Chương 6:
Kiểm toán và Giải trình
(**Audit and Accountability**)

Khoa Khoa học và Kỹ thuật Máy tính
Đại học Bách Khoa Tp.HCM

Nội dung

1. Giới thiệu Kiểm toán và Giải trình
2. Kỹ thuật kiểm toán trong cơ sở dữ liệu
3. Case study: kiểm toán trong Oracle

Giới thiệu Kiểm toán và Giải trình

- ***Kiểm toán (Audit)*** *:* giám sát và ghi lại những hoạt động đã và đang xảy trong hệ thống một cách có chọn lọc.
- Audit = *Ai làm gì với dữ liệu nào khi nào và bằng cách nào*

  (Who did what to which data when and how)
- ***Trách nhiệm giải trình, gọi tắt là giải trình (Accountability)****:* trách nhiệm tìm ra và chứng minh nguồn gốc các hoạt động xảy ra trong hệ thống.
- Hoạt động kiểm toán nhằm phục vụ cho hoạt động giải trình

Tại sao phải kiểm toán?

- **Trách nhiệm giải trình** từ những hành động xảy ra lên các dữ liệu (schema, bảng, dòng, …)
- Kiểm tra **hành động đáng ngờ** (suspicious activity)
  - Ví dụ xóa dữ liệu từ một bảng
- Thông báo nếu có nếu người dùng không được ủy quyền nhưng lại thao tác trên dữ liệu mà đòi hỏi phải có đủ quyền truy cập (**truy cập vượt quyền**)

Tại sao phải kiểm toán?

- Giám sát và ghi lại các hoạt động xảy ra nhằm **phát hiện các vấn đề** trong quá trình định quyền và điều khiển truy cập
- Thống kê tình hình truy xuất tài nguyên để có biện pháp **cải thiện hiệu suất**
  - Ví dụ: dựa vào các trường, bảng thường hay được truy cập

    → chọn cách đánh chỉ mục thích hợp để tăng hiệu suất.
- Kiểm toán để thỏa các yêu cầu chính sách pháp lý (compliance): thể hiện trách nhiệm với dữ liệu của khách hàng

Các chính sách (Compliances)

- Các chính sách đưa ra các quy định cần phải tuân thủ và các hướng dẫn cần thiết khi kiểm toán
- Một số chính sách:
  - Health Insurance Portability and Accountability Act (HIPAA)
  - Sarbanes-Oxley Act
  - Graham-Leach-Bliley Act (GLBA)
- Các chính sách thường không mô tả công nghệ cần thực thi
  - Cần xác định yêu cầu và lựa chọn công nghệ

Khi nào và kiểm toán những gì?

- Khi nào nên kiểm toán?
  - Kiểm toán tại mọi thời điểm từ khi hệ thống bắt đầu hoạt động
- Kiểm toán những gì?
  - Việc kiểm toán có thể làm giảm hiệu suất của hệ thống
  - Chỉ nên kiểm toán những gì cần thiết

Khi nào và kiểm toán những gì?

- Trong chính sách Sarbanes-Oxley, phần 404 có đưa ra những hoạt động cần phải kiểm toán:
  - Hoạt động của những người dùng có quyền
  - Đăng nhập và đăng xuất
  - Những thay đổi trong các application trigger và data trigger
  - Thay đổi quyền và mô tả thông tin của người dùng
  - Cấu trúc dữ liệu bị thay đổi
  - Các truy cập đọc và ghi trên những dữ liệu nhạy cảm
  - Những lỗi và ngoại lệ
  - Nguồn gốc của những hoạt động truy cập dữ liệu
  - Thời gian, tên chương trình, kích thước dữ liệu, câu lệnh …

Quy trình kiểm toán

- Quy trình kiểm toán do NIST đưa ra

1. Phân tích các yêu cầu bảo mật của ứng dụng
2. Chọn các sự kiện/hoạt động/đối tượng sẽ kiểm toán
3. Giám sát và ghi nhận
4. Lưu trữ audit log (nhật ký kiểm toán)
5. Kiểm tra và phân tích audit log
6. Phản hồi

Các vấn đề với kiểm toán

- Kiểm toán là công cụ, không phải là mục tiêu
- Nên sử dụng kết hợp giữa kiểm toán bên trong và kiểm toán bên ngoài
- Lưu trữ và bảo mật thông tin audit log
- Tự động hóa và giám sát hoạt động kiểm toán
- Kích thước của các audit log lớn, cần sử dụng các công cụ kho dữ liệu (data warehouse) và khai phá dữ liệu (data mining) để quản lý và phân tích dữ liệu audit log
- Vấn đề tính riêng tư trong audit log

