở hữu dữ liệu cần được bảo vệ (user tạo ra và chứa dữ liệu cần được bảo vệ trong schema của mình).
  - ✓ User chịu trách nhiệm quản lý ai được phép truy xuất những đối tượng dữ liệu cần được bảo vệ.
  - ✓ User chịu trách nhiệm quản lý chính sách bảo mật và những quy định của chính sách đó.
- Trong phần thực hành, chúng ta sẽ sử dụng các đối tượng dữ liệu thuộc schema **HR** (có sẵn khi cài đặt Oracle Database, chứa dữ liệu quản lý nhân sự của một công ty-Human Resources) như là những đối tượng dữ liệu cần được bảo vệ. Nói cách khác, HR là user tạo ra, quản lý và sở hữu (về mặt nội dung) dữ liệu cần được bảo vệ. Đổi mật khẩu cho schema **HR**:

```
ALTER USER hr IDENTIFIED BY hr ACCOUNT UNLOCK;
```

- Tiếp theo, ta tạo mới user **HR_SEC** chịu trách nhiệm quản lý những user nào được phép truy xuất dữ liệu trong schema **HR**:

```
GRANT connect, create user, drop user,
create role, drop any role
TO hr_sec IDENTIFIED BY hrsec;
```

- Ta tạo user **SEC_ADMIN** chịu trách nhiệm quản lý chính sách bảo mật dành cho dữ liệu trong **HR**.

```
GRANT connect TO sec_admin IDENTIFIED BY secadmin;
```

- Ta cũng cần tạo ra các user là nhân viên trong công ty và role cho các nhân viên:

```
CREATE ROLE emp_role;
GRANT connect TO emp_role;
```

```
-- Steven King (Tổng Giám đốc)
CREATE USER sking IDENTIFIED BY sking;
GRANT emp_role TO sking;

-- Neena Kochhar (Giám đốc điều hành)
CREATE USER nkochhar IDENTIFIED BY nkochhar;
GRANT emp_role TO nkochhar;

-- Karen Partner (Trưởng phòng Sales)
CREATE USER kpartner IDENTIFIED BY kpartner;
GRANT emp_role TO kpartner;

-- Louise Doran (Nhân viên thuộc phòng Sales)
CREATE USER ldoran IDENTIFIED BY ldoran;
GRANT emp_role TO ldoran;
```

- Vì HR là người quản lý về mặt nội dung đối với dữ liệu trong của phòng nhân sự nên HR là người cấp quyền xem dữ liệu cho các nhân viên:

```
CONN hr/hr;
GRANT select ON hr.locations TO emp_role;
```

# II. Chính sách trong Oracle Label Security

## A. Lý thuyết

- Chính sách (*policy*) có thể được xem như là danh sách tập hợp thông tin về các nhãn dữ liệu và nhãn người dùng của chính sách đó, các quy định về quyền truy xuất, các điều kiện áp dụng chính sách. Do vậy, để hiện thực OLS, đầu tiên cần phải tạo ra chính sách.
- Oracle cho phép tạo nhiều chính sách khác nhau. Một chính sách có thể được dùng để bảo vệ nhiều bảng và schema. Một bảng hoặc schema có thể được bảo vệ bởi nhiều chính sách khác nhau. Khi đó, nếu một người dùng muốn truy xuất dữ liệu trong bảng thì phải thỏa mãn quy định của tất cả các chính sách đang được áp dụng cho bảng đó.
- Với mỗi chính sách được áp dụng trên một bảng, một cột dùng để lưu thông tin nhãn dữ liệu (data label) của chính sách đó cho mỗi hàng trong bảng sẽ được thêm vào bảng. Mọi bảng có áp dụng chung 1 chính sách sẽ có cột thông tin với tên cột giống nhau. Vì

vậy, mỗi khi tạo một chính sách, ta phải quy định một tên cột cho chính sách đó và tên này phải là duy nhất trong toàn bộ các chính sách OLS của CSDL.

*Ví dụ*: chính sách A quy định tên cột chứa thông tin là B. Như vậy với mỗi bảng có áp dụng chính sách A, Oracle sẽ thêm vào đó 1 cột có tên là B dùng để lưu nhãn dữ liệu tương ứng với chính sách A cho từng dòng dữ liệu của bảng đó.

