TRƯỜNG ĐẠI HỌC TRẦN ĐẠI NGHĨA

KHOA CÔNG NGHỆ THÔNG TIN

BÁO CÁO

BÀI TẬP LỚN MÔN HỌC

AN TOÀN BẢO MẬT HỆ THỐNG THÔNG TIN

Đề tài: "Xây dựng mô phỏng tính No Write UP trong Oracle"

TP. HỒ CHÍ MINH, THÁNG 10 NĂM 2019

TRƯỜNG ĐẠI HỌC TRẦN ĐẠI NGHĨA

KHOA CÔNG NGHỆ THÔNG TIN

BÁO CÁO

BÀI TẬP LỚN MÔN HỌC

AN TOÀN BẢO MẬT HỆ THỐNG THÔNG TIN

Đề tài: "Xây dựng mô phỏng tính No Write UP trong Oracle"

GVHD: Đặng Thế Hùng

Sinh viên thực hiện:

Nguyễn Lê Xuân Phước

Tôn Nữ Nguyên Hậu

Đỗ Tống Quốc

Lớp: 16DDS06031

TP. HỒ CHÍ MINH, THÁNG 10 NĂM 2019

Mục Lục

LỜI MỞ ĐẦU

Trong một xã hội hiện đại, cơ sở dữ liệu đóng một vai trò hết sức quan trọng và tham gia vào hầu hết các lĩnh vực hoạt động. Sự ngưng trệ hay hoạt động thiếu chính xác của nó có thể gây ra các hậu quả khó lường.

Đặc biệt, khi xã hội chuyển sang giai đoạn xã hội hoá thông tin và nền kinh tế chuyển sang nền kinh tế số hoá với mức độ liên kết chặt chẽ, với quy mô toàn cầu thì vai trò của cơ sở dữ liệu (CSDL) càng trở nên quan trọng. Do vậy, các vấn đề tin cậy, an toàn và bí mật thông tin trong các cơ sở dữ liệu cần được đầu tư nghiên cứu dưới cả góc độ lý thuyết và triển khai thực tiễn. Để đảm bảo an toàn cho một hệ thống thì kiểm soát truy nhập là một trong những biện pháp đầu tiên và quan trọng nhất. Nhờ khả năng kiểm soát truy nhập, chúng ta có thể cho phép hoặc từ chối một chủ thể (một người dùng hay một tiến trình nào đó) truy nhập vào một đối tượng trong hệ thống. Trong an toàn cơ sở dữ liệu, ta hoàn toàn có thể gắn kiểm soát truy nhập cho cơ sở dữ liệu của mình bằng các chính sách kiểm soát truy nhập, cụ thể là chính sách kiểm soát truy nhập bắt buộc (MAC) và chính sách kiểm soát truy nhập tùy ý (DAC).

Có thể nói sự thực thi của MAC trong các hệ quản trị là dựa và các nhãn - label, dùng để gán cho các chủ thể và đối tượng của hệ thống. Do đó, trong Oracle gọi MAC là an toàn dựa vào nhãn - OLS (Oracle Label Security). Với mục đích nghiên cứu và tìm hiểu thành phần và các chính sách áp dụng trong OLS, nhóm chúng em đã chọn đề tài " Xây dựng mô phỏng tính No Write Up trong Oracle" để phân tích Oracle đảm bảo tính toàn vẹn-Integrity trong bằng Oracle Label Security.

Do kinh nghiệm và kiến thức chưa được sâu sắc nên trong báo cáo về đề tài của nhóm mong thầy góp ý thêm để nhóm có thể hoàn thiện tốt hơn các đề tài nghiên cứu về sau !

CHƯƠNG I. GIỚI THIỆU ORACLE LABEL SECURITY

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. DAC và MAC trong Oracle

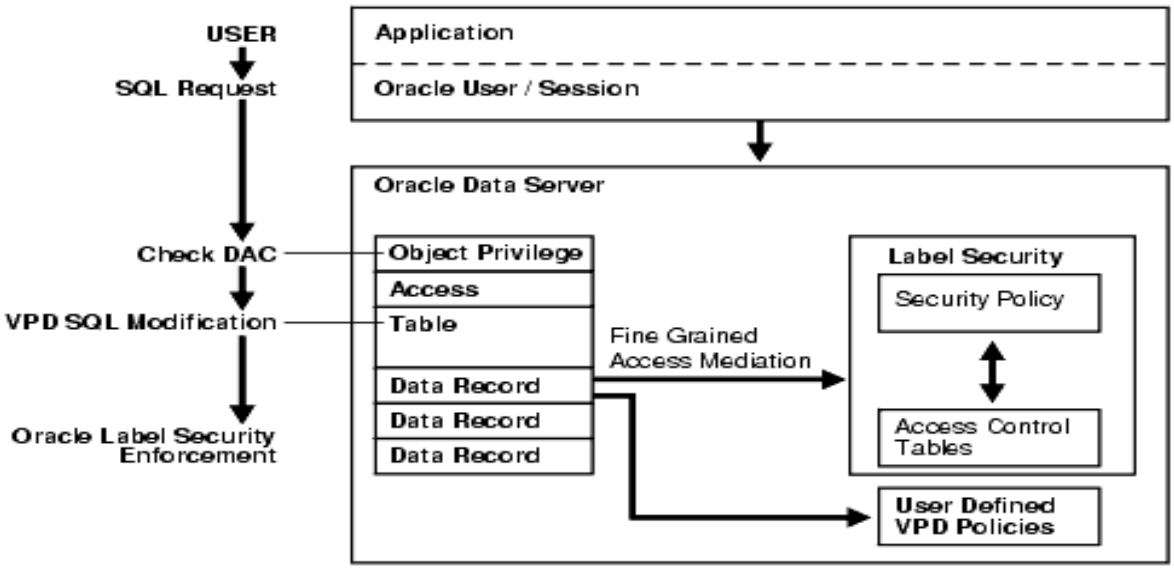
❖ DAC: Trong Oracle Database, các nhà quản trị có thể áp dụng mô hình DAC thông qua việc quản lý các truy xuất theo quyền đối tượng và quyền hệ thống

