# I. Các loại nhãn người dùng

## 1.1. Gán quyền người dùng theo các thành phần của nhãn

- Louise Doran là nhân viên thuộc phòng Sales nên ta sẽ gán các level, compartment và group phù hợp với phòng ban và cấp bậc của Louise.

- Để gán level cho người dùng, ta dùng thủ tục SA\_USER\_ADMIN.SET\_LEVELS.

|  |
| --- |
| BEGIN  sa\_user\_admin.set\_levels (  policy\_name => 'ACCESS\_LOCATIONS',  user\_name => 'LDORAN',  max\_level => 'CONF',  min\_level => 'PUB',  def\_level => 'CONF',  row\_level => 'CONF');  END; |

A white rectangular object with a black border

Description automatically generated with medium confidence

- Gán compartment cho người dùng, ta dùng thủ tục SA\_USER\_ADMIN.SET\_COMPARTMENTS.

|  |
| --- |
| BEGIN  sa\_user\_admin.set\_compartments (  policy\_name => 'ACCESS\_LOCATIONS',  user\_name => 'LDORAN',  read\_comps => 'SM,HR',  write\_comps => 'SM',  def\_comps => 'SM',  row\_comps => 'SM');  END; |

A white rectangular object with yellow lines

Description automatically generated

- Gán group cho người dùng, ta dùng thủ tục SA\_USER\_ADMIN.SET\_GROUPS.

|  |
| --- |
| BEGIN  sa\_user\_admin.set\_groups (  policy\_name => 'ACCESS\_LOCATIONS',  user\_name => 'LDORAN',  read\_groups => 'UK,CA',  write\_groups => 'UK',  def\_groups => 'UK',  row\_groups => 'UK');  END; |

A white rectangular object with a yellow line

Description automatically generated

## 1.2. Gán quyền người dùng theo các nhãn

- Karen Partner là trưởng phòng Sales. Ta sẽ gán các nhãn phù hợp với phòng ban và cấp bậc của Karen.

|  |
| --- |
| BEGIN  sa\_user\_admin.set\_user\_labels (  policy\_name => 'ACCESS\_LOCATIONS',  user\_name => 'KPARTNER',  max\_read\_label => 'SENS:SM,HR:UK,CA',  max\_write\_label => 'SENS:SM:UK',  min\_write\_label => 'CONF',  def\_label => 'SENS:SM,HR:UK',  row\_label => 'SENS:SM:UK');  END; |

A white rectangular object with a yellow line

Description automatically generated

## 1.3. Gán các quyền đặc biệt

- Steven King là tổng giám đốc có toàn quyền trên cơ sở dữ liệu, nên ta cấp quyền FULL cho người dùng này.

|  |
| --- |
| BEGIN  sa\_user\_admin.set\_user\_privs (  policy\_name => 'ACCESS\_LOCATIONS',  user\_name => 'SKING',  PRIVILEGES => 'FULL');  END; |

A white rectangular object with yellow lines

Description automatically generated

- Neena Kochhar là giám đốc điều hành nên ta có thể cấp quyền READ để người này có thể xem toàn bộ dữ liệu.

|  |
| --- |
| BEGIN  sa\_user\_admin.set\_user\_privs (  policy\_name => 'ACCESS\_LOCATIONS',  user\_name => 'NKOCHHAR',  PRIVILEGES => 'READ');  END; |

A whiteboard with a yellow stripe

Description automatically generated

# II. Áp dụng chính sách OLS

## 2.1. Áp dụng chính sách cho bảng

Để gán chính sách cho các bảng ta dung thủ tục SA\_POLICY\_ADMIN.APPLY\_TABLE\_POLICY

|  |
| --- |
| BEGIN  sa\_policy\_admin.apply\_table\_policy (  policy\_name => 'ACCESS\_LOCATIONS',  schema\_name => 'HR',  table\_name => 'LOCATIONS',  table\_options => 'NO\_CONTROL');  END; |

