ACOUG
All China Oracle User Group
中国 Oracle 用户组

YUNHE ENMO (BEIJING) TECHNOLOGY CO.,LTD

Oracle Database Security & Recovery Case Study

盖国强（Eygle）
电话:13911812803
邮件:eygle@enmotech.com
微博:weibo.com/eygle

DTCC2012

YUNHE

Who am I

- 盖国强　云和恩墨（北京）信息技术有限公司　创始人
  - 盖国强是国内第一个Oracle ACE及ACE总监
  - 有超过10年的Oracle从业经验

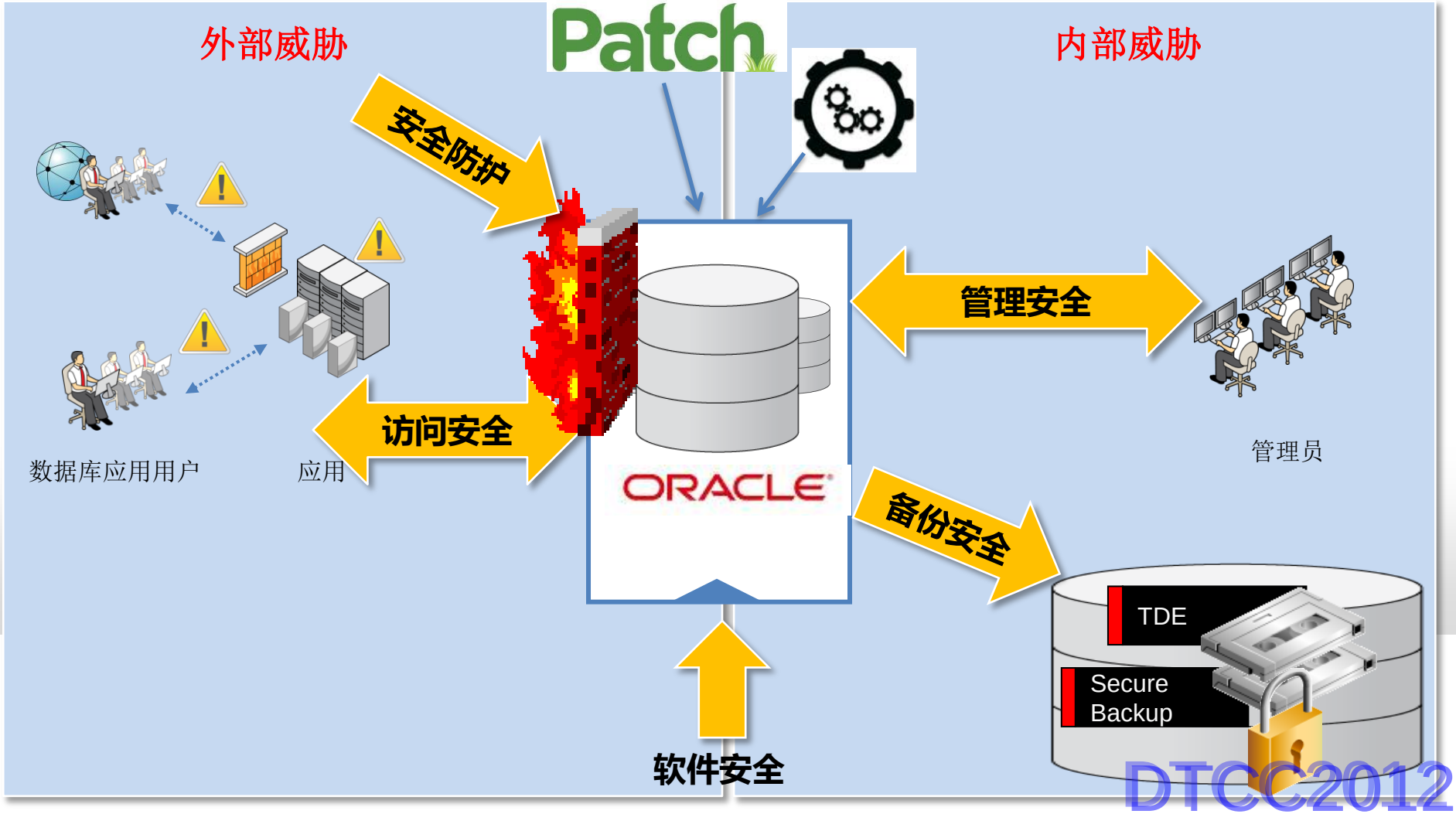
    至今仍然奋战在技术前线
  - 国内最大数据库技术论坛ITPUB的主要发起人之一，致力于技术分享与传播，截至2011年已经出版了10本技术书籍　自2010年开始，主编出版《Oracle DBA手记》系列书
  - 2010年，他和张乐奕共同创建了旨在开展技术交流的中国Oracle用户组（ACOUG - All China