Nội dung

1. Giới thiệu về điều khiển truy cập bắt buộc
2. Kỹ thuật kiểm toán trong cơ sở dữ liệu
3. Case study: kiểm toán trong Oracle

Các yêu cầu của kiểm toán trong CSDL

- Có khả năng hoạt động độc lập, cho phép theo dõi và ghi nhận lại tất cả các hoạt động trong hệ thống kể cả những hoạt động của người quản trị hệ thống.
- Có khả năng lưu trữ audit log một cách an toàn bên ngoài CSDL
- Có khả năng thu thập và kết hợp các hoat động xảy ra ở nhiều loại DBMS (Database management systems) khác nhau.
  - Không phụ thuộc vào DBMS và cú pháp câu lệnh SQL ứng với mỗi DBMS

Các yêu cầu của kiểm toán trong CSDL

- Có khả năng ngăn chặn người quản trị hệ thống chỉnh sửa hoặc xóa dữ liệu trong audit log.
- Có khả năng đưa ra những cảnh báo kịp thời cho người quản trị hệ thống khi có những bất thường xảy ra trong hệ thống

Các phương pháp kiểm toán

- Kiểm toán bằng application server log
- Kiểm toán mức ứng dụng (Application audit)
- Kiểm toán bằng trigger
- Kiểm toán bằng câu lệnh (command)

Các đối tượng cần kiểm toán

- Các hoạt động đăng nhập/đăng xuất trong CSDL
  - Username
  - Client IP mà đăng nhập không thành công
  - Chương trình (source program)
  - Thời gian đăng nhập và đăng xuất
- Kiểm toán nguồn gốc truy cập CSDL
  - Địa chỉ IP và host name được dùng để kết nối CSDL
  - Chương trình nào kết nối CSDL

Các đối tượng cần kiểm toán

- Kiểm toán các hoạt động truy cập CSDL ngoài giờ làm việc
  - Các truy cập CSDL ngoài giờ làm việc đều đáng nghi ngờ
  - Cần ghi lại mọi truy cập CSDL ngoài giờ làm việc trừ những thao tác đã được định giờ
- Kiểm toán các thao tác thuộc ngôn ngữ định nghĩa dữ liệu (Data Definition Language – DDL)
  - Rất quan trọng vì trong nhiều trường hợp DDL có thể được dùng để phá hoại hệ thống
  - Được quy định trong chính sách HIPAA
  - Phương pháp: dùng chức năng built-in của DBMS, sử dụng hệ thống kiểm toán bên ngoài, so sánh snapshot của lược đồ (shema) theo thời gian

Các đối tượng cần kiểm toán

- Các lỗi trong thao tác với CSDL
  - Các lỗi như đăng nhập thất bại, SQL Injection

    → dấu hiệu của sự tấn công
  - Các ứng dụng có thể chứa lỗi và gây ra lỗi: ví dụ sinh ra những câu SQL sai cú pháp

    → Có thể bị lợi dụng để tấn công

    → Sửa lỗi ứng dụng
- Kiểm toán trên sự thay đổi mã nguồn của trigger và stored procedure
  - Kẻ tấn công có thể giấu những đoạn mã độc hại vào trigger hay stored procedure

Các đối tượng cần kiểm toán

- Kiểm toán trên sự thay đổi quyền của người dùng và các thuộc tính bảo mật khác
  - Việc kiểm toán này là bắt buộc: tấn công vượt quyền
  - Các thông tin cần chú ý:
    - Thêm/Xóa trên User/Login/Role
    - Thay đổi quyền của Role
    - Thay đổi quyền hoặc role của người dùng
    - Thay đổi password

Các đối tượng cần kiểm toán

- Kiểm toán sự thay đổi của các dữ liệu nhạy cảm
  - Ghi nhận thay đổi giữa giá trị cũ và giá trị mới trong mỗi thao tác thuộc ngôn ngữ thao tác dữ liệu (Data Manipulation Language – DML)
  - Cần lọc dữ liệu nào quan trọng mới kiểm toán vì dữ liệu kiểm toán sẽ rất lớn (ví dụ: CSDL có 100 bảng với khoảng 1 triệu transaction/ngày…)
- Kiểm toán sự thay đổi của audit log
  - Audit log cần được bảo vệ và không cho phép thay đổi
  - Phương pháp: sử dụng các chức năng built-in của CSDL hoặc một hệ thống kiểm toán bên ngoài khác

Nội dung

1. Giới thiệu về điều khiển truy cập bắt buộc
2. Kỹ thuật kiểm toán trong cơ sở dữ liệu
3. Case study: kiểm toán trong Oracle

