Oracle TDE for large databases

Oracle OpenWorld – October 2017
CCC Information Services

Steve Young – DBA Manager  syoung1@cccis.com
Fei Dong – Sr. Oracle DBA  fdong@cccis.com
Steve Rosenblum – Sr. Oracle DBA  srosenblum@cccis.com
**Auto Physical Damage**

- 12M claims per year in US
- 18 of top 25 carriers
- Statistically significant data for 97% U.S. CBSAs
- 125M photos/year
- ~150M historical claims
- $500B in historical claim data
- 16,000+ staff appraiser
- Industry's ONLY Fully-integrated, cloud-based platform

**Auto Casualty**

- Injury Sciences and AIS Acquisitions
- 25+ years of scientific data
- Science and medical based EXPERTISE
- Review 24,000 repair facilities
- $10B in medicals annually
- Manage 80M pages of documents annually
- 17 of top 25 carriers
- 125M historical claims
- 80M pages of documents annually
Implementing Oracle TDE at CCC

Business Case for Encryption

- No ‘regulated data’ stored in our databases
- Didn’t need to comply with regulations
- Provide customers piece of mind that their data is protected
- Address the potential reputational risk of loss of data
- CCC Business decision in 2015:
  Encrypt ALL customer data by Q3/2017
Implementing Oracle TDE at CCC

CCC DataCenter Topography

Primary Datacenter
- Exadata RAC
- Linux RAC
- Legacy Solaris
- 80% Prod
- 20% Non-Prod

Remote Datacenter
- Exadata RAC
- Linux RAC
- Legacy Solaris
- 80% Non-Prod
- 20% D/R
- Load Testing

Hosted Datacenter
- 2-3 key applications
- Linux RAC
- Prod databases
- Non-Prod
- D/R

Cloud Services
- Primarily Non-Prod
- 24 Pre-Prod DBs
- Soon to be Prod
- EC2 – Oracle
- RDS – SQL Server/ Aurora
Our IT Shop

- Java / Oracle
- 24 x 7 operations
- Oracle Linux, RAC
- Exadata environment:
  - Full Exadata rack, high capacity disk
  - X5 Production, X3 Active Standby, X2 D/R
  - Heavily partitioned, large databases (120TB)
  - Limited to 11g R2 due to legacy application compatibility
Our Challenges

- 24/7 environment
- Busy application release schedule
- Complicated enterprise architecture:
  - Consolidated databases with multiple applications
  - Multiple interacting databases
  - Coordination difficulty
- Disk space constraints
- Can only run production on standby database for limited time
Our Approach to Data Encryption

- **Exadata databases:** encrypt using Oracle TDE
- **Non-Exadata databases:** encrypted via SAN solution
TDE Options Considered

Oracle OpenWorld October 2017
Implementing Oracle TDE at CCC

Options for Implementing TDE

Option 1 - Create new encrypted tablespaces

• Move all objects to encrypted tablespaces during maintenance windows

• Create future partitions in encrypted tablespaces
### Implementing Oracle TDE at CCC

#### Option 1 – Create new encrypted tablespaces

<table>
<thead>
<tr>
<th>PROS</th>
<th>CONS</th>
</tr>
</thead>
<tbody>
<tr>
<td>• Standard Methodology/simple steps</td>
<td>• Time consuming &amp; tedious</td>
</tr>
<tr>
<td>• Leverage online redefinition to reduce downtime</td>
<td>• Operational investment depending on targeted objects</td>
</tr>
<tr>
<td></td>
<td>• Some complex objects cannot use alter/move</td>
</tr>
<tr>
<td></td>
<td>• Requires additional space for online redefinition</td>
</tr>
<tr>
<td></td>
<td>• Requires several downtime windows</td>
</tr>
</tbody>
</table>
Options for Implementing TDE

Option 2 - Logical Standby

• Create all table spaces encrypted on standby
• Move all objects to standby database, switchover, rebuild old primary database as new standby
## Option 2 - Logical Standby

<table>
<thead>
<tr>
<th>PROS</th>
<th>CONS</th>
</tr>
</thead>
<tbody>
<tr>
<td>• Minimizes database downtime / unavailability</td>
<td>• Complicated for complex, large databases</td>
</tr>
<tr>
<td></td>
<td>• Additional disk space required</td>
</tr>
</tbody>
</table>
Options for Implementing TDE

**Option 3 – Off-line datafile conversion**

- Need to take an outage!
- New feature for version 11.2.0.4+ & 12.1.0.2+
- Can be done while database is open or mounted
Option 3 - *Off-line datafile conversion*

<table>
<thead>
<tr>
<th>PROS</th>
<th>CONS</th>
</tr>
</thead>
<tbody>
<tr>
<td>• Fast and relatively simple</td>
<td>• Requires application downtime</td>
</tr>
<tr>
<td></td>
<td>• Performance impact</td>
</tr>
</tbody>
</table>
Options for Implementing TDE

**Option 4 – fast datafile conversion with DataGuard**

- Requires a physical standby database
- Production workload performance is unaffected
- Minimizes application downtime
Implementing Oracle TDE at CCC