YUNHE

信息安全：三个要素和10个Domain

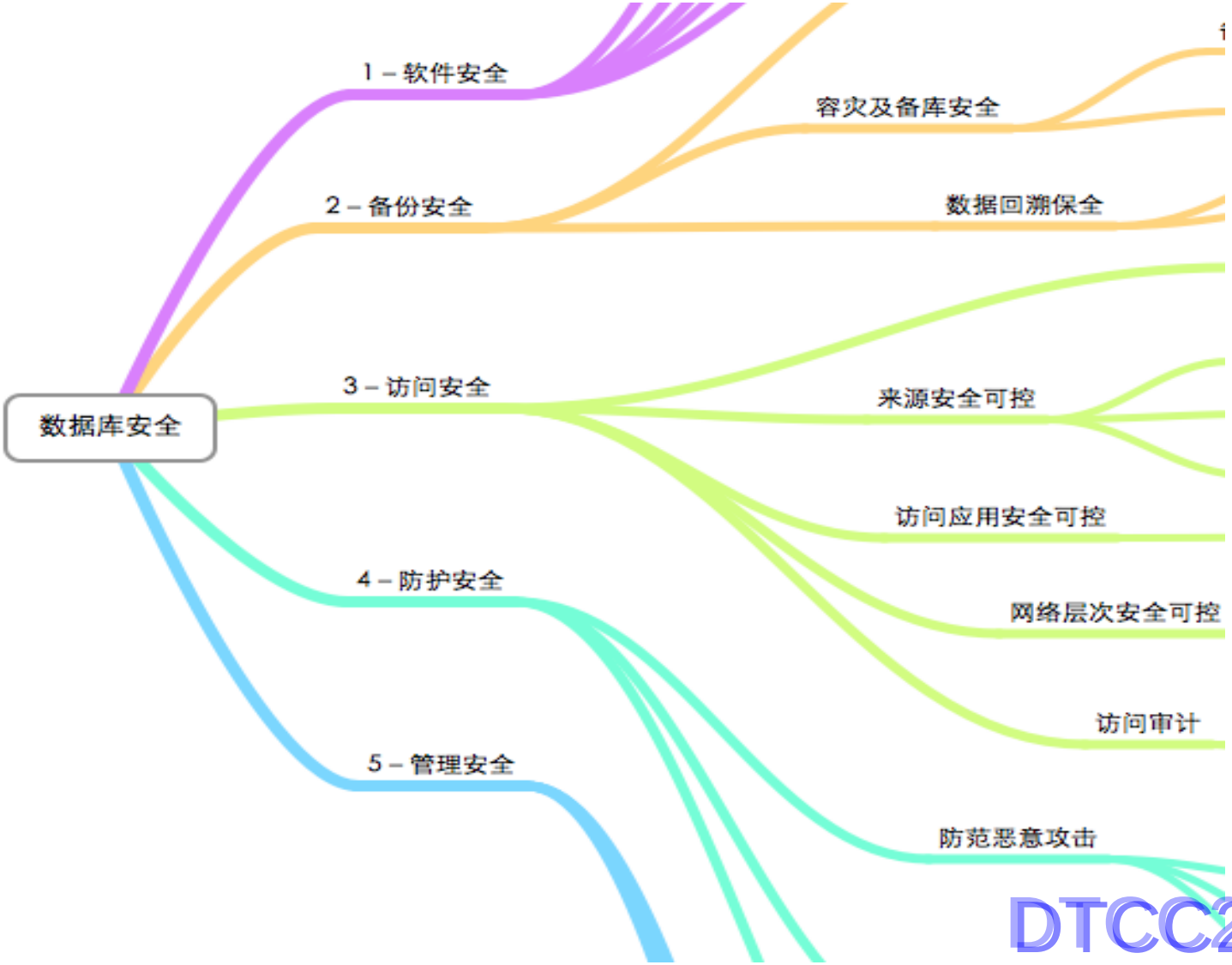
YUNHE

数据库安全-威胁来自何方？



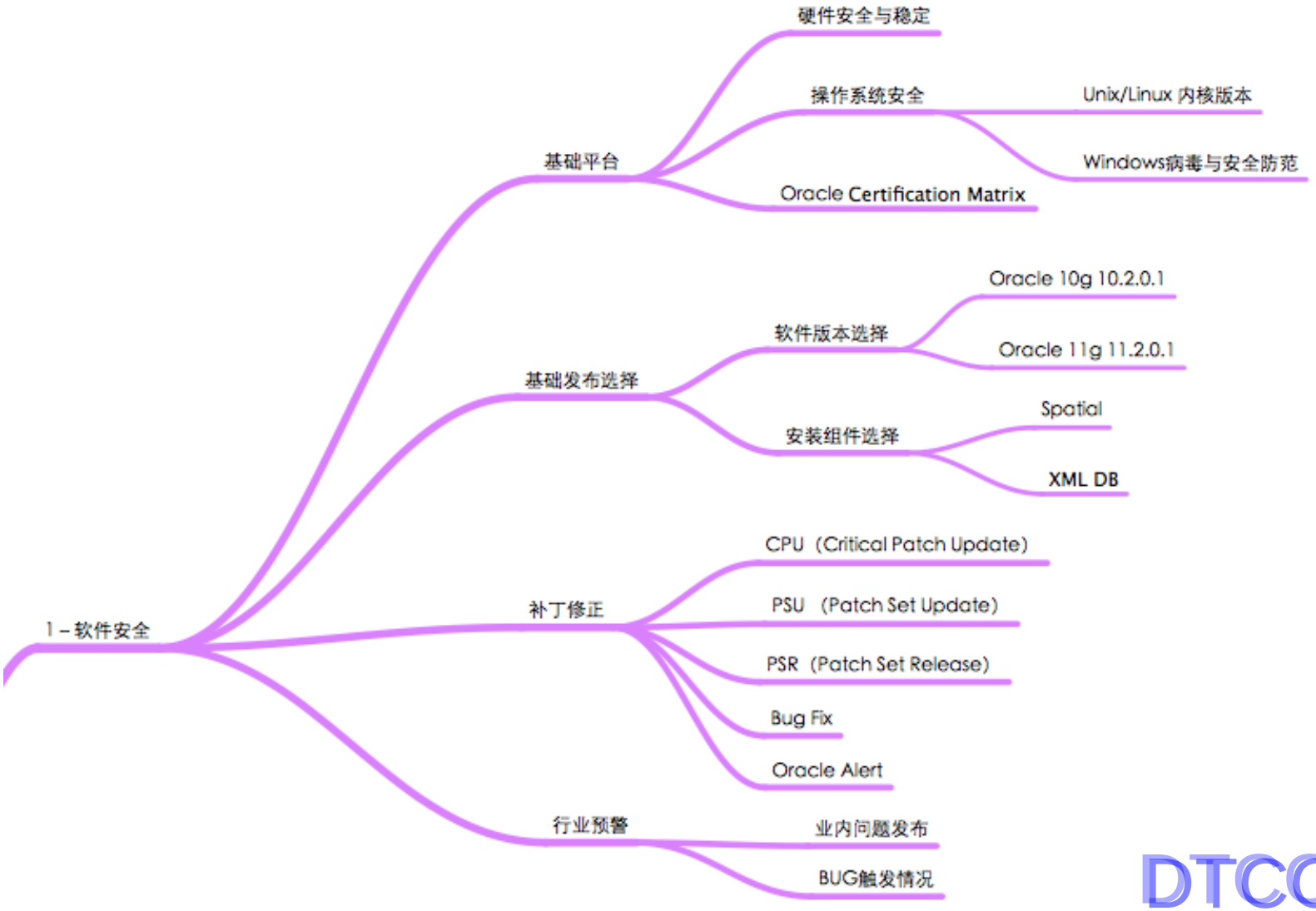
YUNHE

数据库安全-安全的五大方向



YUNHE

数据库安全-软件安全



YUNHE

软件安全-安全补丁和组件安全

```
SQL> connect eygle/eygle
Connected.
SQL> select * from user_role_privs;

USERNAME                       GRANTED_ROLE                   ADM DEF OS_
------------------------------ ------------------------------ --- --- ---
EYGLE                          CONNECT                        NO  YES NO
EYGLE                          RESOURCE                       NO  YES NO
PUBLIC                         PLUSTRACE                      NO  YES NO

SQL> exec ctxsys.driload.validate_stmt('grant dba to eygle');
BEGIN ctxsys.driload.validate_stmt('grant dba to eygle'); END;

*
ERROR at line 1:
ORA-06510: PL/SQL: unhandled user-defined exception
ORA-06512: at "CTXSYS.DRILOAD", line 42
ORA-01003: no statement parsed
ORA-06512: at line 1

SQL> select grantee,table_name from dba_tab_privs where table_name='DRILOAD';

GRANTEE                        TABLE_NAME
------------------------------ ------------------------------
PUBLIC                         DRILOAD

SQL> select grantee,table_name,PRIVILEGE from dba_tab_privs where table_name='DRILOAD';

GRANTEE                        TABLE_NAME                     PRIVILEGE
------------------------------ ------------------------------ ----------
PUBLIC                         DRILOAD                        EXECUTE
```

软件安全-安全补丁和组件安全

- Oracle 10g Exploit

```
SQL> @run.sql

Package created.


Package body created.