Kiểm toán trong Oracle

- Giới thiệu
- Các loại kiểm toán
- Các công cụ kiểm toán trong Oracle
- Kết luận

Giới thiệu

- Oracle kiểm toán các người dùng:
  - Kiểm toán các truy cập thành công hoặc không thành công
  - Kiểm toán 1 người dùng, 1 nhóm người dùng hoặc tất cả các người dùng
  - Kiểm toán ở cấp phiên làm việc (session level) hoặc cấp truy cập (access level).
- Kiểm toán sẽ làm giảm hiệu suất của hệ thống
- Chỉ nên kiểm toán những gì cần thiết

Giới thiệu

- Dữ liệu kiểm toán nên được ghi trên file của hệ điều hành (OS) để tiết kiếm tài nguyên của CSDL
- Các tham số khởi tạo AUDIT_TRAIL trong init.ora

Giá trị tham số	Diễn giải
DB (default)	Audit DB và ghi dữ liệu vào bảng SYS.AUD$
DB_EXTENDED	Giống DB và lưu thêm cột SQL Binding và SQL text vào SYS.AUD$
XML	Audit DB và ghi dữ liệu vào file XML của OS
XML_EXTENDED	Giống XML và lưu thêm SQL bind và cột SQL Text
OS (*)	Audit DB và ghi vào file của OS

Kiểm toán trong Oracle

- Giới thiệu
- **Các loại kiểm toán**
- Các công cụ kiểm toán trong Oracle
- Kết luận

Các loại kiểm toán trong Oracle

- Statement Auditing
- Privilege Auditing
- Schema Object Auditing

Statement Auditing

- **Statement auditing:** kiểm toán những *lệnh hoặc nhóm câu lệnh trên từng đối tượng*
- DDL: AUDIT TABLE sẽ kiểm toán mọi lệnh *Create và Drop* liên quan đến Table
- DML: AUDIT SELECT TABLE sẽ kiểm toán mọi lệnh *Select ... From Table/View*
- Có thể kiểm toán trên mọi người dùng hoặc trên 1 nhóm người dùng cụ thể hoặc trên Role

Privilege Auditing

- **Privilege auditing:** kiểm toán **những quyền hệ thống**
  - AUDIT SELECT ANY TABLE sẽ kiểm toán mọi lệnh được tạo ra từ những người dùng sử dụng quyền SELECT ANY TABLE
- Trường hợp cả statement và privilege cùng được kiểm toán thì chỉ 1 audit record được tạo ra.
- Privilege auditing có độ tập trung hơn statement auditing
  - Statement auditing: AUDIT TABLE

    → CREATE, ALTER, DROP (TABLE) đều được kiểm toán
  - Privilege auditing: AUDIT CREATE TABLE

    → chỉ kiểm toán câu lệnh CREATE (TABLE)

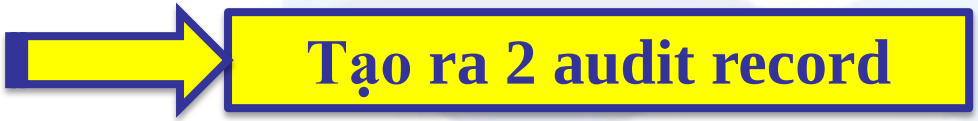
Schema Object Auditing

- Kiểm toán trên những đối tượng của Schema:
  - Table
  - View
  - Procedure
  - Trigger
  - Function
  - Package
- Privilege auditing có độ ưu tiên thấp hơn các schema object auditing

Schema Object Auditing

- Ví dụ:

```
-- Thực hiện kiểm toán câu lệnh SELECT trên Employee
AUDIT SELECT ON Employee;
--Tạo view Emp_Name và kiểm toán câu lệnh SELECT
CREATE VIEW Emp_Name AS
    SELECT EName
    FROM Employee;
AUDIT SELECT ON Emp_Name;
--Thực hiện câu lệnh truy vấn trên view Emp_Name
SELECT * FROM Employee_Name;
```



Kiểm toán trong Oracle

- Giới thiệu
- Các loại kiểm toán
- **Các công cụ kiểm toán trong Oracle**
- Kết luận

Các công cụ kiểm toán trong Oracle

- Oracle audit
- Kiểm toán bằng trigger
- Fine-Grained Auditing

Oracle Audit

- Dùng câu lệnh AUDIT
- Có thể kiểm toán tất cả các quyền gán cho người dùng hoặc role trong CSDL
- Bao gồm: các truy cập đọc, ghi và xóa trên các bảng dữ liệu

Cú pháp câu lệnh kiểm toán

```
Audit
    {statement_option | privilege_option}
    [by user]
    [by {session|access}]
    [whenever {successful | unsuccessful}]
```

- Trong đó, `statement_option` và `privilege_option` là phần bắt buộc, và các phần khác thì không bắt buộc.

