OCP 认证培训教材

备份恢复基本概念

腾科 ORACLE 教学部

备份和恢复的概念

数据库管理员(DBA) 的目标是确保数据库处于打开状态，以供用户在需要时使用。要实现这个目标，应尽量避免数据库出现故障，预计导致故障的常见原因并努力避免，努力延长平均故障间隔时间(MTBF，即数据库出现失败的频繁度，应尽可能增大该值)，确保硬件尽量可靠，也就是通过冗余方式保护关键组件，定期执行操作系统维护。Oracle 数据库提供了高级配置选项，可用于延长 MTBF，其中包括：

RAC 集群技术：位于多台计算机上的多个实例打开一个物理数据库，降低因一个或多实例失败导致的风险。

Streams 利用高级队列技术，通过解析归档日志，将归档日志解析成 DDL 及 DML 语句，从而实现数据库之间的同步。

DG 一个主数据库，多个备用数据库，备用数据库是主数据库在事务上一致的副本，可是在主数据宕机的情况下由备用服务器来继续提供服务。

提前确定恢复过程方案并配置备份，从而缩短平均恢复时间(MTTR，数据失败后出现的停机时间，应尽可能减小该值)，通过配置最佳数据库方案，达到最大程度地保护数据不会丢失，如归档日志文件、闪回和 Oracle Data Guard。

一、故障类别，通常可分为以下几类：

1、语句故障：单个数据库操作（选择、插入、更新或删除）失败

问题		解决方法
在表中输入无效的数据	>>>>>>>>>>	与用户合作来验证并更正数据
执行操作，但权限不足	>>>>>>>>>>	提供适当的对象或系统权限
分配空间失败	>>>>>>>>>>	启用可恢复的空间分配，增加所有者限额，增加表空间的空间。
应用程序存在逻辑错误	>>>>>>>>>>	与开发人员合作来更正程序错误

2、用户进程故障

用户执行了异常断开连接操作；用户会话已异常终止；用户遇到了程序错误并终止了会话，通常不需要DBA执行任何操作就可解决用户进程故障。实例后台进程会回退未提交的更改并解除锁定。

异常断开的用户进程可能包含正在进行的、需要回退的未提交任务。为了确保服务器进程会话仍保持连接，进程监视程序(PMON) 后台进程会定期轮询服务器进程。如果PMON 发现某个服务器进程的用户不再处于连接状态，PMON 会从任何实时事务处理中进行恢复；还会回退未提交的更改并解除失败会话持有的任何锁定。用户进程故障恢复不需要DBA 干预。

3、网络故障

问题		解决方法
监听程序失败	>>>>>>>>>>	配置备份监听程序和连接时故障转移
网络接口卡 (NIC) 故障	>>>>>>>>>>	配置多个网卡
网络连接失败	>>>>>>>>>>	配置备份网络连接

网络故障的最佳解决方法是为网络连接提供冗余路径。通过备份监听程序、网络连接和网络接口卡降低网络故障影响系统的可用性。

4、用户错误

用户可能会无意中删除或修改数据。如果发生这种情况，DBA需要帮助用户从错误中进行恢复。如果用户尚未提交，则进行回退操作。如果用户提交了更改，可以使用闪回查询来确定以前的值是什么（然后，为还原原始信息而更新数据），因超出了还原保留期而无法使用闪回查询的，可通过使用Oracle LogMiner 来恢复原始信息。通过将表闪回到删除前的状态，用户删除表后可从回收站中恢复表。如果清空了回收站，或者用户使用PURGE 选项删除了表，仍可通过使用时间点恢复(PITR) 来恢复删除的表。

问题		解决方法
用户无意中删除或修改了数据	>>>>>>>>>>	回退或使用闪回查询进行恢复

用户删除了表　　>>>>>>>>>>　　从回收站恢复表。

5、实例故障

如果在同步所有数据库文件之前关闭了数据库实例，就会发生实例错误。存在软硬件故障，或者使用SHUTDOWN ABORT 和STARTUP FORCE 紧急关闭命令时，也会发生实例错误。从实例故障进行恢复时，只要重新启动实例。

断电、硬件故障、一个后台进程出现故障、紧急关闭过程会发生实例故障，使用“startup”命令重新启动实例。从实例故障进行恢复是自动执行的，其中包括前滚重做日志中的更改和回退任何未提交的事务处理。查看告警日志、跟踪日志等找出出现故障的原因。

