CHƯƠNG 6. KIỂM TOÁN TRONG CƠ SỞ DỮ LIỆU

TS. Trần Thị Lượng
* Khoa An toàn thông tin *

MỤC TIÊU

- **Kiến thức:**
  - Hiểu và trình bày được các kiến thức cơ bản về kiểm toán CSDL, các loại kiểm toán, các cơ chế kiểm toán, kiến trúc kiểm toán CSDL.
- **Kỹ năng:**
  - Triển khai được một số loại kiểm toán cơ bản trong Oracle, SQL Server.

TÀI LIỆU THAM KHẢO

- [1] TS. Nguyễn Nam Hải, TS. Lương Thế Dũng, ThS. Trần Thị Lượng, *Giáo trình An toàn cơ sở dữ liệu,* Học viện Kỹ thuật Mật mã, 2013.
- [2] Ron Ben Natan, *Implementing Database Security and Auditing,* Elsevier, 2005.
- [3] Alfred Basta, Melissa Zgola, *Database Security*, Cengage Learning US, 2011.
- [4] Ravi S. Sandhu, Sushil Jajodia, *Data and database security and controls*, Handbook of Information Security Management, Auerbach Publishers, 1993, pages 481-499.
- [5] Scott Gaetjen, David Knox, William Maroulis, "*Oracle database 12c security",* Oracle Press, 2015.

NỘI DUNG

1. Tổng quan về kiểm toán
2. Các loại kiểm toán
3. Kiến trúc kiểm toán
4. Cơ chế kiểm toán trong Oracle và SQL Server

NỘI DUNG

1. Tổng quan về kiểm toán
2. Các loại kiểm toán
3. Kiến trúc kiểm toán
4. Cơ chế kiểm toán trong Oracle và SQL Server

TỔNG QUAN VỀ KIỂM TOÁN

- Các định nghĩa
- Vai trò của kiểm toán
- Các cơ chế kiểm toán

CÁC ĐỊNH NGHĨA

- Kiểm toán (Auditing): là toàn bộ các hoạt động giám sát và ghi lại những gì xảy đến cho một hệ thống thông tin.
- Thông tin được ghi lại:
  - Các hoạt động bên trong hệ thống (Internal)
  - Tương tác giữa hệ thống và người dùng (External). Trả lời cho các câu hỏi:
    - Ai?
    - Từ đâu?
    - Làm gì? Vào lúc nào?....

CÁC ĐỊNH NGHĨA

- Kiểm toán CSDL (database auditing): là việc theo dõi và ghi lại các hành động được lựa chọn trên CSDL. Nó có thể dựa trên hành động của cá nhân, chẳng hạn như các loại câu lệnh SQL, hoặc kết hợp các yếu tố bao gồm tên, ứng dụng, thời gian, v.v…
- Nhật ký kiểm toán (audit log): là tài liệu chứa tất cả các hoạt động đang được kiểm toán và được sắp xếp theo thứ tự thời gian.
- Kiểm toán viên (auditor): là người được phép thực hiện công việc kiểm toán.

CÁC ĐỊNH NGHĨA

Một số định nghĩa khác:

- Thủ tục kiểm toán (audit procedure)
- Báo cáo kiểm toán (audit report)
- Các bản ghi kiểm toán (audit records)
- Vết kiểm toán (audit trail)
- Dữ liệu kiểm toán (audit data)
- Kiểm toán nội bộ (internal auditing)
- Kiểm toán mở rộng (external auditing)

=> Kiểm toán giúp cho DBA kiểm soát hoạt động của hệ thống tốt hơn, tuy nhiên cần kiểm toán đúng mức để không làm ảnh hưởng đến hiệu suất hệ thống.

TỔNG QUAN VỀ KIỂM TOÁN

- Các định nghĩa
- Vai trò của kiểm toán
- Các cơ chế kiểm toán

VAI TRÒ CỦA KIỂM TOÁN

- Mục đích của kiểm toán là xem xét và đánh giá tính sẵn sàng, tính an toàn và tính chính xác thông qua việc trả lời những câu hỏi như:
  - Hệ thống máy tính có sẵn sàng cho hoạt động tại mọi thời điểm hay không?
  - Liệu môi trường CSDL có phải chỉ những người có thẩm quyền mới được sử dụng không?
  - Liệu môi trường CSDL đã cung cấp thông tin chính xác, trung thực và kịp thời hay chưa?

VAI TRÒ CỦA KIỂM TOÁN

Kiểm toán thường được sử dụng để:

- Theo dõi các hành động hiện tại trong một lược đồ, bảng, hàng, cột hoặc một nội dung dữ liệu cụ thể.
- Giúp người giám sát thấy được nếu có người sử dụng bất hợp pháp đang thao tác với CSDL.
- Điều tra hoạt động đáng ngờ.
- Theo dõi và thu thập dữ liệu về các hoạt động CSDL cụ thể.

Kiểm toán bắt buộc người dùng phải có trách nhiệm về hành động mà họ thực hiện, bằng cách theo dõi hành vi của họ.

TỔNG QUAN VỀ KIỂM TOÁN

- Các định nghĩa
- Vai trò của kiểm toán
- Các cơ chế kiểm toán

CÁC CƠ CHẾ KIỂM TOÁN

Các cơ chế kiểm toán cơ bản trong CSDL bao gồm:

- Kiểm toán bắt buộc (Mandatory auditing)
- Kiểm toán chuẩn (Standard database auditing)
- Kiểm toán dựa trên giá trị (Value-based auditing)
- Kiểm toán mịn (Fine-grained auditing- FGA):
- Kiểm toán DBA:

CÁC CƠ CHẾ KIỂM TOÁN

Các cơ chế kiểm toán cơ bản trong CSDL bao gồm:

- Kiểm toán bắt buộc (Mandatory auditing):
  - Là các hoạt động kiểm toán mặc định.
  - Dù CSDL kiểm toán có được kích hoạt hay không, thì hệ thống vẫn kiểm tra một số hoạt động liên quan đến CSDL và ghi chúng vào tập tin vận hành hệ thống kiểm toán.

  => Đây được gọi là kiểm toán bắt buộc.

CÁC CƠ CHẾ KIỂM TOÁN

Các cơ chế kiểm toán cơ bản trong CSDL bao gồm:

- Kiểm toán chuẩn (Standard database auditing):
  - Đây là thiết lập kiểm toán ở cấp độ hệ thống bằng cách sử dụng những tham số AUDIT_TRAIL.
  - Sau khi kích hoạt tính năng kiểm toán này, cần lựa chọn các đối tượng và đặc quyền muốn kiểm toán.

CÁC CƠ CHẾ KIỂM TOÁN

- Kiểm toán dựa trên giá trị (Value-based auditing): Là loại kiểm toán dựa trên kiểm toán chuẩn, tuy nhiên nó còn kiểm toán dựa trên giá trị thực tế đã được đưa vào, cập nhật, hoặc bị xóa.
- Kiểm toán mịn (Fine-grained auditing- FGA): FGA mở rộng từ kiểm toán chuẩn, ghi lại các câu lệnh SQL đã được thực hiện thay vì chỉ những sự kiện đã xảy ra.
- Kiểm toán DBA: Thực hiện kiểm toán riêng cho các DBA.

NỘI DUNG

1. Tổng quan về kiểm toán
2. Các loại kiểm toán
3. Kiến trúc kiểm toán
4. Cơ chế kiểm toán trong Oracle và SQL Server

CÁC LOẠI KIỂM TOÁN

- Kiểm toán đăng nhập/đăng xuất CSDL
- Kiểm toán nguồn sử dụng CSDL
- Kiểm toán việc sử dụng CSDL ngoài giờ làm việc
- Kiểm toán câu lệnh DDL
- Kiểm toán câu lệnh DML
- Kiểm toán lỗi CSDL
- Kiểm toán các thay đổi với nguồn của các thủ tục và trigger

KIỂM TOÁN ĐĂNG NHẬP/ ĐĂNG XUẤT CSDL

- Đây là loại kiểm toán đầu tiên được yêu cầu trong hầu hết các môi trường nhằm tạo vết kiểm toán đầy đủ xem bất kỳ ai đã đăng nhập/đăng xuất vào CSDL.
- Nó ghi lại hai sự kiện cho loại kiểm toán này: một sự kiện cho việc đăng nhập và một sự kiện cho việc đăng xuất.
- Đối với mỗi sự kiện như vậy, cần phải lưu ít nhất hai tham số là *tên đăng nhập* và *thời gian đăng nhập*.

KIỂM TOÁN ĐĂNG NHẬP/ ĐĂNG XUẤT CSDL

- Ngoài ra, cũng nên ghi lại tất cả các đăng nhập thất bại. Việc đăng nhập không thành công thường được sử dụng làm cơ sở cho các cảnh báo và thậm chí là việc khóa tài khoản sau này.
- Xem xét dựa trên các yếu tố:
  - Tên người sử dụng.
  - IP của máy khách từ nơi kết nối không thành công.
  - Chương trình nguồn.
  - Thời gian nguồn.

