QUẢN LÝ QUYỀN (PRIVILEGE)

Biên soạn: Nguyễn Việt Hưng

Bộ môn: Khoa Học Máy Tính - Khoa Công Nghệ Thông Tin

Trường Đại Học Giao Thông Vân Tải

Website: https://sites.google.com/site/viethung92gtvt/oracle-dba

Email : viethung92gtvt@gmail.com

Khái niệm

Quyền của một user trong CSDL Oracle là một sự cho phép thực hiện 1 câu lệnh SQL hoặc được phép truy xuất đến một đối tượng nào đó.

VD: quyền tạo bảng CREATE TABLE, quyền đăng nhập vào cơ sở dữ liệu CREATE SESSION, quyền SELECT trên một bảng cụ thể nào đó,...).

Phân loại quyền

- **Oracle có 2 loại quyền cho user:**
  - **Quyền hệ thống (System Privilege):** Cho phép user thực hiện các thao tác cụ thể trong CSDL.
  - **Quyền đối tượng (Object Privilege):** Cho phép user truy xuất và thao tác trên một đối tượng cụ thể.

Các quyền hệ thống

- **Các quyền hệ thống có thể chia ra như sau:**
  - Các quyền cho phép thực hiện các thao tác mức độ rộng trên hệ thống ví dụ như: CREATE SESSION, CREATE TABLESPACE, CREATE USER.
  - Các quyền cho phép quản lý các đối tượng thuộc về một user ví dụ: CREATE TABLE
  - Các quyền cho phép quản lý các đối tượng trong bất cứ một schema nào ví dụ câu lệnh: CREATE ANY TABLE.

Các quyền hệ thống

- Hơn 100 quyền hệ thống khác nhau.
- Từ khóa `ANY` trong câu lệnh gán quyền hệ thống chỉ ra rằng user có quyền thao tác trong bất kỳ schema nào.
- Câu lệnh `GRANT` gán quyền cho một user hoặc một nhóm các user.
- Câu lệnh `REVOKE` xóa các quyền.

Các quyền hệ thống – Ví dụ

Category	Examples
INDEX	CREATE ANY INDEX ALTER ANY INDEX DROP ANY INDEX
TABLE	CREATE TABLE CREATE ANY TABLE ALTER ANY TABLE DROP ANY TABLE SELECT ANY TABLE UPDATE ANY TABLE DELETE ANY TABLE
SESSION	CREATE SESSION ALTER SESSION RESTRICTED SESSION
TABLESPACE	CREATE TABLESPACE ALTER TABLESPACE DROP TABLESPACE UNLIMITED TABLESPACE

Gán các quyền hệ thống cho user

```
GRANT system_privilege[,system_privilege]... TO
  {user|Public} [,user]...[WITH ADMIN OPTION]
```

- **Sử dụng câu lệnh `GRANT` để gán các quyền hệ thống cho user.**
- **Người được *gán quyền có thể gán quyền hệ thống cho user khác nếu có thêm tùy chọn WITH ADMIN OPTION.***

VD:

```
GRANT CREATE SESSION TO emi;
```

```
GRANT CREATE SESSION TO emi WITH ADMIN OPTION;
```

Thu hồi quyền hệ thống

```
REVOKE {system_privilege|role}[,{system_privilege|role}
]...FROM {user|role|PUBLIC} [, {user|role|PUBLIC} ]...
```

- Sử dụng câu lệnh **REVOKE** để thu hồi một quyền hệ thống khỏi user.
- Các user được gán quyền hệ thống với tùy chọn **ADMIN OPTION** có thể thu hồi quyền hệ thống đó của bất kỳ user.
- Chỉ các quyền được gán qua câu lệnh **GRANT** mới có thể bị thu hồi.
- VD:

```
REVOKE CREATE TABLE FROM emi;
```

