CSC12001 – An toàn bảo mật CSDL trong HTTT

Tháng 1/2019

Quyền & Vai trò
trong điều khiển truy cập

Tóm tắt nội dung bài thực hành:

Tài liệu này hướng dẫn sinh viên thực hiện các lệnh phân quyền, vai trò và Data Dictionary trong Oracle 11g. Sinh viên có thể thực hiện các ví dụ bên dưới cũng như bài tập bằng công cụ SQL* Plus hoặc SQL Developer trong gói cái đặt Oracle.

Bộ môn **Hệ thống thông tin**
Khoa Công nghệ thông tin
ĐH Khoa học tự nhiên TP HCM

MỤC LỤC

1 Quyền (privilege) và Vai trò (role)

1.1 Quyền (Privilege)

- Quyền là 1 sự cho phép thực hiện 1 câu lệnh SQL nào đó hoặc được phép truy xuất đến 1 đối tượng dữ liệu nào đó (VD: Quyền tạo bảng CREATE Table, quyền kết nối đến một CSDL CREATE SESSION; quyền thực hiện lệnh SELECT trên 1 bảng cụ thể nào đó, …)
- Chỉ cấp cho user chính xác các quyền mà user cần đến. Việc cấp dư thừa những quyền không cần thiết có thể gây nguy hại cho việc bảo mật hệ thống.
- Có 2 loại quyền:
    - *Quyền hệ thống (System Privilege)*
        - Đây là quyền thực hiện 1 tác vụ CSDL cụ thể hoặc quyền thực hiện 1 loại hành động trên tất cả những đối tượng schema của hệ thống. VD: quyền ALTER SYSTEM, quyền CREATE TABLE, quyền DELETE ANY TABLE (xóa các hàng của bất kỳ bảng nào trong CSDL)
        - User được cấp 1 quyền hệ thống nếu thỏa 1 trong các điều kiện sau:
            - User đã được cấp quyền hệ thống đó với tùy chọn WITH ADMIN OPTION
            - User có quyền GRANT ANY PRIVILEGE
    - *Quyền đối tượng (Schema Object Privilege hoặc Object Privilege)*
        - Là quyền thực hiện một hành động cụ thể trên 1 đối tượng schema cụ thể. VD: quyền xóa dữ liệu khỏi bảng Department.
        - Có nhiều quyền đối tượng khác nhau dành cho các loại đối tượng schema khác nhau
        - Dùng để quản lý truy xuất đến các đối tượng schema cụ thể
        - User có thể được cấp quyền đối tượng nếu thỏa 1 trong các điều kiện sau:

- User có tất cả quyền đối tượng trên tất cả các đối tượng thuộc schema của mình. Vì vậy, user có quyền cấp bất kỳ quyền đối tượng trên bất kỳ đối tượng nào thuộc sở hữu của mình cho bất cứ user nào khác
- User có quyền GRANT ANY OBJECT PRIVILEGE
- User được cấp quyền đối tượng đối với tùy chọn WITH GRANT OPTION.

1.2 Vai trò (Role)

- Vai trò là một tập hợp gồm các quyền và vai trò khác
- Vai trò được gán cho user hoặc các vai trò khác
- Vai trò giúp cho việc quản lý người dùng dễ dàng và tiết kiệm công việc hơn.
- Có một số vai trò có sẵn do hệ thống tự định nghĩa: DBA, RESOURCE, CONNECT, …
- Đa phần các vai trò do người quản trị CSDL tạo ra.
- Vai trò không phải là một đối tượng schema (schema object) nên không được lưu trữ trong schema của user tạo ra nó. Do vậy, user tạo ra một vai trò có thể bị xóa mà không ảnh hưởng đến vai trò đó.
- User có thể được cấp 1 vai trò nếu thỏa điều kiện sau:
    - User đã tạo ra vai trò đó
    - User đã được cấp vai trò với tùy chọn WITH ADMIN OPTION
    - User có quyền GRANT ANY ROLE

1.3 Thực hành

a) Tạo role:

CREATE ROLE myrole;

Lưu ý: để tạo được role, phải có quyền hệ thống CREATE ROLE

b) Lệnh Grant

GRANT quyenhan TO user/role;

