大型数据库应用技术

7-安全管理、备份与恢复

授课教师：王欢

内容提纲

- 安全管理
- 备份与恢复

安全管理

□安全控制策略概述

当前对数据库的主要安全威胁有物理威胁和逻辑威胁。

物理威胁主要是像各种外力，如恐怖袭击，火灾等造成的数据库服务器故障或数据库中存储介质的损坏造成的数据丢失；逻辑威胁主要是指对信息的未授权存取，如恶意用户侵入某银行数据库系统窃取信用卡数据信息。

- 对数据库安全物理威胁的主要解决方案主要是数据备份与恢复等技术；
- 对逻辑威胁的主要解决方案主要是用户管理、权限管理、角色管理、概要文件管理等技术。

安全管理

安全控制策略概述

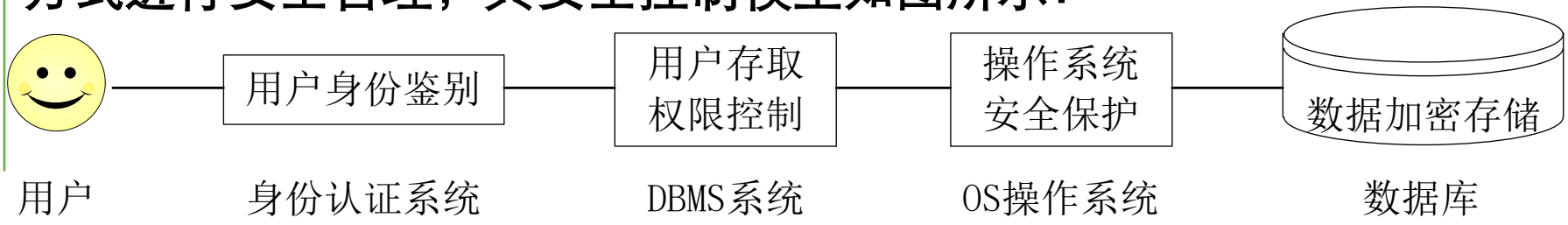
从广义上讲，数据库系统的安全框架可以划分为三个层次：

- 系统安全性。在系统级别控制数据库的存取和使用机制，包括有效的用户名与口令、是否可以连接数据库、可以进行哪些系统级操作等。
- 数据安全性。在模式对象级别控制数据库的存取和使用机制。用户要对某个模式对象进行操作，必须要有操作的权限。
- 网络安全性。Oracle 通过分发 Wallet、数字证书、SSL 安全套接字和数据密钥等办法来保证数据库的网络传输安全性。

安全管理

□安全控制策略概述

除了上述安全框架外，数据库安全主要还是依赖自身内部的安全机制。在数据库系统的安全保障体系中，一般采取分层安全控制方式进行安全管理，其安全控制模型如图所示：



- 当用户进行数据库系统访问时，系统首先根据用户输入的账号和密码进行身份鉴别，只有合法的用户才允许进入系统操作。
- 对于已进入系统的用户，DBMS系统将根据该用户的角色进行访问权限控制，即该用户只能在授权范围内对数据库对象进行操作。
- 当用户进行数据访问操作时，DBMS系统将会验证其是否具有这种操作权限。如果用户拥有该权限，才能被允许进行操作，否则拒绝用户操作。

安全管理

□安全控制策略概述

Oracle 数据库从以下几个方面进行安全管理：

- 用户账户和认证方式管理。
- 权限和角色管理：限制用户对数据库的访问和操作。
- 数据加密管理：保证网络传输的安全性。
- 表空间设置和配额：控制用户对数据库存储空间的使用。
- 用户资源限制：通过概要文件设置，可以限制用户对数据库资源的使用。
- 数据库审计：监视和记录数据库中的活动。

安全管理

□用户管理——预定义用户

管理员用户

- **SYS**：数据库中拥有最高权限的管理员，可以启动、关闭、修改数据库，拥有数据字典。
- **SYSTEM**：一个辅助的数据库管理员，不能启动和关闭数据库，但是可以进行一些管理工作，如创建和删除用户。
- **SYSMAN**：OEM 的管理员，可以对 OEM 进行配置和管理。
- **DBSNMP**：OEM 代理，用来监视数据库。
- 以上这些用户均不能删除。

安全管理

□用户管理——预定义用户

示例方案用户

在安装 Oracle 或使用 odbc 创建数据库时，如果选择了“示例方案”，会创建一些用户，在这些用户对应的 schema 中，有产生一些数据库应用案例。这些用户包括：BI、HR、OE、PM、IX、SH 等。默认情况下，这些用户均为锁定状态，口令过期。

还有 2 个特殊的用户 SCOTT 和 PUBLIC，SCOTT 是一个用于测试网络连接的用户，PUBLIC 实际是一个用户组，数据库中任何用户都属于该用户组，如果要为数据库中的全部用户授予某种权限，只需要对 PUBLIC 授权即可。

安全管理

□用户管理——创建用户

```
CREATE USER user_name  IDENTIFIED --用户认证方式
[BY password] |  --采用数据库身份认证，password为用户密码
[EXTERNALLY [AS 'certificate_DN' | ‘'kerberos_principal_name'] ] |
[GLOBALLY [AS 'directory_DN'] ]
[DEFAULT TABLESPACE tablespace_name]  --默认表空间
[TEMPORARY TABLESPACE tablespace_name |
tablespace_group_name]  --临时表空间/表空间组
[QUOTA  n K | M | UNLIMITED ON tablespace_name ]  --配额
[PROFILE profile_name]  --概要文件
[PASSWORD EXPIRE]  --用户密码期限
[ACCOUNT LOCK | UNLOCK];  --锁定/非锁定状态
```

安全管理

□用户管理——用户属性

创建用户时，必须使用安全属性进行限制，主要包括：

- 用户名：同一数据库中，用户名唯一，且不能与角色名相同。
- 用户身份认证：Oracle 采用多种方式进行身份认证，如数据库认证、操作系统认证、网络认证等。
- 默认表空间：用户创建数据库对象时，如果没有显式指明存储在哪个表空间中，系统会自动将该数据库对象存储在当前用户的默认表空间。
- 临时表空间：临时表空间分配与默认表空间相似。

安全管理

□用户管理——用户属性

创建用户时，必须使用安全属性进行限制，主要包括：

- 表空间配额：表空间配额限制用户在永久表空间中可以使用的存储空间的大小，默认新建用户在表空间都没有配额。
- 概要文件：每个用户必须具有一个概要文件，从会话级和调用级两个层次限制用户对数据库系统资源的使用，同时设置用户的口令管理策略。
- 设置用户的默认角色。
- 账户状态：创建用户时，可以设定用户的初始状态，包括口令是否过期和账户是否锁定等。

