

# 第10章 数据库恢复技术

# 本章目标

- 完成本章的学习，你应该能够
  - 理解并掌握事务的概念及ACID特性
  - 理解事务故障、系统故障、介质故障及计算机病毒发生的原因及后果
  - 理解备份在数据库恢复中的作用
  - 深刻理解并掌握日志文件的内容及使用方法
  - 熟练掌握事务故障、系统故障和介质故障的数据库恢复策略及步骤
  - 熟练掌握利用日志文件进行数据库恢复的技术
  - 掌握使用检查点的数据库恢复技术
  - 理解数据库镜像在数据库恢复中的作用

# 大纲

- **事务的基本概念**
- 数据库恢复概述
- 故障的种类
- 恢复的实现技术
- 恢复策略
- 具有检查点的恢复技术
- 数据库镜像
- 本章小结

# 事务的基本概念

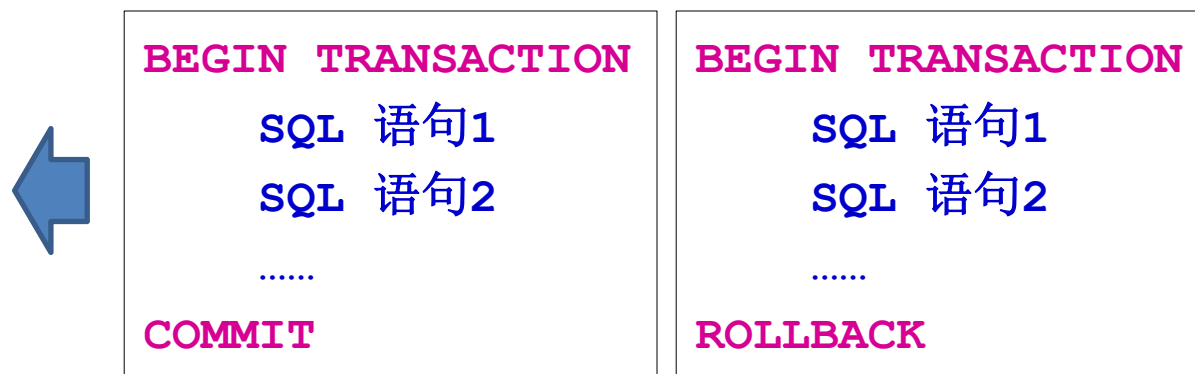
- **事务处理**也称**联机事务处理**(Online transaction processing, **OLTP**)
  - 事务处理技术主要包括**数据库恢复技术**和**并发控制技术**
  - **事务是恢复与并发控制的基本单位**
- **事务(Transaction)**
  - 事务是用户定义的一个数据库操作序列，这些操作要么全做，要么全不做，是一个**不可分割的工作单位**。
- **事务与程序**
  - 事务是数据库应用程序的基本逻辑单元
  - 在关系数据库中，一个事务可以是一条SQL语句，一组SQL语句或整个程序
  - 一个程序通常包含多个事务

## ■ 定义事务的两种方式：

### – 显式定义

- 事务的开始和结束由用户定义
- 事务定义的主要语句：**BEGIN TRANSACTION; COMMIT; ROLLBACK**

- 事务正常结束
- 提交事务的所有操作  
(读+更新)
- 事务中所有对数据库的更新写回到磁盘上的物理数据库



- 事务异常终止
- 事务运行过程中发生了故障, 不能继续下去
- 系统将事务中对数据库的所有已完成的操作全部撤销, 事务滚回到开始时的状态

### – 隐式定义

- 当用户没有显式地定义事务时, DBMS按缺省规定自动划分事务

# openGauss的事务机制

- 启动事务

- START TRANSACTION
- BEGIN

- 设置事务

- SET TRANSACTION

- 提交事务

- COMMIT
- END

- 回滚事务

- ROLLBACK

openGauss事务的具体用法参见：

<https://www.opengauss.org/zh/docs/3.1.0/docs/Developerguide/%E4%BA%8B%E5%8A%A1%E6%8E%A7%E5%88%B6.html>

墨天轮对openGauss高可靠事务的介绍：

<https://www.modb.pro/db/30010>

# Oracle的事务控制语句

## ■ Oracle的常用事务控制语句：

- Commit(work)
- Rollback
- Savepoint

(savepoint必须在commit前使用)

```
set time on

DROP TABLE test;
CREATE TABLE test(a varchar2(6));

INSERT INTO test VALUES('1');
SAVEPOINT b1;
SELECT * FROM test;
```

```
INSERT INTO test VALUES('2');
SAVEPOINT b2;
SELECT * FROM test;

INSERT INTO test VALUES('3');
SAVEPOINT b3;
SELECT * FROM test;

INSERT INTO test VALUES('4');
SAVEPOINT b4;
SELECT * FROM test;
```

```
rollback to b3;
select * from test;

rollback to b1;
select * from test;

rollback to b2;

rollback;
select * from test;
```

# 事务的ACID特性

原子性Atomicity	一致性Consistency	隔离性Isolation	持久性Durability
<ul style="list-style-type: none"><li>事务是数据库的逻辑工作单位，事务中包括的诸操作要么都做，要么都不做</li></ul>	<ul style="list-style-type: none"><li>事务执行的结果必须是使数据库从一个一致性状态变到另一个一致性状态</li><li>一致性状态：只包含成功事务提交的结果</li><li>不一致性状态：不正确的状态（因故障造成）</li><li>确保单个事务的一致性编写该事务的应用程序员的责任</li><li>完整性约束的自动检查是实现一致性的一种方法</li></ul>	<ul style="list-style-type: none"><li>一个事务的执行不能被其他事务干扰</li><li>即一个事务的内部操作及使用的数据对其他并发事务是隔离的，并发执行的各个事务之间不能互相干扰</li></ul>	<ul style="list-style-type: none"><li>指一个事务一旦提交，它对数据库中数据的改变就是永久性的，接下来的其他操作或故障不应该对其执行结果有任何影响</li></ul>
<ul style="list-style-type: none"><li>保证事务ACID特性是事务管理的重要任务</li><li>事务ACID特性可能遭到破坏的因素有：<ul style="list-style-type: none"><li>多个事务并行运行时，不同事务的操作交叉执行；事务中运行过程中被强行终止</li></ul></li></ul>			



