PeteFinnigan.com Limited

Oracle Security Expertise

UKOUG Archive And Purge Special Event, July 15th 2008

Archiving And Purging In A Security Context

By

Pete Finnigan

Written Wednesday, 9th July 2008

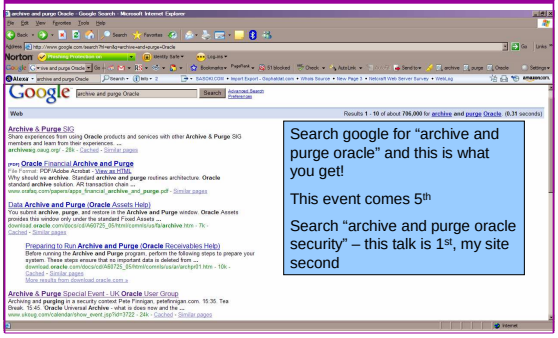
Introduction - Commercial Slide.☹

- PeteFinnigan.com Limited
- Founded February 2003
- CEO Pete Finnigan
- Clients UK, States, Europe
- Specialists in researching and securing Oracle databases providing consultancy and training
- http://www.petefinnigan.com
- Author of Oracle security step-by-step
- Published many papers, regular speaker (UK, USA, Slovenia, Norway, Iceland, more)
- Member of the Oak Table Network

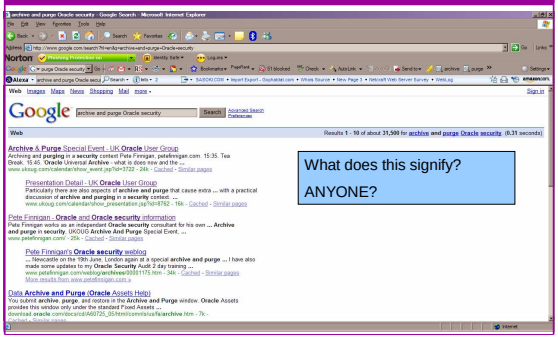
Introduction / Agenda

- We will focus on the database layer not applications
- Not deeply technical..☺
- Also we will focus only on the security aspects of archiving and purging
- Does Oracle provide anything to help?
- Two distinct areas to look at:
  - Archive and purge of security data
  - Security considerations of archive and purge actions, programs and more for business data

The Current State Of Affairs



Security Of Archive And Purge



My Focus

- I am always concerned about the lack of management of log, trace and audit in the database
  - I am seeing recently that this is starting to improve
- Often no audit at DB layer but usually in the application layer
- If there is DB audit usually no plans for:
  - Review, escalation etc
  - Archive and purge often further down the priorities (completely over the horizon...☺)
- In summary
  - If there is audit, its not used, if it is used no thoughts about archive and purge

Security Of Archive And Purge

- Continuing my focus from the last slide
- To be honest a lot of systems I see do not have archive and purge for business data anyway
  - This is one aspect I focus on as part of a security audit
- Those that do have archive and purge generally have not considered the security of the archived data

Awareness

- To summarise I want to raise awareness of two things:
- Often I see lack of security data archiving
- Often I see lack of security of archived data
  - This is often part of a bigger issue of lack of knowledge of exactly where all the data is!
  - e.g. duplication of data, interfaces, de-normalised, indexes….
  - Now also archive data is not protected

Does Oracle Help?

- At a high level and in the database a FIRM NO
- Not obvious to me anyway, anyone know of something I missed?
- The database does not include any archive and purge facilities for security data such as trace, logs and audit
- There is nothing built in but some Oracle APPS documents suggest a 90 day cycle for archive and purge of database audit trails
- More in a minute!

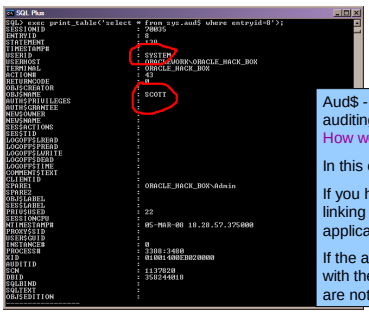
A Contrast

- In general there is coverage at the applications layer
  - Oracle E-Business Suite has standard concurrent processes for instance
  - Commercial products are available, e.g. Applimation – also represented at this conference
  - Other ERP systems have facilities or rely on commercial products to provide the facilities
- Whilst commercial products could be used to archive security data held in the database its not that simple – anyone why?
- Also in general the manufacturers don't support the security side well but they do support the business side

Tools For Purge And Archive

- A look on the net doesn't reveal any specific tools for archive and purge of database audit trails
- There are tools for Oracle Apps, there is a good overview here - http://beginapps.blogspot.com/2008/04/in-oracle-applications-auditing-can-be.html
- Note that purge of AUD$ and RLA for instance have to be done by hand
- If not running APPS we are no further forward
- Look at delete_catalog_role role!