安全管理

□用户管理——用户属性

```
select * from dba_users;
```

--可以通过数据字典 dba_users 查询各个用户的属性

查询结果 ×

SQL | 提取的所有行：35，用时 0.064 秒

	USERNAME	USER_ID	PASSWORD	ACCOUNT_STATUS	LOCK_DATE	EXPIRY_DATE
1	ORACLE_OCM	36	(null)	EXPIRED & LOCKED	07-9月 -19	11-9月 -14
2	OJVMSYS	70	(null)	EXPIRED & LOCKED	11-9月 -14	11-9月 -14
3	SYSKM	2147483619	(null)	EXPIRED & LOCKED	07-9月 -19	11-9月 -14
4	XS$NULL	2147483638	(null)	EXPIRED & LOCKED	11-9月 -14	11-9月 -14
5	GSMCATUSER	61	(null)	EXPIRED & LOCKED	07-9月 -19	11-9月 -14
6	MDDATA	85	(null)	EXPIRED & LOCKED	07-9月 -19	11-9月 -14
7	SYSBACKUP	2147483617	(null)	EXPIRED & LOCKED	07-9月 -19	11-9月 -14
8	DIP	23	(null)	EXPIRED & LOCKED	07-9月 -19	11-9月 -14
9	SYSDG	2147483618	(null)	EXPIRED & LOCKED	07-9月 -19	11-9月 -14
10	APEX_PUBLIC_USER	95	(null)	EXPIRED & LOCKED	07-9月 -19	11-9月 -14
11	SPATIAL_CSW_ADMIN_USR	90	(null)	EXPIRED & LOCKED	07-9月 -19	11-9月 -14
12	SPATIAL_WFS_ADMIN_USR	87	(null)	EXPIRED & LOCKED	07-9月 -19	11-9月 -14
13	GSMUSER	22	(null)	EXPIRED & LOCKED	07-9月 -19	11-9月 -14

试一试

1、创建一个mr用户，口令为mrsoft，并设置默认的表空间为users，临时表空间为temp的用户。

2、用新用户登录数据库，会发生什么情况，如何解决？

```
SQL> create user mr identified by mrsoft

     default tablespace users

     temporary tablespace temp;
```

安全管理

□用户管理——修改用户

修改用户采用ALTER实现，语句与CREATE USER基本相同，但是多了DEFAULT ROLE选项，用于指定用户的默认角色；

ALTER USER user_name

…

[DEFAULT ROLE [role_list] | [ALL [EXCEPT role_list]] | NONE]

…

;

--role_list：指定角色列表；

--ALL：指定全部角色；

--EXCEPT role_list：除了role_list指定的角色之外的角色；

--NONE：不指定角色。

安全管理

用户管理——相关语句

当用户被锁定后，就不能登录数据库了，但是用户的所有数据库对象仍然可以继续使用，当用户解锁后，用户就可以正常连接到数据库。

ALTER USER USERNAME ACCOUNT LOCK/UNLOCK;

使用drop user删除用户，如果用户拥有数据库对象，则必须使用CASCADE选项，Oracle先删除用户的数据库对象，再删除该用户。

DROP USER user_name [CASCADE];

安全管理

用户管理——相关视图

视图名称	说明
DBA_USERS	包含数据库的所有用户的详细信息（15项）
ALL_USERS	包含数据库所有用户的用户名、用户 ID 和用户创建时间（3项）
USER_USERS	包含当前用户的详细信息（10项）
DBA_TS_QUOTAS	包含所有用户的表空间配额信息
USER_TS_QUOTAS	包含当前用户的表空间配额信息
V$SESSION	包含用户会话信息
V$SESSTAT	包含用户会话统计信息

安全管理

□概要文件

在数据库中，对用户的资源限制与用户口令管理是通过数据库概要文件（PROFILE）实现的，每个数据库用户必须具有一个概要文件，通常 DBA 将用户分为几种类型，为每种类型的用户单独创建一个概要文件。概要文件不是一个具体的文件，而是存储在 SYS 模式的几个表中的信息的集合。

概要文件通过一系列资源管理参数，从会话级和调用级两个级别对用户使用资源进行限制。

- 会话资源限制是对用户在一个会话过程中所能使用的资源进行限制；
- 调用资源限制是对一条 SQL 语句在执行过程中所能使用的资源总量进行限制。

安全管理

□概要文件——相关视图

视图名称	说明
DBA_USERS	包含数据库中所有用户属性信息，包括使用的概要文件（profile）
DBA_PROFILES	包含数据库中所有的概要文件及其资源设置、口令管理设置等信息
USER_PASSWORD_LIMITS	包含当前用户的概要文件的口令限制参数设置信息
USER_RESOURCE_LIMITS	包含当前用户的概要文件的资源限制参数设置信息
RESOURCE_COST	每个会话使用资源的统计信息

安全管理

口资源限制

- CPU使用时间：在一个会话或调用过程中使用 CPU 的总量。
- 逻辑读：在一个会话或一个调用过程中读取物理磁盘和逻辑内存数据块的总量；
- 每个用户的并发会话数；
- 用户连接数据库的最长时间

```
1  select * from user_resource_limits;
```

Data Grid

Messages | Data Grid | Trace | DBMS Output | Quer

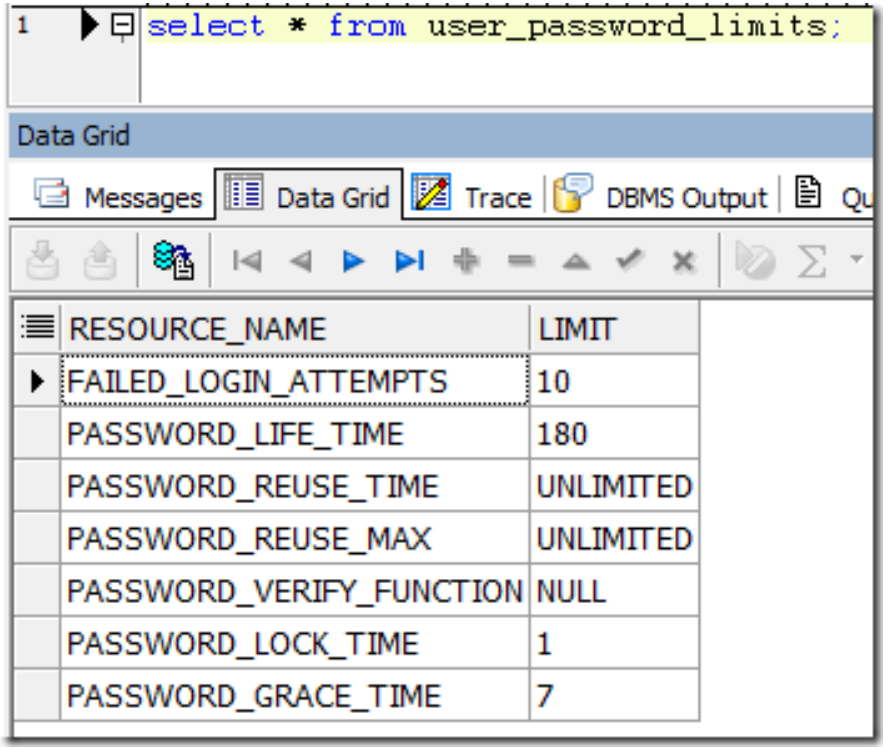
RESOURCE_NAME	LIMIT
COMPOSITE_LIMIT	UNLIMITED
SESSIONS_PER_USER	UNLIMITED
CPU_PER_SESSION	UNLIMITED
CPU_PER_CALL	UNLIMITED
LOGICAL_READS_PER_SESSION	UNLIMITED
LOGICAL_READS_PER_CALL	UNLIMITED
IDLE_TIME	UNLIMITED
CONNECT_TIME	UNLIMITED
PRIVATE_SGA	UNLIMITED

scott用户默认的资源限制信息

安全管理

口口令管理

- FAILED_LOGIN_ATTEMPTS：限制用户失败次数，一旦达到次数，账户锁定；
- PASSWORD_LOCK_TIME：用户登录失败后，账户锁定的时间长度；
- PASSWORD_LIFE_TIME：有效天数，达到设定天数后，口令过期；



