DUY TAN UNIVERSITY

CHƯƠNG 6

AN TOÀN DỮ LIỆU VÀ PHỤC HỒI DỮ LIỆU

NỘI DUNG

1 - An toàn dữ liệu

- Kiểm soát quyền
- Gán quyền

2 - Phục hồi dữ liệu

- Phục hồi dữ liệu khi có sự cố giao dịch, hệ thống và phần cứng.

- **Đường Link you tube**
  - https://www.youtube.com/watch?v=_KjNw7T6ohA&list=PL67CJL04EcjN5PQrippgbVWz9L06a3Atz&index=14

1 - An toàn dữ liệu

An toàn dữ liệu (data security) là một nhiệm vụ quan trọng của hệ thống CSDL nhằm bảo vệ dữ liệu không bị truy xuất "bất hợp pháp".

An toàn dữ liệu bao gồm 2 vấn đề:

Bảo vệ dữ liệu nhằm tránh cho những người "không có phận sự" hiểu được nội dung vật lý của dữ liệu. Chức năng này do hệ thống đảm trách trong các hệ điều hành tập trung và phân tán → Chúng ta sẽ không bàn luận ở đây

Kiểm soát cấp quyền phải đảm bảo rằng chỉ có những người sử dụng được phép mới được thực hiện các thao tác trên CSDL.

Kiểm soát quyền

Ba tác nhân chính có liên quan đến việc kiểm soát cấp quyền là:

1. **Người sử dụng (một người hay 1 nhóm người):** thường được thực hiện bằng 1 cặp (tên người dùng, mật khẩu).
2. **Các thao tác:** insert, select, delete, update, ...
3. **Các đối tượng:** table, database, index, view, ...

Gán quyền

*** Một số quyền:** SELECT , INSERT, DELETE, UPDATE, EXPAND, DROP, INDEX, RUN

**** Có 2 hướng:***

- Tập trung: người có quyền cao nhất (DBA: Database Administrator) thực hiện tất cả các thao tác phân quyền cho người sử dụng

- Không tập trung: người sử dụng có các quyền trên 1 đối tượng nào đó, có thể gán 1 hoặc nhiều quyền cho các người sử dụng khác.

*** Cú pháp:**

GRANT <danh sách quyền> ON <object>

TO <danh sách user> [WITH GRANT OPTION]

*** Ghi chú:**

- Nếu có [**WITH GRANT OPTION**] thì user được gán quyền có thể gán lại 1 số quyền của mình lại cho user khác.

- Có thể thay thế [WITH GRANT OPTION] bằng cách sử dụng ký tự ***** liền sau mỗi quyền trong danh sách các quyền

Ví dụ:

GRANT INSERT* ON table_SINHVIEN TO Huân

GRANT insert, update ON table_SINH VIEN

TO Hoa, Huệ WITH GRANT OPTION

Lấy lại quyền

*** Cú pháp:**

REVOKE <danh sách quyền> ON <object>

FROM <danh sách user>

*** Ví dụ:**

REVOKE insert ON table_SV FROM user1.

Tìm hiểu Security trong SQL Server, Oracle?

2- Phục Hồi Dữ Liệu

- **Mục đích**

  - ✓ **Duy trì CSDL luôn ở trong tình trạng nhất quán.**
  - ✓ **Việc yêu cầu người sử dụng thực hiện lại công việc là ít nhất (khi xảy ra sự cố).**

Các loại sự cố

Sự cố của giao dịch:

Lý do:

- Lỗi trong giao dịch như nhập liệu không đúng
- Xảy ra tình trạng deadlock, livelock
- Bộ lập lịch yêu cầu sắp xếp lại (Rollback)

Tần số: khoảng 3% số giao dịch bị huỷ bỏ 1 cách bất thường.

Ảnh hưởng: Sự cố này không ảnh hưởng đến tính nhất quán của hệ thống.

Sự cố vị trí (hệ thống)

Lý do:

- Sự cố phần cứng: bộ xử lý, bộ nhớ chính, mất điện ...
- Sự cố phần mềm: hệ điều hành, hệ quản trị CSDL ...

Tần số: vài lần/tháng

Ảnh hưởng: Sự cố này làm mất thông tin trên bộ nhớ chính. Vì thế dẫn đến việc đánh mất một phần của CSDL có trong vùng nhớ đệm.

Sự cố vật liệu (media failure)

Liên quan đến sự cố của các thiết bị lưu trữ thứ cấp dùng để lưu CSDL.