❖ 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).



Hình 1.1: Kiến trúc của Oracle Label Security

3. 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 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). 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 thực hiện

Quy trình cơ bản để hiện thực một chính sách OLS gồm 5 bước như sau:

Bước 1: Tạo chính sách OLS.

Bước 2: Định nghĩa các thành phần mà một nhãn thuộc chính sách trên có thể có.

Bước 3: Tạo các nhãn dữ liệu thật sự mà bạn muốn dùng.

Bước 4: Gán chính sách trên cho các bảng hoặc schema mà bạn muốn bảo vệ.

Bước 5: Gán các giới hạn quyền, các nhãn người dùng hoặc các quyền truy xuất đặc biệt cho những người dùng liên quan.

5. Các ứng dụng của Oracle Label Security

OLS được ứng dụng để bảo mật an toàn cho cơ sở dữ liệu, chúng được ứng dụng cho các lĩnh vực có tính bảo mật cao như quân sự, quốc phòng, ngân hàng, các công ty, tổ chức ….

CHƯƠNG II. CÁC THÀNH PHẦN NHÃN TRONG ORACLE LABEL SECURITY

1. Nhãn Dữ liệu (data label)

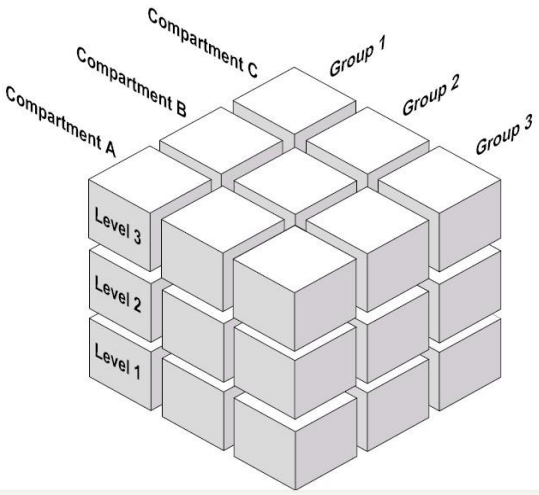
1.1. Cú pháp nhãn dữ liệu

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).

Hình 2.1: Quan hệ của các thành phần trong một 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

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,…

1.2. Các thành phần của nhãn dữ liệu

1.2.1. 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.

1.2.2. 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.

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.

1.2.3. 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

Hình 2.3: Ví dụ Group

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.

2. Các loại nhãn người dùng

2.1. Nhãn người dùng

Tại mỗi thời điểm, mỗi người dùng đều có một nhãn gọi là nhãn người dùng (user label). Nhãn này có tác dụng cho biết mức độ tin cậy của người dùng đối với những dữ liệu được chính sách đó bảo vệ. Nhãn người dùng cũng gồm các thành phần giống như nhãn dữ liệu. Khi một người dùng truy xuất trên bảng được bảo vệ, nhãn người dùng sẽ được so sánh với nhãn dữ liệu của mỗi dòng trong bảng để quyết định những dòng nào người dùng đó có thể truy xuất được.

OLS cung cấp cho chúng ta 2 cách thức để quản lý các **user label**: gán cụ thể từng thành phần của nhãn cho user hoặc gán nguyên nhãn cho user. Trong các phần sau sẽ trình bày kỹ hơn về 2 cách quản lý này.

Dù sử dụng hình thức quản lý nào, mỗi người dùng cũng có một **tập xác thực quyền (set of authorizations)** để lưu giữ thông tin về quyền hạn truy xuất đối với những dữ liệu được chính sách đó bảo vệ. Tập xác thực quyền gồm có:

- ✓ ***Level cao nhất (User Max Level)*** của người dùng trong các tác vụ read và write.
- ✓ ***Level thấp nhất (User Min Level)*** của người dùng trong các tác vụ write. User Min Level phải thấp hơn hoặc bằng User Max Level.
- ✓ ***Tập các compartment được truy xuất***.
- ✓ ***Tập các group được truy xuất.*** (Đối với mỗi compartment và group có lưu kèm thông tin quyền truy xuất được phép là quyền **"chỉ đọc" (read-only)** hay quyền **"đọc-viết" (read-write))**

Với tập xác thực quyền, ta có thể hình thành nên nhiều tổ hợp các thành phần của nhãn. Do vậy mỗi người dùng có thể có nhiều user label khác nhau nhưng vẫn nằm trong giới hạn của tập xác thực quyền.