KIỂM TOÁN ĐĂNG NHẬP/ ĐĂNG XUẤT CSDL

- Hoạt động đăng nhập và đăng xuất có thể kiểm toán bằng hai cách:
  - Tính năng CSDL bên trong
  - Giải pháp an toàn CSDL bên ngoài

KIỂM TOÁN ĐĂNG NHẬP/ ĐĂNG XUẤT CSDL

- Trigger để kiểm toán đăng nhập bên trong CSDL:
  - Đầu tiên, tạo bảng nơi lưu trữ các thông tin
  - Tạo một bảng chứa thông tin kiểm toán

```
SQL> create table user_login_audit(
  2  user_id    varchar2(30),
  3  session_id number(8),
  4  host       varchar2(30),
  5  login_day  date,
  6  login_time varchar2(10),
  7  logout_day date,
  8  logout_time        varchar(10)
  9  );

Table created.
```

KIỂM TOÁN ĐĂNG NHẬP/ ĐĂNG XUẤT CSDL

– Tiếp theo, tạo Trigger để khởi tạo khi đăng nhập mới.

```
SQL> create or replace trigger user_login_audit_trigger
  2  AFTER LOGON ON DATABASE
  3  BEGIN insert into user_login_audit values(
  4  user,
  5  sys_context('USERENV','SESSIONID'),
  6  sys_context('USERENV','HOST'),
  7  sysdate,   to_char(sysdate, 'hh24:mi:ss'),
  8  null,
  9  null );
 10  COMMIT;
 11  END;
 12  /

Trigger created.

SQL>
```

KIỂM TOÁN ĐĂNG NHẬP/ ĐĂNG XUẤT CSDL

– Ngày và giờ đăng xuất được lưu trữ khi sử dụng Trigger khởi tạo người sử dụng đăng xuất:

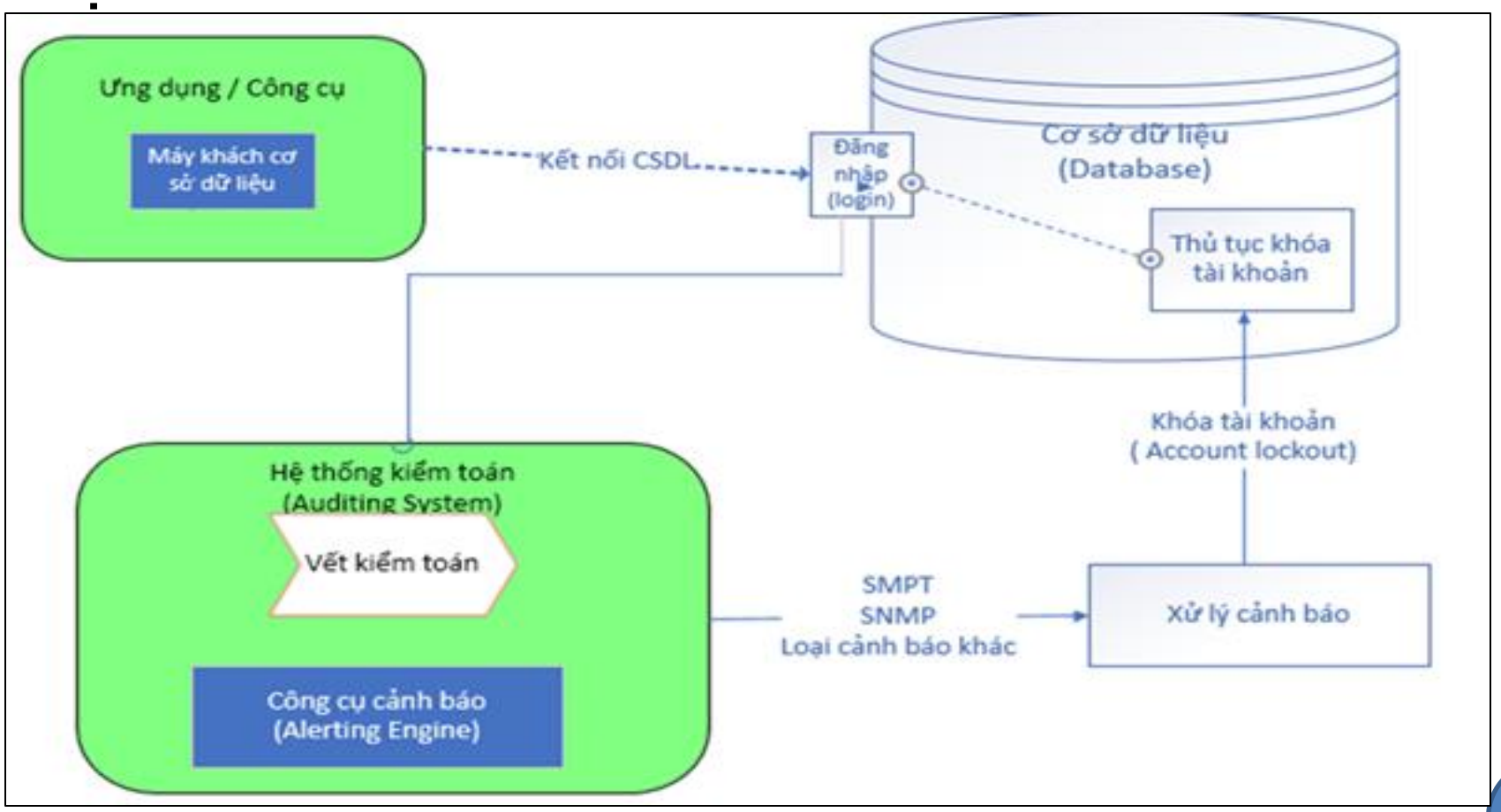
```
SQL> create or replace trigger
  2  user_logout_audit_trigger
  3  BEFORE LOGOFF ON DATABASE
  4  BEGIN
  5  -- logout day
  6  update
  7  user_login_audit
  8  set
  9  logout_day = sysdate
 10  where  sys_context('USERENV','SESSIONID')= session_id;
 11  -- logout time
 12  update
 13  user_login_audit
 14  set
 15  logout_time = to_char(sysdate, 'hh24:mi:ss')
 16  where
 17  sys_context('USERENV','SESSIONID') = session_id;
 18  COMMIT;
 19  END;
 20  /

Trigger created.
```

KIỂM TOÁN ĐĂNG NHẬP/ ĐĂNG XUẤT CSDL

- Thực hiện cảnh cáo hoặc khóa tài khoản dựa trên đăng nhập không thành công yêu cầu hỗ trợ từ nhà cung cấp cơ sở dữ liệu hoặc giải pháp an toàn cơ sở dữ liệu.
- Khi sử dụng một hệ thống an toàn bên ngoài, có thể dùng tường lửa SQL để chặn bất kỳ kết nối nào sau khi một số lượng lần nhất định cố gắng đăng nhập thất bại. Trong trường hợp này, CSDL có thể không được kết nối vì nó sẽ bị từ chối ở cấp tường lửa.

KIỂM TOÁN ĐĂNG NHẬP/ ĐĂNG XUẤT CSDL

- Một tùy chọn khác là sử dụng các thủ tục cơ sở dữ liệu.



KIỂM TOÁN ĐĂNG NHẬP/ ĐĂNG XUẤT CSDL

- Ngoài việc tạo ra một vết kiểm toán, thông tin đăng nhập có thể được dùng để tạo ra một dòng cơ sở (Baseline) có thể giúp trong việc xác định các bất thường.
- Có thể phân loại địa điểm đăng nhập mạng, tên người sử dụng, các chương trình mã nguồn, và thời gian trong ngày, dòng cơ sở có thể tương tự như sau:

```
user1          192.168.1.168       JDBC       24Hrs.

user2          192.168.X.X         Excel    Normal Business Hours (9-5)

user3          10.10.10.x          isql             Weekends
```

CÁC LOẠI KIỂM TOÁN

- Kiểm toán đăng nhập/đăng xuất CSDL
- Kiểm toán nguồn sử dụng CSDL
- Kiểm toán việc sử dụng CSDL ngoài giờ làm việc
- Kiểm toán câu lệnh DDL
- Kiểm toán câu lệnh DML
- Kiểm toán lỗi CSDL
- Kiểm toán các thay đổi với nguồn của các thủ tục và trigger

KIỂM TOÁN NGUỒN SỬ DỤNG CSDL

- Liên quan đến kiểm toán hoạt động đăng nhập là kiểm toán thông tin nguồn của máy khách, bao gồm:
  - Kiểm toán nút mạng được kết nối tới CSDL.
  - Kiểm toán ứng dụng đang được sử dụng để truy cập vào CSDL.

KIỂM TOÁN NGUỒN SỬ DỤNG CSDL

- Chương trình nguồn thường là dữ liệu mà ta nên thu thập cho mỗi truy vấn và các hoạt động trên cơ sở dữ liệu mà ta muốn giữ lại các vết kiểm toán.
- Nếu kiến trúc dựa trên mô hình máy khách/máy chủ, thì địa chỉ IP nguồn thường xác định một người sử dụng duy nhất.
- Nếu sử dụng kiến trúc máy chủ ứng dụng, thì địa chỉ IP sẽ không giúp xác định và báo cáo về người sử dụng cuối và sẽ phải thực hiện bằng cách khác.