RESOURCE_NAME	LIMIT
FAILED_LOGIN_ATTEMPTS	10
PASSWORD_LIFE_TIME	180
PASSWORD_REUSE_TIME	UNLIMITED
PASSWORD_REUSE_MAX	UNLIMITED
PASSWORD_VERIFY_FUNCTION	NULL
PASSWORD_LOCK_TIME	1
PASSWORD_GRACE_TIME	7

scott用户默认的
口令管理参数设置信息

安全管理

口权限管理

在 Oracle 数据库中，用户权限主要分为系统权限与对象权限两类。

- 系统权限是指在数据库基本执行某些操作的权限，或针对某一类对象进行操作的权限。
- 对象权限是指对某个特定模式对象的操作权限。数据库模式对象所有者拥有该对象的所有对象权限，对象权限的管理实际上是对象所有者对其它用户操作该对象的权限管理。有的对象并没有对象权限，只能通过系统权限进行管理，如簇、索引、触发器、数据库链接等。

安全管理

□权限管理——系统权限

在 Oracle 12c 中，一共有 237 项系统权限，可通过数据字典 system_privilege_map 查看所有的系统权限。

```
      -392 EXEMPT DDL REDACTION POLICY                          0
      -393 SELECT ANY MEASURE FOLDER                            0
      -394 ALTER ANY MEASURE FOLDER                             0
      -395 SELECT ANY CUBE BUILD PROCESS                        0
      -396 ALTER ANY CUBE BUILD PROCESS                         0
      -397 READ ANY TABLE                                       0

选定了 237 行
```

安全管理

□权限管理——系统权限

系统权限的授予

GRANT system_privilege_list | [ALL PRIVILEGES]

TO user_name_list | role_list | PUBLIC [WITH ADMIN OPTION];

--system_privilege_list：系统权限列表，以逗号分隔；

--ALL PRIVILEGES：所有系统权限；

---user_name_list：用户列表，以逗号分隔；

--role_list：角色列表，以逗号分隔；

--PUBLIC：给数据库中所有用户授权；

--WITH ADMIN OPTION：允许系统权限接收者再将权限授予其它用户

权限管理——系统权限

系统权限的回收

```
REVOKE system_privilege_list | [ALL PRIVILEGES]
FROM user_name_list | role_list | PUBLIC
```

- 多个管理员授予同一个用户相同的权限，其中一个管理员回收其授予用户的系统权限，该用户将不再具有该系统权限；
- 如果一个用户的权限具有传递性，并且给其它用户授权，那么该用户系统权限被收回后，由它授权用户的系统权限并不会受影响；

安全管理

□权限管理——对象权限

对象权限的授予

Oracle 数据库中，用户可以直接访问同名 Schema 下的数据库对象，如果需要访问其它 Schema 下的数据库对象，就需要具有相应的对象权限。

```
GRANT object_privilege_list | ALL [PRIVILEGES] [ (column,...) ]
ON [schema.]object
TO user_name_list | role_list | PUBLIC [WITH GRANT OPTION];
```

安全管理

□权限管理——对象权限

对象权限的回收

```
REVOKE object_privilege_list | ALL [PRIVILEGES]
ON [schema.]object
FROM user_name_list | role_list | PUBLIC [CASCADE CONSTRAINTS]
| [FORCE];
```

- 如果一个用户的对象权限具有传递性，并且已经给其它用户授权，那么该用户的对象权限被回收后，由它授权用户的对象权限也将被收回（这一条与系统权限传递性不同）。

安全管理

□权限管理——相关视图

视图名称	说明
DBA_SYS_PRIVS	所有**用户**和**角色**获得的系统权限信息
ALL_SYS_PRIVS	当前用户可见的全部**用户**和**角色**获得的系统权限信息
USER_SYS_PRIVS	当前用户获得的系统权限信息
DBA_TAB_PRIVS	包含所有**用户**和**角色**获得的对象权限信息
ALL_TAB_PRIVS	当前用户可见的全部**用户**和**角色**获得的对象权限信息
USER_TAB_PRIVS	当前用户获得的对象权限信息
DBA_COL_PRIVS	数据库中所有列对象的权限信息
ALL_COL_PRIVS	当前用户可见的所有列对象的权限信息
USER_COL_PRIVS	当前用户拥有或授予其它用户的所有列对象的权限
SESSION_PRIVS	当前会话可以使用的所有权限信息

安全管理

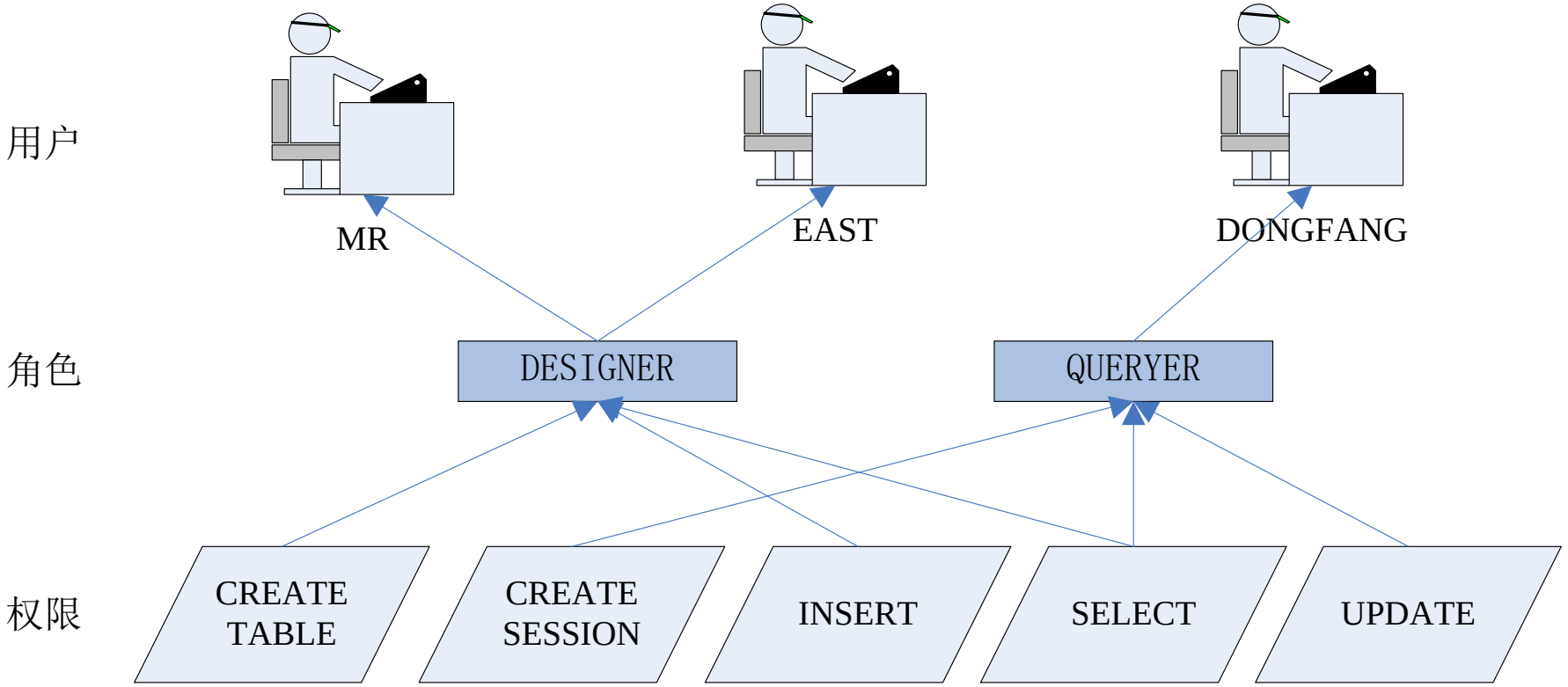
角色管理

角色是一个独立的数据库实体，它包括一组权限。也就是说，角色是包括一个或者多个权限的集合，它并不被哪个用户所拥有。角色可以被授予任何用户，也可以从用户收回。

- **权限管理更方便。**将角色赋予多个用户，实现不同用户相同的授权。如果要修改这些用户的权限，只需修改角色即可；
- **角色的权限可以激活和关闭。**使得 DBA 可以方便的选择是否赋予用户某个角色；
- **提高性能。**使用角色减少了数据字典中授权记录的数量，通过关闭角色使得在语句执行过程中减少了权限的确认。