Session label:

- ✓ Session label là một user label mà người dùng sử dụng để truy xuất dữ liệu trong một session làm việc. Session label có thể là một tổ hợp bất kỳ các thành phần nằm trong giới hạn tập xác thực quyền của user đó.
- ✓ Người quản trị có thể mô tả session label mặc định cho người dùng khi thiết lập tập xác thực quyền cho người dùng đó.

- ✓ Bản thân người dùng có thể thay đổi session label của mình thành một nhãn bất kỳ với điều kiện là nhãn mới nằm trong giới hạn xác thực quyền của họ.

Row label:

- ✓ Khi một hàng mới được insert vào một bảng đang được bảo vệ, cần có một nhãn dữ liệu (data label) được chỉ định cho hàng dữ liệu mới đó. Hoặc khi một hàng được update, nhãn dữ liệu của hàng đó cũng có thể bị thay đổi.
- ✓ Những nhãn dữ liệu trong các trường hợp vừa nói ở trên có thể được gán cho dòng dữ liệu tương ứng theo một trong những cách sau:
  - Người update/insert hàng dữ liệu chỉ định một cách tường mình ngay khi thực hiện tác vụ update/insert đó
  - Hàm gán nhãn (labeling function) của bảng đó tự sinh nhãn theo những điều kiện được hiện thực trong function tương ứng.
  - Bằng giá trị mặc định do người quản trị quy định khi gán quyền hạn truy xuất cho người dùng đó.
  - Bằng giá trị của session label của người dùng đó.
- ✓ Tùy ngữ cảnh và trường hợp mà giá trị nhãn mới thêm vào sẽ rơi vào trường hợp nào trong các trường hợp kể trên.
- ✓ **Row label** là từ dùng để chỉ những nhãn được áp dụng cho các hàng dữ liệu khi insert/update
- ✓ Khi insert/update, người dùng có thể mô tả tường minh row label cho dòng dữ liệu mới được insert/update, với điều kiện row label phải thỏa đồng thời các điều kiện sau:
  - Level thấp hơn hoặc bằng max level của người dùng đó.
  - Level cao hơn hoặc bằng min level của người dùng đó.
  - Chỉ được chứa các compartment xuất hiện trong session label hiện tại của người dùng đó và người dùng có quyền viết (write) trên các compartment đó.
  - Chỉ được chứa các group xuất hiện trong session label hiện tại của người dùng đó và người dùng có quyền viết (write) trên các group đó

2.2. Quản lý người dùng theo từng loại thành phần của nhãn

Để gán quyền theo cách này ta cần chỉ định ra cụ thể các level, compartment, group mà một user có thể truy xuất

Chúng ta cần nắm vững quy tắc quản lý truy xuất của OLS "***no read up - no write up - limited write down***".

Quản lý các level: gồm có 4 thông số:

- ✓ ***max_level:*** level cao nhất mà người dùng có quyền đọc và viết. Vì quy tắc quản lý đòi hỏi "*no read up – no write up*" (không được đọc và viết lên những dữ liệu có độ bảo mật cao hơn độ tin cậy của user) nên max level chính là "*giới hạn trên*" cho việc truy xuất (đọc và viết) của người dùng.
- ✓ ***min_level:*** level thấp nhất mà người dùng có quyền write. Vì quy tắc quản lý yêu cầu "*limited write down*" (chỉ viết lên những dữ liệu có độ bảo mật thấp hơn độ tin cậy của người dùng ở một mức giới hạn nào đó) nên min level chính là "*giới hạn dưới*" cho tác vụ viết của người dùng. "*Giới hạn dưới*" cho tác vụ đọc chính là level thấp nhất mà chính sách đó quy định.
- ✓ ***def_level***: level cho session label mặc định của người dùng (phải thỏa *min level <= default level <= max level*). Nếu người quản trị bảo mật không mô tả thông số này thì *default level* sẽ là *max level*.
- ✓ ***row_level***: level cho *row label* mặc định của người dùng, dùng để gán nhãn cho dữ liệu mà user đó tạo khi truy xuất bảng được bảo vệ bởi chính sách (phải thỏa mãnmin *level <= row level <= max level*). Nếu người quản trị bảo mật không mô tả thông số này thì default row level sẽ là default level.

Quản lý các compartment: Gồm có 4 thông số chính:

- ✓ ***read_comps***: danh sách các compartment mà người dùng được quyền đọc.
- ✓ ***write_comps:*** danh sách các compartment mà người dùng được quyền viết (danh sách này phải là tập con của danh sách *read_comps*).
- ✓ ***def_comps***: danh sách các compartment cho *session label* mặc định của người dùng đó (danh sách này phải là tập con của danh sách *read_comps*).
- ✓ ***row_comps:*** danh sách các compartment cho *row label* mặc định của người dùng, dùng để gán nhãn cho dữ liệu mà người dùng đó tạo khi truy xuất bảng được bảo vệ bởi chính sách (danh sách này phải là tập con của danh sách *read_comps* và *write_comps*).