Issue? - Dump Of SYS.AUD$



Aud$ - if user changes, does auditing change meaning? – How would it change?

In this case no change, BUT

If you have who/when audit linking to database userid or application userid it could

If the audit has a disconnect with the database the links are not maintained

Something From Oracle?

Permission to delete from the dictionary

Why is audit data in the dictionary anyway?

No programs to size, purge, manage, reload, in fact defaults are not well sized….

```
SQL Pl
find_al
Copyright (c) 2004 PeteFinnigan.com Limited. All rights reserved.

NAME OF USER TO CHECK                [ORCL]: DELETE_CATALOG_ROLE
OUTPUT METHOD Screen/File               [S]: S
FILE NAME FOR OUTPUT                [priv.lst]:
OUTPUT DIRECTORY [DIRECTORY  or file (/tmp)]:

User => DELETE_CATALOG_ROLE has been granted the following privileges
================================================================
       TABLE PRIV => DELETE object => SYS.AUD$ grantable => NO
       TABLE PRIV => DELETE object => SYS.FGA_LOG$ grantable => NO

PL/SQL procedure successfully completed.

For updates please visit http://www.petefinnigan.com/tools.htm

SQL>
```


Audit Vault And More

- Audit Vault is not going to be discussed here in detail except to mention that it is an audit repository and does in effect archive audit data from the database but in semi-real time
- There are many commercial audit, virtual patch, IDS, IPS such as Hedgehog from Sentrigo that also in effect archive audit data from the production database
- Products such as Applimation may be useful but there is an application level focus
- Interestingly Audit Vault provides a mechanism to archive and purge the audit trail of vault itself

Regulatory Issues

- There are growing requirements for audit and access data to be saved for periods of years
  - I have experience of this on a number of projects
  - There is a multi-layer issue; the need to save audit data for future regulatory issues: the need to prevent abuse – ***They intertwine but are not the same issue***
- PCI DSS 1.1 calls for review of existing archive and purge policies – see http://www.integrigy.com/security-resources/whitepapers/Integrigy_Oracle_Apps_PCI_Compliance.pdf for example
- Another good example is HIPAA that mandates the audit of any one who views confidential patient data. This must be kept for 7 years
- Both have to be archived in other words

Background Sense

- Archive and purge MUST be linked! (security / generally)
- Whilst normally for business data archive and purge would be done periodically
  - Daily/weekly/bi-weekly
  - For audit we may want to move the data faster but this is for security reasons
  - Often this is not archive or purge – bear this in mind as then it becomes a strategy rather than an archiving and purging policy
- Archive and purge for security data must relate to the business, regulatory, IT-Sec
  - Not just business as per normal archive and purge
  - i.e. we cannot use the same rules as business as we have the risk of a DBA/hacker/? changing or deleting audit data
- BUT if we move the audit data we often make it much harder to read
- Consider; what are the retention requirements?
- If audit data is archived
  - What are reporting requirements?
  - Can the data be read easily?
  - Does the application rely on any data - i.e. who/when/ links to users
  - Consider MLJ issues with audit - often audit is linked to users

An Example Of AUD$

- We are going to discuss SYS.AUD$ audit
- Is there an archive and purge policy?
- Is the audit trail acted upon
- We will then discuss how archive and purge may work and some issues
- We will also discuss the security of the archive process itself – WHY?
- Finally for this section we will look at some issues as to why, regulatory, restore etc

Is There Archiving In Place?

```
SQL Plus
SQL> select count(*) from dba_audit_trail;

  COUNT(*)
----------
      2286

1 row selected.

SQL> select min(timestamp),max(timestamp)
  2  from dba_audit_trail;

MIN(TIMES MAX(TIMES
--------- ---------
15-OCT-07 08-JUL-08

1 row selected.

SQL> select created from v$database;

CREATED
---------
03-MAR-08

1 row selected.

SQL>
```

Anyone?

