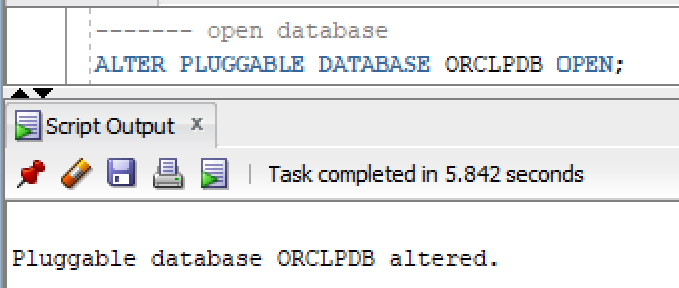
# I.Giới thiệu

## 1.1. Set up

Sử dụng sqldeveloper để mở hết các databases

|  |
| --- |
| ALTER PLUGGABLE DATABASE ORCLPDB OPEN; |



Mở Database Configuration Assistant

A screenshot of a computer

Description automatically generated

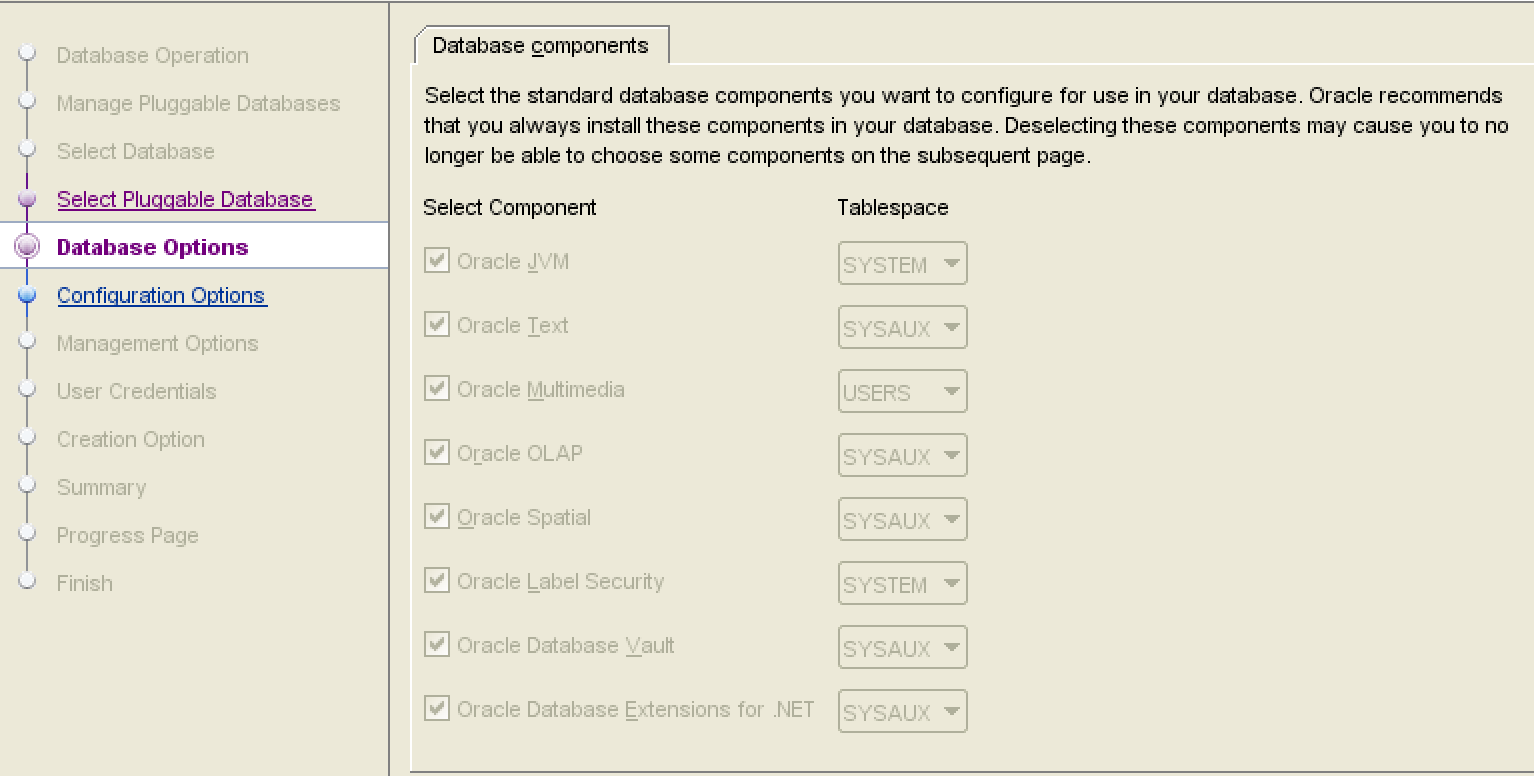
A screenshot of a computer

Description automatically generated

A screenshot of a computer

Description automatically generated

Password: CaoThiNgocPhung1811@



Tiếp tục next cho đến Oracle R and OML 4Py thì bỏ tích

A screenshot of a computer

Description automatically generated

## 1.2. Kích hoạt tài khoản LBACSYS

- Đặt lại mật khẩu của người dùng lbacsys thành lbacsys. Mở khóa tài khoản của người dùng lbacsys nếu nó đang bị khóa.