Quản lý các group: Gồm có 4 thông số chính:

- ✓ ***read_groups:*** danh sách các groups mà người dùng được quyền đọc.
- ✓ ***write_ groups***: danh sách các groups mà người dùng được quyền viết (danh sách này phải là tập con của danh sách *read_ groups*).
- ✓ ***def_ groups:*** danh sách các groups cho *session label* mặc định của người dùng đó (danh sách này phải là tập con của danh sách *read_ groups*).
- ✓ ***row_ groups:*** danh sách các groups cho *row label* mặc định của người dùng đó, dùng để gán nhãn cho dữ liệu mà người dùng đó tạo ra khi truy

xuất bảng được bảo vệ bởi chính sách (danh sách này phải là tập con của danh sách *read_ groups* và *write_ groups*).

Lưu ý: nếu người dùng có quyền đọc trên một group thì đồng thời cũng có quyền đọc trên tất cả các group con (trực tiếp và gián tiếp) của group đó. Tương tự đối với quyền viết cũng vậy. Hình bên dưới minh họa cho việc thừa kế quyền đọc và viết trên các group. Trong hình, người dùng có quyền đọc trên group WESTERN_REGION nên cũng có quyền đọc trên tất cả các group con còn lại. Bên cạnh đó, người dùng chỉ được cấp quyền viết trên group WR_FINANCE nên chỉ có quyền viết trên group này và 2 group con của nó chứ không có quyền viết trên các group WR_SALES, WR_HUMAN_RESOURCES, WESTERN_REGION.

2.3. Quản lý người dùng thông qua các nhãn

Để tiện lợi hơn, OLS cũng cho phép người quản trị thiết lập tập xác thực quyền cho người dùng thông qua việc gán các nhãn thay vì phải chỉ định từng thành phần riêng. Các loại nhãn cần mô tả:

- ***max_read_label***: nhãn thể hiện mức truy xuất cao nhất đối với tác vụ đọc. Nó bao gồm level cao nhất (*max_level*) cho tác vụ đọc, tất cả các compartment và group mà người dùng được phép đọc (*read_comps* và *read_groups*). Đây là nhãn mà người quản trị bắt buộc phải gán cho người dùng nếu chọn cách quản lý quyền truy xuất của người dùng thông qua nhãn.
- ***max_write_label:*** nhãn thể hiện mức truy xuất cao nhất đối với quyền viết. Nó bao gồm level cao nhất (*max_level*) cho tác vụ viết, tất cả các compartment và group mà người dùng được phép viết (*write_comps* và *write_groups*). Nếungười quản trị không thiết lập giá trị cho loại nhãn này, nó sẽ lấy giá trị bằng giá trị của *max_read_label*.
- ***min_write_label:*** nhãn thể hiện mức truy xuất thấp nhất đối với tác vụ viết. Nhãn này chỉ chứa level thấp nhất (*min_level*) của người dùng đó, không chứa bất kỳ compartment và group nào.
- ***def_read_label:*** là *session label* mặc định cho các tác vụ đọc của người dùng. Nó là tập con của max_read_label. Nếu người quản trị không thiết lập giá trị cho loại nhãn này, nó sẽ lấy giá trị bằng giá trị của *max_read_label*.
- ***def_write_label***: là session label mặc định cho tác vụ write của người dùng. Nó là tập con của *def_read_label* (có level bằng level của *def_read_label*; chứa tất cả các compartment và group mà người dùng có quyền viết trong *def_read_label*). Giá trị của nhãn này sẽ được tính một cách tự động bởi OLS từ giá trị của *def_read_label*. Nói cách khác, người quản trị sẽ không mô tả giá trị cho nhãn này.
- ***row_label:*** nhãn mặc định dùng để gán nhãn cho các dòng dữ liệu mà user tạo ra trong bảng được chính sách bảo vệ. Nhãn này là tập con của *max_write_label* và *def_read_label*. Nếu người quản trị không thiết lập giá trị cho loại nhãn này, nó sẽ lấy giá trị bằng giá trị của *def_write_label*.

CHƯƠNG III. CHÍNH SÁCH TRONG ORACLE LABEL SECURITY

1. Chính sách trong Oracle Label Security

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 svới 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.

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.

2. Các quyền đặc biệt trong OLS

Vì một số lý do đặc biệt, một người dùng có thể được cấp những quyền đặc biệt trong OLS để thực hiện một số tác vụ chuyên biệt hoặc truy xuất đến dữ liệu nằm ngoài giới hạn truy xuất được quy định trong tập xác thực quyền của người dùng đó.