- Các cột chứa thông tin của các chính sách trong mỗi bảng có kiểu NUMBER. Thông tin của nhãn dữ liệu được lưu trong cột này là một con số đại diện cho nhãn gọi là tag (sẽ được giới thiệu kỹ hơn trong phần sau).
- Chúng ta sử dụng package SA_SYSDBA để quản lý chính sách. SA_SYSDBA bao gồm các thủ tục (*procedure*) sau:
  - ✓ SA_SYSDBA.CREATE_POLICY: tạo mới một chính sách.
  - ✓ SA_SYSDBA.ALTER_POLICY: thay đổi những điều kiện áp dụng chính sách.
  - ✓ SA_SYSDBA.DISABLE_POLICY: làm cho những quy định của chính sách tạm thời không có hiệu lực đối với những dữ liệu có áp dụng chính sách đó.
  - ✓ SA_SYSDBA.ENABLE_POLICY: kích hoạt chính sách để những quy định của chính sách trên các đối tượng dữ liệu mà nó bảo vệ có hiệu lực. Mặc định ngay khi được tạo ra, chính sách đã được kích hoạt.
  - ✓ SA_SYSDBA.DROP_POLICY: xóa bỏ chính sách và tất cả các nhãn người dùng, nhãn dữ liệu liên quan ra khỏi cơ sở dữ liệu.

## B. Thực hành

- Ta dùng procedure SA_SYSDBA.CREATE_POLICY để tạo ra chính sách mới (bước 1 trong quy trình hiện thực OLS). Quyền thực thi thủ tục này được cấp mặc định cho LBACSYS. Trong phần thực hành sau ta sẽ tạo ra một chính sách dùng để điều khiển các truy xuất đến bảng LOCATIONS của HR với tên gọi là "ACCESS_LOCATIONS" và có cột chứa nhãn tên là "OLS_COLUMN".

```
CONN lbacsys/lbacsys;
BEGIN
    SA_SYSDBA.CREATE_POLICY (
       policy_name => 'ACCESS_LOCATIONS',
       column_name => 'OLS_COLUMN');
END;
/
```

- Khi một chính sách được tạo ra, Oracle tự động tạo ra 1 role quản trị riêng cho chính sách đó và gán role này cho LBACSYS. Tên của role có dạng "<tên_chính_sách>_DBA". Ví dụ, đối với chính sách vừa tạo ở trên thì role tương ứng sẽ có tên là **ACCESS_LOCATIONS_DBA**. Thông thường LBACSYS chỉ có nhiệm vụ chung tạo ra các chính sách, sẽ có những người khác chịu trách nhiệm quản lý chính sách đó. Cụ thể trong ngữ cảnh thực hành của chúng ta, SEC_ADMIN sẽ là user chịu trách nhiệm quản lý chính sách, duy trì hoạt động của nó và HR_SEC sẽ quyết định quyền truy xuất dữ liệu trong schema HR của các user khác dựa trên mức độ tin cậy họ.

- Để SEC_ADMIN có thể quản lý và duy trì hoạt động của chính sách, ta cần cấp cho user này role quản trị của chính sách và các quyền thực thi trên các package liên quan:

```
CONN lbacsys/lbacsys;
GRANT access_locations_dba TO sec_admin;

-- Package dùng để tạo ra các thành phần của nhãn
GRANT execute ON sa_components TO sec_admin;

-- Package dùng để tạo các nhãn
GRANT execute ON sa_label_admin TO sec_admin;

-- Package dùng để gán chính sách cho các table/schema
GRANT execute ON sa_policy_admin TO sec_admin;
```

- Để HR_SEC có thể quản lý việc truy xuất của các user, ta cũng cần cấp cho user này role quản trị của chính sách và các quyền thực thi trên các package liên quan:

```
CONN lbacsys/lbacsys;
GRANT access_locations_dba TO hr_sec;

-- Package dùng để gán các label cho user
GRANT execute ON sa_user_admin TO hr_sec;
```

- Lưu ý: đối với mỗi user quản lý chính sách, ta cấp cho user đó các quyền thực thi trên các package tương ứng. Tuy nhiên có các quyền trên chưa phải là điều kiện đủ để user

đó có thể quản lý các chính sách. Nếu muốn user đó quản lý chính sách nào, ta cần gán thêm role quản trị của chính sách đó cho user. Như vậy những quyền mà user được cấp sẽ chỉ có tác dụng trên những chính sách mà user được gán role quản trị.

```
-- Tạo 1 policy mới nhưng không gán role
CONN lbacsys/lbacsys;
BEGIN
    sa_sysdba.create_policy
       (policy_name  => 'Different_Policy');
END;
/
/** Thử quản lý policy mới tạo ra. Nhưng sẽ bị thất
bại vì sec_admin không được gán role cần thiết.**/
CONN sec_admin/secadmin;
BEGIN
    sa_components.create_level
       (policy_name  => 'Different_Policy',
       long_name     => 'foo',
       short_name    => 'bar',
       level_num     => 9);
END;
/
BEGIN
*
ERROR at line 1:
ORA-12407: unauthorized operation for policy Different_Policy
```