# 原子性示例

## ■ 业务场景-银行转帐：从帐号A中取出一万元，存入帐号B

- 上述业务逻辑可被定义为一个事务，该事务包括两个操作：账号A的余额先减去1万元，然后账号B的余额增加1万元，图示如下：

A	B
$A=A-1$	$B=B+1$

- 这两个操作**要么全做，要么全不做**
- 全做或者全不做，数据库都处于一致性状态
- 如果只做一个操作，用户逻辑上就会发生错误，少了1万元，数据库就处于不一致性状态

# 隔离性示例

$T_1$	$T_2$
① 读A=16	读A=16
②	
③ $A \leftarrow A-1$ 写回A=15	$A \leftarrow A-3$ 写回A=13
④	

- $T_1$ 和 $T_2$ 是两个事务
- 这两个事务同时读取到A的值为16
- $T_1$ 更新A的值为15
- $T_2$ 更新A的值为13
- 因为没有隔离机制，这导致 $T_1$ 的修改被 $T_2$ 的结果所覆盖！，即 $T_1$ 的更新操作没有被体现

# 大纲

- 事务的基本概念
- **数据库恢复概述**
- 故障的种类
- 恢复的实现技术
- 恢复策略
- 具有检查点的恢复技术
- 数据库镜像
- 本章小结

# 数据库恢复概述

- 故障是不可避免的

- 硬件故障、软件错误、操作员失误、恶意破坏

- 故障影响

- 轻：运行事务非正常中断，影响数据库中数据的正确性
- 重：破坏数据库，使数据库中全部或部分数据丢失

- DBMS必须具有数据恢复的功能

- 即把数据库从错误状态恢复到某一已知正确状态(一致性状态或完整状态)的功能

- 恢复子系统是DBMS的一个重要组成部分

- 相当庞大，整个系统代码的10%以上
- 恢复技术衡量系统优劣的重要指标

# 大纲

- 事务的基本概念
- 数据库恢复概述
- **故障的种类**
- 恢复的实现技术
- 恢复策略
- 具有检查点的恢复技术
- 数据库镜像
- 本章小结

# 故障的种类

1. 事务内部故障
2. 系统故障
3. 介质故障
4. 计算机病毒

# 1.事务内部故障

- 事务故障意味着事务没有达到预期的终点(COMMIT或显式的ROLLBACK), 因此数据库可能处于不正确的状态。

- 事务故障的发现

- 有些可通过事务程序本身发现
- 更多的是非预期的, 不能由应用程序处理
  - 运算溢出
  - 并发事务发生死锁而被选中撤销该事务
  - 违反了某些完整性限制而被终止



```
BEGIN TRANSACTION
读账户甲的余额BALANCE;
BALANCE=BALANCE-AMOUNT;
IF(BALANCE < 0 ) THEN
{打印 '金额不足, 不能转账' ;
ROLLBACK;
}
ELSE
{读账户乙的余额BALANCE1;
BALANCE1=BALANCE1+AMOUNT;
写回BALANCE1;
COMMIT;
}
```

- 事务故障的恢复操作

- 事务撤销(UNDO)

## 2.系统故障

- **系统故障**是指造成系统停止运转的任何事件，使得系统要**重新启动**。也称为**软故障**(soft crash)
  - 特定类型的硬件错误（如CPU故障）
  - 操作系统故障
  - DBMS代码错误
  - 系统断电
- **系统故障特点：**
  - 所有运行的事务都非正常终止，但不破坏数据库
  - 内存中数据库缓冲区的信息全部丢失
- **系统故障的恢复操作**
  - 系统重新启动时，恢复程序让所有非正常终止的事务回滚，强行**撤消(UNDO)**所有**未完成事务**
  - 系统重新启动时，恢复程序**重做(RED0)**所有**已完成的事务**



# 3.介质故障

- 介质故障也称为硬故障(Hard crash)，指外存故障。
  - 磁盘损坏
  - 磁头碰撞
  - 瞬时强磁场干扰
- 介质故障特点：
  - 破坏数据库或部分数据库，并影响正在存取这部分数据的所有事务
  - 与事务故障和系统故障相比，发生的可能性小，但破坏性最大

# 4.计算机病毒

- 计算机病毒是一种人为的故障或破坏，是一种恶意计算机程序
- 计算机病毒特点
  - 可以繁殖和传播，造成对计算机系统包括数据库的危害
    - 有的病毒传播很快，一旦侵入系统就马上摧毁系统
    - 有的病毒有较长的潜伏期，计算机在感染后数天或数月才开始发病
    - 有的病毒感染系统所有的程序和数据
    - 有的只对某些特定的程序和数据感兴趣
- 计算机病毒已成为计算机系统的主要威胁，自然也是数据库系统的主要威胁
- 数据库一旦被破坏仍要用恢复技术把数据库加以恢复

# 故障小结

- 各类故障对数据库的影响有两种可能性:
  1. 数据库本身被破坏
  2. 数据库没有被破坏，但数据可能不正确，这是由于事务的运行被非正常终止造成的
- 恢复的基本原理
  - **冗余**
    - 即，可以利用存储在系统别处的**冗余数据**来**重建**数据库中已被破坏或不正确的那部分数据
- 恢复的基本原理简单，但**实现技术的细节**却相当**复杂**
  - 一个大型数据库产品，恢复子系统的代码要占全部代码的10%以上