|  |
| --- |
| ALTER USER lbacsys IDENTIFIED BY lbacsys ACCOUNT UNLOCK ; |

A screenshot of a computer error

Description automatically generated

## 1.3. Chuẩn bị dữ liệu

- Đặt lại mật khẩu của tài khoản hr thành hr. Mở khóa tài khoản hr nếu tài khoản này đã bị khóa.

|  |
| --- |
| ALTER USER hr IDENTIFIED BY hr ACCOUNT UNLOCK; |

A screenshot of a computer

Description automatically generated

- Cấp cho người dùng hr\_sec các quyền

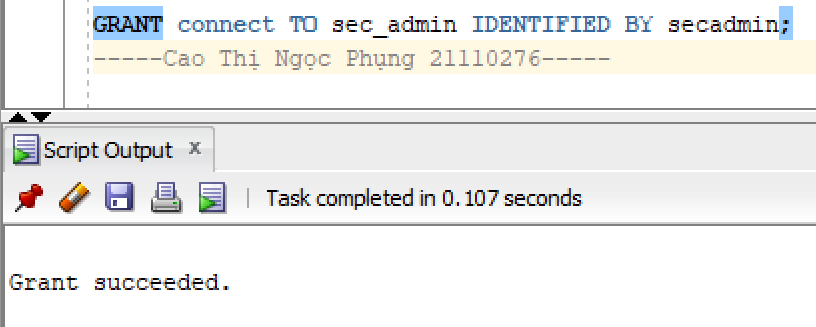
|  |
| --- |
| GRANT connect, create user, drop user, create role, drop any role  TO hr\_sec IDENTIFIED BY hrsec; |

A screenshot of a computer error

Description automatically generated

- Cấp quyền connect cho người dùng sec\_admin, cho phép người dùng này kết nối vào cơ sở dữ liệu. Đồng thời, lệnh đặt mật khẩu cho sec\_admin là secadmin.

|  |
| --- |
| GRANT connect TO sec\_admin IDENTIFIED BY secadmin; |



- Cấp quyền **connect** cho vai trò **emp\_role**, cho phép bất kỳ người dùng nào được gán vai trò này có thể kết nối vào cơ sở dữ liệu.

|  |
| --- |
| CREATE ROLE emp\_role;  GRANT connect TO emp\_role; |

A screenshot of a computer

Description automatically generated

- Gán vai trò emp\_role cho người dùng sking, cho phép người dùng này có các quyền mà emp\_role được cấp.

|  |
| --- |
| CREATE USER sking IDENTIFIED BY sking;  GRANT emp\_role TO sking; |

A screenshot of a computer

Description automatically generated

- Gán vai trò emp\_role cho người dùng nkochhar, cho phép người dùng này có các quyền mà emp\_role được cấp.

|  |
| --- |
| CREATE USER nkochhar IDENTIFIED BY nkochhar;  GRANT emp\_role TO nkochhar; |

A screenshot of a computer

Description automatically generated

- Gán vai trò emp\_role cho người dùng kpartner, giúp người dùng này có các quyền mà emp\_role được cấp.

|  |
| --- |
| CREATE USER kpartner IDENTIFIED BY kpartner;  GRANT emp\_role TO kpartner; |

A screenshot of a computer

Description automatically generated

- Gán vai trò emp\_role cho người dùng ldoran, giúp người dùng này có các quyền mà emp\_role được cấp.

|  |
| --- |
| CREATE USER ldoran IDENTIFIED BY ldoran;  GRANT emp\_role TO ldoran; |

A screenshot of a computer

Description automatically generated

- Cấp quyền **select** (quyền truy vấn dữ liệu) trên bảng **hr.locations** cho vai trò **emp\_role**, cho phép tất cả người dùng có vai trò này có thể xem dữ liệu từ bảng **hr.locations**.

|  |
| --- |
| GRANT select ON hr.locations TO emp\_role; |

A screenshot of a computer

Description automatically generated

# II. Chính sách trong Oracle Label Security

- OLS cho phép bạn gán các nhãn bảo mật (security labels) cho dữ liệu và xác định các chính sách kiểm soát truy cập dựa trên những nhãn này.

- Các nhãn này có thể đại diện cho các mức bảo mật khác nhau (ví dụ: "CONFIDENTIAL", "SECRET", "TOP SECRET") và giúp kiểm soát truy cập vào dữ liệu một cách linh hoạt.