- Ta dùng SA_SYSDBA.DROP_POLICY để xóa chính sách 'Different_Policy' ở trên:

```
CONN lbacsys/lbacsys;
BEGIN
    sa_sysdba.drop_policy
       (policy_name  => 'Different_Policy',
       drop_column   => true);
END;
/
```

# III. Các thành phần của nhãn dữ liệu

## A. Lý thuyết

### 1. Nhãn dữ liệu (data label)

- Như đã biết, mô hình MAC bảo vệ dữ liệu bằng cách quy định một hệ thống biểu diễn mức độ quan trọng, bí mật cho các đối tượng dữ liệu theo cấp bậc từ cao xuống thấp. Ví dụ, một công ty có thể phân loại mức độ bí mật thành 4 cấp với mức độ bảo mật giảm dần: TOP SECRET (tối mật), SECRET (bí mật), CONFIDENTIAL (chỉ lưu hành nội bộ), PUBLIC (công khai).
- Trong OLS, Oracle sử dụng các **nhãn dữ liệu** (***data label***) để phân lớp dữ liệu theo mức độ nhạy cảm của nó và một số tiêu chí khác. Nói cách khác, mỗi nhãn dữ liệu sẽ chứa thông tin về mức độ nhạy cảm của dữ liệu và một số tiêu chí cộng thêm mà người dùng phải đáp ứng để có thể truy xuất đến dữ liệu đó.
- Nhãn dữ liệu là 1 thuộc tính đơn gồm 3 loại thành phần: ***level, compartment, group***.
- Nếu một chính sách được áp dụng cho một bảng, thì mỗi hàng trong bảng đó sẽ được gán một *nhãn dữ liệu (data label)* để biểu diễn mức độ bảo mật của hàng dữ liệu đó. Giá trị của nhãn được lưu trong cột chứa thông tin của chính sách (cột được tự động tạo thêm khi chính sách được áp dụng cho bảng).

### 2. Các thành phần của nhãn

#### a. Level

- Mỗi nhãn có đúng 1 ***level*** biểu thị độ nhạy cảm của dữ liệu. OLS cho phép tối đa 10,000 level trong 1 chính sách.
- Đối với mỗi level, ta cần định nghĩa 1 dạng số và 2 dạng chuỗi cho nó. VD:

| Dạng số | Dạng chuỗi dài | Dạng chuỗi ngắn |
|---|---|---|
| 40 | *HIGHLY_SENSITIVE* | HS |
| 30 | *SENSITIVE* | S |
| 20 | *CONFIDENTIAL* | C |
| 10 | *PUBLIC* | P |

- *Dạng số (numeric form)*: dạng số của level có thể có giá trị trong khoảng 0-9999. Level có giá trị càng cao thì độ nhạy cảm càng tăng. Trong VD trên, *Highly_sensitive* có độ nhạy cảm cao nhất. User nên tránh sử dụng một chuỗi

tuần tự liên tiếp các giá trị để biểu diễn cho 1 bộ level của nhãn để tránh tình trạng khi có level mới thêm vào thì phải định nghĩa lại toàn bộ các level.

- *Dạng chuỗi dài (long form)*: chứa tối đa 80 ký tự, cho biết tên đầy đủ của level.
- *Dạng chuỗi ngắn (short form)*: chứa tối đa 30 ký tự, là dạng rút gọn của tên level. Mỗi khi cần tham khảo đến level ta sử dụng tên rút gọn này.

**b. Compartment**

- Mỗi nhãn có thể có 1 hoặc nhiều hoặc không có ***compartment*** nào. OLS cho phép tối đa 10,000 compartment trong 1 chính sách.
- Compartment giúp cho việc phân loại dữ liệu theo lĩnh vực, chuyên ngành, dự án,…chứ không thể hiện sự phân cấp mức độ nhạy cảm của dữ liệu đó. Nghĩa là nếu ta có 2 dữ liệu thuộc 2 compartment C1 và C2, thì có nghĩa là 2 dữ liệu đó thuộc 2 lĩnh vực khác nhau là C1 và C2 chứ không có nghĩa dữ liệu thuộc C1 nhạy cảm hơn dữ liệu thuộc C2 (hay ngược lại).
- Đối với mỗi compartment, ta cần định nghĩa 1 dạng số và 2 dạng chuỗi. VD:

| Dạng số | Dạng chuỗi dài | Dạng chuỗi ngắn |
|---|---|---|
| 85 | FINANCIAL | FINCL |
| 65 | CHEMICAL | CHEM |
| 45 | OPERATIONAL | OP |