KIỂM TOÁN NGUỒN SỬ DỤNG CSDL

VD: Thông tin kiểm toán dạng thô (IP và kiểu ứng dụng)

SERVER TYPE	SERVER IP	SOURCE PROGRAM	COUNT OF SESSIONS
MS SQL SERVER	155.212.221.84	SAP R/3	989
MS SQL SERVER	155.212.221.84	Aqua_Data_Studio	6
MS SQL SERVER	155.212.221.84	Microsoft SQL Server	1
MS SQL SERVER	155.212.221.84	SQL Query Analyzer	52

SERVER TYPE	SERVER IP	SOURCE PROGRAM	COUNT OF SESSIONS
FINANCIAL	HR DB	SAP R/3	989
FINANCIAL	HR DB	Developer tool	6
FINANCIAL	HR DB	Database link	1
FINANCIAL	HR DB	SQL Query Analyzer	52

CÁC LOẠI KIỂM TOÁN

- Kiểm toán đăng nhập/đăng xuất CSDL
- Kiểm toán nguồn sử dụng CSDL
- Kiểm toán việc sử dụng CSDL ngoài giờ làm việc
- Kiểm toán câu lệnh DDL
- Kiểm toán câu lệnh DML
- Kiểm toán lỗi CSDL
- Kiểm toán các thay đổi với nguồn của các thủ tục và trigger

KIỂM TOÁN CSDL NGOÀI GIỜ LÀM VIỆC

- Kiểm toán sử dụng CSDL ngoài giờ làm việc bình thường là cần thiết vì các hoạt động thực hiện vào giờ này thường đáng nghi ngờ và có thể là kết quả của việc một người sử dụng đang cố gắng truy cập trái phép hoặc sửa đổi dữ liệu.
- CSDL thường làm việc 24 giờ 7 ngày, không muốn tạo ra các báo động sai bất cứ khi nào một kịch bản ETL (Extracts Transforms Load - thu gom, chuyển đổi và cập nhập dữ liệu) diễn ra nhằm thực hiện tải một lượng lớn dữ liệu ngoài giờ làm việc bình thường.

KIỂM TOÁN CSDL NGOÀI GIỜ LÀM VIỆC

- Một cách tiếp cận để lọc ra các hoạt động bình thường xảy ra ở ngoài giờ làm việc là sử dụng một dòng cơ sở. Ví dụ dòng cơ sở truy cập CSDL có dạng như sau:

user1	192.168.1.168	SQLLoader	2am-4am
user2	192.168.1.168	ETL	12am-6am

KIỂM TOÁN CSDL NGOÀI GIỜ LÀM VIỆC

- Chỉ kiểm toán những gì khác biệt với dòng cơ sở sẽ giúp giảm kích thước của các vết kiểm toán khi kiểm tra, bởi vì kiểm toán sẽ chỉ ghi nhận những hoạt động đang xảy ra bên ngoài các chuẩn (đã được định nghĩa trong dòng cơ sở).

CÁC LOẠI KIỂM TOÁN

- Kiểm toán đăng nhập/đăng xuất CSDL
- Kiểm toán nguồn sử dụng CSDL
- Kiểm toán việc sử dụng CSDL ngoài giờ làm việc
- Kiểm toán câu lệnh DDL
- Kiểm toán câu lệnh DML
- Kiểm toán lỗi CSDL
- Kiểm toán các thay đổi với nguồn của các thủ tục và trigger

KIỂM TOÁN CÂU LỆNH DDL

- DDL là ngôn ngữ định nghĩa dữ liệu.
- Là một ngôn ngữ con của SQL giúp định nghĩa cấu trúc của cơ sở dữ liệu, bao gồm: định nghĩa các hàng, các cột, các bảng dữ liệu, các chỉ số và một số thuộc tính khác liên quan đến cơ sở dữ liệu như vị trí của file và là thành phần chính trong các hệ quản trị CSDL.
- DDL bao gồm các câu lệnh như: CREATE, ALTER, DROP, RENAME.

KIỂM TOÁN CÂU LỆNH DDL

- Có ba phương pháp chính để kiểm toán thay đổi lược đồ bao gồm:
  - Sử dụng tính năng kiểm toán CSDL.
  - Sử dụng hệ thống kiểm toán bên ngoài.
  - So sánh nhanh các lược đồ.
- Hầu hết các môi trường CSDL sẽ cho phép kiểm toán hoạt động DDL bằng cách sử dụng cơ chế kiểm toán, giám sát sự kiện, ghi vết.

KIỂM TOÁN CÂU LỆNH DDL

- Ví dụ: Oracle cho phép sử dụng Trigger hệ thống dựa trên câu lệnh DDL.
  - Tạo bảng lưu thông tin kiểm toán

```
SQL> create table ddl_audit_trail(
  2  user_id              varchar2(30),
  3  ddl_date             date,
  4  event_type           varchar2(30),
  5  object_type          varchar2(30),
  6  owner                varchar2(30),
  7  object_name          varchar2(30) );

Table created.
```

KIỂM TOÁN CÂU LỆNH DDL

– Tạo trigger kiểm toán DDL

```
SQL> create or replace trigger
  2  DDL_trigger AFTER DDL ON DATABASE
  3  BEGIN insert into ddl_audit_trail(
  4  user_id, ddl_date, event_type, object_type, owner, object_name)
  5  VALUES(
  6     ora_login_user,
  7     sysdate,
  8     ora_sysevent,
  9     ora_dict_obj_type,
 10     ora_dict_obj_owner,
 11     ora_dict_obj_name);
 12  END;
 13  /

Trigger created.
```

KIỂM TOÁN CÂU LỆNH DDL

- Cách thứ hai là sử dụng công cụ kiểm toán bên ngoài. Những công cụ này không chỉ tập hợp các thông tin mà còn cung cấp các công cụ cho việc báo cáo, cảnh báo, và các chức năng nâng cao như tạo dòng cơ sở.

KIỂM TOÁN CÂU LỆNH DDL

- Cách thứ ba là so sánh nhanh các lược đồ, nó không cung cấp một vết kiểm toán chi tiết của hoạt động DDL và kém hai loại trên nhưng tương đối dễ dàng thực hiện và có thể được sử dụng như là một giải pháp tạm thời cho đến khi ta thực hiện một cơ sở hạ tầng kiểm toán thật sự.

CÁC LOẠI KIỂM TOÁN

- Kiểm toán đăng nhập/đăng xuất CSDL
- Kiểm toán nguồn sử dụng CSDL
- Kiểm toán việc sử dụng CSDL ngoài giờ làm việc
- Kiểm toán câu lệnh DDL
- Kiểm toán câu lệnh DML
- Kiểm toán lỗi CSDL
- Kiểm toán các thay đổi với nguồn của các thủ tục và trigger

KIỂM TOÁN CÂU LỆNH DML

- DML là ngôn ngữ thao tác dữ liệu,
- Là một ngôn ngữ con của SQL giúp thao tác chi tiết hơn trên các đối tượng CSDL cụ thể, bao gồm các lệnh như: SELECT, INSERT, UPDATE, DELETE.

KIỂM TOÁN CÂU LỆNH DML

- Kiểm toán DML, nên chọn lọc các đối tượng và lệnh để kiểm toán để tiết kiệm tài nguyên.
  - Ví dụ, có thể quyết định tạo ra những vết kiểm toán cho một tập hợp con các bảng CSDL, v.v…
  - Thậm chí nên chọn lọc các bảng và cột để duy trì các giá trị cũ và mới, thay vì kiểm toán cho toàn bộ CSDL hay toàn bộ một bảng nào đó.

KIỂM TOÁN CÂU LỆNH DML

- Kiểm toán DML cũng được hỗ trợ thông qua ba phương pháp chính. Ba phương pháp này bao gồm:
  - Sử dụng khả năng của cơ sở dữ liệu.
  - Sử dụng một hệ thống kiểm toán bên ngoài.
  - Sử dụng trigger.

KIỂM TOÁN CÂU LỆNH DML

- Sử dụng khả năng của cơ sở dữ liệu
  - Tất cả các cơ sở dữ liệu đều cung cấp một số cách để thực hiện các vết kiểm toán cho các hoạt động DML.
  - Trong Oracle có thể sử dụng công cụ khai thác nhật ký (log miner tool) dựa trên redo log.
  - Trong SQL Server, có thể sử dụng sự kiện dò vết DOP

KIỂM TOÁN CÂU LỆNH DML

- Sử dụng một hệ thống kiểm toán bên ngoài
  - Dựa trên bất kỳ tiêu chí nào được lọc, bao gồm các đối tượng cơ sở dữ liệu, người sử dụng, ứng dụng, v.v.
  - Hỗ trợ trong việc thu giữ và nén thông tin này và sẵn dùng cho báo cáo, ngay cả khi số lượng dữ liệu rất lớn.