安全管理

□角色管理



用户、角色、权限之间的关系

安全管理

□角色管理——常用预定义角色

Oracle 预定义角色有 25 种，经常用到的角色有 connect、resource、dba 三种。

- connect 角色具有一般应用开发人员需要的大部分权限。
- resource 角色具有开发人员需要的其他权限，如建立存储过程、触发器等，resource角色等，resource角色隐含了unlimited tablespace系统权限（无限制表空间）。
- dba 角色具有所有系统权限及 with admin option 选项，默认 dba 用户为 sys 和 system，它们可以将任何系统权限授予给其他用户。

安全管理

□角色管理——用户定义角色

```
--创建
create role role_name [ not identified | identified by [password] |
[exeternally] | [globally]]
--修改密码
alter role role_name identified by password;
--设置当前用户要生效的角色
set role role_name;
--删除角色
drop role role_name;
```

试一试

创建一个新角色role01，把create session和create table 权限赋予role01，再把role01角色赋予用户user

```
SQL> create role role01 ;

SQL> grant create session, create table to role01 ;

SQL> grant role01 to user;
```

安全管理

□角色管理——相关视图

视图名称	说明
DBA_ROLE_PRIVS	数据库中所有用户拥有的角色信息
USER_ROLE_PRIVS	包含当前用户拥有的角色信息
ROLE_ROLE_PRIVS	角色拥有的角色信息
ROLE_SYS_PRIVS	角色拥有的系统权限信息
ROLE_TAB_PRIVS	角色拥有的对象权限信息
DBA_ROLES	当前数据库中所有角色及描述信息
SESSION_ROLES	当前会话所具有的角色信息

安全管理

口审计

Audit 是监视和记录用户对数据库进行的操作，以供 DBA 进行问题分析。利用 Audit 功能，可以完成以下任务：

- 监视和收集特定数据库活动的数据。例如管理员能够审计哪些表被更新，在某个时间点上有多少个并行用户统计数据；
- 保证用户对自己的活动负责。这些活动包括在特定模式、特定表、特定行等对象上进行的操作；
- 审计数据库中的可疑活动。如一个未经授权的用户正从表中删除数据，那么数据库管理员必须审计所有数据库连接，以及在数据库中所有成功和失败的删除操作。

安全管理

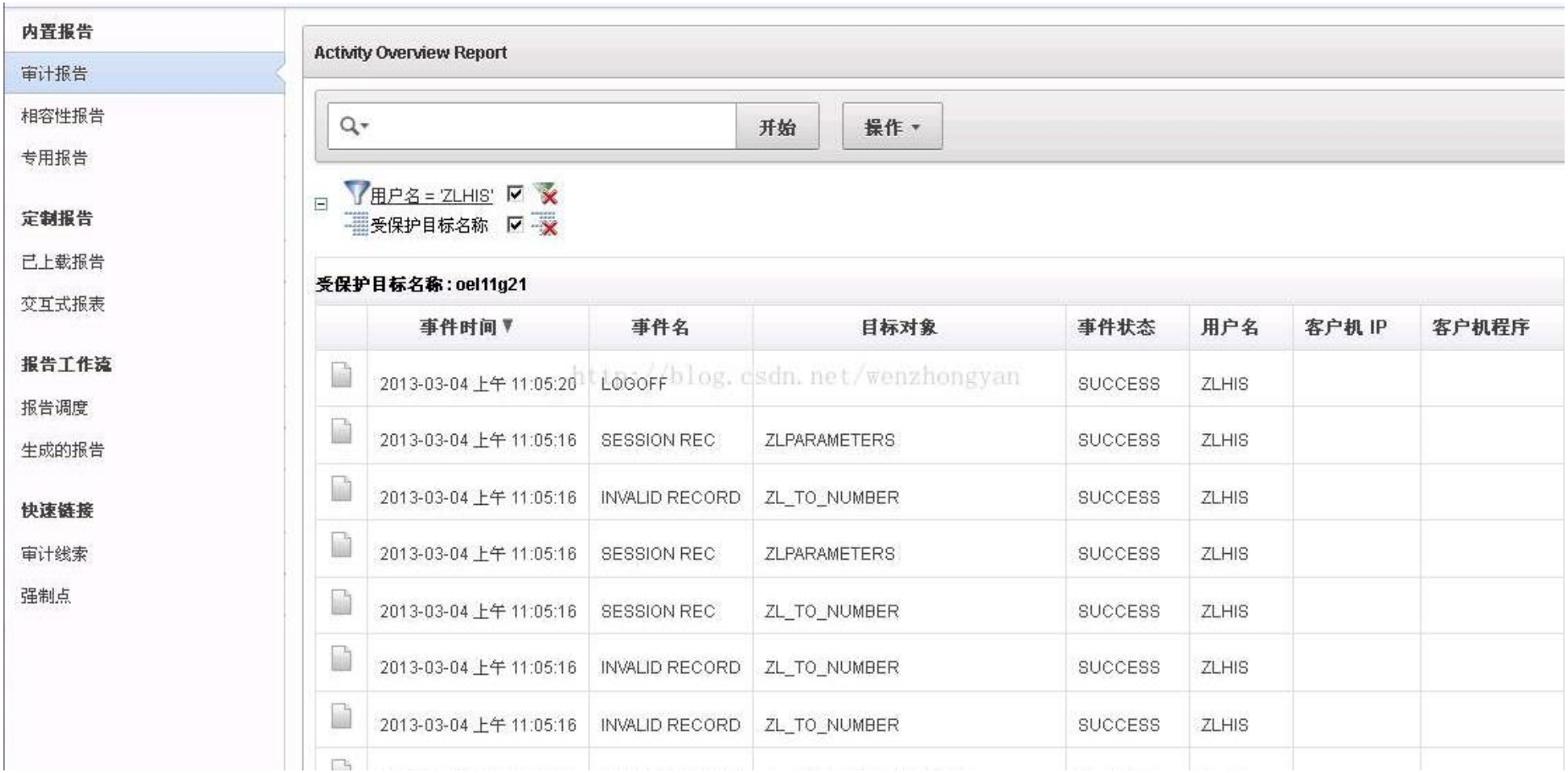
口审计

在 Oracle 12c 中，一共有4种审计类型：

- 语句审计（Statement Auditing）：对特定的 SQL 语句进行审计，不指定具体对象。
- 权限审计（Privilege Auditing）：对特定的系统权限使用情况进行审计。
- 对象审计（Object Auditing）：对特定的模式对象上执行的特定语句进行审计。
- 网络审计（Network Auditing）：对网络协议错误与网络层内部错误进行审计。