# 大纲

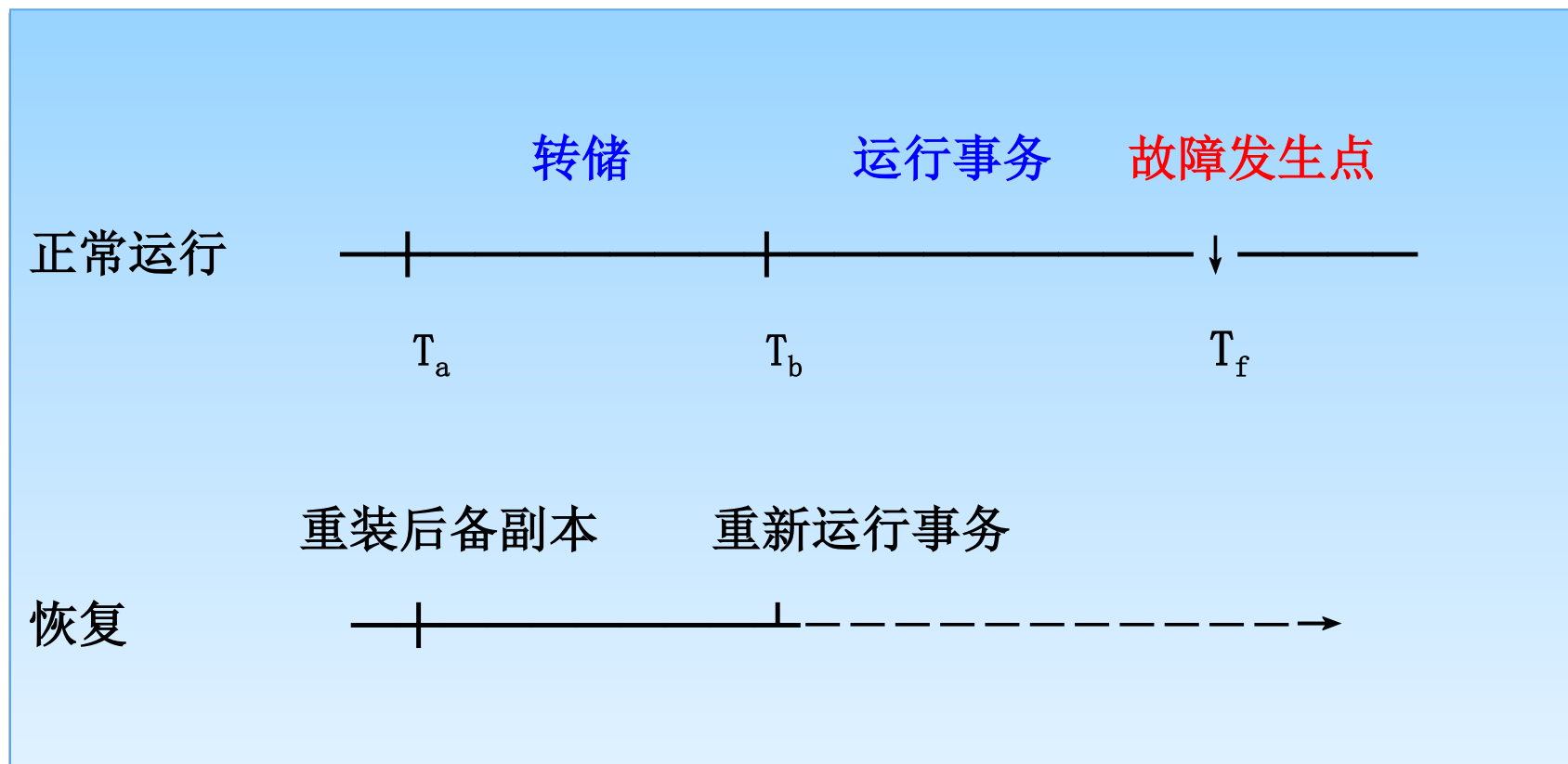
- 事务的基本概念
- 数据库恢复概述
- 故障的种类
- **恢复的实现技术**
- 恢复策略
- 具有检查点的恢复技术
- 数据库镜像
- 本章小结

# 恢复的实现技术

- 恢复机制涉及的关键问题
  - 如何建立冗余数据
  - 如何利用这些冗余数据实施数据库恢复
- 建立冗余数据最常用的技术
  - 数据转储
  - 登记日志文件(logging)
- 通常在一个数据库系统中，这两种方法一起使用。

# 1.数据转储

- **数据转储**是指数据库管理员定期地将整个数据库复制到磁带、磁盘或其他存储介质上保存起来的过程。
  - 备用的数据称为后备副本或后援副本(backup)
  - 数据库恢复采用的基本技术
- **利用后备副本进行数据库的恢复**
  - 当数据库遭到破坏后可以将后备副本重新装入,
  - 但重装后备副本只能将数据库恢复到转储时的状态,
  - 要想恢复到故障发生时的状态, 必须重新运行自转储以后的所有更新事务。



## 转储和恢复

- 转储是十分耗费时间和资源的，不能频繁进行。DBA应根据数据库使用情况确定一个适当的转储周期。
- 转储可分为静态转储和动态转储

静态转储	动态转储
<ul style="list-style-type: none"> <li>• 是在系统中无运行事务时进行的转储操作，即转储操作开始的时刻数据库处于一致性状态，在转储期间不允许(或不存在)对数据库的任何存取、修改。</li> <li>• 静态转储得到的一定是一个数据一致性的副本</li> </ul>	<ul style="list-style-type: none"> <li>• 是指转储期间允许对数据库进行存取或修改，即转储和用户事务可以并发执行</li> </ul>
<b>优点：</b> <ul style="list-style-type: none"> <li>• 实现简单</li> </ul>	<b>优点：</b> <ul style="list-style-type: none"> <li>• 克服了静态转储的缺点，不用等待正在运行的用户事务结束，也不会影响新事务的运行</li> </ul>
<b>缺点：</b> <ul style="list-style-type: none"> <li>• 降低了数据库的可用性</li> <li>• 转储必须等待正运行的用户事务结束</li> <li>• 新的事务必须等转储结束</li> </ul>	<b>缺点：</b> <ul style="list-style-type: none"> <li>• 不能保证转储结束后后援副本的数据正确有效</li> </ul>



## ■ 动态转储缺点示例

- 在转储期间的某时刻 $T_c$ ，系统把数据 $A=100$ 转储到磁带上，而在下一时刻 $T_d$ ，某一事务将 $A$ 改为200，后备副本上的 $A$ 过时了