PL/SQL procedure successfully completed.

SQL> select * from user_role_privs;

USERNAME                       GRANTED_ROLE                   ADM DEF OS_
------------------------------ ------------------------------ --- --- ---
SCOTT                          CONNECT                        NO  YES NO
SCOTT                          DBA                            NO  YES NO
SCOTT                          RESOURCE                       NO  YES NO
```

YUNHE

软件安全-行业案例及软件BUG

Bug 8198906 OERI [kddummy_blkchk] / OERI [5467] for an aborted transaction of allocating extents

This note gives a brief overview of bug 8198906.
The content was last updated on: 19-JAN-2011
Click here for details of each of the sections below.
This bug is alerted in Note:1229669.1

Affects:

Product (*Component*)	Oracle Server (Rdbms)
Range of versions *believed* to be affected	Versions >= 9.2 but BELOW 11.2
Versions *confirmed* as being affected	• 10.2.0.4 • 10.2.0.3 • 9.2.0.8 • 9.2.0.6
Platforms affected	Generic (all / most platforms affected)

Note that this fix can cause / expose the problem described in Bug:9711859

Note that this fix has been superceded **by the fix in** Bug:9711859

Fixed:

This issue is fixed in	• 11.2.0.1 (Base Release) • 10.2.0.5 (Server Patch Set) • 10.2.0.4 Patch 22 on Windows Platforms

YUNHE

备份安全-备份重于一切

[数据恢复]刚刚接到老杨电话，又有一个客户的数据库无法启动，错误的删除文件、试错性的恢复尝试，最终导致数据库无法启动，bootstrap失败，一系列的600错误。看来有很多数据库挺不过这新年的最后一天。

+加标签

2011-12-31 13:13　来自新浪微博　　转发(12) | 收藏 | 评论(15)

延长闪回时间（Undo_Retention）

[数据恢复]今天又接到两起数据恢复请求，一则使用DBCA建库时覆盖了原有的数据库；一则仍然是误删除了一些数据文件。这可真是2011年的最后一天了，坚强的数据库们要值好最后一天岗了！