安全管理

口审计


内置报告
审计报告
相容性报告
专用报告
定制报告
已上载报告
交互式报表
报告工作流
报告调度
生成的报告
快速链接
审计线索
强制点
Activity Overview Report
开始
操作
用户名 = 'ZLHIS'
受保护目标名称
受保护目标名称 : oel11g21
事件时间
事件名
目标对象
事件状态
用户名
客户机 IP
客户机程序
2013-03-04 上午 11:05:20 LOGOFF SUCCESS ZLHIS
2013-03-04 上午 11:05:16 SESSION REC ZLPARAMETERS SUCCESS ZLHIS
2013-03-04 上午 11:05:16 INVALID RECORD ZL_TO_NUMBER SUCCESS ZLHIS
2013-03-04 上午 11:05:16 SESSION REC ZLPARAMETERS SUCCESS ZLHIS
2013-03-04 上午 11:05:16 SESSION REC ZL_TO_NUMBER SUCCESS ZLHIS
2013-03-04 上午 11:05:16 INVALID RECORD ZL_TO_NUMBER SUCCESS ZLHIS
2013-03-04 上午 11:05:16 INVALID RECORD ZL_TO_NUMBER SUCCESS ZLHIS

内容提纲

- 安全管理
- 备份与恢复

备份与恢复

□故障概述

故障类型

- 语句故障：在执行SQL语句过程中发生的逻辑故障
- 用户进程故障：当用户程序出错而无法访问数据库时发生的故障
- 实例故障：数据库实例由于硬件或软件问题无法继续运行
- 介质故障：数据库无法正确读取或写入某个数据库文件

备份与恢复

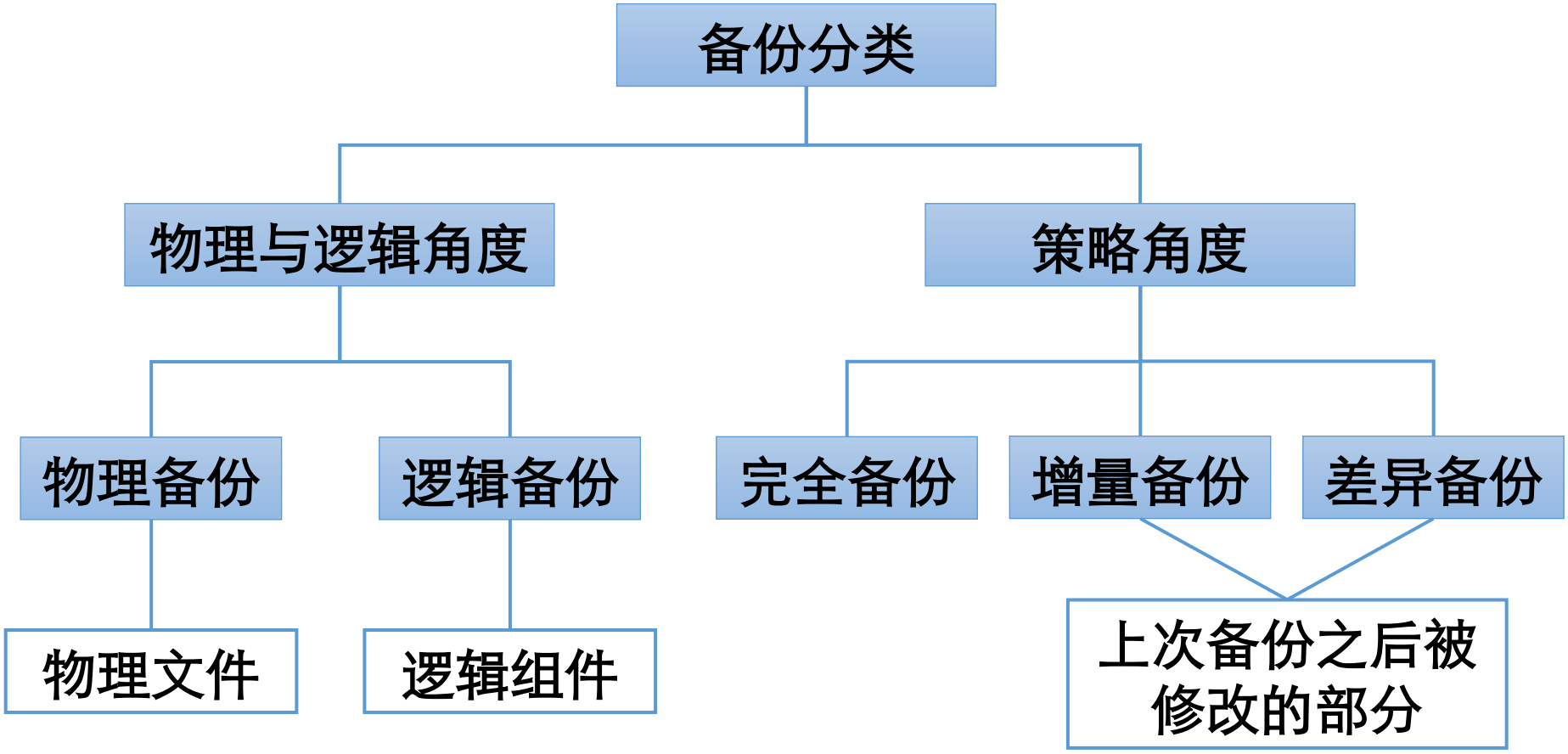
□概述

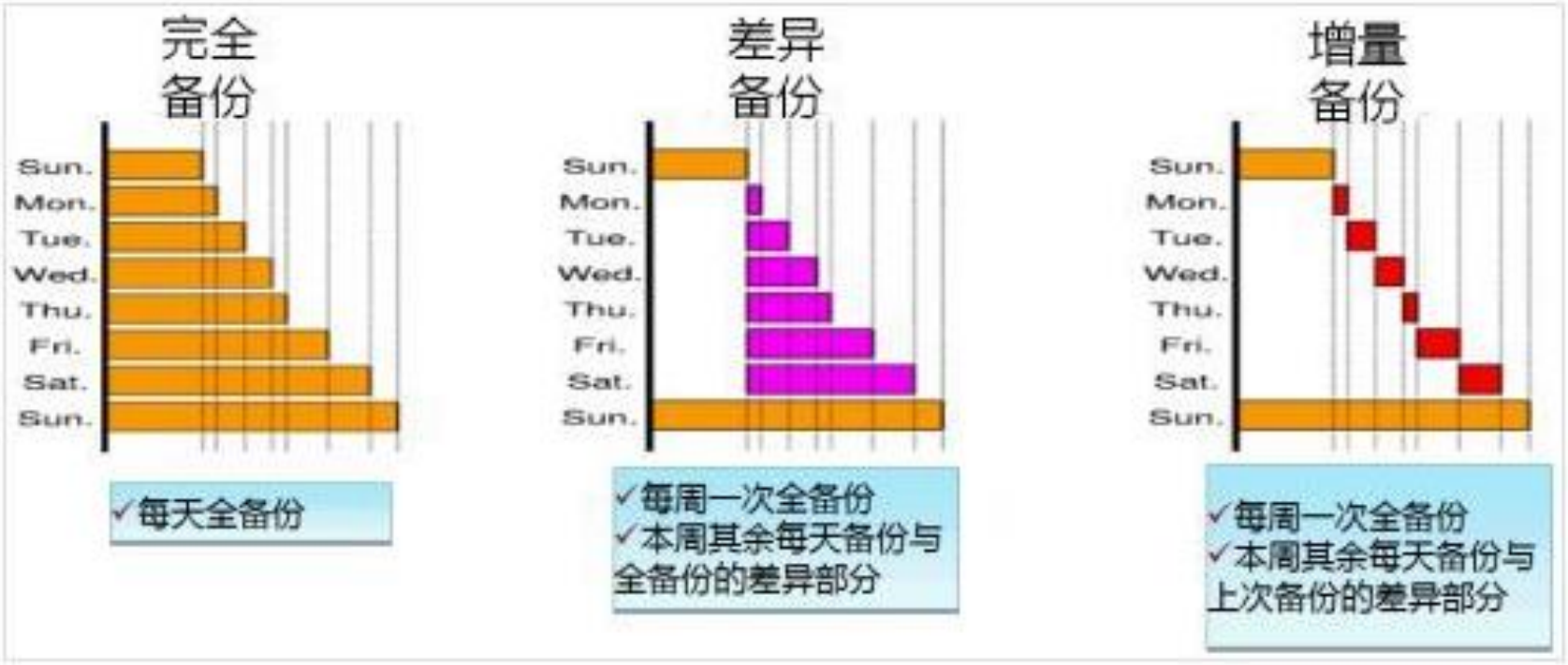
备份(Backup)和恢复(Recovery)是两个互相联系的概念，备份就是将数据库中的数据保存起来，而恢复就是当意外发生或者其他某种需要时，将已备份的数据还原到数据库中。