Các quyền đặc biệt được OLS định nghĩa gồm có 2 nhóm: quyền truy xuất đặc biệt **(Special Access Privilege),** quyền đặc biệt trên *row label* **(Special Row Label Privilege).**

Quyền truy xuất đặc biệt:

- ✓ **READ**: cho phép người dùng có quyền xem (SELECT) tất cả các dữ liệu do chính sách này bảo vệ, ngay cả khi người này không được gán bất cứ tập xác thực quyền nào.
- ✓ **FULL:** cho phép người dùng có quyền viết và xem tất cả các dữ liệu do chính sách này bảo vệ.
- ✓ **COMPACCESS:** quyền COMPACCESS cho phép người dùng truy xuất dữ liệu dựa trên các compartment của nhãn dữ liệu, không quan tâm đến các group mà nhãn dữ liệu đó đang chứa. Nếu nhãn dữ liệu đó không chứa compartment, việc truy xuất được xác định dựa trên các group như bình thường. Nếu dữ liệu đó có chứa các compartment và người dùng có quyền truy xuất (đọc/viết) đến chúng thì việc xác thực các group sẽ được bỏ qua. Hai hình bên dưới lần lượt minh họa cho quy trình xác thực tác vụ đọc và tác vụ viết đối với người dùng có quyền COMPACCESS.
- ✓ **PROFILE_ACCESS**: cho phép thay đổi các session label của bản thân người dùng đó và session privilege của người dùng khác. Đây là một quyền rất "mạnh", vì người có quyền này có thể ngầm trở thành người có quyền FULL.

Quyền đặc biệt trên row label:

- ✓ **WRITEUP**: cho phép người dùng nâng level của một hàng dữ liệu nhưng không làm thay đổi các compartment và group của nó. Người dùng chỉ được nâng tối đa đến max_level của chính họ.
- ✓ **WRITEDOWN**: cho phép người dùng hạ level của một hàng dữ liệu nhưng không làm thay đổi các compartment và group của nó. Người dùng chỉ được phép hạ tối đa xuống đến *min_level* của họ, không được hạ thấp hơn mức này.
- ✓ **WRITEACROSS**: cho phép người dùng thay đổi compartment và group của một hàng dữ liệu nhưng không thay đổi *level* của nó. Người dùng có thể thay đổi các compartment và group đó thành bất cứ compartment và group nào có định nghĩa trong chính sách.

3. Áp dụng chính sách OLS

3.1. Đối tượng được bảo vệ

OLS cho phép ta gán các chính sách cho các đối tượng cần được bảo vệ theo cấp độ: cấp schema và cấp bảng. Khi 1 bảng cần được bảo vệ bởi 1 chính sách nào đó, ta gán chính sách đó cho cụ thể bảng đó. Nếu muốn tất cả các bảng thuộc 1 schema đều được bảo vệ bởi 1 chính sách, ta gán chính sách đó cho schema đó.

Lưu ý: Nếu 1 chính sách được gán cho 1 schema và đồng thời cũng được gán tường minh cho 1 bảng thuộc schema đó thì các tùy chọn, thao tác ở cấp độ bảng sẽ override các tùy chọn, thao tác ở cấp độ schema

3.2. Các thao tác quản trị việc gán chính sách cho table/schema

Áp dụng chính sách (Apply): ta gán chính sách cho cụ thể một bảng/schema cần được bảo vệ. Loại bỏ chính sách (Remove): loại bỏ sự bảo vệ của 1 chính sách khỏi bảng/schema. Lưu ý là khi loại bỏ như vậy, cột chứa nhãn của chính sách đó vẫn còn trong table, trừ khi ta xóa cột đó một cách tường minh. Ta có thể Enable/Disable một chính sách đang được gán cho 1 schema/bảng nào đó trong một khoảng thời gian.

Để thay đổi những thiết lập tùy chọn của một chính sách đối với 1 bảng thì trước hết ta phải remove chính sách đó ra rồi sau đó apply trở lại với những thay đổi trong tùy chọn.

3.3. Các tùy chọn cho việc áp dụng chính sách

Các tùy chọn này cho phép ta quy định một số ràng buộc trong việc áp dụng các chính sách:

- ✓ **LABEL_DEFAULT**: Sử dụng row label mặc định của người dùng hiện tại để làm nhãn cho hàng dữ liệu mới được insert vào trừ khi row label được chỉ định tường minh bởi người insert hoặc hàm gán nhãn.
- ✓ **LABEL_UPDATE**: bình thường, một người dùng khi update dữ liệu có thể thay đổi nhãn dữ liệu kèm theo. Tuy nhiên, nếu tham số này được bật lên, một người muốn thay đổi nhãn dữ liệu thì người đó phải có ít nhất một trong các quyền sau: WRITEUP, WRITEDOWN, hoặc WRITEACROSS.
- ✓ **CHECK_CONTROL**: nếu tùy chọn này được thiết lập, mỗi khi dữ liệu được update/insert và nhãn dữ liệu bị thay đổi/tạo mới, OLS sẽ kiểm tra xem nhãn dữ liệu mới có vượt quá giới hạn quyền của người update/insert hay không để tránh xảy ra tình trạng một người sau khi update/insert dữ liệu thì không thể truy xuất lại dữ liệu đó.
- ✓ **READ_CONTROL**: Chỉ những hàng có xác nhận quyền mới có thể được truy xuất bởi các thao tác SELECT, UPDATE và DELETE.
- ✓ **WRITE_CONTROL**: xác định khả năng INSERT, UPDATE và DELETE dữ liệu tại 1 hàng. Nếu tùy chọn này được kích hoạt, người dùng phải được xác thực quyền đầy đủ trước khi thực hiện các lệnh INSERT, UPDATE, DELETE.
- ✓ **INSERT_CONTROL**: có tác dụng giống tùy chọn WRITE_CONTROL nhưng chỉ đối với loại câu lệnh INSERT.
- ✓ **DELETE_CONTROL**: có tác dụng giống tùy chọn WRITE_CONTROL nhưng chỉ đối với loại câu lệnh DELETE.
- ✓ **UPDATE_CONTROL**: có tác dụng giống tùy chọn WRITE_CONTROL nhưng chỉ đối với loại câu lệnh UPDATE.
- ✓ **ALL_CONTROL**: áp dụng mọi ràng buộc tùy chọn.
- ✓ **NO_CONTROL**: không áp dụng bất cứ ràng buộc nào của chính sách.

3.4. Gán nhãn cho dữ liệu

Có 3 cách để một hàng dữ liệu được gán nhãn chính sách:

- ✓ Gán tường minh nhãn cho từng dòng dữ liệu thông qua các lệnh INSERT (cho dữ liệu mới) và UPDATE (cho dữ liệu đang tồn tại).
- ✓ Thiết lập tùy chọn LABEL_DEFAULT.
- ✓ Viết một function dùng cho việc gán nhãn cho các hàng dữ liệu của 1 bảng tùy theo nội dung của dữ liệu. Function này sẽ tự động được gọi cho mọi lệnh INSERT và UPDATE và nó độc lập với việc xác nhận quyền của mọi user.

CHƯƠNG IV. THỰC HÀNH ÁP DỤNG ORACLE LABEL SECURITY

1. Đặt vấn đề

Ta có một bảng CSDL lưu thông tin về các sinh viên của một đại đội quản lý sinh viên như sau:

SINH VIÊN						
ID	**HOTEN**	**GIOITINH**	**QUEQUAN**	**CHUCVU**	**LOP**	**COSO**
1	Trinh Hoang Son	Nam	Ninh Binh	Lop Truong	AT11D	Mien Bac
2	Do Tong Quoc	Nam	Binh Dinh	Sinh Vien	AT11D	Mien Bac
3	Ton Nu Nguyen Hau	Nu	Phu Yen	Sinh Vien	AT11E	Mien Nam
4	Nguyen Thi Hang	Nu	Binh Dinh	Lop Truong	AT11E	Mien Nam
5	Nguyen Le Xuan Phuoc	Nam	Tay Ninh	Quan Ly		Bac Nam
6	Nguyen Hung	Nam	Binh Duong	Sinh Vien	AT11E	Mien Nam
7	Truong The Luc	Nam	Ho Chi Minh	Sinh Vien	AT11E	Mien Nam
8	Ho Anh Dung	Nam	Thanh Hoa	Sinh Vien	AT11D	Mien Bac
9	Tong Thanh Anh	Nam	Quang Binh	Sinh Vien	AT11D	Mien Bac
10	Phan Thi Thao	Nu	Ha Noi	Quan Ly		Bac Nam

- Các User thực hiện

User	
QLBN	Quản lý
LT11DMB	Lớp trưởng D
LT11EMN	Lớp trưởng E
SV11DMB	Sinh Vien D
SV11EMN	Sinh Vien E

- Mức độ bảo mật (độ nhạy cảm-Level)

Level			
TOP_SECRET	SECRET	CONFIDENTAL	UNCLASSIFIED
TS	S	C	UC
100	75	50	25

- Compartment

Compartment		
Dạng số	**Dạng chuỗi dài**	**Dạng chuỗi ngắn**
65	AT11D	D
55	AT11E	E

- Group

Group		
Dạng số	**Dạng chuỗi dài**	**Dạng chuỗi ngắn**
200	Bac Nam	BN
210	Mien Bac	MB
220	Mien Nam	MN

Đặc tả bài toán:

- Tất cả các sinh viên có thể xem thông tin của các sinh viên của lớp mình.
- Tất cả các lớp trưởng : có thể xem, sửa và thêm thông tin của lớp mình.
- Quản Lý: có thể thực hiện tất cả các hoạt động đối với CSDL.