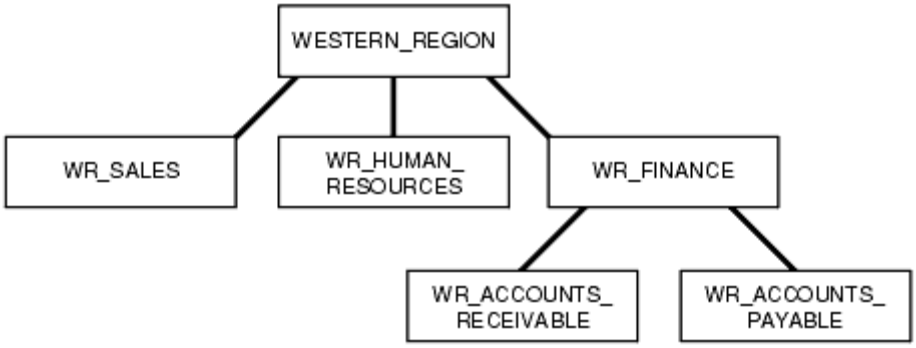
- *Dạng số (numeric form)*: dạng số của compartment có thể có giá trị trong khoảng 0-9999. Nó không liên quan gì đến con số của level. Giá trị của nó dùng để quy định thứ tự hiển thị của các compartment trong một label. Đối với VD trên, ta sẽ có các nhãn dạng như sau:

  `S:OP,CHEM,FINCL` (do OP có giá trị nhỏ nhất nên nó được hiển thị trước nhất)
- *Dạng chuỗi dài (long form)*: tối đa 80 ký tự, là tên đầy đủ của compartment.
- *Dạng chuỗi ngắn (short form)*: tối đa 30 ký tự, là dạng rút gọn của tên compartment. Khi cần tham khảo đến compartment ta sử dụng tên rút gọn này.

**c. Group**

- Mỗi nhãn có thể có 1 hoặc nhiều hoặc không có ***group*** nào. OLS cho phép tối đa 10,000 group trong 1 chính sách.

- Group giúp xác định những tổ chức, cơ quan, bộ phận nào sở hữu hoặc quản lý dữ liệu (thông thường nó thể hiện cơ cấu của công ty). Do vậy group có cấu trúc cây phân cấp. Một group có thể thuộc một group cha và có nhiều group con. Dữ liệu thuộc một group con thì được xem như cũng thuộc group cha. VD:




| Dạng số | Dạng chuỗi dài | Dạng chuỗi ngắn | Group cha |
|---|---|---|---|
| 1000 | WESTERN_REGION | WR | |
| 1100 | WR_SALES | WR_SAL | WR |
| 1200 | WR_HUMAN_RESOURCES | WR_HR | WR |
| 1300 | WR_FINANCE | WR_FIN | WR |
| 1310 | WR_ACCOUNTS_PAYABLE | WR_AP | WR_FIN |
| 1320 | WR_ACCOUNTS_RECEIVABLE | WR_AR | WR_FIN |

- *Dạng số (numeric form)*: dạng số của group có thể có giá trị trong khoảng 0-9999. Nó không liên quan gì đến con số của level. Giá trị của nó dùng để quy định thứ tự hiển thị của các group trong một label. Đối với VD trên, ta sẽ có các nhãn dạng như sau:

  `S:CHEM:WR,WR_HR` (WR có giá trị nhỏ hơn WR_HR nên được hiển thị trước)
- *Dạng chuỗi dài (long form)*: chứa tối đa 80 ký tự, cho biết tên của group.
- *Dạng chuỗi ngắn (short form)*: chứa tối đa 30 ký tự, là dạng rút gọn của tên group. Mỗi khi cần tham khảo đến group ta sử dụng tên rút gọn này.

## B. Thực hành

Ở phần này ta sẽ tạo các thành phần của nhãn (ứng với bước 2 trong quy trình hiện thực OLS) cho chính sách ACCESS_LOCATIONS mà ta đã tạo trong phần II.