Oracle数据库12c提供了多种备份方法，每种方法都有自己的特点，需要根据具体的应用状况来选择合适的备份方法。Oracle设计备份策略的指导思想是：以最小的代价恢复数据。由于备份与恢复是密切联系的，备份策略应与恢复结合起来考虑。备份从不同的角度有不同的分类。

备份与恢复

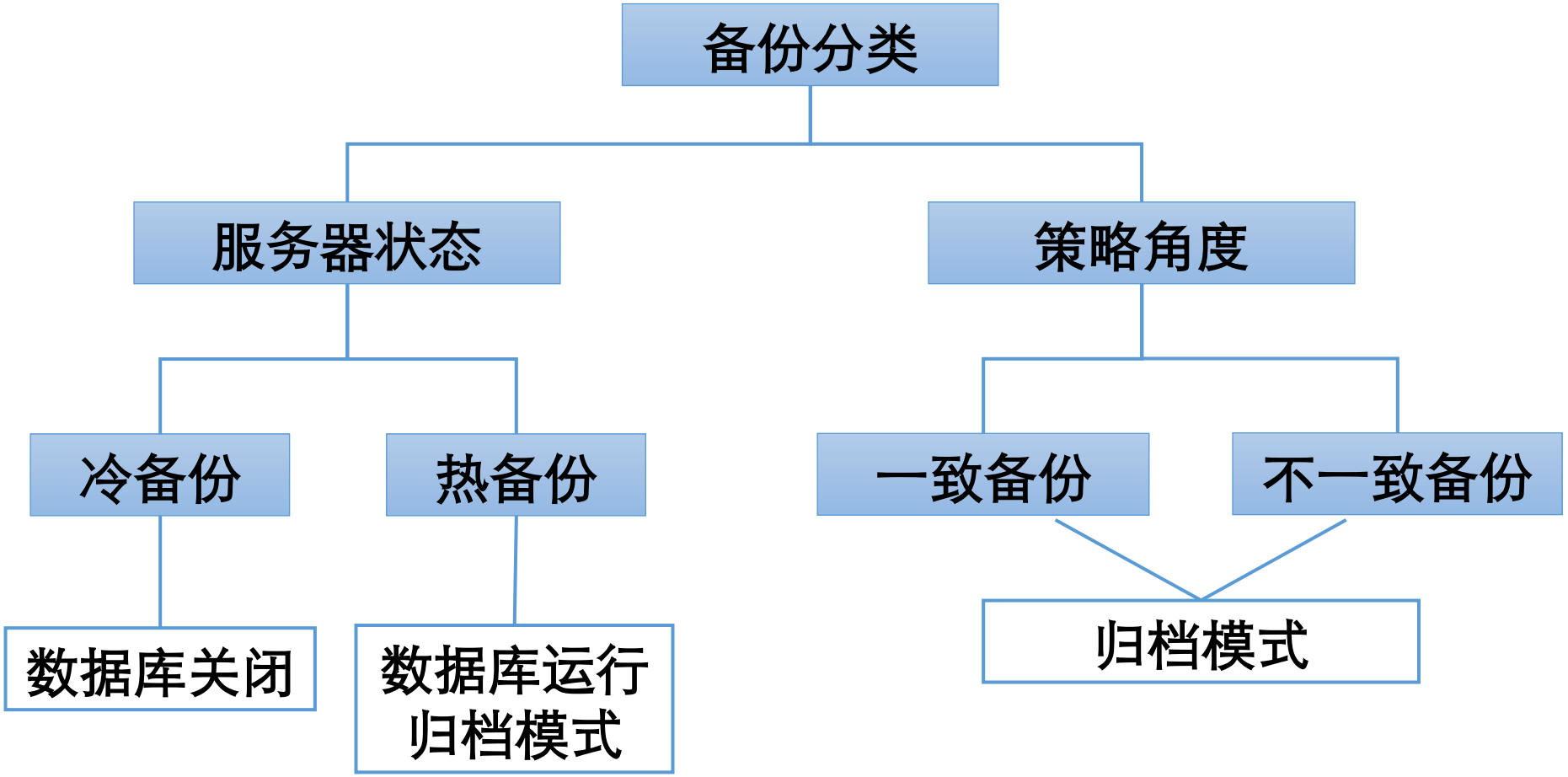
备份概述


备份分类
物理与逻辑角度
策略角度
物理备份
逻辑备份
完全备份
增量备份
差异备份
物理文件
逻辑组件
上次备份之后被修改的部分


完全
备份
Sun.
Mon.
Tue.
Wed.
Thu.
Fri.
Sat.
Sun.
✓每天全备份
差异
备份
Sun.
Mon.
Tue.
Wed.
Thu.
Fri.
Sat.
Sun.
✓每周一次全备份
✓本周其余每天备份与全备份的差异部分
增量
备份
Sun.
Mon.
Tue.
Wed.
Thu.
Fri.
Sat.
Sun.
✓每周一次全备份
✓本周其余每天备份与上次备份的差异部分

备份与恢复

□备份概述



备份与恢复

□恢复(Recovery)

恢复是指在数据库发生故障时，使用备份加载到数据库，使数据库恢复到备份时的正确状态。

1．根据故障原因，恢复可以分为实例恢复和介质恢复。

（1）实例恢复

实例恢复叫自动恢复，指当Oracle实例出现失败后，Oracle自动进行的恢复。

（2）介质恢复

指当存放数据库的介质出现故障时所作的恢复。

备份与恢复

□恢复(Recovery)

2．根据数据库使用的备份不同，恢复可以分为逻辑恢复和物理恢复。

（1）逻辑恢复

利用逻辑备份的二进制的文件，使用Oracle 提供的工具（例如Import，Impdp）将部分信息或全部信息导入数据库，从而进行恢复。

（2）物理恢复

使用物理备份的进行恢复，是在操作系统级别上进行的。

备份与恢复

□恢复(Recovery)