Thu hồi quyền hệ thống với tùy chọn ADMIN OPTION

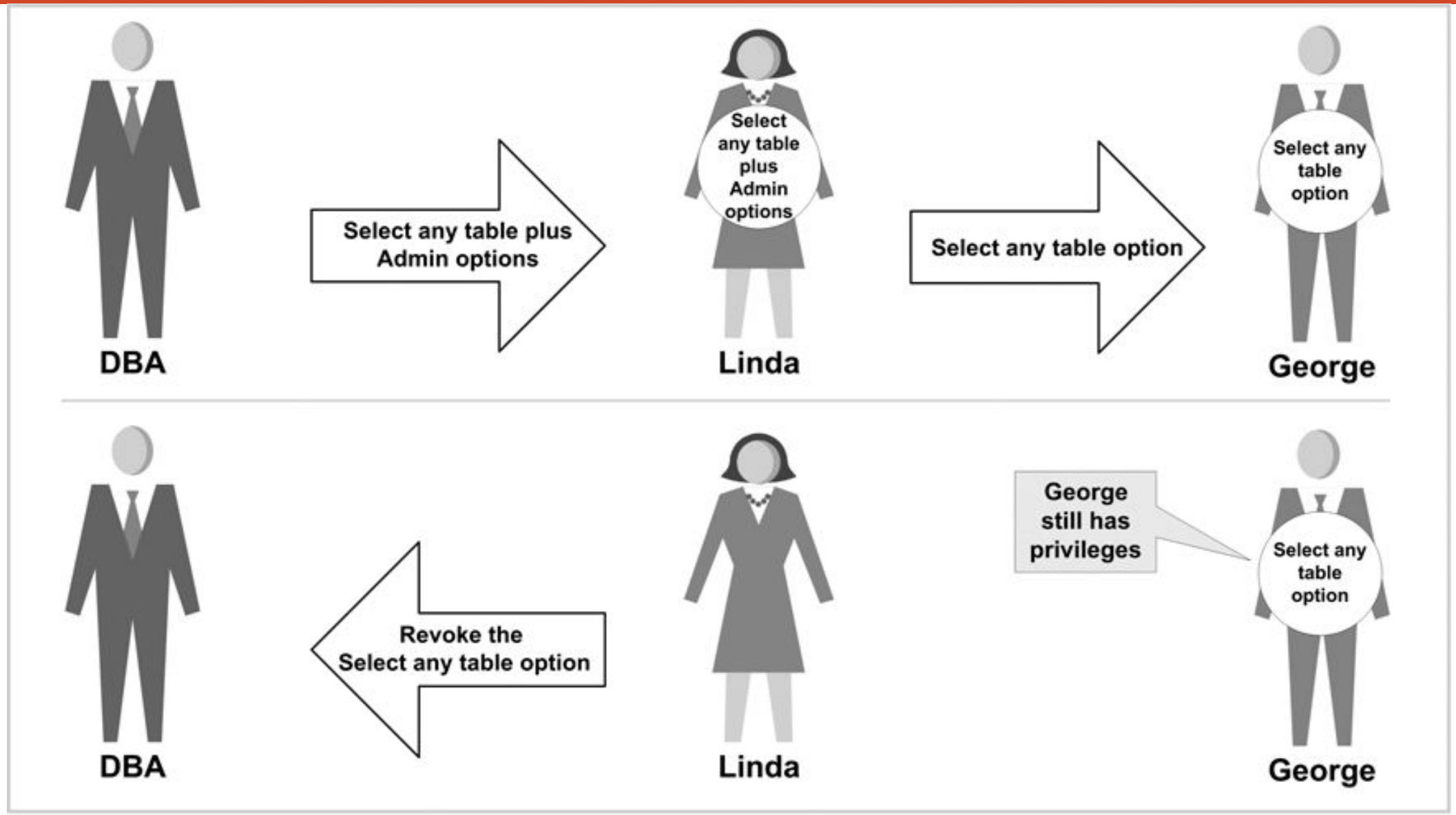


FIGURE 4-14 Revoking a system privilege with the ADMIN option

Quyền đối tượng

- Là quyền thực hiện một hành động cụ thể trên một đối tượng trong schema cụ thể. Vd: quyền xóa các hàng dữ liệu khỏi bảng Department trong schema SCOTT.
- Có nhiều quyền đối tượng khác nhau dành cho các loại đối tượng khác nhau.