## 1. Tạo level

- Ta quy định chính sách ACCESS_LOCATIONS của ta có 3 level (theo thứ tự mức độ bảo mật giảm dần): SENSITIVE, CONFIDENTIAL, PUBLIC. Ta dùng thủ tục SA_COMPONENTS.CREATE_LEVEL để tạo ra các level:

```
CONN sec_admin/secadmin;
BEGIN
    sa_components.create_level
       (policy_name    => 'ACCESS_LOCATIONS',
       long_name       => 'PUBLIC',
       short_name      => 'PUB',
       level_num       => 1000);
END;
/
EXECUTE sa_components.create_level
('ACCESS_LOCATIONS',2000,'CONF','CONFIDENTIAL');
EXECUTE sa_components.create_level
('ACCESS_LOCATIONS',3000,'SENS','SENSITIVE');
```

Đoạn code trên cho ta thấy 2 cách khác nhau để thực thi thủ tục. Người đọc cũng cần chú ý cách chọn số cho các level.

- Để thay đổi tên đầy đủ và tên rút gọn của level, ta dùng thủ tục SA_COMPONENTS.ALTER_LEVEL. Nếu level đang được dùng bởi ít nhất một nhãn dữ liệu nào đó, ta có thể thay đổi tên đầy đủ của nó nhưng không thể thay đổi tên rút gọn. Trong mọi trường hợp, ta đều không thể thay đổi số đại diện của level.

```
CONN sec_admin/secadmin;
EXECUTE sa_components.create_level
('ACCESS_LOCATIONS',4000,'HS','HIGHLY SECRET');
BEGIN
    sa_components.alter_level
       (policy_name    => 'ACCESS_LOCATIONS',
       level_num       => 4000,
       new_short_name  => 'TS',
```

```
        new_long_name    => 'TOP SECRET');
END;
/
BEGIN
    sa_components.alter_level
       (policy_name     => 'ACCESS_LOCATIONS',
       short_name       => 'TS',
       new_long_name    => 'TOP SENSITIVE');
END;
/
```

- Để xóa một level ta dùng thủ tục SA_COMPONENTS.DROP_LEVEL. Nếu level đang được sử dụng bởi bất kỳ nhãn dữ liệu nào, ta không thể xóa nó.

```
CONN sec_admin/secadmin;
BEGIN
    sa_components.drop_level
       (policy_name     => 'ACCESS_LOCATIONS',
       short_name       => 'TS');
END;
/
```

**2. Tạo compartment**

- Giả sử chúng ta có 3 compartment là: Finance, Sales & Marketing, Human Resources. Để tạo compartment chúng ta dùng procedure SA_COMPONENTS.CREATE_COMPARTMENT:

```
CONN sec_admin/secadmin;
BEGIN
    sa_components.create_compartment
       (policy_name    => 'ACCESS_LOCATIONS',
       long_name        => 'SALES_MARKETING',
       short_name       => 'SM',
       comp_num         => 2000);
END;
/
```

```
EXECUTE sa_components.create_compartment
('ACCESS_LOCATIONS',3000,'FIN','FINANCE');
EXECUTE sa_components.create_compartment
('ACCESS_LOCATIONS',1000,'HR','HUMAN RESOURCES');
```

- Để thay đổi tên đầy đủ và tên rút gọn của compartment, ta dùng thủ tục SA_COMPONENTS.ALTER_COMPARTMENT. Các điều kiện của việc thay đổi thuộc tính của compartment giống như đối với level.

```
CONN sec_admin/secadmin;
EXECUTE sa_components.create_compartment('ACCESS_LOCATIONS',
4000, 'PR', 'PUBLIC RELATIONS');
BEGIN
    sa_components.alter_compartment
       (policy_name     => 'ACCESS_LOCATIONS',
       comp_num         => 4000,
       new_short_name   => 'PU',
       new_long_name    => 'PURCHASING');
END;
/

BEGIN
    sa_components.alter_compartment
       (policy_name     => 'ACCESS_LOCATIONS',
       short_name       => 'PU',
       new_long_name    => 'PURCHASE');
END;
/
```

- Để xóa một compartment ta dùng thủ tục SA_COMPONENTS.DROP_COMPARTMENT. Nếu compartment đang được sử dụng bởi bất kỳ nhãn dữ liệu nào, ta không thể xóa nó.

```
CONN sec_admin/secadmin;
BEGIN
    sa_components.drop_compartment
```

```
        (policy_name     => 'ACCESS_LOCATIONS',
        short_name       => 'PU');
END;
/
```