要了解实例恢复，需要了解特定后台进程的功能。实例恢复相关的后台进程

1、检查点进程(CKPT)

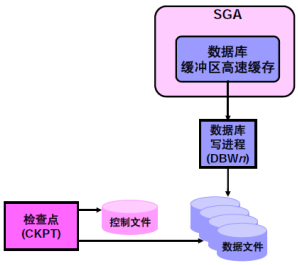
每隔三秒（或频率更高），CKPT 进程就在控制文件中存储一次数据，以记录DBWn 从SGA 写入到磁盘的已修改数据块。这就称为“检查点”。检查点的用途是标识联机重做日志文件开始进行实例恢复的位置（这个位置称为“检查点位置”）。如果使用日志切换，CKPT 进程还会将这个检查点信息写入到数据文件头。

使用检查点的原因如下：

- 确保定期将内存中的已修改数据块写入磁盘，以便在系统或数据库出现故障的情况下不会丢失数据
- 减少实例恢复所需的时间。在进行恢复时只需处理跟在最后一个检查点后面的联机重做日志文件
- 确保在关闭过程中所有已提交数据都写入到数据文件中

由CKPT 进程写入的检查点信息包括检查点位置、系统更改号、联机重做日志文件中开始恢复的位置、关于日志的信息等等。

注：CKPT 进程并不将数据块写入到磁盘，也不将重做块写入到联机重做日志文件。



检查点将当前日志文件的信息更新到数据文件头部，控制文件等

检查点的目的是同步日志文件与数据文件的不同步，从而可以确定实例恢复从最近的检查点开始

检查点的触发条件。

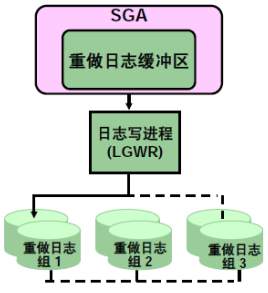
在日志切换的时候

数据库用immediate ， transaction ， normal选项shutdown数据库的时候

根据初始话文件LOG_CHECKPOINT_INTERVAL、LOG_CHECKPOINT_TIMEOUT、FAST_START_IO_TARGET的设置的数值来确定

用户手动触发

2.联机日志文件及日志写入进程（LGWR）



重做日志文件记录因执行事务处理和Oracle 服务器内部操作而对数据库

所做的更改。重做日志文件可保护数据库的完整性，避免断电、磁盘故障等因素所导致的系统故障。重做日志文件必须多路复用，以确保在出现磁盘故障事件时不会丢失其中存储的信息。

重做日志由重做日志文件组组成。重做日志文件组又由重做日志文件和其多路复用的副本组成。每个相同的副本都是该组的一个成员，每个组按编号标识。日志写进程(LGWR)进程将重做记录从重做日志缓冲区写入到重做日志组的所有成员，直至文件已填满或请求了日志切换操作。然后，会切换至下一组中的文件并执行写入。重做日志组以循环方式使用。

日志写入进程

在 commit 时触发

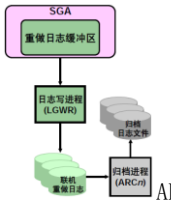
当日志缓冲/3 满时

每秒触发

在 DBWn 之前完成

最佳方案提示：多路复用的重做日志文件应尽量驻留在不同的磁盘中

3.归档进程(ARCn)



ARCn 是一个可选的后台进程。但是，在丢失磁盘后恢复数据库时，这个进程至关重要。联机重做日志组填满后，Oracle 实例便开始对下一个联机重做日志组执行写入。从一个联机重做日志组切换到另一个联机重做日志组的过程称为日志切换。ARCn 进程在每次进行日志切换时都会对已填满的日志组进行归档。它会在重新使用日志组之前自动归档联机重做日志组，因此会保留对数据库所做的所有更改。这样，即使磁盘驱动器损坏，也可以将数据库恢复到故障点。