Các quyền đối tượng

Object priv.	Table	View	Sequence	Procedure
ALTER	√	√		
DELETE	√	√		
EXECUTE			√	
INDEX	√	√		
INSERT	√	√		
REFERENCES		√		
SELECT	√	√		
UPDATE	√	√		

Gán các quyền đối tượng cho user

```
GRANT {object_privilege [(column_list)]
[,object_privilege[(column_list)]] … |ALL} ON
[schema.]object TO {user|role|PUBLIC}
[,{user|role|PUBLIC}]... [WITH GRANT OPTION]
```

- **Sử dụng lệnh `GRANT` để gán các quyền đối tượng cho user.**
- **Gán quyền đối tượng phải nằm trong schema của người gán hoặc người gán phải có tùy chọn `WITH GRANT OPTION` với quyền đó hoặc người gán có quyền hệ thống `GRANT ANY OBJECT PRIVILEGE`.**
- **VD:**

```
GRANT SELECT ON emi.customers TO jeff;
```

```
GRANT UPDATE ON emi.customers TO jeff WITH
GRANT OPTION;
```

Thu hồi quyền đối tượng từ user

```
REVOKE {object_privilege[, object_privilege ]...
      |ALL} ON [schema.]object FROM
user|role|PUBLIC} [,{user|role|PUBLIC}]...
```

- Sử dụng lệnh **REVOKE** để thu hồi các quyền đối tượng từ user.
- Để 1 user **REVOKE** một quyền đối tượng từ 1 user khác, nó cần thỏa mãn 1 trong 2 điều kiện sau:

1. Phải là user trực tiếp gán quyền đó
2. Có quyền hệ thống : **GRANT ANY OBJECT PRIVILEGE**

Thu hồi quyền đối tượng với tùy chọn GRANT OPTION

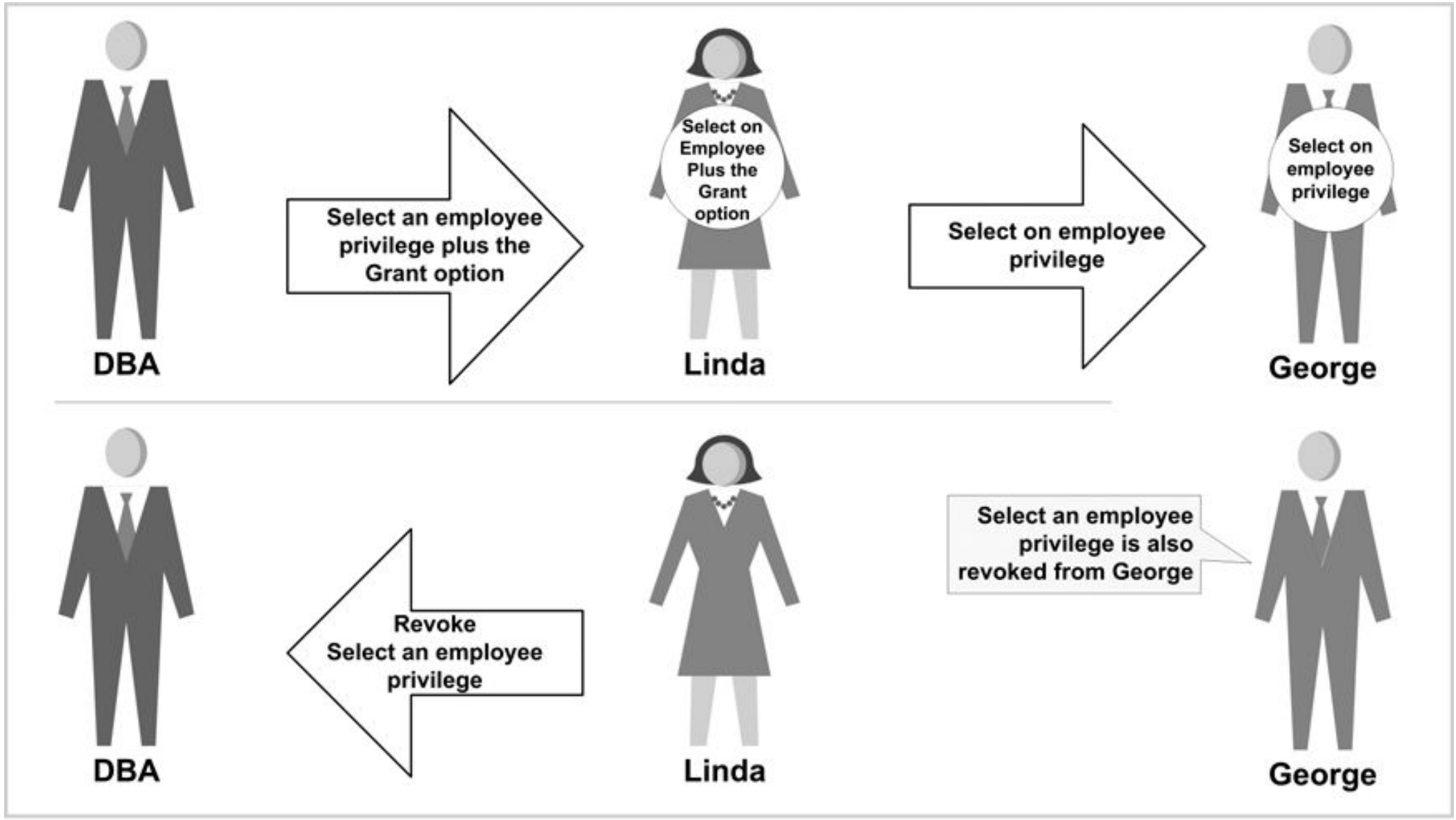


FIGURE 4-16 Revoking an object privilege with the GRANT option

Lấy thông tin về quyền

Có thể lấy thông tin về quyền bằng cách truy vấn các views sau:

- `DBA_SYS_PRIVS`: Hiển thị thông tin về tất cả các quyền hệ thống được gán cho user và role
- `USER_SYS_PRIVS`: Hiển thị thông tin về tất cả các quyền hệ thống được gán cho user hiện tại.
- `DBA_TAB_PRIVS`: Hiển thị tất cả các quyền đối tượng

Thực hành 1. Quyền hệ thống

1. Tạo các user A,B,C chỉ rõ default tablespace là tương ứng lần lượt là DATA1, DATA2, DATA3 và hạn mức trên default tablespace của chúng đều = 1M.
2. Admin gán cho A có thể đăng nhập và tạo bảng, ngoài ra cho A có thể gán quyền tạo bảng cho các user khác.
3. Admin gán cho B có thể đăng nhập và tạo bảng, ngoài ra cho B có thể gán quyền đăng nhập cho các user khác.
4. C được gán quyền đăng nhập và tạo bảng bởi A và B. Kiểm chứng việc đăng nhập, tạo bảng, và insert dữ liệu bởi C
5. C bị thu hồi quyền tạo bảng, hãy thu hồi quyền tạo bảng của C bằng 2 cách.

Thực hành 2. Quyền đối tượng

1. Tạo user A sao cho A có thể đăng nhập và tạo bảng. (Hạn mức trên tablespace USERS = 1M)
2. A Tạo bảng tblA(id number). (Chèn dữ liệu demo, chú ý commit)
3. Tạo user B và C cũng có các quyền như A.
4. A gán quyền select trên tblA cho B và cho B có thể gán quyền đó cho C.
5. B tiến hành gán quyền select trên A.tblA cho C.
6. C muốn có thể insert dữ liệu trên A.tblA, hãy thực giúp C đạt được ý muốn bằng 2 cách.

QUẢN LÝ CHỨC DANH (ROLE)

