**Sinh viên thực hiện:**

18120065 – Đinh Nguyễn Tấn Nguyên

1712779 – Trương Thị Thu Thảo

1612647 – Lê Văn Thi

**GV phụ trách:** Cô Phạm Thị Bạch Huệ / Thầy Lương Vĩ Minh

Đồ án NHÓM 40 môn AN TOÀN VÀ BẢO MẬT DỮ LIỆU TRONG HỆ THỐNG THÔNG TIN

HỌC KỲ II – NĂM HỌC 2020-2021

**AN TOÀN VÀ BẢO MẬT DỮ LIỆU TRONG HỆ THỐNG THÔNG TIN**

**BỘ MÔN HỆ THỐNG THÔNG TIN – KHOA CÔNG NGHỆ THÔNG TIN**

**ĐẠI HỌC KHOA HỌC TỰ NHIÊN, ĐHQG-HCM**

**MỤC LỤC**

**BẢNG THÔNG TIN CHI TIẾT NHÓM 2**

**BẢNG PHÂN CÔNG VÀ ĐÁNH GIÁ 2**

**YÊU CẦU ĐỒ ÁN 4**

1. **YÊU CẦU ĐỒ ÁN 4**
2. **KẾT QUẢ 4**
3. **User 4**
4. Tablespace 4
5. Loại tablespace 5
6. **User profile 6**
7. Profile 6
8. Các loại tài nguyên 6
9. **Quyền 6**
10. **Role 8**
11. **Grant và Revoke 8**

**BẢNG THÔNG TIN CHI TIẾT NHÓM**

|  |  |  |  |
| --- | --- | --- | --- |
| **Mã nhóm:** | 2020-ATBMDLHTTT-40 | | |
| **Tên nhóm:** | 2020-ATBMDLHTTT-40 | | |
| **Số lượng:** | 03 thành viên | | |
| **MSSV** | **Họ tên** | **Email** | **Điện thoại** |
| 18120065 | Đinh Nguyễn Tấn Nguyên | nguyenmottandinh@gmail.com | 0938005804 |
| 1612647 | Lê Văn Thi | [1612647@student.hcmus.edu.vn](mailto:1612647@student.hcmus.edu.vn) | 0334977111 |
| 1712779 | Trương Thị Thu Thảo | [1712779@student.hcmus.edu.vn](mailto:1712779@student.hcmus.edu.vn) | 0339763011 |

|  |  |  |  |
| --- | --- | --- | --- |
| **Bảng phân công & đánh giá hoàn thành công việc** | | | |
| **Công việc thực hiện** | **Người thực hiện** | **Mức độ hoàn thành** | **Đánh giá của nhóm** |
| Mã nguồn ứng dụng, giao diện | * Đinh Nguyễn Tấn Nguyên * Lê Văn Thi * Trương Thị Thu Thảo | Hoàn thành | 100% |
| Script DB | * Đinh Nguyễn Tấn Nguyên * Lê Văn Thi * Trương Thị Thu Thảo | Hoàn thành | 100% |
| Báo cáo | * Đinh Nguyễn Tấn Nguyên * Lê Văn Thi | Hoàn thành | 100% |
| Quay video demo | * Trương Thị Thu Thảo | Hoàn thành | 100% |

**YÊU CẦU ĐỒ ÁN**

|  |  |
| --- | --- |
| **Loại bài tập** | **🗹 Lý thuyết 🗹Thực hành 🗹 Đồ án Bài tập** |
| **Ngày kết thúc** | **11/04/2021** |

# **Yêu cầu của Đồ án:**

# **PHÂN HỆ 1: DÀNH CHO NGƯỜI QUẢN TRỊ CƠ SỞ DỮ LIỆU:** Sinh viên hãy xây dựng ứng dụng cho phép các người dùng có quyền quản trị thực hiện công việc sau:

1. Xem danh sách người dùng trong hệ thống.
2. Thông tin về quyền (privileges) của mỗi user/ role trên các đối tượng dữ liệu.
3. Cho phép tạo mới, xóa, sửa (hiệu chỉnh) user hoặc role.
4. Cho phép thực hiện việc cấp quyền: cấp quyền cho user, cấp quyền cho role, cấp role cho user. Quá trình cấp quyền có tùy chọn là có cho phép người được cấp quyền có thể cấp quyền đó cho user/ role khác hay không (có chỉ định WITH GRANT OPTION hay không). Quyền, select, update thì cho phép phân quyền tính đến mức cột; quyền insert, delete thì không.
5. Cho phép thu hồi quyền từ người dùng/ role.
6. Cho phép kiểm tra quyền của các chủ thể vừa được cấp quyền.
7. Cho phép chỉnh sửa quyền của user/ role.

# **Kết quả**

* + - 1. **User**

1. **Tablespace:**

* Một CSDL Oracle được chia thành những đơn vị lưu trữ luận lý được gọi là các tablespace, nhằm mục đích gom nhóm các cấu trúc luận lý có liên quan với nhau.
* Mỗi CSDL có 1 hoặc nhiều các tablespace. Mỗi tablespace chứa 1 hoặc nhiều các datafile. Datafile là các cấu trúc vật lý tương thích với hệ điều hành bên dưới, dùng để lưu trữ dữ liệu của các cấu trúc luận lý trong tablespace chứa nó. Kích thước tổng cộng của các datafile chính là dung tích lưu trữ tổng cộng của tablespace đó.
* Một CSDL có 2 tablespace SYSTEM và USERS.

