数据安全：
传统企业数据库安全经验分享

——代海鹏

泄密事件

对公司、社会带来持久广泛恶劣影响：

- 十大酒店泄露大量房客开房信息，包括姓名，身份证，房型，时间；
- 韩2000万信用卡信息泄露 引发“销户潮”；
- 某网数据泄漏，全国各地有39名用户被骗，诈骗金额高达140多万；
- 某贷宝被脱裤，导致10G裸条泄露。

▲ 99%数据丢失 ▼ 30%数据丢失

面对泄密 DBA能做什么？

01用户管理

02权限管理

03日志管理

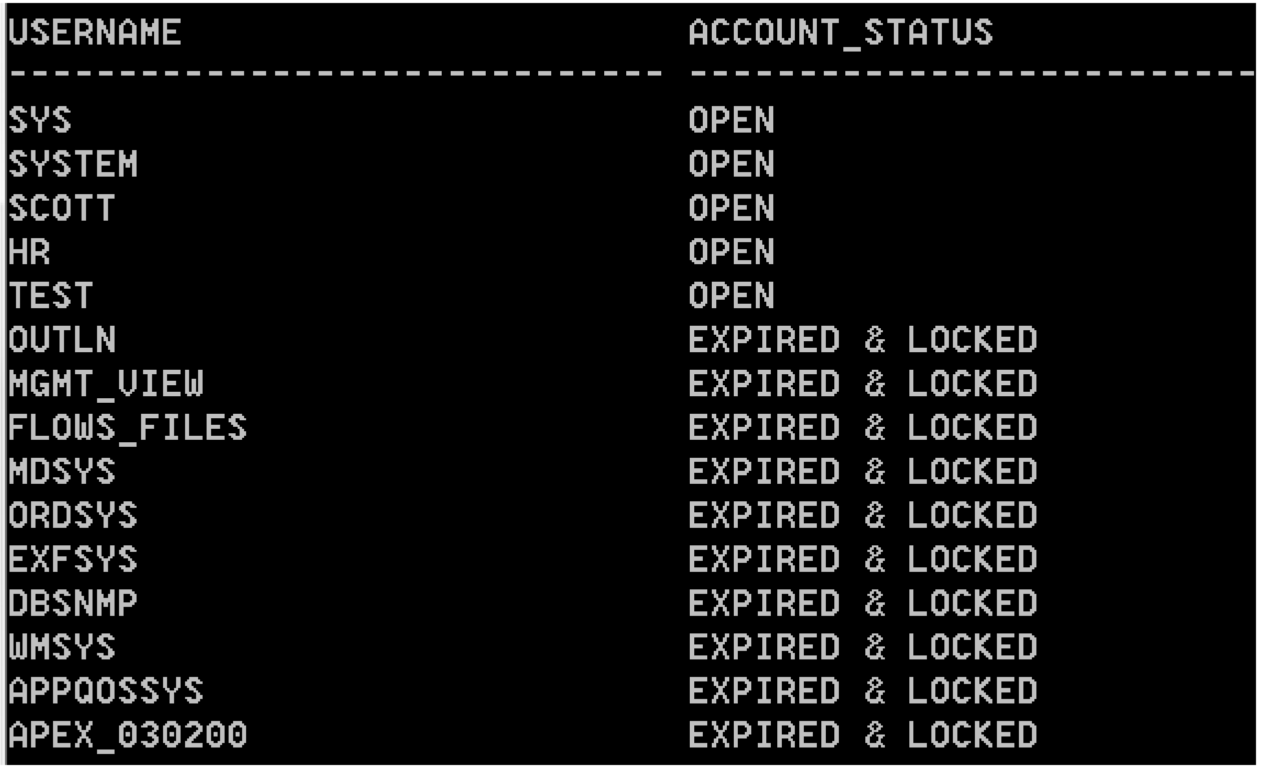
04漏洞管理

VIRUS
CRACKER
INTRUDER
SPYWARE
PASSWORD
IDENTITY
CODE
UNSAFE
HACKER
THEFT

01

用户管理

清理锁定无用数据库帐号



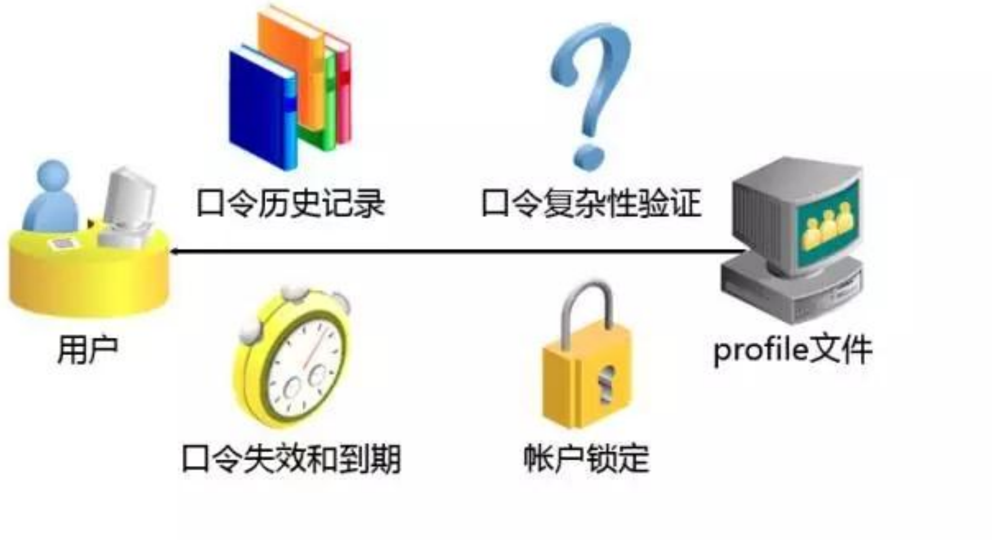
```
USERNAME                       ACCOUNT_STATUS
------------------------------ --------------------------
SYS                            OPEN
SYSTEM                         OPEN
SCOTT                          OPEN
HR                             OPEN
TEST                           OPEN
OUTLN                          EXPIRED & LOCKED
MGMT_VIEW                      EXPIRED & LOCKED
FLOWS_FILES                    EXPIRED & LOCKED
MDSYS                          EXPIRED & LOCKED
ORDSYS                         EXPIRED & LOCKED
EXFSYS                         EXPIRED & LOCKED
DBSNMP                         EXPIRED & LOCKED
WMSYS                          EXPIRED & LOCKED
APPQOSSYS                      EXPIRED & LOCKED
APEX_030200                    EXPIRED & LOCKED
```

默认31个帐号

SCHEMA
OVERVIEW

DEFAULT profile
并没有PASSWORD_VERIFY_FUNCTION

通过执行：
@$ORACLE_HOME/rdbms/admin/utlpwdmg.sql
生成，并自动应用到profile



VERIFY_FUNCTION_11G：
-- Check for the minimum length(8) of the password
-- Check if the password is same as the username or username
-- Check if the password is same as the username reversed
-- Check if the password is the same as server name
    and or servername(1-100)
-- Check if the password is too simple. A dictionary of words may be
    maintained and a check may be made so as not to allow the words
    that are too simple for the password.
-- Check if the password is the same as oracle (1-100)
-- Check if the password contains at least one letter, one digit
   1. Check for the digit
   2. Check for the character
      Check if the password differs from the previous password by at
least 3 letters