在NOARCHIVELOG 模式下，每次发生日志切换时，都会覆盖联机重做日志文件。

在ARCHIVELOG 模式下，必须先归档非活动的已填满联机重做日志文件组，才能再次使用这些组。

6、介质故障

介质故障定义为导致一个或多个数据库文件（数据文件、控制文件或重做日志文件）丢失或损坏的任何故障。要从介质故障进行恢复，需要还原并恢复缺失的文件。

磁盘驱动器故障、磁盘控制器故障、删除或损坏了数据库文件，解决办法：

1. 从备份中还原受影响的文件。

2.通知数据库关于新文件的位置。

3.通过应用重做信息来恢复文件。

二、三大文件的规划

要最有效地保护数据，必须：

- 计划常规备份：大多数介质故障需要从备份还原丢失或损坏的文件。
- 多路复用控制文件：与数据库关联的所有控制文件是完全相同的。丢失一个控制文件后进行恢复并不难。但是丢失了所有控制文件后进行恢复则很困难。为了避免丢失所有控制文件，至少要有三个副本，建议使用RMAN定期自动备份。

控制文件是一个二进制小文件，用于说明数据库的结构。只要装载或打开了数据库，Oracle 服务器就必须能够写入这个文件。如果这个文件不存在，就不能装载数据库，因此需要恢复或重新创建控制文件。数据库必须至少在不同的磁盘上有两个控制文件（最好三个），才能将丢失某个控制文件所造成的影响减至最低。所有控制文件必须随时可用，所以丢失单个控制文件会导致实例出错。但是，这种情况下进行恢复是一项简单的工作，只需复制一个控制文件即可。丢失了所有控制文件后，要进行恢复则困难一些，但这种故障通常也不是灾难性故障。

- 多路复用重做日志组：要从实例故障或介质故障进行恢复，可使用重做日志信息将数据文件

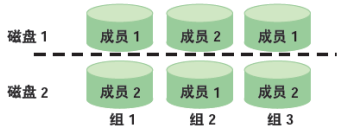
前滚到最后一个提交的事务处理。如果重做日志组依赖于一个重做日志文件，那么这个文件丢失了很可能意味着数据也丢失了。在不同的磁盘控制器中，如果可能的话，至少要确保每个重做日志组有两个副本。

重做日志组由一个或多个重做日志文件组成。组中的每个日志文件都是其它日志文件的副本。Oracle建议每个重做日志组至少包含两个文件，这两个文件要分布在不同的磁盘或控制器上，这样单个设备出现故障时就不会损坏整个日志组。丢失了整个日志组可以算是一种最严重的介质故障，因为这会导致丢失数据。但丢失了包括多个成员的日志组中的一个成员是微不足道的，这并不影响数据库运行，只会导致在预警日志中发布预警。

由于不能在事务处理信息写入到日志之前完成提交，所以重做日志会严重影响数据库的性能。必须将重做日志文件置于速度最快的磁盘中，由速度最快的控制器为其提供服务。如果可能，请不要将其它任何数据库文件与重做日志文件保存在同一磁盘上。

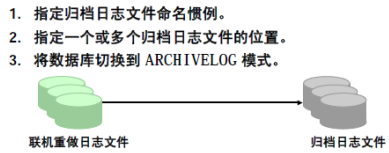
多路复用重做日志组可避免介质故障和数据丢失。建议重做日志组满足以下条件：

- 每个组至少有两个成员（文件）
- 每个成员都位于一个独立的磁盘驱动器上



- 保留重做日志的归档副本：如果某个文件丢失后通过备份已还原，实例就必须应用重做信息，以便将该文件返回到控制文件中包含的最新SCN。使用默认设置时，重做信息写入到数据文件后，数据库会覆盖这些信息。可将数据库配置为在重做日志的归档副本中保留重做信息，也就是将数据库置于ARCHIVELOG 模式下。

实例会将联机重做日志组视为一个可在其中存储事务处理信息的循环缓冲区，因而会填充一个组，然后转到下一个组。写入所有组后，实例开始覆盖第一个日志组中的信息。要配置数据库以获得最大的可恢复性，必须在允许数据库覆盖重做信息之前，指示数据库生成联机重做日志组的副本。这些副本又称为归档日志。



通过将数据库置于ARCHIVELOG 模式，可避免在归档重做日志之前覆盖这些日志。

ARCn 是可选的后台进程。但是，该进程对于在磁盘丢失后恢复数据库非常重要。联机重做日志组填满后，Oracle 实例将开始对下一个联机重做日志组进行写入。从一个联机重做日志组切换到另一个联机重做日志组的进程称为“日志切换”。ARCn 进程在每次日志切换时都会启动对已填满的日志组进行归档。该进程自动归档联机重做日志组后，该日志组才可以重用，这样对数据库所做的所有更改都可得到保留。即使磁盘驱动器损坏，也可以将数据库恢复到故障点。