KIỂM TOÁN CÂU LỆNH DML

- Sử dụng các tùy chọn trigger:
  - Nếu không phải là một dự án kiểm toán mở rộng và chỉ cần tạo một vết kiểm toán DML cho một vài đối tượng, thì nên ghi các thông tin vào một bảng kiểm toán cụ thể bằng cách sử dụng trigger là cách đơn giản và nhanh nhất.

CÁC LOẠI KIỂM TOÁN

- Kiểm toán đăng nhập/đăng xuất CSDL
- Kiểm toán nguồn sử dụng CSDL
- Kiểm toán việc sử dụng CSDL ngoài giờ làm việc
- Kiểm toán câu lệnh DDL
- Kiểm toán câu lệnh DML
- Kiểm toán lỗi CSDL
- Kiểm toán các thay đổi với nguồn của các thủ tục và trigger

KIỂM TOÁN LỖI CSDL

- Kiểm toán lỗi do CSDL trả lại là quan trọng và là một trong những vết kiểm toán đầu tiên nên được thực hiện.
- Chống lại được các tấn công:
  - SQL Injection
  - Đăng nhập không thành công
  - Leo thang đặc quyền
  - …
- Giúp tìm ra các vấn đề có ảnh hưởng đến thời gian phản hồi và tính sẵn sàng.

KIỂM TOÁN LỖI CSDL

- Để kiểm toán lỗi CSDL:
  - Trong Oracle, có thể sử dụng lại các trigger hệ thống:
    - Đầu tiên, tạo bảng để ghi lỗi, bảng có tên error_audit

```
create table error_audit
(
(
    User_id varchar2(30),
    Session_id number(8),
    Host varchar2(30),
    Error_date date,
    Error varchar2(100),
);
```

KIỂM TOÁN LỖI CSDL

- Tiếp theo, tạo trigger để ghi lỗi vào bảng error_audit khi có lỗi xảy ra:

```
create or replace trigger
audit_errors_trigger
AFTER SERVERERROR ON DATABASE
BEGIN
insert into error_audit values(
        user,
        sys_context('USERENV','SESSIONID'),
        sys_context('USERENV','HOST'),
        sysdate,
        dbms_standard.server_error(1)
);
COMMIT;
END;
```

KIỂM TOÁN LỖI CSDL

- Trong SQL Server, có thể sử dụng:
  - Tính năng kiểm toán (auditing feature)
  - Tính năng dò vết (trace feature)

CÁC LOẠI KIỂM TOÁN

- Kiểm toán đăng nhập/đăng xuất CSDL
- Kiểm toán nguồn sử dụng CSDL
- Kiểm toán việc sử dụng CSDL ngoài giờ làm việc
- Kiểm toán câu lệnh DDL
- Kiểm toán câu lệnh DML
- Kiểm toán lỗi CSDL
- Kiểm toán các thay đổi với nguồn của các thủ tục và trigger

1. Tổng quan về kiểm toán
2. Các loại kiểm toán
3. Kiến trúc kiểm toán
4. Cơ chế kiểm toán trong Oracle và SQL Server

KIẾN TRÚC KIỂM TOÁN

- Hiểu rõ về vai trò an toàn của kiểm toán
- Chọn vết kiểm toán độc lập/dự phòng
- Kiến trúc cho hệ thống kiểm toán bên ngoài
- Đảm bảo an toàn cho thông tin kiểm toán
- Kiểm tra hệ thống kiểm toán
- Tự động hóa và giám sát các hoạt động kiểm toán

KIẾN TRÚC KIỂM TOÁN

- Hiểu rõ về vai trò an toàn của kiểm toán
- Chọn vết kiểm toán độc lập/dự phòng
- Kiến trúc cho hệ thống kiểm toán bên ngoài
- Đảm bảo an toàn cho thông tin kiểm toán
- Kiểm tra hệ thống kiểm toán
- Tự động hóa và giám sát các hoạt động kiểm toán

HIỂU RÕ VỀ VAI TRÒ CỦA KIỂM TOÁN

- Kiểm toán là một phương tiện, cách thức chứ không phải là một mục tiêu.
- Mục đích của kiểm toán là nâng cao tính an toàn và làm người kiểm toán gần gũi hơn với các chính sách và quy định an toàn khác.

HIỂU RÕ VỀ VAI TRÒ CỦA KIỂM TOÁN

- Để nâng cao tính an toàn bằng cách sử dụng kiểm toán, phải thực hiện một giải pháp thực tiễn và phải có khả năng sử dụng dữ liệu được thu thập thông qua cơ chế kiểm toán
- Giải pháp kiểm toán phải cho phép ta khai thác thông tin để đưa ra các dị thường, xâm nhập, sai sót, hành vi xấu, vi phạm chính sách,…

HIỂU RÕ VỀ VAI TRÒ CỦA KIỂM TOÁN

- Một giải pháp kiểm toán và kiến trúc kiểm toán được đưa ra sẽ có hai phần quan trọng:
  - Phần thu thập thông tin
  - Phần sử dụng thông tin.

KIẾN TRÚC KIỂM TOÁN

- Hiểu rõ về vai trò an toàn của kiểm toán
- Chọn vết kiểm toán độc lập/dự phòng
- Kiến trúc cho hệ thống kiểm toán bên ngoài
- Đảm bảo an toàn cho thông tin kiểm toán
- Kiểm tra hệ thống kiểm toán
- Tự động hóa và giám sát các hoạt động kiểm toán

CHỌN VẾT KIỂM TOÁN ĐỘC LẬP DỰ PHÒNG

- Giải pháp kiểm toán của các bên thứ ba tạo ra các vết kiểm toán độc lập/dự phòng. Nó có giá trị hơn vết kiểm toán được tạo ra bởi cơ sở dữ liệu.
- Vết kiểm toán độc lập và bên ngoài sẽ phù hợp với chiến lược phòng thủ theo chiều sâu.

CHỌN VẾT KIỂM TOÁN ĐỘC LẬP DỰ PHÒNG

- Ưu điểm:
  - Khó bị xâm phạm
  - Không nhạy cảm với các lỗi và lỗ hổng mà cơ sở dữ liệu có thể có
  - Hỗ trợ tốt hơn sự tách bạch các nhiệm vụ.

CHỌN VẾT KIỂM TOÁN ĐỘC LẬP DỰ PHÒNG

- Một vết kiểm toán độc lập cũng có thể được sử dụng cùng với một kiểm toán cơ sở dữ liệu để hỗ trợ môi trường có yêu cầu nghiêm ngặt về an toàn và tuân thủ.

KIẾN TRÚC KIỂM TOÁN

- Hiểu rõ về vai trò an toàn của kiểm toán
- Chọn vết kiểm toán độc lập/dự phòng
- Kiến trúc cho hệ thống kiểm toán bên ngoài
- Đảm bảo an toàn cho thông tin kiểm toán
- Kiểm tra hệ thống kiểm toán
- Tự động hóa và giám sát các hoạt động kiểm toán

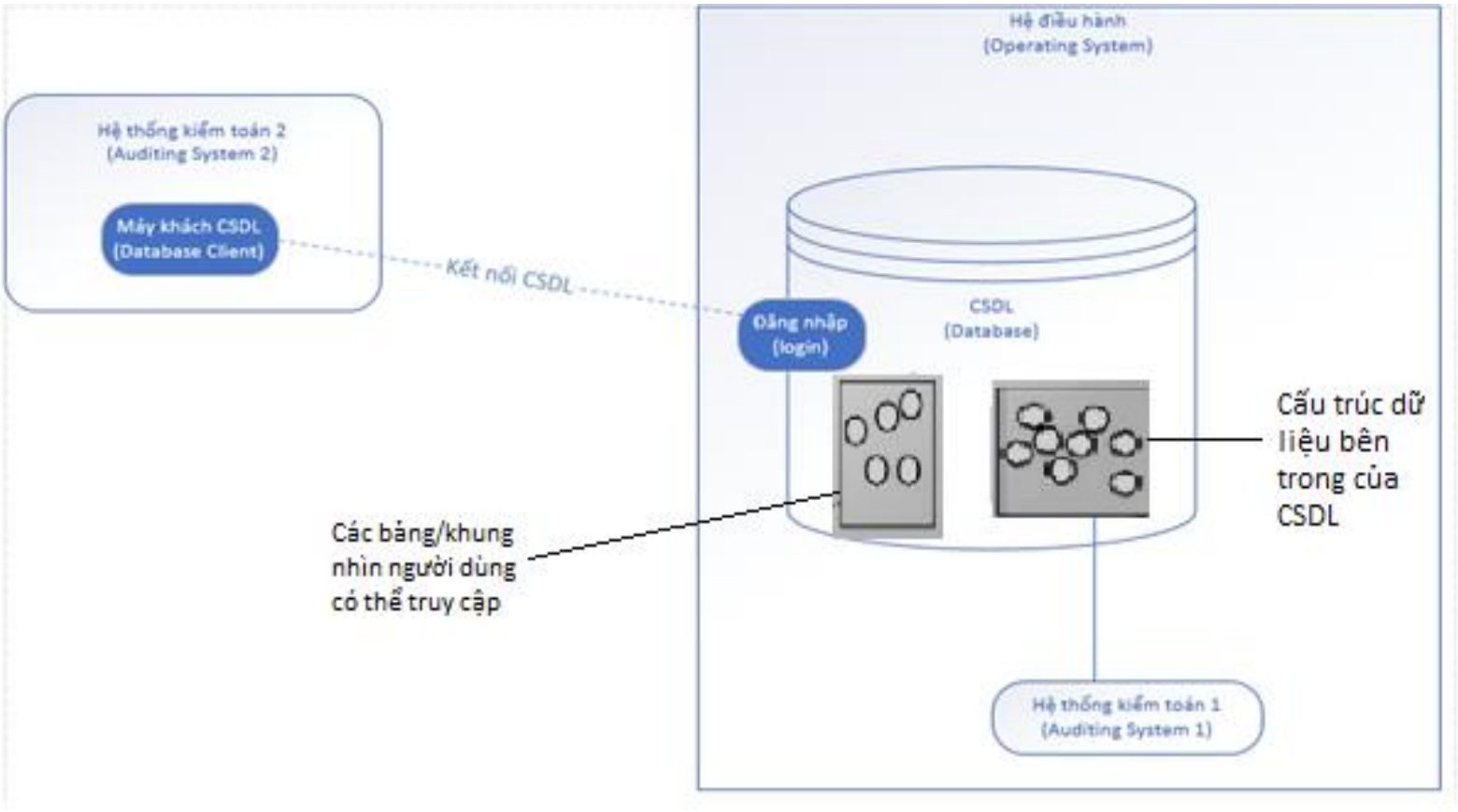
KIẾN TRÚC CHO HỆ THỐNG KIỂM TOÁN BÊN NGOÀI