VIRUS
CRACKER
PASSWORD
CODE
HACKER
INTRUDER
SPYWARE
IDENTITY
UNSAFE
THEFT

02

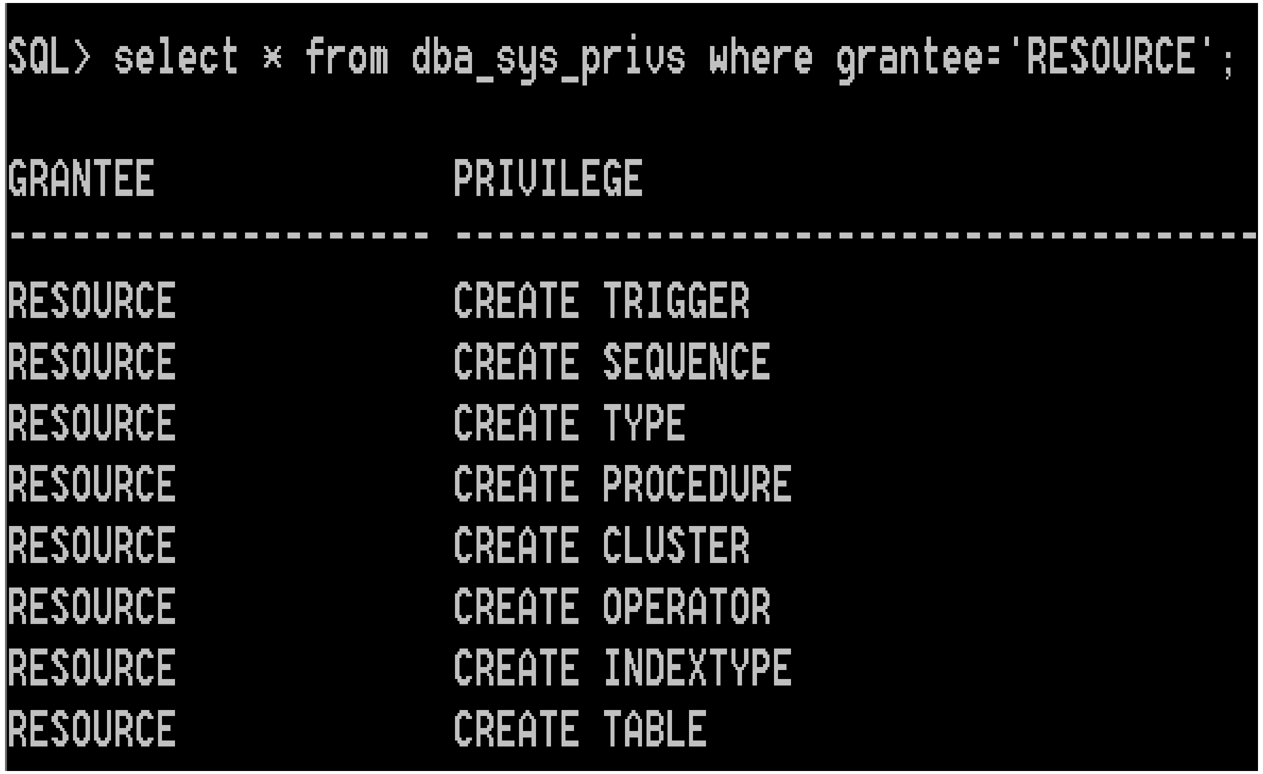
权限管理

最小化应用账户权限

- 默认connect,reousrce，加create view权限。
- 数据字典普通用户禁止访问
- O7_DICTIONARY_ACCESSIBILITY
- 通过设置ROLE进行赋权

最小化DBA权限拥有者数量

- DBA组只有oracle用户（操作系统）
- 检查拥有DBA权限的用户



```
SQL> select * from dba_sys_privs where grantee='RESOURCE';

GRANTEE                PRIVILEGE
--------------------   --------------------------------------
RESOURCE               CREATE TRIGGER
RESOURCE               CREATE SEQUENCE
RESOURCE               CREATE TYPE
RESOURCE               CREATE PROCEDURE
RESOURCE               CREATE CLUSTER
RESOURCE               CREATE OPERATOR
RESOURCE               CREATE INDEXTYPE
RESOURCE               CREATE TABLE
```