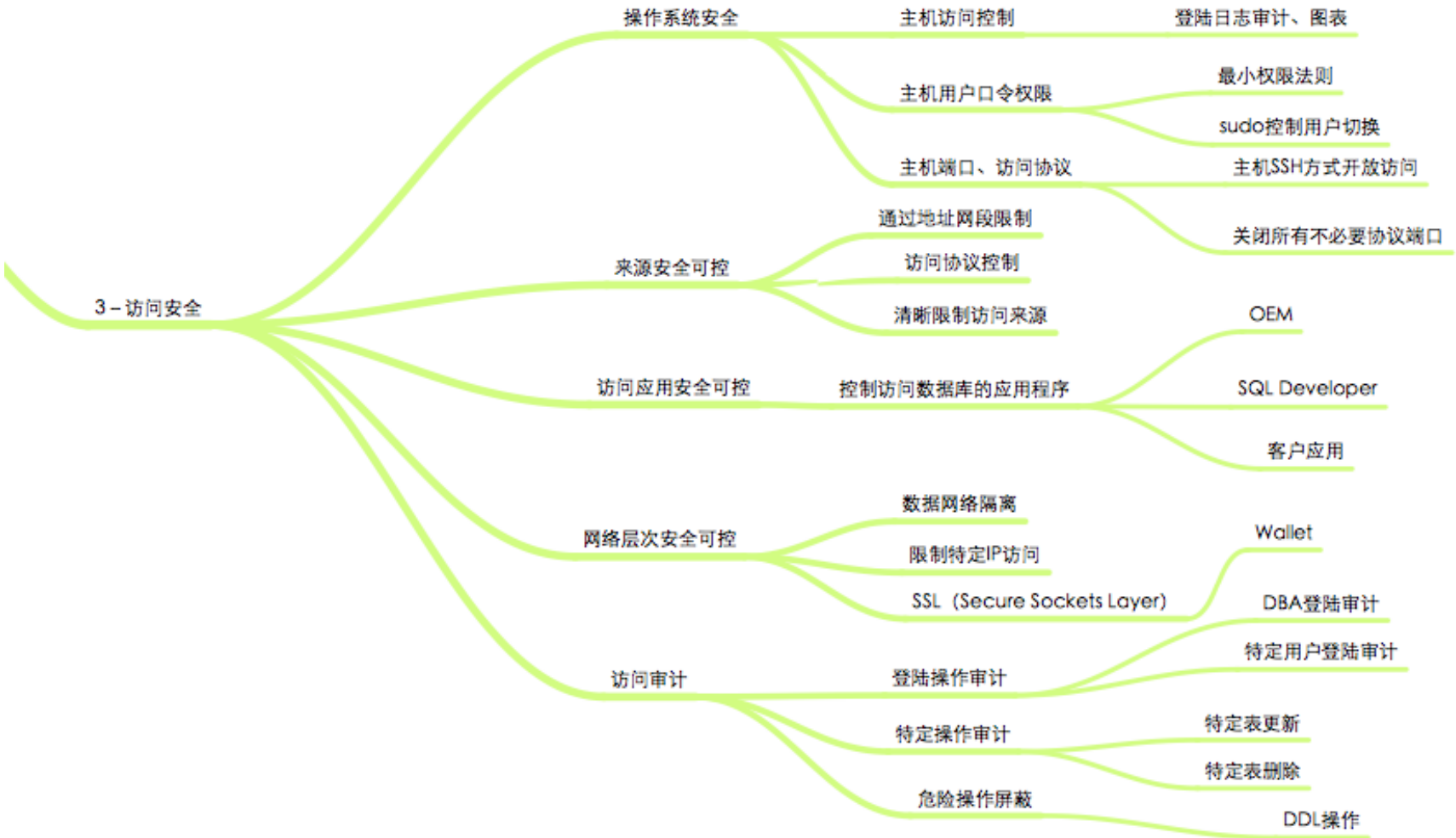
+加标签

2011-12-31 01:09　来自新浪微博　　转发(1) | 收藏 | 评论(11)