### 3. Tạo group

- Chính sách của chúng ta sẽ có 1 group cấp cao nhất là Corporate (CORP) tương ứng với cấp độ toàn công ty. Công ty này có các chi nhánh hoạt động ở 3 nước: Mỹ (American United States), Anh (United Kingdom) và Canada. Ứng với mỗi khu vực đó ta tạo 1 group con cho group CORP.
- Ta dùng procedure SA_COMPONENTS.CREATE_GROUP để tạo ra các group:

```
CONN sec_admin/secadmin;
BEGIN
    sa_components.create_group
       (policy_name     => 'ACCESS_LOCATIONS',
       long_name        => 'CORPORATE',
       short_name       => 'CORP',
       group_num        => 10,
       parent_name      => NULL);
END;
/

EXECUTE sa_components.create_group
('ACCESS_LOCATIONS',30,'US','UNITED STATES','CORP');
EXECUTE sa_components.create_group
('ACCESS_LOCATIONS',50,'UK','UNITED KINGDOM','CORP');
EXECUTE sa_components.create_group
('ACCESS_LOCATIONS',70,'CA','CANADA','CORP');
```

Để thay đổi tên đầy đủ và tên rút gọn của group, ta dùng thủ tục SA_COMPONENTS.ALTER_GROUP. Các điều kiện của việc thay đổi thuộc tính của group giống như đối với level.

```
CONN sec_admin/secadmin;
EXECUTE sa_components.create_group
('ACCESS_LOCATIONS',90,'FR','FRANCE','CORP');
```

```
BEGIN
    sa_components.alter_group
       (policy_name     => 'ACCESS_LOCATIONS',
       group_num        => 90,
       new_short_name   => 'RFR',
       new_long_name    => 'REPUBLIC FRANCE');
END;
/
BEGIN
    sa_components.alter_group
       (policy_name     => 'ACCESS_LOCATIONS',
       short_name       => 'RFR',
       new_long_name    => 'PURCHASE');
END;
/
```

- Để xóa một group ta dùng thủ tục SA_COMPONENTS.DROP_GROUP. Nếu group đang được sử dụng bởi bất kỳ nhãn dữ liệu nào, ta không thể xóa nó.

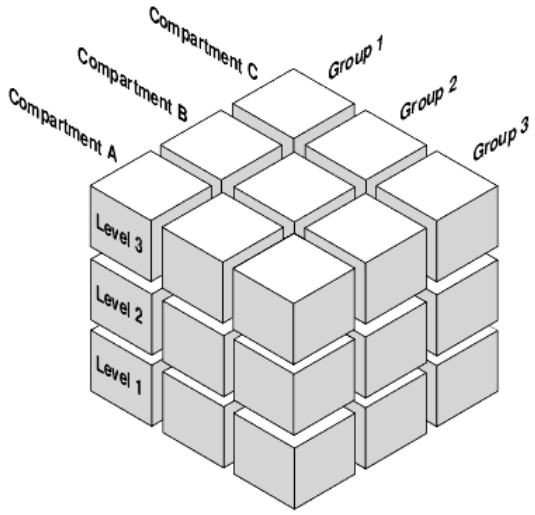
```
CONN sec_admin/secadmin;
BEGIN
    sa_components.drop_group
       (policy_name     => 'ACCESS_LOCATIONS',
       short_name       => 'RFR');
END;
/
```

# IV. Chi tiết về nhãn dữ liệu

## A. Lý thuyết

### 1. Cú pháp của nhãn dữ liệu

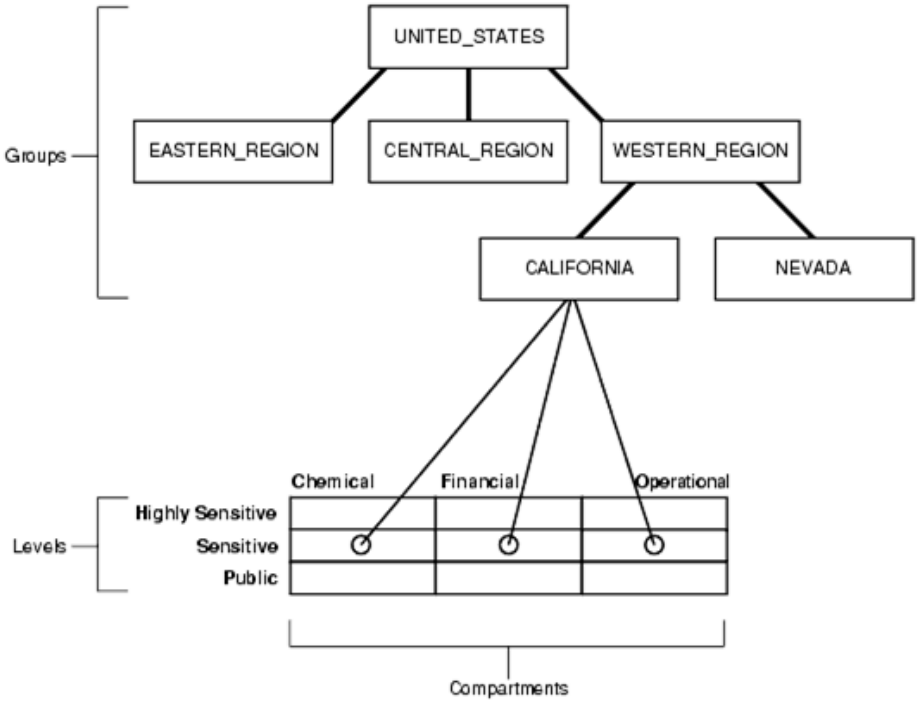
- Hình sau minh họa quan hệ của các thành phần trong 1 nhãn:




- Một nhãn dữ liệu bất kỳ có cú pháp sau:

  ***LEVEL*:*COMPARTMENT*$_1$,...,*COMPARTMENT*$_n$:*GROUP*$_1$,...,*GROUP*$_n$**

- Chuỗi ký tự mô tả một nhãn có thể chứa tối đa 4000 ký tự, bao gồm các ký tự số, ký tự chữ, khoảng trắng, dấu gạch dưới (_).
- Các nhãn không phân biệt chữ hoa, chữ thường. Tuy nhiên chuỗi được lưu trữ trong data dictionary sẽ hiển thị dưới dạng chữ hoa.
- Dấu hai chấm (":") dùng để phân cách giữa các loại thành phần. VD:
  - ✓ `SENSITIVE`
  - ✓ `HIGHLY_SENSITIVE:FINANCIAL`
  - ✓ `SENSITIVE::WESTERN_REGION`
  - ✓ `CONFIDENTIAL:FINANCIAL:VP_GRP`
  - ✓ `SENSITIVE:FINANCIAL,CHEMICAL:EASTERN_REGION,WESTERN_REGION`
- Hình sau đây là một ví dụ minh họa cho việc kết hợp *level*, *compartment*, *group* để phân loại dữ liệu của một tổ chức:




- Không phải mọi tổ hợp của các thành phần đều hình thành nên một nhãn hợp lệ. Ta chỉ định nghĩa những nhãn nào có tổ hợp thành phần mà ta có nhu cầu sử dụng thật sự trong thực tế.
- Sử dụng package SA_COMPONENTS để định nghĩa các thành phần của nhãn.
- Sử dụng package SA_LABEL_ADMIN để tạo và quản lý nhãn.

## 2. Label Tag

- Khi một nhãn dữ liệu mới được tạo, Oracle sẽ tự động tạo cho nhãn đó một con số đại diện được gọi là ***label tag***.
- Mỗi *label tag* xác định duy nhất 1 nhãn trong toàn bộ các nhãn của tất cả các chính sách có trong cơ sở dữ liệu đó. Nói cách khác, trong một cơ sở dữ liệu, không có bất kỳ 2 label tag nào (cùng 1 chính sách hoặc khác chính sách) có giá trị giống nhau.
- Giá trị của *label tag* không có tính chất so sánh như con số đại diện cho level.
- Đây là con số thật sự được lưu vào cột chứa thông tin nhãn của chính sách trong các bảng được bảo vệ.
- Ngoài hình thức tạo tự động, Oracle cũng cho phép ta tự định nghĩa giá trị tag cho các nhãn nhằm mục đích dễ quản lý, sắp xếp, so sánh và xử lý trong quá trình quản trị. Trong ví dụ bên dưới, ta quy định các nhãn có level "highly_sensivitve" (HS) có tag bắt đầu bằng số 4, "sensitive" (S) có tag bắt đầu bằng số 3,…

| Label Tag | Nhãn dữ liệu |
|---|---|
| 10000 | P |
| 20000 | C |
| 21000 | C:FNCL |
| 21100 | C:FNCL,OP |
| 30000 | S |
| 31110 | S:OP:WR |
| 40000 | HS |
| 42000 | HS:OP |

