

Never a DULL Moment

How to Avoid Costly Data Recovery

RMOUG QEW
November 2008

Who am I?

- Daniel Fink
 - Oracle DBA since 1996
 - Diagnosis, Optimization, Data Recovery and Training
 - Member of Oak Table, BAARF and BAAG

www.optimaldba.com

daniel.fink@optimaldba.com

Agenda

- DULs
- Recoveries
- Case Studies
 - Worst Practices
 - Best Practices

Some case studies provided by Kurt Van Meerbeeck (www.ora600.be)

Never a DULL Moment

- DUL - Data UnLoader
 - Extract data from a down database
- Option of last resort
 - Downtime
 - Expensive
 - May or May not work

Why do you need a DUL?

- Seed
 - Incorrect Configurations
 - Poor Policies/Procedures
 - Inflexible Processes
 - Lack of Security
- Trigger
 - Human Error
 - Technology Failure

Bullet Proof Backups

- Simply don't exist
 - There will always be a point of failure
- Keep it simple, but thorough
 - Added complexity = Added risk
 - Change management
- Protect redo
 - Once redo is lost, recovery stops

An Unrecovered Backup

- Is No Backup At ALL!
- Recovery is Job One
 - "Contrary to common opinion, a DBA does not have a responsibility to back up a database. The DBA's real responsibility is to be able to *recover* the database."
 - Essential Oracle8i Data Warehousing (Dodge/Gorman)
 - "The actual responsibility is to restore or recover the database to the point in time and within the downtime window determined by the business needs."
 - Real Life Recovery (RMOUG Training Days 1999)

Audience Participation

- Today
 - Did you check your backup log?
- This Week/Month
 - Did you check the backup process?
 - Did you recover a backup?
- Ever
 - Did you check your backup log?
 - Did you recover a backup?

Best Core Practices

- Find Recovery Opportunities
 - Environment Refreshes
 - Upgrade/Patch Testing
 - Disaster Recovery Training
- Every single case study presented would have been avoided if they had tested recovery

Best Core Practices

- You have known, good processes
 - This does not mean every backup is good
 - Always test after any changes
- You have documented the processes
 - Help when thinking is not clear

Best Core Practices

- Prevention
 - Audits
 - Implementation Checklists
- Find Opportunities to Recover
 - Refreshes
 - DBA sandboxes

Case Studies

- Situation
 - Summary of the issue
- Seed
 - A condition that is present
- Trigger
 - An event that causes the failure
- Red Flag
 - A "*recognized*" indication of a future problem

“Hot” Backups

- Files were not being properly backed up
- Seed
 - DBA did not understand how files were managed
 - Backup the files without putting them into backup mode
- Trigger
 - Media failure
- Red Flag
 - Lack of desire to learn

Best Practice

- Basic Oracle, Backup and Recovery knowledge
 - Oracle Documentation
 - DBA Training
- Good backup process

No Backup

- No backup for production
- Seed
 - Backups not set up
- Trigger
 - Media failure
- Red Flag
 - Production use of a database without backup

Best Practice

- Backups are part of the implementation check off/hand over
- Test Recovery before implementation

A backup that may work

- Backup set does not encapsulate full recovery set
- Seed
 - Custom script does not include all commands within backup set
- Trigger
 - Fraud investigation
- Red Flag
 - Custom hot backup script command sequence incorrect

Best Practice

- Custom scripts require complete knowledge
 - Full backup set
 - Command sequence
- Every backup set should be self-contained
- Can you backup your worst-case recovery scenario?

Known Bad Backup

- Archived redo logs were known to be corrupt
- Seed
 - Bug in Oracle caused corrupt archived redo logs
 - Application owner "could not afford downtime to fix"
- Trigger
 - Rollback segment tablespace went offline
 - Monitoring software failed
- Red Flag
 - Backups known to be unrecoverable

Best Practice

- Be careful of complicated application architectures
- Have the political will to do the right thing
- Find an interim solution

User not in the Specs

- User level export as only backup
- Seed
 - User added to database, but not script
- Trigger
 - Media failure
- Red Flag
 - Static scripts
 - Development responsible for backups

Best Practice

- If you are responsible for the database, for recovery of the database...you are responsible for the backup!
 - Export can only restore a database, not perform full recovery
- Audit
 - schema owners v. users being backed up

You are...the weakest link

- Improper tape management
- Seed
 - Unskilled, unmotivated operations personnel
- Trigger
 - Anything...
- Red Flag
 - Non-technical personnel in charge of tape management

Best Practice

- If you are responsible for the database, for recovery of the database...you are responsible for the backup!
- You have to trust those responsible for operations

We can just Reload

- Data warehouse recovery strategy was to reload
- Seed
 - Database grew, but backup strategy did not
- Trigger
 - Current redo log corruption
- Red Flag
 - Backup strategy not revisited as database grew

Best Practice

- Periodically revisit non-standard backup strategies
- Better yet...avoid non-standard backup strategies

We don't need no stinkin' SYSTEM tablespace

- Default installation on local drive with additional datafiles on external drives
- Seed
 - Single database has files on separate storage systems
- Trigger
 - Media Failure
- Red Flag
 - Never checking backup process

Best Practice

- Properly plan and install databases
- Verify that all needed parts of the database are being backed up
 - Without `SYSTEM` tablespace, you lose the 'map' to tables...and data
 - Know what is and is not needed

Security

- Table is dropped in production
- Seed
 - Improper security
 - Invalid Backups
- Trigger
 - Wrong environment
 - Wrong action
- Red Flag
 - Access to production

Best Practice

- **Appropriate Architecture and Policies**
 - Schema owner logins
 - Non-database tier authentication
- **Security Audits**
 - Know who has what and why
 - Balance safety v. security

It's Hammer Time!

- Disks failed and user level export was incomplete
- Seed
 - Known bad hardware
 - Exports not dynamic
- Trigger
 - Disk crash...finally
- Red Flag
 - A hammer attached to a storage device is rarely a good sign

Best Practice

- DON'T USE A HAMMER!!!!
- Use dynamic scripting techniques
 - Backups
 - Exports
- Validate scripting

SOX and Recoveries

- 7 years of data
- Could you recover a 7 year old backup?
 - 2001 - Oracle 9i introduced
 - Most systems 7.3 and 8.x
 - Do you have a 7.3 install?
- Do you have 7 year old
 - Hardware?
 - O/S and drivers?

How to avoid calling me...

- Backups are part of any installation
 - Test recovery before turning over to user/developer
 - Document the process
 - Understand the implications of changes
 - Adapt the strategy to the system
- Monitor backups on a daily basis
 - Exception reporting is good, but not perfect
 - Know what to do if a backup fails

- The only good recovery is a successful recovery
 - Determine likely, unlikely and worst-case scenarios
 - Look for opportunities to perform recoveries
 - Understand the implications of changes
 - Don't uncover issues on production systems

- **Audit security**
 - Know who can access production and how
 - Establish policies and procedures to minimize risk
- **Annual Reviews**

Go Forth
and
Recover!