VIRUS
CRACKER
INTRUDER
SPYWARE
PASSWORD
IDENTITY
CODE
UNSAFE
THEFT
HACKER

03

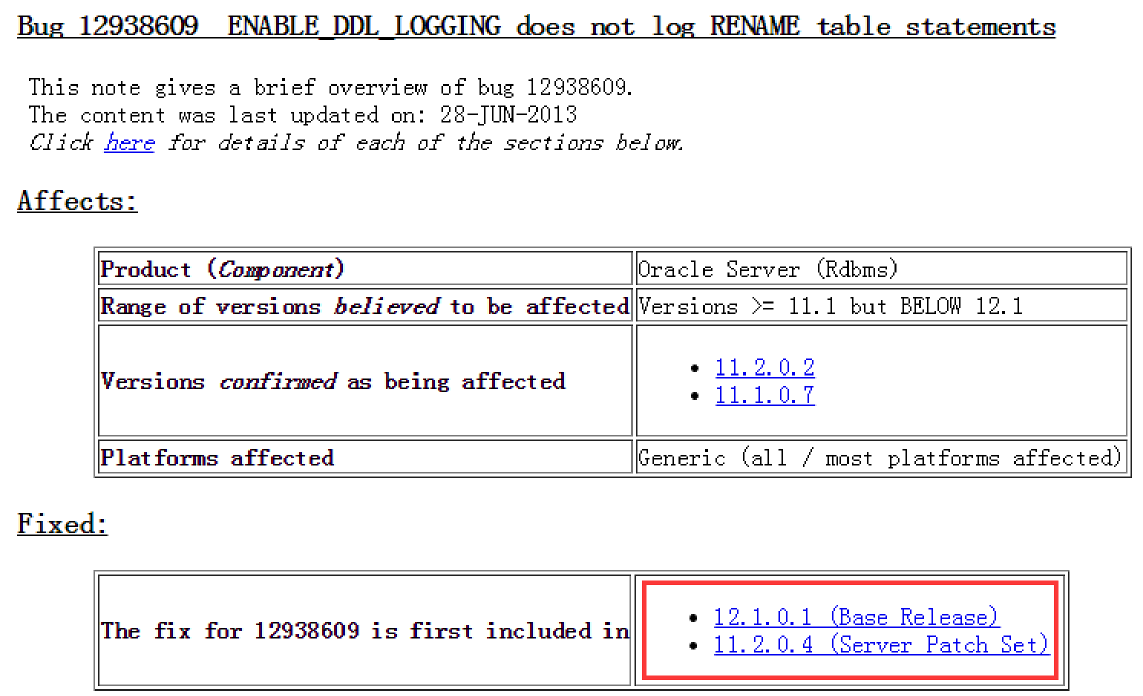
日志管理

审计

AUDIT_TRAIL： 审计普通用户
AUDIT_SYS_OPERATIONS：审计sys权限用户
注意：
aud$表挪出SYSTEM表空间
AUDIT_FILE_DEST审计文件位置更改为单独LV
NOAUDIT CREATE SESSION默认停止审计命令

ENABLE_DDL_LOGGING
11G新特性
Wed Jun 10 01:46:52 2015
create table lc0039999.t1 as select * from dba_objects

12C
存放路径：
$ORACLE_BASE/diag/rdbms/DBNAME/log|ddl, xml
文件中包含DDL命令，**IP地址，时间戳**等信息



Bug 12938609 ENABLE_DDL_LOGGING does not log RENAME table statements

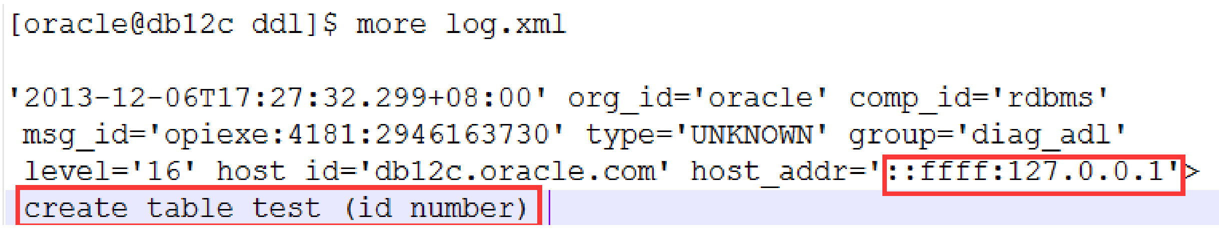
This note gives a brief overview of bug 12938609.
The content was last updated on: 28-JUN-2013
Click here for details of each of the sections below.

