Audit Management with DBMS_AUDIT_MGMT

Stefan Oehrli
Senior Consultant &
Discipline Manager Security
stefan.oehrli@trivadis.com

Zürich, March 24, 2011

trivadis
makes IT easier.

Agenda

- Introduction
- Oracle database audit in nutshell
- The DBMS_AUDIT_MGMT package
- Manage audit trail and audit records
- Restrictions and known issues
- Availability and licensing
- Conclusion

Introduction

- General activities within an Oracle can be logged with Oracle audit facilities
  - Standard Auditing to audit on Statement-, System-, Privilege- or Object-Level
  - Fine Grained Auditing (FGA) to audit more detailed e.g who queried the salary column on the emp table where salaries are > 10’000 CHF
- Depending on what is audited a high amount of data can be created
- But how are the audit records maintained?
  - Oracle Audit Vault
  - Custom scripts

Agenda

- Introduction
- Oracle database audit in nutshell
- The DBMS_AUDIT_MGMT package
- Manage audit trail and audit records
- Restrictions and known issues
- Availability and licensing
- Conclusion

Oracle database audit in nutshell

- Enable database audit with the init.ora parameter AUDIT_TRAIL
- Audit records are written to the AUDIT_TRAIL
  - OS — Audit records are written to *.aud files in AUDIT_FILE_DEST
  - XML — Audit records are written as XML files in AUDIT_FILE_DEST
  - DB — Audit Records are stored within the database (AUD$ or FGA_LOG$)
  - XML, EXTENDED — analog to XML but with extended information
  - DB, EXTENDED — analog to DB but with extended information

Oracle database audit in nutshell

- For AUDIT_TRAIL set to DB / DB,EXTENDED all records are stored in AUD$ and FGA_LOG$ respectively
  - Tables are stored in SYSTEM
  - Moving tables is not supported
  - => SYSTEM TS can get big and fragmented
- Audit records can also be written to SYSLOG or Windows Event Log => AUDIT_SYSLOG_LEVEL
- Audit of sys operation is enabled by AUDIT_SYS_OPERATION

Agenda

- Introduction
- Oracle database audit in nutshell
- The DBMS_AUDIT_MGMT package
- Manage audit trail and audit records
- Restrictions and known issues
- Availability and licensing
- Conclusion

The DBMS_AUDIT_MGMT package

- New package to manage AUDIT_TRAIL's
- Initially required by Oracle Audit Vault
- Provides a set of procedures and functions to
  - Initialize audit management infrastructure
  - Move AUD$ and FGA_LOG$ tables to an other location
  - Clean up AUDIT_TRAIL and create purge jobs
  - Set AUDIT_TRAIL properties
- Provides a set of new views
  - DBA_AUDIT_MGMT_CLEANUP_JOBS
  - DBA_AUDIT_MGMT_CLEAN_EVENTS
  - DBA_AUDIT_MGMT_CONFIG_PARAMS
  - DBA_AUDIT_MGMT_LAST_ARCH_TS

Agenda

- Introduction
- Oracle database audit in nutshell
- The DBMS_AUDIT_MGMT package
- Manage audit trail and audit records
- Restrictions and known issues
- Availability and licensing
- Conclusion

Manage audit trail and audit records

- Situation before initializing the audit management infrastructure

```
select PARAMETER_NAME, PARAMETER_VALUE, AUDIT_TRAIL
from DBA_AUDIT_MGMT_CONFIG_PARAMS
where audit_trail = 'STANDARD AUDIT TRAIL';

PARAMETER_NAME              PARAMETER_VALUE AUDIT_TRAIL
--------------------------- --------------- --------------------
DB AUDIT TABLESPACE         SYSTEM          STANDARD AUDIT TRAIL
DB AUDIT CLEAN BATCH SIZE   10000           STANDARD AUDIT TRAIL

select OWNER, SEGMENT_NAME, SEGMENT_TYPE, TABLESPACE_NAME
from DBA_SEGMENTS where SEGMENT_NAME='AUD$';

OWNER SEGMENT_NAME SEGMENT_TYPE TABLESPACE_NAME
----- ------------ ------------ ---------------
SYS   AUD$         TABLE        SYSTEM
```