- Người dùng có thể được gán các nhãn bảo mật tương ứng và chỉ được phép truy cập dữ liệu phù hợp với nhãn mà họ được cấp quyền.

|  |
| --- |
| EXEC LBACSYS.CONFIGURE\_OLS;  EXEC LBACSYS.OLS\_ENFORCEMENT.ENABLE\_OLS; |

A screenshot of a computer program

Description automatically generated

- Cấp quyền **SYSDBA** cho user **LBACSYS**.

|  |
| --- |
| GRANT SYSDBA TO LBACSYS |

A screenshot of a computer

Description automatically generated

- Tạo một chính sách bảo mật có tên ACCESS\_LOCATIONS, sử dụng cột OLS\_COLUMN để áp dụng nhãn bảo mật trong Oracle Label Security.

|  |
| --- |
| BEGIN  SA\_SYSDBA.CREATE\_POLICY (  policy\_name => 'ACCESS\_LOCATIONS',  column\_name => 'OLS\_COLUMN');  END; |

A screenshot of a computer

Description automatically generated

- Cấp quyền access\_locations\_dba cho user sec\_admin.

|  |
| --- |
| GRANT access\_locations\_dba TO sec\_admin; |

A screenshot of a computer

Description automatically generated

- Cấp quyền **EXECUTE** cho user **sec\_admin** trên đối tượng **sa\_components**.

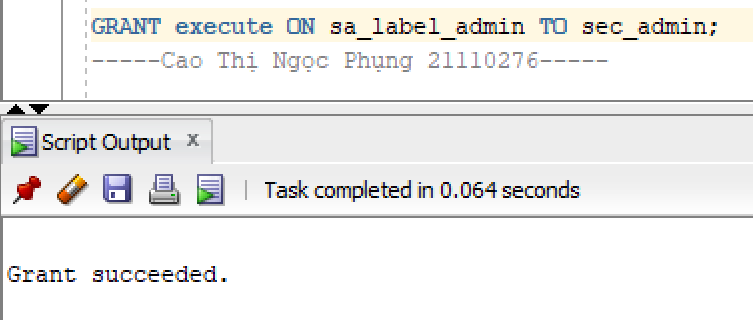
|  |
| --- |
| GRANT execute ON sa\_components TO sec\_admin; |

A screenshot of a computer

Description automatically generated

- Cấp quyền **EXECUTE** cho user **sec\_admin** trên đối tượng **sa\_label\_admin**.

|  |
| --- |
| GRANT execute ON sa\_label\_admin TO sec\_admin; |



- Cấp quyền **EXECUTE** cho user **sec\_admin** trên đối tượng **sa\_policy\_admin**.

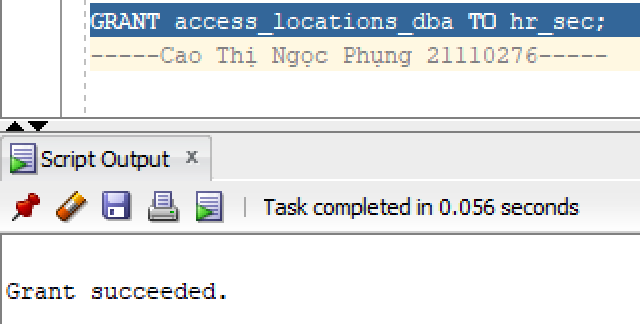
|  |
| --- |
| GRANT execute ON sa\_policy\_admin TO sec\_admin; |

A screenshot of a computer

Description automatically generated

- Cấp quyền access\_locations\_dba cho user hr\_sec.

|  |
| --- |
| GRANT access\_locations\_dba TO hr\_sec; |



- Cấp quyền **EXECUTE** cho user **hr\_sec** trên đối tượng **sa\_user\_admin**.

|  |
| --- |
| GRANT execute ON sa\_user\_admin TO hr\_sec; |

A screenshot of a computer

Description automatically generated

- Gọi thủ tục **create\_policy** từ package **sa\_sysdba** để tạo một chính sách bảo mật mới.

|  |
| --- |
| BEGIN sa\_sysdba.create\_policy (  policy\_name => 'Different\_Policy');  END; |

A screenshot of a computer program

Description automatically generated

- Gọi thủ tục **create\_level** từ package **sa\_components** để tạo một cấp độ bảo mật mới cho chính sách bảo mật.

|  |
| --- |
| BEGIN sa\_components.create\_level (  policy\_name => 'Different\_Policy',  long\_name => 'foo',  short\_name => 'bar',  level\_num => 9);  END; |

A screenshot of a computer program

Description automatically generated

**ORA-12407: unauthorized operation for policy Different\_Policy**  
Đây là lỗi chính, cho biết rằng chính sách bảo mật (**Different\_Policy**) không cho phép phiên làm việc hiện tại thực hiện thao tác đang cố gắng thực hiện.