A white box with yellow lines

Description automatically generated

- Ta đăng nhập vào tài khoản HR để xem sự thay đổi của bảng sau khi gán chính sách

|  |
| --- |
| DESCRIBE locations; |

A white rectangular object with a yellow border

Description automatically generated

## 2.2. Gán nhãn cho dữ liệu

- Để sec\_admin có thể thiết lập nhãn cho các dòng dữ liệu ta cần gán quyền cho sec\_admin

|  |
| --- |
| GRANT select, insert, update ON locations TO sec\_admin; |

A white rectangular object with yellow lines

Description automatically generated

- Khi đã có đủ quyền ta gán nhãn cho các dòng dữ liệu. Đầu tiên ta gán nhãn CONF cho mọi dữ liệu trong bảng:

|  |
| --- |
| UPDATE hr.locations  SET ols\_column = char\_to\_label ('ACCESS\_LOCATIONS', 'CONF'); |

A white rectangular object with yellow lines

Description automatically generated

|  |
| --- |
| UPDATE hr.locations  SET ols\_column = char\_to\_label ('ACCESS\_LOCATIONS', 'CONF::UK')  WHERE country\_id = 'UK'; |

A screenshot of a computer

Description automatically generated

|  |
| --- |
| UPDATE hr.locations  SET ols\_column = char\_to\_label ('ACCESS\_LOCATIONS', 'CONF::CA')  WHERE country\_id = 'CA'; |

A screenshot of a computer

Description automatically generated

- Giả sử có một số địa chỉ là thông tin đặc biệt cần bảo mật, nên ta gán cho những dòng này nhãn có độ bảo mật cao hơn

|  |
| --- |
| UPDATE hr.locations  SET ols\_column = char\_to\_label  ('ACCESS\_LOCATIONS', 'CONF:SM:UK,CA')  WHERE (country\_id = 'CA'  AND city = 'Toronto')  OR (country\_id = 'UK'  AND city = 'Oxford'); |

A white rectangular object with a yellow stripe

Description automatically generated

|  |
| --- |
| UPDATE hr.locations  SET ols\_column = char\_to\_label ('ACCESS\_LOCATIONS', 'CONF:HR:UK')  WHERE country\_id = 'UK'  AND city = 'London'; |

A screenshot of a computer

Description automatically generated

|  |
| --- |
| UPDATE hr.locations  SET ols\_column = char\_to\_label ('ACCESS\_LOCATIONS', 'SENS:HR,SM,FIN:CORP')  WHERE country\_id = 'CH'  AND city = 'Geneva'; |

A screenshot of a computer

Description automatically generated

- Do ở trên chúng ta đã thiết lập tùy chọn „NO\_CONTROL‟ cho việc áp dụng chính sách nên ở đây chúng ta cần remove chính sách khỏi bảng rồi áp dụng lại chính sách với tùy chọn mới để chính sách có thể được kích hoạt bảo vệ cho bảng.

|  |
| --- |
| BEGIN  sa\_policy\_admin.remove\_table\_policy (  policy\_name => 'ACCESS\_LOCATIONS',  schema\_name => 'HR',  table\_name => 'LOCATIONS');  sa\_policy\_admin.apply\_table\_policy (  policy\_name => 'ACCESS\_LOCATIONS',  schema\_name => 'HR',  table\_name => 'LOCATIONS',  table\_options => 'READ\_CONTROL,WRITE\_CONTROL,CHECK\_CONTROL');  END; |

A screenshot of a computer

Description automatically generated

# III. Một số kĩ thật nâng cao trong OLS

## 3.1. Che dấu cột thông tin chính sách

- Do trong bài lab trước, ta đã áp dụng chính sách cho bảng mà không có tùy chọn HIDE nên trong bài lab này ta phải remove chính sách (xóa cả cột thông tin chính sách), thực hiện lại đoạn code gán nhãn trong bài lab trước và gán lại chính sách.

|  |
| --- |
| BEGIN  sa\_policy\_admin.remove\_table\_policy (  policy\_name => 'ACCESS\_LOCATIONS',  schema\_name => 'HR',  table\_name => 'LOCATIONS',  drop\_column => true);  END; |

A white rectangular object with a white border

Description automatically generated

|  |
| --- |
| SELECT \*  FROM hr.locations; |

A screenshot of a computer

Description automatically generated

🡪 Ta nhận thấy bây giờ cột OLS\_COLUMN đã được xóa.