- Có 3 phương pháp:
  - Kiểm tra cấu trúc cơ sở dữ liệu nội bộ.
  - Kiểm tra tất cả các liên lạc với cơ sở dữ liệu.
  - Kiểm tra các yếu tố được tạo ra bởi cơ sở dữ liệu trong quá trình hoạt động bình thường.

KIẾN TRÚC CHO HỆ THỐNG KIỂM TOÁN BÊN NGOÀI

- Cơ sở dữ liệu có cấu trúc dữ liệu nội bộ được sử dụng để xử lý lệnh, lưu trữ kết quả, v.v.
  - Ví dụ, Oracle có một bộ các bảng bên trong được gọi là các bảng X được sử dụng để lưu trữ SQL và xử lý nó.

KIẾN TRÚC CHO HỆ THỐNG KIỂM TOÁN BÊN NGOÀI

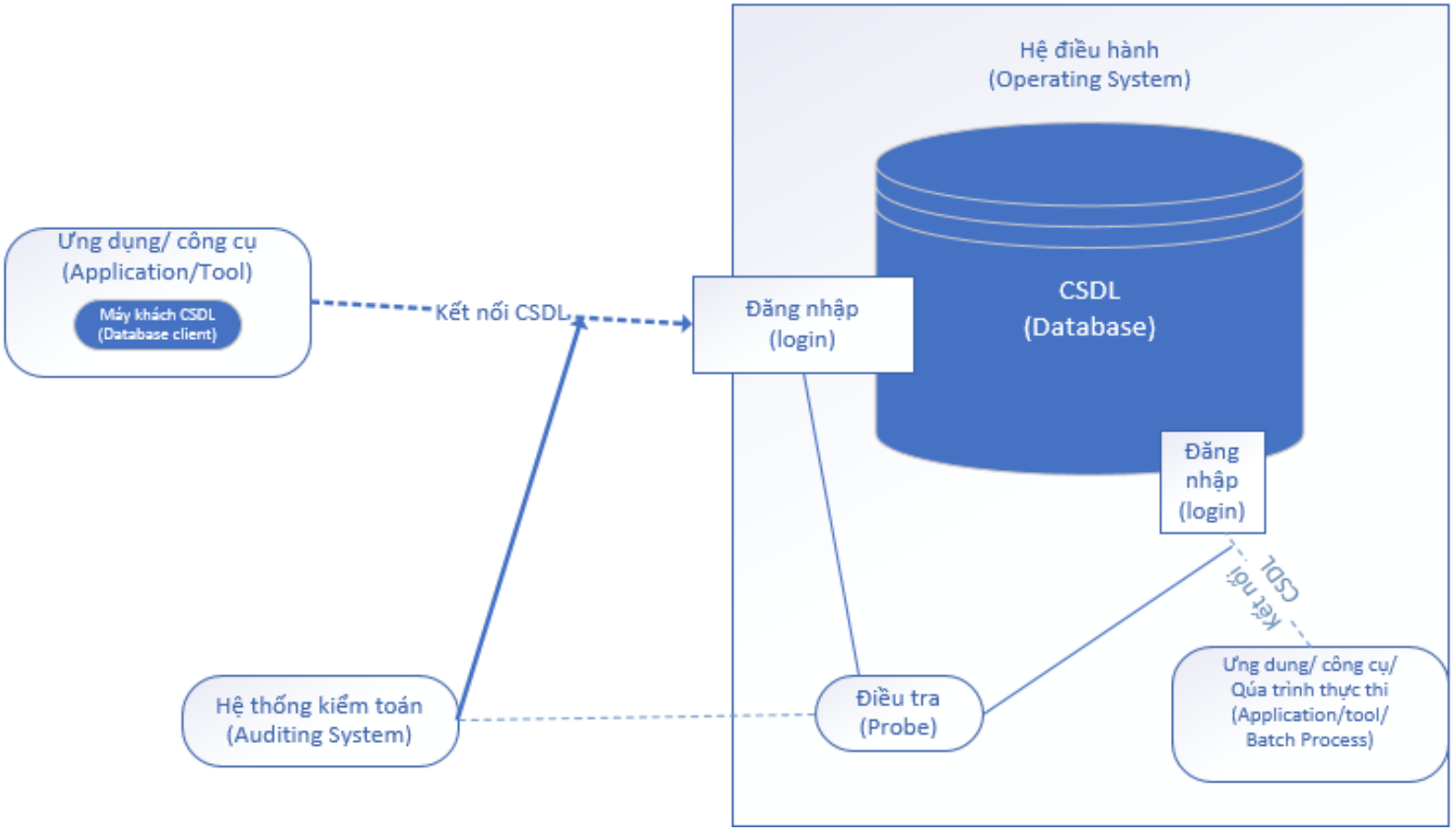


Kiểm toán bằng cách kiểm tra trong cấu trúc dữ liệu trong bộ nhớ của cơ sở dữ liệu

KIẾN TRÚC CHO HỆ THỐNG KIỂM TOÁN BÊN NGOÀI

- *Kiến trúc kiểm toán thứ hai* liên quan đến việc kiểm toán tất cả các luồng kết nối đã kết thúc bởi cơ sở dữ liệu.
- Các máy khách cơ sở dữ liệu kết nối tới tiến trình cơ sở dữ liệu bằng cách sử dụng các giao thức mạng hoặc bằng cách sử dụng các cơ chế giao tiếp liên tiến trình (interprocess -IPC) nếu máy khách nằm trên cùng một máy chủ với cơ sở dữ liệu.