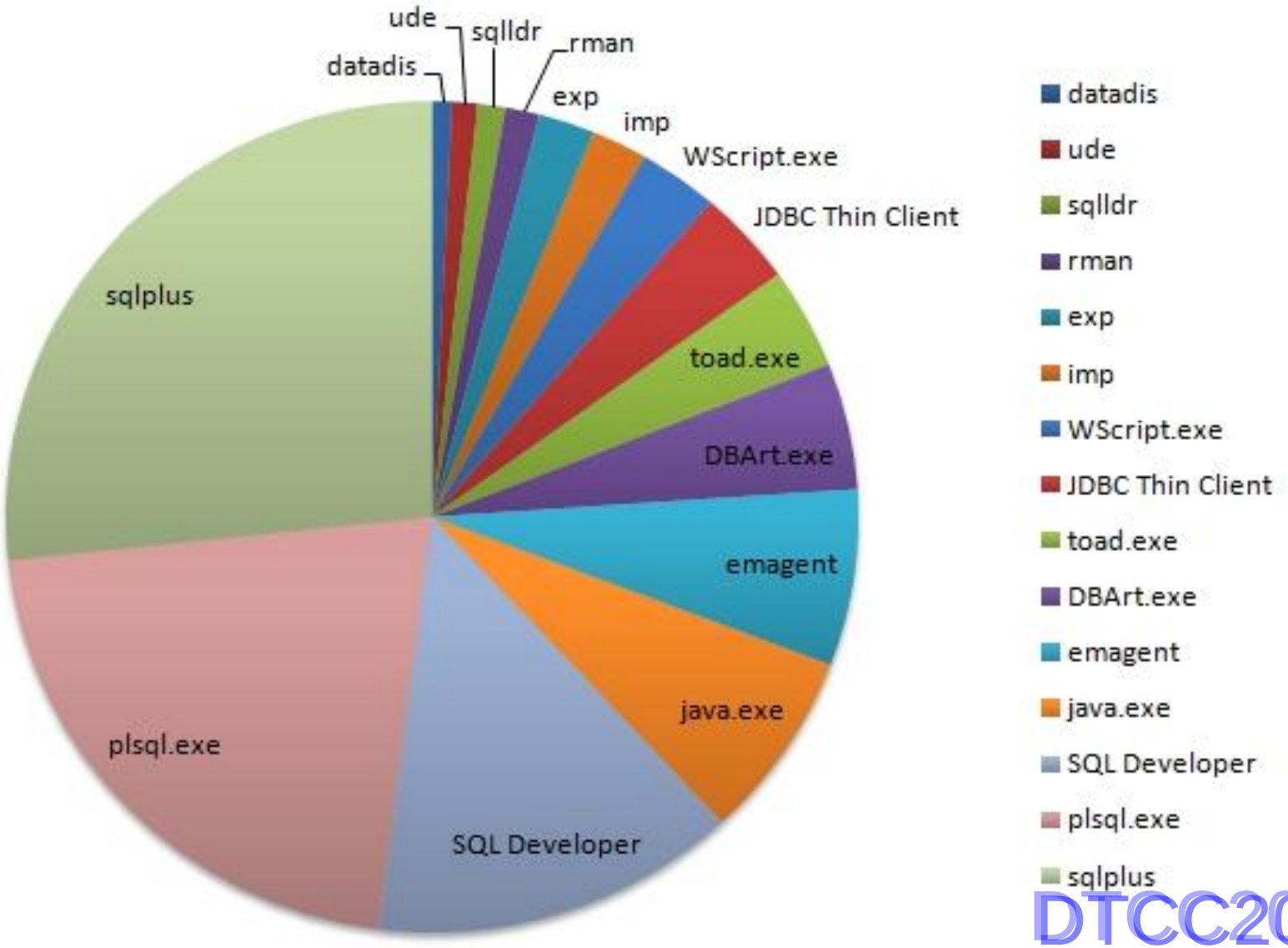
数据变更追溯

YUNHE

访问安全-4W1H



访问安全-明确访问来源



YUNHE

防护安全-从零开始

口令的加密内容存储在底层的核心表（USERS是 Oracle 数据库的元数据表之一）中，以下 PASSWORD 字段存储的是 DES 加密值，SPARE4 存储的是 SHA-1 加密串：

```
SQL> select * from v$version where rownum <2;

BANNER
--------------------------------------------------------------------------------
Oracle Database 11g Enterprise Edition Release 11.2.0.3.0 - 64bit Production

SQL> select name,password,spare4 from user$
  2  where name in ('SYS','SYSTEM','EYGLE');

NAME       PASSWORD         SPARE4
---------- ---------------- ----------------------------------------------------
SYS        8A8F025737A9097A S:BBEFCBB86319E6A40372B9584DBCCA6B015BFE0C7DDF5B9593FB618E0D80
SYSTEM     2D594E86F93B17A1 S:C576FB5A54D009440AC047827392215C673528067BC06659EC56E3178BAB
EYGLE      B726E09FE21F8E83 S:65857F36842AEE4470828E9BE630FEED90A67CEF0D2B40C9FE9B558F6B49
```

重视安全问题，是安全增强的第一要义！

触发器

YUNHE

防护安全-提升请从今日始

Oracle Database 11g

Data Masking

TDE Tablespace Encryption

Oracle Total Recall

Oracle Audit Vault

Oracle Database 10g

Oracle Database Vault

Transparent Data Encryption (TDE)

Real Time Masking

Oracle Database 9i

Secure Config Scanning

Fine Grained Auditing

Oracle Label Security

Enterprise User Security

Oracle8i

Virtual Private Database (VPD)

Database Encryption API

Strong Authentication

Oracle7

Native Network Encryption

Database Auditing

Government customer

DTCC2012

YUNHE

管理安全-主要威胁来自内部

YUNHE

Recovery Case Study

- 10046事件、sql_trace、DTrace
  - DBMS_SYSTEM / DBMS_MONITOR
  - alter session set events ‘10046 trace name context forever,level 12’;
- 控制文件与文件头的转储与分析
  - alter session set events ‘immediate trace name controlf ,level 12’;
  - alter session set events ‘immediate trace name file_hdrs,level 12’;
  - systemstate 的转储与分析

What’s Oracle RBA

- RBA – Redo Byte Address
  - Log File Sequence Number (4 Bytes)
  - Log File Block Number (4 Bytes)
  - Redo Record Start Offset (2 Bytes)

	RBA信息	Log Sequence	Blcok Number
Low Cache RBA	0x27.6c.0	0x27 = 39	6c=108
On Disk RBA	0x27.f9.0	0x27=39	F9=249

  - 参考链接
  - http://www.eygle.com/archives/2011/02/cache_low_rba.html

YUNHE

Controlfile inconsistent

- 断电后导致控制文件不一致

```
SQL> startup pfile=initora9i.ora
ORACLE instance started.

Total System Global Area  126950956 bytes
Fixed Size                   454188 bytes
Variable Size              92274688 bytes
Database Buffers           33554432 bytes
Redo Buffers                 667648 bytes
ORA-00214: controlfile 'D:\ORACLE\ORADATA\SXXHDTS\CONTROL03.CTL' version 2623
inconsistent with file 'D:\ORACLE\ORADATA\SXXHDTS\CONTROL02.CTL' version 2619
```

How to verify controlfile?