- Gán lại chính sách cho bảng với NO\_CONTROL và HIDE

|  |
| --- |
| BEGIN  sa\_policy\_admin.apply\_table\_policy (  policy\_name => 'ACCESS\_LOCATIONS',  schema\_name => 'HR',  table\_name => 'LOCATIONS',  table\_options => 'HIDE,NO\_CONTROL');  END; |

A white rectangular object with a yellow line

Description automatically generated

- Gán lại nhãn cho dữ liệu trong bảng (do lúc remove đã xóa mất cột chứa thông tin chính sách)

|  |
| --- |
| UPDATE hr.locations  SET ols\_column = char\_to\_label ('ACCESS\_LOCATIONS', 'CONF'); |

A screenshot of a computer

Description automatically generated

|  |
| --- |
| UPDATE hr.locations  SET ols\_column = char\_to\_label ('ACCESS\_LOCATIONS', 'CONF::US')  WHERE country\_id = 'US'; |

A screenshot of a computer

Description automatically generated

|  |
| --- |
| UPDATE hr.locations  SET ols\_column = char\_to\_label ('ACCESS\_LOCATIONS', 'CONF::UK')  WHERE country\_id = 'UK'; |

A screenshot of a computer

Description automatically generated

|  |
| --- |
| UPDATE hr.locations  SET ols\_column = char\_to\_label ('ACCESS\_LOCATIONS', 'CONF::CA')  WHERE country\_id = 'CA'; |

A white rectangular object with blue and yellow text

Description automatically generated

|  |
| --- |
| UPDATE hr.locations  SET ols\_column = char\_to\_label ('ACCESS\_LOCATIONS', 'CONF:SM:UK,CA')  WHERE (country\_id = 'CA'  AND city = 'Toronto')  OR  (country\_id = 'UK'  AND city = 'Oxford'); |

A screenshot of a computer

Description automatically generated

|  |
| --- |
| UPDATE hr.locations  SET ols\_column = char\_to\_label ('ACCESS\_LOCATIONS', 'CONF:HR:UK')  WHERE country\_id = 'UK'  AND city = 'London'; |

A screenshot of a computer

Description automatically generated

|  |
| --- |
| UPDATE hr.locations  SET ols\_column = char\_to\_label ('ACCESS\_LOCATIONS', 'SENS:HR,SM,FIN:CORP')  WHERE country\_id = 'CH' AND city = 'Geneva'; |

A screenshot of a computer

Description automatically generated

- Tiếp theo ta cần gán lại chính sách với tùy chọn HIDE và READ\_CONTROL

|  |
| --- |
| BEGIN  sa\_policy\_admin.remove\_table\_policy (  policy\_name => 'ACCESS\_LOCATIONS',  schema\_name => 'HR',  table\_name => 'LOCATIONS'  );  sa\_policy\_admin.apply\_table\_policy (  policy\_name => 'ACCESS\_LOCATIONS',  schema\_name => 'HR',  table\_name => 'LOCATIONS',  table\_options => 'HIDE,READ\_CONTROL,WRITE\_CONTROL,CHECK\_CONTROL'  );  END; |

A white screen with a yellow line

Description automatically generated

- Bây giờ ta thử truy xuất bảng Locations

|  |
| --- |
| SELECT \*  FROM hr.locations; |

A screenshot of a computer

Description automatically generated

|  |
| --- |
| DESCRIBE hr.locations; |

A screenshot of a computer

Description automatically generated

- Kết quả của lệnh SELECT là “no rows selected”. Chỉ có lệnh DESCRIBE có trả về kết quả. Nguyên nhân là do bây giờ bảng này đã được bảo vệ, chỉ những người được cấp quyền OLS cụ thể mới có thể truy xuất. Ta log in lại bằng user SKING:

|  |
| --- |
| SELECT \*  FROM hr.locations  WHERE city = 'Bern'; |

A screenshot of a computer

Description automatically generated

|  |
| --- |
| SELECT label\_to\_char (ols\_column) as label, locations.\*  FROM hr.locations  WHERE city = 'Bern'; |

A screenshot of a computer

Description automatically generated

## 3.2. Dùng hàm gán nhãn

- Trong phần thực hành này, ta sẽ dùng bảng Employees của schema HR để minh họa.