**ORA-06512: tại LBACSYS.SA\_COMPONENTS**  
Lỗi này xảy ra khi thực hiện một lệnh PL/SQL, cụ thể là liên quan đến gói (**package**) SA\_COMPONENTS thuộc về schema **LBACSYS**. LBACSYS là schema chứa các thành phần của Oracle Label Security (OLS).

🡪 Ta dùng SA\_SYSDBA.DROP\_POLICY để xóa chính sách 'Different\_Policy' ở trên:

|  |
| --- |
| BEGIN sa\_sysdba.drop\_policy (  policy\_name => 'Different\_Policy',  drop\_column => true);  END; |

A screenshot of a computer program

Description automatically generated

# III. Các thành phần của nhãn dữ liệu

## 3.1. Level

### 3.1.1 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

|  |
| --- |
| BEGIN sa\_components.create\_level (  policy\_name => 'ACCESS\_LOCATIONS',  long\_name => 'PUBLIC',  short\_name => 'PUB',  level\_num => 1000);  END; |

A screenshot of a computer program

Description automatically generated

- Mức độ bảo mật này sẽ được sử dụng để phân quyền truy cập dữ liệu dựa trên nhãn bảo mật của Oracle Label Security.

|  |
| --- |
| BEGIN  sa\_components.create\_level(  'ACCESS\_LOCATIONS',  2000,  'CONF',  'CONFIDENTIAL'  );  END; |

A screenshot of a computer program

Description automatically generated

- Mức độ bảo mật này sẽ được sử dụng để kiểm soát quyền truy cập dữ liệu, giúp phân cấp mức độ bảo mật cho các bản ghi dữ liệu trong hệ thống dựa trên nhãn bảo mật của Oracle Label Security.

|  |
| --- |
| BEGIN  sa\_components.create\_level (  'ACCESS\_LOCATIONS',  3000,  'SENS',  'SENSITIVE');  END; |

A screenshot of a computer program

Description automatically generated

### 3.1.2. Chỉnh sửa 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.

|  |
| --- |
| BEGIN  sa\_components.alter\_level (  policy\_name => 'ACCESS\_LOCATIONS',  level\_num => 4000,  new\_short\_name => 'TS',  new\_long\_name => 'TOP SECRET');  END; |

A screenshot of a computer program

Description automatically generated

- Cho phép cập nhật mô tả của mức độ bảo mật mà không thay đổi giá trị số hoặc các thông tin khác, đảm bảo rằng thông tin bảo mật được quản lý chính xác trong hệ thống Oracle Label Security.

|  |
| --- |
| BEGIN  sa\_components.alter\_level (  policy\_name => 'ACCESS\_LOCATIONS',  short\_name => 'TS',  new\_long\_name => 'TOP SENSITIVE');  END; |

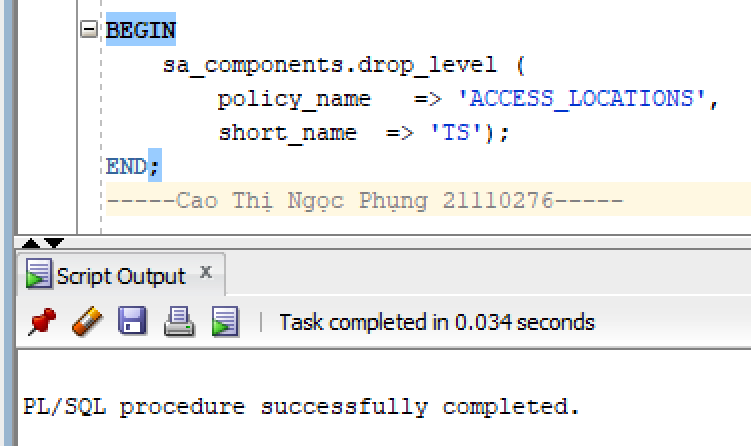
A screenshot of a computer program

Description automatically generated

- Lệnh này xóa mức độ bảo mật có tên ngắn TS ra khỏi chính sách bảo mật ACCESS\_LOCATIONS. Sau khi lệnh này được thực hiện, mức độ bảo mật TS sẽ không còn tồn tại trong chính sách này, và các dữ liệu được bảo vệ bởi mức độ bảo mật đó sẽ không còn bị áp dụng chính sách bảo mật tương ứng nữa.

### 3.1.3. Xóa level

|  |
| --- |
| BEGIN  sa\_components.drop\_level (  policy\_name => 'ACCESS\_LOCATIONS',  short\_name => 'TS');  END; |



## 3.2. Compartment

### 3.2.1 Tạo compartment

- Tạo một ngăn bảo mật mới cho chính sách **ACCESS\_LOCATIONS** với tên dài là **'SALES\_MARKETING'**, tên ngắn là **'SM'**, và số ngăn là **2000**.

|  |
| --- |
| BEGIN  sa\_components.create\_compartment (  policy\_name => 'ACCESS\_LOCATIONS',  long\_name => 'SALES\_MARKETING',  short\_name => 'SM',  comp\_num => 2000);  END; |

A screenshot of a computer program

Description automatically generated

Lỗi gặp phải là do vi phạm ràng buộc duy nhất (unique constraint) của bảng, cụ thể là ràng buộc LBACSYS.OLS\_COMP\_PK. Điều này xảy ra khi bạn cố gắng chèn một bản ghi có khóa chính trùng với bản ghi đã tồn tại.