Manage audit trail and audit records

- Initializing the audit management infrastructure

```
exec DBMS_AUDIT_MGMT.INIT_CLEANUP(AUDIT_TRAIL_TYPE =>
DBMS_AUDIT_MGMT.AUDIT_TRAIL_AUD_STD, DEFAULT_CLEANUP_INTERVAL => 12 /
*hours*/);
```

- New situation / location of AUD$

```
select PARAMETER_NAME, PARAMETER_VALUE, AUDIT_TRAIL
from DBA_AUDIT_MGMT_CONFIG_PARAMS
where audit_trail = 'STANDARD AUDIT TRAIL';

PARAMETER_NAME                 PARAMETER_VALUE AUDIT_TRAIL
------------------------------ --------------- --------------------
DB AUDIT TABLESPACE            SYSAUX          STANDARD AUDIT TRAIL
DB AUDIT CLEAN BATCH SIZE      10000           STANDARD AUDIT TRAIL
DEFAULT CLEAN UP INTERVAL      12              STANDARD AUDIT TRAIL

select OWNER, SEGMENT_NAME, SEGMENT_TYPE, TABLESPACE_NAME
from DBA_SEGMENTS where SEGMENT_NAME='AUD$';
OWNER SEGMENT_NAME SEGMENT_TYPE TABLESPACE_NAME
----- ------------ ------------ ---------------
SYS   AUD$         TABLE        SYSAUX
```

Manage audit trail and audit records

- Move AUD$ to a new location

```
BEGIN
  DBMS_AUDIT_MGMT.SET_AUDIT_TRAIL_LOCATION(
    AUDIT_TRAIL_TYPE => DBMS_AUDIT_MGMT.AUDIT_TRAIL_DB_STD,
    AUDIT_TRAIL_LOCATION_VALUE => 'AUDIT_DATA');
END;
/
```

- Define a archive timestamp

```
BEGIN
  DBMS_AUDIT_MGMT. SET_LAST_ARCHIVE_TIMESTAMP(
    AUDIT_TRAIL_TYPE => DBMS_AUDIT_MGMT.AUDIT_TRAIL_AUD_STD,
    LAST_ARCHIVE_TIME =>
      TO_TIMESTAMP('27-09-2010 23:29:10','DD-MM-YYYY HH24:MI:SS'));
END;
/
```

Manage audit trail and audit records

- Audit records for create session

```
select USERNAME,ACTION_NAME,EXTENDED_TIMESTAMP ,RETURNCODE
from DBA_AUDIT_SESSION order by EXTENDED_TIMESTAMP;

USERNAME   ACTION_NAME  EXTENDED_TIMESTAMP                          RETURNCODE
---------- ------------ ----------------------------------- ----------
HR         LOGON        27-SEP-10 11.28.28.036902 PM +00:00         1017
SCOTT      LOGON        27-SEP-10 11.28.34.302721 PM +00:00            0
SCOTT      LOGOFF       27-SEP-10 11.28.39.540208 PM +00:00            0
SCOTT      LOGON        27-SEP-10 11.30.13.632495 PM +00:00            0
SCOTT      LOGOFF       27-SEP-10 11.30.18.094916 PM +00:00            0
HR         LOGON        27-SEP-10 11.30.18.116640 PM +00:00        28000
8 rows selected.
```

- Purge audit records before archive timestamp

```
 DBMS_AUDIT_MGMT.CLEAN_AUDIT_TRAIL(
    AUDIT_TRAIL_TYPE => DBMS_AUDIT_MGMT.AUDIT_TRAIL_AUD_STD,
    USE_LAST_ARCH_TIMESTAMP => TRUE);
END;
/
```