Lý do:

- Vỡ đầu đọc
- Hư hại bộ điều khiển

Tần số: 1-2 lần/năm

Ảnh hưởng: Sự cố này làm mất 1 phần hay toàn bộ dữ liệu.

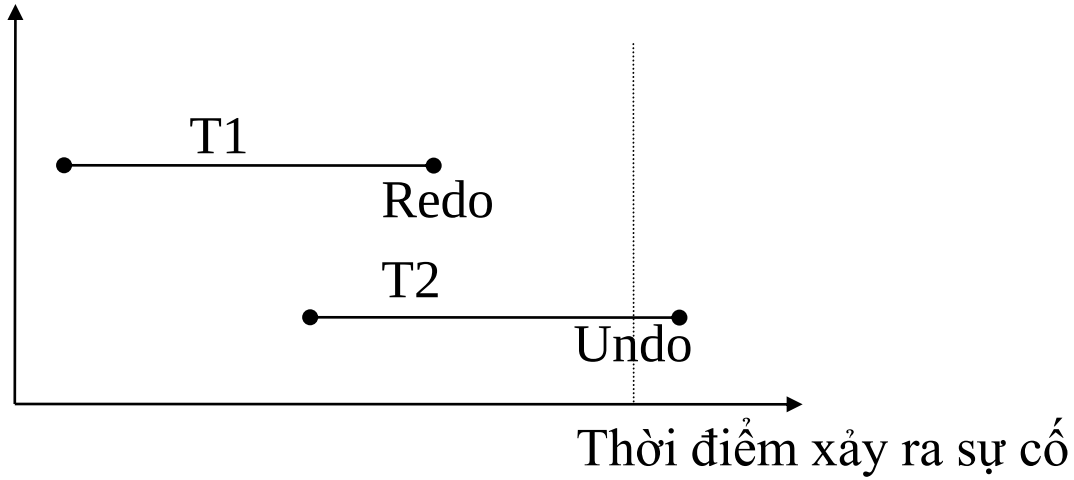
Nhật Kí Giao Dịch (Log File)

Log file chứa các thông tin được dùng cho phép xử lý phục hồi dữ liệu.

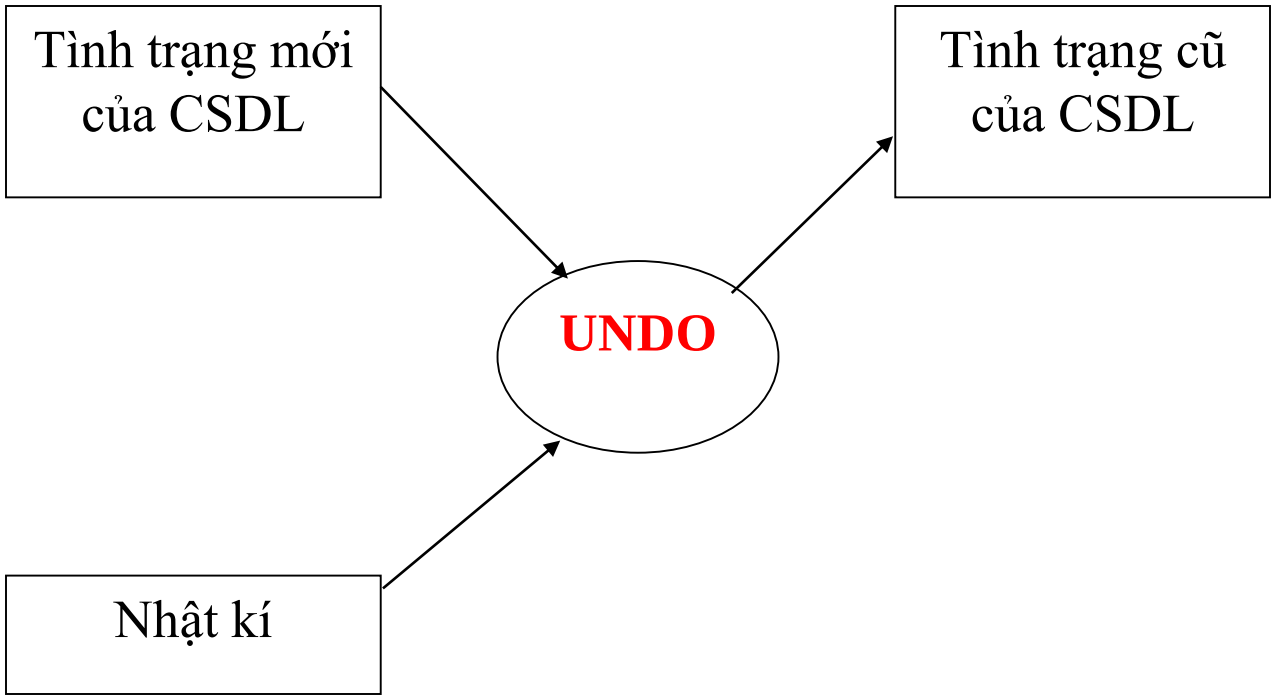
Các thông tin trong 1 mẫu tin của logfile bao gồm:

- Định danh của các giao dịch được cập nhật
- Điểm bắt đầu 1 giao dịch (Begin Transaction)
- Điểm kết thúc giao dịch và xác nhận việc cập nhật(Commit)
- Điểm kết thúc giao dịch và hủy bỏ giao dịch(Rollback hay Abort)
- Đơn vị dữ liệu được truy xuất bởi giao dịch để thực hiện thao tác
- Giá trị cũ của đơn vị dữ liệu (Before Image)
- Giá trị mới của đơn vị dữ liệu (After Image)

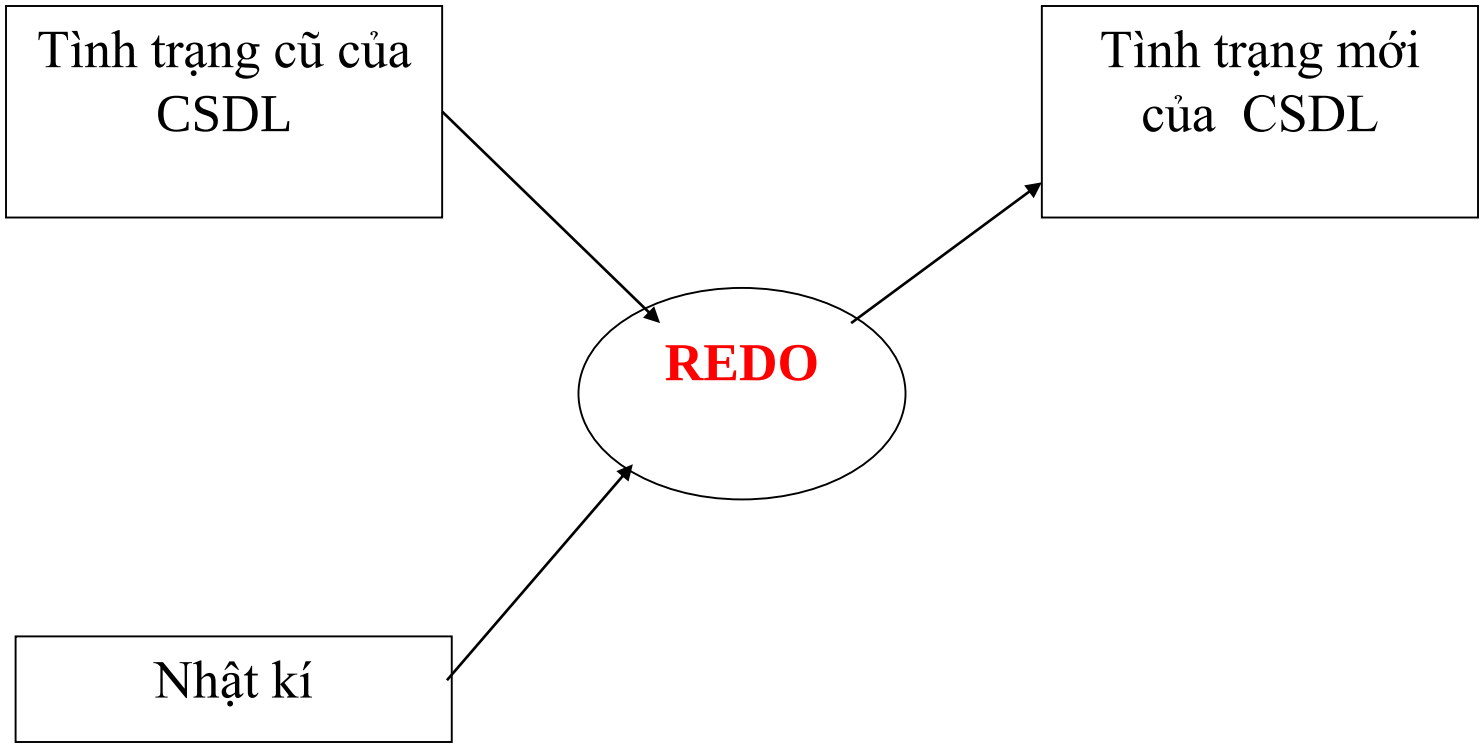
Các Nghi Thức Phục Hồi Dữ Liệu Sau Sự Cố Của Giao Dịch