Option 4 – fast datafile conversion with DataGuard

<table>
<thead>
<tr>
<th>PROS</th>
<th>CONS</th>
</tr>
</thead>
<tbody>
<tr>
<td>• Minimizes downtime</td>
<td>• Requires physical standby database</td>
</tr>
<tr>
<td>• Simple, straightforward solution</td>
<td>• Additional disk space required if you don’t already have a standby database</td>
</tr>
<tr>
<td>• Less impact to the production system</td>
<td></td>
</tr>
</tbody>
</table>
# Implementing Oracle TDE at CCC

## Implementation Option Matrix

<table>
<thead>
<tr>
<th>OPTION</th>
<th>PROS</th>
<th>CONS</th>
</tr>
</thead>
</table>
| 1. Create new encrypted tablespaces | • Standard Methodology/simple steps  
• Leverage online redefinition to reduce downtime | • Time consuming & tedious  
• Operational investment depending on targeted objects  
• Some complex objects cannot use alter/move  
• Additional space for online redefinition  
• Requires several downtime windows |
| 2. Logical Standby Database | • Minimizes database downtime/unavailability | • Complicated for complex, large databases  
• Additional disk space required |
| 3. Fast datafile Conversion | • Fast and simple | • Requires application downtime  
• Performance impact |
| 4. Fast Datafile conversion to TDE with DataGuard | • Minimizes downtime  
• Simple, straightforward solution  
• Less impact to the production system | • Requires a physical standby database  
• Additional disk space required if you don’t already have a standby database |
Implementing Oracle TDE at CCC

**CCC Solution:** *Fast datafile conversion with DataGuard*

**Why?**
- Encrypt all data in our databases
- Large databases
- Limited extra storage
- Limited downtime window
- Limited time to run applications on our Standby databases
- Complex application environments: unusual data types, heavily partitioned & highly integrated apps
- Existing DataGuard environment
How we implemented TDE

Oracle OpenWorld October 2017
Implementing Oracle TDE at CCC

**CCC Solution:** *Fast datafile conversion with DataGuard*

**Preparation**
- Consult and review approach with Oracle

- Identify pre-requisites:
  - Existing physical standby per Oracle MAA best practice
  - Patching to enable the new feature – see MOS 2148746.1

- Build TDE key management strategy

- Test & verify assumptions:
  - Encrypt on standby in given timeframes
  - Encrypt partial database --- YES
  - Encrypt partial data file --- YES
Primary Data Center

**X5 Exadata (Primary)**
*Oracle 11.2.0.4*

Data Guard replication

**X3 Exadata (Local Standby)**
*Oracle 11.2.0.4*

Remote Datacenter (Disaster Recovery Site)

**X2 Exadata (Remote Standby)**
*Oracle 11.2.0.4*
Implementing Oracle TDE at CCC

Implementation Approach

- Encrypt standby, perform switchover
  - Stop recovery for standby
  - Convert datafiles - issue encryption command for each datafile
    
    SQL> alter database datafile 'xxxxx' encrypt;

  - Optional: use dbverify to confirm used blocks are encrypted
    Unix>dbverify file='xxxxx' USERID=<user>/<password>

- Resume recovery to sync with primary
- Switchover

- Encrypt (original) primary & switchover
Implementing Oracle TDE at CCC

Performance Considerations

- 3 databases with total size of 140TB
- About 500 datafiles to encrypt
- Strategies to encrypt:
  - Ran multiple encryption threads in parallel
  - Group datafiles threads based on similar sizing
- Encryption time range from 5hr/TB on X2 - to 2.5hr/TB on Exadata X5
Implementing Oracle TDE at CCC

To improve our chances of success...

- Attended Oracle Database 12C Security Workshop
- Created use cases
- Built a test lab
- Lots of testing CCC & Oracle {patches needed to address specific issues}
- Oracle verified assumptions
- Oracle certified the approach
  - Multiple approaches (different methodologies in prod and non-prod)
- Checked Oracle TDE performance patches
- Consulted with other companies about lessons learned
- Held conference calls with Oracle support and TDE development teams
- Researched Oracle TDE whitepapers!
Implementing Oracle TDE at CCC

Lessons Learned

- Encryption keys
  - Make sure you have all the patches needed
  - Backup the keys and don’t delete them!

- Release 12 much easier to implement TDE, but not an option for us

- Performance after encryption – Oracle estimates were accurate

- Build a test lab with multiple clusters; test different scenarios

- Find out what approaches work best for your different objects
Implementing Oracle TDE at CCC

References:

- **Whitepapers:**
  - Transparent Data Encryption (TDE) Frequently Asked Questions
  - Oracle Advanced Security Transparent Data Encryption Best Practices
  - Converting to Transparent Data Encryption with Oracle Data Guard using Fast Offline Conversion

- **Oracle Security Solutions:** Oracle Database 12C Security Workshop
Questions ?
Thanks for Attending!
APPENDIX

Patch level to enable fast datafile conversion for 11.2.0.4 & 12.1.0.2

see MOS 2148746.1