**Bài thực hành số 11**

**ORACLE LABEL SECURITY (4)**

* ***Tóm tắt nội dung:***
* Che dấu cột thông tin chính sách
* Sử dụng hàm gán nhãn
* Các view của OLS

# Một số kỹ thuật nâng cao trong OLS

## Lý thuyết

### Che dấu cột thông tin nhãn dữ liệu

* Để tránh việc hiển thị cột chứa thông tin chính sách, người quản trị có thể thiết lập tùy chọn HIDE khi gán chính sách cho bảng.
* Một khi chính sách đã được áp dụng, trạng thái Ẩn/Không Ẩn của cột không thể được thay đổi trừ khi ta remove chính sách khỏi bảng với tham số DROP\_COLUMN bằng TRUE. Sau đó chính sách có thể được áp dụng lại với trạng thái mới.
* Khi người dùng INSERT dữ liệu vào bảng có trạng thái ẩn cột chính sách, giá trị của cột chứa nhãn sẽ không bị yêu cầu phải insert.
* Câu lệnh SELECT \* sẽ không tự động trả về giá trị của cột ẩn, trừ khi nó được truy xuất trực tiếp.
* Câu lệnh DESCRIBE cũng sẽ không hiển thị thông tin cột ẩn.

### Hàm gán nhãn

* Có những bảng dữ liệu lớn, ta không thể ngồi gán nhãn cho từng trường hợp. OLS cung cấp cho ta một cách gán nhãn khác. Đó là sử dụng một hàm (function) do mình hiện thực để OLS sẽ tự động gán nhãn mỗi khi có hàng mới được insert vào bảng dữ liệu được bảo vệ. Xem phần thực hành để hiểu rõ hơn về cách thức làm việc này.
* Hàm gán nhãn sẽ override 2 tùy chọn LABEL\_DEFAULT và LABEL\_UPDATE.

## Thực hành

### 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 bải lab này ta phải remove chính sách (xóa luôn cột thông tin), thực hiện lại đoạn code gán nhãn trong bài lab trước và gán lại chính sách.

CONN sec\_admin/secadmin;

BEGIN

sa\_policy\_admin.remove\_table\_policy

(policy\_name => 'ACCESS\_LOCATIONS',

schema\_name => 'HR',

table\_name => 'LOCATIONS',

drop\_column => true);

END;

/

SELECT \* FROM hr.locations;

* Ta nhận thấy lúc này cột OLS\_COLUMN vẫn chưa bị xóa dù Oracle báo thực hiện thành công thủ tục. Lý do là khi remove chính sách, ta sẽ xóa cột OLS\_COLUMN, tức là đã thay đổi bảng Locations. Do vậy ta cần cấp thêm quyền ALTER trên bảng Locations cho sec\_admin để cột OLS\_COLUMN thật sự bị xóa. Bây giờ ta gán lại chính sách trên để thấy sự thay đổi sau khi sec\_admin được gán quyền.

CONN sec\_admin/secadmin;

BEGIN

sa\_policy\_admin.apply\_table\_policy

(policy\_name => 'ACCESS\_LOCATIONS',

schema\_name => 'HR',

table\_name => 'LOCATIONS',

table\_options => 'NO\_CONTROL');

END;

/

CONN system/system;

GRANT alter ON hr.locations TO sec\_admin;

CONN sec\_admin/secadmin;

BEGIN

sa\_policy\_admin.remove\_table\_policy

(policy\_name => 'ACCESS\_LOCATIONS',

schema\_name => 'HR',

table\_name => 'LOCATIONS',

drop\_column => true);

END;

/

SELECT \* FROM hr.locations;

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

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

CONN sec\_admin/secadmin;

BEGIN

sa\_policy\_admin.apply\_table\_policy

(policy\_name => 'ACCESS\_LOCATIONS',

schema\_name => 'HR',

table\_name => 'LOCATIONS',

table\_options => 'HIDE,NO\_CONTROL');

END;

/

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

CONN sec\_admin/secadmin;

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

UPDATE hr.locations SET ols\_column = char\_to\_label ('ACCESS\_LOCATIONS', 'CONF::US')