2. Các bước thực hành

Bước 1: Tạo chính sách OLS

```
SA_SYSDBA.CREATE_POLICY(
      policy_name => 'chinhsach',
      column_name =>'lb_col',
      default_options =>'no_control');
```

Bước 2: Định nghĩa các thành phần nhãn - label component(Level, Compartment, Group)

```
SA_COMPONENTS.CREATE_LEVEL(
       policy_name => 'chinhsach',
       level_num => 100,
       short_name => 'TS',
       long_name => 'TOP_SECRET');
```

```
SA_COMPONENTS.CREATE_COMPARTMENT(
           policy_name => 'chinhsach',
           comp_num => 65,
           short_name => 'D',
           long_name => 'AT11D');
```

```
SA_COMPONENTS.CREATE_GROUP(
           policy_name => 'chinhsach',
           group_num => 210,
           short_name => 'MB',
           long_name => 'Mien Bac');
```

Bước 3: Tạo các data label để sử dụng

```
SA_LABEL_ADMIN.CREATE_LABEL(
          policy_name => 'chinhsach',
          label_tag => 110,
          label_value => 'S:D:MB',
          data_label => TRUE);
```

Bước 4 :Áp dụng chính sách an toàn trên cho các bảng

```
SA_POLICY_ADMIN.APPLY_TABLE_POLICY(
    policy_name =>'chinhsach',
    schema_name => 'test',
    table_name => 'sinhvien',
    table_options =>  'LABEL_DEFAULT, READ_CONTROL,
                       WRITE_CONTROL,LABEL_UPDATE,
                       CHECK_CONTROL',
    label_function => null,
    predicate => null);
```

Bước 5 : Gán nhãn cho các user hay các ứng dụng

```
SA_USER_ADMIN.SET_USER_LABELS(
      POLICY_NAME=>'chinhsach',
      user_name=>'LT11DMB',
      MAX_READ_LABEL=>'S:D:MB',
      MAX_WRITE_LABEL=>'S:D:MB',
      MIN_WRITE_LABEL=>'UC',
      DEF_LABEL=>'S:D:MB',
      ROW_LABEL=>'S:D:MB');
```

3. Thực hành (Demo)

- ***Truy xuất từng User***

User QLBN:

ID	HOTEN	GIOITINH	QUEQUAN	CHUCVU	LOP	COSO	LB_COL
1	Trinh Hoang Son	Nam	Ninh Binh	Lop Truong	AT11D	Mien Bac	110
2	Do Tong Quoc	Nam	Binh Dinh	Sinh Vien	AT11D	Mien Bac	120
3	Ton Nu Nguyen Hau	Nu	Phu Yen	Sinh Vien	AT11E	Mien Nam	140
4	Nguyen Thi Hang	Nu	Binh Dinh	Lop Truong	AT11E	Mien Nam	130
5	Nguyen Le Xuan Phuoc	Nam	Tay Ninh	Quan Ly		Bac Nam	100
6	Nguyen Hung	Nam	Binh Duong	Sinh Vien	AT11E	Mien Nam	140
7	Truong The Luc	Nam	Ho Chi Minh	Sinh Vien	AT11E	Mien Nam	140
8	Ho Anh Dung	Nam	Thanh Hoa	Sinh Vien	AT11D	Mien Bac	120
9	Tong Thanh Anh	Nam	Quang Binh	Sinh Vien	AT11D	Mien Bac	120
10	Phan Thi Thao	Nu	Ha Noi	Quan Ly		Bac Nam	100

User LT11DMB:

ID	HOTEN	GIOITINH	QUEQUAN	CHUCVU	LOP	COSO	LB_COL
1	Trinh Hoang Son	Nam	Ninh Binh	Lop Truong	AT11D	Mien Bac	110
2	Do Tong Quoc	Nam	Binh Dinh	Sinh Vien	AT11D	Mien Bac	120
8	Ho Anh Dung	Nam	Thanh Hoa	Sinh Vien	AT11D	Mien Bac	120
9	Tong Thanh Anh	Nam	Quang Binh	Sinh Vien	AT11D	Mien Bac	120

User LT11EMN:

ID	HOTEN	GIOITINH	QUEQUAN	CHUCVU	LOP	COSO	LB_COL
4	Nguyen Thi Hang	Nu	Binh Dinh	Lop Truong	AT11E	Mien Nam	130
3	Ton Nu Nguyen Hau	Nu	Phu Yen	Sinh Vien	AT11E	Mien Nam	140
6	Nguyen Hung	Nam	Binh Duong	Sinh Vien	AT11E	Mien Nam	140
7	Truong The Luc	Nam	Ho Chi Minh	Sinh Vien	AT11E	Mien Nam	140

User SV11DMB

ID	HOTEN	GIOITINH	QUEQUAN	CHUCVU	LOP	COSO	LB_COL
2	Do Tong Quoc	Nam	Binh Dinh	Sinh Vien	AT11D	Mien Bac	120
8	Ho Anh Dung	Nam	Thanh Hoa	Sinh Vien	AT11D	Mien Bac	120
9	Tong Thanh Anh	Nam	Quang Binh	Sinh Vien	AT11D	Mien Bac	120

User SV11EMN

ID	HOTEN	GIOITINH	QUEQUAN	CHUCVU	LOP	COSO	LB_COL
3	Ton Nu Nguyen Hau	Nu	Phu Yen	Sinh Vien	AT11E	Mien Nam	140
6	Nguyen Hung	Nam	Binh Duong	Sinh Vien	AT11E	Mien Nam	140
7	Truong The Luc	Nam	Ho Chi Minh	Sinh Vien	AT11E	Mien Nam	140

- ***Kiểm tra kết quả theo tính No Write Up***

Quản lý (QLBN) có thể thực hiện mọi thao tác trên CSDL, các Lớp trưởng có thể xem, sửa thông tin của các sinh viên thuộc lớp của mình nhưng không thể xem thông tin của các lớp khác, các sinh viên thì chỉ có thể xem thông tin của lớp mình và sửa đổi thông tin của các sinh viên thuộc lớp mình nhưng không có quyền thêm (tức là không có quyền Insert) sinh viên thuộc lớp mình.