3．根据数据库恢复程度的不同，恢复可以分为完全恢复和不完全恢复。

（1）完全恢复

利用备份使数据库恢复到出现故障时的状态。

（2）不完全恢复

利用备份使数据库恢复到出现故障时刻之前的某个状态。

备份策略

1. 在刚建立数据库时，应该立即进行数据库的完全备份；
2. 将所有数据库备份保存在一个独立磁盘或磁盘组上，并通过使用基于RAID的存储系统来建立系统冗余数据；
3. 应该保持控制文件的多路复用，且控制文件的副本应该存放在不同磁盘控制器下的不同磁盘设备上；
4. 应该保持归档重做日志文件的多个拷贝。
5. 在磁盘上保持最小备份和数据库文件前滚所需的所有归档重组日志文件；
6. 保持多个联机日志文件组，每个组中至少应该有两个日志成员，同一日志组的多个成员应该分散存放在不同的磁盘上；
7. 保证两个归档重做日志文件的归档目标，不同归档目标应分散于不同的磁盘，且不要与数据库文件或联机重做日志文件存储在同一个物理磁盘设备上；
8. 定期执行数据库备份以减少恢复时间；
9. 如果条件允许，尽量保证数据库运行于归档模式；

备份策略

10. 增加、重命名、删除日志文件和数据文件，改变数据库结构，控制文件都应备份；
11. 在非归档模式下，当数据库结构发生变化时，应该进行数据库的完全备份；
12. 在归档模式下，对于经常使用的表空间，可以采用表空间备份方法提高备份效率；
13. 在归档模式下，通常不需要对联机重做日志文件进行备份；
14. 使用RESETLOGS方式打开数据库后，应该进行一个数据库的完全备份；
15. 对于重要的表中的数据，可以采用逻辑备份方式进行备份；
16. 确保应用数据位于独立的表空间中，以保证出现介质故障时其他应用可以继续使用

恢复策略

1. 根据数据库介质故障原因，确定采用完全介质恢复还是不完全介质恢复；
2. 如果数据库运行在非归档模式，则当介质故障发生时，只能进行数据库的不完全恢复，将数据库恢复到最近的备份时刻的状态；
3. 如果数据库运行在归档模式，则当一个或多个数据文件损坏时，可以使用备份的数据文件进行完全或不完全恢复数据库；
4. 如果数据库运行在归档模式，则当数据库的控制文件损坏时，可以使用备份的控制文件实现数据库的不完全恢复：
5. 如果数据库运行在归档模式，则当数据库的联机日志文件损坏时，可以使用备份的数据文件和联机重做日志文件不完全恢复数据库；
6. 如果执行了不完全恢复，则当重新打开数据库时应该使用RESETLOGS选项。

备份与恢复

归档模式和非归档模式

Oracle 运行的时候至少需要两组联机日志，每当一组日志写满后会发生日志切换，继续向下一组联机日志写入。

- 归档模式：触发 ARCn 进程，把写满的重做日志文件复制到归档日志文件。
- 非归档模式：重做日志直接被覆盖。非归档模式只能进行脱机备份，备份过程中数据库不能使用；必须备份整个数据库，不能备份部分数据库，只能部分恢复，如果数据文件丢失，只能恢复最后一次的完全备份，而之后的所有数据库改变将全部丢失。

备份与恢复

归档模式的优点

- 对于数据库所作的全部改动都记录在日志文件中，如果发生磁盘故障等导致数据文件丢失的话，则可以利用物理备份和归档日志完全恢复数据库，不会丢失任何数据。
- 可以进行联机热备，就是在数据库运行的状态下对数据库进行备份，其它用户不受影响。
- 能够增量备份。

备份与恢复

切换归档模式

```
sqlplus  / as sysdba  --sys用户登录数据库
archive log list;  --查看当前模式，默认为非归档模式
shutdown immediate;  --关闭数据库
（建议先备份数据库，以免切换过程中出现异常）
startup mount;  --启动数据库到mount模式
alter database archivelog;  --修改数据库为归档模式
alter database open;  --打开数据库
SELECT name,created,log_mode FROM v$database;  --查看刚创建的归档
show parameter db_recovery_file_dest;  --查看归档日志的路径和目录
--修改归档日志的目录和路径
alter system set db_recovery_file_dest_size=4000M;
alter system set db_recovery_file_dest='path';
```

安全管理

RMAN 概述

RMAN（Recovery Manager）是一种用于备份（backup）、还原（restore）和恢复（recover）数据库的 Oracle 工具。RMAN 默认随 Oracle 一同安装只能用于 ORACLE 8 或更高的版本中。

```
C:\Users\ICESPARK5>rman

恢复管理器: Release 12.1.0.2.0 - Production on 星期六 12月 7 23:27:09 2019

Copyright (c) 1982, 2014, Oracle and/or its affiliates.  All rights reserved.

RMAN>
```