1. **Có 2 loại tablespace:**

* System tablespace:

+ Mọi CSDL Oracle đều có 2 system tablespace là SYSTEM và SYSAUX, được tạo ra một cách tự động.

+ Chứa thông tin về các data dictionary views, các định nghĩa của stored procedures, packages, và các database triggers dưới dạng PL/SQL program units, SYSTEM rollback segment,…

+ Không nên chứa dữ liệu người dùng trong tablespace này mặc dù có thể.

* Non-system tablespace:

+ Dùng để chứa các loại dữ liệu còn lại, đặc biệt là các dữ liệu của người dùng.

1. Một cách phân loại khác của tablespace:

* Temporary tablespace: được sử dụng để dành riêng cho các thao tác sắp xếp dữ liệu.
* Permanent tablespace: Các tablespaces không phải là temporary tablespaces được gọi là các permanent tablespaces. Các permanent tablespace được sử dụng để lưu trữ dữ liệu trong database.

1. Schema:

* Schema là một tập hợp các đối tượng cơ sở dữ liệu (vd: table, view, index,…)
* Mỗi schema được sở hữu bởi một user và có cùng tên với user.
* Không có mối quan hệ nào giữa schema và tablespace. Các đối tượng thuộc 1 schema có thể nằm trên các tablespace khác nhau và 1 tablespace có thể chứa các đối tượng thuộc nhiều schema khác nhau
  + - 1. **User profile:**

1. **Profile:**

* Một profile là một tập hợp có tên của các giới hạn tài nguyên, được gán cho một hay nhiều user trong CSDL Oracle.
* Profile cung cấp một cách quản lý dễ dàng việc giới hạn tài nguyên. Nó giúp giới hạn việc sử dụng quá mức các tài nguyên của toàn hệ thống. Profile cũng là cách để quản lý các chính sách về password.
* Trong một CSDL có thể tạo nhiều profile. Một profile mặc định sẽ được dùng để gán cho những user không được gán profile một cách tường minh.
* Lưu ý rằng các giá trị mặc định đều được thiết lập là “unlimited”.

1. **Các loại tài nguyên:**

* Một profile có thể mô tả các loại giới hạn tài nguyên sau:

+ Số lượng các session đồng thời mà user có thể thực hiện.

+ Thời gian xử lý CPU cho một session của user đó hoặc cho một cuộc gọi (call) tới Oracle bởi 1 câu lệnh SQL.

+ Số lần đọc luận lý I/O cho một session của user đó hoặc cho một cuộc gọi (call) tới Oracle bởi 1 câu lệnh SQL.

+ Lượng thời gian nhàn rỗi cho session của user.

+ Lượng thời gian connect cho một session.

+ Các quy định về password (số lần cố gắng login thất bại, thời gian hiệu lực của 1 password,…)

* + - 1. **Quyền:**
* Một quyền là 1 sự cho phép thực hiện 1 câu lệnh SQL nào đó hoặc được phép truy xuất đến một đối tượng nào đó (vd: quyền tạo bảng CREATE TABLE, quyền connect đến cơ sở dữ liệu CREATE SESSION, quyền SELECT trên một bảng cụ thể nào đó,…)

+ Chỉ cấp cho user chính xác những 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): Là quyền thực hiện một tác vụ CSDL cụ thể hoặc quyền thực hiện một 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 có thể cấp 1 quyền hệ thống nếu có một 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 một đối tượng schema cụ thế.

Vd: quyền xóa các hàng 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 việc truy xuất đến các đối tượng schema cụ thể nào đó.

+ User có thể cấp 1 quyền đối tượng nếu có một trong các điều kiện sau:

+ User có tất cả mọi 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 đó với tùy chọn WITH GRANT OPTION.
  + - 1. **Role**
* Là một tập hợp bao gồm các quyền và các role khác.
* Role được gán cho các user hoặc các role khác.
* Role giúp cho việc quản trị người dùng dễ dàng và tiết kiệm công sức hơn.
* Có một số role có sẵn do hệ thống định nghĩa (VD: DBA, RESOURCE, CONNECT,…) nhưng đa phần các role là do người quản trị CSDL tạo ra.
* Role 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 role có thể bị xóa mà không ảnh hưởng đến role đó.
* User có thể cấp 1 role nếu có một trong các điều kiện sau:

+ User đã tạo ra role đó.

+ User đã được cấp role đó với tùy chọn WITH ADMIN OPTION.

+ User có quyền GRANT ANY ROLE

* + - 1. **Grant và Revoke**
* Grant được sử dụng để cấp quyền truy cập hoặc các đặc quyền với đối tượng cơ sở dữ liệu cho người dùng
* Revoke được sử dụng để thu hồi quyền truy cập của người dùng hoặc các đặc quyền với các đối tượng cơ sở dữ liệu