配置快速恢复区

快速恢复区是为保存归档日志、备份、闪回日志、镜像控制文件和镜像重做日志而在磁盘上专门留出的空间。快速恢复区可简化备份存储管理，因此强烈建议使用该功能。快速恢复区在磁盘上的保留位置应不同于数据库文件的工作区所在的位置。否则，磁盘将成为数据库的单点故障。

分配给快速恢复区的磁盘空间量取决于数据库的大小和活动级别。通常情况下，快速恢复区越大，就越有用。理想情况下，快速恢复区应足够大，可存放数据文件和控制文件副本，以及基于保留策略从保留的备份恢复数据库所需的闪回日志、联机重做日志和归档日志。（简而言之，快速恢复区至少应为数据库大小的两倍，以便可保留一个备份和若干归档日志。）

一、物理备份与逻辑备份

1、物理备份：

是所有物理文件的一个副本，比如数据文件，控制文件，归档日志等。该副本能被存储在本地磁盘或磁带等等。物理备份是备份或恢复的基础，包括冷备份(非归档模式)或热备份(归档模式)

2、逻辑备份：

将表、存储过程等数据使用 Oracle 的 export 等工具导出到二进制文件，后续根据需要再使用 import 工具导入数据库。逻辑备份是对物理备份的方式的一种补充，多用于数据迁移。

二、备份恢复工具

1.使用 RMAN 来备份恢复，支持命令行及 GUI 接口，支持第三方磁带库备份，功能比较强大。支持备份数据库、表空间、数据文件、控制文件、归档日志等，可以使用备份恢复脚本，支持增量备份，跳过未使用的块，以及控制备份速度，在备份期间侦测损坏的数据，通过自动并发、限制 I/O 等提高备份性能。

2.用户托管的备份与恢复，是一种手动备份恢复的方式。使用操作系统命令和 SQL*plus 来完成相关的备份与恢复。

三、备份与恢复的策略

1.多路复用控制文件及多个并发备份

2.多路复用联机重做日志文件

3.在 ARCHIVELOG 模式下运行数据库，并将重做日志存档至多个位置

4.时常备份物理数据文件，尽可能创建多个副本到可靠的位置

四、备份与恢复的几类重要数据结构

1.数据文件

2.联机重做日志文件

3.控制文件

4.自动管理的撤销

5.可选的备份文件(参数文件、密码文件)

五、常见的备份类型

联机数据库备份 -->使用 archivelog 模式,SCN 不一致

脱机数据库备份 -->使用 noarchivelog 模式,SCN 保持一致

整个数据库 -->可以在不同的时间段来备份，减轻 I/O 压力，从而构建整个数据库

表空间 -->在 archivelog 模式下，当处于 noarchivelog 模式下，则该表空间必须为只读或脱机

数据文件 -->同表空间备份

控制文件 -->可以使用 SQL 语句或 RMAN 来备份

归档日志

参数文件

六、备份的分类

前面提到了逻辑备份与物理备份的概念，下面描述根据备份的内容、大小、性质等进行再分类。

1.全部备份与部分备份

1）全部备份：包含所有的数据文件及至少一个控制文件，参数文件，密码文件等。

2）部分备份：包含零个或多个表空间，零个或多个数据文件，可能包含控制文件等。部分备份仅在归档模式下才有效。

2.完整备份与增量备份

1）完整备份：一个或多个数据文件的一个完整副本，包含从备份开始处所有的数据块。

2）增量备份：包含从最近一次次备份以来被修改或添加的数据块。又可分为：

a)差异增量：是备份上级及同级备份以来所有变化的数据块，差异增量是默认增量备份方式

b)累计增量：是备份上级备份以来所有变化的块

增量备份的几种形式:

- 0 级增量备份：是所有备份的基础，是一个完整备份，包含所有的数据块
- 1 级差异增量备份：包含最近一次 1 级累计备份或差异备份以来被更改的数据块
- 1 级累计增量备份：只包含最近一次 0 级备份以来被更改的数据块