## ■ 动态转储缺点的解决方案

- 把动态转储期间各事务对数据库的修改活动登记下来，建立日志文件(log file)。
- 后援副本加上日志文件就能把数据库恢复到某一时刻的正确状态。

- 转储也可分为海量转储和增量转储。

- 海量转储是指每次转储全部数据库

- 增量转储是指每次只转储上一次转储后更新过的数据

- 海量转储与增量转储比较

- 从恢复角度看，使用海量转储得到的后备副本进行恢复往往更方便

- 如果数据库很大，事务处理又十分频繁，则增量转储方式更实用更有效

### 数据转储分类

转储方式	转储状态	
	动态转储	静态转储
海量转储	动态海量转储	静态海量转储
增量转储	动态增量转储	静态增量转储

# openGauss的备份与恢复

- openGauss的备份与恢复可参见官网：
  - <https://www.opengauss.org/zh/docs/3.1.0/docs/Administratorguide/%E5%A4%87%E4%BB%BD%E4%B8%8E%E6%81%A2%E5%A4%8D.html>
- 墨天轮：
  - <https://www.modb.pro/doc/46420>

# oracle的逻辑备份

- Oracle的逻辑备份是用使用Oracle提供的操作系统工具Export、Import将数据库中的数据导出、导入。
  - Export、Import都是在操作系统而不是SQL\*PLUS环境下使用
  - 在每一个Oracle数据库中，可以使用Export命令将数据库中的数据备份成一个二进制的操作系统文件，文件格式为DMP(Export Dump File)，称为输出转储文件。
  - 导出的文件可以使用另一个操作系统命令Import重新导入到另一个数据库中。
- 物理备份是操作系统文件的备份，即，即使某个数据文件、没有数据也必须备份。逻辑备份是数据的备份，不拷贝物理文件，可以只将数据文件中的某一个表导出，节省空间。逻辑备份中导出数据时没有操作系统信息，所以可以在不同的平台之间传输。

C:\Windows\system32\cmd.exe

Microsoft Windows [版本 6.1.7601]

版权所有 (c) 2009 Microsoft Corporation。保留所有权利。

C:\Users\apple>exp hr/hr@XE file=d:\hr\_2019\_04\_05.dmp tables=(locations, jobs)

Export: Release 11.2.0.2.0 - Production on 星期五 4月 5 11:37:25 2019

Copyright (c) 1982, 2009, Oracle and/or its affiliates. All rights reserved.

连接到: Oracle Database 11g Express Edition Release 11.2.0.2.0 - 64bit Production

已导出 ZHS16GBK 字符集和 AL16UTF16 NCHAR 字符集

服务器使用 AL32UTF8 字符集 (可能的字符集转换)

即将导出指定的表通过常规路径...

.. 正在导出表

LOCATIONS导出了

23 行

EXP-00091: 正在导出有问题的统计信息。

EXP-00091: 正在导出有问题的统计信息。

EXP-00091: 正在导出有问题的统计信息。

EXP-00091: 正在导出有问题的统计信息。

EXP-00091: 正在导出有问题的统计信息。

.. 正在导出表

JOB\$导出了

19 行


EXP-00091: 正在导出有问题的统计信息。

EXP-00091: 正在导出有问题的统计信息。

导出成功终止, 但出现警告。

参考资料: <https://blog.csdn.net/jiushancunmonkeyking/article/details/78851461>

## 2.登记日志文件

- **日志文件**是用来记录事务对数据库的**更新操作**的文件。
- **日志文件的格式和内容：**
  - 以记录为单位的日志文件，需要登记的内容包括：
    - 各个事务的开始标记(BEGIN TRANSACTION)
    - 各个事务的结束标记(COMMIT或ROLLBACK)
    - 各个事务的所有更新操作 作为一个日志记录(log record)
  - 每个日志记录的内容主要包括：
    - 事务标识（标明是哪个事务）
    - 操作的类型（插入、删除或修改）
    - 操作对象（记录内部标识）
    - 更新前数据的旧值（对插入操作而言，此项为空值）
    - 更新后数据的新值（对删除操作而言，此项为空值）

## ■ 日志文件的格式和内容

- 以数据块为单位的日志文件，日志记录的内容包括：
  - 事务标识
  - 更新的数据块
  - 由于将更新前的整个块和更新后的整个块都放入日志文件中，操作类型和操作对象等信息就无需放入日志记录中

