HỌC VIỆN CÔNG NGHỆ BƯU CHÍNH VIỄN THÔNG

BÀI GIẢNG MÔN HỌC
AN TOÀN ỨNG DỤNG WEB & CSDL

CHƯƠNG 7 – SAO LƯU, KHÔI PHỤC DỰ PHÒNG, KIỂM TOÁN VÀ GIÁM SÁT HOẠT ĐỘNG CƠ SỞ DỮ LIỆU

Giảng viên: PGS.TS. Hoàng Xuân Dậu

E-mail: dauhx@ptit.edu.vn

Khoa: An toàn thông tin

NỘI DUNG CHƯƠNG 7

1. Sao lưu và khôi phục dự phòng CSDL
   - Giới thiệu chung
   - Sao lưu cơ sở dữ liệu
   - Khôi phục cơ sở dữ liệu
   - An toàn dữ liệu sao lưu
2. Kiểm toán cơ sở dữ liệu
   - Giới thiệu chung
   - Các dạng kiểm toán CSDL
   - Một số vấn đề liên quan đến kiểm toán CSDL
   - Một số công cụ kiểm toán CSDL

7.1.1 Giới thiệu chung

- Sao lưu CSDL (Database backup) là thao tác tạo bản sao của một phần hoặc toàn bộ CSDL.
  - Bản sao có thể được tạo và lưu trên cùng phương tiện lưu trữ với CSDL hoặc sử dụng một phương tiện lưu trữ riêng (đĩa cứng, băng từ, ổ mạng);
  - Sao lưu có thể được thực hiện định kỳ hoặc không định kỳ, theo chính sách của cơ quan, tổ chức.

7.1.1 Giới thiệu chung

- Khôi phục dự phòng CSDL (Database recovery) là thao tác khôi phục lại CSDL sau các sự cố.
  - Khôi phục CSDL sử dụng một phần bản sao đã tạo
  - Khôi phục CSDL sử dụng toàn bộ bản sao đã tạo.

7.1.1 Giới thiệu chung

- Vai trò của sao lưu và khôi phục dự phòng CSDL:
  - Là các khâu chủ động chuẩn bị nhằm đối phó với các sự cố với cơ sở dữ liệu hoặc các hệ thống có liên quan đến CSDL.
  - Nhằm đảm bảo tính sẵn dùng và toàn vẹn CSDL.

7.1.1 Giới thiệu chung

- Việc sao lưu CSDL cần được thực hiện định kỳ, theo chu kỳ phù hợp:
  - Yêu cầu đảm bảo an toàn dữ liệu;
  - Khả năng lưu trữ của phương tiện sao lưu dữ liệu;
  - Tải lên hệ thống khi thực hiện sao lưu;
  - Nên xem xét kết hợp giữa backup on-site và off-site.

7.1.1 Giới thiệu chung

- Các sự cố có thể xảy ra với hệ thống máy chủ CSDL và bản thân CSDL có thể được chia thành 3 loại:
  - Sự cố với hệ quản trị CSDL (Instance failures)
  - Sự cố ứng dụng hoặc giao dịch (Application/Transaction failures)
  - Các sự cố phương tiện lưu trữ (Media failures)

7.1.1 Giới thiệu chung

- Sự cố với hệ quản trị CSDL (Instance failures):
  - Có thể gây ra bởi lỗi bên trong hệ quản trị CSDL, lỗi hệ điều hành;
  - Một số trường hợp có thể gây hỏng hóc hoặc mất mát dữ liệu yêu cầu phải khôi phục.

7.1.1 Giới thiệu chung

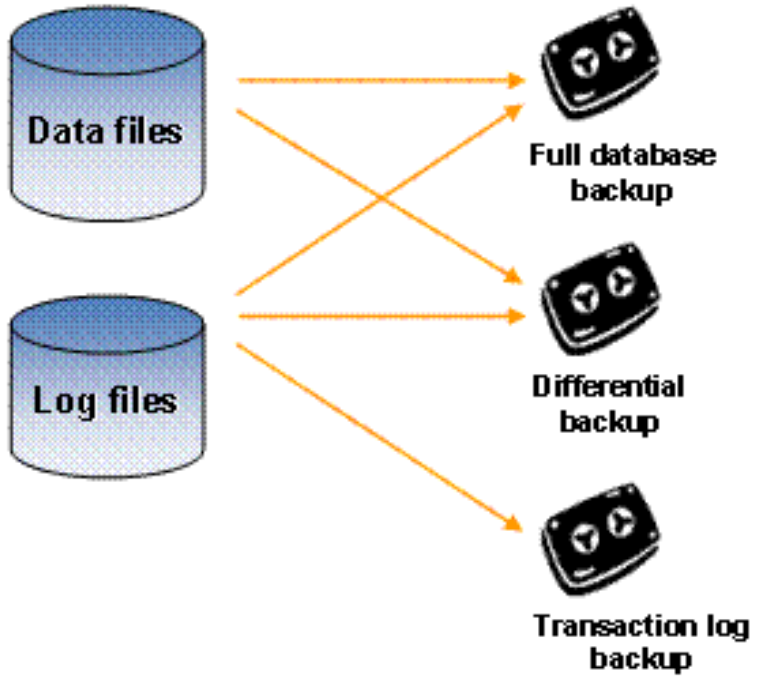
- Sự cố ứng dụng hoặc giao dịch (Application/Transaction failures):
  - Do các lỗi xử lý dữ liệu;
  - Một số trường hợp cũng có thể gây hỏng hóc hoặc mất mát dữ liệu yêu cầu phải khôi phục.

7.1.1 Giới thiệu chung

- Các sự cố phương tiện lưu trữ (Media failures):
  - Gồm các hỏng hóc đối với các phương tiện lưu trữ như đĩa cứng, RAID, băng từ hoặc các phương tiện lưu trữ khác;
  - Có thể gây hỏng hóc, mất một phần hoặc toàn bộ CSDL đòi hỏi phải khôi phục.

7.1.2 Sao lưu CSDL

- Các dạng sao lưu (SQL Server):
  - Sao lưu CSDL (Database backup);
  - Sao lưu log giao dịch (Transaction log backup);
  - Sao lưu các files (File backup).

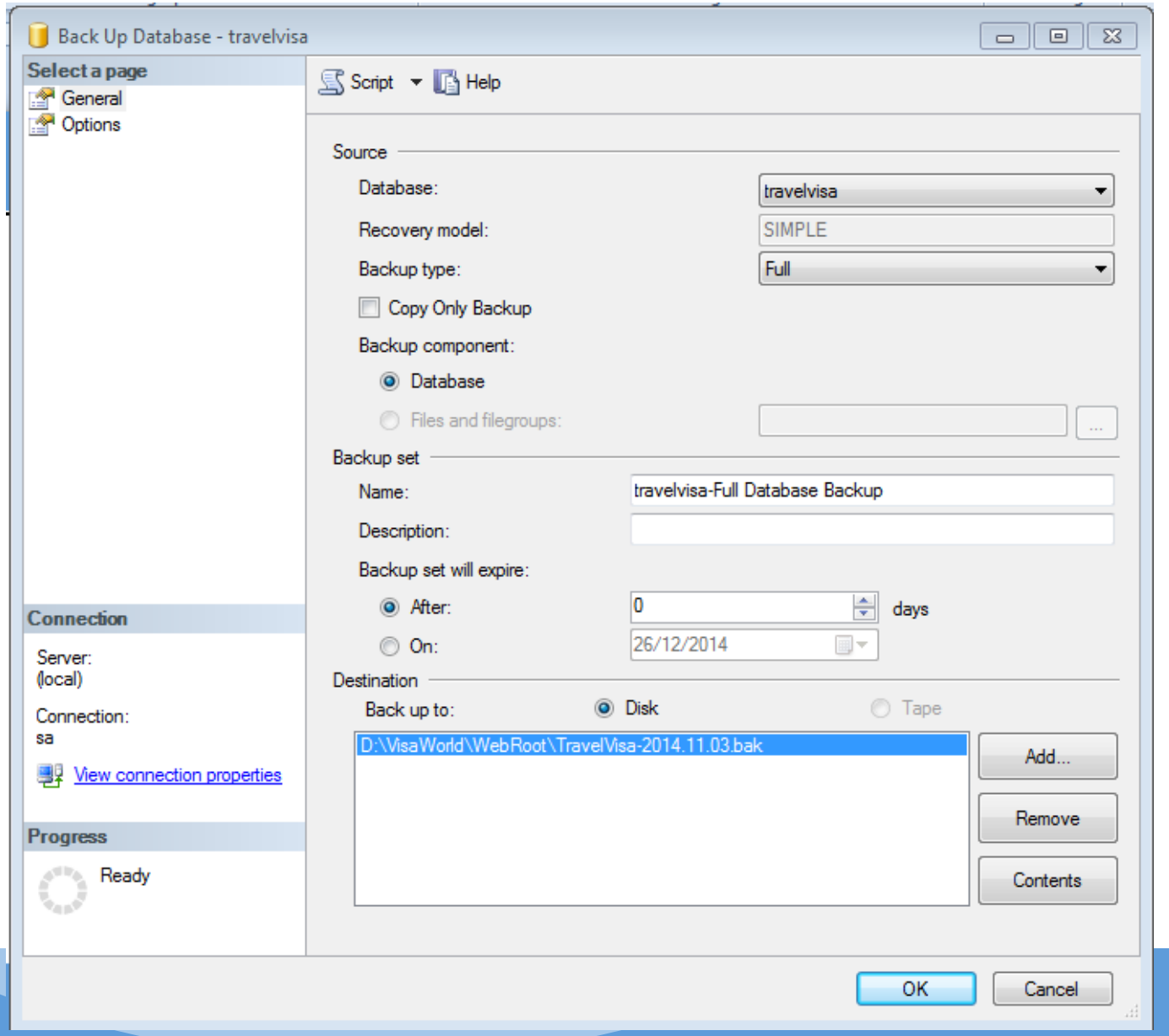


7.1.2 Sao lưu CSDL

- Các dạng sao lưu CSDL:
  - Sao lưu toàn bộ (Full backup): Sao lưu toàn bộ dữ liệu tại thời điểm CSDL đang hoạt động.
    - Thường được sử dụng ở lần sao lưu đầu tiên.
    - Nhược điểm: tốn nhiều thời gian và dung lượng đĩa.
  - Sao lưu phần thay đổi (Incremental/Differential backup): chỉ sao lưu phần thay đổi kể từ lần sao lưu gần nhất;
    - Ưu điểm: Thời gian sao lưu ngắn và lượng chiếm đĩa cũng ít hơn.
    - Nhược điểm: Thời gian khôi phục có thể dài hơn do một dòng có thể được cập nhật nhiều lần cho đến bản cập nhật mới nhất.