增量备份支持 archivelog 和 noarchivelog 模式，也可以在打开或关闭时进行。但只有 RMAN 才能实现增量备

3.脱机备份与联机备份

1)脱机备份：

在数据库关闭阶段发生的备份，又称为一致性备份或冷备份。在一致性关闭数据库后，控制文件 SCN 与数据文件头部 SCN 一致

2)联机备份：

在数据库使用阶段发生的备份，又称为非一致性备份或热备份。联机备份一个数据文件不与任何特定的 SCN 以及控制文件同步，可以是全部备份，也可以是部分备份，能够使用 RMAN 或操作系统命令完成，仅仅在 archivelog 模式下

4.映像副本与备份集

1)映像副本：

是某个文件的完整拷贝，未经过任何压缩处理，每个字节都与源文件相同。不支持增量备份也不能备份到磁带。

2)备份集：

由一个或多个称为 piece 的物理文件组成的逻辑结构。备份片中可以是数据文件，控制文件以及归档日志文件。

支持数据的压缩，支持增量备份。可以备份到磁盘，也可以备份到磁带。

七、还原与恢复

数据库恢复的策略，是使用最近的一次备份来实现数据库的还原，然后使用归档日志和联机日志将数据库恢复到最新或特定状态。

- 还原：

从最近的备份文件中检索所需要的内容，并将其拷回到原来位置的过程称为还原。可以基于数据库、表空间、数据文件、控制文件、参数文件进行还原

- 恢复：

在还原的基础上，使用归档日志和联机日志将数据库刷新到最新的 SCN，使数据库保持一致性。

1、恢复的类型

1）实例恢复：

在 RAC 中，当一个实例崩溃，则幸存的实例将自动使用联机日志来前滚已提交的事务，撤销未提交的事务并释放锁。

2）崩溃恢复：

指在单实例的环境中，或多实例环境中所有的实例崩溃发生。在崩溃恢复中，实例必须首先打开数据库，然后执行恢复操作。 一般而言，在崩溃或关机退出之后第一个打开数据库的实例将自动执行崩溃恢复。

3）介质恢复：

介质恢复通常为响应介质故障并根据用户的命令来执行恢复。可以使用联机或归档日志来使还原的备份为最新或将其更新至一个特定的时间点。介质恢复可以将整个数据库、一个表空间一个数据文件还原至指定的时间点

可分为完全恢复或不完全恢复

a) 完全恢复：

使用归档、联机日志与数据库、表空间或数据文件等的备份结合使用以将其更新至最新的时间点。

步骤

a.将受损的数据文件脱机

b.还原受损的数据文件

c.恢复受损的数据文件

d.将已恢复的数据文件联机

b)不完全恢复：

使用归档、联机日志与数据库、表空间或数据文件等的备份结合使用以将其更新至过去的某个时间点或 SCN 等

步骤

a.加载数据库

b.还原所有数据文件，同时可以选择还原控制文件

c.将数据库恢复至某个时间点、序列、或系统改变号

d.使用 RESETLOGS 关键字打开数据库

不完全恢复选项

- 基于时间的恢复，也称为时点恢复，将数据库恢复到一个指定的时间点
- 基于表空间时间点恢复，使用户能够将一个或多个表空间恢复至与数据库其余的部分不同的某个时间点。

- 基于取消的恢复，它恢复到执行 CANCEL 命令为止。
- 基于更改的恢复或日志序列恢复,如果使用了 O/S 命令,则基于更改的恢复将一直恢复到重做记录中一个指定的 SCN 为止

从人为错误中闪回

使用闪回特性从人为的错误中恢复

2、恢复工具

1）使用 RMAN 来进行恢复

RMAN 可以从备份机或映像副本中将数据文件还原至当前位置或新位置。当需要使用归档日志时，RMAN 将自动还原并应用归档日志， RMAN 支持完全介质恢复、不完全介质恢复， RMAN 恢复的基本命令式 restore 和 recover

2）使用 SQL*plus 来进行恢复

确定要恢复哪些文件。通常可以查询视图 V$RECOVER_FILE。从备份中还原介质故障损坏的文件.当用户没有备份时,可以使用必要的重做日志且控制文件包含损坏文件名称时仍可以执行恢复。如果无法将文件还原至其原始位置，则用户必须重新定位还原的文件并将该新位置更新到控制文件。还原必要的存档重做日志文件。