- 控制文件的一致性判断

```
=====================
PARSING IN CURSOR #1 len=20 dep=0 uid=0 oct=35 lid=0 tim=12378053544 hv=1379354989 ad='6a3c8d64'
alter database mount
END OF STMT
PARSE #1:c=0,e=3026,p=0,cr=0,cu=0,mis=1,r=0,dep=0,og=4,tim=12378053538
BINDS #1:
WAIT #1: nam='reliable message' ela= 27 p1=1760935332 p2=1760905580 p3=1761534860
WAIT #1: nam='rdbms ipc reply' ela= 2724 p1=5 p2=900 p3=0
WAIT #1: nam='control file sequential read' ela= 254 p1=0 p2=1 p3=1
WAIT #1: nam='control file sequential read' ela= 219 p1=1 p2=1 p3=1
WAIT #1: nam='control file sequential read' ela= 208 p1=2 p2=1 p3=1
WAIT #1: nam='reliable message' ela= 996893 p1=1760935332 p2=1760905876 p3=1761534860
WAIT #1: nam='reliable message' ela= 999155 p1=1760935332 p2=1760905876 p3=1761534860
WAIT #1: nam='reliable message' ela= 990131 p1=1760935332 p2=1760905876 p3=1761534860
EXEC #1:c=0,e=3010793,p=0,cr=0,cu=0,mis=0,r=0,dep=0,og=4,tim=12381070548
ERROR #1:err=214 tim=1237671
WAIT #1: nam='SQL*Net break/reset to client' ela= 5 p1=1111838976 p2=1 p3=0
WAIT #1: nam='SQL*Net break/reset to client' ela= 83 p1=1111838976 p2=0 p3=0
WAIT #1: nam='SQL*Net message to client' ela= 6 p1=1111838976 p2=1 p3=0
```

How to verify controlfile?

- 控制文件的一致性判断

```
*** 2012-01-10 11:13:27.919
*** SESSION ID:(9.3) 2012-01-10 11:13:27.868
DUMP OF CONTROL FILES, Seq # 2626 = 0xa42
 FILE HEADER:
    Software vsn=153092096=0x9200000, Compatibility Vsn=134217728=0x8000000
    Db ID=615401347=0x24ae4783, Db Name='SXXHDTS'
    Activation ID=0=0x0
    Control Seq=2626=0xa42, File size=246=0xf6
    File Number=0, Blksiz=8192, File Type=1 CONTROL
```

File to recovery

- 数据文件恢复提示

```
SQL> startup pfile=initora9i.ora
ORACLE instance started.

Total System Global Area  126950956 bytes
Fixed Size                   454188 bytes
Variable Size              92274688 bytes
Database Buffers           33554432 bytes
Redo Buffers                 667648 bytes
Database mounted.
ORA-01113: file 2 needs media recovery
ORA-01110: data file 2: 'D:\ORACLE\ORADATA\SXXHDTS\UNDOTBS01.DBF'
```

YUNHE

Why Undo tablespace?

- 通过跟踪获进行深入探索

```
SQL> alter session set events '10046 trace name context forever,level 12';

Session altered.

SQL> alter database open;
alter database open
*
ERROR at line 1:
ORA-01113: file 2 needs media recovery
ORA-01110: data file 2: 'D:\ORACLE\ORADATA\SXXHDTS\UNDOTBS01.DBF'
'
```

Why Undo tablespace?

- UNDO的恢复判断

```
=====================
PARSING IN CURSOR #1 len=19 dep=0 uid=0 oct=35 lid=0 tim=7129363012 hv=2631704207 ad='6a3c6d48'
alter database open
END OF STMT
PARSE #1:c=0,e=205,p=0,cr=0,cu=0,mis=1,r=0,dep=0,og=4,tim=7129363006
BINDS #1:
WAIT #1: nam='control file sequential read' ela= 745 p1=0 p2=1 p3=1
WAIT #1: nam='control file sequential read' ela= 148 p1=1 p2=1 p3=1
WAIT #1: nam='control file sequential read' ela= 142 p1=2 p2=1 p3=1
WAIT #1: nam='control file sequential read' ela= 144 p1=0 p2=239 p3=1
WAIT #1: nam='control file sequential read' ela= 147 p1=0 p2=1 p3=1
WAIT #1: nam='control file sequential read' ela= 155 p1=1 p2=1 p3=1
WAIT #1: nam='control file sequential read' ela= 144 p1=2 p2=1 p3=1
WAIT #1: nam='control file sequential read' ela= 144 p1=0 p2=239 p3=1
WAIT #1: nam='rdbms ipc reply' ela= 90731 p1=3 p2=910 p3=0
WAIT #1: nam='control file sequential read' ela= 188 p1=0 p2=1 p3=1
WAIT #1: nam='control file sequential read' ela= 147 p1=1 p2=1 p3=1
WAIT #1: nam='control file sequential read' ela= 144 p1=2 p2=1 p3=1
WAIT #1: nam='control file sequential read' ela= 141 p1=0 p2=239 p3=1
WAIT #1: nam='control file sequential read' ela= 158 p1=0 p2=12 p3=1
```

Why Undo tablespace?