Nếu bản ghi đã tồn tại nhưng không còn cần thiết, thử xóa bản ghi cũ:

|  |
| --- |
| BEGIN  sa\_components.drop\_compartment(  policy\_name => 'ACCESS\_LOCATIONS',  short\_name => 'SM');  END; |

A screenshot of a computer program

Description automatically generated

Sau đó chạy lại lệnh trên là được

A screenshot of a computer program

Description automatically generated

- Tạo một ngăn bảo mật mới cho chính sách **ACCESS\_LOCATIONS** với số ngăn là **3000**, tên ngắn là **'FIN'**, và tên dài là **'FINANCE'**.

|  |
| --- |
| BEGIN  sa\_components.create\_compartment (  'ACCESS\_LOCATIONS',  3000,  'FIN',  'FINANCE');  END; |

A white rectangular object with yellow lines

Description automatically generated

- Tạo một ngăn bảo mật mới cho chính sách **ACCESS\_LOCATIONS** với số ngăn là **1000**, tên ngắn là **'HR'**, và tên dài là **'HUMAN RESOURCES'**.

|  |
| --- |
| BEGIN  sa\_components.create\_compartment (  'ACCESS\_LOCATIONS',  1000,  'HR',  'HUMAN RESOURCES');  END; |

A white rectangular object with yellow lines

Description automatically generated

- 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.

- Tạo một ngăn bảo mật mới cho chính sách **ACCESS\_LOCATIONS** với số ngăn là **4000**, tên ngắn là **'PR'**, và tên dài là **'PUBLIC RELATIONS'**.

|  |
| --- |
| BEGIN  sa\_components.create\_compartment (  'ACCESS\_LOCATIONS',  4000,  'PR',  'PUBLIC RELATIONS');  END; |

A white rectangular object with a white border

Description automatically generated

### 3.2.2 Chỉnh sửa compartment

- Thay đổi ngăn bảo mật số **4000** trong chính sách **ACCESS\_LOCATIONS** với tên ngắn mới là **'PU'** và tên dài mới là **'PURCHASING'**.

|  |
| --- |
| BEGIN  sa\_components.alter\_compartment (  policy\_name => 'ACCESS\_LOCATIONS',  comp\_num => 4000,  new\_short\_name => 'PU',  new\_long\_name => 'PURCHASING');  END; |

A white rectangular object with yellow lines

Description automatically generated

- Thay đổi ngăn bảo mật có tên ngắn **'PU'** trong chính sách **ACCESS\_LOCATIONS** với tên dài mới là **'PURCHASE'**.

|  |
| --- |
| BEGIN  sa\_components.alter\_compartment (  policy\_name => 'ACCESS\_LOCATIONS',  short\_name => 'PU',  new\_long\_name => 'PURCHASE');  END; |

A white rectangular object with a yellow stripe

Description automatically generated

### 3.2.3 Xóa compartment

- 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.

|  |
| --- |
| BEGIN  sa\_components.drop\_compartment (  policy\_name => 'ACCESS\_LOCATIONS',  short\_name => 'PU');  END; |

A white rectangular object with yellow lines

Description automatically generated

## 3.3. Group

### 3.3.1 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.

- Tạo một nhóm bảo mật mới cho chính sách **ACCESS\_LOCATIONS** với tên dài là **'CORPORATE'**, tên ngắn là **'CORP'**, số nhóm là **10**, và không có nhóm cha (**parent\_name = NULL**).

|  |
| --- |
| BEGIN  sa\_components.create\_group (  policy\_name => 'ACCESS\_LOCATIONS',  long\_name => 'CORPORATE',  short\_name => 'CORP',  group\_num => 10,  parent\_name => NULL);  END; |

A white rectangular object with a white border

Description automatically generated

- Tạo một nhóm bảo mật mới cho chính sách **ACCESS\_LOCATIONS** với số nhóm là **30**, tên ngắn là **'US'**, tên dài là **'UNITED STATES'**, và nhóm cha là **'CORP'**.

|  |
| --- |
| BEGIN  sa\_components.create\_group(  'ACCESS\_LOCATIONS',  30,  'US',  'UNITED STATES',  'CORP');  END; |

A white rectangular object with yellow lines

Description automatically generated

- Tạo một nhóm bảo mật mới cho chính sách **ACCESS\_LOCATIONS** với số nhóm là **50**, tên ngắn là **'UK'**, tên dài là **'UNITED KINGDOM'**, và nhóm cha là **'CORP'**.