Biên soạn: Nguyễn Việt Hưng

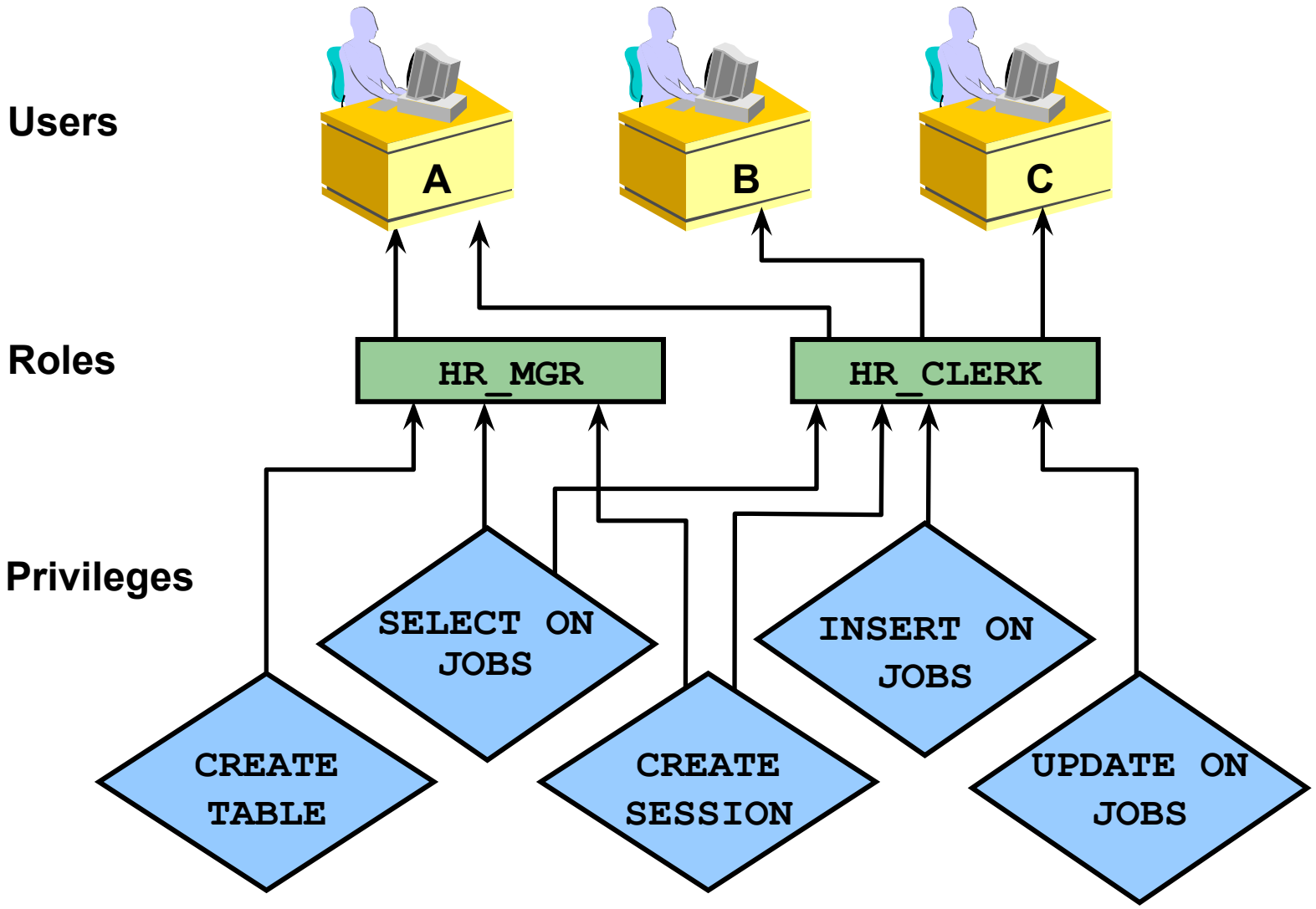
Bộ môn: Khoa Học Máy Tính - Khoa Công Nghệ Thông Tin

Trường Đại Học Giao Thông Vân Tải

Website: https://sites.google.com/site/viethung92gtvt/oracle-dba

Email : viethung92gtvt@gmail.com

Các chức danh



Oracle cung cấp công cụ cho phép quản lý một cách dễ dàng các quyền thông qua việc sử dụng chức danh (Roles). Chức danh là một nhóm các quyền được đặt tên có liên quan đến nhau và được gán cho một user hay một chức danh khác.

Một số Role định sẵn

ROLE NAME	DESCRIPTION
CONNECT	Từ phiên bản Oracle 10*g* Release 2, chức danh Connect chỉ còn 1 quyền là CREATE SESSION
RESOURCE	Bao gồm các quyền: CREATE CLUSTER, CREATE INDEXTYPE, CREATE OPERATOR, CREATE PROCEDURE, CREATE SEQUENCE, CREATE TABLE, CREATE TRIGGER,CREATE TYPE, UNLIMITED TABLESPACE (quyền này không hiện ra khi truy vấn trong data dictionary)
DBA	All system privileges WITH ADMIN OPTION

Đặc điểm

1. Role có thể gán cho user hoặc role và thu hồi từ user hoặc role giống như gán và thu hồi quyền.
2. Role có thể gán cho bất kỳ user và role. Tuy nhiên, 1 role không thể gán cho chính nó hoặc gán vòng quanh.
3. Role có thể bao gồm cả quyền hệ thống và quyền đối tượng.
4. Tên của role phải duy nhất, không trùng tên với bất kỳ user hoặc role khác đã tồn tại trong CSDL.
7. Role không thuộc sở hữu của bất kỳ user và không được lưu trữ trong bất kỳ schema nào. Role được lưu trữ trong data dictionary.
8. 1 user có thể enable, disable các role gán cho nó.
9. Khi 1 role có đặt mật khẩu, cần phải nhập mật khẩu khi enable role.

Tạo chức danh

Chú ý: để tạo được role, user phải có quyền hệ thống CREATE ROLE.