## B. Thực hành

- Phần này ta sẽ thực hiện bước 3 trong quy trình hiện thực OLS tạo các nhãn thật sự cần dùng từ các thành phần đã tạo ở phần III.
- Để tạo nhãn ta dùng thủ tục SA_LABEL_ADMIN.CREATE_LABEL. Khi sử dụng thủ tục này để tạo nhãn, ta phải tự định ra *label tag* (là một số nguyên có tối đa 8 chữ số) cho nhãn được tạo.

```
CONN sec_admin/secadmin;
BEGIN
    sa_label_admin.create_label
       (policy_name  => 'ACCESS_LOCATIONS',
       label_tag     => 10000,
       label_value   => 'PUB');
END;
/
EXECUTE sa_label_admin.create_label
('ACCESS_LOCATIONS',20000,'CONF');
----------------------------------------
EXECUTE sa_label_admin.create_label
('ACCESS_LOCATIONS',20010,'CONF::US');
EXECUTE sa_label_admin.create_label
('ACCESS_LOCATIONS',20020,'CONF::UK');
EXECUTE sa_label_admin.create_label
('ACCESS_LOCATIONS',20030,'CONF::CA');
----------------------------------------
EXECUTE sa_label_admin.create_label
```

```
('ACCESS_LOCATIONS',21020,'CONF:HR:UK');
EXECUTE sa_label_admin.create_label
('ACCESS_LOCATIONS',22040,'CONF:SM:UK,CA');
-----------------------------------------
EXECUTE sa_label_admin.create_label
('ACCESS_LOCATIONS',34000,'SENS:SM,FIN');
EXECUTE sa_label_admin.create_label
('ACCESS_LOCATIONS',39090,'SENS:HR,SM,FIN:CORP');
```

- Thông thường, khi xây dựng chính sách, ta cũng nên xây dựng hệ thống quy ước đặt *label tag* để tiện lợi trong việc quản lý. Trong đoạn code trên, ta quy ước chữ số đầu tiên biểu diễn level (1 là PUB, 2 là CONF, 3 là SENS), 2 chữ số kế tiếp biểu diễn các compartment (00 cho biết không có compartment), 2 chữ số cuối biểu diễn group (00 cho biết không có group).
  (Lưu ý là trong phần thực hành này chỉ tạo một số nhãn để minh họa, chứ không tạo hết tất cả các nhãn cần thiết).

- Để thay đổi nhãn, ta dùng thủ tục SA_LABEL_ADMIN.ALTER_LABEL. Ta có thể thay đổi giá trị của nhãn nhưng không thể thay đổi giá trị của *label tag*. Do vậy, độ nhạy cảm của dữ liệu có thể thay đổi được mà không cần phải cập nhật lại bảng chứa dữ liệu đó, do trong bảng chỉ lưu *label tag* chứ không lưu giá trị của nhãn.

```
CONN sec_admin/secadmin;
EXECUTE sa_label_admin.create_label
('ACCESS_LOCATIONS',30000,'SENS');
EXECUTE sa_label_admin.create_label
('ACCESS_LOCATIONS',30090,'SENS::CORP');

BEGIN
    sa_label_admin.alter_label
       (policy_name       => 'ACCESS_LOCATIONS',
       label_tag          => 30000,
       new_label_value    => 'SENS:SM');
```

```
    sa_label_admin.alter_label
       (policy_name       => 'ACCESS_LOCATIONS',
       label_value        => 'SENS:SM',
       new_label_value    => 'SENS:HR');
END;
/
```

- Ta có thể xóa nhãn bằng thủ tục SA_LABEL_ADMIN.DROP_LABEL:

```
BEGIN
    sa_label_admin.drop_label
       (policy_name       => 'ACCESS_LOCATIONS',
       label_value        => 'SENS:HR');
END;
/
BEGIN
    sa_label_admin.drop_label
       (policy_name       => 'ACCESS_LOCATIONS',
       label_tag          => 30090);
END;
/
```

# V. Bài tập

1. Tạo user *ols_test* và cấp quyền để user này truy cập vào hệ thống được. Cấp quyền thực thi trên các gói thủ tục cần thiết để user này quản lý được một chính sách.

2. Tạo chính sách *region_policy* với tên cột chính sách là *region_label*. Thực hiện lệnh cần thiết để *ols_test* trở thành người quản lý chính sách này.

3. Disable thủ tục đã tạo ở câu 2. Sau đó enable nó lại.

4. Tạo các thành phần nhãn cho chính sách *region_policy*:
   - Level: level 1, level 2, level 3
   - Compartment: MANAGEMENT, EMPLOYEE
   - Group: REGION NORTH, REGION SOUTH, REGION EAST,REGION WEST