VD:

- GRANT DELETE ANY TABLE TO Tom;
- GRANT CREATE USER TO myrole;

- GRANT myrole TO Tom;
- GRANT myrole TO Janilen;

c) Lệnh Revoke

REVOKE Quyen FROM user/role;

d) Lệnh Enable, Disable một Role

SET ROLE myrole;

SET ROLE ALL;

SET ROLE NONE;

SET ROLE ALL EXCEPT lavender;

2 Từ điển dữ liệu (Data Dictionary)

2.1 Tổng quan

- Mọi CSDL Orclae đều có 1 tự điển dữ liệu (Data Dictionary). Từ điển dữ liệu được tạo ra khi CSDL được khởi tạo.
- Từ điển dữ liệu trong Oracle là 1 tập các bảng và view được sử dụng như một tham khảo dạng chỉ đọc (read-only) về bản thân CSDL đó
- Từ điển dữ liệu nằm trên tablespace SYSTEM, thuộc schema của user SYS. Bao gồm 2 loại:
    - Các bảng cơ bản (Base table): Là các bảng lưu trữ thông tin của Từ điển dữ liệu. Dữ liệu được lưu trong bảng này dưới dạng mã hóa.
    - Các View dành cho người dùng truy xuất (User-accessible View): Tổng hợp và hiển thị thông tin được lưu trong các bảng cơ bản ở dạng người bình thường có thể đọc hiểu. tùy vào quyền của mỗi user mà user đó có thể truy xuất view nào và truy xuất những dữ liệu nào của view đó.
- Một từ điển dữ liệu sẽ lưu trữ tất cả các thông tin về cấu trúc luận lý và cấu trúc vật lý của CSDL:
    - Định nghĩa của tất cả các đối tượng schema trong CSDL
    - Các quy định, giới hạn về sử dụng tài nguyên của user, …
    - Danh sách các user, các quyền, role được cấp cho user
    - Các ràng buộc toàn vẹn dữ liệu
    - Thông tin audit
    - Các thông tin CSDL tổng quát khác
- Oracle tự động cập nhật từ điển dữ liệu để phản ánh chính xác trạng thái thực tế của CSDL.

2.2 Các tiếp đầu ngữ trong tên View

- Trong nhiều trường hợp, một tập gồm 3 view chứa những thông tin tương tự và tên của chúng chỉ khác nhau ở các tiếp đầu ngữ như: user, all, dba.
- Danh sách các tiếp đầu ngữ:
    - USER: hiển thị những gì thuộc schema của user đó
    - ALL: Hiển thị những gì mà user đó có thể truy xuất

- DBA: Hiển thị tất cả thông tin thuộc schema của mọi user (View dành cho người quản trị).

2.3 Các View thường sử dụng

- DBA USERS: cung cấp thông tin của các user trong CSDL.
- DBA TS QUOTAS: cung cấp thông tin quota của các user.
- DBA PROFILES: cung cấp thông tin về các profile.
- DBA SYS PRIVS: Hiển thị những user được cấp các quyền hệ thống.
- DBA ROLES: Hiển thị tất cả các role có trong CSDL.
- DBA COL PRIVS: Hiển thị thông tin về việc gán quyền hệ thống mức cột.
- DBA ROLE PRIVS: Hiện thị tất cả các user và role của họ.
- DBA TAB PRIVS: Hiện thị tất cả user và quyền trên các bảng của họ.
- ROLE ROLE PRIVS: Hiện thị thông tin về các role được cấp cho các role.
- ROLE SYS PRIVS: Hiển thị quyền hệ thống được cấp cho các role.
- ROLE TAB PRIVS: Hiển thị các quyền trên bảng được cấp cho các role.
- SESSION PRIVS: Hiển thị các quyền hiện tại được enable cho user.
- SESSION ROLES: Hiển thị các role hiện tại đang được enable cho user.

2.4 Thực hành

- Sinh viên dùng tài liệu tham khảo Reference trên Oracle Document Library để tra cứu danh sách các View của từ điển dữ liệu
- Viết lệnh truy xuất các view trên đề xem dữ liệu được hiện thị