KIẾN TRÚC CHO HỆ THỐNG KIỂM TOÁN BÊN NGOÀI

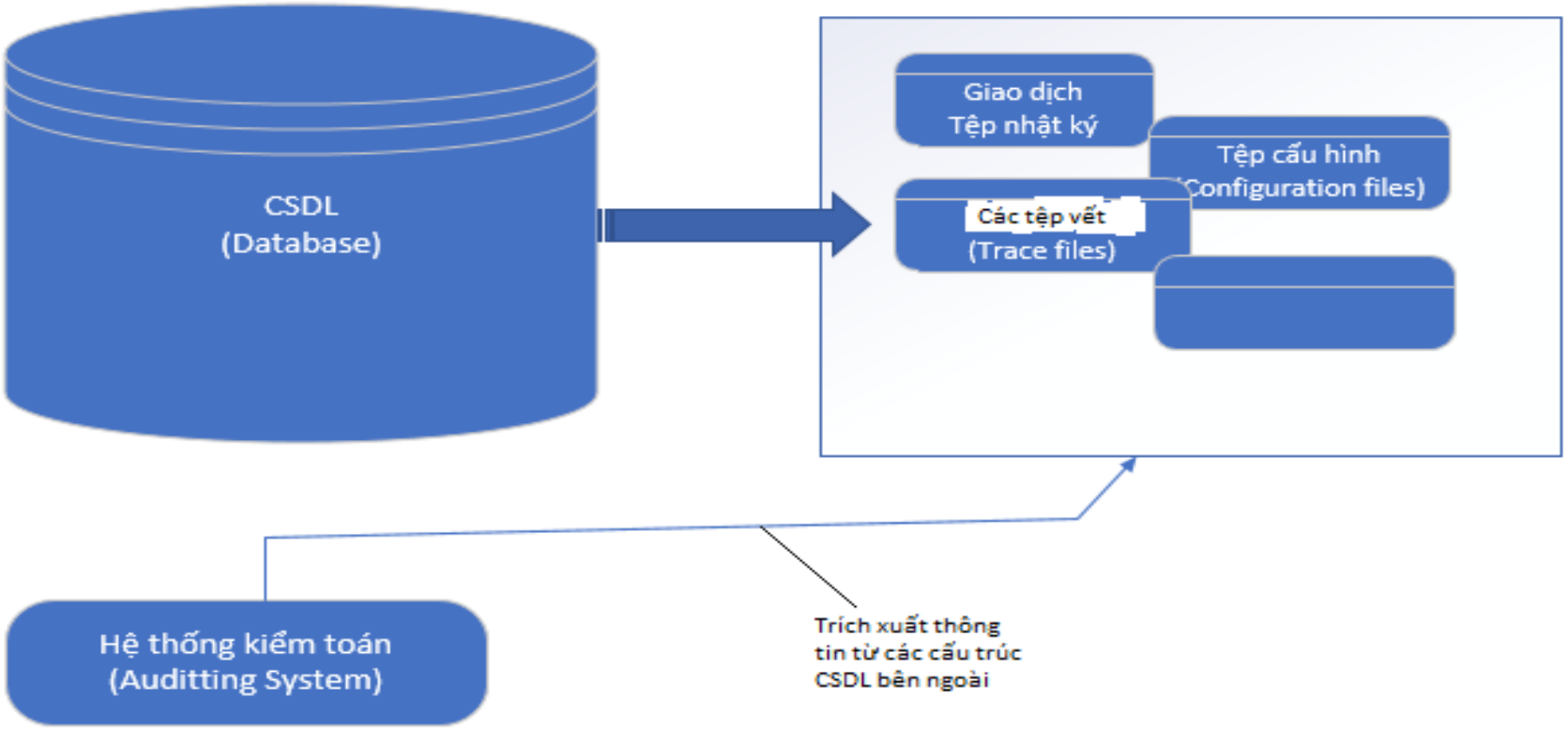


Kiểm toán bằng cách kiểm tra các luồng truyền thông (qua mạng và cục bộ)

KIẾN TRÚC CHO HỆ THỐNG KIỂM TOÁN BÊN NGOÀI

- *Kiến trúc kiểm toán thứ ba* sử dụng các tập tin được sử dụng bởi cơ sở dữ liệu trong quá trình hoạt động bình thường và trích xuất các thông tin có liên quan từ chúng.

KIẾN TRÚC CHO HỆ THỐNG KIỂM TOÁN BÊN NGOÀI



Kiểm toán bằng cách kiểm tra các tệp cơ sở dữ liệu hỗ trợ

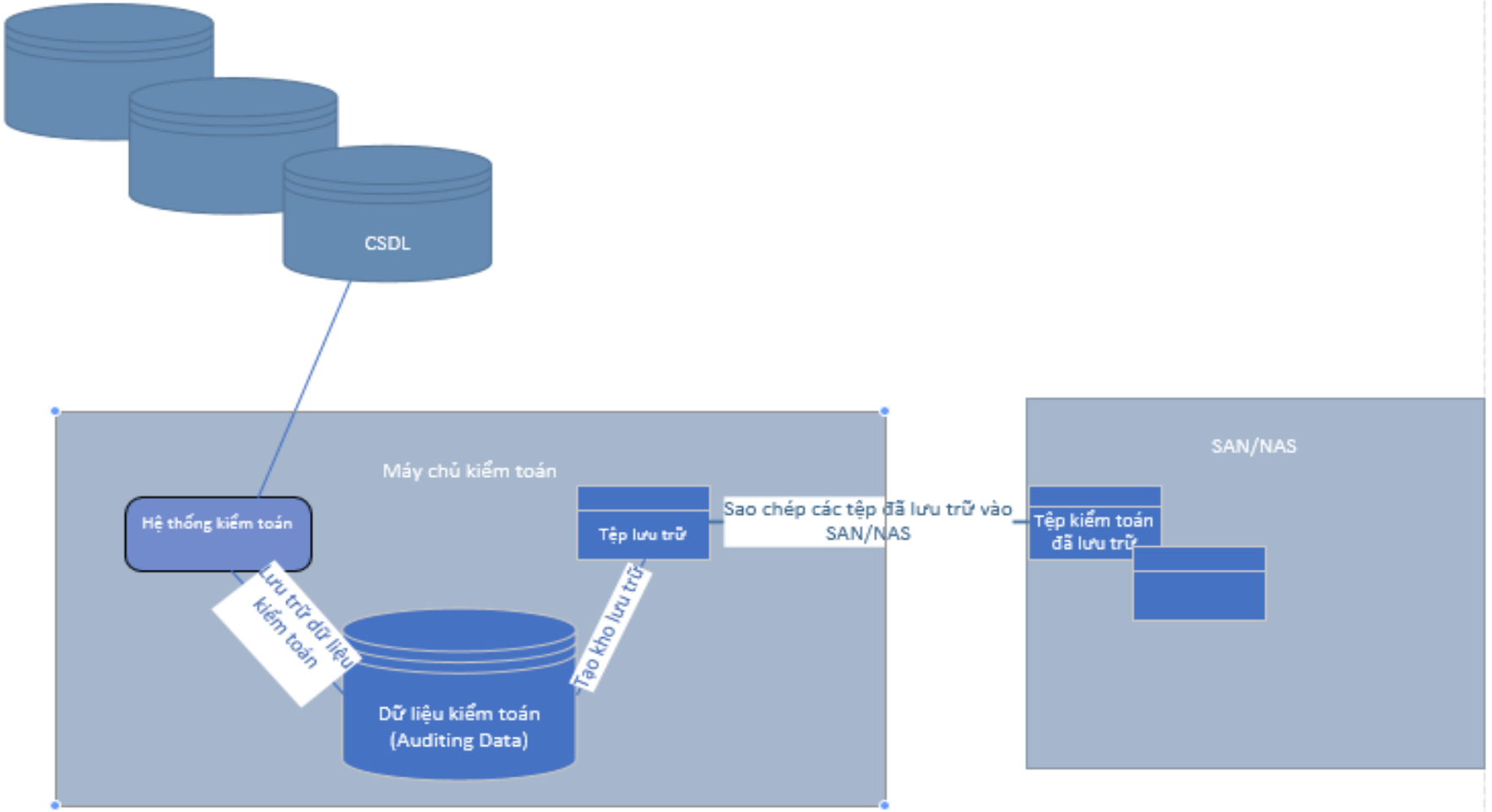
KIẾN TRÚC KIỂM TOÁN

- Hiểu rõ về vai trò an toàn của kiểm toán
- Chọn vết kiểm toán độc lập/dự phòng
- Kiến trúc cho hệ thống kiểm toán bên ngoài
- Đảm bảo an toàn cho thông tin kiểm toán
- Kiểm tra hệ thống kiểm toán
- Tự động hóa và giám sát các hoạt động kiểm toán

ĐẢM BẢO AN TOÀN CHO THÔNG TIN KIỂM TOÁN

- Giải pháp kiểm toán phải có các điều khoản an toàn tốt, chứ không chỉ dừng lại ở việc đảm bảo an toàn cho dữ liệu đã lưu.
- Giải pháp kiểm toán an toàn phải giải quyết tất cả bốn "vị trí" lưu trữ thông tin kiểm toán.
  - Kho lưu trữ chính - nơi lưu trữ thông tin kiểm toán.
  - Các tệp lưu trữ bên trong máy chủ kiểm toán.
  - Các tệp lưu trữ trên đường truyền
  - Các tệp lưu trữ tại vị trí lưu trữ.

ĐẢM BẢO AN TOÀN CHO THÔNG TIN KIỂM TOÁN



Đảm bảo an toàn cho vòng đời dữ liệu kiểm toán

KIẾN TRÚC KIỂM TOÁN

- Hiểu rõ về vai trò an toàn của kiểm toán
- Chọn vết kiểm toán độc lập/dự phòng
- Kiến trúc cho hệ thống kiểm toán bên ngoài
- Đảm bảo an toàn cho thông tin kiểm toán
- Kiểm tra hệ thống kiểm toán
- Tự động hóa và giám sát các hoạt động kiểm toán

KIỂM TRA HỆ THỐNG KIỂM TOÁN

- Đảm bảo rằng có vết kiểm toán đầy đủ cho các truy cập và những thay đổi được thực hiện đối với thông tin kiểm toán.
- Điều này bao gồm cả *dữ liệu* và *các định nghĩa* kiểm toán

KIỂM TRA HỆ THỐNG KIỂM TOÁN

- Ví dụ:
  - *Dữ liệu* là một bản ghi kiểm toán về một người dùng hệ thống kiểm toán đã đưa ra một báo cáo hiển thị tất cả các lệnh DDL đã xảy ra trong tháng trước.
  - *Các định nghĩa* bao gồm các bản ghi kiểm toán cho thấy một người dùng của hệ thống kiểm toán đã thay đổi định nghĩa của báo cáo kiểm toán và báo cáo đánh giá.