Nghi thức Undo



Nghi thức Redo



Nghi thức WAL (Write Ahead Log)

Nghi thức WAL được mô tả như sau:

- Trước khi một CSDL ổn định được cập nhật (có thể do các hành động của một giao dịch chưa được uỷ thác), các thay đổi trước phải được ghi vào nhật kí ổn định. Điều này tạo dễ dàng cho hành động hồi lại Undo.

- Khi một giao dịch uỷ thác, các thay đổi sau phải được lưu vào nhật kí ổn định trước khi cập nhật lên CSDL ổn định. Điều này tạo dể dàng cho hành động Redo thực hiện

Phục Hồi Dữ Liệu Sau Sự Cố Của Hệ Thống

Điểm Checkpoint (điểm phục hồi của hệ thống)

Điểm checkpoint chỉ ra rằng CSDL từ điểm đó trở về trước CSDL đã được cập nhật và nhất quán. Trong trường hợp đó hành động thực hiện lại chỉ phải khởi đi từ điểm đó và hành động hồi lại chỉ phải trở ngược đến điểm đó.

Quá trình xây dựng điểm checkpoint thực hiện qua 3 bước:

- Ghi mẫu tin begin_checkpoint vào nhật kí.
- Thu thập các dữ liệu từ điểm kiểm tra vào bộ nhớ ổn định.
- Ghi mẫu tin end_checkpoint vào nhật kí.

Phục hồi bình thường

Sau 1 cái dừng bình thường của hệ thống, 1 checkpoint được ghi nhận vào log file như là mẫu tin cuối cùng của log file.

Khi hệ thống được khởi động lại, nếu mẫu tin cuối cùng trong log file là checkpoin thì thủ tục phục hồi bình thường được gọi.

Phục hồi sau sự cố của hệ thống

*** Phân loại giao dịch:**

Nhóm 1: Giao dịch được commit trước khi xảy ra sự cố hệ thống-> REDO

Nhóm 2: - Giao dịch bị rollback trước khi xảy ra sự cố hệ thống ->UNDO

- Giao dịch chưa commit trước khi xảy ra sự cố hệ thống

*** Giải quyết:**

Nhóm 1: Redo các thao tác sau checkpoint cuối cùng

Nhóm 2: Undo các thao tác:

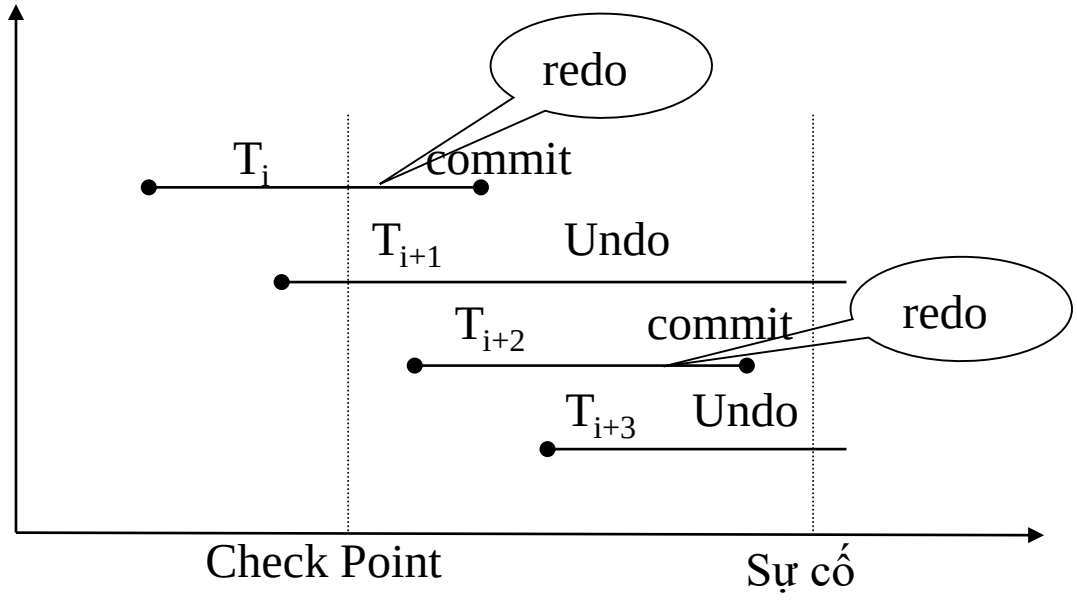
- Trước checkpoint undo trên CSDL
- Sau checkpoint undo trên buffer