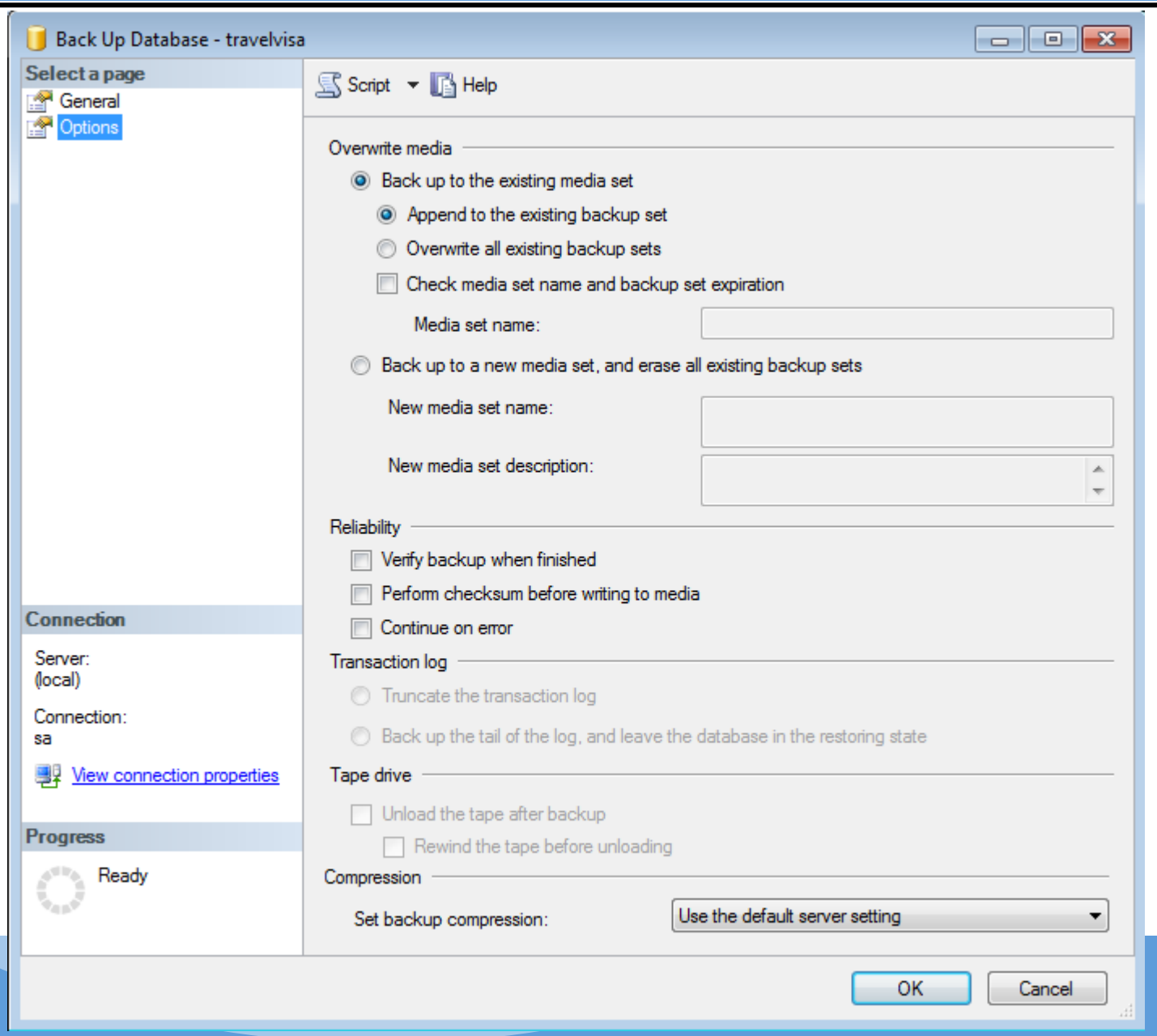
7.1.2 Sao lưu CSDL

- Sao lưu CSDL trong MS-SQL



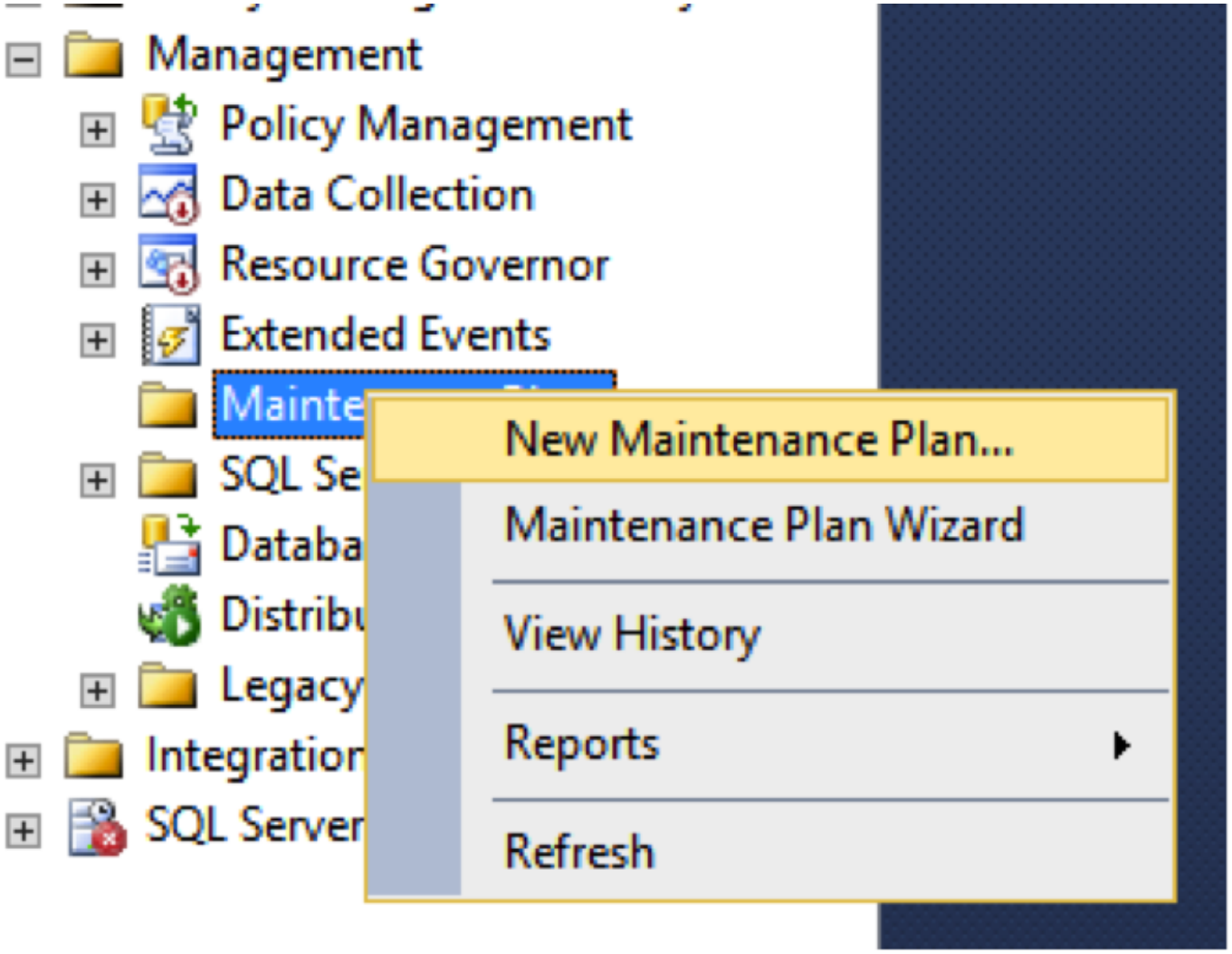
7.1.2 Sao lưu CSDL

- Sao lưu CSDL trong MS-SQL



7.1.2 Sao lưu CSDL

- Tạo nhiệm vụ sao lưu CSDL trong MS-SQL sử dụng Maintenance Plan



7.1.2 Sao lưu CSDL

- Các mô hình khôi phục (Recovery) khi lựa chọn sao lưu:
  - Simple: Mô hình khôi phục đơn giản
  - Full: Mô hình khôi phục đầy đủ
  - Bulk_log: Mô hình khôi phục theo log khối.

- Các mô hình khôi phục có ưu & nhược điểm riêng, nhưng trong thực tế, mô hình Simple và Full được sử dụng phổ biến.

7.1.2 Sao lưu CSDL

- Các mô hình khôi phục (Recovery) khi lựa chọn sao lưu:
  - Simple: Mô hình khôi phục đơn giản
    - Một số thao tác có thể tạo log tối thiểu (ít log);
    - Không hỗ hợ sao lưu logs;
    - Không hỗ trợ khôi phục theo trang và theo thời điểm;
    - Hỗ trợ khôi phục file, nhưng chỉ giới hạn với các file dữ liệu thứ cấp theo chế độ chỉ đọc.

7.1.2 Sao lưu CSDL

- Các mô hình khôi phục (Recovery) khi lựa chọn sao lưu:
  - Full: Mô hình khôi phục đầy đủ
    - Tất cả các thao tác được logs đầy đủ;
    - Hỗ trợ sao lưu logs;
    - Hỗ trợ khôi phục tất cả các thao tác, bao gồm cả khôi phục theo thời điểm, theo trang và khôi phục theo file.

7.1.2 Sao lưu CSDL

- Các mô hình khôi phục (Recovery) khi lựa chọn sao lưu:
  - Bulk_log: Mô hình khôi phục the log khối
    - Hoạt động tương tự như mô hình Full, trừ khi một số thao tác theo mẻ được log tối thiểu;
    - Hỗ trợ khôi phục các thao tác tương tự như Full;
    - Tuy nhiên Bulk_log không hỗ trợ khôi phục theo thời điểm khi các thao tác được log tối thiểu.

7.1.2 Sao lưu CSDL

❖ Sao lưu sử dụng lệnh (MS-SQL):

BACKUP DATABASE { database_name | @database_name_var } TO <backup_device> [WITH { DIFFERENTIAL | <general_WITH_options>

trong đó:

<backup_device>::= { { logical_device_name | @logical_device_name_var } | { DISK | TAPE | URL} = { 'physical_device_name' | @physical_device_name_var } }

Ví dụ:

BACKUP DATABASE test_db to DISK = 'D:\backups\test_db.bak'

7.1.2 Sao lưu CSDL

- Sao lưu sử dụng lệnh (MS-SQL): Sao lưu với tên file tạo theo thời gian:

```
DECLARE @FileName AS NVARCHAR(255)
SET @FileName = 'D:\backups\MyDatabase-' + CAST(DATEPART
   (yy, GETUTCDATE()) AS NVARCHAR(4))

  +CASE WHEN DATEPART(mm, GETUTCDATE()) BETWEEN 1 AND 9 THEN '0'
     ELSE '' END + CAST(DATEPART(mm, GETUTCDATE()) AS NVARCHAR
     (2))
  +CASE WHEN DATEPART(dd, GETUTCDATE()) BETWEEN 1 AND 9 THEN '0'
     ELSE '' END + CAST(DATEPART(dd,GETUTCDATE()) AS NVARCHAR
     (2))
  +CASE WHEN DATEPART(hh, GETUTCDATE()) BETWEEN 1 AND 9 THEN '0'
     ELSE '' END + CAST(DATEPART(hh, GETUTCDATE()) AS NVARCHAR
     (2))
  +CASE WHEN DATEPART(mi, GETUTCDATE()) BETWEEN 0 AND 9 THEN '0'
     ELSE '' END + CAST(DATEPART(mi, GETUTCDATE()) AS NVARCHAR
     (2))
  +CASE WHEN DATEPART(ss, GETUTCDATE()) BETWEEN 0 AND 9 THEN '0'
     ELSE '' END + CAST(DATEPART(ss, GETUTCDATE()) AS NVARCHAR
     (2)) + '.bak'
BACKUP DATABASE MyDatabase TO DISK=@FileName
```

7.1.2 Sao lưu CSDL

- Sao lưu log giao dịch:
  - File log giao dịch (transaction log) lưu một dãy các bản ghi log, lưu trữ các bản ghi quá khứ, các thay đổi đã được thực hiện trên CSDL;
  - Log giao dịch cũng cần được sao lưu định kỳ, kèm theo việc sao lưu CSDL;
  - Đây là việc cần thiết để hỗ trợ khả năng khôi phục theo thời điểm và khống chế kích thước của file log;
  - Phụ thuộc vào kiểu ghi log lựa chọn trong kiểu backup (Simple, Full hoặc Bulk_Log), khả năng khôi phục CSDL là khác nhau.

7.1.2 Sao lưu CSDL

- Sao lưu file:
  - Cho phép sao lưu một file, hoặc một nhóm các file dữ liệu cụ thể;
  - Giảm thời gian sao lưu, trong trường hợp không phải sao lưu toàn bộ CSDL;
  - Hỗ trợ các kiểu sao lưu file:
    - Full: Sao lưu toàn bộ
    - Partial: Sao lưu một phần
    - Differential: Chỉ sao lưu thay đổi so với lần sao lưu trước đó. Dạng này có thể áp dụng với cả Full và Partial.