KIỂM TRA HỆ THỐNG KIỂM TOÁN

Date	Event Time	Server Instance Name	Action ID	Class Type	Sequence Number	Succeeded
23/05/2018 10:29:32 SA	10:29:32.1005798	HONGHUONG-PC	AUDIT SESSION CHANGED	SERVER AUDIT	0	True
23/05/2018 1:12:16 SA	01:12:16.7242210	HONGHUONG-PC	AUDIT SESSION CHANGED	SERVER AUDIT	0	True
22/05/2018 1:52:31 CH	13:52:31.2267682	HONGHUONG-PC	AUDIT SESSION CHANGED	SERVER AUDIT	0	True
21/05/2018 4:59:15 CH	16:59:15.3262891	HONGHUONG-PC	AUDIT SESSION CHANGED	SERVER AUDIT	0	True
21/05/2018 4:52:42 CH	16:52:42.6292256	HONGHUONG-PC	AUDIT SESSION CHANGED	SERVER AUDIT	0	True
20/05/2018 3:56:21 CH	15:56:21.9721734	HONGHUONG-PC	AUDIT SESSION CHANGED	SERVER AUDIT	0	True
20/05/2018 2:36:57 CH	14:36:57.5826366	HONGHUONG-PC	AUDIT SESSION CHANGED	SERVER AUDIT	0	True
19/05/2018 2:51:56 CH	14:51:56.6950672	HONGHUONG-PC	AUDIT SESSION CHANGED	SERVER AUDIT	0	True
18/05/2018 2:44:50 CH	14:44:50.3112631	HONGHUONG-PC	AUDIT SESSION CHANGED	SERVER AUDIT	0	True
17/05/2018 8:54:02 SA	08:54:02.4114652	HONGHUONG-PC	AUDIT SESSION CHANGED	SERVER AUDIT	0	True
16/05/2018 2:59:48 CH	14:59:48.2196859	HONGHUONG-PC	AUDIT SESSION CHANGED	SERVER AUDIT	0	True
15/05/2018 11:21:58 CH	23:21:58.0583248	HONGHUONG-PC	AUDIT SESSION CHANGED	SERVER AUDIT	0	True

Các vết của hệ thống kiểm toán

KIẾN TRÚC KIỂM TOÁN

- Hiểu rõ về vai trò an toàn của kiểm toán
- Chọn vết kiểm toán độc lập/dự phòng
- Kiến trúc cho hệ thống kiểm toán bên ngoài
- Đảm bảo an toàn cho thông tin kiểm toán
- Kiểm tra hệ thống kiểm toán
- Tự động hóa và giám sát các hoạt động kiểm toán

TỰ ĐỘNG HÓA VÀ GS CÁC HOẠT ĐỘNG KIỂM TOÁN

- Tự động hóa là một phần quan trọng của một giải pháp kiểm toán mạnh. Ta có thể có hệ thống tốt nhất để tự động phân phối dữ liệu kiểm toán, nhưng cũng phải đảm bảo rằng mọi người vẫn đang xem xét và đăng xuất trên dữ liệu.

TỰ ĐỘNG HÓA VÀ GS CÁC HOẠT ĐỘNG KIỂM TOÁN

- Ví dụ:
  - Quá trình kiểm toán có thể xác định rằng một báo cáo DDL phải được xem xét lại bởi DBA và sau đó được xem xét bởi người quản lý hoạt động.
  - Luồng công việc cung cấp báo cáo cho DBA, và chỉ khi được chấp thuận bởi DBA thì báo cáo mới đi đến người quản lý hoạt động. Trong trường hợp này, nếu DBA không xem xét và phát hành báo cáo, thì người quản lý hoạt động sẽ không bao giờ có được nó.

TỰ ĐỘNG HÓA VÀ GS CÁC HOẠT ĐỘNG KIỂM TOÁN

- Giải pháp: phải có sự giám sát chặt chẽ trong quá trình kiểm toán. Đảm bảo rằng các nhiệm vụ kiểm toán liên tục được kích hoạt và người đánh giá phải nắm giữ các quy trình.
- Việc giám sát có thể thụ động hoặc dựa trên quản lý ngoại lệ.

TỰ ĐỘNG HÓA VÀ GS CÁC HOẠT ĐỘNG KIỂM TOÁN

- Giám sát thụ động nghĩa là hệ thống kiểm toán cung cấp cách để báo cáo về tất cả các hoạt động và số lần đánh giá/đăng xuất vẫn đang chờ xử lý.
- Giám sát dựa trên ngoại lệ (hoặc giám sát hoạt động) không yêu cầu liên tục theo dõi tình trạng của luồng công việc. Thay vào đó, người kiểm toán sẽ nhận được cảnh báo khi ai đó đang nắm giữ quy trình và không xem xét lại các kết quả kiểm toán.

1. Tổng quan về kiểm toán
2. Các loại kiểm toán
3. Kiến trúc kiểm toán
4. Cơ chế kiểm toán trong Oracle và SQL Server

CƠ CHẾ KIỂM TOÁN TRONG ORACLE VÀ SQL SERVER

- Kiểm toán trong Oracle
- Kiểm toán trong SQL Server

KIỂM TOÁN TRONG ORACLE

- Kiểm toán hệ thống bắt buộc (Mandatory SYS auditing - MSA)
- Kiểm toán chuẩn (Standard auditing-SA)
- Kiểm toán mịn (Fine grained auditing-FGA)

KIỂM TOÁN HỆ THỐNG BẮT BUỘC

- Đặc điểm: Tất cả người dùng kể cả các quản trị viên đều không nên, hay không thể vô hiệu hóa kiểm toán này.
- Oracle luôn luôn kiểm toán và ghi lại các hoạt động vào file kiểm toán hệ thống đối với người dùng đăng nhập dưới quyền SYSDBA hoặc SYSOPER.

KIỂM TOÁN HỆ THỐNG BẮT BUỘC

- Mặc định, vị trí lưu file kiểm toán:

$ORACLE_BASE/admin/$ORACLE_SIS/adump

Trên cả Windows và Unix. Riêng windows, Oracle còn lưu thông tin vào Event Viewer. Ta có thể thay đổi file lưu trữ dùng tham số AUDIT_FILE_DEST.

KIỂM TOÁN TRONG ORACLE

- Kiểm toán hệ thống bắt buộc (Mandatory SYS auditing - MSA)
- Kiểm toán chuẩn (Standard auditing-SA)
- Kiểm toán mịn (Fine grained auditing-FGA)

KIỂM TOÁN CHUẨN

- Kiểm toán 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, loại hành động, đối tượng, đặc quyền, user truy cập…
- Kiểm toán tiêu chuẩn có thể được chia nhỏ thành ba loại sau:
  - *Kiểm toán câu lệnh (Statement auditing)*
  - *Kiểm toán các đặc quyền (Privilege auditing)*
  - *Kiểm toán các đối tượng lược đồ cơ sở dữ liệu (Schema Object auditing)*

KIỂM TOÁN CHUẨN

- *Kiểm toán câu lệnh*: Kiểm toán câu lệnh cho phép ghi lại mỗi lần thực thi một loại câu lệnh nào đó. Cú pháp như sau:

```
AUDIT <statements_list>
[BY <users_list>]
[BY {ACCESS|SESSION}]
[WHERE [NOT] SUCCESSFUL]
```

KIỂM TOÁN CHUẨN

- *<Statements_list>* là danh sách các câu lệnh cách nhau bởi dấu phẩy. Chẳng hạn: CREATE TABLE, DROP TABLE, CREATE USER là một danh sách lệnh.
- *<user_list>*: là danh sách người dùng cách nhau bởi dấu phẩy. Chẳng hạn: SYS, SCOTT.
- *BY ACCESS*: một bản ghi cho mỗi lần thực thi câu lệnh được giám sát.
- *BY SESSION*: một bản ghi cho nhiều lần thực thi một câu lệnh cùng loại trên cùng một đối tượng trong một phiên làm việc. Mặc định là BY ACCESS.
- *WHEN SUCCESSFUL* hay *WHEN NOT SUCCESSFUL*: chỉ lưu lại khi câu lệnh truy vấn thành công hay thất bại.

KIỂM TOÁN CHUẨN

- *Kiểm toán đặc quyền* là loại kiểm toán các câu lệnh sử dụng quyền hệ thống.
- Có thể kiểm toán quyền SELECT ANY TABLE nếu muốn kiểm toán tất cả các lệnh SELECT trên bất cứ TABLE nào. Ngoài ra có thể kiểm toán bất cứ quyền hệ thống nào.

KIỂM TOÁN CHUẨN

- *Kiểm toán các đối tượng lược đồ cơ sở dữ liệu (Schema Object auditing)*

Loại kiểm toán này có thể kiểm toán tất cả câu lệnh SELECT và DML cho phép bởi quyền đối tượng, như câu lệnh SELECT hoặc DELETE trên một bảng thông dụng. Câu lệnh GRANT và REVOKE dùng để điều khiển các quyền hạn cũng được kiểm toán.