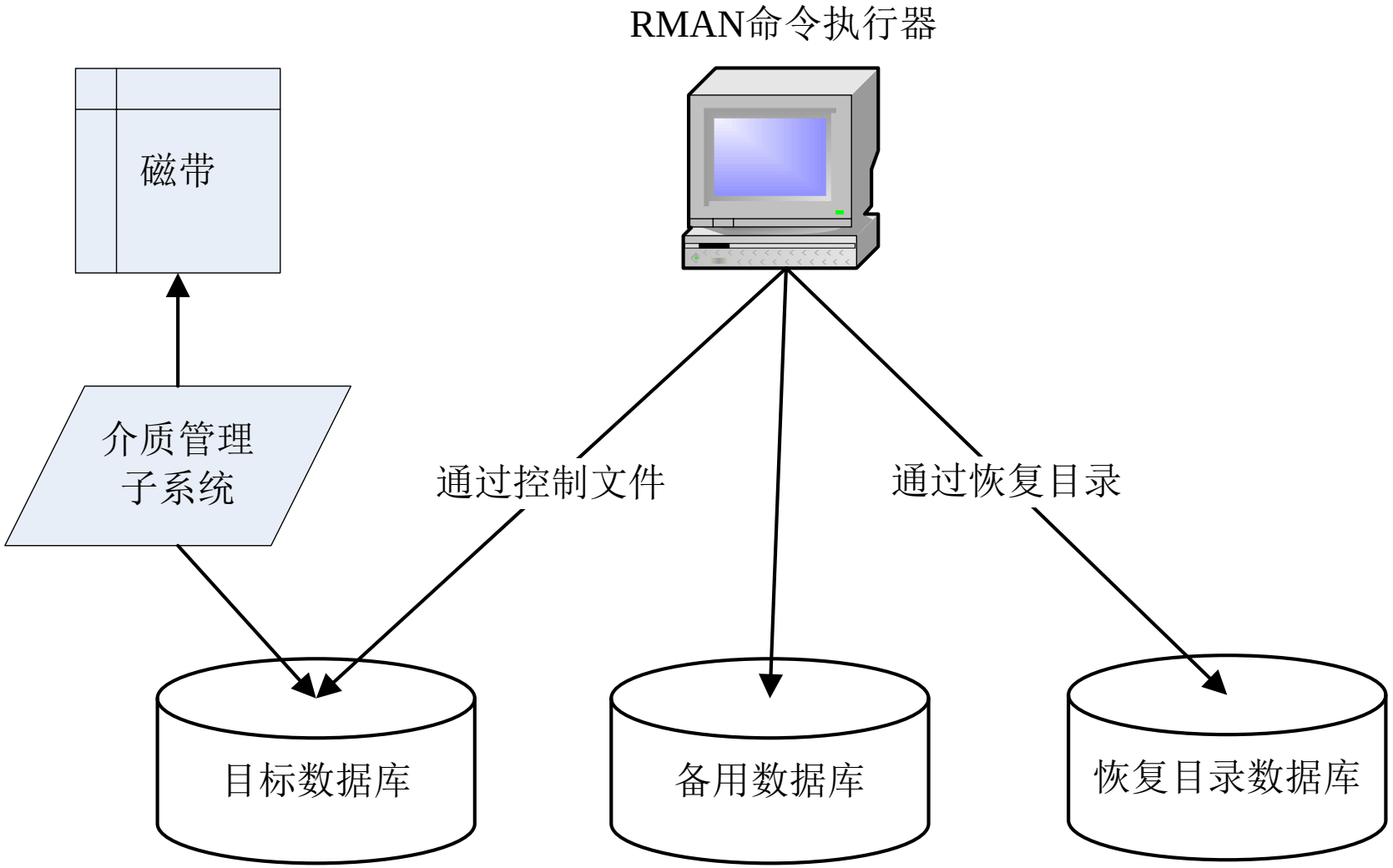
备份与恢复

RMAN 概述

- 能够实现对目标数据库的控制文件、数据文件、归档日志文件以及 SPFILE 的联机备份。
- 能够实现对数据库的完全或不完全的恢复操作。
- 支持在线热备份、多级增量备份、并行备份和恢复。
- RMAN的新的块比较特性允许在备份中跳过数据文件中从未使用的数据块的备份，从而节省了存储空间和备份时间。
- 操作简单，一条简单的命令，如 BACKUP DATABASE 就可以备份整个数据库，而不需要复杂的脚本。
- 可以容易地进行自动化备份和恢复。

备份与恢复

RMAN 组件



备份与恢复

RMAN 组件

- **RMAN 命令执行器**：提供对 RMAN 实用程序的访问，DBA 可以使用命令行或 GUI 工具与 RMAN 进行交互。
- **目标数据库**：即指想要备份、还原与恢复的数据库。
- **恢复目录和恢复目录数据库**：用于存放 RMAN 元数据，可以将目标数据库的 RMAN 元数据等相关信息写入到一个单独的数据库。通过使用恢复目录，可以永久保留需要的RMAN 元数据。
- **介质管理子系统**：用于RMAN从磁带进行备份与还原。
- **备份数据库**：目标数据库的一个副本，可用于故障转移。

备份与恢复

RMAN 备份

当数据库打开时，可以使用 RMAN BACKUP 命令备份：

- 数据库：如果备份操作是在数据库被安全关闭之后进行的，那么对整个数据库的备份是一致的；与之相对应，如果是在打开状态下对整个数据库进行的备份，则该备份是非一致的。
- 表空间：当数据库打开或关闭时，RMAN 还可以对表空间进行备份。但是，所有打开的数据库备份都是非一致的。如果在 RMAN 中对联机表空间进行备份，则不需要在备份前执行 ALTER TABLESPACE…BEGIN BACKUP 语句将表空间设置为备份模式。

备份与恢复

RMAN 备份

当数据库打开时，可以使用 RMAN BACKUP 命令备份如下对象：

- 数据文件：可以使用 BACKUP DATAFILE 命令对单独的数据文件进行备份，备份数据文件时，既可以使用其名称指定数据文件，也可以使用其在数据库中的编号指定数据文件。
- 控制文件：最简单的方法是设置 CONFIGURE CONTROLFILE AUTOBACKUP 为 ON，这样将启动自动备份功能，当在 RMAN 中执行 BACKUP 或 COPY 命令时，RMAN 都会对控制文件进行一次自动备份。

备份与恢复

RMAN 备份

当数据库打开时，可以使用 RMAN BACKUP 命令备份如下对象：

- 归档重做日志：归档重做日志是成功进行介质恢复的关键，需要周期性地进行备份。在 RMAN 中，可以使用 BACKUP ARCHIVELOG 命令对归档重做日志文件进行备份，或者使用 BACKUP PLUS ARCHIVELOG 命令，在对数据文件、控制文件进行备份的同时备份。

备份与恢复

RMAN 恢复

- 恢复处于非归档模式的数据库：当数据库处于非归档模式时，如果出现介质故障，则在最后一次备份之后对数据库所做的任何操作都将丢失。通过 RMAN 执行恢复时，只需要执行 RESTORE 命令将数据库文件修复到正确的位置，然后就可以打开数据库。
- 恢复处于归档模式的数据库：管理员还需要将归档重做日志文件的内容应用到数据文件上。在恢复过程中，RMAN 会自动确定恢复数据库所需要的归档重做日志文件。

备份与恢复

RMAN 恢复——部分恢复

- 基于时间的不完整恢复：如果知道存在问题的事务的确切发生时间，执行基于时间的不完全恢复时非常适合的。例如，假设用户在 10:00 将大量数据加载到一个错误的表中，那么 DBA 可以执行基于时间的恢复，即将数据库恢复到 9:59 时的状态。
- 基于更改的不完整恢复：对于基于更改的不完全恢复，则已存在问题的事务的 SCN 号来终止恢复过程，在恢复数据库之后，将包含低于指定 SCN 号的所有事务。可以使用 SET UNTIL SCN 命令来指定恢复过程的终止 SCN 号。

备份与恢复

RMAN 恢复——restore 和 recover

- Restore 是使用备份文件，将数据库还原到过去的某个状态。
- Recovery 是使用 redo 日志和归档日志将数据库向前恢复到现在这个时点。

某数据库，每天凌晨一点会作一次备份。某天下午两点时数据库文件损害，同时数据库宕机。接着DBA开始恢复数据库。

1. 首先，使用最近一次的备份文件还原数据库到当天凌晨一点的状态。但是凌晨一点到下午两点的数据丢失了。
2. 接着，使用 redo 日志和归档日志，把当天凌晨一点开始的数据库操作重做一遍，直到下午两点数据库宕机前。

备份与恢复

□RMAN 备份和恢复的简单示例

将数据库改为归档模式；

查看 pdborcl 的归档模式；

rman target / --Windows命令行下RMAN连接数据库

backup pluggable database pdborcl;

针对pdborcl做一定的修改，保证修改生效

restore pluggable database pdborcl;

recover pluggable database pdborcl;

查看是否恢复成功。

备份与恢复

□数据泵简介

Oracle 使用数据泵（DATA PUMP）技术实现逻辑备份。逻辑备份时创建数据库对象的逻辑副本，并存入一个二进制转储文件的过程。从本质上来讲逻辑备份与恢复实际就是对数据库事实数据的导入和导出。

- 导出：即数据库的逻辑备份，实质是读取一个数据库记录并将这个记录集写入一个文件（扩展名通常是dmp），这些记录的导出与物理位置无关。
- 导入：即数据库的逻辑恢复，实质是读取被导出的二进制转储文件并将其恢复到数据库。

课后作业

1. 查看 Oracle12c 预定义的用户和角色，查看系统权限。

2. 尝试新建用户和角色，并为用户分配该角色。

3. 尝试使用 RMAN 进行简单备份和恢复。