- Cấp các quyền cần thiết cho sec\_admin trên bảng Employees:

|  |
| --- |
| GRANT select, insert, update ON hr.employees TO sking;  GRANT select, insert, update ON hr.employees TO sec\_admin;  GRANT create procedure TO sec\_admin; |

A screenshot of a computer

Description automatically generated

|  |
| --- |
| GRANT execute ON to\_lbac\_data\_label TO sec\_admin WITH GRANT OPTION; |

A screenshot of a computer

Description automatically generated

- Tiếp theo ta viết một hàm gán nhãn dựa trên điều kiện của thông tin nhân viên

|  |
| --- |
| CREATE OR REPLACE FUNCTION sec\_admin.gen\_emp\_label  (  Job VARCHAR2,  Sal NUMBER  )  RETURN LBACSYS.LBAC\_LABEL AS i\_label VARCHAR2(80);  BEGIN  /\*\*\*\*\*\*\*\*\*\*\*\*\* Xác định level \*\*\*\*\*\*\*\*\*\*\*\*\*/  IF Sal > 17000 THEN i\_label := 'SENS:';  ELSIF Sal > 10000 THEN i\_label := 'CONF:';  ELSE i\_label := 'PUB:';  END IF;  /\*\*\*\*\*\*\*\*\*\*\*\*\* Xác định compartment \*\*\*\*\*\*\*\*\*\*\*\*\*/  IF Job LIKE '%HR%' THEN i\_label := i\_label || 'HR:';  ELSIF Job LIKE '%MK%' OR Job LIKE '%SA%' THEN i\_label := i\_label || 'SM:';  ELSIF Job LIKE '%FI%' THEN i\_label := i\_label || 'FIN:';  ELSE i\_label := i\_label || ':';  END IF;  /\*\*\*\*\*\*\*\*\*\*\*\*\* Xác định groups \*\*\*\*\*\*\*\*\*\*\*\*\*/  i\_label := i\_label || 'CORP';  RETURN TO\_LBAC\_DATA\_LABEL('ACCESS\_LOCATIONS', i\_label);  END; |

A screenshot of a computer

Description automatically generated

- Ta cần gán cho LBACSYS quyền thực thi trên hàm gán nhãn vừa được tạo

|  |
| --- |
| GRANT execute ON sec\_admin.gen\_emp\_label TO lbacsys; |

A white rectangular object with a white border

Description automatically generated with medium confidence

|  |
| --- |
| BEGIN  SA\_POLICY\_ADMIN.APPLY\_TABLE\_POLICY (  policy\_name => 'ACCESS\_LOCATIONS',  schema\_name => 'HR',  table\_name => 'EMPLOYEES',  table\_options => 'READ\_CONTROL,WRITE\_CONTROL,CHECK\_CONTROL',  label\_function => 'sec\_admin.gen\_emp\_label (:new.job\_id, :new.salary)',  PREDICATE => NULL);  END; |

A screenshot of a computer

Description automatically generated

# IV. Các view thông tin của OLS

|  |
| --- |
| select \*  from DBA\_SA\_USERS; |

A screenshot of a computer

Description automatically generated

|  |
| --- |
| select \*  from DBA\_SA\_USER\_LEVELS; |

A screenshot of a computer

Description automatically generated

|  |
| --- |
| SELECT \*  FROM DBA\_SA\_USER\_COMPARTMENTS; |

A screenshot of a computer

Description automatically generated

|  |
| --- |
| SELECT \*  FROM DBA\_SA\_USER\_GROUPS; |

A screenshot of a computer

Description automatically generated

# V. Bài Tập

## 5.1. Tạo bảng CUSTOMERS

- Để áp dụng chính sách *region\_policy* (đã tạo trong phần bài tập của Lab 06). Sau đó insert dữ liệu vào.

|  |
| --- |
| CREATE TABLE CUSTOMERS (  id NUMBER(10) NOT NULL,  cust\_type VARCHAR2(10),  first\_name VARCHAR2(30),  last\_name VARCHAR2(30),  region VARCHAR2(5),  credit NUMBER(10,2),  CONSTRAINT customer\_pk PRIMARY KEY (id),  CONSTRAINT customer\_cust\_type\_ck CHECK (cust\_type IN ('silver', 'gold', 'platinum')),  CONSTRAINT customer\_region\_ck CHECK (region IN ('north', 'west', 'east', 'south'))  ); |