WHERE country\_id = 'US';

UPDATE hr.locations SET ols\_column = char\_to\_label ('ACCESS\_LOCATIONS', 'CONF::UK')

WHERE country\_id = 'UK';

UPDATE hr.locations SET ols\_column = char\_to\_label ('ACCESS\_LOCATIONS', 'CONF::CA')

WHERE country\_id = 'CA';

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');

UPDATE hr.locations SET ols\_column = char\_to\_label ('ACCESS\_LOCATIONS', 'CONF:HR:UK')

WHERE country\_id = 'UK' and city = 'London';

UPDATE hr.locations SET ols\_column = char\_to\_label ('ACCESS\_LOCATIONS', 'SENS:HR,SM,FIN:CORP')

WHERE country\_id = 'CH' and city = 'Geneva';

COMMIT ;

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

CONN sec\_admin/secadmin;

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;

/

* Bây giờ ta thử truy xuất bảng Locations:

CONN sec\_admin/secadmin;

SELECT \* FROM hr.locations;

DESCRIBE hr.locations;

* Kết quả của dòng code SELECT là “no rows selected”. Chỉ có câu 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:

CONN sking/sking;

SELECT \* FROM hr.locations;

SELECT label\_to\_char (ols\_column) as label, locations.\*

FROM hr.locations;

* Ta thấy trong câu lệnh SELECT thứ 2, ta có chỉ định rõ cột ols\_column nên cột này mới xuất hiện. Trong kết quả truy vấn của câu SELECT thứ nhất không có cột thông tin chính sách này.

### Dùng hàm gán nhãn

* Trong phần thực hành này, ta sẽ dùng bảng Employees của schem HR để minh họa.
* Cấp các quyền cần thiết cho sec\_admin trên bảng Employees:

CONN system/system;

GRANT select, insert, update, alter

ON hr.employees TO sec\_admin;

GRANT create procedure TO sec\_admin;

CONN lbacsys/lbacsys

GRANT execute ON to\_lbac\_data\_label

TO sec\_admin WITH GRANT OPTION;

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

CONN sec\_admin/secadmin;

CREATE OR REPLACE FUNCTION sec\_admin.gen\_emp\_label

(Job varchar2, Depto number, 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;

/

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

CONN sec\_admin/secadmin;

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

* Ta chỉ định thủ tục vừa hiện thực làm hàm gán nhãn cho bảng Employees:

CONN sec\_admin/secadmin;

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.department\_id,:new.salary)');

END;

/

# Các view thông tin của OLS

* Các thông tin về các chính sách của OLS được lưu trong data dictionary. Ta có thể xem các thông tin này thông qua các view của OLS.
* View DBA\_SA\_USERS: hiển thị thông tin về tất cả các chính sách có trong CSDL.
* DBA\_SA\_USER\_LEVELS: hiển thị thông tin level của mọi người dùng.
* DBA\_SA\_USER\_COMPARTMENTS: hiển thị thông tin compartment của mọi người dùng.
* DBA\_SA\_USER\_GROUPS: hiển thị thông tin group của mọi người dùng.
* Để xem tất cả các view trên cần log in vào tài khoản LBACSYS hoặc được cấp quyền SELECT từ LBACSYS.

conn lbacsys/lbacsys;

select \* from DBA\_SA\_USERS;

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

select \* from DBA\_SA\_USER\_COMPARTMENTS;

select \* from DBA\_SA\_USER\_GROUPS;

# Bài tập

1. Viết hàm gán nhãn GET\_CUSTOMER\_LABEL cho các khách hàng trong bảng CUSTOMERS đã tạo ở bài lab 9 theo điều kiện sau:

* Credit > 2000: level 3; 500 < credit <= 2000: level 2; còn lại level 1
* Cust\_type = ‘Platinum’ thì compartment là Manager, còn lại là Employee
* Group gán theo region.

1. Thực hiện các câu lệnh cần thiết để bảng trên được gán nhãn và được áp dụng chính sách REGION\_POLICY đã tạo trong bài lab 8.
2. Thực hiện một số câu lệnh để kiểm tra tác dụng của chính sách.