Affects:

Product (*Component*)	Oracle Server (Rdbms)
Range of versions *believed* to be affected	Versions >= 11.1 but BELOW 12.1
Versions *confirmed* as being affected	- 11.2.0.2 - 11.1.0.7
Platforms affected	Generic (all / most platforms affected)

Fixed:

The fix for 12938609 is first included in	- 12.1.0.1 (Base Release) - 11.2.0.4 (Server Patch Set)



```
[oracle@db12c ddl]$ more log.xml

'2013-12-06T17:27:32.299+08:00' org_id='oracle' comp_id='rdbms'
 msg_id='opiexe:4181:2946163730' type='UNKNOWN' group='diag_adl'
 level='16' host_id='db12c.oracle.com' host_addr='::ffff:127.0.0.1'>
 create table test (id number)
```

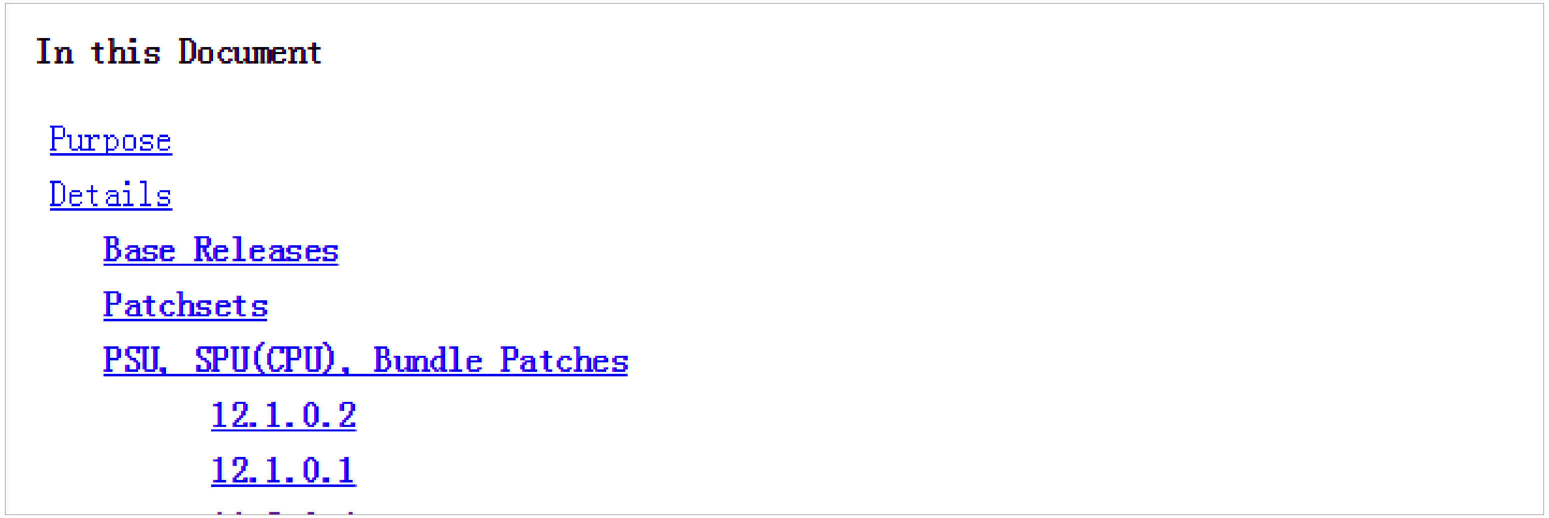
VIRUS
CRACKER
INTRUDER
SPYWARE
PASSWORD
IDENTITY
CODE
UNSAFE
THEFT
HACKER

04

漏洞管理

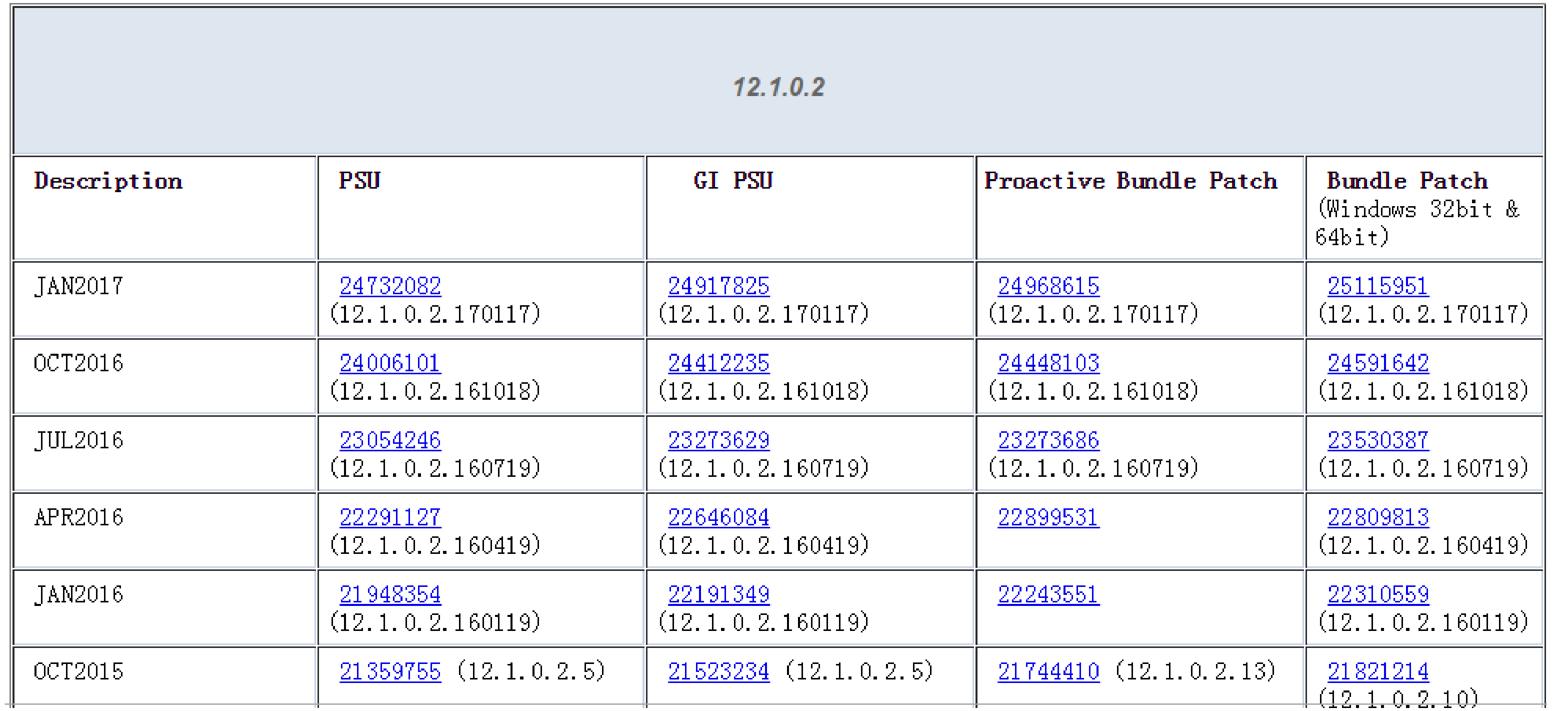
最新的PSU：

1454618.1



In this Document

- Purpose
- Details
  - Base Releases
  - Patchsets
  - PSU, SPU(CPU), Bundle Patches
    - 12.1.0.2
    - 12.1.0.1