Manage audit trail and audit records

- Setup a automatic clean job

```
BEGIN
  DBMS_AUDIT_MGMT.CREATE_PURGE_JOB(
    AUDIT_TRAIL_TYPE => DBMS_AUDIT_MGMT.AUDIT_TRAIL_AUD_STD,
    AUDIT_TRAIL_PURGE_INTERVAL => 24 /* hours */,
    AUDIT_TRAIL_PURGE_NAME => 'Daily_Purge_Job',
    USE_LAST_ARCH_TIMESTAMP => TRUE);
END;
/
```

- Clean job as defined above

```
select JOB_NAME,JOB_STATUS,AUDIT_TRAIL,JOB_FREQUENCY
from DBA_AUDIT_MGMT_CLEANUP_JOBS;

JOB_NAME          JOB_STAT AUDIT_TRAIL            JOB_FREQUENCY
----------------- -------- ---------------------- -------------------------
DAILY_PURGE_JOB    ENABLED  STANDARD AUDIT TRAIL FREQ=HOURLY;INTERVAL=24
```

Manage audit trail and audit records

- Rolling “Audit Window” 1-2 weeks where audit records are kept
- Enabling auditing allows to be able to review what happened during an application installation / upgrade
- Write custom scripts to archive audit records and set the archive timestamp

Agenda

- Introduction
- Oracle database audit in nutshell
- The DBMS_AUDIT_MGMT package
- Manage audit trail and audit records
- Restrictions and known issues
- Availability and licensing
- Conclusion

Restrictions and known issues

- No management of SYS audit records
  - AUDIT_SYS_OPERATION
- No management of audit records send to
  - SYSLOG
  - Windows Event Log
- A few bugs are around… as wall as bug fix (11.2.0.2)
  - SET_AUDIT_TRAIL_LOCATION does not move the lob segments
  - Audit file switches before it reaches 1k (FILE_MAXSIZE not set)
  - CLEAN_AUDIT_TRAIL should clean up entries in adx_sid.txt
  - CLEAN_AUDIT_TRAIL does not work for AUDIT_TRAIL=OS with uppercase ORACLE_SID
- *Known Issues When Using: DBMS_AUDIT_MGMT [ID 804624.1]*

Agenda

- Introduction
- Oracle database audit in nutshell
- The DBMS_AUDIT_MGMT package
- Manage audit trail and audit records
- Restrictions and known issues
- Availability and licensing
- Conclusion

Availability and licensing

- Starting with Oracle 11g R2 DBMS_AUDIT_MGMT is part of the release
- For older releases the following patch's and patch sets are available:
  - 11.1.0.7 DBMS_AUDIT_MGMT is part of the patch set
  - 10.2.0.5 DBMS_AUDIT_MGMT is part of the patch set
  - 10.2.0.4 Patch 6996030
  - 10.2.0.3 Patch 6989148
- Oracle will not support DBMS_AUDIT_MGMT version 9.2.0.x and 10.1.0.x.
- See Metalink Note *New Feature DBMS_AUDIT_MGMT To Manage And Purge Audit Information [ID 731908.1]* for more information

Availability and licensing

- Oracle Audit Vault License is required for 10.2.0.x – 11.1.0.x
- According to Metalink Note 731908.1 it is not supported to use DBMS_AUDIT_MGMT outside of Oracle Audit Vault
- But what about 11.2.0.x?

  "… I now have some further feedback from the audit development team, and can confirm this package is available with SE and EE starting with 11.2. No further license is required."

Agenda

- Introduction
- Oracle database audit in nutshell
- The DBMS_AUDIT_MGMT package
- Manage audit trail and audit records
- Restrictions and known issues
- Availability and licensing
- Conclusion

Conclusion

- Simplifies the management of audit trail and audit records
- Set of procedure to create a custom audit strategy
- Does not simplify the process of setting up the audit
  - What (Objects, Statements,…) do we have to audit
  - Create of audit statements (e.g.. `audit xyz;`)
- Does not simplify the analysis of the audit data

Many thanks!