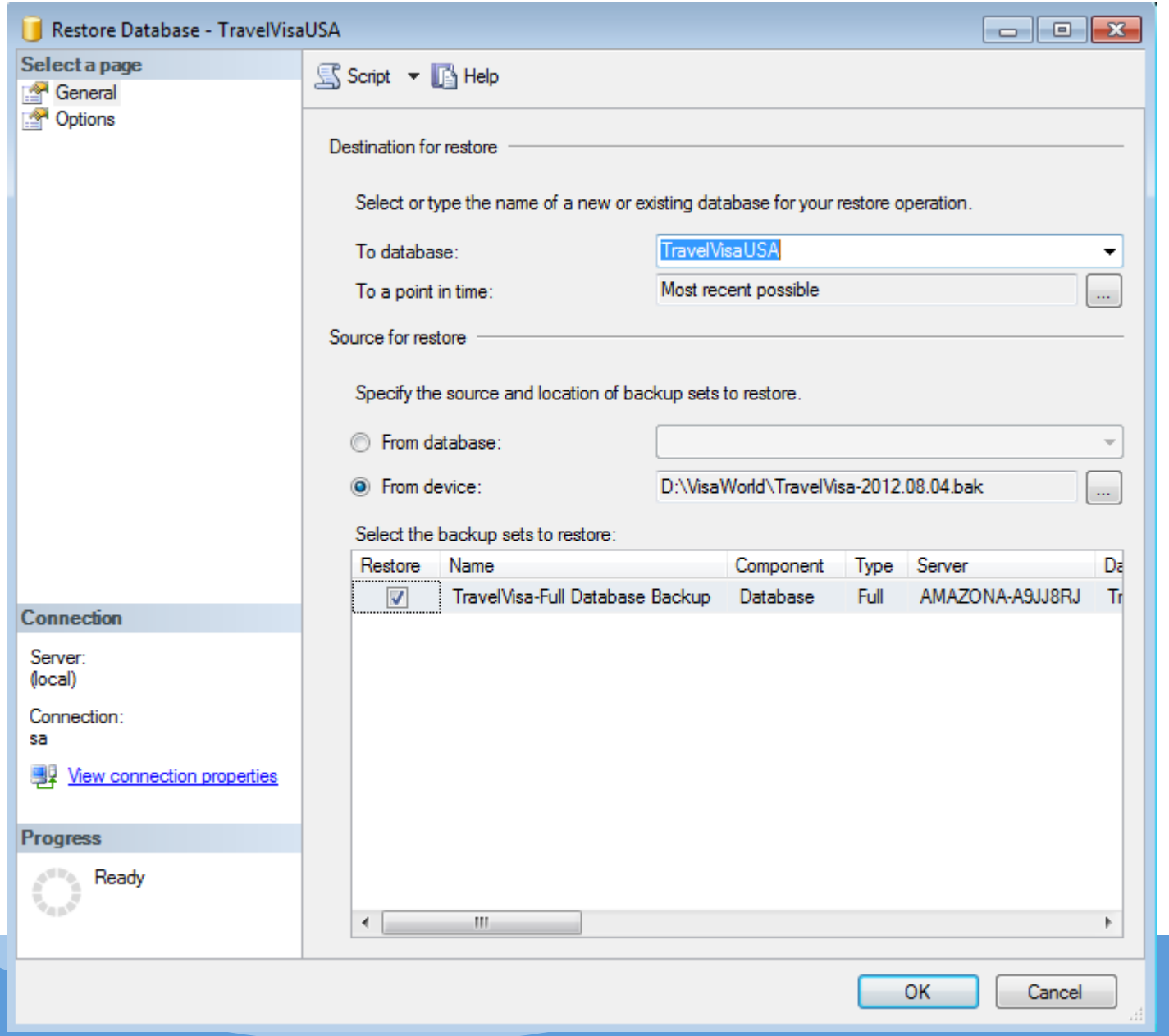
7.1.3 Khôi phục dự phòng CSDL

- Khôi phục dự phòng CSDL là việc khôi phục lại một phần hoặc toàn bộ CSDL khi CSDL có sự cố;
- Đây một nhiệm vụ khó khăn đòi hỏi người thực hiện cần có kiến thức và kinh nghiệm về quản trị CSDL;
- Khôi phục dự phòng CSDL có thể được thực hiện nhờ:
  - Sử dụng bản sao lưu CSDL;
  - Sử dụng file sao lưu CSDL;
  - Sử dụng log giao dịch CSDL.

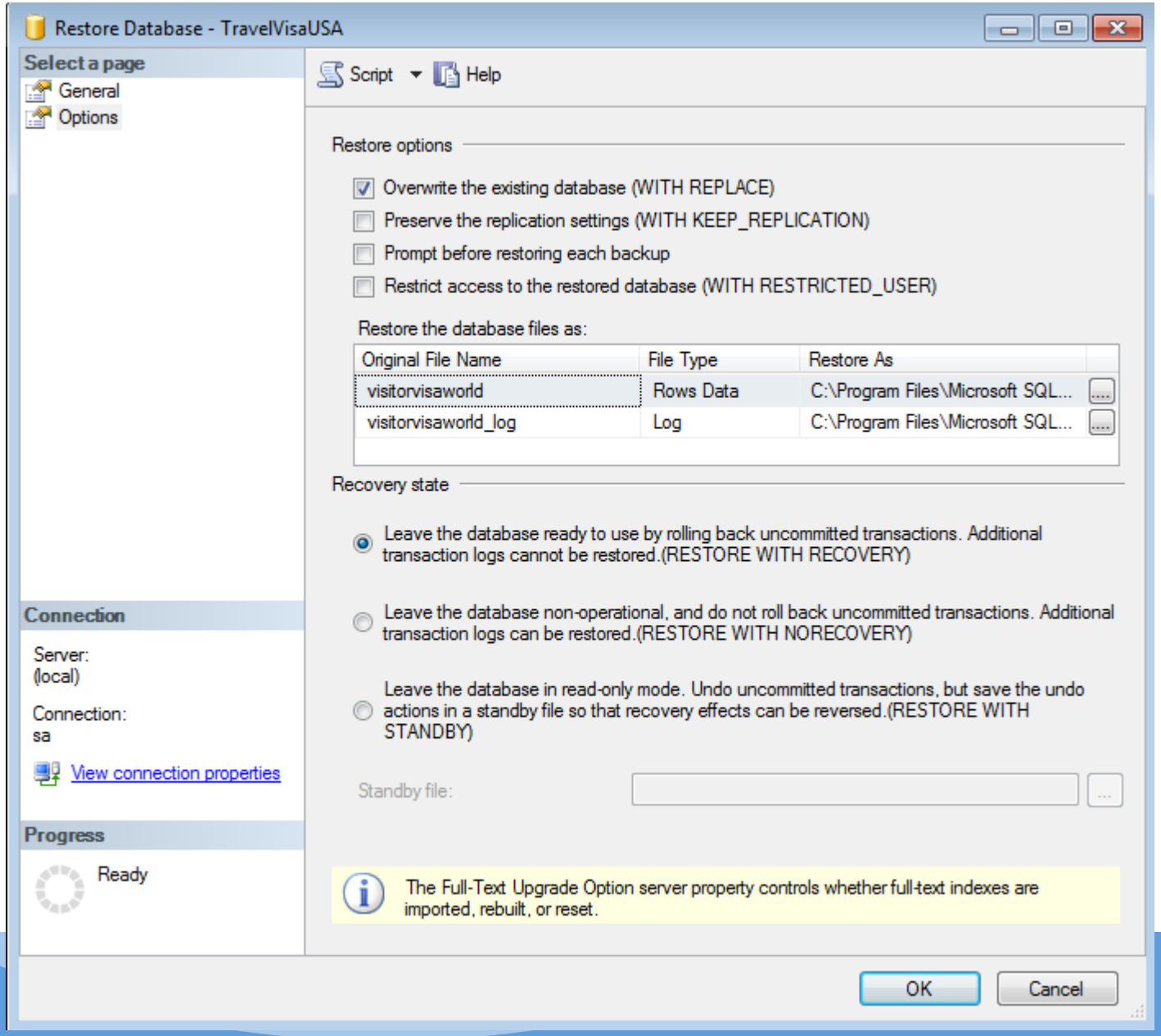
7.1.3 Khôi phục dự phòng CSDL

- Xác định kiểu khôi phục:
  - Khôi phục toàn bộ (Full recovery)
  - Khôi phục một phần (Partial recovery): Khôi phục đến một thời điểm nào đó.
  - Khôi phục theo giao dịch (Transactional recovery): đòi hỏi công cụ bổ sung của bên thứ 3.
- Kiểm tra sau khôi phục:
  - Kiểm tra dữ liệu để đảm bảo dữ liệu được khôi phục đầy đủ, chính xác.

7.1.3 Khôi phục dự phòng CSDL



7.1.3 Khôi phục dự phòng CSDL



7.1.3 Khôi phục dự phòng

❖ Khôi phục sử dụng lệnh (MS-SQL):

RESTORE DATABASE { database_name | @database_name_var }

[FROM <backup_device> [,...n]]

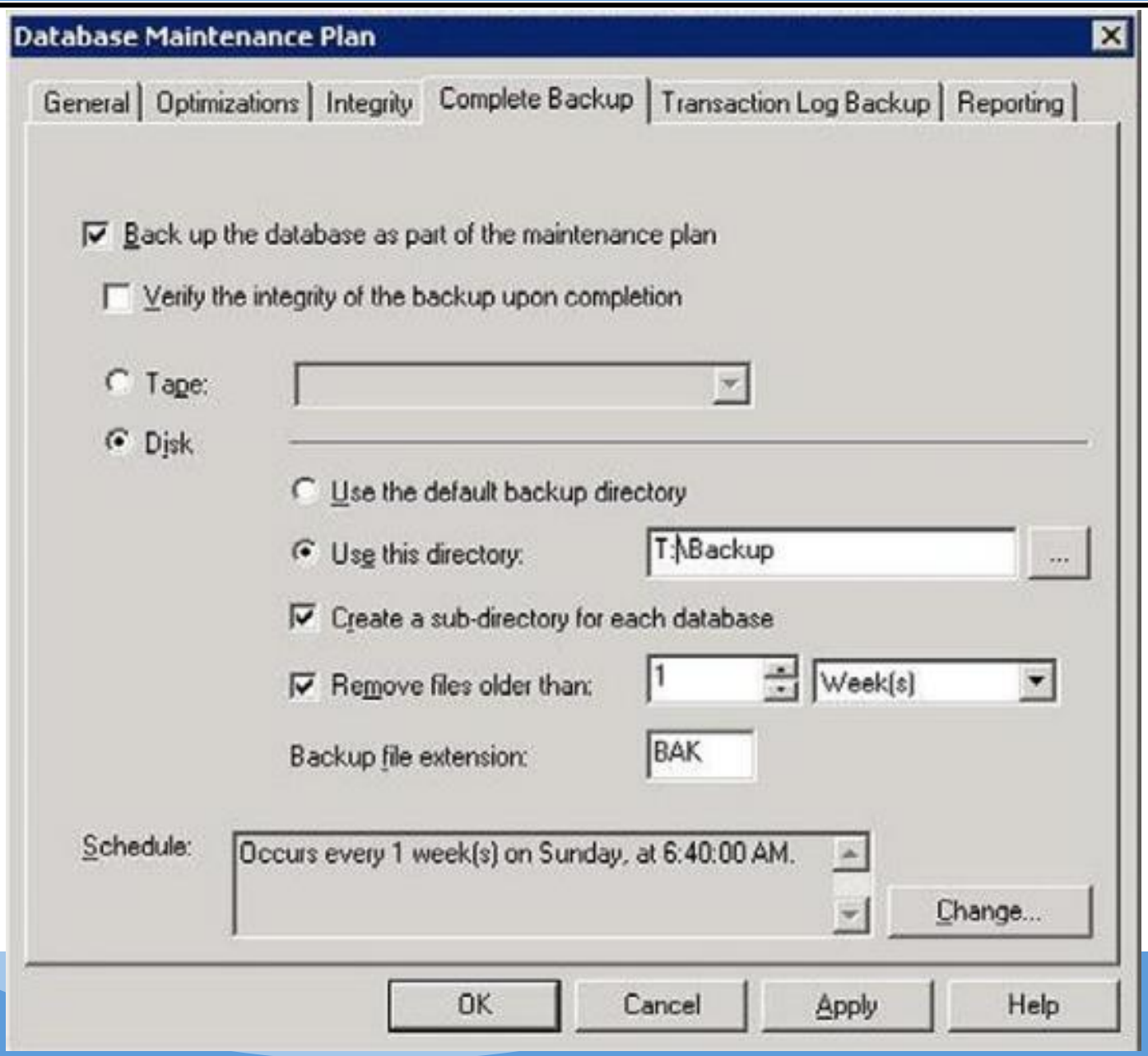
[WITH { [RECOVERY | NORECOVERY | STANDBY
= {standby_file_name | @standby_file_name_var }] | ,
<general_WITH_options> [,...n] | , <replication_WITH_option> | ,
<change_data_capture_WITH_option> | ,
<FILESTREAM_WITH_option> | , <service_broker_WITH
options> | , <point_in_time_WITH_options—RESTORE_DATABASE> } [
,...n]]

7.1.4 An toàn dữ liệu sao lưu

- Ghi đè/dọn dẹp file sao lưu nhằm hạn chế "rác" sao lưu:
  - Có thể sử dụng lựa chọn ghi đè lên file sao lưu cũ
  - Hoặc ghi file mới và xóa các file sao lưu cũ.
- Sử dụng mật khẩu để bảo vệ file sao lưu:
  - Đặt mật khẩu cho phương tiện lưu trữ
  - Đặt mật khẩu cho file sao lưu để tránh khôi phục ngẫu nhiên.

```
BACKUP DATABASE YourDB TO DISK='D:\YourDB.bak'
WITH MEDIANAME='YourMediaPassword',
   PASSWORD='YourBackupSetPassword',
   FORMAT
```