Phục hồi sau sự cố của hệ thống

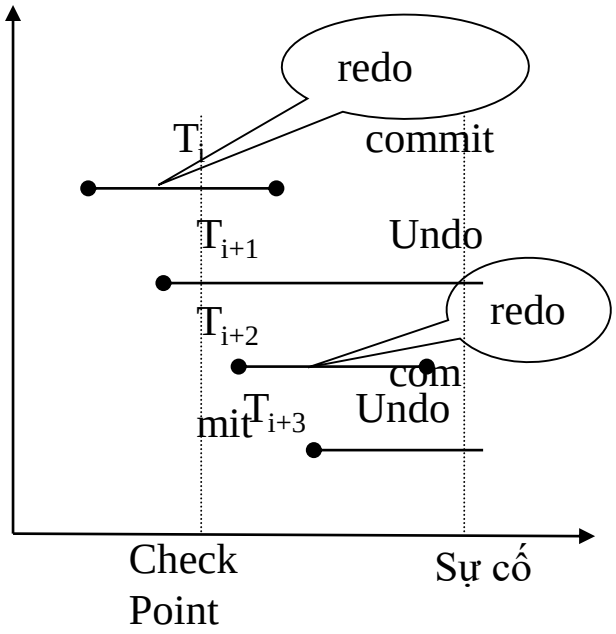
Giả sử sau khi sự cố hệ thống xảy ra, DBMS khởi động lại với tập tin nhật kí như sau:

Thời điểm	Thao tác
1	BOTi
2	$U_1(i)$
3	BOT_{i+1}
4	$U_1(i+1)$
5	Checkpoint
6	BOT_{i+2}
7	$U_1(i+2)$
8	$U_2(i)$
9	Commit i
10	$U_2(i+1)$
11	BOT_{i+3}
12	$U_1(i+3)$
13	$U_2(i+3)$
14	$U_2(i+2)$
15	Commit i+2
16	$U_3(i+1)$
	Sự cố xảy ra

Ui (j) thao tác cập nhật thứ j của giao dịch Ti. Hãy mô tả tiến trình khôi phục dựa trên tập tin nhật kí này.



Thời điểm	Thao tác	Thao tác sau sự cố
1	BOTi	
2	U_1(i)	
3	BOT_{i+1}	
4	U_1(i+1)	Undo trên CSDL
5	Checkpoint	
6	BOT_{i+2}	
7	U_1 (i+2)	Redo
8	U_2(i)	Redo
9	Commit i	
10	U_2 (i+1)	Undo trên buffer
11	BOT_{i+3}	
12	U_1(i +3)	Undo trên buffer
13	U_2(i +3)	Undo trên buffer
14	U_2(i +2)	Redo
15	Commit i+2	
16	U_3(i +1)	Undo trên buffer
	Sự cố xảy ra	



Phục Hồi Dữ Liệu Sau Sự Cố Của Thiết Bị Lưu Trữ

Để thích ứng được với sự cố của thiết bị lưu trữ không lường trước được (do thảm họa chẳng hạn), một bản lưu của CSDL và nhật kí được duy trì trên một thiết bị lưu trữ khác, điển hình là trên băng từ hoặc trên CD-ROM.

=> Thực hiện backup dữ liệu theo chu kỳ.

Tìm hiểu Backup/Restore, Import/Export trong SQL Server, Oracle?

Q & A

1. An toàn dữ liệu là gì?
2. Cơ chế phục phồi dữ liệu sau sự cố giao dịch?
3. Cơ chế phục phồi dữ liệu sau sự cố hệ thống?
4. Cơ chế phục phồi dữ liệu sau sự cố phần cứng?

- **Bài tập nhóm**
  - Các sinh viên chia nhóm. Mỗi nhóm 3 sinh viên thực hiện yêu cầu sau:
  - Sinh viên 1: ***Tìm hiểu Backup/Restore,***
  - Sinh viên 2: ***Import/Export trong SQL Server, Oracle?***
  - Sinh viên 3: ***Phục hồi dữ liệu khi có sự cố giao dịch***

- **Tóm tắt**

  Có 3 cơ chế phục hồi dữ liệu

  – Giao dịch

  – Hệ thống

  – Phần cứng