A screenshot of a computer

Description automatically generated

- Nạp dữ liệu vào

|  |
| --- |
| INSERT INTO CUSTOMERS (id, cust\_type, first\_name, last\_name, region, credit)  VALUES (1, 'silver', 'John', 'Doe', 'north', 3000);  INSERT INTO CUSTOMERS (id, cust\_type, first\_name, last\_name, region, credit)  VALUES (2, 'gold', 'Jane', 'Smith', 'west', 1500);  INSERT INTO CUSTOMERS (id, cust\_type, first\_name, last\_name, region, credit)  VALUES (3, 'platinum', 'Emily', 'Johnson', 'east', 400); |

A screenshot of a computer

Description automatically generated

## 5.2. Tạo chính sách *region\_policy* (có thể bỏ qua nếu đã thực hiện Lab 06)

- 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

## 5.3 Gán nhãn bảo mật cho các hàng trong bảng

- Sau khi tạo chính sách gán nhãn bảo mật (security labels) cho từng dòng dữ liệu trong bảng dựa trên vùng (region)

|  |
| --- |
| ALTER TABLE CUSTOMERS ADD region\_label VARCHAR2(100);  UPDATE CUSTOMERS  SET region\_label = 'SENS:SM:NORTH'  WHERE region = 'north';  UPDATE CUSTOMERS  SET region\_label = 'SENS:SM:WEST'  WHERE region = 'west';  UPDATE CUSTOMERS  SET region\_label = 'SENS:SM:EAST'  WHERE region = 'east'; |

A screenshot of a computer

Description automatically generated

## 5.4 Tạo user

|  |
| --- |
| CREATE USER sales\_north IDENTIFIED BY salesnorth;  CREATE USER sales\_west IDENTIFIED BY saleswest;  CREATE USER sales\_east IDENTIFIED BY saleseast;  CREATE USER sales\_south IDENTIFIED BY salessouth;  GRANT CONNECT TO sales\_north;  GRANT CONNECT TO sales\_west;  GRANT CONNECT TO sales\_east;  GRANT CONNECT TO sales\_south;  GRANT CREATE SESSION TO sales\_north;  GRANT CREATE SESSION TO sales\_west;  GRANT CREATE SESSION TO sales\_east;  GRANT CREATE SESSION TO sales\_south; |

A screenshot of a computer

Description automatically generated

## 5.5 Gán nhãn cho các user

### 5.5.1 Gán nhãn bảo mật cho user sales\_north

|  |
| --- |
| BEGIN  SA\_USER\_ADMIN.SET\_USER\_LABELS (  policy\_name => 'region\_policy',  user\_name => 'sales\_north',  max\_read\_label => 'L1:MN:RN',  max\_write\_label => 'L1:MN:RN',  min\_write\_label => 'L1',  def\_label => 'L1:MN:RN',  row\_label => 'L1:MN:RN'  );  END; |

A white rectangular object with yellow lines

Description automatically generated

### 5.5.2 Gán nhãn bảo mật cho user sales\_south

|  |
| --- |
| BEGIN  SA\_USER\_ADMIN.SET\_USER\_LABELS (  policy\_name => 'region\_policy',  user\_name => 'sales\_south',  max\_read\_label => 'L1:MN:RS',  max\_write\_label => 'L1:MN:RS',  min\_write\_label => 'L1',  def\_label => 'L1:MN:RS',  row\_label => 'L1:MN:RS'  );  END; |

A screenshot of a chat

Description automatically generated

### 5.5.3 Gán nhãn bảo mật cho user sales\_east

|  |
| --- |
| BEGIN  SA\_USER\_ADMIN.SET\_USER\_LABELS (  policy\_name => 'region\_policy',  user\_name => 'sales\_east',  max\_read\_label => 'L1:MN:RE',  max\_write\_label => 'L1:MN:RE',  min\_write\_label => 'L1',  def\_label => 'L1:MN:RE',  row\_label => 'L1:MN:RE'  );  END; |

A white rectangular object with yellow lines

Description automatically generated

### 5.5.4 Gán nhãn bảo mật cho user sales\_west'

|  |
| --- |
| BEGIN  SA\_USER\_ADMIN.SET\_USER\_LABELS (  policy\_name => 'region\_policy',  user\_name => 'sales\_west',  max\_read\_label => 'L1:MN:RW',  max\_write\_label => 'L1:MN:RW',  min\_write\_label => 'L1',  def\_label => 'L1:MN:RW',  row\_label => 'L1:MN:RW'  );  END; |

A white rectangular object with a yellow line

Description automatically generated