|  |
| --- |
| BEGIN  sa\_components.create\_group(  'ACCESS\_LOCATIONS',  50,  'UK',  'UNITED KINGDOM',  'CORP');  END; |

A white rectangular object with a yellow edge

Description automatically generated

- Tạo một nhóm bảo mật mới cho chính sách **ACCESS\_LOCATIONS** với số nhóm là **70**, tên ngắn là **'CA'**, tên dài là **'CANADA'**, và nhóm cha là **'CORP'**.

|  |
| --- |
| BEGIN  sa\_components.create\_group(  'ACCESS\_LOCATIONS',  70,  'CA',  'CANADA',  'CORP');  END; |

A white rectangular object with yellow lines

Description automatically generated

- 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.

|  |
| --- |
| BEGIN  sa\_components.create\_group (  'ACCESS\_LOCATIONS',  90,  'FR',  'FRANCE',  'CORP');  END; |

A white rectangular object with a yellow border

Description automatically generated

### 3.3.2 Chỉnh sửa group

- Thay đổi nhóm bảo mật có số nhóm **90** trong chính sách **ACCESS\_LOCATIONS**, cập nhật tên ngắn thành **'RFR'** và tên dài thành **'REPUBLIC FRANCE'**.

|  |
| --- |
| BEGIN  sa\_components.alter\_group (  policy\_name => 'ACCESS\_LOCATIONS',  group\_num => 90,  new\_short\_name => 'RFR',  new\_long\_name => 'REPUBLIC FRANCE');  END; |

A screenshot of a computer

Description automatically generated

- Lệnh này cập nhật nhóm bảo mật có tên ngắn là **'RFR'** trong chính sách **ACCESS\_LOCATIONS**, thay đổi tên dài của nhóm thành **'PURCHASE'**. Sau khi thực thi, nhóm **'RFR'** sẽ có tên dài mới là **'PURCHASE'**.

|  |
| --- |
| BEGIN  sa\_components.alter\_group (  policy\_name => 'ACCESS\_LOCATIONS',  short\_name => 'RFR',  new\_long\_name => 'PURCHASE');  END; |

A screenshot of a computer

Description automatically generated

### 3.3.3 Chỉnh sửa group

- 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.

|  |
| --- |
| BEGIN  sa\_components.drop\_group (  policy\_name => 'ACCESS\_LOCATIONS',  short\_name => 'RFR');  END; |

A screenshot of a computer

Description automatically generated

# IV. Chi tiết về nhãn dữ liệu

## 4.1 Tạo label

- 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.

- Tạo ra một nhãn bảo mật với giá trị 'PUB' trong chính sách 'ACCESS\_LOCATIONS' và gán cho nhãn đó một mã số 10000.

|  |
| --- |
| BEGIN  sa\_label\_admin.create\_label (  policy\_name => 'ACCESS\_LOCATIONS',  label\_tag => 10000,  label\_value => 'PUB');  END; |

A white rectangular object with a yellow line

Description automatically generated

- Tạo một nhãn bảo mật với giá trị 'CONF' trong chính sách 'ACCESS\_LOCATIONS' và gán mã số 20000 cho nhãn đó, sử dụng hàm sa\_label\_admin.create\_label.

|  |
| --- |
| BEGIN  sa\_label\_admin.create\_label (  'ACCESS\_LOCATIONS',  20000,  'CONF');  END; |

A white and yellow rectangle

Description automatically generated

- Tạo một nhãn bảo mật với giá trị 'CONF' trong chính sách 'ACCESS\_LOCATIONS' và gán mã số 20000 cho nhãn đó, sử dụng hàm sa\_label\_admin.create\_label.

|  |
| --- |
| BEGIN  sa\_label\_admin.create\_label (  'ACCESS\_LOCATIONS',  20010,  'CONF::US');  END; |

A screenshot of a computer

Description automatically generated

- Tạo một nhãn bảo mật với giá trị 'CONF::UK' trong chính sách 'ACCESS\_LOCATIONS' và gán mã số 20020 cho nhãn đó, sử dụng hàm sa\_label\_admin.create\_label.

|  |
| --- |
| BEGIN  sa\_label\_admin.create\_label (  'ACCESS\_LOCATIONS',  20020,  'CONF::UK');  END; |

A white rectangular object with yellow lines

Description automatically generated

- Câu lệnh này tạo một nhãn bảo mật với giá trị 'CONF::CA' trong chính sách 'ACCESS\_LOCATIONS' và gán mã số 20030 cho nhãn đó, sử dụng hàm sa\_label\_admin.create\_label.

|  |
| --- |
| BEGIN  sa\_label\_admin.create\_label(  'ACCESS\_LOCATIONS',  20030,  'CONF::CA');  END; |

A white rectangular object with yellow lines

Description automatically generated

- Tạo một nhãn CONF:HR' bảo mật trong chính sách 'ACCESS\_LOCATIONS' với mã số 21020 sử dụng hàm sa\_label\_admin.create\_label.