7.1.4 An toàn dữ liệu sao lưu



7.1.4 An toàn dữ liệu sao lưu

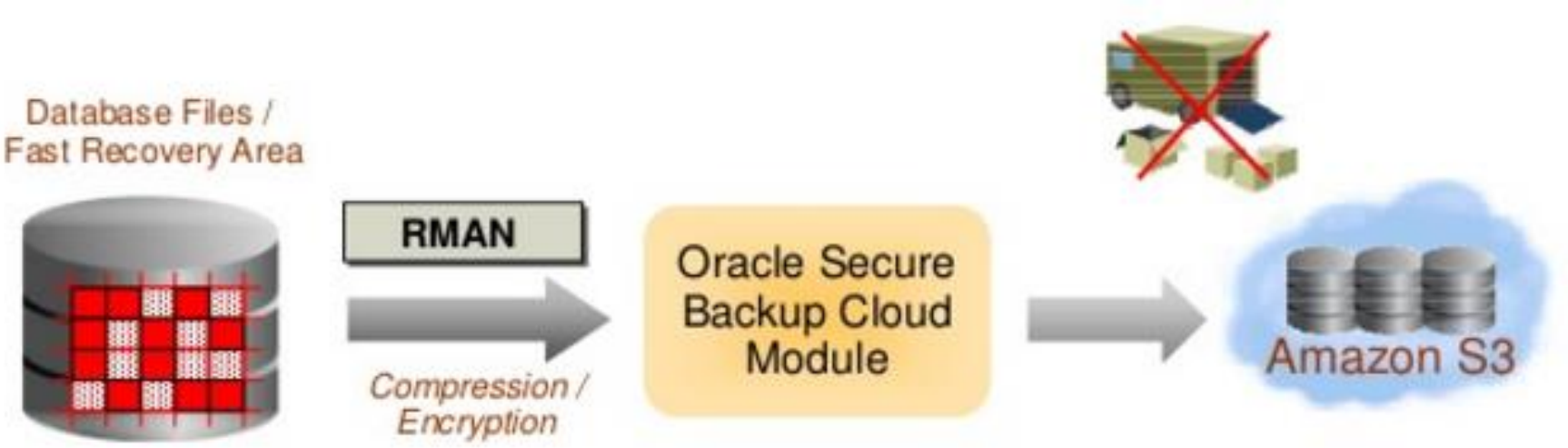
- Mã hóa file sao lưu: dùng để bảo vệ CSDL lưu trong file sao lưu.
  - Một số công cụ mã hóa file sao lưu:
    - LiteSpeed for SQL Server
    - Red Gate SQL HyperBac
    - Các giải pháp sao lưu của bên thứ 3
  - Mã hóa sử dụng Transparent Data Encryption
    - Transparent Data Encryption là một công nghệ của Microsoft cho phép mã hóa dữ liệu theo khối khi ghi vào và giải mã khi đọc ra.
- Nén và mã hóa file sao lưu CSDL
  - Kết hợp nén và mã hóa để giảm kích thước file sao lưu CSDL.

7.1.4 An toàn dữ liệu sao lưu

- Offsite backup:
  - Là dạng sao lưu CSDL và/hoặc các thông tin liên quan sang thiết bị lưu trữ/hệ thống khác;
  - Nhằm đảm bảo an toàn cho dữ liệu trong trường hợp có sự cố đối với tòa nhà hoặc một khu vực/thành phố.
  - Tuy nhiên, cần đảm bảo an ninh cho các file sao lưu offsite do chúng có thể bị đánh cắp và lạm dụng:
    - Mã hóa file sao lưu;
    - Mã hóa đường truyền dữ liệu từ hệ thống nguồn đến hệ thống lưu trữ file sao lưu;
    - Sử dụng nhân viên có thể tin cậy trong trường hợp vận chuyển file sao lưu trong các thiết bị lưu trữ như ổ đĩa hoặc băng từ.

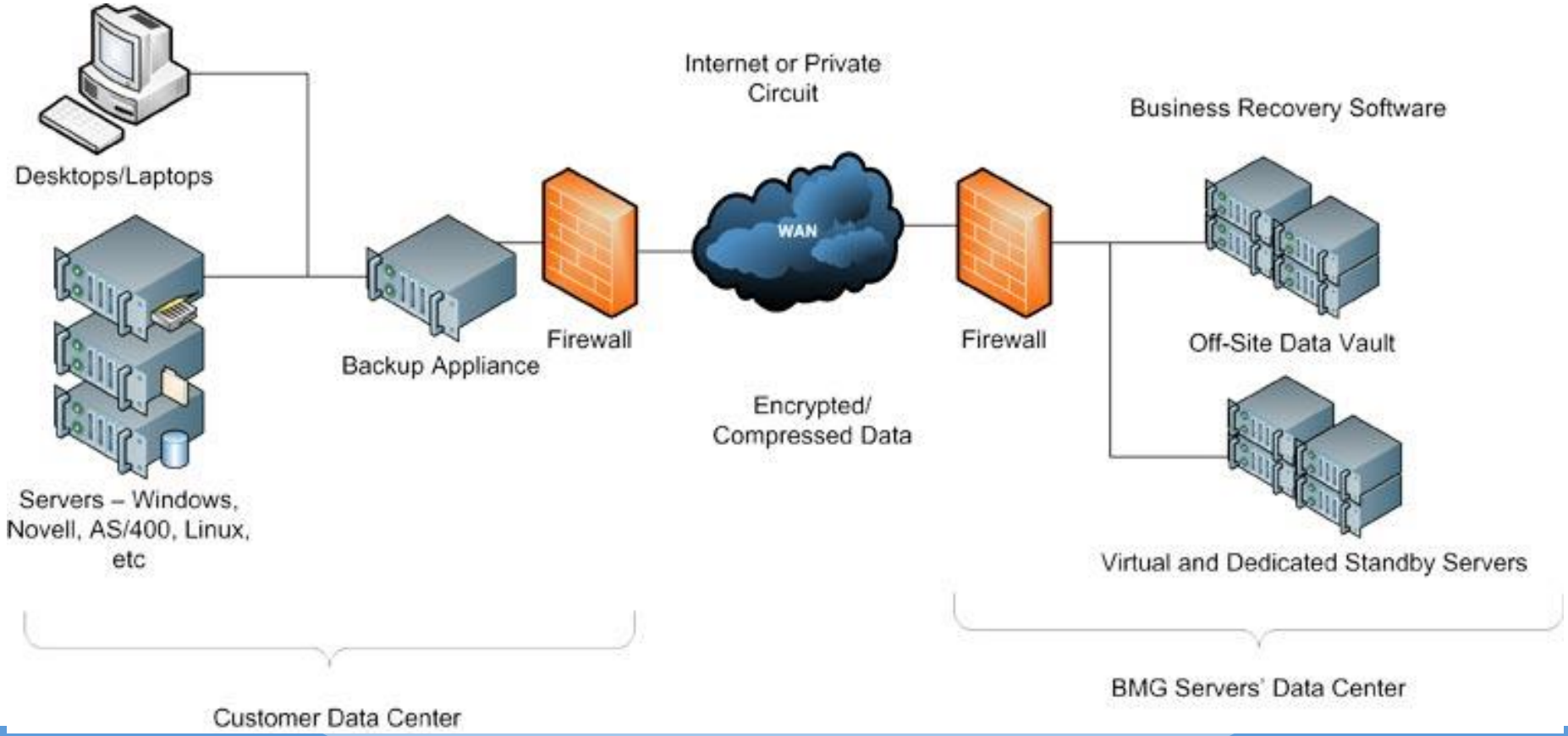
7.1.4 An toàn dữ liệu sao lưu

❖ Offsite backup to Cloud



7.1.4 An toàn dữ liệu sao lưu

❖ Một mô hình Offsite backup



7.2 Kiểm toán cơ sở dữ liệu

1. Giới thiệu chung
2. Các dạng kiểm toán CSDL
3. Một số vấn đề liên quan đến kiểm toán CSDL
4. Một số công cụ kiểm toán CSDL

Tại sao cần kiểm toán CSDL?

Kiểm toán CSDL giúp trả lời câu hỏi:

Who did what to which data, when and how?

(Ai đã thực hiện cái gì trên dữ liệu nào, vào khi nào và bằng cách nào?)

7.2.1 Giới thiệu chung

- Kiểm toán CSDL (Database auditing):
  - Là việc giám sát các hành vi của người dùng thực hiện trên CSDL;
  - Người quản trị CSDL thường cài đặt tính năng kiểm toán CSDL vì mục đích an ninh, nhằm đảm bảo những người không có thẩm quyền không được phép truy nhập vào dữ liệu.
  - Là một trong khâu quan trọng giúp người quản trị CSDL truy tìm nguyên nhân của các vấn đề/sự cố xảy ra với hệ thống và từ đó có biện pháp khắc phục phù hợp.

7.2.1 Giới thiệu chung

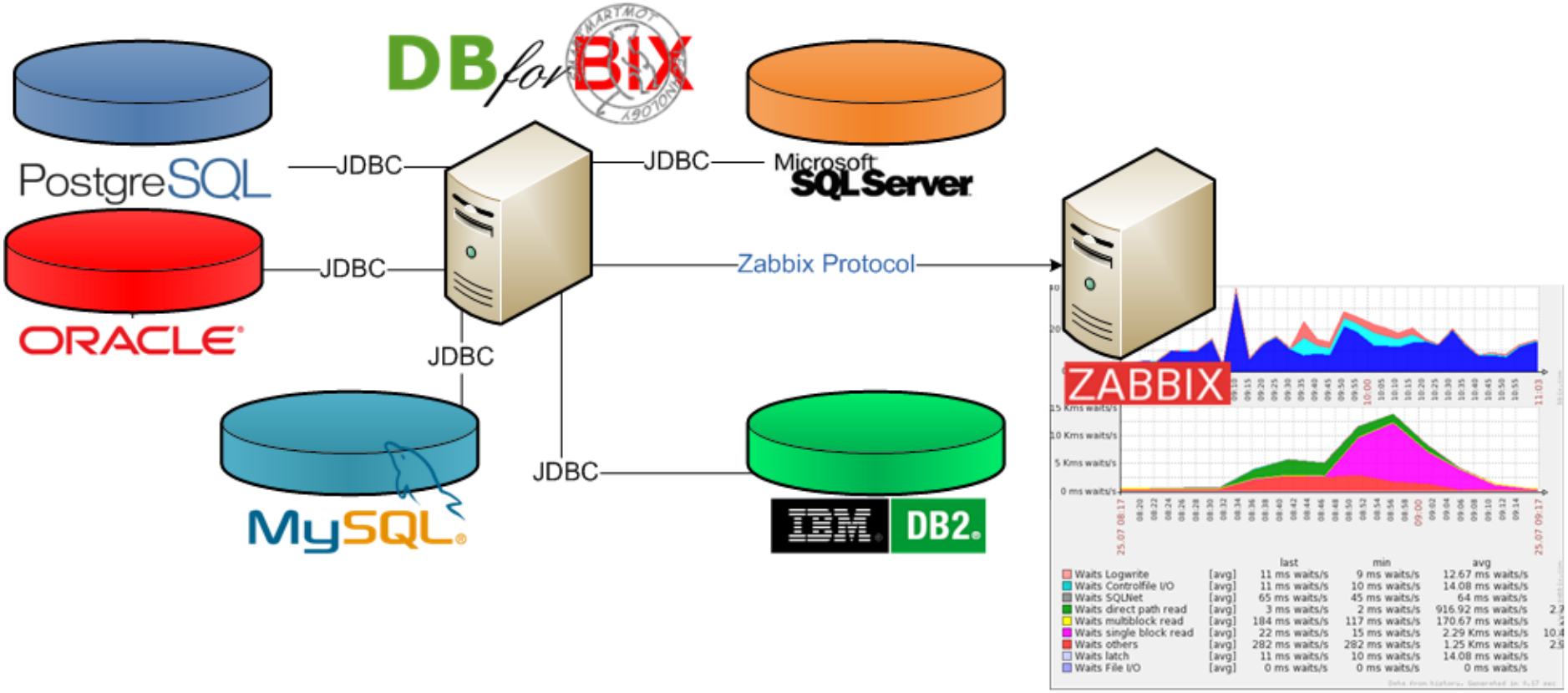
- Kiểm toán CSDL (Database auditing):
  - Việc giám sát cần được thực hiện thường xuyên trong suốt quá trình hoạt động của CSDL.
  - Việc xem xét các thông tin giám sát cần được thực hiện định kỳ để sớm phát hiện các bất thường/sự cố trong hệ thống.

7.2.1 Giới thiệu chung

- Kiểm toán CSDL =
  Giám sát CSDL +
  Xem xét việc tuân thủ các chính sách quản trị và bảo mật CSDL;
- Giám sát là một khâu bắt buộc nhằm thu thập dữ liệu cần thiết cho kiểm toán CSDL.