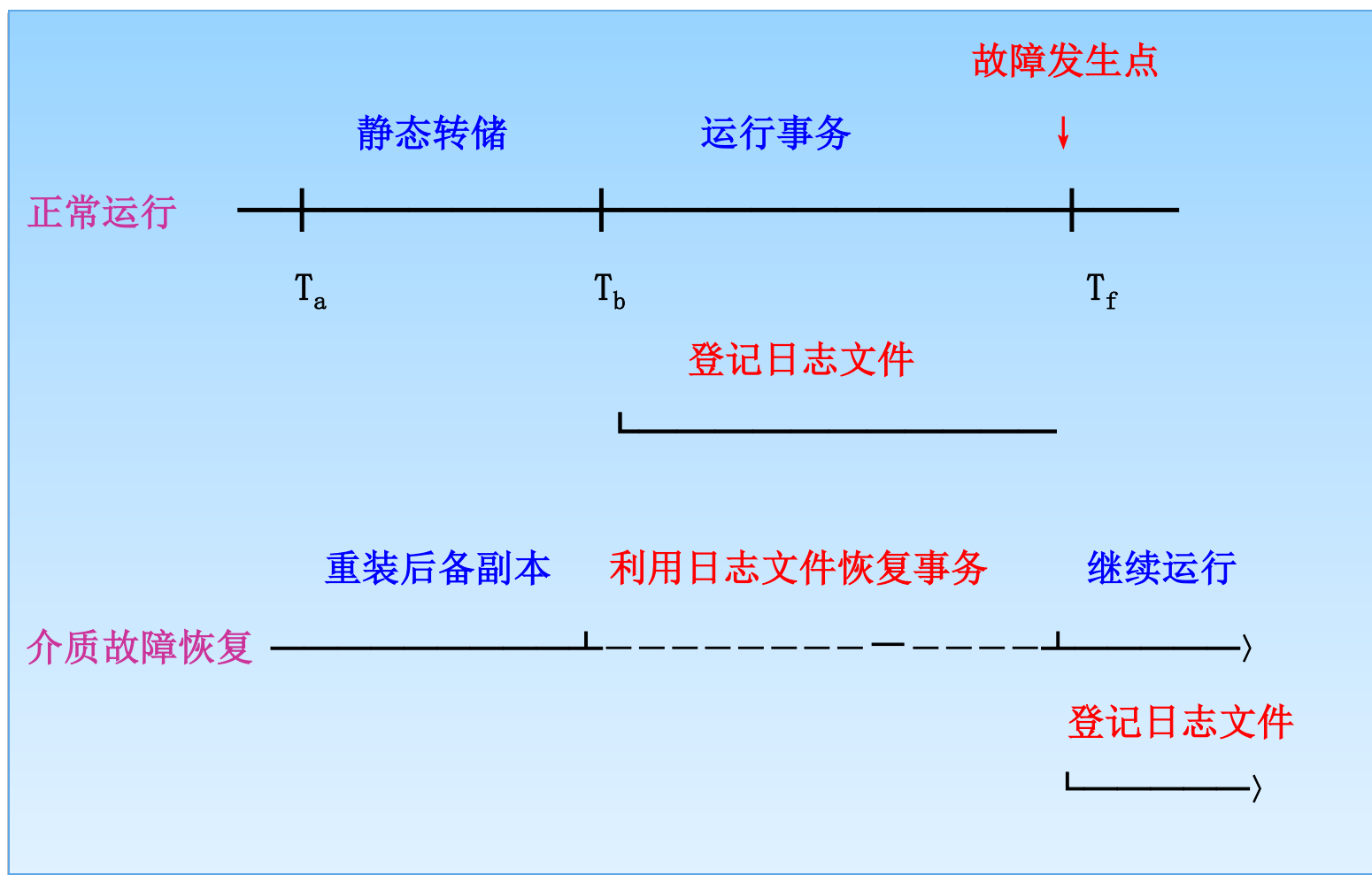
## ■ 日志文件的作用

- 用来进行事务故障恢复和系统故障恢复
- 协助后备副本进行介质故障恢复

## ■ 日志文件的具体作用

1. 事务故障恢复和系统故障恢复必须用日志文件。
2. 在动态转储方式中必须建立日志文件，后备副本和日志文件结合起来才能有效地恢复数据库。
3. 在静态转储方式中，也可以建立日志文件。
  - 当数据库毁坏后可重新装入后备副本把数据库恢复到转储结束时刻的正确状态
  - 利用日志文件，把已完成的事务进行重做处理
  - 对故障发生时尚未完成的事务进行撤销处理
  - 不必重新运行那些已完成的事务程序就可把数据库恢复到故障前某一时刻的正确状态





利用日志文件恢复

- 为保证数据库是可恢复的，登记日志文件必须遵循两条原则：

1. 登记的次序严格按并发事务执行的时间次序
2. 必须先写日志文件，后写数据库
  - 写日志文件操作：把表示这个修改的日志记录写到日志文件中
  - 写数据库操作：把对数据的修改写到数据库中

- 为什么要先写日志文件再写数据库？

- 把对数据的修改写到数据库中和把表示这个修改的日志记录写到日志文件中是两个不同的操作。有可能在这两个操作之间发生故障，即这两个写操作只完成了一个。如果先写了数据库修改，而在运行记录中没有登记这个修改，则以后就无法恢复这个修改。如果先写日志，但没有修改数据库，按日志文件恢复时只不过多执行一次不必要的UNDO操作，并不会影响数据库的正确性。

# 大纲

- 事务的基本概念
- 数据库恢复概述
- 故障的种类
- 恢复的实现技术
- **恢复策略**
- 具有检查点的恢复技术
- 数据库镜像
- 本章小结

# 恢复策略

- 当对数据库进行恢复时，不同故障（事务故障、系统故障和介质故障）的恢复策略和方法也都不一样。
- 事务故障的恢复
  - 事务故障是指事务中运行至正常终点前被终止。
  - 恢复策略
    - 由恢复子系统利用日志文件撤消（UNDO）此事务已对数据库进行的修改
  - 事务故障的恢复由系统自动完成，对用户透明。

## ■ 事务故障的恢复步骤：

1. 反向扫描日志文件（即从最后向前扫描日志文件），查找该事务的更新操作
2. 对该事务的更新操作执行逆操作，即将日志文件中“更新前的值”写入数据库
  - 插入操作，“更新前的值”为空，则相当于做删除操作
  - 删除操作，“更新后的值”为空，则相当于做插入操作
  - 修改操作，则相当于用修改前值代替修改后值
3. 继续反向扫描日志文件，查找该事务的其他更新操作，并做同样处理
4. 如此处理下去，直到读到此事务的开始标记，事务故障恢复就完成了

## ■ 系统故障的恢复：

- 系统故障造成数据库不一致状态的原因
  - 未完成事务对数据库的更新可能已写入数据库
  - 已提交事务对数据库的更新可能还留在缓冲区没来得及写入数据库
- 恢复策略
  - 撤消（UNDO）故障发生时未完成的事务；
  - 重做（REDO）已完成的事务
- 系统故障的恢复由系统在重新启动时自动完成，对用户透明

## ■ 系统故障的恢复步骤:

1. 正向扫描日志文件(即从头向后扫描日志文件), 找出故障发生前已提交的事务(特征: 既有BEGIN TRANSACTION记录, 也有COMMIT记录), 将其事务标识记入重做队列(REDO-LIST)。同时找出故障发生时尚未完成的事务(特征: 只有BEGIN TRANSACTION记录, 无相应的COMMIT记录), 将其事务标识记入撤销队列(UNDO-LIST)
2. 对撤销队列中的各个事务进行撤销(UNDO)处理
  - 反向扫描日志文件, 对每个撤销事务的更新操作执行逆操作, 即将日志文件中“更新后的值”写入数据库
3. 对重做队列中的各个事务进行重做处理
  - 正向扫描日志文件, 对每个重做事务重新执行日志文件登记的操作, 即将日志文件中“更新后的值”写入数据库