- **Không xác định:**

```
CREATE ROLE r01 [NOT IDENTIFIED];
```

- **Bằng mật khẩu:**

```
CREATE ROLE r02  IDENTIFIED BY abc123;
```

Gán các chức danh

```
GRANT role [, role ]... TO {user|role|PUBLIC}
    [, {user|role|PUBLIC} ]...[WITH ADMIN
OPTION]
```

Để gán chức danh cho 1 user hoặc role khác, user phải có chức danh đó với tùy chọn **WITH ADMIN OPTION** hoặc có quyền hệ thống: **GRANT ANY ROLE**

Chú ý: User tạo ra chức danh thì mặc định có tùy chọn **WITH ADMIN OPTION** đối với chức danh đó.

VD:

```
GRANT oe_clerk TO scott;
```

```
GRANT hr_clerk TO hr_manager;
```

```
GRANT hr_manager TO scott WITH ADMIN OPTION;
```

Gán quyền hệ thống cho chức danh

```
GRANT system_privilege [, system_privilege]...
TO role [WITH ADMIN OPTION]
```

- Để gán 1 quyền hệ thống cho chức danh, user phải có tùy chọn **WITH ADMIN OPTION** với quyền hệ thống đó hoặc user phải có quyền **GRANT ANY PRIVILEGE**.

- VD: grant create table to R01;

Đặc điểm tùy chọn ADMIN OPTION

- Tùy chọn WITH ADMIN OPTION sẽ cho phép người được cấp role/quyền:

✔ Cấp lại role/quyền đó cho một user hoặc role khác.

✔ Thu hồi lại role/quyền đó từ một user hoặc role bất kỳ.

✔ Thay đổi role đó bằng lệnh ALTER ROLE.

✔ Xóa role đó.

Ví dụ khi gán role ***new_dba*** cho user ***bob*** với tùy chọn WITH ADMIN OPTION, thì bob không chỉ được sử dụng các quyền có trong role new_dba mà có thể grant, revoke hoặc drop role này.

Gán quyền đối tượng cho chức danh

```
GRANT object_privilege[,object_privilege]...
   TO role [,role];
```

- Để gán 1 quyền đối tượng cho chức danh, user phải thỏa mãn 1 trong các yêu cầu sau:
- User sở hữu đối tượng đó.
- Tùy chọn WITH GRANT OPTION phải đi kèm khi gán quyền đối tượng đó cho user đó.
- User đó phải có quyền hệ thống GRANT ANY OBJECT PRIVILEGE.
- Không có tùy chọn GRANT OPTION khi gán 1 quyền đối tượng cho chức danh.

Enable và Disable các chức danh

- Trong 1 session, user có thể enable và disable các role mà được gán cho nó qua mệnh đề SET ROLE.
- Role có đặt mật khẩu cần phải chỉ rõ mật khẩu để enable role đó.
- Ví dụ:

```
SET ROLE hr_clerk;
```

```
SET ROLE oe_clerk IDENTIFIED BY order;
```

```
SET ROLE ALL EXCEPT oe_clerk;
```

Thiết lập hoặc hủy bỏ mật khẩu của chức danh

User phải thõa mãn 1 trong các yêu cầu sau:

1. **User phải có tùy chọn WITH ADMIN OPTION của chức danh đó.**
2. **User phải có quyền ALTER ANY ROLE**

VD:

Thiết lập mật khẩu:

```
ALTER ROLE r01 IDENTIFIED BY abc123;
```

Hủy bỏ mật khẩu:

```
ALTER ROLE r02   NOT IDENTIFIED;
```

Thiết lập chức danh mặc định

- Một user có thể được gán nhiều chức danh.
- Mặc định khi chưa thiết lập chức danh mặc định, tất cả các chức danh được enable khi user đăng nhập.
- Khi thiết lập chức danh mặc định, thì chỉ các chức danh mặc định được enable khi user đăng nhập mà không phải nhập mật khẩu đối với các role có mật khẩu.

```
ALTER USER scott DEFAULT ROLE hr_clerk, oe_clerk;
```

```
ALTER USER scott DEFAULT ROLE ALL;
```

```
ALTER USER scott DEFAULT ROLE ALL EXCEPT  hr_clerk;
```

```
ALTER USER scott DEFAULT ROLE NONE;
```