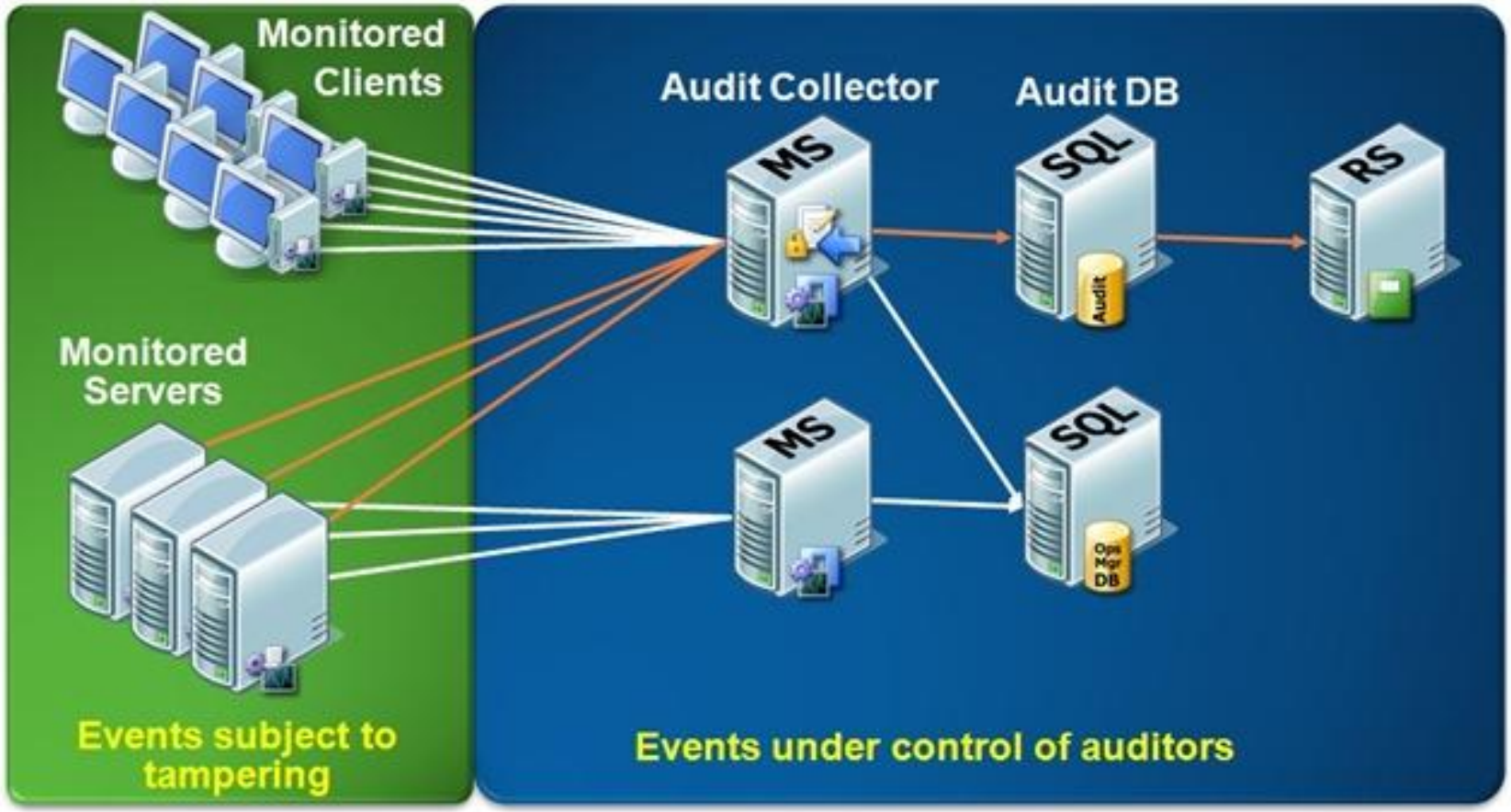
7.2.1 Giới thiệu chung

❖ Giám sát tập trung sử dụng hệ thống Zabbix



7.2.1 Giới thiệu chung

- Mô hình giám sát & kiểm toán các sự kiện diễn ra trong CSDL



7.2.2 Các dạng kiểm toán CSDL

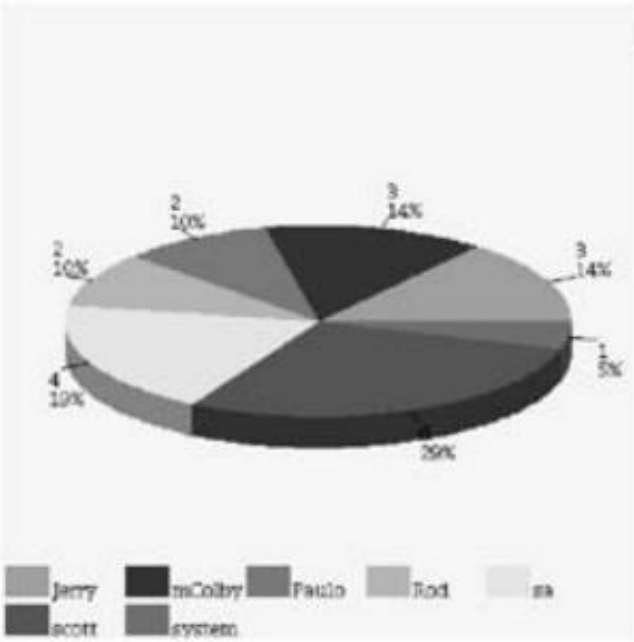
- Kiểm toán đăng nhập/đăng xuất CSDL
- Kiểm toán nguồn sử dụng CSDL
- Kiểm toán hoạt động DDL
- Kiểm toán lỗi CSDL
- Kiểm toán thay đổi mã nguồn của thủ tục, triger
- Kiểm toán thay đổi đặc quyền và thông tin truy nhập
- Kiểm toán việc thay đổi các dữ liệu nhạy cảm

7.2.2 Các dạng kiểm toán CSDL

- Kiểm toán đăng nhập/đăng xuất CSDL:
  - Giám sát các thao tác đăng nhập (sign-on, log-on) và đăng xuất (sign-out, log-out) của người dùng CSDL;
  - Các thông tin cần thu thập về 2 sự kiện trên bao gồm:
    - Username
    - Địa chỉ IP của client
    - Tên ứng dụng client
    - Thời gian
    - Trạng thái (thành công, thất bại).

7.2.2 Các dạng kiểm toán CSDL

- Kiểm toán đăng nhập/đăng xuất CSDL:
  - Logs chi tiết các sự kiện đăng nhập thất bại:



Failed Login Details

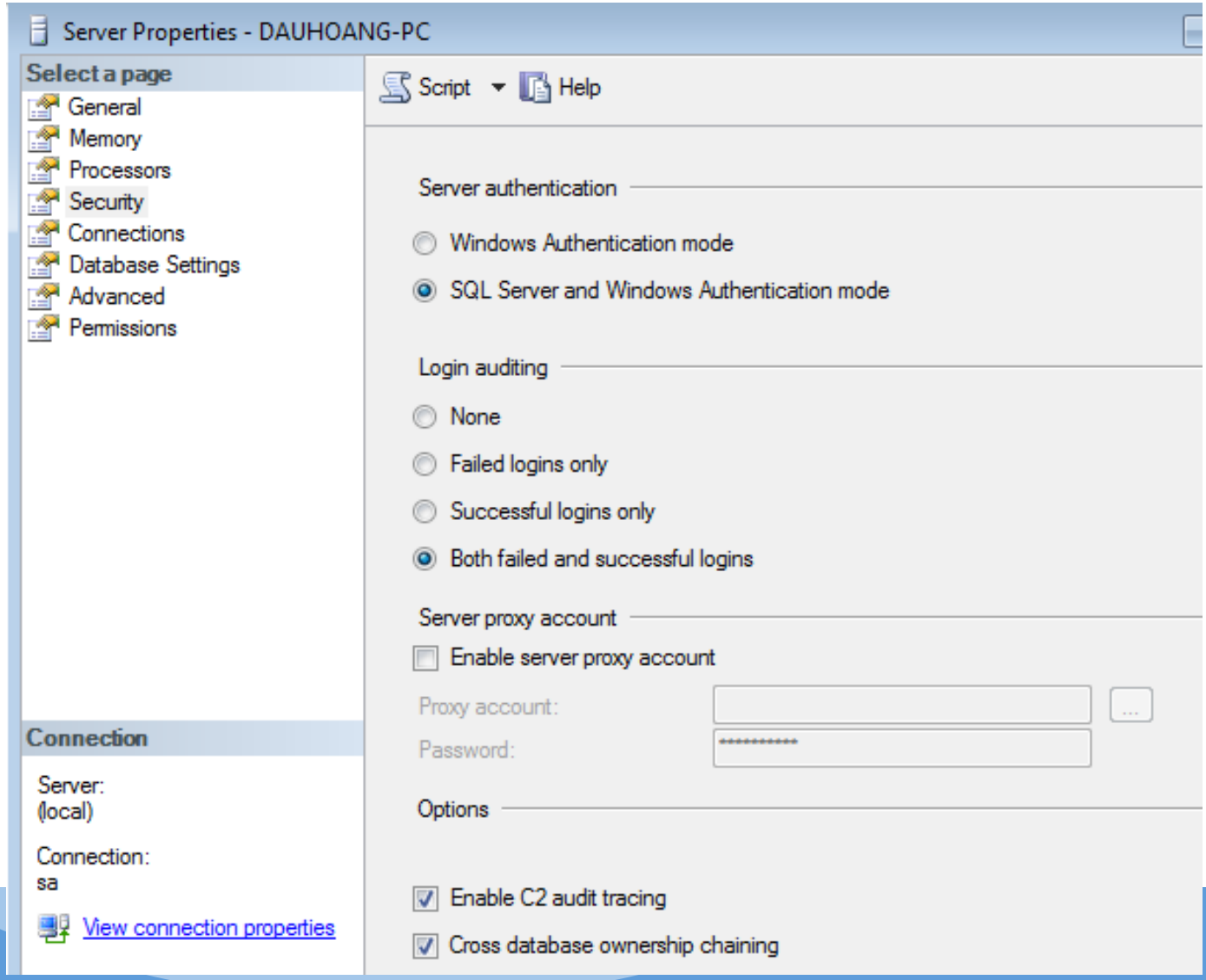
Time	User	coming from	to	using	Count of Exceptions
2004-08-11 12:06:06	scott	192.168.1.106	192.168.2.12	TNS	1
2004-08-11 12:06:11	scott	192.168.1.106	192.168.2.12	TNS	1
2004-08-11 12:06:12	scott	192.168.1.106	192.168.2.12	TNS	1
2004-08-11 12:06:15	scott	192.168.1.106	192.168.2.12	TNS	1
2004-08-11 12:06:17	scott	192.168.1.106	192.168.2.12	TNS	2
2004-08-11 12:06:19	system	192.168.1.106	192.168.2.12	TNS	1
2004-08-26 11:36:16	sa	155.212.221.82	155.212.221.84	MS SQL SERVER	1
2004-08-26 12:12:21	sa	155.212.221.82	155.212.221.84	MS SQL SERVER	1
2004-08-26 14:58:34	mColby	155.212.221.82	155.212.221.84	MS SQL SERVER	1
2004-08-26 14:58:36	mColby	155.212.221.82	155.212.221.84	MS SQL SERVER	1
2004-08-26 14:58:38	mColby	155.212.221.82	155.212.221.84	MS SQL SERVER	1
2004-10-04 17:22:50	Rod	155.212.221.82	155.212.221.84	MS SQL SERVER	1
2004-10-04 17:22:52	Rod	155.212.221.82	155.212.221.84	MS SQL SERVER	1
2004-11-02 15:14:03	sa	155.212.221.82	155.212.221.84	MS SQL SERVER	1
2004-11-02 15:16:24	Jerry	155.212.221.82	155.212.221.84	MS SQL SERVER	1
2004-11-02 15:16:26	Jerry	155.212.221.82	155.212.221.84	MS SQL SERVER	1
2004-11-02 15:16:27	Jerry	155.212.221.82	155.212.221.84	MS SQL SERVER	1
2004-11-03 13:53:58	Paulo	155.212.221.82	155.212.221.84	MS SQL SERVER	1
2004-11-03 13:54:01	Paulo	155.212.221.82	155.212.221.84	MS SQL SERVER	1
2004-12-01 15:18:56	sa	155.212.221.82	155.212.221.84	MS SQL SERVER	1

Records: 1 To 20 From 20

Show Aliases: OFF

7.2.2 Các dạng kiểm toán CSDL

- Thiết lập audit cho các sự kiện đăng nhập, đăng xuất.



