**ĐẠI HỌC QUỐC GIA THÀNH PHỐ HỒ CHÍ MINH**

**TRƯỜNG ĐẠI HỌC KHOA HỌC TỰ NHIÊN**

BỘ MÔN: AN TOÀN VÀ BẢO MẬT HỆ THỐNG THÔNG TIN

-----OO-----

**BÁO CÁO GIỮA KÌ**

**STANDARD AUDIT**

Giảng viên hướng dẫn:

* **GV: Phạm Thị Bạch Huệ**

Nhóm thực hiện: **Nhóm 29**

* 1612642: Tống Thị Cam Thảo
* 1612684: Trần Hồ Như Thủy

**01/06/2019**

**MỤC LỤC**

[**I.** **Standard Audit là gì?** 3](#_Toc10333218)

[**II.** **Cách kích hoạt Standard Audit:** 3](#_Toc10333219)

[**1.** **Thiết lập Audit với tham số DB:** 3](#_Toc10333220)

[**2.** **Thiết lập Audit với tham số DB, EXTENDED:** 5](#_Toc10333221)

[**3.** **Thiết lập Audit với tham số XML:** 6](#_Toc10333222)

[4. **Thiết lập Audit với tham số** XML,EXTENDED: 7](#_Toc10333223)

[**III.** **Nơi lưu trữ dữ liệu audit:** 8](#_Toc10333224)

1. **Standard Audit là gì?**

**Standard Audit (Kiểm soát chuẩn)** là cơ sở kiểm soát toàn diện và đầy đủ nhất trong cơ sở dữ liệu **Oracle**. Nó cho phép kiểm soát hành động (Action), loại hành động, đối tượng, đặc quyền (Privilege), user truy cập..

Có 2 giai đoạn liên quan đến sử dụng **Standard Audit**.

* Kích hoạt cơ chế kiểm soát (***Audit***).
* Xác định các chuyên mục (category) cần kiểm soát, tức là xác định các hành động nào sẽ được ghi lại dấu vết (Tạo ra **Audit Trail**).

**Audit trail**: bao gồm các bản ghi cho phép tìm những gì đã được thực hiện trong cơ sở dữ liệu.

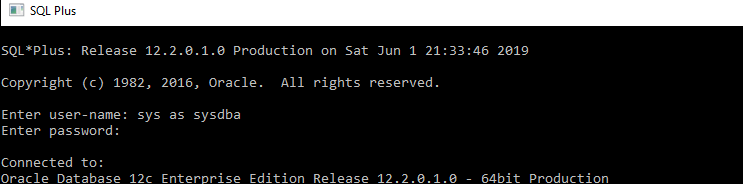
Căn cứ vào đó để biết những gì các user đã làm, và những đặc quyền nào đã sử dụng…

Đối với mỗi bản ghi có các thông tin quan trọng như:

* + Ai đã thực hiện
  + Thực hiện ở đâu (**Schema** nào hay **Object** nào)
  + Thực hiện khi nào.
  + Thực hiện như thế nào (Các câu lệnh SQL nào được thực hiện).
  + Cũng như các thông tin hữu ích khác trong việc điều tra giám sát.

1. **Cách kích hoạt Standard Audit:**

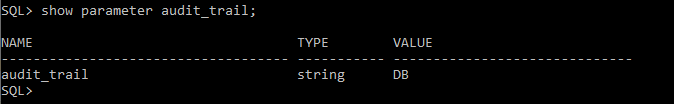
Để kích hoạt chế độ kiểm soát cơ sở dữ liệu, bạn cần truy cập vào **Oracle**với user có đặc quyền **sysdba**.



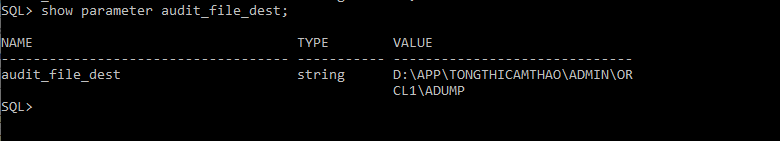
* + 1. **Thiết lập Audit với tham số DB:**
* Kích hoạt chế độ kiểm soát với tham số là **DB** ( **audit\_trail = DB**), thực hiện các lệnh dưới đây:

**Alter system set audit\_trail=db scope=spfile;**

* Kiểm tra thiết lập DB thành công hay không bằng câu lệnh:



* Kiểm tra vị trí file đích lưu kết quả Audit:



* Thực hiện kiểm soát (audit) bảng cho **Scott.EMP**, với tham số **DB:**

***Trước khi thực hiện bước này bạn phải kiểm tra mình đã có user Scott hay chưa? Trong user Scott đã có dữ liệu hay chưa (cụ thể của mình là bảng emp1).***