Ví dụ

```
AUDIT SESSION BY Scott;

AUDIT DROP ANY TABLE;

AUDIT SELECT, INSERT, DELETE
    ON Test.Table1
    BY ACCESS
    WHENEVER SUCCESSFUL;
```

Kiểm toán bằng trigger

- System trigger: Trigger được tự động thực thi khi có các sự kiện của hệ thống xảy ra
  - Khởi động hoặc tắt CSDL
  - Đăng nhập hoặc đăng xuất
  - Tạo, chỉnh sửa hoặc xóa các đối tượng của lược đồ
- Trigger CSDL:
  - Trigger trên các câu lện Update, Delete, Insert
  - Các trigger CSDL có thể ghi lại các thay đổi ở cấp hàng và cột của bảng dữ liệu
  - Các truy cập đọc (SELECT) không thể được ghi lại bằng các trigger CSDL thông thường

Fine-Grained Auditing – FGA

- Fine-Grained Auditing do package DBMS_FGA quản lý
- Kiểm toán những truy cập dữ liệu dựa theo nội dung.
- Kiểm toán được đến cấp hàng và cột.
- Các câu lệnh INSERT, UPDATE, DELETE thường được kiểm toán. Câu lệnh SELECT ít được kiểm toán hơn cho chi phí cao (được sử dụng thường xuyên)
- FGA cung cấp 1 giao diện cho phép kiểm toán lệnh SELECT. Khi có 1 record trong tập records trả về thỏa điều kiện cho trước thì 1 record audit mới được tạo ra.

Fine-Grained Auditing – FGA

- Ví dụ: Audit trên cột EMP.SAL

```
BEGIN
  DBMS_FGA.add_policy
  (
  object_schema => 'AUDIT_TEST',
  object_name => 'EMP',
  policy_name => 'SALARY_AUDIT',
  audit_condition => 'SAL > 50000',
  audit_column => 'SAL',
  statement_types =>'SELECT, INSERT, UPDATE,
     DELETE'
  );
END;
```

Kết quả kiểm toán

- Trường hợp Statement, Privilege, Schema Object
  - Kết quả trả về trong bảng **Sys.Aud$**
  - View: **dba_audit_trail**
- Trường hợp Fine-Grained Audit
  - Kết quả trả về trong bảng **fga_log$**
  - View: **dba_fga_audit_trail**
- Trường hợp lưu file OS
  - Lưu thành file XML trong thư mục **$Oracle\orcl\adump**

Các lưu ý với AUD$

- Kiểm soát kích thước và sự phát triển của AUDIT_TRAIL
  - AUD$ nằm trong SYSTEM tablespace
  - Tấn công kiểu DOS có thể làm đầy SYSTEM tablespace, và làm cho CSDL không thể hoạt động được
  - Số record trong AUD$ phụ thuộc vào 2 yếu tố: số kiểm toán được bật lên và tần suất thực thi của các thao tác được kiểm toán
- Giải pháp:
  - Kiểm toán có chọn lọc
  - Lưu file audit trên file OS
  - Di chuyển các record trong AUD$ ra ngoài nếu AUD$ quá lớn

Bảo vệ AUDIT TRAIL

- Chỉ cấp quyền DELETE ANY TABLE hoặc DELETE trên Sys.Aud$ cho những người dùng tin cậy
- Kiểm toán chính Sys.Aud$

```
AUDIT INSERT UPDATE DELETE
    ON sys.aud$
    BY ACCESS;
```

Kiểm toán trong Oracle

- Giới thiệu
- Các loại kiểm toán
- Các công cụ kiểm toán trong Oracle
- **Kết luận**

Kết luận

- Thực hiện và duy trì việc kiểm toán là một trong các bước quan trọng đảm bảo sự an toàn cho hệ thống
- Kiểm toán giúp phát hiện vấn đề chứ không giải quyết vấn đề
- Kiểm toán nhiều sẽ làm giảm hiệu suất của hệ thống nên cần có chính sách kiểm toán hợp lý:
  - Chọn lọc các đối tượng và sự kiện cần kiểm toán
  - Bảo vệ dữ liệu kiểm toán
  - Quản lý kích thước của audit log
  - Phân tích dữ liệu kiểm toán thường xuyên để sớm phát hiện vấn đề

Nội dung

1. Giới thiệu về điều khiển truy cập bắt buộc
2. Kỹ thuật kiểm toán trong CSDL
3. Kiểm toán trong Oracle