## ■ 介质故障的恢复：

- 发生介质故障后，磁盘上的物理数据和日志文件被破坏，这是最严重的一种故障。

- 恢复策略

  - 重装数据库，然后重做已完成的事务。

- 介质故障的恢复需要DBA介入

  - DBA只需要重装最近转储的数据库副本和有关的各日志文件副本，然后执行系统提供恢复命令即可，具体的恢复操作仍由DBMS完成。



## ■ 介质故障的恢复步骤：

1. 装入最新的数据库后备副本(离故障发生时刻最近的转储副本)，使数据库恢复到最近一次转储时的一致性状态。

- 对静态转储的数据库副本，装入后数据库即处于一致性状态。
- 对于动态转储的数据库副本，还须同时装入转储时刻的日志文件副本，利用恢复系统故障的方法（即REDO+UNDO），才能将数据库恢复到一致性状态。

2. 装入相应的日志文件副本（转储结束时刻的日志文件副本），重做已完成的事务。

- 即首先扫描日志文件，找出故障发生时已提交的事务的标识，将其记入重做队列；然后正向扫描日志文件，对重做队列中的所有事务进行重做处理，即将日志记录中“更新后的值”写入数据库。

# 大纲

- 事务的基本概念
- 数据库恢复概述
- 故障的种类
- 恢复的实现技术
- 恢复策略
- **具有检查点的恢复技术**
- 数据库镜像
- 本章小结

# 具有检查点的恢复技术

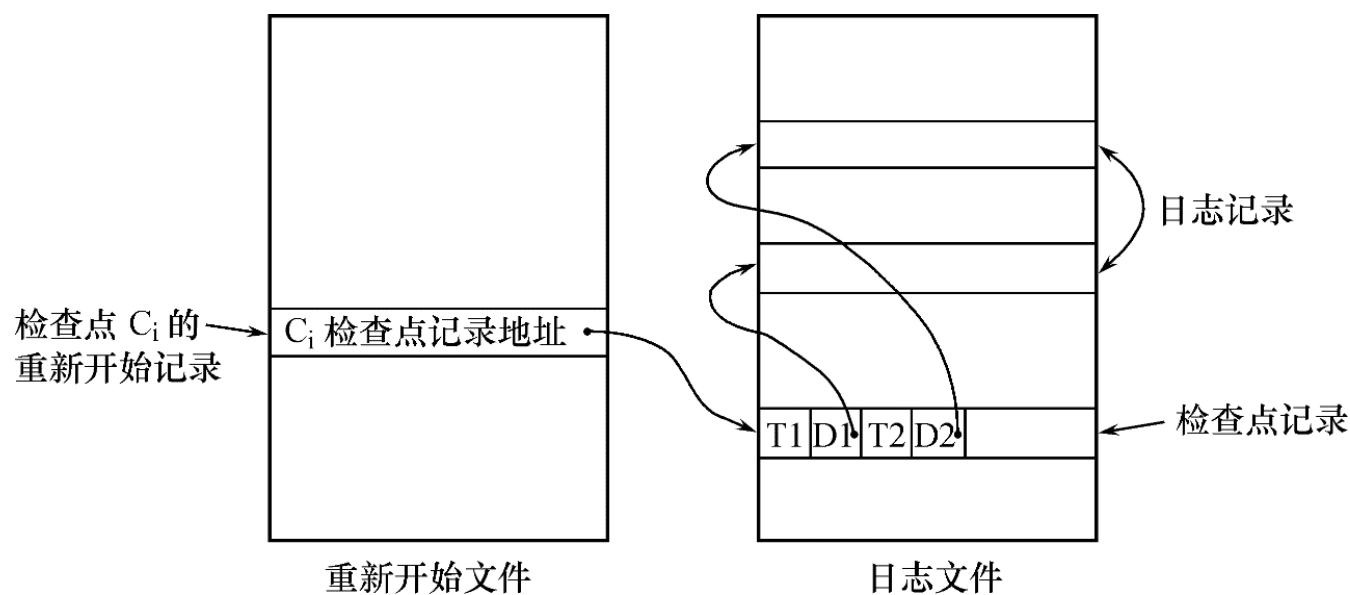
- 利用日志技术进行数据库恢复时，恢复子系统必须搜索日志，确定哪些事务需要重做，哪些事务需要撤销。
- 搜索过程中存在两个问题：
  1. 搜索整个日志将耗费大量的时间；
  2. 重做处理：重新执行，浪费了大量时间
- 解决方案：具有检查点的恢复技术
  - 在日志记录中增加检查点(checkpoint)记录
  - 增加重新开始文件
  - 恢复子系统在登录日志文件期间动态地维护日志

## ■ 检查点记录的内容

- 建立检查点时刻所有正在执行的事务清单
- 这些事务最近一个日志记录的地址

## ■ 重新开始文件

- 重新开始文件用来记录各个检查点记录在日志文件中的地址



## ■ 动态维护日志文件的方法

– 周期性地执行如下操作：建立检查点、保存数据库状态

– 具体步骤如下：

1. 将当前日志缓冲区中的所有日志记录写入磁盘的日志文件上
2. 在日志文件中写入一个检查点记录
3. 将当前数据缓冲区的所有数据记录写入磁盘的数据库中
4. 把检查点记录在日志文件中的地址写入一个重新开始文件

## ■ 恢复子系统建立检查点的一般方法

- 定期：按预定的一个时间间隔建立。如每隔一小时建立一个检查点
- 不定期：按照某种规则建立。如日志文件已写满一半建立一个检查点

## ■ 利用检查点的恢复策略：

### – 使用检查点方法可以改善恢复效率

- 当事务T在一个检查点之前提交，T对数据库所做的修改一定都已写入数据库，写入时间是在这个检查点建立之前或在这个检查点建立之时，
- 这样，在进行恢复处理时，没有必要对事务T执行重做操作