KIỂM TOÁN TRONG ORACLE

- Kiểm toán hệ thống bắt buộc (Mandatory SYS auditing - MSA)
- Kiểm toán chuẩn (Standard auditing-SA)
- Kiểm toán mịn (Fine grained auditing-FGA)

KIỂM TOÁN MỊN

- Cho phép kiểm toán ở cấp chi tiết nhất, truy cập dữ liệu và hành động dựa trên nội dung, sử dụng bất kỳ biện pháp Boolean nào, chẳng hạn như value > 1,000,000.
- Cho phép kiểm toán dựa trên quyền truy cập hoặc thay đổi trong một cột.

KIỂM TOÁN MỊN

- Có thể sử dụng kiểm toán mịn để kiểm toán các loại hành động sau:
  - Truy cập trong một khoảng thời gian cụ thể (chẳng hạn, từ: 9h tối đến 6h sáng của thứ bảy hoặc chủ nhật).
  - Sử dụng địa chỉ IP bên ngoài mạng công ty.
  - Select hoặc update một cột của bảng.
  - Chỉnh sửa một giá trị trong một cột của bảng.

KIỂM TOÁN MỊN

- Tạo vết kiểm toán cho các bản ghi kiểm toán mịn:
  - Để tạo chính sách kiểm toán mịn ta sử dụng thủ tục DBMS_FGA.ADD_POLICY.
  - Cú pháp cho thủ tục ADD_POCILY:

```
DBMS_FGA.ADD_POLICY(
   object_schema       VARCHAR2,
   object_name         VARCHAR2,
   policy_name         VARCHAR2,
   audit_condition     VARCHAR2,
   audit_column        VARCHAR2,
   handler_schema      VARCHAR2,
   handler_module      VARCHAR2,
   enable              BOOLEAN,
   statement_types     VARCHAR2,
   audit_trail         BINARY_INTEGER IN DEFAULT,
   audit_column_opts   BINARY_INTEGER IN DEFAULT);
```

KIỂM TOÁN MỊN

- *Object_schema*: Chỉ định lược đồ của đối tượng cần kiểm toán.
- *Object_name*: Chỉ định tên của đối tượng cần kiểm kiểm toán.
- *Policy_name*: Chỉ định tên của chính sách được tạo. Đảm bảo rằng tên này là duy nhất.
- *Audit_condition*: Chỉ định một điều kiện Boolean trong một hàng. NULL được cho phép và hoạt động như TRUE. Nếu chỉ định NULL hoặc không có điều kiện kiểm toán, thì bất kỳ hành động nào trên một bảng với chính sách đó sẽ tạo ra một bản ghi kiểm toán, có hay không các hàng được trả về.

KIỂM TOÁN MỊN

- *Audit_column*: Chỉ định một hoặc nhiều cột để kiểm toán, bao gồm các cột bị ẩn. Nếu được đặt thành NULL hoặc bị bỏ qua, tất cả các cột sẽ được kiểm toán. Chúng có thể bao gồm các cột bị ẩn của Oracle Label Security hoặc các cột kiểu đối tượng. Mặc định, NULL gây ra kiểm toán nếu bất kỳ cột nào được truy cập hoặc bị ảnh hưởng.
- *Handler_schema*: Nếu một cảnh báo được sử dụng để kích hoạt phản hồi khi chính sách bị vi phạm, thì chỉ định tên của lược đồ chứa trình xử lý sự kiện. Mặc định, NULL là sử dụng lược đồ hiện tại.
- *Handler_module*: Chỉ định tên của trình xử lý sự kiện.

KIỂM TOÁN MỊN

- *Enable*: kích hoạt hoặc tắt sử dụng policy là true hay fail. Nếu bỏ qua, mặc định sẽ là TRUE.
- *Statement_types*: chỉ định các câu lệnh SQL được kiểm toán: INSERT, UPDATE, DELETE, hoặc SELECT. Mặc định là SELECT.
- *Audit_trail:* chỉ định nơi lưu trữ (DB hoặc XML) các bản ghi kiểm toán. Nếu thiết lập audit_trail là XML, khi đó các file XML được ghi vào AUDIT_FILE_DEST.
- *Audit_column_opts*: Nếu ta chỉ định nhiều hơn một trong các tham số audit_column, khi đó sẽ xác định rằng có kiểm toán tất cả các cột hay chỉ kiểm toán các cột đã được chỉ định.

CƠ CHẾ KIỂM TOÁN TRONG Oracle VÀ SQL Server

- Kiểm toán trong Oracle
- Kiểm toán trong SQL Server

KIỂM TOÁN TRONG SQL Server

- Có từ phiên bản SQL Server 2008 Enterprise. Tính năng này đơn giản hóa khả năng giám sát tự động và có thể thay thế cho việc cài đặt các trigger.
- Kiểm toán trong SQL Server có thể cấu hình giám sát ở hai mức: instance và database.

KIỂM TOÁN TRONG SQL Server

- Các thành phần của kiểm toán SQL Server:
  - Kiểm toán máy chủ (Server Audit): thành phần cha của một kiểm toán SQL Server.
    - Có thể chứa cả đặc tả kiểm toán máy chủ và đặc tả cơ sở dữ liệu.
    - Thuộc về cơ sở dữ liệu siêu dữ liệu, dùng để định nghĩa nơi lưu trữ thông tin của các kiểm toán.

KIỂM TOÁN TRONG SQL Server

– Đặc tả kiểm toán máy chủ (Server audit specification): quy định cho một kiểm toán cụ thể nào đó gồm một tập các hành động của Instance cần giám sát.

  - ví dụ: CREATE LOGIN, ALTER DATABASE, vv. Chúng ta có thể tạo một đặc tả kiểm toán máy chủ cho mỗi SQL Server audit.

KIỂM TOÁN TRONG SQL Server

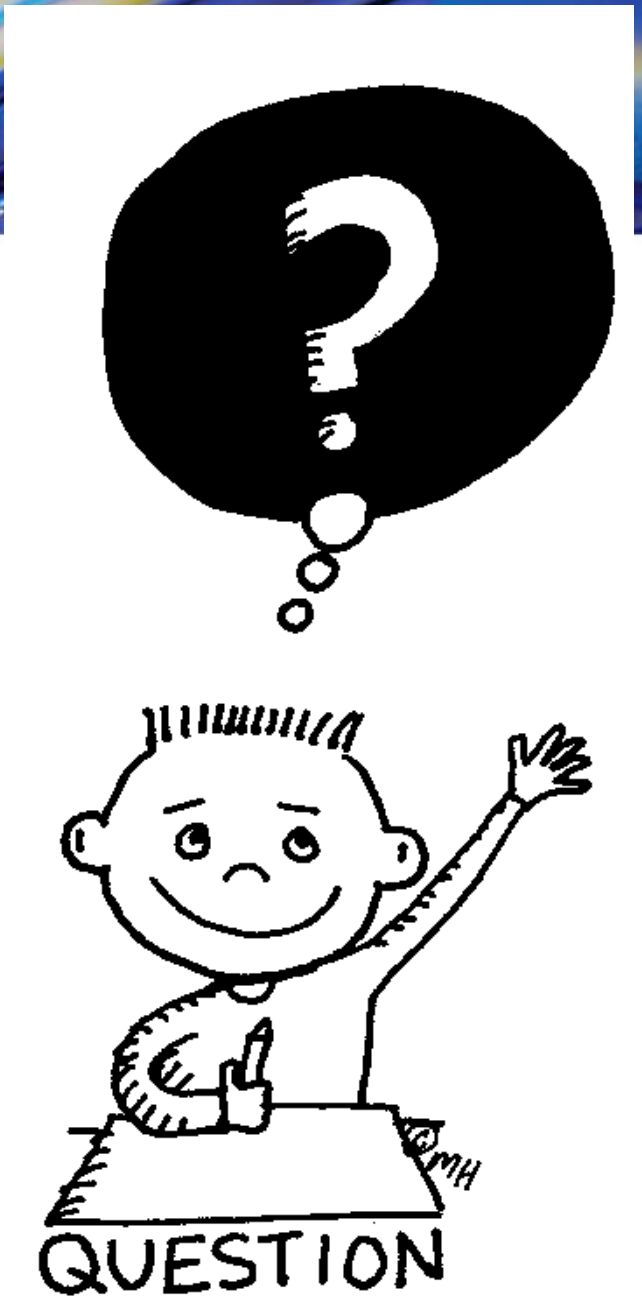
– Đặc tả kiểm toán cơ sở dữ liệu (Database audit specification): quy định cho một kiểm toán cụ thể nào đó một tập các hành động của đối tượng cơ sở dữ liệu cần giám sát,

- ví dụ: CREATE TABLE, ALTER VIEW, v.v. Chúng ta có thể tạo một đặc tả kiểm toán cơ sở dữ liệu cho mỗi SQL Server audit.

KIỂM TOÁN TRONG SQL Server

- Đích (Target): chính là đích kiểm toán được chỉ ra trong mỗi kiểm toán. Target có thể là một file, một nhật ký sự kiện an toàn của Windows, hay một nhật ký sự kiện ứng dụng Windows

1. Tổng quan về kiểm toán
2. Các loại kiểm toán
3. Kiến trúc kiểm toán
4. Cơ chế kiểm toán trong Oracle và SQL Server


QUESTION