* **Nếu chưa có thì bạn thực hiện các bước sau:**

***create user scott identified by tiger;***

***grant all privileges to scott;***

***connect scott;***

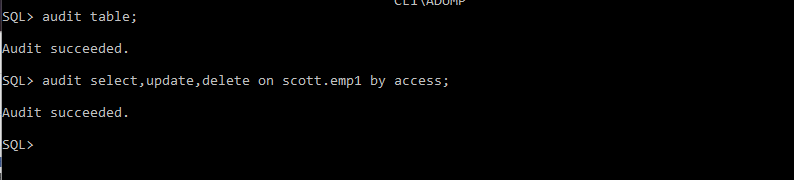
***--Tạo bảng EMP1 và Insert dữ liệu vào bảng EMP1***

**🡪 Connect trở lại user sys để thực hiện việc Audit:**

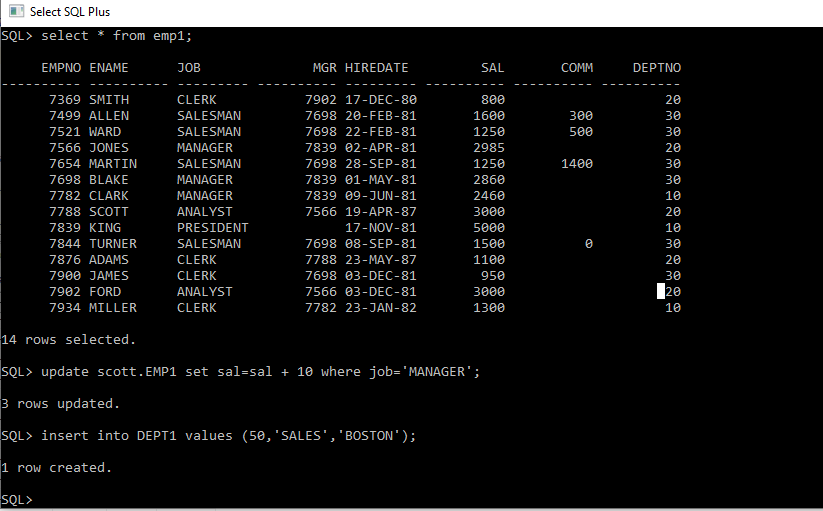
***Connect;***

***Username: sys as sysdba***

***pass:***

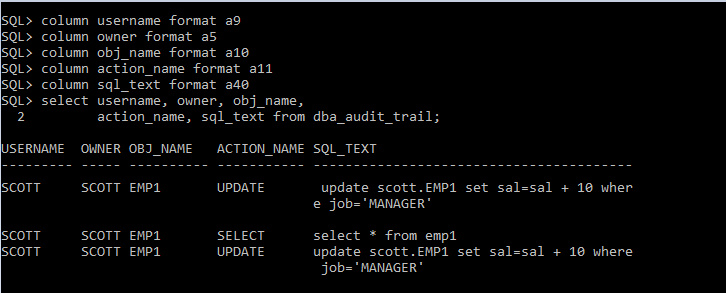


* Thực hiện một vài hành động trên bảng **Scott.EMP**, chẳng hạn **update**, insert, select:



* Truy vấn (query) bảng DBA\_AUDIT\_TRAIL để nhận được kết quả của Audit:

**Kết quả Audit:**



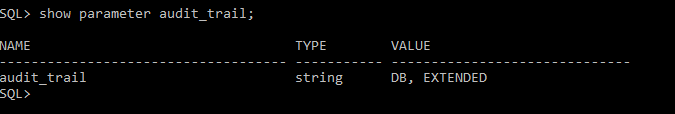
* + 1. **Thiết lập Audit với tham số DB, EXTENDED:**
* Để chuyển từ DB sang DB, EXTENDED dùng các câu lệnh sau:

***Alter system set audit\_trail=db, extended scope=spfile;***

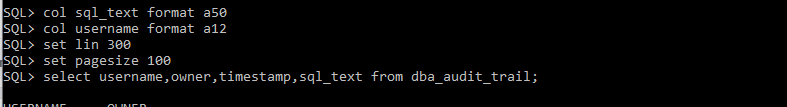
***Shu immediate;***

***Startup;***

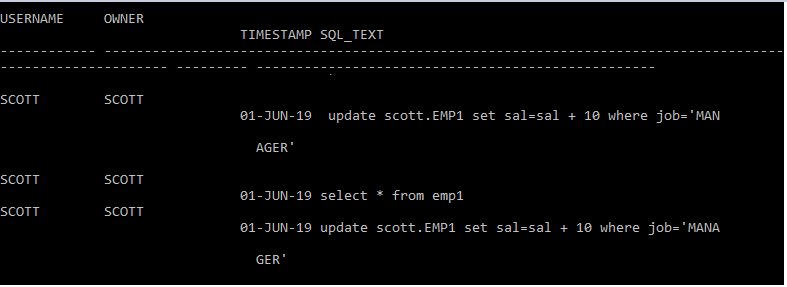
* Kiểm tra lại bằng lệnh:



* **Các bước còn lại làm tương tự như DB.**



**Kết quả Audit:**

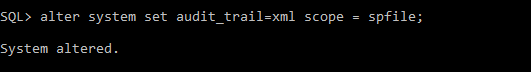


* + 1. **Thiết lập Audit với tham số XML:**
* Chuyển đổi thông số thành XML bằng câu lệnh:

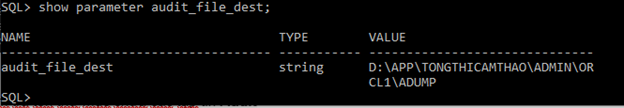
***Alter system set audit\_trail=XML scope=spfile;***

***Shu immediate;***

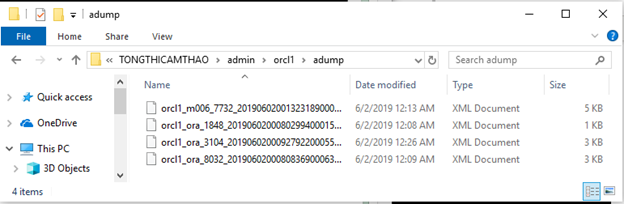
***Startup;***



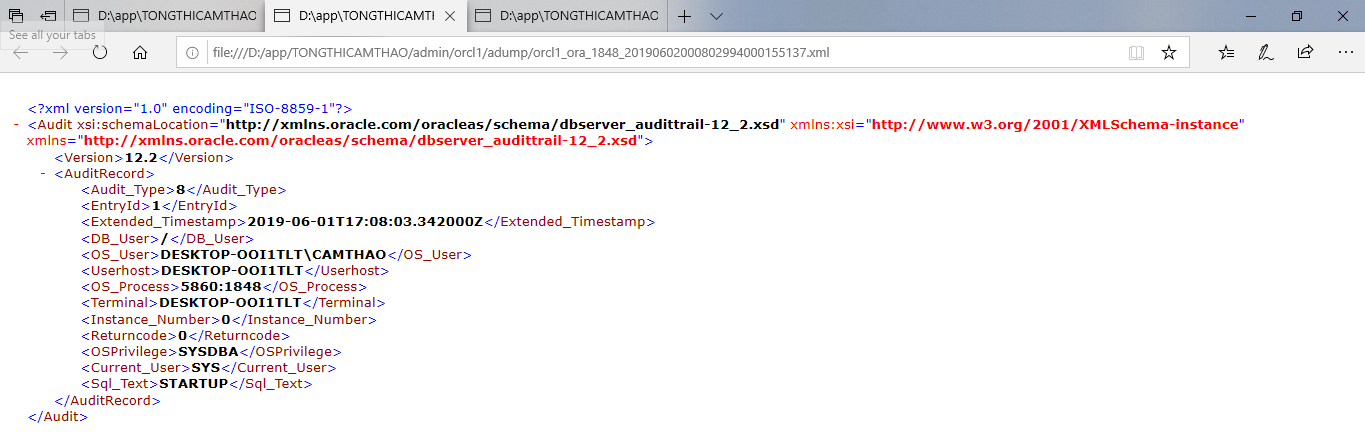
* Khác với DB và DB, EXTENDED lưu kết quả Audit ở bảng AUD$ thì XML sẽ lưu kết quả Audit thành 1 tập tin và sẽ lưu ở vị trí theo đường link như phía dưới:



* Các file kết quả sẽ được hiển thị như sau:



* Nội dung file kết quả Audit:



* + 1. **Thiết lập Audit với tham số XML,EXTENDED:**
* Chuyển đổi thông số thành XML,EXTENTDED bằng câu lệnh:

***Alter system set audit\_trail=os scope=spfile;***

***Shu immediate;***

***Startup;***



* Vị trí file lưu kết quả tương tự như XML:
* Nội dung file kết quả:

Nhóm chưa tìm được sự khác nhau giữa XML và XML,EXTENDED

1. **Nơi lưu trữ dữ liệu audit:**

|  |  |
| --- | --- |
| **Tham số** | **Giải thích** |
| **DB** | Dấu vết được lưu trữ trong bảng **AUD$**, chỉ chứa lệnh (statement) không phải văn bản đầy đủ. |
| **DB, EXTENDED** | Dấu vết được lưu trữ trong bảng **AUD$**, văn bản đầy đủ (Giá trị các biến (variable) đối với mỗi bản ghi..) |
| **XML** | Dấu vết được lưu trữ trên tập tin của hệ điều hành, theo định dạng **XML**, nội dung giống tham số **DB**. |
| **XML, EXTENDED** | Dấu vết được lưu trữ trên tập tin của hệ điều hành, theo định dạng **XML**, nội dung giống tham số **DB,EXTENDED**. |