# openGauss的检查点

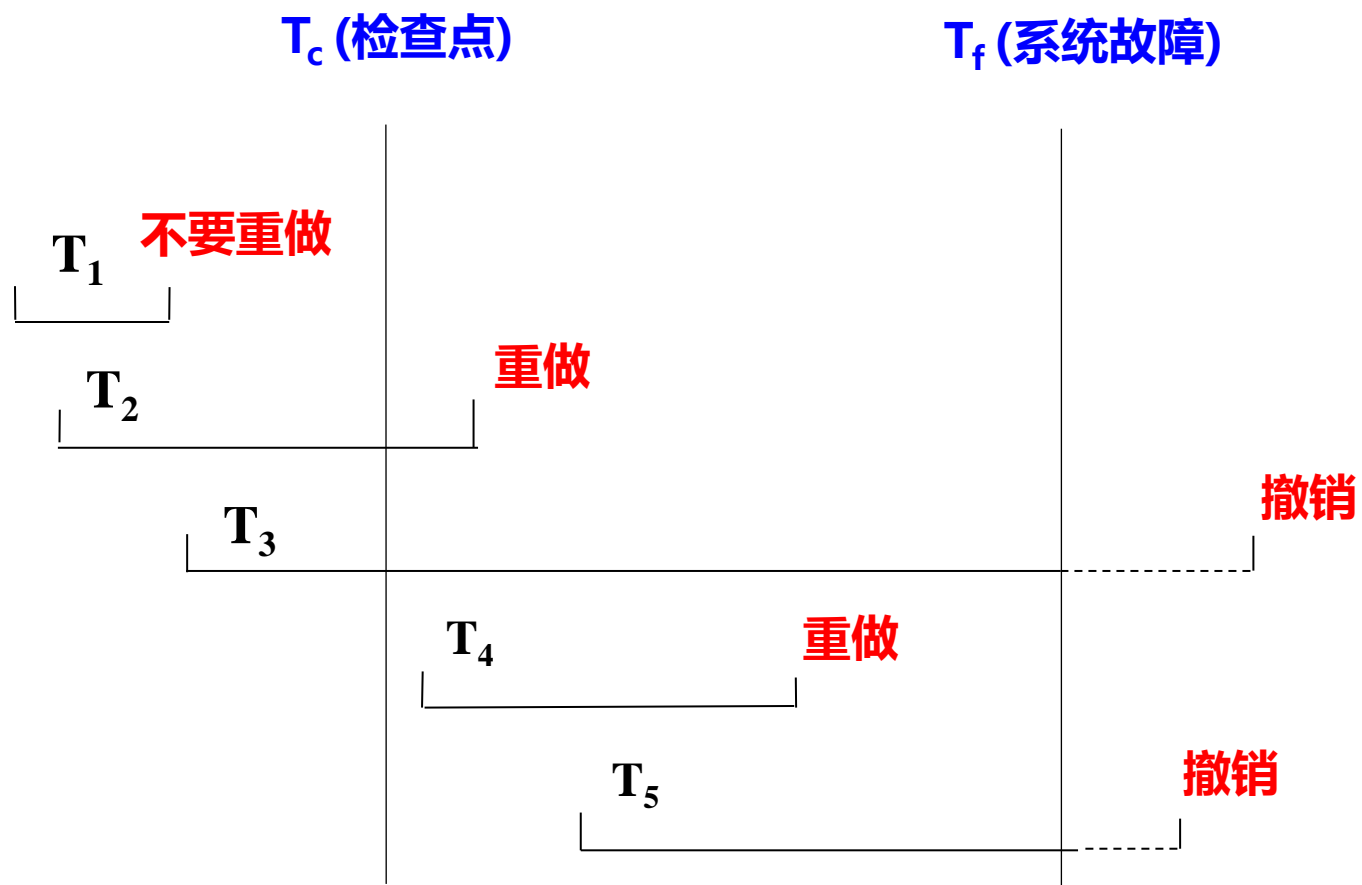
- 官网：

<https://www.opengauss.org/zh/docs/3.1.0/docs/Developerguide/%E6%A3%80%E6%9F%A5%E7%82%B9.html>

- 墨天轮：

<https://www.modb.pro/db/30794>

<https://www.modb.pro/db/214502>



恢复子系统采取的不同策略



## ■ 恢复子系统使用检查点方法进行恢复的步骤：

1. 从重新开始文件中找到最后一个检查点记录在日志文件中的地址，由该地址在日志文件中找到最后一个检查点记录
2. 由该检查点记录得到检查点建立时刻所有正在执行的事务清单ACTIVE-LIST
  - UNDO-LIST：需要执行UNDO操作的事务集合
  - REDO-LIST：需要执行REDO操作的事务集合
3. 从检查点开始正向扫描日志文件：
  - ① 如有新开始的事务 $T_i$ ，把 $T_i$ 暂时放入UNDO-LIST队列；
  - ② 如有提交的事务 $T_j$ ，把 $T_j$ 从UNDO-LIST队列移到REDO-LIST队列；
  - ③ 继续以上过程，直到日志文件结束。
4. 对UNDO-LIST中的每个事务执行UNDO操作，对REDO-LIST中的每个事务执行REDO操作。

# 示例

## ■ 考虑如下的日志记录:

如果系统故障发生在13之后, 系统该如何恢复?