AUD$ Analysis

- Our example shows
  - No archive and purge
  - Therefore probably no plan to archive and purge
  - Most likely no one is looking at the audit data
- Let's discuss how to archive:
  - Summary data?
  - Archive all data?
  - Poll, or real time
  - Export or text dump or different

Remember to apply to all audit data not just AUD$

- Syslog in 10gR2 and 11gR1
  - Not archive, not purge, real time, hard to report on, missing data, hard to reload and use, easier to actually archive; paradoxically

Security Of Audit Archive / Purge

- Security of audit data itself
- Protect the mechanism
- Protect the data
- Plus protect the interfaces – i.e. all copies
- More?
- SPECIAL CONCERNS FOR audit and logging
  - Move quick to prevent loss/change
  - Size of data is very specific to site/use of system/used to store the archive. Don't ignore sizing

Are There Issues?

- If you keep audit data – i.e. archive it do you need to keep everything it refers to?
  - Will the audit trail be useful with or without connected data
  - What if some data changes?
  - More?
- Often no tools to read data off line
- Audit and logs are designed to be read in-situ not in archive state
- Correlation becomes difficult if not all the security data is archived or in the same place
- Tampering – real time movement of audit is not an archive solution

More Issues

- Broken links
- Reload – some requirements call for this in my experience
- (**Let's emphasise this**) An additional requirement of archive for audit is the need to move the data off the production system in real time to prevent abuse.
  - This is not really an archive requirement
  - This is not archiving as the data is simply stored elsewhere and should be archived and purged from there
- Difficult to read off line (as we said, no tools) –
  - Could store in same format? And use internal tools (SQL)
  - Perhaps link to live? To avoid all audit being archived

Archive And Purge Policy

- A policy must be created
  - Should be a document
  - Could be a plan?
  - Could be a set of tools
- Any Oracle database examples out there?
- O'Reilly Oracle Security book - http://safari.oreilly.com/1565924509/ch10-18168 has very, very, very basic policy ideas
  - It is simple – too simple
  - It is very old – Oracle 7 / 8.0 days
- Cannot find a free policy on the net specifically aimed at security

The Policy

- What should the policy include?
- Unfortunately there is not real "*one size fits all*"
- Decide what to archive / purge
- Decide on frequency – include security issues
- Decide on the format
- Decide on the mechanism
- Decide on re-load / read
- Document it
- Remember at all times the audit data may contain actual data

Audit The Archive And Purge

- The archive and purge process must also be audited
- Access to archived security audit data must be audited
- We need to audit the audit
  - Does this require an ever decreasing circle
  - i.e. audit the audit that audits the audit that audits the audit…… ad infinitum
  - NO, we must use strong RBAC at the next level

Security Of Archive And Purge

- The second aspect of security in relation to archive and purge is the security of the business archive and purge processes
- Security of archive in a business context must be considered
- Data is data no matter where you "**steal**" it from!
- Often I see no consideration of this
- BUT this is a general issue in my opinion

Concerns

- SECURITY CONCERNS OF NORMAL PURGE AND ARCHIVE (i.e. it's a copy of the real data, special data, any data
- Protections in database are often lost when the data moves in the database and outside it….
- This is a practical high-level discussion of security of archive and purge of security data
- Create a plan
  - As above in the first section
  - Ensure that the archive process is considered in the same light as the rest of the data security

Issues

- Recycle bin for archived data
- Flashback includes archived data
- Archive logs include archived data
- **There is a pattern emerging!**
- The security risks increase due to extra data copies and movements of data
- Links to production to support archive open up potential "***leaks***"
- Audit is detached from the archive data (if audit exists)
  - i.e. the audit may be under a different process or not at all as discussed
- Links broken that link to core audit data
- If archive is on line (Applimation for example) then its an additional copy of data and must be protected in the same manner as live
- In the case of security be careful removing data related to the audit, i.e. user/roles/responsibilities
  - Links can break, change…

Audit Archive And Purge

- Auditing the business archive and purge processes
- These processes may be used to "**steal**" data or delete data / evidence
- Remember the above discussions though, this audit must be integrated

Conclusions

- I wanted to focus on two things specifically
  - The archiving of security data
  - The security of archived data
- We also discussed what Oracle provides
- My conclusions
  - Not many sites archive security data at the database level
  - In my experience data not in the core tables is not often secured, this includes archived data
- Let's change these observations

Any Questions?

Contact - Pete Finnigan

PeteFinnigan.com Limited
9 Beech Grove, Acomb
York, YO26 5LD

Phone: +44 (0) 1904 791188
Mobile: +44 (0) 7742 114223
Email: pete@petefinnigan.com