**Bài thực hành số 9**

**ORACLE LABEL SECURITY (2)**

* ***Tóm tắt nội dung:***
* Các thành phần của nhãn trong Oracle Label Security
* Nhãn dữ liệu (data label)

# Các thành phần của nhãn dữ liệu

## Lý thuyết

### 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).

### Các thành phần của nhãn

#### 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 giả 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.

#### 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 giả 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 compartmet. Khi cần tham khảo đến compartment ta sử dụng tên rút gọn này.

#### 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 giả 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.

## Thực hành

### Tạo level

* Ở phần này ta sẽ tạo các thành phần level cho chính sách ACCESS\_LOCATIONS mà ta đã tạo trong bài lab “*Oracle Label Security (1)*”.
* 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 procedure 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 procedure. Người đọc cũng cần chú ý cách chọn số cho các level.

* Để thay đổi 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;

/

### 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 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;

/

### 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 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;

/

# Chi tiết về nhãn dữ liệu

## Lý thuyết

### 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 : COMPARTMENT1, ..., COMPARTMENTn : GROUP1, ..., GROUPn***

* 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.

### 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” (H) 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 |

## Thực hành

* Các bước ta vừa làm ở phần I tương ứng với bước 2 trong quy trình hiện thực OLS. Ở phần này ta sẽ thực hiện bước 3: tạo các nhãn thật sự cần dùng từ các thành phần trên.
* 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;

/

# Bài tập

1. Tạo các thành phần nhãn cho chính sách region\_policy (trong bài tập của Lab 8):
* Level: level 1, level 2, level 3
* Compartment: MANAGEMENT, EMPLOYEE
* Group: REGION NORTH, REGION SOUTH, REGION EAST, REGION WEST
1. Tạo bảng CUSTOMERS để áp dụng chính sách trên. Sau đó insert dữ liệu vào.

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));

Vùng giá trị của một số cột:

* cust\_type : silver, gold, platinum
* region: north, west, east, south
* credit: học viên cần nhập dữ liệu đủ cho 3 trường hợp tương ứng với 3 khoảng giá trị >2000, từ 500 đến 2000, < 500.

Bảng dữ liệu này sẽ được sử dụng cho bài lab 10.