|  |
| --- |
| BEGIN  sa\_label\_admin.create\_label(  'ACCESS\_LOCATIONS',  21020,  'CONF:HR:UK'  );  END; |

A white and yellow line on a white background

Description automatically generated

- Tạo một nhãn 'CONF:SM,CA' bảo mật trong chính sách 'ACCESS\_LOCATIONS' với mã số 22040 sử dụng hàm sa\_label\_admin.create\_label.

|  |
| --- |
| BEGIN  sa\_label\_admin.create\_label(  'ACCESS\_LOCATIONS',  22040,  'CONF:SM:UK,CA'  );  END; |

A screenshot of a computer

Description automatically generated

- Tạo một nhãn bảo mật với giá trị 'SENS:SM,FIN' trong chính sách 'ACCESS\_LOCATIONS' và gán mã số 34000 cho nhãn đó, sử dụng hàm sa\_label\_admin.create\_label.

|  |
| --- |
| BEGIN  sa\_label\_admin.create\_label(  'ACCESS\_LOCATIONS',  34000,  'SENS:SM,FIN'  );  END; |

A screenshot of a computer

Description automatically generated

- Tạo một nhãn bảo mật với giá trị 'SENS:HR,SM,FIN:CORP' trong chính sách 'ACCESS\_LOCATIONS' và gán mã số 39090 cho nhãn đó, sử dụng hàm sa\_label\_admin.create\_label.

|  |
| --- |
| BEGIN  sa\_label\_admin.create\_label(  'ACCESS\_LOCATIONS',  39090,  'SENS:HR,SM,FIN:CORP'  );  END; |

A white rectangular object with a white border

Description automatically generated

- 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.

- Tạo một nhãn bảo mật với giá trị 'SENS' trong chính sách 'ACCESS\_LOCATIONS' và gán mã số 30000 cho nhãn đó, sử dụng hàm sa\_label\_admin.create\_label.

|  |
| --- |
| BEGIN  sa\_label\_admin.create\_label (  'ACCESS\_LOCATIONS',  30000,  'SENS');  END; |

A white rectangular object with a white border

Description automatically generatedTop of Form

- Tạo một nhãn bảo mật với giá trị 'SENS::CORP' trong chính sách 'ACCESS\_LOCATIONS' và gán mã số 30090 cho nhãn đó, sử dụng hàm sa\_label\_admin.create\_label.

|  |
| --- |
| BEGIN  sa\_label\_admin.create\_label (  'ACCESS\_LOCATIONS',  30090,  'SENS::CORP');  END; |

A white rectangular object with yellow lines

Description automatically generated

## 4.2 Chỉnh sửa labelBottom of Form

- Thay đổi giá trị của hai nhãn bảo mật trong chính sách 'ACCESS\_LOCATIONS'. Nhãn có mã số 30000 ban đầu có giá trị 'SENS' được thay đổi thành 'SENS:SM'.Nhãn có giá trị 'SENS:SM' được thay đổi thành 'SENS:HR'.Sử dụng hàm sa\_label\_admin.alter\_label để thực hiện các thay đổi này.

|  |
| --- |
| 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; |

A white rectangular object with yellow lines

Description automatically generated

## Xóa label

- Ta có thể xóa nhãn bằng thủ tục SA\_LABEL\_ADMIN.DROP\_LABEL

- Câu lệnh đầu tiên xóa nhãn bảo mật có giá trị 'SENS:HR' trong chính sách 'ACCESS\_LOCATIONS'.

|  |
| --- |
| BEGIN  sa\_label\_admin.drop\_label(  policy\_name => 'ACCESS\_LOCATIONS',  label\_value => 'SENS:HR');  END; |

A white rectangular object with yellow lines

Description automatically generated

- Câu lệnh thứ hai xóa nhãn bảo mật có mã số 30090 trong cùng chính sách 'ACCESS\_LOCATIONS'.

|  |
| --- |
| BEGIN  sa\_label\_admin.drop\_label(  policy\_name => 'ACCESS\_LOCATIONS',  label\_tag => 30090);  END; |

A white rectangular object with yellow lines

Description automatically generated

# V. Bài tập

## 5.1. Tạo user *ols\_test* và cấp quyền

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.

Dùng user SYS để tạo một user mới tên **ols\_test** với mật khẩu **olstest**, sau đó cấp cho user này quyền **CONNECT** để có thể đăng, quyền **CREATE SESSION** để tạo phiên làm việc, quyền **CREATE TABLE** để tạo bảng, và quyền **UNLIMITED TABLESPACE** để sử dụng không gian bảng không giới hạn.

|  |
| --- |
| GRANT connect TO ols\_test IDENTIFIED BY olstest;  GRANT CREATE SESSION TO ols\_test;  GRANT CREATE TABLE TO ols\_test;  GRANT UNLIMITED TABLESPACE TO ols\_test; |

A screenshot of a computer

Description automatically generated

## 5.2. Tạo chính sách *region\_policy*

- 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.

|  |
| --- |
| BEGIN  SA\_SYSDBA.CREATE\_POLICY(  policy\_name => 'region\_policy',  column\_name => 'region\_label' );  END; |

A white rectangular object with a yellow border

Description automatically generated

Khi một **chính sách bảo mật** được tạo ra, Oracle tự động tạo một vai trò quản trị (role) với tên dạng **<policy\_name>\_DBA**, và vai trò này ban đầu được gán cho **user LBACSYS**. Để người dùng khác có thể quản lý chính sách.