Để kiểm tra kết quả theo tính *No Write Up* bằng cách thực hiện **Update/Insert** với từng user để cho ra kết quả tương ứng

- *User QLBN:*

1 row updated./ 1 row inserted.

- *User LT11DMB:*

```
UPDATE test.sinhvien SET gioitinh = 'Nu' WHERE ID = 2;
```

⇨ *1 row updated.*

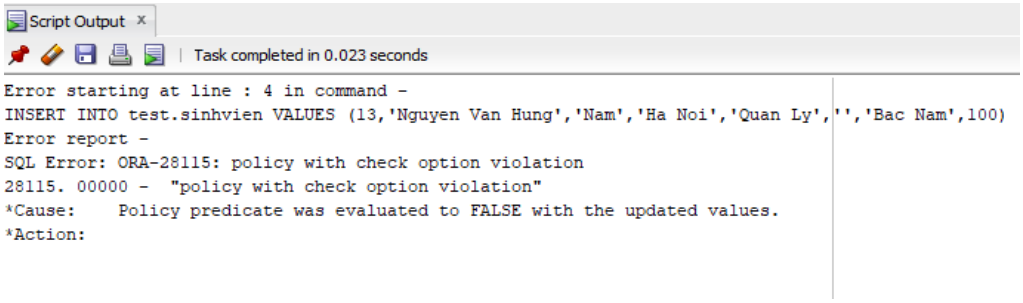
ID	HOTEN	GIO	QUEQUAN	CHUCVU	LOP	COSO	LB_COL
1	Trinh Hoang Son	Nam	Ninh Binh	Lop Truong	AT11D	Mien Bac	110
2	Do Tong Quoc	Nu	Binh Dinh	Sinh Vien	AT11D	Mien Bac	120
8	Ho Anh Dung	Nam	Thanh Hoa	Sinh Vien	AT11D	Mien Bac	120
9	Tong Thanh Anh	Nam	Quan Binh	Sinh Vien	AT11D	Mien Bac	120

```
UPDATE test.sinhvien SET gioitinh = 'Nu' WHERE HOTEN= 'Phan Thi Thao';
```

⇨ *No row updated.*

- *User LT11EMN:*

```
INSERT INTO test.sinhvien VALUES (13,'Nguyen Van Hung','Nam','Ha
Noi','Quan Ly','','Bac Nam',100);
```



- *User SV11DMB:*

```
UPDATE test.sinhvien SET QueQuan = 'Tay Ninh' WHERE Chucvu='Quan Ly';
```

⇨ *0 rows updated.*

```
UPDATE test.sinhvien SET QueQuan = 'Tay Ninh' WHERE Chucvu='Lop truong'
```

⇨ *0 rows updated.*

- *User SV11EMN:*

```
UPDATE test.sinhvien SET QUEQUAN = 'Soc trang' WHERE HOTEN='Nguyen Hung';
```

⇨ *1 row updated.*

ID	HOTEN	GIO	QUEQUAN	CHUCVU	LOP	COSO	LB_COL
3	Ton Nu Nguyen Hau	Nu	Phu Yen	Sinh Vien	AT11E	Mien Nam	140
6	Nguyen Hung	Nam	Soc trang	Sinh Vien	AT11E	Mien Nam	140
7	Truong The Luc	Nam	Ho Chi Minh	Sinh Vien	AT11E	Mien Nam	140

KẾT LUẬN

Việc bảo vệ an toàn cho CSDL luôn là một việc vô cùng quan trọng. Tuy nhiên, bảo vệ như thế nào lại là một vấn đề không hề đơn giản. Với những nội dung được trình bày trong đề tài này, chúng ta có thể thấy rằng bên trong các hệ quản trị CSDL luôn có các cơ chế an toàn được hỗ trợ sẵn. Các cơ chế an toàn như VPD và OLS trong hệ quản trị Oracle có thể hỗ trợ trong việc bảo vệ CSDL mức hàng kết hợp với mức cột. Đây có thể là một gợi ý tốt cho các nhà quản trị an toàn khi cần thiết lập các biện pháp để bảo vệ CSDL

TÀI LIỆU THAM KHẢO

1. Label security administrators guide, 12*c* Release 2 (12.2), 2019
2. Oracle Label Security with Oracle Database 12c, Oracle White Paper, 2013
3. DBA – Oracle Label Security, Kidus Mamuye Tekeste, 2007
4. Lab Bảo Mật hệ thống thông tin, Đại học Bách khoa Tp.Hồ Chí Minh