- UNDO的恢复判断
  - Direct Path read Datafile header

```
WAIT #1: nam='direct path read' ela= 23 p1=1 p2=1 p3=1
WAIT #1: nam='direct path read' ela= 4 p1=2 p2=1 p3=1
WAIT #1: nam='direct path read' ela= 5 p1=3 p2=1 p3=1
WAIT #1: nam='direct path read' ela= 4 p1=4 p2=1 p3=1
WAIT #1: nam='direct path read' ela= 4 p1=5 p2=1 p3=1
WAIT #1: nam='direct path read' ela= 4 p1=6 p2=1 p3=1
WAIT #1: nam='direct path read' ela= 5 p1=7 p2=1 p3=1
WAIT #1: nam='direct path read' ela= 4 p1=8 p2=1 p3=1
WAIT #1: nam='direct path read' ela= 7 p1=9 p2=1 p3=1
WAIT #1: nam='direct path read' ela= 4 p1=10 p2=1 p3=1
WAIT #1: nam='direct path read' ela= 4 p1=201 p2=1 p3=1
WAIT #1: nam='rdbms ipc reply' ela= 171 p1=3 p2=2147483647 p3=0
EXEC #1:c=10014,e=101420,p=11,cr=0,cu=0,mis=0,r=0,dep=0,og=4,tim=7129464473
```

Why Undo tablespace?

- UNDO的恢复判断
  - Checkpoint SCN / RBA

```
*********************************************************************
REDO THREAD RECORDS
*********************************************************************
 (blkno = 0x4, size = 104, max = 1, in-use = 1, last-recid= 0)
THREAD #1 - status:0xf thread links forward:0 back:0
 #logs:3 first:1 last:3 current:1 last used seq#:0x13d
 enabled at scn: 0x0000.0002e872 06/12/2011 18:30:27
 disabled at scn: 0x0000.00000000 01/01/1988 00:00:00
 opened at 12/31/2011 08:28:19 by instance sxxhdts
Checkpointed at scn:  0x0000.0155b0f1 12/31/2011 08:28:19
 thread:1 rba:(0x13d.2.10)
 enabled  threads:  01000000 00000000 00000000 00000000 00000000 00000000
  00000000 00000000
 log history: 316
```

YUNHE

Why Undo tablespace?

```
FILE HEADER:
    Software vsn=153092096=0x9200000, Compatibility Vsn=134217728=0x8000000
    Db ID=615401347=0x24ae4783, Db Name='SXXHDTS'
    Activation ID=0=0x0
    Control Seq=2618=0xa3a, File size=25600=0x6400
    File Number=2, Blksiz=8192, File Type=3 DATA
FILE HEADER:
    Software vsn=153092096=0x9200000, Compatibility Vsn=134217728=0x8000000
    Db ID=615401347=0x24ae4783, Db Name='SXXHDTS'
    Activation ID=0=0x0
    Control Seq=2624=0xa40, File size=52480=0xcd00
    File Number=1, Blksiz=8192, File Type=3 DATA
Tablespace #0 - SYSTEM  rel_fn:1
Creation   at   scn: 0x0000.0000000b 05/12/2002 16:17:58
Backup taken at scn: 0x0000.00000000 01/01/1988 00:00:00 thread:0
 reset logs count:0x2cebbf43 scn: 0x0000.0002e872 recovered at 12/31/2011 17:47:30
 status:0x4 root dba:0x004001a1 chkpt cnt: 942 ctl cnt:941
begin-hot-backup file size: 0
Checkpointed at scn:  0x0000.0156eaa8 12/31/2011 17:47:31
 thread:1 rba:(0x13e.2.10)
 enabled  threads:  01000000 00000000 00000000 00000000 00000000 00000000
  00000000 00000000
```

DTCC2012

YUNHE

ORA-600 2758

- What is mean ORA-600 2758?

```
SQL> recover datafile 2;
Media recovery complete.

SQL> alter database open;
alter database open
*
ERROR at line 1:
ORA-00600: internal error code, arguments: [2758], [1], [4294967295], [204800],[10], [], [], []
```

```
SQL> select power(2,32) -1 from dual;

POWER(2,32)-1
-------------
   4294967295
```

DTCC2012

Why Ora-00600 ?

- Checkpoint SCN & RBA

```
*********************************************************************
CHECKPOINT PROGRESS RECORDS
*********************************************************************
 (blkno = 0x4, size = 104, max = 1, in-use = 1, last-recid= 0)
THREAD #1 - status:0x1 flags:0x0 dirty:0
low cache rba:(0xffffffff.ffffffff.ffff) on disk rba:(0x13d.ac56.0)
on disk scn: 0x0000.01569c86 12/31/2011 17:45:38
resetlogs scn: 0x0000.0002e872 06/12/2011 18:30:27
heartbeat: 772188978 mount id: 633905756
MTTR statistics status: 3
Init time: Avg: 9938392, Times measured: 3
File open time: Avg: 12349, Times measured: 39
Log block read time: Avg: 24, Times measured: 32770
Data block handling time: Avg: 2067, Times measured: 301
```

Why Ora-00600 ?

- After Undo Recovery

```
WAIT #1: nam='db file sequential read' ela= 166 p1=2 p2=1 p3=1
 FILE HEADER:
    Software vsn=153092096=0x9200000, Compatibility Vsn=134217728=0x8000000
    Db ID=615401347=0x24ae4783, Db Name='SXXHDTS'
    Activation ID=0=0x0
    Control Seq=2625=0xa41, File size=25600=0x6400
    File Number=2, Blksiz=8192, File Type=3 DATA
Tablespace #1 - UNDOTBS1  rel_fn:2
Creation   at   scn: 0x0000.0002dd31 05/12/2002 20:22:54
Backup taken at scn: 0x0000.00000000 01/01/1988 00:00:00 thread:0
 reset logs count:0x2cebbf43 scn: 0x0000.0002e872 recovered at 01/10/2012 13:35:35
 status:0x0 root dba:0x00000000 chkpt cnt: 930 ctl cnt:929
begin-hot-backup file size: 0
Checkpointed at scn:  0x0000.01569c86 12/31/2011 17:45:38
 thread:1 rba:(0x13d.ac56.0)
```

Why Ora-00600 ?