Vì vậy, đối với chính sách **region\_policy**, role quản trị sẽ có tên là **region\_policy\_dba**. Để user **ols\_test** quản lý chính sách.

Các lệnh này cấp quyền cho user **ols\_test** để quản lý chính sách bảo mật **region\_policy**. Cụ thể, lệnh **GRANT region\_policy\_dba TO ols\_test** cấp vai trò quản trị của chính sách **region\_policy**, cho phép **ols\_test** quản lý chính sách này

|  |
| --- |
| GRANT region\_policy\_dba TO ols\_test;  GRANT EXECUTE ON sa\_user\_admin TO ols\_test;  GRANT EXECUTE ON sa\_policy\_admin TO ols\_test;  GRANT EXECUTE ON sa\_label\_admin TO ols\_test;  GRANT EXECUTE ON sa\_components TO ols\_test;  GRANT EXECUTE ON sa\_session TO ols\_test; |

A screenshot of a computer

Description automatically generated

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

- Bạn cần cấp quyền **INHERIT PRIVILEGES** cho user thực thi thủ tục **DISABLE\_POLICY**

|  |
| --- |
| GRANT INHERIT PRIVILEGES ON USER LBACSYS TO LBACSYS; |

A white rectangular object with a light

Description automatically generated

- disable policy

|  |
| --- |
| BEGIN  SA\_SYSDBA.DISABLE\_POLICY(  policy\_name => 'region\_policy');  END; |

A screenshot of a computer

Description automatically generated

- enable policy

|  |
| --- |
| BEGIN  SA\_SYSDBA.ENABLE\_POLICY(  policy\_name => 'region\_policy');  END; |

A screenshot of a computer

Description automatically generated

## 5.4. Tạo các thành phần nhãn cho chính sách *region\_policy*:

### 5.4.1. Level

- level 1

|  |
| --- |
| BEGIN  sa\_components.create\_level (  policy\_name => 'region\_policy',  long\_name => 'Level 1',  short\_name => 'L1',  level\_num => 1);  END; |

A screenshot of a computer

Description automatically generated

- level 2

|  |
| --- |
| BEGIN  sa\_components.create\_level (  policy\_name => 'region\_policy',  long\_name => 'Level 2',  short\_name => 'L2',  level\_num => 2);  END; |

A screenshot of a computer

Description automatically generated

- level 3

|  |
| --- |
| BEGIN  sa\_components.create\_level (  policy\_name => 'region\_policy',  long\_name => 'Level 3',  short\_name => 'L3',  level\_num => 3);  END; |

A screenshot of a computer

Description automatically generated

### 5.4.2 Compartment

- MANAGEMENT

|  |
| --- |
| BEGIN  sa\_components.create\_compartment (  policy\_name => 'region\_policy',  long\_name => 'MANAGEMENT',  short\_name => 'MN',  comp\_num => 1000);  END; |

A screenshot of a computer

Description automatically generated

- EMPLOYEE

|  |
| --- |
| BEGIN  sa\_components.create\_compartment (  policy\_name => 'region\_policy',  long\_name => 'EMPLOYEE',  short\_name => 'EMP',  comp\_num => 2000);  END; |

A screenshot of a computer

Description automatically generated

### 5.4.3 Group

- REGION NORTH

|  |
| --- |
| BEGIN  sa\_components.create\_group (  policy\_name => 'region\_policy',  long\_name => 'REGION NORTH',  short\_name => 'RN',  group\_num => 101);  END; |

A screenshot of a computer

Description automatically generated

- REGION SOUTH

|  |
| --- |
| BEGIN  sa\_components.create\_group (  policy\_name => 'region\_policy',  long\_name => 'REGION SOUTH',  short\_name => 'RS',  group\_num => 102);  END; |

A screenshot of a computer

Description automatically generated

- REGION EAST

|  |
| --- |
| BEGIN  sa\_components.create\_group (  policy\_name => 'region\_policy',  long\_name => 'REGION EAST',  short\_name => 'RE',  group\_num => 103);  END; |

A screenshot of a computer

Description automatically generated

- REGION WEST

|  |
| --- |
| BEGIN  sa\_components.create\_group (  policy\_name => 'region\_policy',  long\_name => 'REGION WEST',  short\_name => 'RW',  group\_num => 104);  END; |

A screenshot of a computer

Description automatically generated