7.2.2 Các dạng kiểm toán CSDL

❖ Tạo bảng lưu thông tin đăng nhập, đăng xuất:

```
create table user_login_audit
(
   user_id              varchar2(30),
   session_id           number(8),
   host                 varchar2(30),
   login_day            date,
   login_time           varchar2(10),
   logout_day           date,
   logout_time          varchar2(10)
);
```

7.2.2 Các dạng kiểm toán CSDL

- Ghi sự kiện đăng nhập kích hoạt bởi triger:

```
create or replace trigger
  user_login_audit_trigger
AFTER LOGON ON DATABASE
BEGIN
insert into user_login_audit values(
   user,
   sys_context('USERENV','SESSIONID'),
   sys_context('USERENV','HOST'),
   sysdate,
   to_char(sysdate, 'hh24:mi:ss'),
   null,
   null
);
COMMIT;
END;
```

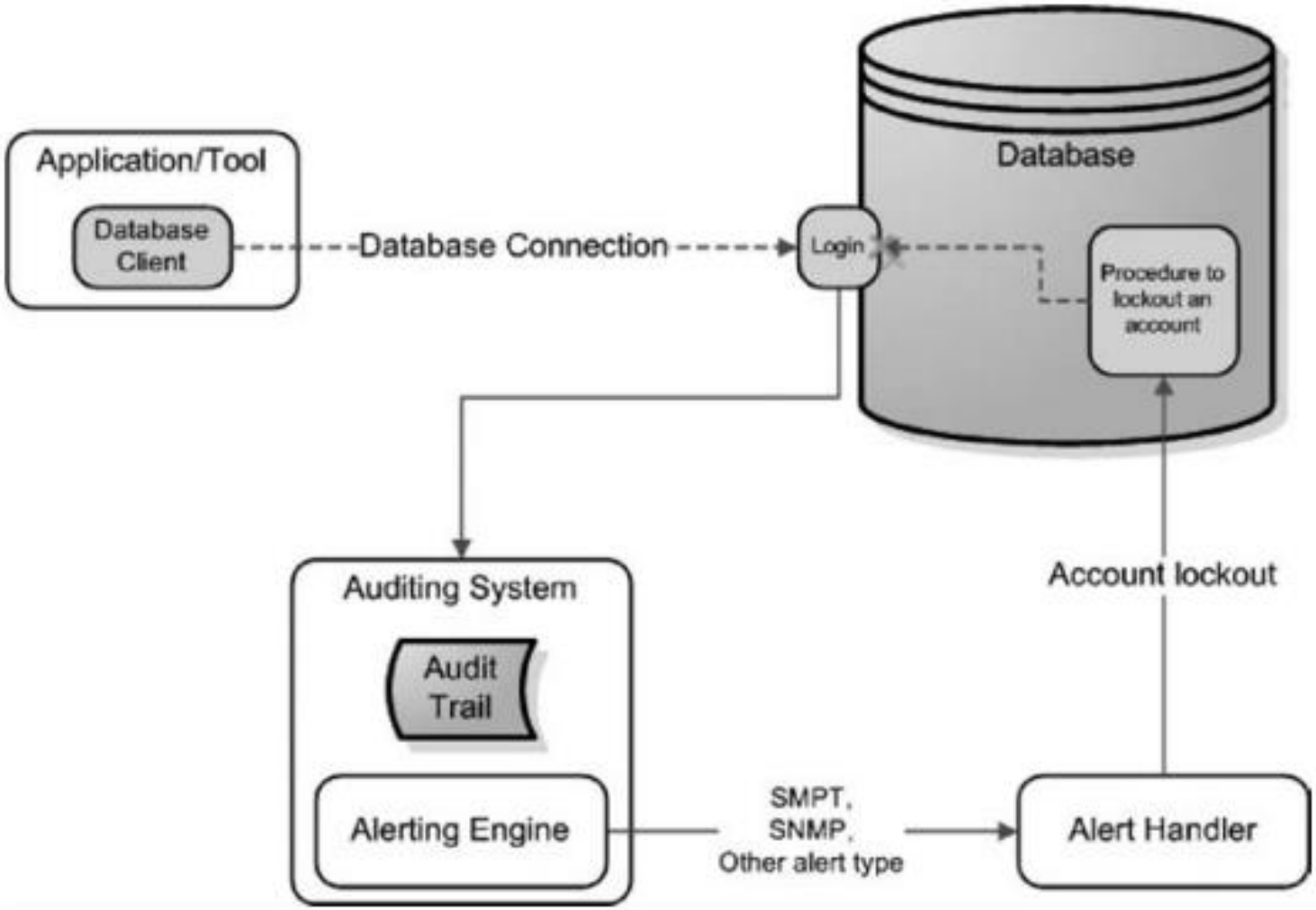
7.2.2 Các dạng kiểm toán CSDL

- Ghi sự kiện đăng xuất kích hoạt bởi triger:

```
create or replace trigger
   user_logout_audit_trigger
BEFORE LOGOFF ON DATABASE
BEGIN
-- logout day
update
   user_login_audit
set
   logout_day = sysdate
where
   sys_context('USERENV','SESSIONID') = session_id;
-- logout time
update
   user_login_audit
set
   logout_time = to_char(sysdate, 'hh24:mi:ss')
where
   sys_context('USERENV','SESSIONID') = session_id;
COMMIT;
END;
```

7.2.2 Các dạng kiểm toán CSDL

❖ Tạm khóa tài khoản khi đăng nhập thất bại nhiều lần:



7.2.2 Các dạng kiểm toán CSDL

- Kiểm toán nguồn sử dụng CSDL
  - Nguồn sử dụng CSDL gồm địa chỉ IP và tên ứng dụng, hoặc nút mạng kết nối đến CSDL.
  - Cần thu thập thông tin nguồn sử dụng CSDL cho các hoạt động:
    - Kết nối và đăng nhập vào CSDL
    - Thực hiện các lệnh SQL.

7.2.2 Các dạng kiểm toán CSDL

❖ Kiểm toán nguồn sử dụng CSDL

Client IP	Source Program	SQL Verb	Depth	Object Name	Total access
155.212.221.82	SQL Query Analyzer	SELECT	0	products	9
155.212.221.82	SQL Query Analyzer	SELECT	0	customers	4
155.212.221.82	SQL Query Analyzer	SELECT	0	fred1	6
155.212.221.82	SQL Query Analyzer	CREATE TABLE	0	fred	3
155.212.221.82	SQL Query Analyzer	SELECT	0	fred	7
155.212.221.82	SQL Query Analyzer	INSERT	0	fred	6
155.212.221.82	SQL Query Analyzer	DELETE	0	fred	4
155.212.221.82	SQL Query Analyzer	DROP TABLE	0	fred	4
155.212.221.82	SQL Query Analyzer	EXECUTE	0	sp_addcgn	8
155.212.221.82	SQL Query Analyzer	GRANT	0	mcolby	4
155.212.221.82	SQL Query Analyzer	SELECT	0	@@trancount	14
155.212.221.82	SQL Query Analyzer	GRANT	0	dave	2
155.212.221.82	Aqua_Data_Studio	SELECT	0	master.dbo.sysobjects	1
155.212.221.82	Aqua_Data_Studio	SELECT	0	charindex	1
155.212.221.82	Aqua_Data_Studio	SELECT	0	type_name	1
155.212.221.82	Aqua_Data_Studio	SELECT	0	convert	1
155.212.221.82	Aqua_Data_Studio	USE	0	master	3
155.212.221.82	Aqua_Data_Studio	SELECT	0	char	1
155.212.221.82	Aqua_Data_Studio	SELECT	0	odbcscale	1
155.212.221.82	Aqua_Data_Studio	SELECT	0	master.dbo.syscolumns	1

Records: 21 To 40 From 1364

7.2.2 Các dạng kiểm toán CSDL

- Kiểm toán hoạt động DDL (Data description language):
  - Là kiểm toán việc thay đổi lược đồ (schema), hoặc cấu trúc các bảng trong CSDL;
  - Các thay đổi về cấu trúc CSDL cần được giám sát chặt chẽ do chúng ảnh hưởng lớn đến các thao tác khác và hiệu năng vận hành CSDL;
  - Có thể thực hiện sử dụng:
    - Tính năng kiểm toán cung cấp bởi CSDL;
    - Sử dụng hệ thống kiểm toán độc lập;
    - So sánh các snapshot của các lược đồ CSDL.

7.2.2 Các dạng kiểm toán CSDL

❖ Kiểm toán hoạt động DDL: Tạo bảng lưu thông tin DDL:

```
create table ddl_audit_trail
(
   user_id              varchar2(30),
   ddl_date             date,
   event_type           varchar2(30),
   object_type          varchar2(30),
   owner                varchar2(30),
   object_name          varchar2(30)
);
```

7.2.2 Các dạng kiểm toán CSDL

❖ Kiểm toán hoạt động DDL: Ghi thông tin DDL sử dụng triger:

```
create or replace trigger
  DDL_trigger
AFTER DDL ON DATABASE
BEGIN
    insert into ddl_audit_trail (
       user_id,
       ddl_date,
       event_type,
       object_type,
       owner,
       object_name
    )
    VALUES
    (
                                    ora_login_user,
                                    sysdate,
                                    ora_sysevent,
                                    ora_dict_obj_type,
                                    ora_dict_obj_owner,
                                    ora_dict_obj_name
                                );
END;
```

7.2.2 Các dạng kiểm toán CSDL

- Kiểm toán lỗi CSDL:
  - Giám sát và ghi các thông tin về các lỗi xảy ra khi thực hiện các thao tác với CSDL;
  - Từ thông tin giám sát có thể phân tích, tìm ra các lỗ hổng, hoặc các nỗ lực tấn công CSDL;
    - Tin tặc chèn thêm các ký tự đặc biệt vào dữ liệu gây lỗi câu lệnh SQL để tìm lỗ hổng chèn mã SQL.

7.2.2 Các dạng kiểm toán CSDL

❖ Kiểm toán lỗi CSDL: Ví dụ về thông tin lỗi ghi được

Event ID	Event Class	Description
16	Attention	Collects all attention events, such as client-interrupt requests or when a client connection is broken.
21	ErrorLog	Error events have been logged in the error log.
22	EventLog	Events have been logged in the application log.
33	Exception	Exception has occurred in the server.
67	Execution Warnings	Any warnings that occurred during the execution of a server statement or stored procedure.

7.2.2 Các dạng kiểm toán CSDL

- Kiểm toán thay đổi mã nguồn của thủ tục, hàm, triger
  - Cần giám sát và ghi logs sự thay đổi mã nguồn của các thủ tục, hàm và các triger;
  - Cần logs các thông tin: ai thực hiện sửa, nội dung thay đổi và thời gian;
  - Từ đó có thể lần vết và khắc phục khi có lỗi xảy ra;
  - Có thể sử dụng công cụ quản lý mã nguồn (hỗ trợ change tracking), hoặc sử dụng tính năng audit trong CSDL.

7.2.2 Các dạng kiểm toán CSDL

- Kiểm toán thay đổi đặc quyền và thông tin truy nhập:
  - Các thay đổi thông tin người dùng và quyền truy nhập cần được giám sát và ghi logs;
  - Các thông tin cần ghi logs có thể gồm:
    - Thêm hoặc xóa người dùng, tài khoản đăng nhập và các vai trò;
    - Các thay đổi với các ánh xạ giữa tài khoản đăng nhập và người dùng/vai trò;
    - Thay đổi đặc quyền (có thể do người dùng hoặc vai trò);
    - Thay đổi mật khẩu;
    - Thay đổi các thuộc tính an ninh tại máy chủ, CSDL, lệnh, hoặc ở mức đối tượng CSDL.

7.2.2 Các dạng kiểm toán CSDL

- Kiểm toán thay đổi đặc quyền và thông tin truy nhập: Các sự kiện được ghi logs:

Event ID	Event Class	Description
102	Audit Statement GDR	Occurs every time a GRANT, DENY, REVOKE for a statement permission is issued by any user in SQL Server.
103	Audit Object GDR	Occurs every time a GRANT, DENY, REVOKE for an object permission is issued by any user in SQL Server.
104	Audit Add/Drop Login	Occurs when a SQL Server login is added or removed—`sp_addlogin` and `sp_droplogin`.
105	Audit Login GDR	Occurs when a Windows login right is added or removed—`sp_grantlogin`, `sp_revokelogin`, and `sp_denylogin`.

7.2.2 Các dạng kiểm toán CSDL

- Kiểm toán việc thay đổi các dữ liệu nhạy cảm:
  - Các thay đổi với dữ liệu nhạy cảm cần được giám sát để có thể phát hiện các sửa đổi bất hợp pháp;
  - Dữ liệu lưu ngoài sự kiện xảy ra còn cần phải lưu thông tin (bản ghi) trước thay đổi và bản ghi sau thay đổi;
  - Cần xem xét thực hiện giám sát và ghi logs trong những trường hợp thực sự cần thiết do lượng dữ liệu phát sinh có thể rất lớn.

7.2.3 Một số vấn đề liên quan đến kiểm toán CSDL

- Cần xử lý dữ liệu giám sát, kiểm toán:
  - Dữ liệu giám sát, kiểm toán cần được xử lý để trích xuất ra các thông tin có giá trị, làm cơ sở cho các hành động phù hợp:
    - Đăng nhập sai nhiều lần → Cảnh báo + Tạm khóa tài khoản
    - Truy nhập dữ liệu nhạy cảm ngoài giờ vận hành thông thường → cảnh báo và tạm khóa truy nhập.