- Checkpoint RBA Wrong

```
*******************************************************************************
REDO THREAD RECORDS
*******************************************************************************
 (blkno = 0x4, size = 104, max = 1, in-use = 1, last-recid= 0)
THREAD #1 - status:0xf thread links forward:0 back:0
 #logs:3 first:1 last:3 current:1 last used seq#:0x13d
 enabled at scn: 0x0000.0002e872 06/12/2011 18:30:27
 disabled at scn: 0x0000.00000000 01/01/1988 00:00:00
 opened at 01/10/2012 13:41:37 by instance ora9i
Checkpointed at scn:  0x0000.0156eaa9 01/10/2012 13:41:37
 thread:1 rba:(0x13d.ffffffff.10)
 enabled  threads:  01000000 00000000 00000000 00000000 00000000 00000000
  00000000 00000000
 log history: 316
```

Why Ora-00600 ?

- Tablespace Checkpoint Wrong

```
Tablespace #0 - SYSTEM  rel_fn:1
Creation   at   scn: 0x0000.0000000b 05/12/2002 16:17:58
Backup taken at scn: 0x0000.00000000 01/01/1988 00:00:00 thread:0
 reset logs count:0x2cebbf43 scn: 0x0000.0002e872 recovered at 12/31/2011 17:47:30
 status:0x4 root dba:0x004001a1 chkpt cnt: 943 ctl cnt:941
begin-hot-backup file size: 0
Checkpointed at scn:  0x0000.0156eaa9 01/10/2012 13:41:37
 thread:1 rba:(0x13d.ffffffff.10)
 enabled  threads:  01000000 00000000 00000000 00000000 00000000 00000000
  00000000 00000000
Backup Checkpointed at scn:  0x0000.00000000
 thread:0 rba:(0x0.0.0)
 enabled  threads:  00000000 00000000 00000000 00000000 00000000 00000000
  00000000 00000000
```

YUNHE

Where RBA Ended?

```
SQL> alter system dump logfile 'c:\redo01.log' rba min 317 . 44117 ;

System altered.

DUMP OF REDO FROM FILE 'c:\redo01.log'
 Opcodes *.*
 DBA's: (file # 0, block # 0) thru (file # 65534, block # 4194303)
 RBA's: 0x00013d.0000ac55.0000 thru 0xffffffff.ffffffff.ffff
 SCN's scn: 0x0000.00000000 thru scn: 0xffff.ffffffff
 Times: creation thru eternity
 FILE HEADER:
    Software vsn=153092096=0x9200000, Compatibility Vsn=153092096=0x9200000
    Db ID=615401347=0x24ae4783, Db Name='SXXHDTS'
    Activation ID=615377539=0x24adea83
    Control Seq=2618=0xa3a, File size=204800=0x32000
    File Number=1, Blksiz=512, File Type=2 LOG

REDO RECORD - Thread:1 RBA: 0x00013d.0000ac55.0090 LEN: 0x0054 VLD: 0x01
SCN: 0x0000.01569c85 SUBSCN:  1 12/31/2011 17:45:38
CHANGE #1 TYP:0 CLS:17 AFN:2 DBA:0x00800009 SCN:0x0000.01569c84 SEQ:  1 OP:5.4
ktucm redo: slt: 0x0006 sqn: 0x00004336 srt: 0 sta: 9 flg: 0x2
ktucf redo: uba: 0x00800370.01ef.34 ext: 2 spc: 4390 fbi: 0
END OF REDO DUMP
----- Redo read statistics for thread 1 -----
Read rate (ASYNC): 22058Kb in 0.92s => 22.83 Mb/sec
Longest record: 1Kb, moves: 4/91535 (0%)
Change moves: 31544/212533 (14%), moved: 2Mb
-----------------------------------------------
```

Make RBA Back

- Database can open smoothly

```
SQL> startup nomount pfile=initora9i.ora
ORACLE instance started.

Total System Global Area  126950956 bytes
Fixed Size                   454188 bytes
Variable Size              92274688 bytes
Database Buffers           33554432 bytes
Redo Buffers                 667648 bytes
SQL> alter database mount;

Database altered.

SQL> alter database open;

Database altered.
```

Did you see alert carefully?

- Logseq / block / scn

```
Tue Jan 10 16:01:22 2012
Ended recovery at
 Thread 1: logseq 317, block 44118, scn 0.22493386
 0 data blocks read, 0 data blocks written, 0 redo blocks read
Crash recovery completed successfully
Tue Jan 10 16:01:22 2012
Thread 1 advanced to log sequence 318
Thread 1 opened at log sequence 318
  Current log# 2 seq# 318 mem# 0: D:\ORACLE\ORADATA\SXXHDTS\REDO02.LOG
Successful open of redo thread 1
Tue Jan 10 16:01:22 2012
SMON: enabling cache recovery
Tue Jan 10 16:01:23 2012
Successfully onlined Undo Tablespace 1.
Tue Jan 10 16:01:23 2012
SMON: enabling tx recovery
Tue Jan 10 16:01:23 2012
Database Characterset is ZHS16GBK
```

YUNHE

Q&A

DTCC2012