- T1:不操作
- T2: 撤销
- T3: 撤销
- T4:重做

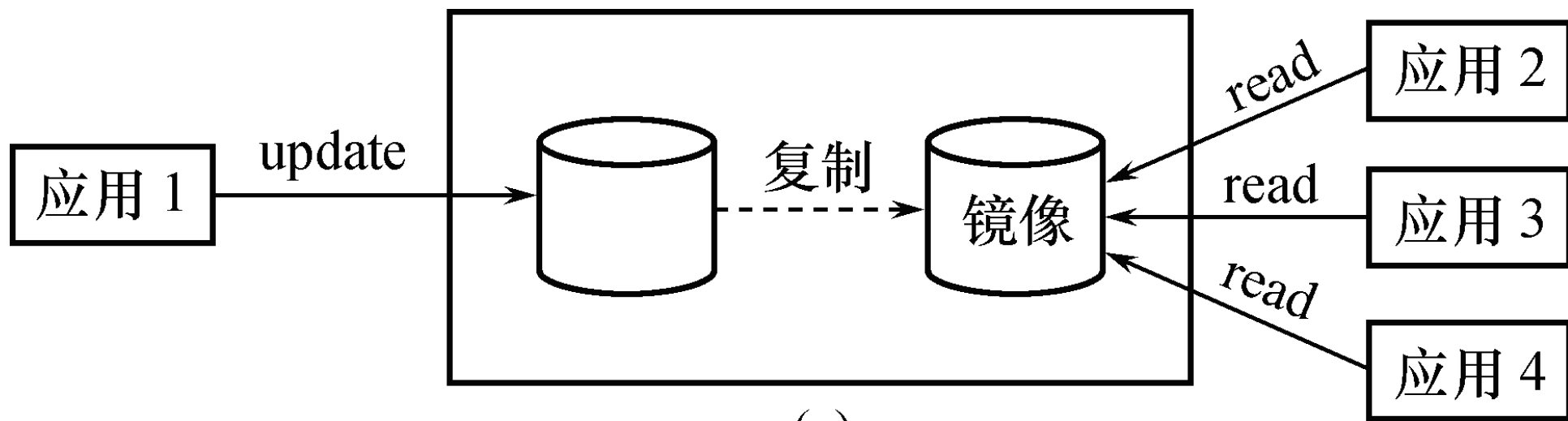
序号	日志
1	T1:开始
2	T1:写D
3	T1:提交
4	检查点
5	T4:开始
6	T4:写B
7	T4:写A
8	T4:提交
9	T2:开始
10	T2:写B
11	T3:开始
12	T3:写A
13	T2:写D

# 大纲

- 事务的基本概念
- 数据库恢复概述
- 故障的种类
- 恢复的实现技术
- 恢复策略
- 具有检查点的恢复技术
- **数据库镜像**
- 本章小结

# 数据库镜像

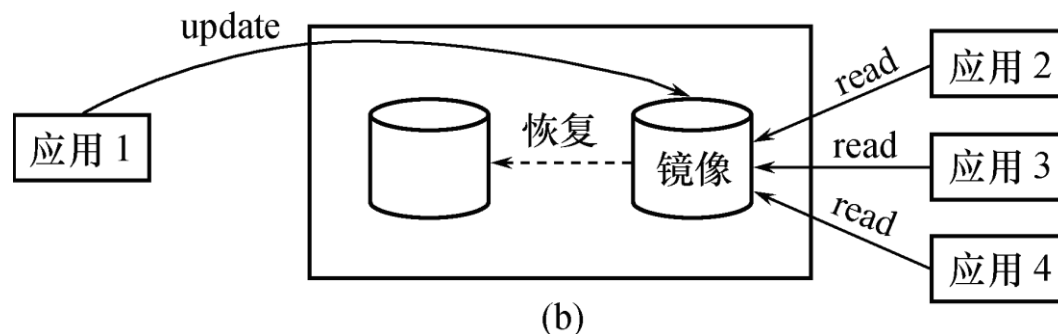
- 介质故障是对系统影响最为严重的一种故障，严重影响数据库的可用性。
  - 用户应用全部中断，恢复比较费时
  - DBA必须周期性地转储数据库，加重了DBA的负担
- 数据库镜像(Mirror)是解决介质故障、提高数据库可用性的一种常用方法。
  - 即根据DBA的要求，自动把整个数据库或其中的关键数据复制到另一个磁盘上。每当主数据库更新时，DBMS自动把更新后的数据复制过去，由DBMS自动保证镜像数据与主数据库的一致性。



(a)

## ■ 镜像数据库的使用：

- 当出现介质故障时，可由镜像磁盘继续提供使用，同时DBMS自动利用镜像磁盘数据进行数据库的恢复，不需要关闭系统和重装数据库副本。



- 当没有故障时，数据库镜像还可以用于并发操作，即当一个用户对数据加排他锁修改数据时，其他用户可以读镜像数据库上的数据，而不必等待该用户释放锁。
- 由于数据库镜像是通过复制数据实现，频繁地复制数据自然会降低系统运行效率，因此在实际应用中只对关键数据和日志文件进行镜像，而不是整个数据库。

# openGauss主备

- 官网

<https://www.opengauss.org/zh/docs/3.1.0/docs/CharacteristicDescription/%E4%B8%BB%E5%A4%87%E6%9C%BA.html>

- 墨天轮

<https://www.modb.pro/db/30014>

<https://www.modb.pro/db/31066>

# 课堂练习

## 问答题：

1. 在系统故障的恢复策略中，为什么UNDO处理反向扫描日志文件， REDO处理正向扫描日志文件。
2. 说明恢复系统是否可以保证事务的原子性和持久性。



## ■ 综合题

- 考虑如图所示的日志记录，如果系统故障发生在12之后，说明系统如何进行恢复。

序号	日志
1	T1:开始
2	T1:写D
3	T1:提交
4	检查点
5	T2:开始
6	T2:写B
7	T4:开始
8	T4:写D
9	T3:开始
10	T3:写C
11	T4:提交
12	T2:写D

# 本章小结

## ■ 事务的概念和性质

- 事务是数据库的逻辑工作单位。
- 数据库管理系统保证系统中一切事务的ACID特性，就保证了事务处于一致状态。
- 事务既是数据库恢复的基本单位，也是并发控制的基本单位。

## ■ 故障的种类

- 事务故障、系统故障、介质故障

## ■ 系统恢复最经常使用的技术

- 数据库转储、日志文件

## ■ 系统恢复的基本原理

- 利用存储在后备副本、日志文件和数据库镜像中的冗余数据来重建数据库。

# 本章作业

- 教材第十章全部习题：1-10题.