7.2.3 Một số vấn đề liên quan đến kiểm toán CSDL

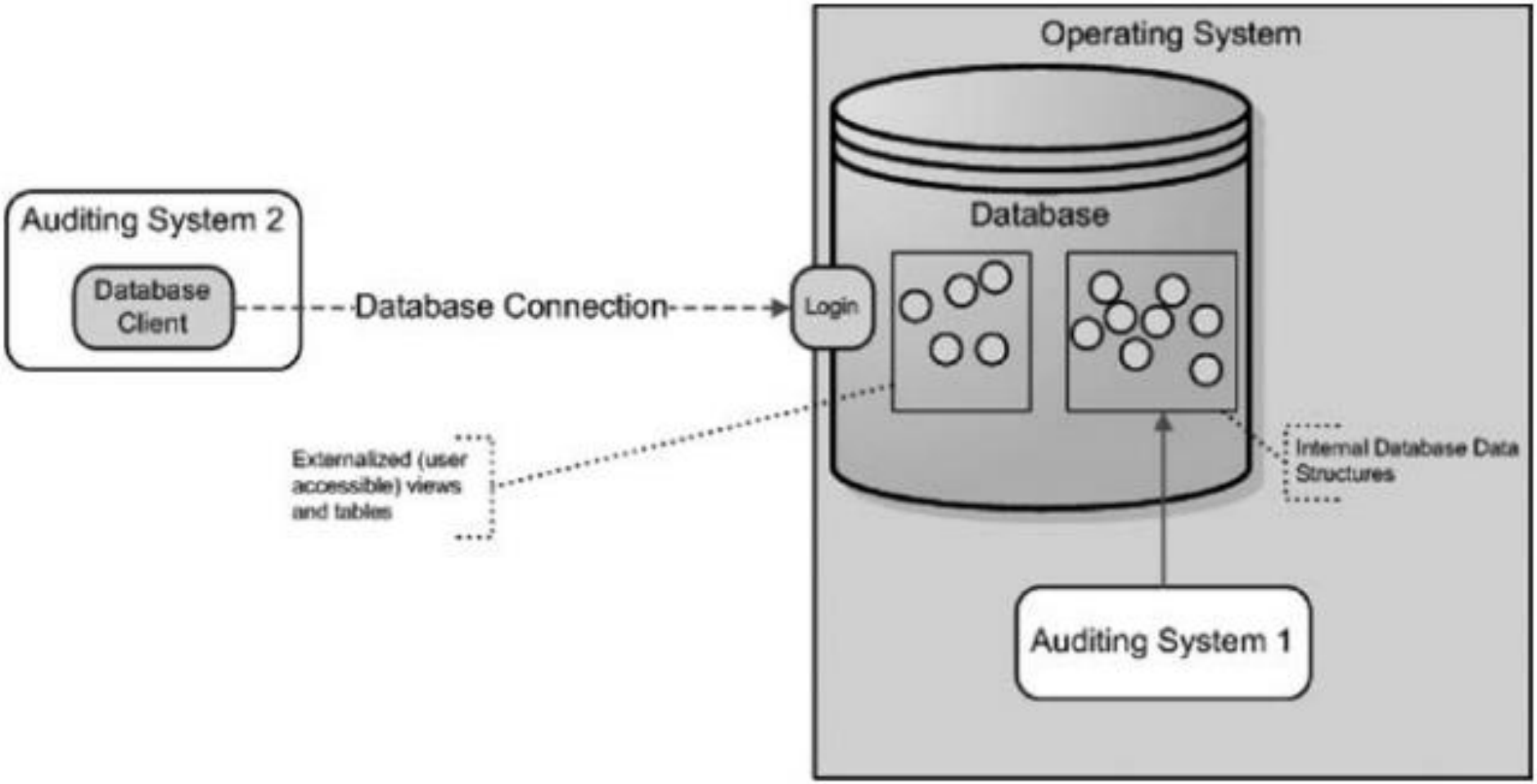
- Xem xét sử dụng hệ thống giám sát – kiểm toán độc lập:
  - Các tính năng giám sát – kiểm toán hỗ trợ bởi CSDL có:
    - Ưu điểm: đơn giản, rẻ tiền;
    - Nhược điểm: Tính năng hạn chế, độ an toàn không cao.
  - Các hệ thống giám sát – kiểm toán độc lập:
    - Được thiết kế theo mô hình defense-in-depth nên thường có độ an toàn cao;
    - Cung cấp tính năng thu thập và xử lý dữ liệu phong phú;
    - Xử lý độc lập nên ít ảnh hưởng đến hiệu năng vận hành của CSDL.

7.2.3 Một số vấn đề liên quan đến kiểm toán CSDL

- Các kiến trúc của các hệ thống kiểm toán độc lập: gồm 3 dạng kiến trúc sử dụng cho các mục đích sau:
  - Kiểm tra cấu trúc dữ liệu nội bộ của cơ sở dữ liệu
  - Kiểm tra tất cả các giao tiếp 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.

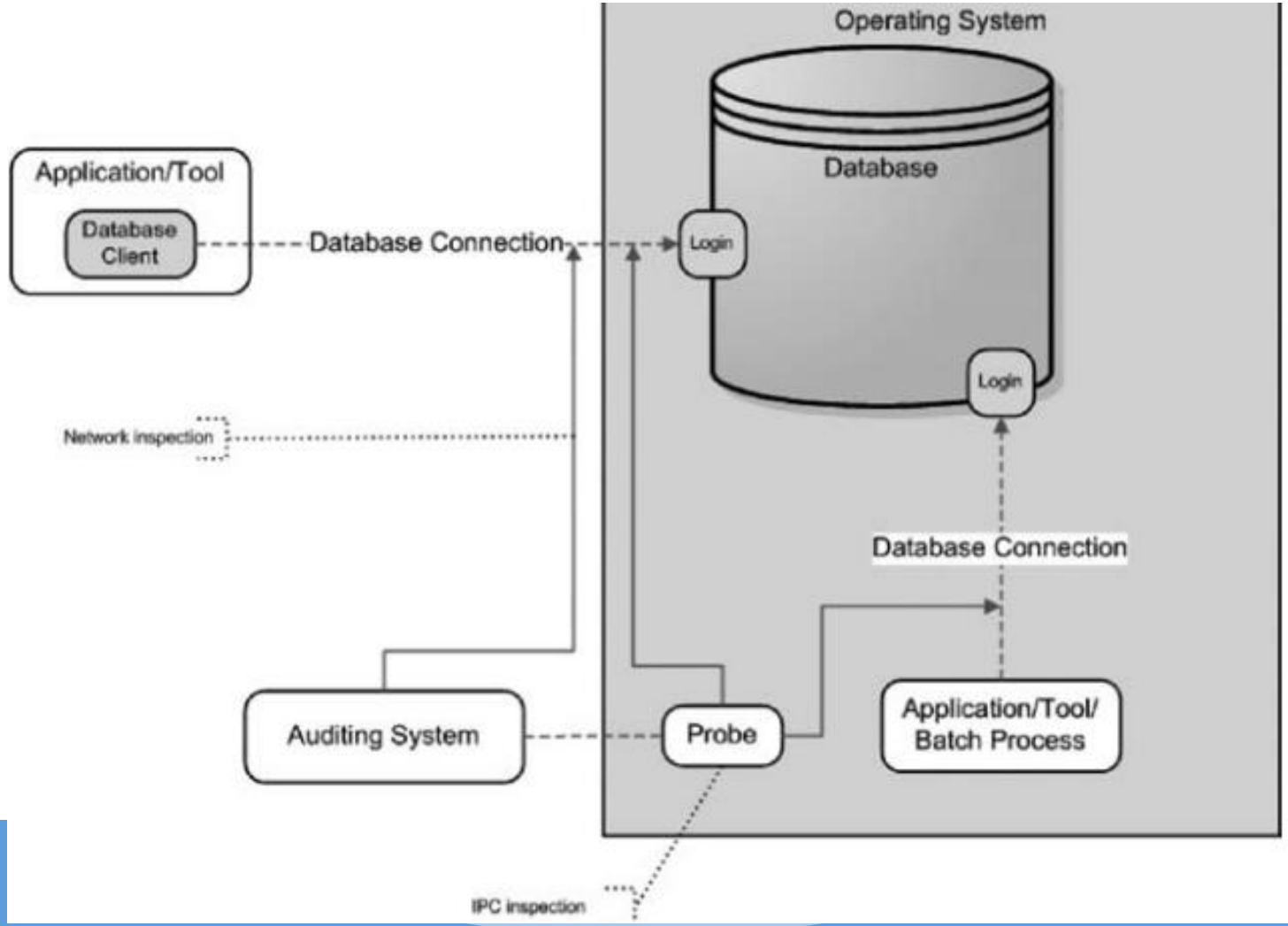
7.2.3 Một số vấn đề liên quan đến kiểm toán CSDL

❖ Kiểm tra cấu trúc dữ liệu nội bộ của cơ sở dữ liệu



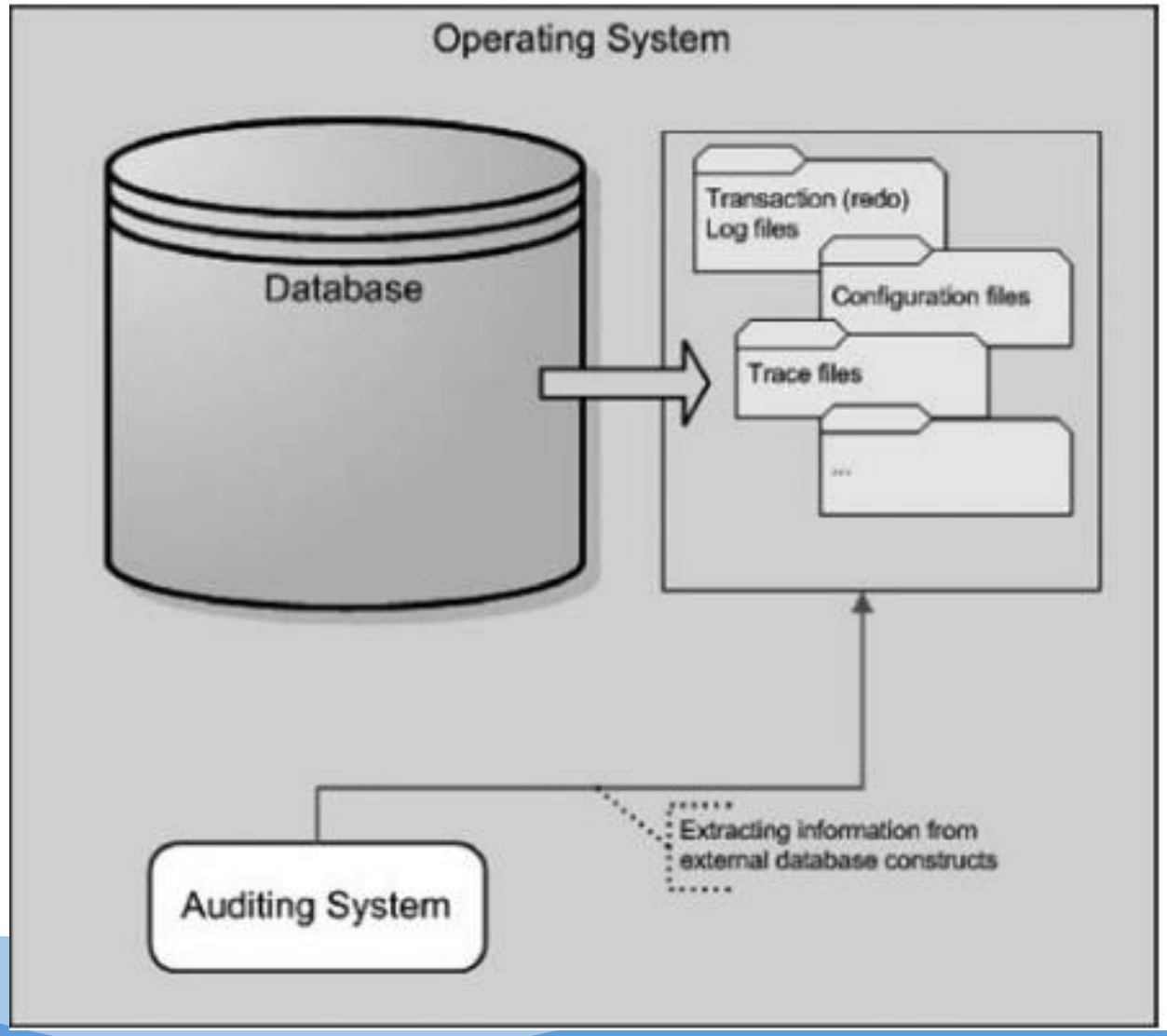
7.2.3 Một số vấn đề liên quan đến kiểm toán CSDL

❖ Kiểm tra tất cả các giao tiếp với cơ sở dữ liệu



7.2.3 Một số vấn đề liên quan đến kiểm toán CSDL

Kiểm tra các yếu tố được tạo ra bởi cơ sở dữ liệu trong quá trình hoạt động bình thường