Thu hồi các chức danh khỏi User

- **Thu hồi các chức danh khỏi user đòi hỏi tùy chọn `ADMIN OPTION` hoặc quyền `GRANT ANY ROLE`.**
- **Để thu hồi một chức danh:**

```
REVOKE role [, role ]
    FROM {user|role|PUBLIC}
    [, {user|role|PUBLIC}];
```

VD:

```
REVOKE oe_clerk FROM scott;
```

Hủy bỏ các chức danh

- Xóa một chức danh:
  - Hủy bỏ chức danh đó với tất cả user và các chức danh mà nó được gán.
  - Hủy bó nó khỏi CSDL.
- Đòi hỏi tùy chọn `ADMIN OPTION` hoặc quyền `DROP ANY ROLE`
- Để xóa một chức danh:

```
DROP ROLE role;
```

Lấy thông tin chức danh

Thông tin về chức danh có thể lấy bằng cách truy vấn các views sau:

- `DBA_ROLES`: Tất cả các chức danh có trong CSDL
- `DBA_ROLE_PRIVS`: Các chức danh gán cho user và chức danh
- `DBA_SYS_PRIVS`: Các quyền hệ thống gán cho user và chức danh
- `ROLE_SYS_PRIVS`: Các quyền hệ thống gán cho chức danh của user hiện tại.
- `ROLE_TAB_PRIVS`: Các quyền đối tượng gán cho chức danh hiện tại
- `DBA_TAB_PRIVS`: Các quyền đối tượng gán cho tất cả chức danh trong hệ thống
- `SESSION_ROLES`: Các chức danh user hiện enable

Practice : Managing Roles

1 Examine the data dictionary view and list the system privileges of the RESOURCE role.

2 Create a role called DEV, which will enable a user assigned the role to create a table, create a view, and select from Emi's CUSTOMERS1 table.

3 a Assign the RESOURCE and DEV roles to Bob, but make only the RESOURCE role automatically enabled when he logs on.

b Give Bob the ability to read all the data dictionary information.

4 Bob needs to check the undo segments that are currently used by the instance. Connect as Bob and list the undo segments used.

Hint: Use SET ROLE SELECT_CATALOG_ROLE

5 As SYSTEM, try to create a CUST_VIEW view on Emi's CUSTOMERS1 table. What happens?

6 As user Emi, grant SELECT on CUSTOMERS1 to SYSTEM. As SYSTEM, create a CUST_VIEW view on Emi's CUSTOMERS1 table.

Bài tập 1: User ADMIN Tạo một vai trò có tên là "HR_MANAGER" và gán cho vai trò này các quyền sau:

- SELECT trên bảng EMPLOYEES để có thể xem thông tin về nhân viên.
- SELECT trên bảng DEPARTMENTS để xem thông tin về các phòng ban.

Gán vai trò "HR_MANAGER" cho một người dung A

Bài tập 2: Tạo một vai trò có tên là "DEPARTMENT_MANAGER" và gán cho vai trò này các quyền sau:

- SELECT trên bảng EMPLOYEES để có thể xem thông tin về nhân viên.
- SELECT và UPDATE trên bảng DEPARTMENTS để có thể xem thông tin và cập nhật thông tin về phòng ban.

Gán vai trò "DEPARTMENT_MANAGER" cho một người dung B.

Bài tập 3: Sử dụng người dùng được gán vai trò "HR_MANAGER" và người dùng được gán vai trò "DEPARTMENT_MANAGER" để kiểm tra xem họ có quyền thực hiện các thao tác tương ứng trong schema HR hay không. Hãy thử truy vấn dữ liệu từ các bảng **EMPLOYEES** và **DEPARTMENTS**, cũng như cố gắng cập nhật dữ liệu trong bảng **DEPARTMENTS** để kiểm tra quyền hạn.

Bài tập 4: Thu hồi vai trò "HR_MANAGER" và "DEPARTMENT_MANAGER" từ các người dùng tương ứng. Sau đó, thử lại các truy vấn và thao tác để đảm bảo họ không còn có quyền truy cập.

Bài tập 5: Tạo một vai trò có tên là "READ_ONLY" và gán cho vai trò này quyền SELECT trên tất cả các bảng trong schema HR. Gán vai trò "READ_ONLY" cho một người dùng cụ thể và kiểm tra xem họ có thể truy cập dữ liệu từ các bảng trong schema HR hay không.

Bài tập 6: a. Truy vấn các quyền được gán cho các chức danh vừa tạo.
b. Truy vấn các chức danh được gán cho các user xuất hiện ở các bài tập trên.