12.1.0.2				
Description	PSU	GI PSU	Proactive Bundle Patch	Bundle Patch (Windows 32bit & 64bit)
JAN2017	24732082 (12.1.0.2.170117)	24917825 (12.1.0.2.170117)	24968615 (12.1.0.2.170117)	25115951 (12.1.0.2.170117)
OCT2016	24006101 (12.1.0.2.161018)	24412235 (12.1.0.2.161018)	24448103 (12.1.0.2.161018)	24591642 (12.1.0.2.161018)
JUL2016	23054246 (12.1.0.2.160719)	23273629 (12.1.0.2.160719)	23273686 (12.1.0.2.160719)	23530387 (12.1.0.2.160719)
APR2016	22291127 (12.1.0.2.160419)	22646084 (12.1.0.2.160419)	22899531	22809813 (12.1.0.2.160419)
JAN2016	21948354 (12.1.0.2.160119)	22191349 (12.1.0.2.160119)	22243551	22310559 (12.1.0.2.160119)
OCT2015	21359755 (12.1.0.2.5)	21523234 (12.1.0.2.5)	21744410 (12.1.0.2.13)	21821214 (12.1.0.2.10)

面对数据丢失，
DBA能做什么？

常见数据丢失类型

在平时运行维护时，总会有种种情况导致业务数据丢失或者损坏，无论丢失是多是少，我们DBA都应该尽量避免发生

系统故障

CPU损坏、内存损坏、主板损坏、操作系统故障等问题

存储故障

UPS电源掉电、存储控制器损害、物理硬盘损坏

数据库BUG

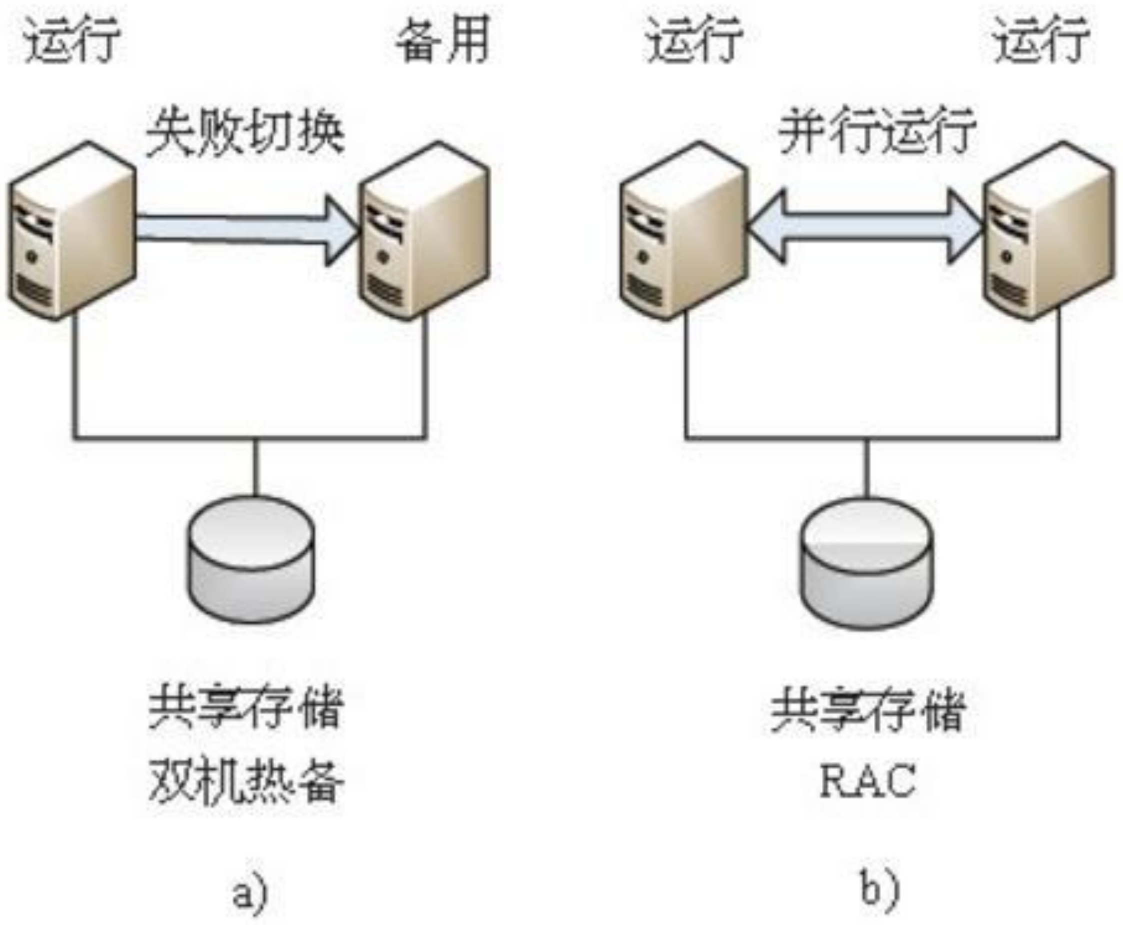
因触发数据库bug导致刷入存储的数据块逻辑损坏

人为操作故障

错误/恶意删除数据；错误/恶意执行程序或命令等

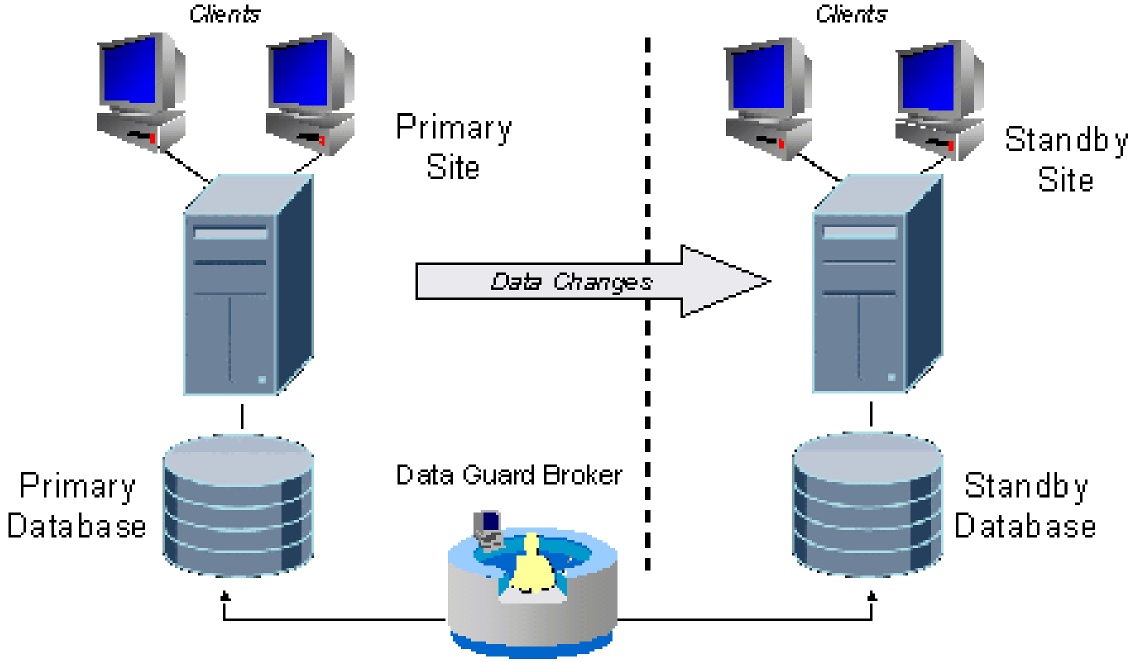
系统故障

Oracle **Real** Application Cluster



存储故障

Oracle Active Data Guard



数据库BUG

Oracle Active Data Guard Redo Log **Delay** Apply

```
alter database recover managed standby database
delay 120 disconnect from session;
```

人为操作故障

防为主、治为辅

制定变更规范

制定变更方案

延时容灾方案

最后一道防线

备份

DBAplus

www.dbaplus.cn

THANK YOU