7.2.3 Một số vấn đề liên quan đến kiểm toán CSDL

❖ Lưu trữ dữ liệu kiểm toán:

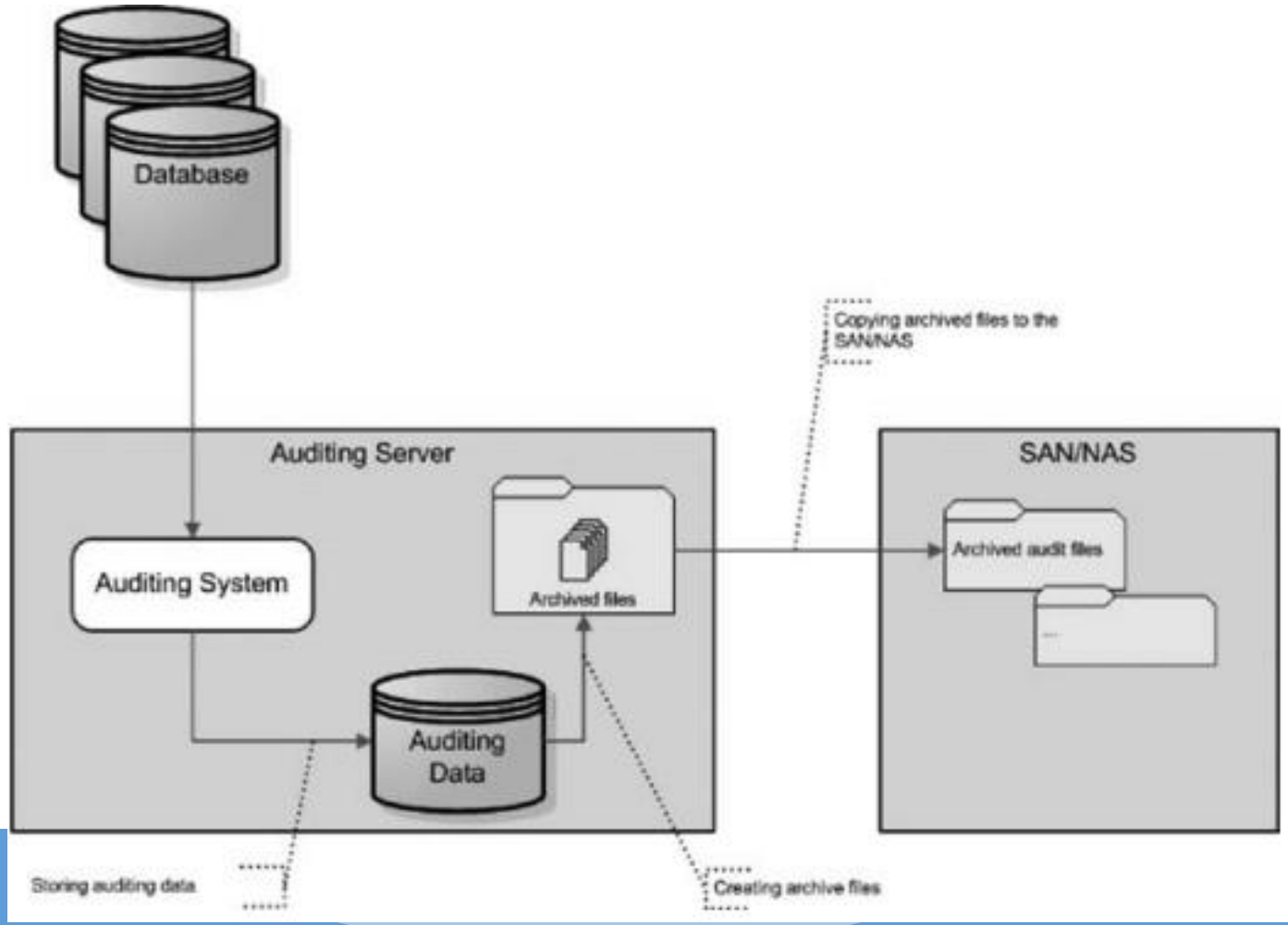
- Dữ liệu giám sát/kiểm toán có thể rất lớn → cần lựa chọn thiết bị lưu trữ và phương pháp quản lý, lưu trữ cho phù hợp;
  - Lưu tại máy chủ CSDL
  - Sử dụng các hệ thống lưu trữ chuyên dụng (RAID, NAS, SAN,...)
- Nếu dữ liệu kiểm toán được lưu trong cùng CSDL chính, hoặc trong cùng máy chủ CSDL, cần có cơ chế giám sát bổ sung do dữ liệu kiểm toán có thể chiếm hết dung lượng đĩa và làm máy chủ CSDL ngừng hoạt động;
- Định kỳ, dữ liệu kiểm toán cần được chuyển ra thiết bị lưu trữ khác, giải phóng dung lượng đĩa cho dữ liệu mới.

7.2.3 Một số vấn đề liên quan đến kiểm toán CSDL

- Bảo mật dữ liệu kiểm toán:
  - Dữ liệu kiểm toán có thể chứa nhiều thông tin nhạy cảm → cần các biện pháp bảo mật lưu trữ, tránh truy nhập trái phép;
  - Các biện pháp bảo mật cần được thực hiện trên:
    - Kho chứa dữ liệu kiểm toán
    - Các file lưu trữ trong máy chủ kiểm toán
    - Các file lưu trữ trong quá trình vận chuyển
    - Các file lưu trữ tại nơi lưu trữ lâu dài.

7.2.3 Một số vấn đề liên quan đến kiểm toán CSDL

❖ 4 vị trí cần bảo mật dữ liệu kiểm toán:



7.2.3 Một số vấn đề liên quan đến kiểm toán CSDL

- Kiểm toán hệ thống kiểm toán:
  - Dữ liệu kiểm toán có thể chứa nhiều thông tin nhạy cảm, nên cần được giám sát quá trình sử dụng, thay đổi.

Activity Type Description	User Name	Timestamp	Modified Entity	Modified Attribute	Modified Value	Orig. Value
UPDATE	infosec	2004-11-29 11:00:41	USER	USER.USER_ID	1	1
UPDATE	infosec	2004-11-29 11:59:58	USER	USER.USER_ID	15	1
UPDATE	infosec	2004-11-29 12:13:04	AUDIT_RULE	AUDIT_RULE.AUDIT_RULE_ID	20001	1
UPDATE	infosec	2004-11-29 12:52:01	USER	USER.USER_ID	15	1
UPDATE	infosec	2004-11-29 12:52:54	AUDIT_RULE	AUDIT_RULE.AUDIT_RULE_ID	20001	1
UPDATE	infosec	2004-11-29 13:51:24	USER	USER.USER_ID	15	1
UPDATE	infosec	2004-11-29 13:58:43	USER	USER.USER_ID	15	1
UPDATE	infosec	2004-11-29 15:18:47	AUDIT_RULE	AUDIT_RULE.AUDIT_RULE_ID	20001	1
UPDATE	infosec	2004-11-29 15:45:55	USER	USER.USER_ID	1	1
UPDATE	infosec	2004-11-29 16:54:57	USER	USER.USER_ID	15	1
UPDATE	infosec	2004-11-29 16:58:00	USER	USER.USER_ID	1	1
UPDATE	infosec	2004-11-29 16:58:04	AUDIT_RULE	AUDIT_RULE.AUDIT_RULE_ID	20001	1
UPDATE	infosec	2004-11-29 17:12:21	AUDIT_RULE	AUDIT_RULE.AUDIT_RULE_ID	20001	1
UPDATE	infosec	2004-11-29 17:14:14	AUDIT_RULE	AUDIT_RULE.AUDIT_RULE_ID	20001	1
UPDATE	infosec	2004-11-29 17:15:51	USER	USER.USER_ID	1	1
UPDATE	infosec	2004-11-29 17:16:23	USER	USER.USER_ID	15	1
UPDATE	infosec	2004-11-29 17:18:28	USER	USER.USER_ID	1	1
UPDATE	infosec	2004-11-29 17:20:25	AUDIT_RULE	AUDIT_RULE.AUDIT_RULE_ID	20002	1
UPDATE	infosec	2004-11-29 17:23:50	AUDIT_RULE	AUDIT_RULE.AUDIT_RULE_ID	20002	1
UPDATE	infosec	2004-11-29 17:27:57	USER	USER.USER_ID	1	1

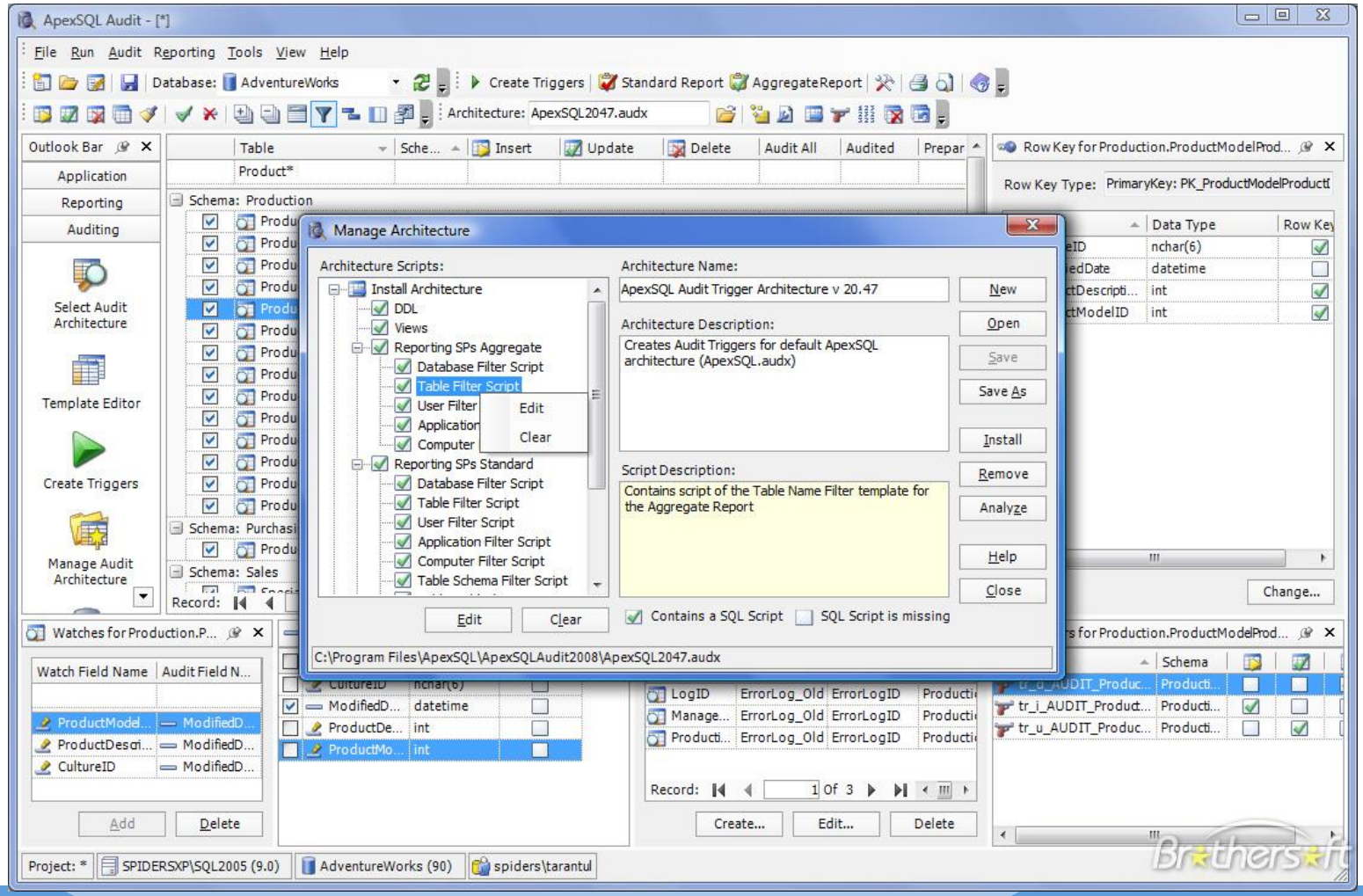
Records: 1 To 20 From 25

7.2.4 Một số công cụ kiểm toán CSDL

- ApexSQL Audit: http://www.apexsql.com/sql_tools_audit.aspx
- Enforcive: http://www.enforcive.com/database-audit-software
- DB Audit: http://www.softtreetech.com/dbaudit/
- PowerBroker Auditor: http://www.beyondtrust.com/Products/PowerBrokerAuditorSQLServer/
- Zabbix: http://www.zabbix.com

7.2.4 Một số công cụ kiểm toán CSDL

ApexSQL Audit



7.2.4 Một số công cụ kiểm toán CSDL

Zabbix